

Resource Center Documentação



1

| 1. NGFW - HISTORICO DE REVISOES |
|---|
| 2. UIM - INI RODUÇÃO |
| 2.2 UTM - Verificação de ambiente para instalação |
| 2.3 UTM - Sobre o Guia do Administrador |
| 3. UTM - ARQUITETURA |
| 4. UIM - INSTALAÇÃO |
| 4.2 UTM - Iniciando Máguina Virtual - Primeiro Acesso |
| 4.3 UTM - Gravações das imagens nos pendrives |
| 5. UTM - CONFIGURAÇÃO DE EXCEÇÃO |
| 6. UTM - ASSISTENTE DE INSTALAÇÃO |
| 8. UTM - INTERFACE WEB |
| 8.1 Acessando a Interface Web – Blockbit UTM 48 |
| 8.2 Acessando a Interface Web – Licenciamento |
| 9 UTM - OPERAÇÃO BÁSICA |
| 10. UTM - MENU DE PERFIL DO USUÁRIO |
| 10.1 UTM - Profile |
| 10.2 UTM - Logout |
| 11. UTM - FILA DE COMANDOS |
| 12. UTM - NOTIFICAÇÕES |
| 13. UTM - MENU DE OBJETOS |
| 14. UTM - MUNITOR |
| 14.1.1 Dashboard - Widgets |
| 14.2 Monitor - Live Sessions |
| 14.2.1 Live Sessions - Connections |
| 14.2.1.1 Connections - Componentes |
| 14.2.1.3 Connections - Web |
| 14.2.2 Live Sessions - Users |
| 14.2.2.1 Users - Componentes |
| 14.2.3 Live Sessions - VPN |
| 14.3 Monitor - Traffic Monitor |
| 14.3.1 Traffic Monitor - Network |
| 14.4 Monitor - System Status |
| 14.4.1 System Status - Widgets |
| 14.5 Monitor - Security Events |
| 14.5.1 Security Events - Sessions |
| 14.5.1.2 Sessions - Expandir Sessions |
| 14.5.1.3 Sessions - Query Editor |
| 14.5.2 Security Events - Authentication |
| 14.5.2.2 Authentication - Description |
| 14.5.2.3 Authentication - Rules |
| 14.5.3 Security Events - VPN |
| 14.5.3.1 VPN - Query Editor |
| 14.6 Monitor - Diagnostics |
| 14.6.1 Diagnostics - Packet Capture |
| 14.0.2 Diagnostics - Category Lookup |
| 14.7.1 Monitor - Reports - Menu de Ações |
| 14.7.1.1 Monitor - Reports - Menu de ações - Create Report |
| 14.7.1.1.1 Exemplos - Criação de Reports |
| 14.7.1.2 Monitor - Reports - Colunas |
| 15. UTM - ANALYZER |
| 15.1 UTM - Firewall |
| 15.1.1 UTM - Firewall – Geolocation |
| 15.1.3 UTM - Firewall – Top User |
| 15.1.4 UTM - Firewall – Top Service |
| 15.1.5 UTM - Firewall – Top Source |
| 15.2 NGFW - Web Filter |
| 15.2.1 UTM - Web Filter - Allowed Sites e History |
| 15.2.2 UTM - Web Filter - Denied Sites e History |
| 15.2.5 UTM - Web Filter - History Categories - Total Traffic e Total Hits |
| 15.2.5 UTM - Web Filter - History Domains - Total Traffic e Total Hits |
| 15.2.6 UTM - Web Filter - History Profiles - Total Traffic e Total Hits |
| וט. <i>ב.ר</i> וווע - web Fliter - Lop Categories 211 |

| 15.2.8 UTM - Web Filter - Top Content Type | 2 | 212 |
|--|---|--|
| 15.2.9 UIM - Web Filter - Top Domains | | 214 |
| 15.2.10 UTM - Web Filter - Top Domains by Time | | 210 |
| 15.2.12 UTM - Web Filter - Top Users | | 210 |
| 15.2.13 UTM - Web Filter - Total Traffic e History | | 20 |
| 15.2.14 UTM - Web Filter - Users - Total Traffic e Total Hits | 2 | 221 |
| 15.3 UTM - Application Control | 2 | 223 |
| 15.3.1 UTM - Application Control - Allowed Application | 2 | 226 |
| 15.3.2 UTM - Application Control - Denied Application | 2 | 227 |
| 15.3.3 UTM - Application Control - History | 2 | 228 |
| 15.3.4 UTM - Application Control - Top Allowed Categories | 2 | 230 |
| 15.3.5 UTM - Application Control - Top Denied Categories | 2 | 231 |
| 15.3.6 UTM - Application Control - Top Allowed Applications | | 232 |
| 15.3.7 UTM - Application Control - Top Denied Applications | | 233 |
| 15.4 UTM - Influsion Flevenhold | | 204 |
| 15.4.2 UTM - Intrusion Prevention - Alerte by Goologation | | 230 |
| 15.4.3 UTM - Intrusion Prevention - Ministry Generation | | 241 |
| 15.4.4 UTM - Intrusion Prevention - Impact - Medium | | 245 |
| 15.4.5 UTM - Intrusion Prevention - Impact - Low | 2 | 249 |
| 15.4.6 UTM - Intrusion Prevention - Laver 3 Intrusion Protection | 2 | 253 |
| 15.4.7 UTM - Intrusion Prevention - Intrusion Classification | 2 | 256 |
| 15.4.8 UTM - Intrusion Prevention - Top Source | 2 | 258 |
| 15.4.9 UTM - Intrusion Prevention - Top Destination | 2 | 260 |
| 15.5 UTM - Threat Protection | 2 | 262 |
| 15.5.1 UTM - Threat Protection - Threats e History | 2 | 267 |
| 15.5.2 UTM - Threat Protection - Malwares e History | 2 | 268 |
| 15.5.3 UTM - Threat Protection - Geolocation | 2 | 269 |
| 15.5.4 UIM - Threat Protection - Impact - High | 2 | 270 |
| 15.5.5 UIM - Threat Protection - Impact - Medium | 2 | 272 |
| 15.5.6 UTM - Inreat Protection - Impact - Low | | 274 |
| 15.5.7 UTM - Threat Protection - Malicious IP Classification | | 270 |
| 15.5.0 UTM - Threat Protection - Top Threat types | | 279 |
| 15.5.10 JITM - Threat Protection - Ton Users by Malware | | 201 |
| 15.5.11 UTM - Threat Protection - Top Malwares | | 284 |
| 15.5.12 UTM - Threat Protection - Top Infected Domains | 2 | 285 |
| 15.5.13 UTM - Threat Protection - Top Source | 2 | 286 |
| 15 5 14 LITM - Threat Protection - Ton Destination | ~ | 000 |
| | | 200 |
| 15.6 UTM - User Behavior | | 288 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History | · · · · · · 2 · · · · · · 2 · · · · · 2 | 288 290 293 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel | | 290 293 294 |
| 15.6.2.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic | · · · · · · 2 · · · · · 2 · · · · · 2 · · · · | 290 293 294 302 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage | · · · · · 2 · · · · · 2 · · · · · 2 · · · · | 290 293 294 302 305 |
| 15.6.2.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage | · · · · · 2 · · · · · 2 · · · · · 2 · · · · | 290 293 294 302 305 306 |
| 15.6 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Web Usage | · · · · · 2 · · · · · 2 · · · · · 2 · · · · | 290 293 294 302 305 306 307 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 290 293 294 302 305 305 306 307 310 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Geolocation Information | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 290 293 294 302 305 306 307 310 313 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrast Protection 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.7 UTM - VPN | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 290 293 294 302 305 306 307 310 313 316 318 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrast Protection 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN - Traffic Usage | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 | 290 293 294 302 305 306 310 313 316 318 321 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN 15.7.2 UTM - VPN - Remote User | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 290 293 294 302 305 306 310 313 316 318 321 322 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrast Protection 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.3 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 290 293 294 302 305 306 310 313 316 318 321 322 323 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 | 290 293 294 302 305 306 310 313 316 318 321 322 323 324 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Remote User 15.7.3 UTM - VPN - Top Remote User 16. UTM - POLICIES | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 | 290 293 294 302 305 306 313 316 313 321 322 323 324 326 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16. UTM - POLICIES 16.1 Politicas IPv4 | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | 288 290 293 294 302 305 306 310 313 322 3316 3322 3323 324 3223 324 326 327 328 329 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1 Politicas IPv4 16.1.1 IPv4 - Menu de ações | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 | 288 290 293 294 302 305 306 310 313 316 322 323 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 325 325 325 325 327 327 327 327 327 327 327 327 327 327 |
| 15.6 UTM - User Behavior - History 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Remote User 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1 IPv4 - Menu de ações 16.1.1.1 IPv4 - Menu de ações - Create Group | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 | 288 290 293 294 302 306 307 310 313 316 322 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 3233 3224 3233 3224 3233 3224 3233 3234 3233 3224 3233 3234 3234 324 32 |
| 15.6 UTM - User Behavior 15.6 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrast Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1 Politicas IPv4 16.1.1 IPv4 - Menu de ações 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 2 3 | 288 290 293 294 302 305 306 307 310 313 322 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 324 3223 3231 3223 3231 3232 3233 324 325 329 329 329 329 329 329 329 329 329 329 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Intreat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.7.4 UTM - VPN - Top Remote User 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Groups 16.1.1.2 IPv4 - Menu de ações - Create Groups 16.1.1.2 IPv4 - Menu de ações - Create Groups 16.1.1.1 IPv4 - Menu de ações - Create Groups 16.1.1.2 IPv4 - Menu de ações - Create Groups | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 | 288 290 293 294 302 306 307 310 313 322 324 3223 324 3223 324 3223 324 3223 324 3230 331 333 334 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.3 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.7 UTM - VPN 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.2 IPv4 - Menu de ações - Create Groups 16.1.1.3 IPv4 - Menu de ações - Create Prolicy 16.1.1.3 IPv4 - Menu de ações - Create Prolicy 16.1.1.3 IPv4 - Menu de ações - Create Prolicy | 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 | 288 290 293 2 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.7 UTM - VPN 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Groups 16.1.1.2 IPv4 - Menu de ações - Create Groups 16.1.1.3 IPv4 - Menu de ações - Create Groups 16.1.1.3.1 Create Policy - Aba Cronerties 16.1.1.3.2 Create Policy - Aba Connection | 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 | 288 290 293 294 302 306 310 313 322 306 310 313 322 323 324 3223 324 3223 324 3223 324 323 324 323 324 323 324 323 324 324 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.3 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Web Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - My Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.7 UTM - VPN 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.2 IPv4 - Menu de ações - Create Group 16.1.1.3 IPv4 - Menu de ações - Create Policy 16.1.1.3.1 Create Policy - Aba Properties 16.1.1.3.2 Create Policy - Aba Connection | 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 | 288 290 293 294 302 306 310 313 316 312 223 324 329 330 331 333 331 333 331 333 331 333 3341 333 3341 333 3341 333 3341 335 335 335 335 335 335 335 335 335 33 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.2 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Intruston Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Intruston Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intruston Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.6.3 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Remote User 15.7.3 UTM - VPN - Remote User 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.3 I Create Group - Exemplos - Criação de Grupos 16.1.1.3 Create Policy - Aba Connection 16.1.3.3 Create Policy - Aba Roteamento | 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 | 288 290 293 294 302 306 307 316 312 322 306 307 313 322 322 322 322 322 322 322 322 322 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.5 UTM - User Behavior - Analysis Panel - Intreat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intreat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.6.3 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1 Políticas IPv4 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.3 IPv4 - Menu de ações - Create Groups 16.1.1.3 IPv4 - Menu de ações - Create Policy 16.1.1.3 Create Policy - Aba Connection 16.1.1.3 Create Policy - Aba Roteamento | 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 | 288 290 293 2 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.4 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.4 UTM - User Behavior - Analysis Panel - Network Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Netw Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Intruston Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intruston Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intruston Prevention 15.6.3 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Remote User 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.11 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.3 IPv4 - Menu de ações - Create Groups 16.1.1.3 IPv4 - Menu de ações - Create Policy 16.1.1.3 ICreate Policy - Aba Properties 16.1.1.3 Create Policy - Aba Properties 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3.6 Create Policy - Aba Roteamento | 2 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 | 288 290 293 2 |
| 15.6 UTM - User Behavior 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.2 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.5 UTM - User Behavior - Analysis Panel - Intruston Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intruston Prevention 15.6.2.6 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1 IPv4 - Menu de ações 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.3.1 Create Policy - Aba Properties 16.1.1.3.2 Create Policy - Aba Properties 16.1.1.3.2 Create Policy - Aba Properties 16.1.1.3.4 Create Policy - Aba Roteamento 16.1.1.4 IPv4 - Menu de ações - Create Policy | 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 | 288 288 290 293 293 294 302 305 303 313 313 314 3224 326 333 3341 346 357 356 365 366 365 |
| 15.6 UTM - User Behavior - History 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1 IPV4 - Menu de ações 16.1.1.1 IPV4 - Menu de ações - Create Group 16.1.1.2 IPV4 - Menu de ações - Create Groups 16.1.1.3 IPV4 - Menu de ações - Create Policy 16.1.3.3 Create Policy - Aba Properties 16.1.1.3 Create Policy - Aba Connection 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 IPV4 - Menu de ações - Criação de Políticas 16.1.1.3 IPV4 - Menu de ações - Create Policy 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 IPV4 - Menu de ações - Criação de Políticas 16.1.1.3 IPV4 - Menu de ações - Criação de Políticas 16.1.1.3 IPV4 - Menu de ações - Criação de Políticas 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 IPV4 - Menu de ações - Delete Policies 16.1.1.4 IPV4 - Menu de ações - Delete Pol | 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 | 288 2993 2993 2993 2993 2993 2993 2993 2 |
| 15.6 UTM - User Behavior - History 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Meplication Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meplication Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Geolocation Information 15.7 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16. UTM - POLICIES 16.1 Politicas IPv4 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Groups 16.1.1.3 IPv4 - Menu de ações - Create Policy 16.1.1.3 Create Policy - Aba Connection 16.1.1.3 Create Policy - Aba Connection 16.1.1.3 Create Policy - Aba Connection 16.1.1.3 Create Policy - Aba Roperties 16.1.1.3 Create Policy - Aba Roperties 16.1.1.3 Create Policy - Aba Roperties 16.1.1.3 Create Policy - Aba Advanced 16.1.1.4 IPv4 - Menu de ações - Sepand All e Collapse All 16.1.1.6 IPv4 - Menu de ações - Sepand All e Collapse All 16.1.1.6 IPv4 - Menu de ações - Sepand All e Collapse All 16.1.1.6 IPv4 - Menu de ações - Validate Policies 16.1.1.6 IPv4 - Menu de ações - Validate Policies | 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 | 288 2993 2993 2993 2993 2993 2993 2993 2 |
| 15.6 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.2 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Threat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Traffic Usage 15.7.4 UTM - VPN - Traffic Usage 15.7.4 UTM - VPN - Traffic Usage 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16. UTM - POLICIES 16. 11.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Groups 16.1.1.3 ICreate Group - Exemplos - Criação de Grupos 16.1.1.3 ICreate Policy - Aba Properties 16.1.1.3.1 Create Policy - Aba Properties 16.1.1.3.2 Create Policy - Aba Connection 16.1.1.3.4 Create Policy - Aba Roteamento 16.1.1.3.6 Exemplos - Criação de Politicas 16.1.1.4 IPv4 - Menu de ações - Delete Polices 16.1.1.4 IPv4 - Menu de ações - Delete Polices 16.1.1.3.6 Exemplos - Criação de Politicas 16.1.1.3.6 Exemplos - Criação de Politicas 16.1.1.4 IPv4 - Menu de ações - Delete Polices 16.1.1.4 IPv4 - Menu de ações - Delete Polices 16.1.1.4 IPv4 - Menu de ações - Delete Polices 16.1.1.4 IPv4 - Menu de ações - Delete Polices 16.1.1.4 IPv4 - Menu de ações - Delet | 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 | 288 2993 2903 2903 2005 205 <tr< th=""></tr<> |
| 15.6 UTM - User Behavior - History 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.2 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - Veser Behavior - Analysis Panel - Intrusion Prevention 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.4 UTM - VPN - Traffic Usage 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16. UTM - POLICIES 16.1 Politicas IPv4 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.2 IPv4 - Menu de ações - Create Groups 16.1.1.3 ICreate Policy - Aba Properties 16.1.1.3 ICreate Policy - Aba Properties 16.1.1.3 Create Policy - Aba Properties 16.1.1.3 Create Policy - Aba Properties 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Create Policy - Aba Advanced 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Evemplos - Criação de Politicas 16.1.1.4 IPv4 - Menu de ações - Create Polices 16.1.1.5 IPv4 - Menu de ações - Create Polices 16.1.1.5 IPv4 - Menu de ações - Create Polices 16.1.1.5 IPv4 - Menu de ações - Create Polices 16.1.1.6 IPv4 - Menu de ações - Create Polices 16.1.1.6 IPv4 - Menu de ações - Delete Policices 16.1.1.6 IPv4 - Menu de ações - | 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 3 | 288 2993 2903 2005 2013 2013 2013 2013 2014 2015 2015 2016 2017 2018 2019 2010 2011 2011 2012 2013 2014 2015 2016 2017 2018 2019 2010 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2019 2010 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2019 2010 2010 <tr< th=""></tr<> |
| 15.6 UTM - User Behavior - History 15.6.2 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Metwork Traffic 15.6.2.5 UTM - User Behavior - Analysis Panel - Metwork 15.6.2.5 UTM - User Behavior - Analysis Panel - Network 15.6.2.5 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.5 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.5 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN + Top Sterbeto-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1.1 PV4 - Menu de ações 16.1.1.1 PV4 - Menu de ações 16.1.1.1 PV4 - Menu de ações 16.1.1.2 IPV4 - Menu de ações - Create Group 16.1.1.3 I Create Policy - Aba Properties 16.1.1.3 I Create Policy - Aba Inspection 16.1.1.3 Evemplos - Criação de Políticas 16.1.1.4 IPV4 - Menu de ações - Delete Groups 16.1.1.3 Create Policy - Aba Inspection 16.1.1.3 Evemplos - Criação de Políticas 16.1.1.4 IPV4 - Menu de ações - Delete Policies 16.1.1.4 IPV4 - Men | 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 | 2293 2993 2905 30007 3116 32223 2223 2223 3333 3413 3457 35635 3997 9901 2023 2020 2020 2020 2020 2020 2020 20 |
| 15.6 UTM - User Behavior - History 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Policy Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Metwork Traffic 15.6.2.4 UTM - User Behavior - Analysis Panel - Metwork Traffic 15.6.2.5 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.6 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - To a femote User 15.7.3 UTM - VPN - To premote User 16.1.1 IPv4 - Menu de ações 16.1.1 IPv4 - Menu de ações 16.1.1.1 IPv4 - Menu de ações 16.1.1.2 IPv4 - Menu de ações - Create Group 16.1.1.3 IPv4 - Menu de ações - Create Policy 16.1.1.3 Create Policy - Aba Properties 16.1.1.3.1 Create Policy - Aba Properties 16.1.1.3.2 Create Policy - Aba Roteamento 16.1.1.3.4 Create Policy - Aba Roteamento 16.1.1.3.5 Create Policy - Aba Roteamento 16.1.1.3.6 Exemplos - Criação de Politicas 16.1.1.4 IPv4 - Menu de ações - Delete Policies 16.1.1.4 IPv4 - Menu de ações - Delete Policies 16.1.1.4 IPv4 - Menu de ações - Delete Policies 16.1.1.4 IPv4 - Menu de ações - Create Policy 16.1.1.3.6 Exemplos - Criação de Politicas 16.1.1.4 IPv4 - Menu de ações - Create Policy 16.1.1.4 IPv4 - Menu de ações - Create Policy 16.1.1.4 IPv4 - Menu de ações - Valdate Policies 16.1.1.4 IPv4 - Menu de ações - Valdate Policies 16.1.1.4 IPv4 - Menu de ações - Valdate Policies 16.1.1.4 IPv4 - Menu de ações - | 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 | 2890 2993 2993 2902 2005 2007 2007 2007 2007 2007 2007 20 |
| 15.6 UTM - User Behavior - History 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.1 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.5 UTM - User Behavior - Analysis Panel - Meb Usage 15.6.2.6 UTM - User Behavior - Analysis Panel - Intreat Protection 15.6.2.6 UTM - User Behavior - Analysis Panel - Intreat Protection 15.6.2.6 UTM - User Behavior - Geolocation Information 15.7.1 UTM - VPN - Traffic Usage 15.7.2 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1.1.1 IPV4 - Menu de ações 16.1.1.1 IPV4 - Menu de ações - Create Group 16.1.1.1 IPV4 - Menu de ações - Create Group 16.1.1.1 IPV4 - Menu de ações - Create Group 16.1.1.1 IPV4 - Menu de ações - Create Group 16.1.1.2 IPV4 - Menu de ações - Create Group 16.1.1.3 Create Policy - Aba Connection 16.1.3.3 Create Policy - Aba Connection 16.1.3.3 Create Policy - Aba Advanced 16.1.1.3.4 Create Policy - Aba Advanced 16.1.1.3 IPV4 - Menu de ações - Veate Policies 16.1.1.3 Create Policy - Aba Advanced 16.1.1.3 IPV4 - Menu de ações - Create Group 16.2.1.1 IPV4 - Menu de ações - Create Group 16.2.1.1 IP | 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 | 2293 2993 2993 2993 2993 2993 2993 2993 |
| 15.6 UTM - User Behavior - History 15.6.1 UTM - User Behavior - Analysis Panel 15.6.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.2 UTM - User Behavior - Analysis Panel - Network Traffic 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Application Usage 15.6.2.3 UTM - User Behavior - Analysis Panel - Meto Usage 15.6.2.4 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.5 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.2.5 UTM - User Behavior - Analysis Panel - Intrusion Prevention 15.6.3 UTM - VPN - Traffic Usage 15.7.1 UTM - VPN - Traffic Usage 15.7.3 UTM - VPN - Remote User 15.7.3 UTM - VPN - Romote User 15.7.3 UTM - VPN - Top Site-to-Site Connections 15.7.4 UTM - VPN - Top Remote User 16.1 Politicas IPv4 16.1.1 IPv4 - Menu de ações - Create Group 16.1.1.1 IPv4 - Menu de ações - Create Group 16.1.1.3 IPv4 - Menu de ações - Create Groups 16.1.1.3 IPv4 - Menu de ações - Create Policy 16.1.1.3 IPv4 - Menu de ações - Create Policy 16.1.1.3 Create Policy - Aba Properties 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Evretholicy - Aba Roteamento 16.1.1.3 Evretholicy - Aba Roteamento 16.1.1.3 IPv4 - Menu de ações - Create Policies 16.1.1.3 IPv4 - Menu de ações - Delete Policies 16.1.1.3 IPv4 - Menu de ações - Create Roup 16.1.1.3 IPv4 - Menu de ações - Delete Policies 16.1.1.3 Evretholicy - Aba Roteamento 16.1.1.3 Create Policy - Aba Roteamento 16.1.1.3 Evretholicy - Aba Roteamento 16.1.1.3 Evretholicy - Aba Roteamento 16.1.1.3 IPv4 - Menu de ações - Create Group 16.2.1.1 IPv6 - Menu de ações - Create Group 16.2.1.1 IPv6 - | 2 2 | 2890 29300 2930 2930 |

| | 16.2.1.3.3 IPv6 - Create Policy - Aba Inspection | 423 |
|-----|---|--------------|
| | 16.2.1.3.4 IPv6 - Create Policy - Aba Routing | . 425 |
| | 16.2.1.4.Dr/c - Create Policy - Aba Advanced | 428 |
| | 16.2.1.5 IPV6 - Menu de ações - Efecer folicies | 430 |
| | 16.2.1.6 IPV6 - Colunas | 433 |
| 17. | UTM - SERVICES | 435 |
| | 17.1 UTM - Services - Firewall | 436 |
| | 17.1.1 Firewall - Zone Protection | . 438 |
| | 17.1.1.1 Zone Protection - Botao de Criação | 439 |
| | 17.1.1.1.1 Exemple 1 - Acesso a menato SSH - pela WAN "Internet" – (Suporte Blockhit) | . 443 446 |
| | 17.1.1.2 Zone Protection - Columas | 449 |
| | 17.1.1.3 Zone Protection - Coluna Services | 450 |
| | 17.1.1.4 Zone Protection - Remove | 455 |
| | 17.1.1.5 Firewall - Port Forwarding | 456 |
| | 17.1.1.5.1 Port Forwarding - Botao de Adição | . 458 478 |
| | 17.1.1.5.3 Port Forwarding - Criar Port Forwarding | 479 |
| | 17.1.1.5.4 Port Forwarding - Excluir Port Forwarding | 492 |
| | 17.1.1.5.5 Port Forwarding - Colunas | . 494 |
| | 17.1.2 Firewall - General Settings | 497 |
| | 17.2 NGFW - Services - Proxy | . 512 |
| | 17.2.1 FIOXy - FIOXY SERVICES | 514 516 |
| | 17.2.1.2 Proxy HTTP | 517 |
| | 17.2.1.3 Proxy FTP | 519 |
| | 17.2.1.4 Proxy SSH | 520 |
| | 17.2.1.5 Proxy SMTP | . 525 |
| | 17.2.1.6 Proxy POP | . 527 |
| | 17.2.1.7 PT0XY - SSL Inspection - Menu de acões | . 529 530 |
| | 17.2.1.7.2 Proxy - SSL Inspection - Mend de S | . 539 |
| | 17.3 UTM - Services - Web Cache | 540 |
| | 17.3.1 Web Cache - Cache | 542 |
| | 17.4 UTM - Services - Application Control | . 544 |
| | 17.4.1 Services - Application Control - Menu de ações | . 546 547 |
| | 17.4.1.2 Services - Application Control - Menu de ações - Delete Profile | 554 |
| | 17.4.2 Services - Application Control - Colunas | 556 |
| | 17.4.3 Application Control - Lista de Categorias | . 557 |
| | 17.5 UTM - Services - Web Filter | . 638 |
| | 17.5.1 Web Filter - Profiles - Monu de Acões | . 640 642 |
| | 17.5.1.1 Web Filter - Profiles - Menu de Ações - Create Profile | 643 |
| | 17.5.1.1.2 Web Filter - Profiles - Menu de Ações - Delete Profile | 654 |
| | 17.5.1.2 Web Filter - Profiles - Colunas | 656 |
| | 17.5.2 Web Filter - Settings | . 657 |
| | 17.6 UIM - Services - Intrusion Prevention | 659 |
| | 17.6.1 Intrusion Flevenion - Aba Allowed Addresses - Manu de Acões | 662 |
| | 17.6.1.1.1 Allowed Addresses - Menu de Acões - Create | . 663 |
| | 17.6.1.1.2 Allowed Addresses - Menu de Ações - Delete | 665 |
| | 17.6.1.1.3 Allowed Addresses - Menu de Ações - Import Allowed Addresses list | 667 |
| | 17.6.2 Intrusion Prevention - Aba Blocked Addresses list | 669 |
| | 17.6.2.1 Initiusion Prevention - Aba blocked Addresses - Menu de Ações | . 070 671 |
| | 17.6.2.1.2 Blocked Addresses - Menu de Ações - Delete | 673 |
| | 17.6.2.1.3 Blocked Addresses - Menu de Ações - Import Blocked Addresses | 675 |
| | 17.6.3 Intrusion Prevention - Aba Custom Signatures | 677 |
| | 17.6.4 Intrusion Prevention - Aba PCAP | . 679 |
| | 17.6.5 Intrusion Prevention - Aba Profiles | 680 |
| | 17.6.5.1.1 Intrusion Prevention - Aba Profiles - Create Profile | . 682 |
| | 17.6.5.1.2 Intrusion Prevention - Aba Profiles - Delete Profile | 691 |
| | 17.6.5.2 Intrusion Prevention - Aba Profiles - Colunas | . 693 |
| | 17.6.6 Intrusion Prevention - Aba Quarantine | . 694 |
| | 17.6.6.1 Quarantine - Menu de Ações - Timeout | . 695 696 |
| | 17.6.6.1.2 Quarantine - Menu de Ações - Move to Allowed Addresses List | . 697 |
| | 17.6.6.1.3 Quarantine - Menu de Ações - Move to Blocked Addresses List | . 698 |
| | 17.6.6.1.4 Quarantine - Menu de Ações - Remove | 699 |
| | 17.6.6.2 Quarantine - Colunas | 700 |
| | 1/./ UIM - Services - Threat Protection | . 701 |
| | 17.7.1 11ileal Flotection - Aba Flotiles - Menu de ações | 703 |
| | 17.7.1.1.1 Threat Protection - Profiles - Menu de Ações - Create Profile | . 705 |
| | 17.7.1.1.2 Threat Protection - Profiles - Menu de Ação - Delete Profile | 713 |
| | 17.7.1.2 Threat Protection - Profiles - Colunas | 715 |

| 17.7.2 Threat Protection - Aba Settings | 716 |
|---|-----|
| 17.7.3 Threat Protection - Aba Quarantine | 718 |
| 17.7.4 Inreat Protection - Aba ATP Sandbox | 721 |
| 17.0 UTM - Setvices - SD-WAN | 726 |
| 17.8.1 SD-WAN - Abd i foldes - Menu de acões | 727 |
| 17.8.1.1.1 SD-WAN - Profiles - Menu de Acões - Create Profile | 728 |
| 17.8.1.1.2 SD-WAN - Profiles - Menu de ações - Delete Profile | 753 |
| 17.8.1.2 SD-WAN - Profiles - Colunas | 755 |
| 17.8.2 SD-WAN - Aba Settings | 756 |
| 17.8.2.1 SD-WAN - Settings - Menu de Ações | 757 |
| 17.8.2.1.1 SD-WAN - Settings - Menu de Ações - Create Service | 758 |
| 17.8.2.1.2 SD-WAN - Settings - Menu de Ações - Delete Service | 760 |
| 17.6.2.2 SD-WAIN - Settlings - Columbas | 763 |
| 17.8.3 1 SD-WAN - Configurar Interface Tunnel | 764 |
| 17.8.3.2 SD-WAN: Configurar VPN | 776 |
| 17.8.3.3 SD-WAN: Configurar SD-WAN | 788 |
| 17.8.3.4 SD-WAN: Adicionar Policies | 793 |
| 17.8.3.4.1 SD-WAN Regras de NAT por Mac Address | 800 |
| 17.8.3.5 SD-WAN: Validação da Configuração do SD-WAN | 806 |
| 17.9 NGFW - Serviços - DHCP | 809 |
| 17.9.1 DHCP - Aba Leases IPv4 | 811 |
| 17.9.2 DHCP - Aba Leases IPV6 | 813 |
| 17.9.3 DHCF - Add Reidy IPV4 | 017 |
| 17.9.4 DHCF - Aba Nelay IFVO | 819 |
| 17.9.5.1 DHCP Server - Settings | 821 |
| 17.9.5.2 DHCP Server - Ranges | 824 |
| 17.9.5.3 DHCP Server - Radius | 827 |
| 17.9.5.4 DHCP Server - Static Addresses | 830 |
| 17.9.6 DHCP - Aba Server IPv6 | 833 |
| 17.10 UTM - Services - DNS | 835 |
| 17.10.1 DNS - Settings | 837 |
| 17.10.2 UNS - Realifect | 042 |
| 17.11 0 INI - Services - DDNS (UMIDIS) | 8/5 |
| 17 11 2 DDNS - Denu de arções | 848 |
| 17.11.2.1 DDNS - Menu de Acões - Select all | 849 |
| 17.11.2.2 DDNS - Menu de Ações - Remove | 850 |
| 17.11.3 DDNS - Colunas | 851 |
| 17.12 UTM - Services - VPN IPSEC | 852 |
| 17.12.1 VPN IPSEC - Aba Túneis | 855 |
| 17.12.1.1 Tuneis - Botao Acrescentar | 857 |
| 17.12.1.2 Turnels - Botao Editar | 858 |
| 17.12.12.1 UIIIIelis - Full-Westi 17.12.1 2.0 Tunnals - Star | 867 |
| 17.12.1.2.1 Junnels - Site | 875 |
| 17.12.13 Túneis - Colunas | 884 |
| 17.12.2 VPN IPSEC - Aba Acesso Remoto | 885 |
| 17.12.2.1 Acesso Remoto - IKEv1 | 889 |
| 17.12.2.2 Acesso Remoto - IKEv2 | 891 |
| 17.12.2.3 Acesso Remoto - Rede | 896 |
| 17.12.2.4 Remote Access - Cryptography | 897 |
| 17.12.2.5 Acesso Remoto - Avançado | 902 |
| 17.12.2.0 Exempto - Autenticação Device/User/Password com cient de VPN delauit do Windows | 903 |
| 17.12.3 VTNT GLO - Aba 1 allover | 929 |
| 17.12.3.2 Failover - Colunas | 933 |
| 17.12.4 Padrões Relacionados ao Protocolo IPSec | 934 |
| 17.12.5 Troubleshooting das VPNs | 938 |
| 17.13 UTM - Services - VPN SSL | 941 |
| 17.13.1 VPN SSL - Criptografia e Autenticação | 944 |
| 17.13.2 VPN SSL - Lista de aplicações no acesso VPN SSL | 945 |
| 17.13.3 VFN SSL - Add Selver | 940 |
| 17.13.3.1 VFN SSL - Authentication | 0/Q |
| 17.13.3.3 VPN SSL - Tunnels | 950 |
| 17.13.3.4 VPN SSL - Advanced | 952 |
| 17.13.3.5 VPN SSL - Cryptography | 953 |
| 17.13.4 VPN SSL - Aba Client | 954 |
| 17.13.4.1 Client - Painel Authentication | 956 |
| 17.13.4.2 Client - Painel Servers | 957 |
| 17.13.4.3 Client - Painel Advanced | 958 |
| 17.13.5 VFN 55L - Aba Portal | 959 |
| 17.13.5.1 ГОЛАІ - КОР | 961 |
| 17.13.5.2 Portal - SSH | 964 |
| 17 12 5 4 Dorth WED | 965 |

| | 17.13.5.5 Portal - SMB | 966 |
|-----|--|------|
| | 17 13 5 6 Portal - Definição e Gerencimanto de Permissões | 970 |
| | 17.12.5.7 Dottal Dominique o VCNI SSI | 071 |
| | 17.15.5.7 Folial - Negulisius ua VFN SSE | 070 |
| | 17.13.6 VPN SSL - Estabelecendo Acesso VPN SSL Portal | 972 |
| | 17.14 UTM - Services - NG VPN | 975 |
| | 17.14.1 NGFW - Services - NGVPN Client | 979 |
| 18. | UTM - SETTINGS | 988 |
| | 18.1 UTM - Settings - Network | 989 |
| | 10.1.1 Notwork Solitings | 001 |
| | 10.1.1 Network - Settings | 991 |
| | 18.1.1.1 Network - Settings - Botoes de Ação | 993 |
| | 18.1.2 Network - Interfaces | 996 |
| | 18.1.2.1 Interfaces - Suporte a MPLS | 997 |
| | 18.1.2.2 Interfaces - Interface Ethernet | 1003 |
| | 18.1.2.3 Interfaces - Conexão 3G/4G/I TE | 1008 |
| | 18 1 2 3 1 Examples - Derêmetres de Conevão 3G//G// TE | 1014 |
| | | 4047 |
| | 18.1.2.4 Interfaces - Botao de Adição | 1017 |
| | 18.1.2.4.1 Adição de Interface - ALIAS | 1018 |
| | 18.1.2.4.2 Adição de Interfaces - Virtual (MAC VLAN) | 1021 |
| | 18.1.2.4.3 Adicão de Interfaces - VLAN | 1026 |
| | 18 1 2 4 4 Adição de Interfaces - DSI | 1031 |
| | 10.1.2.4.5 Adiože de Interfeces – LAC (Link Agreentien) | 4004 |
| | 18.1.2.4.5 Adição de Internaces - LAG (Link Aggregation) | 1034 |
| | 18.1.2.4.6 Adiçao de Interfaces - Bridge | 1050 |
| | 18.1.2.4.7 Adição de Interfaces - Tunnel | 1055 |
| | 18.1.2.5 Interfaces - Menu de acões | 1060 |
| | 18.1.2.5.1 Interfaces - Menu de Acões - Select All | 1061 |
| | 19.1.2.5.2 Interfaces Manu de Aciaco Lindeta | 1062 |
| | | 1002 |
| | 18.1.2.5.3 Interfaces- Menu de Ações - Remove | 1063 |
| | 18.1.2.6 Interfaces - Colunas | 1065 |
| | 18.1.2.7 Fragmentação de Pacotes e MTU | 1066 |
| | 18.1.3 Network - Static Routing | 1069 |
| | 19.1.2.1 Statio Douting Datão do Adiaão | 1070 |
| | 18.1.3.1 Stalic Routing - Botao de Adição | 1070 |
| | 18.1.3.1.1 Static Routing - MPLS | 1072 |
| | 18.1.3.1.2 Dynamic Routing - ECMP | 1114 |
| | 18.1.3.2 Static Routing - Menu de acões | 1146 |
| | 18 1 3 2 1 Static Routing - Menu de Acões - Select All | 1147 |
| | 10.1.0.2.1 Otatie Routing - Menu de Ayões - Deleti Ali | 4440 |
| | 18.1.3.2.2 Static Routing - Menu de Ações - Remove | 1148 |
| | 18.1.3.3 Static Routing - Colunas | 1150 |
| | 18.1.4 Network - Dynamic Routing | 1151 |
| | 18.1.4.1 Dynamic Routing - Habilitação e Configuração | 1152 |
| | 18 1 5 Naturat - IDv6 Sattings | 1156 |
| | 10.1.5 Network 11 vo Gettings | 4450 |
| | 18.1.5.1 IPv6 Settings - IPv6 Settings | 1158 |
| | 18.1.5.2 IPv6 Settings - Router Advertising | 1159 |
| | 18.1.5.3 IPv6 Settings - IP address Mapping | 1162 |
| | 18.1.6 Network - Traffic Shaping | 1163 |
| | 18 1 6 1 Traffic Shaping - Priorities Definition | 1164 |
| | 10.4 C. J. Traffic Charging, Malacidade de Deumland, et Jaland | 4400 |
| | 18.1.6.2 Trainc Snaping - Velocidade de Download e Opload | 1100 |
| | 18.1.6.3 Traffic Shaping - Velocidade de Download e Upload - Exemplo Link DSL e IP | 1168 |
| | 18.2 UTM - Settings - Authentication | 1170 |
| | 18.2.1 Authentication - Conceitos Gerais | 1172 |
| | 18.2.2 Authentication - Aba Users | 1174 |
| | | 1175 |
| | 10.2.2.1 Users - Dunians | 4470 |
| | 10.2.2.1.1 USERS - Domains - Add Domain | 11/6 |
| | 18.2.2.1.2 Users - Domains – Actions Menu | 1181 |
| | 18.2.2.1.3 Users - Domains - Colunas | 1184 |
| | 18.2.2.2 Users - Groups | 1188 |
| | 18 2 2 2 1 Users - Groups – Add Group | 1180 |
| | 18.2.2.2.1 Borr - Groupe - Actione Manu | 1100 |
| | | 1192 |
| | 18.2.2.2.3 Users - Groups - Colunas | 1195 |
| | 18.2.2.3 Users - MFA | 1198 |
| | 18.2.2.4 Users - Users | 1202 |
| | 18 2 2 4 1 Users - Users - Import User | 1203 |
| | 19.2.4.2 Users Users - did User | 1200 |
| | | 1205 |
| | 18.2.2.4.3 Users - Users - Actions Menu | 1207 |
| | 18.2.2.4.4 Users - Users - Colunas | 1213 |
| | 18.2.3 Authentication - Aba Servers | 1217 |
| | 18 2 3 1 Servers - Integração de domínio e sincronismo Windows AD/I DAP | 1218 |
| | 18.2.3.2 Sanjare - Windows Sanjar | 1224 |
| | 10.2.9.2 Gervers - Williauws Gerver | 1221 |
| | 18.2.3.2.1 WINDOWS Server - Adicionar Servidor | 1225 |
| | 18.2.3.2.2 Windows Server – Connection Test | 1230 |
| | 18.2.3.2.3 Windows Server - Edit Server | 1231 |
| | 18 2 3 2 4 Windows Server – Remove Server | 1232 |
| | 18.2.3.2.5 Windows Conver – Kuno betweel | 1000 |
| | | 1233 |
| | 10.2.3.3 Servers - LDAP Server | 1235 |
| | 18.2.3.3.1 LDAP Server - Edit Server | 1236 |
| | 18.2.3.3.2 LDAP Server - Adicionar Servidor | 1237 |
| | 18.2.3.3 LDAP Server - Remove Server | 1242 |
| | 18 2 3 3 4 I DAP Server - Connection Test | 12/2 |
| | 18.2.3.5 LDAD Sonyer - Super Internal | 1044 |
| | 10.2.3.3.3 LDAF SEIVEL - SYNCHILEIVÄL | 1244 |
| | | 4040 |

| 18.2.3.4.1 TACACS+ Server – Edit Server | 1247 |
|--|--|
| 18.2.3.4.2 TACACS+ Server – Add Server | 1248 |
| 18.2.3.4.3 TACACS+ Server – Connection Test | 1250 |
| 18.2.3.4.4 TACACS+ Server – Delete Server | 1252 |
| 18.2.3.5 Servers - RADIUS Server | 1253 |
| 18.2.3.5.1 RADIUS SERVER – Radius Single Sign ON | 1254 |
| 18.2.3.5.2 RADIUS SERVER – Add Server | 1256 |
| 18.2.4 Authentication - Synchronism | 1258 |
| 18.2.4.1 Authentication - Synchronism - Filial | 1261 |
| 18.2.5 Authentication - Aba Rules | 1262 |
| 18.2.5.1 Rules - Menu de Ações | 1263 |
| 18.2.5.1.1 Rules - Menu de Ações - Create | 1264 |
| 18.2.5.1.2 Rules - Menu de Ações - Delete | 1267 |
| 18.2.5.2 Rules - Colunas | 1268 |
| 18.2.6 Authentication - Aba Portal | 1269 |
| 18.2.6.1 Portal – Add Profile | 1270 |
| 18.2.6.1.1 Add Profile - Properties | 1273 |
| 18.2.6.1.2 Add Profile – Personal Information | 1274 |
| 18.2.6.1.3 Add Profile – Social Login | 1275 |
| 18.2.6.1.4 Add Profile – Available Options | 1306 |
| 18.2.6.1.5 Add Profile – Terms of Use | 1307 |
| 18.2.6.1.6 Add Profile – Customize Logo | 1308 |
| 18.2.6.2 Portal – Menu de Ações | 1309 |
| 18.2.6.2.1 Portal - Menu de Ações - Select e Select All | 1310 |
| 18.2.6.2.2 Portal - Menu de Ações - Remove | 1311 |
| 18.2.6.3 Portal - Colunas | 1312 |
| 18.2.6.4 Portal de Autenticação | 1313 |
| 18.2.6.4.1 Gerenciamento do portal de autenticação | 1321 |
| 18.2.7 Authentication - Aba Settings | 1323 |
| 18.2.7.1 Settings - Certificates | 1325 |
| 18.2.7.1.1 Autenticação de Dois Fatores – 2FA (Two Factor Authentication) | 1327 |
| 18.2.7.1.2 Como funciona a autenticação 2FA (Two Factor Authentication) | 1328 |
| 18.2.7.1.3 Estabelecendo acesso por autenticação 2FA | 1330 |
| 18.2.7.1.4 Configuração 2FA | 1333 |
| 18.2.7.2 Settings - Sessions | 1335 |
| 18.2.7.3 Settings - Permissions | 1336 |
| 18.3 UIM - Settings - Administration | 1337 |
| 18.3.1 Administration - Aba Settings | 1339 |
| | 1 3/11 |
| 18.3.1.1 Settings - Administration - Certificates | 12/2 |
| 18.3.1.1 Settings - Administration - Certificates | 1342 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Ports | 1342 1350 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions | 1342 1350 1351 1352 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators | 1342 1350 1351 1352 1356 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2 1 Administrators - Users | 1342 1350 1351 1352 1356 1357 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles | 1342 1350 1351 1352 1356 1357 1360 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management | 1342 1350 1351 1352 1356 1357 1360 1363 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administrators - Users 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Audit Logs | 1342 1350 1351 1352 1356 1357 1360 1363 1366 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Blocked Addresses | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Addresses 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Addresses 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - DDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administrators - Profiles 18.3.4 Administration - Aba Central Management 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.1.1 License - Data License | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Versions 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Central Management 18.3.4 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.1.2 License - Data License 18.4.1.2 License - Signatures | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - DDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Central Management 18.3.4 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.1.2 License - Data License 18.4.2 System - Aba Updates | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 |
| 18.3.1.1 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Ports 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.4 Administration - Aba Central Management 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.12 License - Signatures 18.4.2 System - Aba Updates 18.4.2.1 Updates - Hotfixes & Patches | 1341 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - DAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.2.3 Administration - Aba Central Management 18.3.4 Administration - Aba Audit Logs 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.2 System - Aba Updates 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1.1 Hotfixes | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 |
| 18.3.1.1 Settings - Administration - LDAP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Vortiles 18.3.2.1 Administrators - Profiles 18.3.2.2 Administration - Aba Central Management 18.3.4 Administration - Aba Audit Logs 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.1.2 License - Data License 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1.1 Hotfixes 18.4.2.1.2 Patches | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 |
| 18.3.1.1 Settings - Administration - LDAP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.1.2 License - Data License 18.4.2 System - Aba Updates 18.4.2.1.1 Hotfixes 18.4.2.1.2 Patches 18.4.2.1.3 Rollback | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1373 1374 1375 1377 1378 1379 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - DAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administrators - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.2 Administration - Aba Central Management 18.3.4 Administration - Aba Audit Logs 18.3.5 Administration - Aba Audit Logs 18.3.6 Administration - Aba Audit Logs 18.3.7 Administration - Aba Audit Logs 18.3.8 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 License - Data License 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1.2 Patches 18.4.2.1 Updates - Proxy Server 18.4.2.2 Updates - Proxy Server 18.4.2.2 Updates - Proxy Server | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - Dats 18.3.1.3 Settings - Administration - Sessions 18.3.1.4 Settings - Administration - TACACS+ 18.3.2.4 Administrators - Users 18.3.2.4 Administrators - Versions 18.3.2.4 Administrators - Profiles 18.3.2.4 Administration - Aba Central Management 18.3.4 Administration - Aba Audit Logs 18.3.5 Administration - Aba Blocked Addresses 18.4.1 System - Aba License 18.4.1.2 License - Data License 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1.2 Hotfixes 18.4.2.1.2 Hotfixes 18.4.2.1.3 Rollback 18.4.2.2 Updates - Proxy Server 18.4.2.3 Updates - Hopfare | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1380 1381 |
| 18.3.1.1 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administrators - TACACS+ 18.3.2 Administrators - Users 18.3.2.2 Administrators - Vsers 18.3.2.2 Administrators - Profiles 18.3.3 Administrators - Profiles 18.3.4 Administrators - Aba Central Management 18.3.5 Administration - Aba Central Management 18.3.6 Administration - Aba Blocked Addresses 18.4.1 System - Aba Blocked Addresses 18.4.1.1 License - Data License 18.4.2.1 Updates - Hoffixes & Patches 18.4.2.1 Updates - Hoffixes & Patches 18.4.2.1.2 Rollback 18.4.2.1.2 Rollback 18.4.2.1.3 Rollback 18.4.2.3 Updates - Proxy Server 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1381 |
| 18.3.1.1 Settings - Administration - LDAP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administrators - Sessions 18.3.1.5 Settings - Administrators - TACACS+ 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Audit Logs 18.3.5 Administration - Aba Audit Logs 18.4 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1.1 License - Data License 18.4.2.1 Updates - Data License 18.4.2.1.1 Hoffixes 18.4.2.1.2 Patches 18.4.2.1.2 Patches 18.4.2.2 Updates - Proxy Server 18.4.2.3 Updates - Update 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups 18.4.3 Deakups - Device Backups 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1383 1385 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - IDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - TACACS+ 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.1 Administrators - Viers 18.3.2.2 Administrators - Viers 18.3.2 Administration - Aba Central Management 18.3.4 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.1.2 License - Dignatures 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Hotfixes 18.4.2.1.2 Patches 18.4.2.1.3 Rollback 18.4.2.2 Updates - Proxy Server 18.4.2.3 Updates - Proxy Server 18.4.2.3 Updates - Proxy Server 18.4.2.3 Updates - Proxy Server 18.4.3.1 Backups - Device Backups 18.4.3.2 Backups - Settings 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups 18.4.3 Updates - Server 18.4.3 Updates - Device Backups 18.4.3 Updates - Settings | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1383 1385 1387 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administrations 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.1 Administrators - Profiles 18.3.2 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Blocked Addresses 18.3.5 Administration - Aba Blocked Addresses 18.4.1 System - Aba License 18.4.1 System - Aba License 18.4.1.1 License - Data License 18.4.2 System - Aba Updates 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Proxy Server 18.4.2.3 Updates - Update 18.4.3.1 Backups - Device Backups 18.4.3.2 Backups - Settings 18.4.3.2 Backups - Settings | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1377 1378 1379 1380 1381 1385 1387 1390 1390 |
| 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.1.5 Settings - Administrators 18.3.2 Administrators - Users 18.3.2 Administrators - Users 18.3.2 Administrators - Profiles 18.3.3 Administrator - Aba Central Management 18.3.4 Administration - Aba Elocked Addresses 18.4.1 System - Aba License 18.4.1 License - Data License 18.4.2 System - Aba Updates 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Patches 18.4.2.1 admines 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Update 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Update 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Update 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Update 18.4.3 Updates - Update 18.4.4 System - Aba Storages 18.4.4 Storage - SME 18.4.4 Storage - SME | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1377 1378 1379 1380 1381 1383 1385 1387 1390 1391 |
| 18.3.1.1 Settings - Administration - LDAP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administrators 18.3.2 Administrators - Vsers 18.3.2 Administrators - Vsers 18.3.2 Administrator - Aba Administrators 18.3.2 Administrators - Profiles 18.3.2 Administration - Aba Addresses 18.3.4 Administration - Aba Blocked Addresses 18.4.1 System - Aba License 18.4.1 System - Aba License 18.4.2 System - Aba Updates 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Patches 18.4.2.1 Patches 18.4.2.3 Updates - Proxy Server 18.4.3 System - Aba Backups 18.4.3 Backups - Device Backups 18.4.3 Express 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups 18.4.3 System - Aba Backups 18.4.3 Librage - SMB 18.4.4 Storage - SMB | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1383 1385 1387 1390 1391 1393 1395 |
| 18.3.1.1 Settings - Administration - Certificates 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2 Administration - Aba Central Management 18.3.4 Administration - Aba Central Management 18.3.4 Administration - Aba Addiresses 18.3.5 Administration - Aba Blocked Addresses 18.4 JTM - Settings - System 18.4.1 License - Data License 18.4.2 System - Aba Udit Logs 18.4.2 System - Aba Udites & Patches 18.4.2.1 Updates - Hortixes & Patches 18.4.2.1 Updates - Hortixes & Patches 18.4.2.1 Updates - Update 18.4.2.3 Updates - Update 18.4.3 System - Aba Blockups 18.4.3 System - Aba Blockups 18.4.3 System - Aba Blockups 18.4.4.3 Storage - SMB 18.4.3 Storage - SHB 18.4.4 Storage - SHE | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1377 1378 1379 1380 1381 1385 1387 1390 1391 1393 1395 |
| 18.3.1.1 Settings - Administration - DAP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administrators 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administration - Aba Central Management 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Addresses 18.3.5 Administration - Aba Central Management 18.3.4 Administration - Aba Central Management 18.3.5 Administration - Aba Central Management 18.3.6 Administration - Aba Blocked Addresses 18.4.1 System - Aba License 18.4.1 System - Aba License 18.4.2 System - Aba Updates 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Dipdates 18.4.2.1 Dipdates 18.4.2.1 Dipdates 18.4.2.3 Updates - Update 18.4.3 System - Aba Backups 18.4.3 Storage - SMB 18.4.4 Storage - SMB 18.4.4 Storage - SH 18.4.4 Storage - Disc 18.4.4 Storage - Disc | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1377 1378 1379 1380 1381 1385 1387 1390 1391 1393 1395 1398 |
| 18.3.1.1 Settings - Administration - Cortificates 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Porfiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Bocked Addresses 18.4.5 Administration - Aba Bicked Addresses 18.4.4 Diffuses - Data License 18.4.1 System - Aba License 18.4.2 System - Aba Updates 18.4.2.1 Updates - Hoftixes & Patches 18.4.2.1 Updates - Hoftixes & Patches 18.4.2.1 Updates - Hoftixes & Patches 18.4.2.1 System - Aba Backups 18.4.2.2 Updates - Proxy Server 18.4.2.3 Updates - Update 18.4.2.4 Suptates - Device Backups 18.4.3.1 Backups - Device Backups 18.4.3.2 Backups - Settings 18.4.4.3 Storage - SMB 18.4.4.3 Storage - SMB 18.4.4.3 Storage - SMB 18.4.4.3 Storage - SMB | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1383 1385 1387 1390 1391 1393 1395 1398 1402 |
| 18.3.1.1 Settings - Administration - Cortificates 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Secons 18.3.2 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Profiles 18.3.3 Administration - Aba Audit Logs 18.3.4 Administration - Aba Blocked Addresses 18.4.1 Microsse - Data License 18.4.1 License - Signatures 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.2 Updates - Proxy Server 18.4.2.3 Updates - Update 18.4.3.1 Backups - Device Backups 18.4.3.1 Backups - Device Backups 18.4.3.2 Backups - Settings 18.4.3.3 Backups - Settings 18.4.4.3 Storage - SISH 18.4.4.3 Storage - SISH 18.4.4.3 Storage - SISH 18.4.4.3 Storage - SISH 18.4.4.3 Storage - SISK 18.4.4.3 Storage - SISH 18.4.4.3 Storage - SISK | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1383 1385 1387 1390 1391 1393 1395 1398 1402 |
| 18.3.1.1 Settings - Administration - Uchrificates 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - Sessions 18.3.2.1 Administration - Aba Administrators 18.3.2.1 Administrators - Users 18.3.2.2 Administrators - Verofiles 18.3.3 Administrators - Na Central Management 18.3.3 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 System - Aba License 18.4.1.1 License - Data License 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Proxy Server 18.4.2.2 Updates - Update 18.4.2.3 Updates - Update 18.4.3.4 Backups - Device Backups 18.4.3.5 Backups - Settings 18.4.4.3 Updates - Update 18.4.3.4 Storage - SIM 18.4.4.3 Storage - SIM 18.4.4.3 Storage - SIM 18.4.4.3 Storage - SIM 18.4.4.3 Storage - SIM 18.4.5.3 Logging - Rot | 1341 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1383 1385 1387 1390 1391 1393 1395 1398 1402 1403 1404 1405 |
| 18.3.1.1 Settings - Administration - UchP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Ports 18.3.1.4 Settings - Administration - Ports 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administration - TACACS+ 18.3.2 Administrators - Users 18.3.2.1 Administrators - Profiles 18.3.2 Administrators - Verofiles 18.3.2 Administrators - No a Central Management 18.3.3 Administration - Aba Audit Logs 18.3.5 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1 License - Data License 18.4.1 License - Signatures 18.4.2 System - Aba License 18.4.2 Lipdates - Hotfixes & Patches 18.4.2 Lipdates - Hotfixes & Patches 18.4.2 Lipdates - Hotfixes & Patches 18.4.2.1 Lipdates - Hotfixes & Patches 18.4.2.1 Jeatches 18.4.2.1 Updates - Voy Server 18.4.2.3 Updates - Update 18.4.3.4 System - Aba Backups 18.4.3.1 Backups - Device Backups 18.4.3.2 Updates - NFS 18.4.4.3 Storage - NFS 18.4.4.3 Storage - NFS 18.4.4.4 Storage - NFS 18.4.4.5 Storage - NFS < | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1381 1383 1385 1387 1390 1391 1393 1395 1398 1402 1403 1404 5 1408 |
| 18.3.1.1 Settings - Administration - LOAP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.1.5 Settings - Administrators 18.3.2.1 Administrators - Vorsi 18.3.2.1 Administrators - Vorsi 18.3.2.1 Administrators - Vorsi 18.3.2.1 Administrators - Vorsi 18.3.2.2 Administrators - Profiles 18.3.3 Administrators - Aba Central Management 18.3.4 Administration - Aba Blocked Addresses 18.3.5 Administration - Aba Blocked Addresses 18.4.1 System - Aba License 18.4.1 License - Data License 18.4.1.2 License - Signatures 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.2 Updates - Proxy Server 18.4.2.3 Updates - Update 18.4.3.4 Sotape - Subridges 18.4.3.5 Updates - Update 18.4.4.3 Storage - SHB </th <th>1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1377 1378 1377 1378 1377 1378 1377 1378 1375 1385 1385 1385 1385 1398 1402 1403 1404 1405</th> | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1377 1378 1377 1378 1377 1378 1377 1378 1375 1385 1385 1385 1385 1398 1402 1403 1404 1405 |
| 18.3.1.1 Settings - Administration - IDAP 18.3.1.2 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administrators - Aba Administrators 18.3.2 Administrators - Versions 18.3.2 Administrators - Profiles 18.3.2 Administrators - Profiles 18.3.3 Administrators - Near Control Management 18.3.4 Administratori - Aba Central Management 18.3.5 Administration - Aba Blocked Addresses 18.4.1 System - Aba Blocked Addresses 18.4.1 System - Aba License 18.4.1 System - Aba Updates 18.4.2.1 Updates - Indixe & Patches 18.4.2.1 Updates - Indixes & Patches 18.4.2.3 Updates - Update 18.4.2.4 Updates - Proxy Server 18.4.3.5 Updates - Update 18.4.3.6 Updates - Update 18.4.3.8 Updates - Update 18.4.4.3 Updates - Update 18.4.4.4 Storage - SINB 18.4.4.3 Updates - Update 18.4.4 | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1377 1378 1377 1378 1377 1378 1377 1378 1379 1380 1381 1383 1385 1385 1398 1402 1403 1404 1405 1408 1415 1417 |
| 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.5 Settings - Administration - TACACS+ 18.3.1.5 Settings - Administrators 18.3.1.4 Settings - Administrators 18.3.2.1 Administrators - Profiles 18.3.2.4 Administrators - Profiles 18.3.3 Administration - Aba Central Management 18.3.4 Administration - Aba Central Management 18.3.5 Administration - Aba Central Management 18.3.6 Administration - Aba Central Management 18.3.7 Administration - Aba Blocked Addresses 18.4 UTM - Settings - System 18.4.1.1 License - Data License 18.4.1.2 License - Signatures 18.4.2.1 Updates - Hottixes & Patches 18.4.2.1 Updates - Hottixes & Patches 18.4.2.1 a Rollback 18.4.2.1 Clobes - Signatures 18.4.2.1 Updates - Hottixes & Patches 18.4.2.1 Detitizes - Proxy Server 18.4.2.3 Updates - Update 18.4.3.1 Backups - Device Backups 18.4.3.2 Backups - Settings 18.4.4.1 Storage - SMB 18.4.4.3 Storage - SMB 18.4.4.3 Storage - SSH 18.4.4.3 Storage - SSH 18.4.4.4 Storage - SSH 18.4.5.1 Lingração com Elastiflow 18.4.6.1 Notifications via Email | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1374 1375 1377 1378 1379 1380 1371 1378 1377 1378 1377 1378 1377 1378 1379 1380 1381 1393 1395 1398 1402 1403 1404 1405 1405 1405 |
| 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.4 Settings - Administration - TACACS+ 18.2.2 Administrators - No error 18.3.2.1 Administrators - Profiles 18.3.2.1 Administrators - Profiles 18.3.2.4 Administrators - Profiles 18.3.3 Administration - Aba Cantral Management 18.3.4 Administration - Aba Audit Logs 18.3.5 Administration - Aba Audit Logs 18.4 JTM - Settings - System 18.4.1 Settings - System 18.4.1.1 License - Data License 18.4.1.2 License - Signatures 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Hotfixes & Patches 18.4.2.1 Updates - Hotfixes 18.4.2.1 Updates - Hotfixes 18.4.2.1 Updates - Hotfixes 18.4.2.2 Updates - Proy Server 18.4.2.3 Updates - Proy Server 18.4.3.3 Backups - Device Backups 18.4.3.4 Storage - SSH 18.4.4.3 Excups - SSH 18.4.4.3 Storage - SSH 18.4.5.1 Logging - Rotation 18.4.5.1 Logging - Rotation 18.4.5.1 Logging - Rotation 18.4.5.1 Updates - Integrations 18.4.6.2 Notifications in Email 18.4.6.3 Notifications in SIMMP | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1383 1377 1378 1377 1378 1379 1380 1381 1393 1395 1398 1402 1403 1404 1405 1408 1417 1420 1421 |
| 18.3.1.2 Settings - Administration - LDAP 18.3.1.3 Settings - Administration - Ports 18.3.1.3 Settings - Administration - Sessions 18.3.1.5 Settings - Administration - TACACS+ 18.3.2 Administrations - Vessions 18.3.2.1 Administrators - Users 18.3.2.4 Administrators - Profiles 18.3.4 Administration - Aba Education - Aba Educations 18.3.4 Administration - Aba Audit Logs 18.3.5 Administration - Aba Audit Logs 18.3.4 Administration - Aba Audit Logs 18.3.5 Administration - Aba Audit Logs 18.3.4 Administration - Aba Blocked Addresses 18.4.1 System - Aba Ulcense 18.4.1.1 License - Data License 18.4.2.1 Updates - Hottixes & Patches 18.4.2.2 Updates - Proxy Server 18.4.2.3 Rollback 18.4.3.4 Backups - Device Backups 18.4.3.4 Backups - Settings 18.4.4.5 Storage - SNH 18.4.4.5 Storage - SNH 18.4.4.5 Storage - SNH 18.4.5.1 Logging - Rotation 18.4.5.1 Logging - Rotation 18.4.5.1 Logging - Rotation 18.4.5.1 Logging - Forwarding 18.4.5.1 Logging - Forwarding 18.4.5.1 Logging - Forwarding 18.4.5.1 Logging - Rotation 18.4.5.1 Logging - Forwarding 18.4.5.1 Logging - Rotation 18.4.5.1 Logging - Forwarding 18.4.5.1 Logging - Forwarding 18.4.6.1 Notifications in Email 18.4.6.2 Notifications via Email 18.4.6.2 Notifications via Email 18.4.6.2 Notifications via Email 18.4.6.3 Nullis a Blockbit | 1342 1350 1351 1352 1356 1357 1360 1363 1366 1367 1368 1369 1370 1373 1374 1375 1377 1378 1379 1380 1371 1383 1374 1375 1380 1381 1383 1395 1390 1391 1393 1395 1398 1402 1403 1404 1405 1415 1417 1420 |

| | 1430 |
|--|--|
| 18.4.7.1 Topologia de rede - Modo H.A. | 1432 |
| 18.4.7.2 Considerações importantes no modo H.A. | 1433 |
| 18.4.7.3 Configuração do modo H.A. no dispositivo principal | 1434 |
| 18.4.7.3.1 High Availability - Heartbeat #1 | 1436 |
| 18.4.7.3.2 High Availability - Heartbeat #2 | 1437 |
| 18.4.7.3.3 Tigh Availability – Teal/Deal #3 | 1438 |
| 10.4.7.3.4 Filgh Availability - Information | 1439 |
| 18.4.7.4. Vizzard de configuração de dispositivo H.A. socundário | 1440 |
| 18.4.7.5 Example - Configuração de USPOSITIVO T.A. Securidano | 1441 |
| 18.4.7.5 L Configuração de H.A. Cluster Primário | 1440 |
| 18.4.7.5.2 Configuração de H.A Cluster Secundário e Sincronismo | 1459 |
| 18 4 7 5 3 Configuração de H A - Validação das Configurações | 1464 |
| 18.4.7.6 IPS em modo transparente | 1467 |
| 18.4.7.7 IPS em modo transparente Inline | 1468 |
| 18.4.7.8 Bypass do IPS | 1469 |
| 18.4.7.8.1 Configurações de Bypass em uma estrutura H.A. | 1470 |
| 18.4.8 System - Aba Virtual Domains | 1472 |
| 18.5 UTM - Settings - Maintenance | 1474 |
| 18.5.1 UTM - Maintenance - All Files | 1476 |
| 18.5.2 UTM - Maintenance - Temporary | 1477 |
| 18.5.3 UTM - Maintenance - Quarantine | 1478 |
| 18.5.4 UTM - Maintenance - PCAP | 1479 |
| 18.5.5 UTM - Maintenance - Logs | 1480 |
| 18.5.6 UTM - Maintenance - Statistics | 1482 |
| 18.5.7 UTM - Maintenance - Cache | 1483 |
| 18.5.8 UTM - Maintenance - Reports | 1484 |
| 18.6 UTM - Settings - Certificates | 1485 |
| 18.6.1 Certificates - Entendendo o funcionamento SSL | 1487 |
| 18.6.2 Certificates - Aba Authorities | 1488 |
| 18.6.2.1 Authorities - Local CA | 1489 |
| 18.6.2.2 Authorities - Remote CA | 1491 |
| 18.6.3 Certilicates - Add Services | 1490 |
| 10.0.3.1 Services - Bota Aucional | 1497 |
| 19.6.4 Confliction Ab Lloser | 1490 |
| 10.0.4 Cettilitates - Abd Users | 1500 |
| 18.6.4.2 Ulers - Instalando um Certificado de Usuário | 1502 |
| 18.65 Certificates - Aba Revolution | 1511 |
| 18.6.5.1 Aba Revokation - Importar Lista de Revogação | 1513 |
| | |
| 18.7 UTM - Settings - Objects | 1514 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses | 1514 1516 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas | 1514 1516 1518 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping | 1514 1516 1518 1519 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações | 1514 1516 1518 1519 1520 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object | 1514 1516 1518 1519 1520 1521 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações 18.7.1.2.2 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group | 1514 1516 1518 1519 1520 1521 1529 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object | 1514 1516 1518 1519 1520 1521 1529 1531 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2 Content | 1514 1516 1518 1519 1520 1521 1529 1531 1533 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.2 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações 18.7.2.1 Contents - Menu de ações 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações 18.7.2.1.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações 18.7.2.1.1 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Delete Object | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 1540 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Delete Object 18.7.2.1.2 Contents - Menu de ações - Delete Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Delete Object 18.7.2.1.2 Contents - Menu de ações - Delete Object 18.7.2.1.2 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Object Manping | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 1540 1542 1542 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.2 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Object Mapping 18.7.2.3 Dictionaries | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 1540 1542 1544 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.2 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Colunas 18.7.3 Dictionaries - Colunas 18.7.3 1 Dictionaries - Colunas | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 1540 1542 1543 1544 1545 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.2 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Menu de ações - Delete Object 18.7.3.1 Dictionaries - Colunas 18.7.3.1 Dictionaries - Colunas 18.7.3.1 Dictionaries - Colunas 18.7.3.1 Dictionaries - Object Mapping | 1514 1516 1518 1519 1521 1521 1523 1533 1533 1533 1535 1538 1542 1544 1544 1545 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Object Mapping 18.7.3 Dictionaries - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Object Mapping | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 1540 1542 1543 1544 1545 1546 1547 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Create Object 18.7.2.2 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.2 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.2 Contents - Colunas 18.7.3.2 Dictionaries - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações 18.7.3.2 Dictionaries - Menu de ações 18.7.3.2 Dictionaries - Menu de ações | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 1540 1542 1543 1544 1545 1546 1547 1548 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Create Group 18.7.2.2 Addresses - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações 18.7.2.1.2 Content - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.1.3 Contents - Object Mapping 18.7.3.1 Dictionaries - Colunas 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object | 1514 1516 1518 1519 1520 1521 1529 1531 1533 1534 1535 1538 1540 1542 1543 1544 1545 1546 1547 1548 1547 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.2 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Create Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.1.4 Contents - Object Mapping 18.7.3.1 Dictionaries - Colunas 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações 18.7.3.2 Dictionaries - Menu de ações 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object | 1514 1516 1518 1519 1520 1521 1529 1533 1534 1535 1538 1540 1542 1543 1544 1545 1546 1547 1548 1546 1547 1548 1565 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Create Group 18.7.2.4 Addresses - Menu de ações - Create Object 18.7.2.3 Addresses - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2.1 Contents - Menu de ações - Delete Object 18.7.2.2.1 Contents - Menu de ações - Delete Object 18.7.2.2.1 Contents - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.4 Schedules | 1514 1516 1518 1519 1520 1521 1533 1534 1535 1538 1540 1542 1543 1544 1545 1546 1547 1565 1567 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Menu de ações 18.7.1.2 Addresses - Menu de ações 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Create Object 18.7.2 Content 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Crea | 1514 1514 1518 1519 1520 1521 1533 1534 1533 1534 1543 1544 1543 1544 1545 1546 1547 1548 1563 1565 1567 1568 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Content 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Create Object 18.7.2.2 Contents - Object Mapping 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Object | 1514 1514 1518 1519 1520 1521 1533 1534 1533 1534 1543 1544 1545 1546 1547 1548 1565 1567 1568 1569 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.2.2 Addresses - Menu de ações - Create Object 18.7.2.3 Addresses - Menu de ações - Create Object 18.7.2.1.1 Contents - Menu de ações - Delete Object 18.7.2.1.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Object Mapping 18.7.3.1.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1.1 Schedules - Menu de ações - Create Group 18.7.4.1.2 Schedules - Menu de ações - Create Group 18.7.4.1.2 Schedules - Menu de ações - Create Group | 1514 1514 1518 1519 1520 1521 1533 1534 1538 1535 1535 1535 1540 1542 1543 1544 1546 1547 1548 1563 1567 1568 1569 1571 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.1.2 Contents - Menu de ações - Create Group 18.7.2.2 Contents - Menu de ações - Create Group 18.7.2.2 Contents - Object Mapping 18.7.2.2 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 | 1514 1514 1518 1520 1521 1529 1531 1533 1534 1540 1542 1543 1544 1545 1544 1545 1547 1548 1563 1567 1568 1567 1568 1571 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses - Colunas 18.7.1.1 Addresses - Colunas 18.7.1.2 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.2 Addresses - Menu de ações - Create Group 18.7.2.2 Addresses - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.1 Contents - Menu de ações - Create Group 18.7.2.1.1 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.2 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Sch | 1514 1514 1518 1519 1520 1521 1523 1534 1533 1534 1540 1542 1543 1544 1545 1546 1547 1548 1565 1567 1568 1567 1568 1567 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses - Colunas 18.7.1.1 Addresses - Colunas 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.3 Addresses - Menu de ações - Create Group 18.7.2.2 Addresses - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Create Object 18.7.2.1.3 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1.3 Schedules - Menu de ações - Create Group 18.7.4.1.3 Schedules - Menu de ações - Create Group 18.7.4.1.3 Schedules - Menu de ações - Create Group 18.7.4.1.3 Schedules - Menu de ações - Create Group 18.7.4.1.3 Schedules - Menu de ações - Delete Object 18.7.4.2.1 Schedules - Menu de ações - Delete Object 18.7.4.2.1 Schedules - Menu de ações - Create Group 18.7.4.2.1 Schedules - Menu de ações - Create Group 18.7.4.2.1 Sch | 1514 1514 1518 1519 1520 1521 1523 1534 1533 1534 1540 1542 1543 1544 1545 1544 1545 1546 1547 1565 1567 1568 1567 1569 1571 1573 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.2 Addresses - Menu de ações 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Create Group 18.7.2.1.2 Addresses - Menu de ações - Create Object 18.7.2.1.2 Addresses - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Create Object 18.7.2.1.2 Contents - Menu de ações - Delete Object 18.7.2.2.1 Contents - Menu de ações - Delete Object 18.7.3.2.1 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.2 Dictionaries - Menu de ações - Create Group 18.7.3.2.2 Dictionaries - Menu de ações - Create Group 18.7.3.2.1 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Group 18.7.3.2.3 Dictionaries - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.2 Sch | 1514 1514 1518 1519 1520 1521 1533 1534 1533 1534 1542 1543 1544 1545 1544 1545 1546 1547 1568 1567 1568 1567 1571 1573 1575 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses 18.7.1.1 Addresses - Colunas 18.7.1.2 Addresses - Menu de ações 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.2.1 Addresses - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Object Mapping 18.7.4.2 Schedules - O | 1514 1514 1518 1519 1520 1521 1531 1533 1534 1535 1538 1540 1542 1543 1544 1545 1544 1545 1546 1547 1568 1567 1578 1576 1577 |
| 18.7 UTM - Settings - Objects 18.7.1.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Group 18.7.1.2.3 Addresses - Menu de ações - Delete Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.2 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Object Mapping 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.2 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.3.2.1 Dictionaries - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.2 Schedules - Menu de ações - Create Group 18.7.4.2 Schedules - Menu de ações - Create Group 18.7.4.2 Schedules - Object Mapping 18.7.4.2 Schedules - Object Map | 1514 1514 1516 1518 1519 1520 1521 1533 1534 1535 1538 1540 1542 1543 1544 1545 1546 1547 1568 1567 1576 1577 1578 1578 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Group 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.2.3 Addresses - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Object Mapping 18.7.2.1 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.4.1 Dictionaries - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.5.2 Schedules - Colunas 18.7.5.2 Schedules - Colunas 18.7.5.1 Services - Colunas 18.7.5.1 Services - Object Mapping<td>1514 1514 1516 1518 1519 1520 1521 1533 1534 1535 1534 1545 1546 1547 1548 1569 1577 1578 1576 1577 1578</td> | 1514 1514 1516 1518 1519 1520 1521 1533 1534 1535 1534 1545 1546 1547 1548 1569 1577 1578 1576 1577 1578 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Group 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Object Mapping 18.7.3.1 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.3.2 Dictionaries - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.2 Schedules - Menu de ações - Create Group 18.7.4.2 Schedules - Menu de ações - Create Group 18.7.4.2 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Group 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Menu de ações - Create Object 18.7.5.1 Services - Object Mapping 18.7.5.2 Services - Colunas 18.7.5.2 Services - M | 1514 1514 1516 1518 1520 1521 1523 1524 1533 1534 1535 1535 1535 1536 1542 1543 1544 1543 1544 1545 1567 1568 1569 1571 1578 1577 1578 1579 1580 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Group 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.1.2 Addresses - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Create Group 18.7.2.1 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Menu de ações - Delete Object 18.7.2.2 Contents - Object Mapping 18.7.3.2 Dictionaries - Colunas 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Object Mapping 18.7.5.2 Services - Menu de ações - Create Object 18.7.5.1 Services - Object Mapping 18.7.5.2.1 Ser | 1514 1514 1516 1518 1519 1520 1521 1523 1534 1535 1538 1540 1542 1543 1544 1545 1547 1548 1563 1567 1568 1577 1568 1577 1578 1577 1578 1579 1580 1571 1578 |
| 18.7 UTM - Settings - Objects 18.7.1 Addresses - Colunas 18.7.1.1 Addresses - Object Mapping 18.7.1.2.1 Addresses - Venu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.1.2.1 Addresses - Menu de ações - Create Object 18.7.2.2 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.1 Contents - Menu de ações - Create Object 18.7.2.2 Contents - Menu de ações - Create Object 18.7.2.2 Contents - Menu de ações - Create Object 18.7.2.2 Contents - Object Mapping 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Object Mapping 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.3.2 Dictionaries - Menu de ações - Create Object 18.7.4.1 Dictionaries - Menu de ações - Create Object 18.7.4.1 Dictionaries - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.1 Schedules - Menu de ações - Create Object 18.7.4.2 Schedules - Object Mapping 18.7.5.2 Services - Colunas 18.7.5.2 Services - Object Mapping 18.7.5.2 Services - Menu de ações - Create Object 18.7.5.2 Services - | 1514 1514 1516 1518 1519 1520 1521 1523 1533 1534 1540 1542 1543 1544 1545 1546 1547 1548 1567 1568 1577 1578 1579 1578 1579 1578 1579 1578 |

| | 18.7.6.1.1 Times - Menu de ações - Create Object | i95 |
|-----------------------------|---|-------------|
| | 18.7.6.1.2 Times - Menu de ações - Delete Object | 198 |
| 18 7 | 10.7.0.1.5 Times - Melliu de ações - Cleate Group | 300 |
| 10.7 | 10.2 Times - Columas 10 | 302 |
| 19 LITM - SNAPS | HOT | 304 |
| 20 UTM - TERMI | NAI 16 | 306 |
| 21. UTM - INTERI | ACE BLOCKBIT CLI - LINHA DE COMANDOS | 307 |
| 21.1 UTM - [a | rp] | 511 |
| 21.2 UTM - [a | rping] 16 | 513 |
| 21.3 UTM - [c | onfigure-bgp] | 514 |
| 21.4 UTM - [c | onfigure-ospf] | 515 |
| 21.5 UTM - [c | onfigure-ospf6] | 516 |
| 21.6 UTM - [c | onfigure-pim] | 517 |
| 21.7 UTM - [c | onfigure-rip] | 19ز |
| 21.8 UTM - [c | onfigure-rip6] 16 | 20ز |
| 21.9 UTM - [c | onfigure-syslog] | 521 |
| 21.10 UTM - | constrack] | 522 |
| 21.11 UTM - | datej | 524 |
| 21.12 UTM - | debug-atpj 10 | 026 |
| 21.13 UTM - | debug-aumj | 21 |
| 21.14 UTM - | debug-dirlp] | 320 |
| 21.15 UTM - | ueoug-upij 10 Jachura-events] | 320 |
| 21.10 UTM - | debug-firewall | 331 |
| 21.18 UTM - | debug-hal 16 | 332 |
| 21.19 UTM - | debug-ppp] | 333 |
| 21.20 UTM - | debug-sdwan] | 34 |
| 21.21 UTM - | debug-smtp-proxy] | 36 |
| 21.22 UTM - | debug-sync] | 37 |
| 21.23 UTM - | debug-threats] | 38 |
| 21.24 UTM - | debug-vpn] | ;39 |
| 21.25 UTM - | debug-webfilter] | 540 |
| 21.26 UTM - | debug-web] | j41 |
| 21.27 UTM - | algj |)4Z |
| 21.28 UTM - | losable-ogpj | 240 |
| 21.29 UTM - | uisable-ospij dicable-nim] | 340 |
| 21.30 UTM - | uisable-pinij disable-rini | 348 |
| 21.37 UTM - | disable-sin] 16 | 349 |
| 21.33 UTM - | disable-snmp] 16 | 350 |
| 21.34 UTM - | enable-bgp] | 551 |
| 21.35 UTM - | enable-ospf] | i52 |
| 21.36 UTM - | enable-pim] | 53 |
| 21.37 UTM - | enable-rip] | 54ز |
| 21.38 UTM - | enable-root] | 555 |
| 21.39 UTM - | enable-sip] | 56 |
| 21.40 UTM - | enable-snmp] | 157 |
| 21.41 UTM - | etnicolj | 109 |
| 21.42 UTIVI - | exil] | 200 |
| 21.43 UTM - | 100snj 10 | 363 |
| 21.44 UTM - | 16 fsckl | 364 |
| 21.46 UTM - | fwrecovervl 16 | 365 |
| 21.47 UTM - | fwreload] | 666 |
| 21.48 UTM - | grep] | 67 |
| 21.49 UTM - | help] | 68 |
| 21.50 UTM - | history] | 69 |
| 21.51 UTM - | host] | 70ز |
| 21.52 UTM - | hostname] | 571 |
| 21.53 UTM - | ifconfig] 16 | 572 |
| 21.54 UTM - | Irstat] | 574 775 |
| 21.55 UTM - | 10stat] | 276 |
| 21.50 UTM - | loiesti ini | 377 |
| 21.57 UTM - | ابر) المحماد] | 378 |
| 21.59 UTM - | nponoj inlisti | 379 |
| 21.60 UTM - | iotrafi 16 | 380 |
| 21.61 UTM - | [dapsearch] | 382 |
| 21.62 UTM - | less] | 385 |
| 21.63 UTM - | lscpu] 16 | 386 |
| 21.64 UTM - | [susb] 16 | 387 |
| 21.65 UTM - | migrate-logsessions] | 886 |
| 21.66 UTM - | [mkfs]16 | 690 |
| 21.67 UTM - | morej | <i>i</i> 91 |
| 21.68 UTM - | mtrj | i92 |
| 21.69 UTM - | netatati | 193 305 |
| ∠1.70 U1IVI - 21 71 LITM | וידיטומון האומהלויח] | 306 |
| 21.1 I U I W - | | 100 |

| 21.72 UTM - | [ntpdate] | 1697 |
|--------------|--|------|
| 21.73 UTM - | [passwd] | 1698 |
| 21.74 UTM - | [ping] | 1699 |
| 21.75 UTM - | [reboot] | 1700 |
| 21.76 UTM - | [reset] | 1701 |
| 21.77 UTM - | [reset-admin-blocks] | 1702 |
| 21.78 UTM - | [reset-admin-password] | 1703 |
| 21.79 UTM - | [reset-admin-sessions] | 1704 |
| 21.80 UTM - | [reset-logs] | 1705 |
| 21.81 UTM - | [reset-stats] | 1706 |
| 21.82 UTM - | rewizard | 1707 |
| 21.83 UTM - | [route] | 1708 |
| 21.84 UTM - | sarl | 1709 |
| 21.85 NGFW | / - [schedule-restart] schedule commands | 1710 |
| 21.86 UTM - | [sensors] | 1712 |
| 21.87 UTM - | [service-disable] | 1713 |
| 21.88 UTM - | [service-enable] | 1714 |
| 21.89 UTM - | [service-start] | 1715 |
| 21.90 UTM - | [service-status] | 1716 |
| 21.91 UTM - | [service-stop] | 1717 |
| 21.92 UTM - | [set-bypass] | 1718 |
| 21.93 UTM - | [set-ethernet-channels] | 1722 |
| 21.94 UTM - | [set-irgbalance-dynamic] | 1724 |
| 21.95 UTM - | [set-irobalance-static] | 1725 |
| 21.96 UTM - | [show-license] | 1726 |
| 21.97 UTM - | [show-sessions] | 1727 |
| 21.98 UTM - | [show-uuid] | 1728 |
| 21.99 UTM - | [show-version] | 1729 |
| 21.100 UTM | - [show-von-conn] | 1730 |
| 21.101 UTM | - [show-von-info] | 1731 |
| 21.102 UTM | - [show-wwan] | 1732 |
| 21.103 UTM | - [shutdown] | 1735 |
| 21.104 UTM | - [speedtest] | 1736 |
| 21.105 UTM | - [ssh-client] | 1737 |
| 21.106 UTM | - [ssh-proxy-sessions] | 1739 |
| 21.107 UTM | - [sync-users] | 1740 |
| 21.108 UTM | - [sysctl] | 1741 |
| 21.109 UTM | - [tcpdump] | 1742 |
| 21.110 UTM | - [tcptop] | 1743 |
| 21.111 UTM | - [tcptrack] | 1744 |
| 21.112 UTM | - [telnet] | 1745 |
| 21.113 UTM | - [tracepath] | 1746 |
| 21.114 UTM | - [traceroute] | 1747 |
| 21.115 UTM | - [update-license] | 1750 |
| 21.116 UTM | - [update-system] | 1751 |
| 21.117 UTM | - [upgrade-blockbit] | 1753 |
| 21.118 UTM | - [uptime] | 1755 |
| 21.119 UTM | - [vmstat] | 1756 |
| 21.120 UTM | - [vtysh] | 1757 |
| 21.121 UTM | - [watch-cpu] | 1758 |
| 21.122 UTM | - [watch-io] | 1759 |
| 21.123 UTM | - [watch-mem] | 1760 |
| 21.124 UTM | - [watch-srv] | 1761 |
| 21.125 UTM | - [wc] | 1762 |
| 21.126 UTM | - [whois] | 1763 |
| Blockbit NGF | W versão 2.4.0 | 1765 |

22.

NGFW - HISTÓRICO DE REVISÕES

Controle de Versão do Documento

| DATA | DESCRIÇÃO DAS MUDANÇAS |
|------------|---|
| 17/06/2017 | Lançamento do manual. |
| 28/02/2018 | Revisão 3, correções e mudanças estruturais. |
| 09/09/2018 | Atualização para a versão UTM 1.5. |
| 08/10/2018 | Revisão 4, correção. |
| 31/10/2018 | Atualização para a versão UTM 1.5.2. |
| 20/12/2018 | Revisão 5, correção. |
| 07/01/2019 | Atualização para a versão UTM 1.5.4. |
| 22/03/2019 | Migração do Manual do UTM para o Confluence. |
| 23/04/2019 | Atualização para a versão UTM 1.5.5. |
| 10/03/2020 | Atualização para a versão UTM 2.0. |
| 18/05/2020 | Atualização para a versão UTM 2.0.3. |
| 22/06/2020 | Atualização para a versão UTM 2.0.4. |
| 04/09/2020 | Atualização para a versão UTM 2.0.5. |
| 04/11/2020 | Atualização para a versão UTM 2.0.6. |
| 14/12/2020 | Atualização para a versão UTM 2.0.7. |
| 25/03/2021 | Atualização para a versão UTM 2.0.8. |
| 17/05/2021 | Atualização para a versão UTM 2.0.9. |
| 23/08/2021 | Atualização para a versão UTM 2.0.10. |
| 24/08/2021 | Atualização para a versão UTM 2.0.11. |
| 30/05/2022 | Atualização para a versão UTM 2.0.12. |
| 02/08/2022 | Atualização para a versão UTM 2.0.13. |
| 25/03/2021 | Atualização para a versão UTM 2.1.0. |
| 23/08/2021 | Atualização para a versão UTM 2.1.1. |
| 22/09/2021 | Atualização para a versão UTM 2.2.0. |
| 30/05/2022 | Atualização para a versão UTM 2.2.1. |
| 02/08/2022 | Atualização para a versão UTM 2.2.2. |
| 31/10/2022 | Atualização para a versão UTM 2.3.0. |
| 27/02/2023 | Atualização de UTM (Unified Threat Manager) para NGFW (Next Generation Firewall) com o lançamento da versão (NGFW) 2.4.0. |

UTM - INTRODUÇÃO

Obrigado por escolher o Blockbit UTM.

Este Guia do Administrador tem como objetivo auxiliar você e sua empresa a realizar o processo de instalação, configuração e utilização do Blockbit UTM. Ao término deste Guia, você estará apto a utilizar todas as funcionalidades e recursos necessários para seu funcionamento.

O Blockbit UTM – é um produto de cibersegurança multifuncional de última geração que inclui os principais recursos para segurança de rede: Como Firew all de última geração, Autenticação, Antimalwares, IPS (Sistema de Prevenção de Intrusão), VPN IPSec, VPN SSL, Secure Web Gateway, ATP (Proteção Contra Ameaças Avançadas), Dashboard, Relatórios e muito mais.

Operando em todas as camadas do modelo OSI (Open Systems Interconnection), com recursos de segurança avançados e tendo todo seu gerenciamento feito através de uma interface web fácil de navegar, o Blockbit UTM oferece toda a proteção que você precisa centralizada em um único equipamento.

Como principais diferenciais, temos:

- Proteção Avançada Contra Ameaças: Segurança inovadora, incluindo detecção e proteção em tempo real contra malwares, callbacks maliciosos e até mesmo ataques desconhecidos;
- Controle Avançado de Aplicações: Gerencie facilmente o acesso a serviços e aplicações, graças à função de atribuição de "nomes" ao invés de "endereços ou portas", a gestão é agilizada, o que melhora a segurança e reduz a necessidade do conhecimento de protocolos;
- Antivírus e AntiMalware: Conte com recursos avançados, como Antivírus e AntiMalware integrados, visando impedir a execução de aplicações não autorizadas e potencialmente perigosas. Faça a varredura de arquivos protegidos por senha e escaneie o tráfego nos protocolos HTTP /HTTPS possibilitando a interrupção de downloads maliciosos;
- Timeline: Sendo visível apenas por administradores e gestores, a Timeline permite o acompanhamento do histórico de acessos, de ameaças detectadas e aplicações em execução em uma linha do tempo exclusiva;
- Controle de Banda Flexível: Gerencie a largura de banda das conexões de acordo com suas respectivas prioridades, podendo definir velocidades de acesso para usuários, grupos, categorias web, tipos de serviço e mais;
- Painel Unificado de Políticas: A definição de políticas de conformidade e níveis de acesso podem ser criadas e aplicadas por grupos de forma simples e inovadora, reduzindo erros de configuração e falhas de segurança causadas ao simplificar as regras de usuário, grupos de usuários, serviços e aplicações em execução;
- Balanceamento de Link por Política: Gerencie múltiplos links de maneira revolucionária, atribua conexões de dados conforme cada política de segurança, tenha maior flexibilidade ao determinar: Conexões por endereços de rede, conteúdo de conexão, categorias web, aplicações, usuários, grupos de usuários e mais;
- Acesso Remoto sem Aplicação Cliente: Utilizando tecnologia compatível de maneira nativa com sistemas Windows, iOS e Android, permita que seus usuários se conectem com segurança à sua rede, sem a necessidade de instalar qualquer software adicional.

UTM - Recursos

- Next Generation Firewall: Aumentando a capacidade de proteção contra ataques, o Blockbit vai além do firewall tradicional, unindo o que há de melhor em segurança de redes em uma única solução. O Next Generation Firewall do Blockbit UTM simplifica a criação de políticas complexas e regras utilizando endereços, usuários, grupos, aplicações, ameaças e serviços apresentados como objetos nomeados de forma unificada, o que facilita o entendimento das políticas mantendo o controle no máximo;
- VPN SSL: A partir de qualquer estação de trabalho, utilizando apenas um navegador, é possível acessar um portal Web que oferece acesso as aplicações internas, configuradas de forma fácil e intuitiva com o máximo de segurança e privacidade;
- QoS: Proporcionando a priorização e o controle de banda nas políticas de conformidade de forma rápida e eficiente, este recurso avançado de Q
 oS permite categorizar o tráfego baseado em sua importância, possibilitando também a priorização de pacotes usando protocolos DSCP e TOS;
- VPN IPSEC: Nossa VPN possui uma robusta implementação IPSec, padrão que garante a interoperabilidade com outros produtos no mercado e vai além, oferecendo ainda mais opções de criptografia e segurança;
- Inspeção SSL: Atualmente grande parte do tráfego web é feito através de conexões cifradas, o Blockbit UTM, permite inspecionar o conteúdo criptografado de sua escolha através das políticas de conformidade, permitindo o controle total no acesso e uso de todos os recursos de proteção: Como Proteção Avançada Contra Ameaças e Filtragem de Conteúdo;
- Alta disponibilidade: Os produtos da Blockbit suportam alta disponibilidade (High Availability) tendo a capacidade de manter um appliance em modo backup, permitindo que entrem em operação rapidamente no caso de falha com o appliance primário. De forma transparente, mantém as sessões de Firewall e Autenticação de Usuário, diminuindo ao máximo o tempo de indisponibilidade;
- Controle de aplicação em nuvem: Com o avanço da Internet, aplicações como Facebook, Youtube, Google, Twitter, LinkedIn, Dropbox e outras têm se tornado muito populares. O Blockbit UTM permite o controle total no acesso das aplicações de controle em nuvem, permitindo que seus colaboradores permaneçam focados no que é necessário para a produtividade, sem distrações;
- Filtragem de Conteúdo: Possuindo mais de 40 milhões de endereços classificados em mais de 80 categorias e ainda contando com assinaturas de navegadores web, nosso filtro de conteúdo, atua em conjunto com a Inspeção SSL, viabilizando o controle completo sobre qualquer tipo de conteúdo que possa ser acessado. É possível monitorar o acesso através da criação simplificada de políticas de conformidade, especificando usuários, grupos, IPs, uso de banda e prioridade, links, navegador e versão, tamanho de downloads, aplicativos web, limite de tempo e muito mais;
- Suporte a Gerenciamento Centralizado: Com integração ao Blockbit GSM (Global Security Management) é possível gerenciar múltiplos dispositivos através de um único ponto central;
 - Demais recursos:
 - *IPv6*;
 - Captive portal com autenticação Social (Facebook, Twitter, Google);
 - Roteamento Avançado e Dinâmico;
 - BGPv4+;
 - OSPFv2 e v3;
 - RIPv1, v2 e RIPng;
 - IGMP;
 - Roteamento multicast (PIM-SM).
 - VLAN;
 - DNS dinâmico;
 - Integração do Active Directory/LDAP;
 - SNMP;
 - Servidor DHCP;
 - Proxy:
 - Filtragem de e-mails (POP3/S e SMTP/S);
 - HTTP e HTTPS;
 - *FTP*.
 - Link Aggregation Ethernet Bonding (802.3ad);
 - Entre outros…

UTM - Verificação de ambiente para instalação

Este guia fornece informações sobre como configurar e gerenciar o Blockbit UTM, antes de prosseguir, verifique os requisitos de instalação. Lembre-se que oferecemos suporte total por meio de nossos canais de atendimento, que terão a maior satisfação em ajudá-lo.

Requisitos de instalação

Certifique-se de que a comunicação com a internet está ativa, os processos de licenciamento, atualização de sistema e bases de dados necessitam conexão com a internet.

Requisitos mínimos de instalação:

- Processamento: 2 x Cores x86_x64;
- Memória: 2GB RAM;
- Armazenamento: 32GB.

Os requisitos acima suportam até 5 usuários, para até 15 usuários o recomendado é: 4 x Cores x86_x64, 4 GB de RAM e 32 GB de disco. Para mais usuários, por favor, consulte uma Revenda Blockbit ou um dos nossos especialistas.

Plataforma de virtualização: VMware, XenServer, KVM e ProxMox.

Para seguir com a instalação e a configuração é necessário um cliente SSH, console serial e um navegador web. Segue abaixo uma lista das aplicações mínimas recomendadas:

Navegador Web:

- Mozilla Firefox versão 45;
- Google Chrome versão 51.

Acesso remoto (SSH e Console):

- PUTTY;
- CygWin;
- MobaXterm.

UTM - Sobre o Guia do Administrador

Este guia foi desenvolvido especialmente para você administrador, todas as seções foram estruturadas de modo a tornar o processo de instalação fácil e rápido. Todo o passo a passo é apresentado com exemplos, facilitando a compreensão e esclarecendo dúvidas.

No decorrer do guia, você poderá encontrar alguns símbolos seguidos de texto, eles têm o objetivo de alertá-lo sobre uma importante observação ou nota referente àquela seção.

Vamos conhecer esses símbolos:

 Alerta: Refere-se a observações ou notas que devem ser seguidas por você com muita cautela durante o processo de instalação do Blockbit UTM:

Exemplo de uma mensagem de Alerta.

Símbolo - "Alerta"

• CLI - Command Line Interface: Também conhecido como Shell, refere-se aos comandos que devem ser digitados, ao lado desse símbolo estará disposto o comando a ser digitado:

Linha de Comando

Exemplo de uma Linha de Comando.

Símbolo - CLI - Command Line Interface

• Dica: Refere-se a sugestões que tem como função facilitar o processo de instalação do Blockbit UTM:

| Exemplo de uma mensagem de Dica. |
|---|
| Símbolo – "Dica" |
| • Nota: Refere-se a observações ou notas que tem como função auxiliar o processo de instalação do Blockbit UTM: |
| Exemplo de uma mensagem de Nota. |
| Símbolo – "Nota" |
| Informações: Refere-se a informações adicionais a respeito do Blockbit UTM: |

Exemplo de uma mensagem de Informações.

Símbolo - "Informações"

Este guia foi desenvolvido especialmente para você administrador, todas as seções foram estruturadas de modo a tornar o processo de instalação fácil e rápido. Todo o passo a passo é apresentado com exemplos, facilitando a compreensão e esclarecendo dúvidas.

No decorrer do guia, você poderá encontrar alguns símbolos seguidos de texto, eles têm o objetivo de alertá-lo sobre uma importante observação ou nota referente àquela seção.

Vamos conhecer esses símbolos:

• Alerta: Refere-se a observações ou notas que devem ser seguidas por você com muita cautela durante o processo de instalação do Blockbit UTM:

Exemplo de uma mensagem de Alerta.

Símbolo - "Alerta"

CLI - Command Line Interface: Também conhecido como Shell, refere-se aos comandos que devem ser digitados, ao lado desse símbolo estará disposto o comando a ser digitado:

Linha de Comando

Exemplo de uma Linha de Comando.

Símbolo - CLI - Command Line Interface

• Dica: Refere-se a sugestões que tem como função facilitar o processo de instalação do Blockbit UTM:

Símbolo - "Dica"

• Nota: Refere-se a observações ou notas que tem como função auxiliar o processo de instalação do Blockbit UTM:



Exemplo de uma mensagem de Nota.

Símbolo - "Nota"

Informações: Refere-se a informações adicionais a respeito do Blockbit UTM:



Exemplo de uma mensagem de Informações.

Símbolo - "Informações"

UTM - ARQUITETURA

A arquitetura do BLOCKBIT UTM é apresentada por um conjunto de camadas de componentes, que integradas, definem os aspectos técnicos relativos aos serviços oferecidos pelo sistema. A imagem abaixo representa a integração dos módulos.







Arquitetura do Sistema - Gerenciamento Centralizado



Packetflow

A seguir os módulos da arquitetura serão detalhados.

Arquitetura – Modelos de Componentes

A arquitetura é dividida nos seguintes modelos de componentes:

- API; Frontend;
- Backend;
- Data storage;Operating System.



Componentes

A seguir explicaremos estes modelos.

Arquitetura – API

A Interface de Programação de Aplicativos (*API*) é a camada de gerenciamento *WEB*, sendo esta executada através de uma *API*, que segue a especificação *RESTful* com transferência de dados em formato *JSON*. Podendo ser utilizada para integrar o produto a ferramentas de terceiros e outros produtos da Blockbit, como por exemplo o Blockbit GSM e o Blockbit EPS (*End Point Security*). Todas as requisições são autenticadas usando uma chave habilitada pelo usuário de administração do sistema e a autenticação é realizada através do método *BASIC* do protocolo *HTTP*.

Arquitetura – Frontend

Frontend é a camada de desenvolvimento que disponibiliza a interface de apresentação e controles do sistema, por meio de seus recursos é possível ao administrador, acessar qualquer tipo de informação e executar os comandos de configuração nos serviços do Blockbit UTM.

Graças às interfaces disponibilizadas na camada de *Frontend*, é garantido que o usuário final não tenha acesso direto aos componentes disponibilizados nas camadas mais profundas da arquitetura do sistema.

O sistema foi projetado para oferecer dois tipos de interface na camada de Frontend:

- Manager: É uma aplicação WEB para administração dos dispositivos. Nela, o administrador define todos os parâmetros de configuração do sistema, efetua Scans e realiza a gestão de vulnerabilidades;
- Portal: É uma outra aplicação Web, onde os usuários da rede que são inspecionados, têm acesso a alguns recursos do sistema, ex.: Portal de autenticação, dados pessoais, sessões, certificados, relatórios, troca de senha, quarentena e Virtual Office;
- **Console:** O console CLI disponibiliza acesso a diversos comandos para configuração e diagnóstico. Esta interface pode ser acessada por meio de conexão através de um terminal SSH e serial.

Arquitetura - Data storage

No sistema, o Database (Banco de Dados) é dividido em 3 partes:

- Settings: Camada intermediária, serve para armazenamento e transferência de informações entre os componentes de Frontend e Backend. Por meio do sistema de banco de dados, o Frontend escreve configurações e parâmetros que serão aplicados nos componentes de Backend e no Sistema Operacional;
- Definitions: Armazena dados de inteligência e definições de sistema, como regras de compliance e assinaturas maliciosas, entre outras;
- Reports: Base de dados onde são gravados os relatórios de todo o sistema após a realização de um scan.

Arquitetura – Backend

Backend é a camada que disponibiliza comandos e programas que aplicam configurações solicitadas, sendo executados através das interfaces de Fronte nd para os serviços de Scanner e ao Sistema Operacional.

Graças ao sistema possuir característica modular, possuindo serviços independentes entre si, as informações entre os recursos de *Frontend* e *Backend* são transportadas por dois caminhos criptografados e autenticados por chave: Banco de Dados ou Conexão SSH.

- Apply Queue: A execução de comandos entre as interfaces de Frontend e os serviços de Backend, são realizadas através de uma fila de comandos dentro do banco de dados. Esta fila organiza estes comandos por prioridade, de modo a garantir que as configurações dos serviços sejam aplicadas na ordem correta pelo sistema;
- Apply Scripts: Lê os parâmetros de configuração armazenados no banco de dados e reescreve essas configurações nos serviços e no sistema
 operacional;
- Daemons: São os principais programas que implementam os serviços de inspeção de tráfego de rede no produto, tratam-se de processos executados em segundo plano (background) pelo sistema;
- Helpers: São programas acoplados aos daemons e complementam as funções destes mesmos, na maioria das vezes, são executados através de PIPE;
- Summarizers: São programas que coletam informações de logs do sistema, resumindo as estatísticas com objetivo de armazená-las nos bancos de dados de relatórios. Graças ao alto fluxo de informações coletadas pelo sistema, esses programas foram desenvolvidos visando execução a cada 5 minutos.

A solução conta com mecanismo de indexação de logs, permitindo assim uma busca acelerada de eventos, sem a necessidade de abertura de arquivos de logs mais antigos, e também com integração com o SIEM. Suporta também a troca automática de arquivo de Log, de maneira regular ou através do tamanho do arquivo.

Em caso de falha da comunicação entre o appliance de segurança Blockbit e a solução gerenciamento Centralizado e armazenamento de logs (GSM) é realizada uma retenção temporária dos logs no Blockbit até que a comunicação seja restabelecida.

Arquitetura - Sistema Operacional

O Sistema Operacional do Blockbit UTM também é mantido pela equipe de pesquisa e desenvolvimento da Blockbit, onde são disponibilizados os pacotes de ferramentas de código aberto utilizados na implementação dos serviços.

Para simplificar a compatibilidade com os Appliances e garantir o desempenho na execução dos serviços, o Blockbit UTM é executado em um Sistema Operacional com Kernel Linux baseado em arquitetura Intel x86_x64.

UTM - INSTALAÇÃO

O Blockbit UTM pode ser instalado em dois tipos de Appliances: Hardware e Virtual, sendo estes compatíveis com as seguintes soluções: VMware, XenSe rver e KVM.

A seguir, exemplificaremos como instalar o Blockbit UTM usando o software VMware ESXi 6.5.0.

- Importando a Máquina Virtual;
 Iniciando Máquina Virtual Primeiro Acesso;
 Gravações das imagens nos pendrives.

UTM - Importando a Máquina Virtual

Inicialmente é importante considerar as características mínimas do Appliance Virtual, conforme demonstrado na tabela abaixo:

| Modelo | Memória | Disco | CPU | Interfaces |
|-----------|---------|--------|-----|-------------------------|
| BBv-2 | 2 GB | 32 GB | 2 | 4 |
| BBv-5 | 4 GB | 32 GB | 4 | 4 |
| BBv-10 | 4 GB | 32 GB | 4 | 4 |
| BBv-100 | 8 GB | 120 GB | 4 | 8 |
| BBv-1000 | 16 GB | 240 GB | 8 | 9, com limite de até 26 |
| BBv-10000 | 32 GB | 480 GB | 32 | 9, com limite de até 26 |

Tabela - Características mínimas do Appliance Virtual

Para efetuar a importação, faça o download do Open Virtual Appliance (OVA) do Blockbit UTM, que pode ser solicitado por meio do cadastro de Trial em nosso site: http://www.blockbit.com.

1. Usando o navegador de internet de sua preferência, acesse o console de gerenciamento do VMware ESXi no VMware Host Client;

2. Preencha os campos com as seguintes informações:

- User name: Usuário cadastrado no VMware;
- Password: Senha do usuário;
- Clique no botão "Log in".



Login VMware

3. Clique em "Create/Register VM";

| vmware ESXi | | |
|-------------|--|---|
| Mavigator C | Control Contro | Create/Register VM 🔯 Shut down 💽 Reboot 🦿 Ref t.localdomain 6.0.0 (Switt 2620759) Homal (not successfiel to any vCenter Derver) 8.29 48ys |
| | = Rardware Manufacturier Model | Advantech FWA-6520 |

Console VMware

4. Selecione a opção "Deploy a virtual machine from an OVF or OVA file";

| This option galitati you through the precises of creating a |
|---|
| eritual machine Som an CVF and VMDX Bas. DNA deployment is connectly limited to the under 1 pipeline in title due to wait, brownar limitations. Pytou ministic deploy an CVA greater than 1 popely/e, prease admit the DVA using tartent provide the DVF and VAIDX. Bien repersitely |
| |

Select creation type

Clique no botão "Next".
Selecione a imagem do Blockbit UTM cujo download foi realizado pelo site da Blockbit e digite o nome da máquina no campo "Enter a name for the virtual machine". Ex.: Blockbit UTM;

| Dillew virtual muchine - BLOCABI | IT UTM | |
|---|---|--------|
| 1 Select creation type 2 Select CWT and VMDR files 3 Select storage | Select OVF and VMDK files Select the OVF and WMDK files or Over, for the VM year would like to deploy | |
| 5 Deployment options | Error a care to the what weather | |
| 6 Additional autorga 7 Ready to complete | Videal machine nerves can contain as to 00 characters and they read its singles within each ESK instance. | |
| vmware | * 🕿 88v-2-UTM-172 xva | |
| | Back Next Free | Canool |

Select OVF and VMDK files

• Clique no botão "Nexť";

5. Selecione o storage desejado. Ex.: datastore1;

| 1 Select creation type 2 Select OVF and VMOK files Select OVF and VMOK files Locance agreements 5 Deployment options | Select storage | n to staré the carr | lguration india | nox Red. | | | | |
|--|---|---------------------|-----------------|----------|---------|----------|--------|----|
| | The following detectives are exceptible from the destination resource that you selected. Select the destination astactore for the virtual machine configuration files and all of the virtual dists: | | | | | | | |
| Additional settings | tern | 10 | Depetts ~ | Ties - | Type | · Therap | Access | 40 |
| | Instantor#1 | | 800.5 58 | 64.38 GR | VMF SIT | Baparter | Single | |
| | | | | | | | | |
| | | | | | | | | |
| vm ware | | | | | | | | |

Select Storage

• Clique no botão "Nexť";

6. Aguarde o upload da OVA. Enquanto ocorre o upload, aparecerá a seguinte mensagem: "Extracting OVA, this could take some time..." Espere a conclusão deste processo, que deverá ocorrer automaticamente;

| B Now with a matching - 80.02CH801 1 | 15.00 |
|---|---|
| Select creation type Select OVF and VMOR Ten Select 2004 and VMOR Ten Select 2004 and VMOR Ten Galaxies and vertices Galaxies and vertices Teady to compare | Select storage Selective relative is which is store the configuration and claim flux Extending Oge, they population come time . |
| | |
| | Back Next Fault Cancel |

Select Storage - "Extracting OVA, this could take some time..."

- 7. Defina as configurações da máquina virtual:
 - Network mappings: Defina o modo de rede adequado para o seu ambiente. Ex.: Mode bridged;
 - Disk provisioning: Defina a opção de sua preferência. Segue uma breve descrição sobre as opções:
 - Disco Thick: São discos totalmente alocados no datastore, ou seja, se você criar um disco Thick com 20GB, ele irá ocupar 20GB do seu datastore;
 - Disco Thin: É um tipo de disco que aloca apenas o espaço que é gravado pelo sistema operacional da máquina virtual. Por exemplo, se você criar um disco de 20GB para uma VM, inicialmente ele irá ocupar apenas alguns KB/MB no datastore, porém, no momento que você começar a gravar dados no mesmo através do sistema operacional, o tamanho dele pode chegar até o limite de 20GB.

Para maiores informações consulte o manual do VMware. Neste exemplo será utilizado a configuração "Disk provisioning - Disco Thin".

| Mess virtue machine - BLOCKBIT | UTM . | | | |
|--|---|---------|------------|------------------|
| 1 Select coston type 2 Select OVF and WIDK Res 3 Select strate 1 Ready in complete | Deployment options Select deployment entions | | | |
| | Network missings | bedged | vM Netzoni | • |
| | Dok travisional | * the 1 | P Trice | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| vm ware | | | | |
| | | | Bedi | Nest Film Cancel |

Deployment options

- Clique no botão "Nexť".
- 8. Revise as configurações definidas antes de finalizar upload;



Ready to complete

• Clique no botão "Finish".

A importação foi concluída, basta clicar no botão "Power on" para iniciar a máquina virtual e seguir para instalação do Blockbit UTM.

UTM - Iniciando Máquina Virtual - Primeiro Acesso

Ao iniciar a máquina virtual pela primeira vez, será exibida a seguinte tela:



Iniciando o Blockbit UTM pela primeira vez

O processo de iniciação da máquina virtual apresentado a seguir é o mesmo tanto para Appliances em Hardware como para Appliances Virtuais. Não é necessário realizar nenhum passo, apenas aguardar até a liberação da tela de *login*.



Tela de login - Blockbit UTM

Agora será necessário configurar o IP. Para tanto, realize os seguintes passos:

- 1. Localhost login: Efetue o login através do console CLI;
- 2. Após realizar a Autenticação no console CLI, preencha os seguintes campos:
- · Login: admin
- Pass: admin

É altamente recomendada a alteração da senha padrão do usuário "admin" de console. Para alteração da senha padrão, é necessário criar uma senha segura. Esta senha deve conter no mínimo 8 caracteres com letras maiúsculas e minúsculas, números e caracteres especiais.

Para alterar a senha, digite o comando abaixo:

```
Digite o comando "passwd" e digite "Enter".
Digite a senha atual e digite "Enter".
Digite a nova senha e confirme ela.
```

Após realizar esse procedimento a senha terá sido alterada com sucesso.

3. Altere o endereço IP do Blockbit UTM;

O endereço IP padrão do Blockbit Network Security é 192.168.1.1. Este IP é utilizado na porta eth1. Neste guia utilizaremos o endereço IP 172.16.102.136 como exemplo. Caso deseje alterar, siga os passos a seguir:

Detalhes da configuração:

IP: 172.16.102.136 *Mask*: 255.255.255.0 *Default Gateway*: 172.16.102.1

Caso seja necessário verificar o UUID do seu appliance, digite o comando [show-uuid]

Em antigas versões do UTM, a interface de gerência era a eth0, à partir do UTM 2.0 esta interface é utilizada para Zero Touch Provisioning, para mais informações, cheque o manual do GSM. Tendo isso em vista:

A eth0 é a interface principal, é uma interface dinâmica WAN, utilizada para acesso à internet e provisionamento de device.

A eth1 é a interface de gerência com o IP padrão para configuração do UTM, ela será configurada a seguir.

Digite os comandos:

```
ifconfig ethl 172.16.102.136/24
ifconfig ethl down
ifconfig ethl up
route add default gw 172.16.102.1 dev ethl
```

Após realizar esse procedimento o endereço *IP* terá sido alterado. Com o comando abaixo é possível também editar o endereço *IP* do Blockbit UTM:

Digite o comando blockbit>changeip. Tecle "Enter".

UTM - Gravações das imagens nos pendrives

No site da Blockbit realize o download da imagem de instalação correspondente.

As imagens devem ser baixadas e salvas em uma pasta do computador. Verifiquem o *MD5SUM* dos arquivos para garantir que não estão corrompidos. A aplicação para realizar o *MD5SUM* em *Microsoft Windows* é a *WinMD5Free* (http://www.winmd5.com/), para executar essa verificação siga os passos abaixo:

Verificação dos arquivos

1. Abra a aplicação, a seguinte tela será exibida:

| ₩inMD5Free v1.20 | — | | × |
|--|--------------------|------------------------|-----------|
| WinMD5Free | w | ww.winm | d5.com |
| Select a file to compute MD5 checksum (or drag and drop a file onto | o this wir | ndow) <u>B</u> rows | se |
| | | <u>C</u> an | cel |
| File Name and Size: n/a Current file MD5 checksum value: | | | |
| n/a | | | |
| Original file MD5 checksum value (optional). It usually can be found paste its original md5 value to verify | l from we erify | ebsite or | .md5 file |
| <u>W</u> ebsite <u>A</u> bout | | Ex | it |
| WinMD5 | | | |

2. Selecione o arquivo da imagem e aguarde o cálculo:

| 🐼 WinMD5Free v1.20 | _ | | × |
|---|----------|------------------------|----------|
| WinMD5Free | w | ww.winmo | d5.com |
| Select a file to compute MD5 checksum (or drag and drop a file onto t C:\Users\Ipereira\Downloads\UTM-Install-firmware.img | this wir | ndow) <u>B</u> rows | ie |
| File Name and Size: C:\Users\Ipereira\Downloads\UTM-Install-firmw Current file MD5 checksum value: | /are.im | <u>C</u> ano | tel |
| Saf7e9490872ecf6caf8fa605efeb9e1 Original file MD5 checksum value (optional). It usually can be found fi | rom w | ebsite or | .md5 fil |
| paste its original md5 value to verify | fy | | |
| <u>W</u> ebsite <u>A</u> bout | | E <u>x</u> i | t |
| MD5 Check | | | |

3. Compare os valores obtidos das duas imagens no WinMD5 com os respectivos valores salvos na seção.

Gravando as imagens

Para gravar as imagens é necessário o aplicativo Rufus que poderá ser baixado clicando neste link: https://rufus.ie/.

1. Insira um *pendrive*, de no mínimo 8 GB;



2. Ao abrir a aplicação, a seguinte tela será exibida:

| Rufus 3.11.1678 (Portable) | – 🗆 × |
|--|--|
| Drive Properties | |
| | |
| NO LABEL (D:) [16 GB] | ~ |
| Boot selection | |
| Disk or ISO image (Please select) | ✓ Ø SELECT ▼ |
| Partition scheme | Target system |
| MBR | BIOS (or UEFI-CSM) |
| Show advanced drive properties | |
| Farmat Onting a | |
| Format Options | |
| Volume label | |
| 16 GB | |
| File system | Cluster size |
| | |
| FAT32 (Default) \sim | 8192 bytes (Default) $$ |
| FAT32 (Default) ∨ Show advanced format options | 8192 bytes (Default) \sim |
| FAT32 (Default) ~ Show advanced format options | 8192 bytes (Default) V |
| FAT32 (Default) ~ Show advanced format options Status | 8192 bytes (Default) V |
| FAT32 (Default) Show advanced format options Status RE | 8192 bytes (Default) ~ |
| FAT32 (Default) Show advanced format options Status RE | 8192 bytes (Default) ~ |
| FAT32 (Default) ✓ ✓ Show advanced format options Status RE ③ (i) 差 □ | 8192 bytes (Default) ~ ADY START CLOSE |
| FAT32 (Default) ✓ ✓ Show advanced format options Status RE ③ ① 葦 ■ | ADY START CLOSE |

3. Clique em [

SELECT

-

] e selecione a imagem adequada a ser gravada nos pendrives. Ex.: UTM-Install-firmware.img;

| | | | | _ |
|--|----------------------|--------|--------|---|
| 🖋 Rufus 3.11.1678 (Portable) | _ | | × | |
| Drive Properties | | | | |
| Drive Properties | | | | |
| Device | | | | |
| NO_LABEL (D:) [16 GB] | | | \sim | |
| Boot selection | | | | |
| UTM-2.0-Install-firmware-2.0.4-66.img | ~ 🕗 | SELECT | - | |
| Partition scheme | Target system | | | |
| MBR \sim | BIOS (or UEFI-CSM) | | \sim | ? |
| Show advanced drive properties | | | | |
| Format Options | | | | |
| Volume label | | | | |
| 16 GB | | | | |
| 51 | a | | | |
| File system | Cluster size | | - | |
| FAI32 (Default) | 8192 bytes (Default) | | \sim | |
| Show advanced format options | | | | |
| Status | | | | |
| Status — | | | | |
| READY | , , | | | |
| ① 差 Ⅲ | START | CLOSE | | |
| Using image: UTM-2.0-Install-firmware-2.0.4-6 | 6.img | | | |
| Gravando a ir | nagem | | | Ī |

4. Caso, não esteja selecionado, selecione o Device correspondente ao pendrive que deseja gravar a imagem. Ex.: NO_LABEL (D:) [16 GB];

| 5. Para gravar a imagem clique em [| START | , ao fazer isso, a mensagem abaixo será exibida; |
|-------------------------------------|-------|--|
|-------------------------------------|-------|--|

| Rufus | | × |
|-------|--|---|
| | WARNING: ALL DATA ON DEVICE 'NO_LABEL (D:) [16 GB]' WILL BE DESTROYED. To continue with this operation, click OK. To quit click CANCEL. | |
| | OK Cancel | |

WARNING

] e aguarde a gravação ser concluída com sucesso;

| Rufus 3.11.1678 (Portable) | | | | |
|--|----------------------|--|--|--|
| Drive Properties —— | | | | |
| Device | | | | |
| NO_LABEL (D:) [16 GB] | | | | |
| Boot selection | | | | |
| UTM-2.0-Install-firmware-2.0.4-66.img | V 🔗 SELE | | | |
| Partition scheme | Target system | | | |
| MBR \sim | BIOS (or UEFI-CSM) | | | |
| ✓ Show advanced drive properties | | | | |
| Format Options | | | | |
| Volume label | | | | |
| 16 GB | | | | |
| File system | Cluster size | | | |
| FAT32 (Default) 🗸 | 8192 bytes (Default) | | | |
| Show advanced format options | | | | |
| Ctature | | | | |
| status — | | | | |
| Writing image: 43.5% | | | | |
| Writing im | | | | |
| Writin <mark>g im</mark> | | | | |
| Writing im | START CAN | | | |
| Writing im | START CAN | | | |

7. Após a conclusão da barra de progresso, clique em [

OK

6. Clique em [

CLOSE

] para fechar o Rufus.

| 🖋 Rufus 3.11.1678 (Portable) | _ | | × |
|--|----------------------|--------|---------|
| Drive Properties | | | |
| Drive Properties | | | |
| Device | | | |
| usboot (D:) [16 GB] | | | \sim |
| Boot selection | | | |
| UTM-2.0-Install-firmware-2.0.4-66.img | ~ 📀 | SELECT | |
| Partition scheme | Target system | | |
| MBR \sim | BIOS (or UEFI-CSM) | | ~ ? |
| Show advanced drive properties | | | |
| Format Options | | | |
| | | | |
| Volume label | | | |
| usboot | | | |
| File system | Cluster size | | _ |
| FAT32 (Default) \vee | 8192 bytes (Default) | | \sim |
| Show advanced format options | | | |
| Status | | | |
| Status | | | |
| READ | Y | | |
| | | | |
| 🔇 i) 🛱 🗐 | START | CLOSE | E |
| | | | |
| 1 device found | | 0 | 0:10:00 |

Rufus - Concluído

Acesso ao Console - Putty

Antes de iniciar os procedimentos a seguir o aplicativo Putty deverá estar disponível na máquina na qual será feita a conexão ao Equipamento. O Putty é um software de emulação de terminal grátis e de código livre.

Agora configure o emulador de terminal com os parâmetros a seguir:

- Porta: COM1 (a porta pode variar, verifique seu gerenciador de dispositivos do *Windows*);
 Taxa de transmissão padrão: 115200; *Bits* de dados padrão: 8;

- Stop bits padrão: 1; ٠
- Paridade padrão: Nenhum.

| 😵 PuTTY Configuration | | ? X | | | | |
|----------------------------|---------------------------|---------------------|--|--|--|--|
| Catagony | | | | | | |
| Session | Options controlling | local serial lines | | | | |
| | Select a serial line | | | | | |
| - Keyboard | Serial line to connect to | COM1 | | | | |
| Bell | Configure the serial line | | | | | |
| | <u>Speed (baud)</u> | 115200 | | | | |
| Appearance Behaviour | Data <u>b</u> its | 8 | | | | |
| Translation | Stop bits | 1 | | | | |
| Selection Colours | <u>P</u> arity | None \checkmark | | | | |
| | Flow control | XON/XOFF < | | | | |
| Proxy | | | | | | |
| Telnet | | | | | | |
| ⊞. SSH | | | | | | |
| Serial | | | | | | |
| | | | | | | |
| | | | | | | |
| <u>A</u> bout <u>H</u> elp | <u> </u> |)pen <u>C</u> ancel | | | | |
| Putty Settings | | | | | | |
| 🕵 PuTTY Configuration | | ? | \times |
|----------------------------|--|---|------------|
| Category: | Basic options for your PuTTY se Specify the destination you want to conne Serial line COM1 Connection type: Raw Telnet Rogin SSF Load, save or delete a stored session Saved Sessions Default Settings Logan Serial Blockbit | ssion Speed 115200 Segin Load Save Delete | a l |
| Serial | Close window on exit: Always Never Only on cl | ean exit | |
| <u>A</u> bout <u>H</u> elp | <u>O</u> pen | <u>C</u> ancel | |

Putty Connect

UTM - CONFIGURAÇÃO DE EXCEÇÃO

Esta seção irá apresentar como configurar exceção nos navegadores web: Google Chrome e Mozilla Firefox. Ao realizar o primeiro acesso a Interface Web do Blockbit UTM é normal que os browsers emitam um alerta de segurança informando um erro de certificado. Isso ocorre porque o browser não reconhece como confiável nenhuma autoridade certificadora que valide o acesso a esta página. Portanto, é necessário fazer a configuração de exceção no navegador web.

Para configurar a exceção, siga os passos:

1. Conecte no navegador de internet e acesse o endereço: https://172.16.102.136:98. Caso tenha alterado o endereço IP, utilize o IP alterado;

Caso o Browser emita um ALERTA DE SEGURANÇA, siga as recomendações abaixo.

Cada Browser possui um procedimento para liberar a conexão como confiável. Siga as orientações de como proceder.

Configurando exceção no Google Chrome

Para configurar a exceção no Google Chrome siga os seguintes passos:

1. Clique no botão "Advanced";



2. Clique no link "Proceed to 172.16.102.136 (unsafe)" para aceitar esta página como confiável;



A configuração de exceção no Google Chrome foi realizada com sucesso.

Configurando exceção no Mozilla Firefox

Para configurar a exceção no Mozilla Firefox siga os seguintes passos:

- 1. Clique no botão "Advanced";
- 2. Clique no botão "Add Exception ... ";

| 1 | Your connection is not secure |
|---|---|
| | The owner of 172.16.102.136 has configured their website improperty. To protect your information from being stolen Fireflix has not connected to this website. |
| | Lears more |
| | Report errors like this to help Mozilla identify and block malicious sites |
| | Tin Back Advanced |
| | |
| | 172.16.102.136 uses an invalid security certificate. |
| | The certificate is not trusted because it is self-signed. The certificate is not valid for the name 172.16.102.136. |
| | Error code: SEC_ERROR_UNKNOWN_ISSUER |
| | Add Exception |

Exceção Mozilla Firefox - Your connection is not secure

3. Clique no botão "Confirm Security Exception".

| Add Security Exception X |
|--|
| You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this. |
| Server Location: https://172.16.102.136/ |
| Certificate Status This site attempts to identify itself with invalid information. Wrong Site |
| The certificate belongs to a different site, which could mean that someone is trying to impersonate this site. |
| Unknown Identity |
| The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature. |
| Permanently store this exception |
| <u>C</u> onfirm Security Exception Cancel |

Exceção Mozilla Firefox - Confirm Security Exception

A configuração de exceção no Mozilla Firefox foi realizada com sucesso.

UTM - ASSISTENTE DE INSTALAÇÃO

Esta seção irá apresentar como configurar o Assistente de Instalação do Blockbit UTM.

A seguir será apresentado o processo de instalação e o correto preenchimento de todos os campos requisitados pelo formulário.

Instalação do Blockbit UTM

Para instalar o Blockbit UTM, siga os seguintes passos:

1. Conecte no navegador de internet e acesse o endereço: https://172.16.102.136:98. Caso tenha alterado o endereço IP, utilize o IP alterado;

| E storaution + | | | | Circle 1 |
|----------------|--|---|-----------|----------|
| + Claiming | And Print Market Statements and Statements | | | a) (|
| | H A. Without an another server | | (initered | |
| | Name of the state of the state of | | | |
| | Der Ver Heffings Personen sensen ver Ferenen Ferenen Ferenen Effiniente sensen ver | Applaans proceedings Without un- Without | | |
| | Andreastic and and a second se | | 141 | |
| | - Long - | NO | | |
| | 1.0 | 100 (11) | | |
| | | th gad ballion | | |
| | - April - | - Color | | |
| | Test | Separate and the | | |
| | | 18 | | |
| | Anjates (print) | Buchasan | | |
| | 1 | and Add Add Com- | | |
| | Aufligefrutten Infactoren Infactoren | Adviduation while outpassed | | |
| | | | | |

Installation Wizard

2. Digite os seguintes dados no frame "Server settings", para as configurações iniciais de rede do Blockbit UTM:

- Description: Campo para descrever o nome do servidor. Ex.: Blockbit UTM;
- Language: Selecionar o idioma padrão. Ex.: English;
- Time Zone: Selecionar o fuso horário no qual sua empresa se encontra. Ex.: America/New York;
- NTP Server: Defina o servidor de sincronização de relógio. Ex.: pool.ntp.org;
- Hostname: Nome do Hostname. Pode ser qualquer um desde que esteja conforme padrão FQDN Fully Qualified Domain Name. Ex.: utm. blockbit.com;
- DNS suffix: Domínio da rede. Ex.: blockbit.com;

- DNS server 1: Defina o servidor DNS da rede ou da internet. Ex.: 176.16.102.161;
- DNS server 2: Defina o DNS secundário da sua rede ou da internet,
- Gateway: Defina a rota padrão da rede. Ex.: 176.16.102.1;
- Integrity key: Chave de integridade do sistema, utilizada no processo de criptografia dos arquivos de backups. Este campo é gerado automaticamente.

3. Digite os seguintes dados no frame "Certificate", estas informações serão utilizadas para a criação do certificado SSL no console de administração do Blockbit UTM:

- Country: Defina o país. Ex.: US;
- State: Defina o estado. Ex.: New York;
- City: Defina a cidade. Ex.: New York;
- Organization: Defina o nome da empresa. Ex.:Blockbit;
- E-mail: Defina o e-mail do administrador. Ex.: admin@blockbit.com;
- Organizational Unit: Defina o departamento. Ex.: QA;
- Expires (years): Defina o tempo de validade do certificado. Ex.: 10 anos;
- Hostname: Defina o FQDN para o certificado. Ex.: utm.blockbit.com.

4. Digite os seguintes dados no frame "Authentication", define o domínio local padrão para a autenticação de usuários do Blockbit UTM.

• Default domain: Defina o domínio default de autenticação. Ex.: blockbit.com.

5. Digite os seguintes dados no frame "Administration", a senha do usuário "admin" da console de administração do Blockbit UTM:

- Admin user password: Insira uma senha com no mínimo oito caracteres. A senha deve conter letras maiúsculas, minúsculas e caracteres especiais. Ex.: q1W@e3R\$;
- Confirmation Save: Confirme a senha inserida acima.

6. Clique no botão "Save". A tela abaixo será exibida solicitando a confirmação, ao clicar em "ok" o sistema irá aplicar as configurações e será reinicializado.

| Hereigner Hittig Soldande | Name And Market Market Market | 18 | |
|---------------------------|--|--|------------|
| - | Yes | | |
| | Aprenda Armer Aproprior () Aproximation Apr | | |
| | Admendiation Administration and Continuation | | |
| | | Administration Administration Administration Administration Calification Calification | Adversaria |

Installation Wizard – Formulário

• Clique no botão "OK". O sistema irá aplicar as configurações e será reinicializado.

Ao finalizar esses passos o Assistente de Instalação terá sido finalizado com sucesso. Aguarde a inicialização, o navegador fará um AUTO-REFRESH do endereço de acesso à interface WEB e retornará a interface de logon.



Tela de LOGON de administração do Blockbit UTM

UTM - AMBIENTE DE REDES

Esta seção irá apresentar um exemplo de ambiente de rede. No Blockbit UTM, é possível instalar duas configurações de servidores: Standalone e H.A. Para melhor contextualização, utilizaremos uma topologia fictícia, porém muito comum entre os prováveis ambientes que devem utilizar o Blockbit UTM.

Blockbit UTM - Standalone

Nesta configuração, é instalado apenas um servidor dedicado.



Topologia da rede - Blockbit UTM Manager.

As vantagens de utilizar essa topologia são: Economia de máquinas e facilidade de implementação.

Blockbit UTM – H.A.

Nesta configuração, são instalados dois servidores. Ou seja, um servidor Primário e um servidor Secundário.



Topologia da rede – Blockbit UTM H.A.

As vantagens de utilizar essa topologia são: Alta disponibilidade e flexibilidade. Para ilustrar o processo de instalação e configuração do Blockbit UTM, durante este manual criaremos uma rede tomando como base a seguinte tabela de endereçamento *IP* como exemplo:

| NOME | ENDEREÇO IP EXTERNO | REDE INTERNA |
|----------------|---------------------|--------------------|
| Blockbit UTM | 172.16.102.93 | 172.16.102.0/24 |
| Windows Server | 172.16.102.81 | 172.16.102.0/24 |
| Linux CentOS | 172.16.102.39 | 172.16.102.0/24 |
| Windows 7 | 172.16.12.223 | 172.16.12.0/23 |
| Windows 10 | 172.16.12.224 | 172.16.12.0/23 |
| Site | www.blockbit.com | 104.239.173.143/32 |

Tabela 1 - Endereçamento IP.

UTM - INTERFACE WEB

Esta seção irá demonstrar como realizar o acesso a Interface Web do Blockbit UTM.

O Blockbit UTM possui uma interface moderna, de fácil utilização e responsiva, ou seja, ela é capaz de se adequar a tela de qualquer dispositivo utilizado para acesso (*tablets, smartphones, notebook*, etc.). Isso garante agilidade e facilidade para sua empresa, podendo ser acessado a qualquer hora e local.

Para acessar a Interface Web do Blockbit UTM, siga as orientações desta página.

Para Licenciar o UTM, cheque esta página.

Acessando a Interface Web – Blockbit UTM

Utilize um dos navegadores recomendados.

- 1. Conecte-se à internet e acesse o endereço: https://172.16.102.136:98. Caso tenha alterado o endereço IP, utilize o IP alterado;
- 2. Acesse utilizando os seguintes dados:
- User: O Login do usuário cadastrado, além disso, caso o E-mail tenha sido cadastrado, é possível utilizá-lo para efetuar o login. Ex.: admin;
- Password: Senha cadastrada;
- Language selection box: Define-se o idioma desejado para acessar a Interface Web. O idioma pode ser Inglês, Português ou Espanhol. Ex.: En glish.

| E | Bloo | ckb | it |
|----------|--------------|------------|----|
| Log | ç-in to yoı | ur account | : |
| A the | | | |
| A Heren | rd | | |
| English | | | - |
| English | | | |
| Portugué | s Brasileiro | | |
| | | | |

Tela de Login - Blockbit UTM

Clique no botão Login[

Login J para acessar a Interface Web.

Será exibido a tela principal do Blockbit UTM, denominada Dashboard.

| Blockt | oit | = | | | | | | | | 8.4 | = <u>1</u> - |
|------------------|------|-----------|---|--------|---------|---------|--------|--------|---|-------|--------------|
| • • • • • | • | Dashboard | | BHACK* | - | armente | and to | Barris | - | i i i | - |
| · Detherd · | | 0.008 🔶 0 | Å | 0.00B | • | 0 | Ģ | n | 0 | 0 | 0 |
| · Summer | | 1.55 | | | | | | | | | |
| i≥ Analymi | - 51 | | | | | 1100 | | | | | |
| · interes | | | | | | 3.586 | | | | | |
| al second in the | 10 | | | | | | | | | | |
| 12 Hang | - 50 | | | | | | | | | | |
| + mant | | hjepel | | | | - | | | | | |
| 0 5000 | | 4 Mart | | 4 | Apres - | a. 1140 | | | | | Riden . |

Tela principal do Blockbit UTM - Dashboards

Para mais informações sobre a Licenciamento, clique nesta página.

Caso deseje ver mais informações sobre a interface Web, clique nesta página.

Acessando a Interface Web – Licenciamento

Para a utilização dos recursos do Blockbit UTM é necessário realizar o licenciamento de sua instalação, siga os passos a seguir:

Para realizar o licenciamento do Blockbit Network Security é necessário estar conectado à internet e com acesso a Porta 443 sem proxy para os seguintes endereços: https://license.blockbit.com https://update.blockbit.com

Para aplicar ou renovar a licença de ativação é necessário fornecer o UUID - Indicador Único Universal do seu Blockbit UTM.

1. Para visualizar o UUID de seu equipamento acesse o menu Settings, na aba System:

| License Information | |
|-----------------------|--------------------------------------|
| Serial number | 564D539F-DE39-F996-7A1D-6001D6FE130B |
| License number | - |
| License status | Inactive |
| License registry date | - |
| License expire date | - |
| | |
| | |
| | |
| | |
| | |

Dashboard - System

• O widget License Information irá informar o Serial Number (ou UUID): Ex.: 564D539F-DE39-F996-7A1D-6001D6FE130B.

Ø

Também é possível descobrir o UUID usando do comando "show-uuid" no console. Para mais informações cheque esta página: [show-uuid].

- Copie o UUID e o encaminhe para seu canal de atendimento, para que seu número da licença seja fornecido;
 Você receberá o código *License number*, do seu canal de atendimento. Ex.: D845-61F9-9CBA-8145.

Ø], a tela abaixo será exibida: 2. Clique em [

| Atualizar Licença | × |
|--|----|
| License number | |
| D845-61F9-9CBA-8145 | |
| Terms | |
| BLOCKBIT | ^ |
| END USER LICENSE AGREEMENT | |
| BY CLICKING "CONTINUE", YOU OR THE ENTITY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS END USER LICENSE AGREEMENT ("AGREEMENT") WITH Cipher Security LLC AND ITS AFFILIATES ("BLOCKBIT"). IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO SUCH TERMS. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO THE FOREGOING, CLICK THE "CANCEL" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. IF YOU CLICK THE "ACCEPT" BUTTON TO CONTINUE WITH INSTALLATON YOU ARE REPRESENTING AND WARRANTING THAT YOU ARE AUTHORIZED TO BIND LICENSEE. | |
| 1. Grant of License and Restrictions. Subject to the terms hereof, payment of all fees, and any applicable user/use limitations, BLOCKBIT grants Licensee a personal, nonsublicensable, nonexclusive, right to use | • |
| Accept and Sav | ve |

Update License

• Serial Number: Digite o número da licença neste campo. Ex.: D845-61F9-9CBA-8145;



J a tela abaixo será exibida.

| License Information | đ |
|-----------------------|--------------------------------------|
| Serial number | 564D539F-DE39-F996-7A1D-6001D6FE130B |
| License number | D845-61F9-9CBA-8145 |
| License status | Inactive |
| License registry date | - |
| License expire date | - |
| | |
| | |
| | |
| | |
| | |

Update License - Inactive

Após salvar a licença, a solicitação será enviada para uma fila de comando onde poderá ser aplicada no sistema. Para acessar a fila de comandos, clique

em [=]]. A tela abaixo exibe a fila de comandos no aguardo para serem executados;

| | | A | |
|-------------------|-------|---|---------|
| Settings > System | | | Waiting |
| | Apply | | |

Apply queue

• Após clicar em [Apply], aguarde até o sistema aplicar as configurações referentes ao licenciamento do produto. Conforme demonstrado abaixo:



Update License - Active

Isso conclui o licenciamento do produto.



Para mais informações sobre a Operação básica do UTM, clique nesta página.

Caso deseje ver mais informações sobre a interface Web, clique nesta página.

UTM - OPERAÇÃO BÁSICA

O Blockbit UTM é composto de algumas funcionalidades básicas que estão disponíveis em diversos painéis diferentes, de forma a facilitar sua utilização, segue um guia básico de como utilizar esses recursos:

Barra de busca

A barra de busca, fica alocada no topo dos painéis e possibilita localizar itens específicos.



| | ~ | |
|----------|------|----------|
| Botão do | menu | de ações |

Ao clicar neste botão, um menu com um conjunto de opções contextuais ao painel onde ele estiver localizado será exibido, por exemplo:

| ۹ 🗸 |
|-----------------|
| Create Group |
| Delete Groups |
| Create Policy |
| Delete Policies |
| Expand All |
| Collapse All |
| Menu de ações |

Quantidade de Resultados

Na parte inferior da tela, é possível selecionar quantos resultados serão exibidos por página, sendo o mínimo 10 e o máximo de 40 itens por página.



Quantia de resultados

Por fim, quanto a navegação, os botões de "Alternar Páginas" permite navegar entre as páginas.



UTM - OPERAÇÃO BÁSICA

O Blockbit UTM é composto de algumas funcionalidades básicas que estão disponíveis em diversos painéis diferentes, de forma a facilitar sua utilização, segue um guia básico de como utilizar esses recursos:

Barra de busca

A barra de busca, fica alocada no topo dos painéis e possibilita localizar itens específicos.



| | ~ | |
|----------|------|----------|
| Botão do | menu | de ações |

Ao clicar neste botão, um menu com um conjunto de opções contextuais ao painel onde ele estiver localizado será exibido, por exemplo:

| ۹ 🗸 |
|-----------------|
| Create Group |
| Delete Groups |
| Create Policy |
| Delete Policies |
| Expand All |
| Collapse All |
| Menu de ações |

Quantidade de Resultados

Na parte inferior da tela, é possível selecionar quantos resultados serão exibidos por página, sendo o mínimo 10 e o máximo de 40 itens por página.



Quantia de resultados

Por fim, quanto a navegação, os botões de "Alternar Páginas" permite navegar entre as páginas.



UTM - MENU DE PERFIL DO USUÁRIO

O menu de perfil do usuário encontra-se localizado no canto superior direito da tela. Para acessar basta clicar no ícone user





Menu de perfil do usuário

O menu de perfil do usuário é composto das opções:

- Profile;
- Logout.

A seguir eles serão explicados detalhadamente.

UTM - Profile

Na opção "Profile" é possível editar as informações de perfil do usuário. Para acessá-lo, siga os seguintes passos:

1. No canto superior direito. Clique na opção "Profile";



Menu do usuário - Botão "Profile"

2. Realize as alterações de edição de perfil desejadas. Esta tela contém as seguintes informações:

- Name: O nome do usuário cadastrado;
- Email: O e-mail do usuário cadastrado. Este campo é utilizado para realizar o login no Blockbit GSM;
- Password: Caso deseja alterar a senha, insira-a neste campo;
- Password Confirmation: Caso necessário, confirme a senha digitada no item anterior.

A senha deve conter maiúsculas, minúsculas, números, deve possuir mais de 4 caracteres, e não pode conter os seguintes caracteres especiais: * & | ; > < ' .

Profile

4

| Name | | |
|---------------------------|---------------------------------------|-------|
| Administrador | | |
| Email | | |
| admin@blockbit.com | | |
| Password (fill to change) | | *1 |
| ••••• | | |
| Password confirmation | | |
| ••••• | | |
| | | |
| | | |
| | | 🖺 Sav |
| | | |
| | Menu do usuário – <i>Edit Profile</i> | |
| | | |

Para sair desta janela, basta clicar em [X] do topo direito da tela para voltar à janela anterior.

🖺 Save

Clique no botão **Save**[realizado novamente.] para salvar as alterações, caso a senha tenha sido alterada, o sistema irá atualizar e solicitar que o *Login* seja

UTM - Logout

A qualquer momento é possível sair do sistema. Basta clicar no botão "Logout".



Menu do usuário – Botão "Logout"

Isso levará o usuário de volta a página de "Login".

UTM - ASSISTENTE DE INSTALAÇÃO

Esta seção irá apresentar como configurar o Assistente de Instalação do Blockbit UTM.

A seguir será apresentado o processo de instalação e o correto preenchimento de todos os campos requisitados pelo formulário.

Instalação do Blockbit UTM

Para instalar o Blockbit UTM, siga os seguintes passos:

1. Conecte no navegador de internet e acesse o endereço: https://172.16.102.136:98. Caso tenha alterado o endereço IP, utilize o IP alterado;

| E scontone e | 140. · | | | 0.1 |
|--------------|--|--|-----------|-----|
| + Children 1 | and ATL NO. NO. IN CONTRACTOR OF A DESCRIPTION OF A DESCR | | | 911 |
| | H A Software presenter percent | | Contigues | |
| | 110 dist. No an el filma de porte la straja | | | |
| | Derver until ngs Perspese Perspese Perspese Personal | Andrease princetto P | | |
| | Martin Land Contractor | | | |
| | Card Dyala James | Not . | | |
| | | me tet Manhatine | | |
| | Tent | Superior State | | |
| | agencipres) | Barbaran - malandal an | | |
| | Automation in the second se | Antonio | | |
| | Information and American | Allow one passion of | *** | |
| | | Circle and | | |
| | | | | |

Installation Wizard

2. Digite os seguintes dados no frame "Server settings", para as configurações iniciais de rede do Blockbit UTM:

- Description: Campo para descrever o nome do servidor. Ex.: Blockbit UTM;
- Language: Selecionar o idioma padrão. Ex.: English;
- Time Zone: Selecionar o fuso horário no qual sua empresa se encontra. Ex.: America/New York;
- NTP Server: Defina o servidor de sincronização de relógio. Ex.: pool.ntp.org;
- Hostname: Nome do Hostname. Pode ser qualquer um desde que esteja conforme padrão FQDN Fully Qualified Domain Name. Ex.: utm. blockbit.com;
- DNS suffix: Domínio da rede. Ex.: blockbit.com;

- DNS server 1: Defina o servidor DNS da rede ou da internet. Ex.: 176.16.102.161;
- DNS server 2: Defina o DNS secundário da sua rede ou da internet;
- Gateway: Defina a rota padrão da rede. Ex.: 176.16.102.1;
- Integrity key: Chave de integridade do sistema, utilizada no processo de criptografia dos arquivos de backups. Este campo é gerado automaticamente.

3. Digite os seguintes dados no frame "Certificate", estas informações serão utilizadas para a criação do certificado SSL no console de administração do Blockbit UTM:

- Country: Defina o país. Ex.: US;
- State: Defina o estado. Ex.: New York;
- City: Defina a cidade. Ex.: New York;
- Organization: Defina o nome da empresa. Ex.:Blockbit;
- E-mail: Defina o e-mail do administrador. Ex.: admin@blockbit.com;
- Organizational Unit: Defina o departamento. Ex.: QA;
- Expires (years): Defina o tempo de validade do certificado. Ex.: 10 anos;
- Hostname: Defina o FQDN para o certificado. Ex.: utm.blockbit.com.

4. Digite os seguintes dados no frame "Authentication", define o domínio local padrão para a autenticação de usuários do Blockbit UTM.

• Default domain: Defina o domínio default de autenticação. Ex.: blockbit.com.

5. Digite os seguintes dados no frame "Administration", a senha do usuário "admin" da console de administração do Blockbit UTM:

- Admin user password: Insira uma senha com no mínimo oito caracteres. A senha deve conter letras maiúsculas, minúsculas e caracteres especiais. Ex.: q1W@e3R\$;
- Confirmation Save: Confirme a senha inserida acima.

6. Clique no botão "Save". A tela abaixo será exibida solicitando a confirmação, ao clicar em "ok" o sistema irá aplicar as configurações e será reinicializado.

| Hereigner Hittig Soldande | Name And Market Market Market | 18 | |
|---------------------------|--|--|------------|
| - | Yes | | |
| | Aprenda Armer Aproprior () Aproximation Apr | | |
| | Admendiation Administration and Continuation | | |
| | | Administration Administration Administration Administration Calification Calification | Adversaria |

Installation Wizard – Formulário

• Clique no botão "OK". O sistema irá aplicar as configurações e será reinicializado.

Ao finalizar esses passos o Assistente de Instalação terá sido finalizado com sucesso. Aguarde a inicialização, o navegador fará um AUTO-REFRESH do endereço de acesso à interface WEB e retornará a interface de logon.



Tela de LOGON de administração do Blockbit UTM

UTM - FILA DE COMANDOS

Ao executar comandos entre as interfaces *Frontend* e os serviços de *Backend* do sistema, todas essas instruções são ordenadas de acordo com a prioridade pela fila de comandos, certificando-se que as configurações sejam aplicadas na ordem correta.

Para visualizar a fila de comandos, basta clicar no ícone localizado no topo direito da tela, do lado do menu do usuário:



| | | A | |
|------------------|-------|---|---------|
| Serviços > Proxy | | | Waiting |
| | Apply | | |

Fila de comandos pendentes

Nesta fila, é exibido o caminho até o comando, seu status atual, a barra de progresso até sua conclusão e finalmente, o botão de apply para executar todos os comandos desta lista.

Para aplicar todos os comandos, basta clicar no botão [Apply], o processo iniciará, como exemplificado pela imagem abaixo:

| | ï | A | |
|------------------|-------|---|---------|
| Serviços > Proxy | | | Running |
| | Apply | | |

Fila de comandos em progresso

Ao término deste processo ou caso, não haja nenhum comando a ser aplicado a lista será exibida em branco:

| | | A | |
|---------------|------------|---|--|
| No item found | | | |
| Арр | ly | | |
| Fila de Comar | ndos Ocios | а | |

UTM - NOTIFICAÇÕES

r

Ŀ.

Alguns eventos que ocorrerão no Blockbit UTM irão gerar alertas, estes serão exibidos no painel de notificações, elas são configuradas na aba Notificationa em System no menu Settings, para mais informações consulte esta página.

Para visualizar as notificações, clique no ícone notifications 🛕 localizado no canto superior direito da tela, ao lado da fila de comandos.

| Noti | ifications | | × |
|------|------------------|------------------|---|
| | 22-01-2020 11:42 | Outdated license | 0 |
| | 22-01-2020 11:42 | Outdated license | 0 |
| | 22-01-2020 11:32 | Outdated license | 0 |
| | 22-01-2020 11:31 | Outdated license | 0 |
| | | | |

Clear

7

Painel de Notificações

Para saber ter mais informações a respeito da notificação, deixe o mouse em cima do ícone de **informações** [1], uma janela com detalhes relevantes será exibida:

Notifications



×

UTM - MENU DE OBJETOS

Para agilizar o processo de configuração do Blockbit UTM, no topo da tela o menu de objetos disponibiliza a possibilidade de criar um objeto imediatamente ou acessar o painel de objetos.

Para acessar o menu de objetos basta clicar no ícone objects[



O menu é composto de todos os tipos disponíveis no painel de objetos:

- Address;
- Service;
- Time;
- Schedules;
- Dictionaries;
- Content.

Ao clicar em alguma destas opções, surgirá uma janela de criação de objetos idêntica à exibida no painel de objetos, por exemplo:

| Blockbit = | | | | | | | |
|-------------|--|------------------|-----------------|------------|-------|-------|--------|
| | Objects | Daala Athrono Ob | Ret | | | | |
| a | 1000 | TIMPE | | | | | |
| diame 1 | - | - 104 | | | | | |
| Section 1 | Contraction of the local data | (database) | | - 10 min 1 | | | |
| diame A | and the second s | · Address | Mark. | | 3123 | 10000 | APLC - |
| 2 mm - | TO DE LA DELLA DEL | Sec | (0.05.05.05 | | | | |
| 1. market | Contraction of the | | | 100 | 100 | | - 20 |
| 1.0.000 | | | | - 111 | | | See. |
| | Charles and Charles | beactprise. | | | 1.000 | | 1 |
| a statement | Paratest | | | - 11 | | 0 | 1.00 |
| a contract | - and a | | | | 1.000 | | 2.2 |
| 1.000 | - Anna income | - | Carlos I Carlos | | 1.000 | | 1.2 |
| 4 | and shares in | | | | 1.000 | | 13 |
| B Second | - Annual and | | | | 100 | | 11-1 |
| | | | | | | | |

Menu de Objetos - Criando objeto de endereço

Por fim, ao clicar em [View all], você será redirecionado para a tela de objetos.

UTM - MONITOR

No Monitor as informações coletadas nos módulos de segurança são reunidas e exibidas de forma sumarizada por usuários, grupos, serviços, políticas, w eb filter, aplicativos, ameaças entre outros.

Este recurso proporciona uma visão abrangente e dinâmica dos eventos na rede e de seus usuários, viabilizando uma gestão mais precisa e facilitando tomadas de decisão.

Através do Monitor, o administrador consegue entender rapidamente o que está acontecendo na rede, sem gastar tempo correlacionando milhares de linhas de log ou eventos.



Monitor

Contém as opções:

- Dashboard;
- ٠ Live Sessions;
- Traffic Monitor,
- System Status;
- Security Events;
 Diagnostics;
- ٠ Reports.

Monitor - Dashboard

O Dashboard exibe em tempo real o estado atual do sistema de forma centralizada e consistente através de vários *logs* sumarizados os principais eventos do sistema, histórico de acesso de usuários, monitor de tráfego e diversos outros registros que podem ser utilizados para análise de risco, comportamento e impacto no uso da banda.

O Dashboard propicia acesso em tempo real de forma centralizada e consistente a vários logs sumarizados, eventos dos principais serviços do sistema, histórico dos usuários e diversos outros registros. Estes recursos podem ser utilizados para análise de comportamento do usuário, risco e impacto no uso de banda, também exibe alertas, notificações em tempo real e que podem ser disparados através de agendamento.

O Dashboard exibe informações referentes aos últimos 5 minutos ou à última hora em seus widgets (graças à característica de ser um monitor em tempo real, o Traffic Monitor sempre irá exibir os últimos 5 minutos).

Por padrão, todas as informações dos relatórios detalhados, de todos os módulos, são armazenadas por 7 (sete) dias ou até atingir 70% de uso do disco. Caso a capacidade máxima de armazenamento seja atingida, a retenção destas informações será interrompida. Caso deseje alterar este limite de armazenamento, acesse System - Aba Logging em settings.

Ao se logar no Blockbit UTM, a opção "Dashboard" do menu "Monitor" estará automaticamente selecionada. Caso seja necessário, é possível acessar o "Dashboard", clicando na opção localizada no menu vertical lateral, conforme exibido abaixo.

| 🚯 Monitor 🛛 👻 | | | | |
|---------------|-----------------|--|--|--|
| » | Dashboard | | | |
| » | Live Sessions | | | |
| » | Traffic Monitor | | | |
| » | System Status | | | |
| » | Security Events | | | |
| » | Diagnostics | | | |
| » | Reports | | | |
| | | | | |

Monitor - Dashboard

A tela abaixo será exibida:




A janela de Monitor - Dashboard permite definir a exibição das informações dos widgets no período dos últimos 5 minutos ou da última hora, através do menu localizado no topo direito dessa tela, conforme exibido na imagem abaixo:

| Last 5 minutes | \wedge |
|----------------|----------|
| Last 5 minutes | |
| Last hour | |

Dashboard - Menu

- Last 5 minutes: Ao selecionar essa opção, os widgets passarão a exibir os resultados referentes aos últimos 5 minutos. Por padrão, esta opção estará pré-selecionada;
- Last Hour: Ao selecionar essa opção, os widgets passarão a exibir os resultados referentes à última hora.



Os relatórios e gráficos disponíveis no Dashboard são:

- Network Traffic;
- Live Users;
- Web Activity; ٠
- Network Attacks;
- Malware Detections;
- Threat Blocking;
- ٠ Connections Map;
- Traffic Monitor;
- Top Users;
- Top Sources;
- Top Services;
- •
- Top Policies; Top Categories; •
- Top Applications;
- Top Attacks;
- Top Malware.

A seguir, analisaremos cada um dos componentes do painel Dashboard.

Dashboard - Widgets

A principal função do *Dashboard* é proporcional uma visão holística do sistema em tempo real de forma clara e objetiva, para tanto o painel é composto de diversos *widgets*, focados em exibir dados específicos do estado atual do sistema.

A seguir analisaremos cada um deles:

Network Traffic

O widget "Network Traffic" exibe o volume total de todo o tráfego de rede realizado em todas as interfaces de rede do Blockbit UTM.



Live Users

O widget "Live Users" exibe quantos usuários estão online neste momento no Blockbit UTM.



Web Activity

O widget "Web Activity" exibe o total de todo a atividade web realizada em tempo real no Blockbit UTM.



Network Attacks

O widget "Network Attacks" exibe o volume total de tentativas de ataques realizados em todas as interfaces de rede do Blockbit UTM.



Malware Detections

O widget "Malware Detections" exibe o total de malwares detectados em todas as interfaces de rede do Blockbit UTM.



Threat Blocking

O widget "Threat Blocking" exibe o total de ameaças bloqueadas através de todas as técnicas do módulo Advanced Threat Protection (ATP) em todas as interfaces de rede do Blockbit UTM.



Connections Map

Em "Connections Map" é exibido o destino das conexões dos usuários da rede, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários.

Além disso, ao passar o mouse por cima dos países, o país referente a esse valor é destacado no mapa e um número total de acessos é exibido.



Dashboard – Connections Map

Traffic Monitor



Em "Traffic Monitor", é possível visualizar o tráfego de rede em tempo real. Ao passar o mouse por cima do gráfico, um resumo de todo o tráfego do período é exibido.

Dashboard – Traffic Monitor

Top Users

Em "Top Users", temos uma listagem de dez usuários classificados por ordem de maior quantia de acessos e seu respectivo consumo e seu respectivo uso.

| Тор | Users | |
|-----|------------------|--------|
| # | User | Bytes |
| 1 | user1@domain.com | 30.00B |
| 2 | user2@domain.com | 30.00B |
| 3 | user3@domain.com | 30.00B |
| 4 | user4@domain.com | 30.00B |
| 5 | user5@domain.com | 30.00B |
| | | |

Dashboard – Top Users

Top Sources

Em "Top Sources", temos uma listagem de dez maiores fontes de tráfego de rede classificadas por ordem de acesso e seu respectivo uso.

| Top S | Sources | |
|-------|----------------|---------|
| # | Source | Bytes |
| 1 | 172.31.240.24 | 3.65MB |
| 2 | 172.31.190.251 | 46.57KB |
| 3 | 172.31.102.184 | 13.08KB |
| 4 | 172.16.100.144 | 2.93KB |
| 5 | 172.31.240.20 | 2.81KB |
| 6 | 172.31.250.163 | 2.52KB |
| 7 | 172.31.240.252 | 1.61KB |
| 8 | 172.31.240.251 | 1.54KB |
| 9 | 0.0.0.0 | 1.34KB |
| 10 | 172.31.0.100 | 1.15KB |

Dashboard – Top Sources

Top Services

Em "Top Services", temos uma listagem de dez tipos de serviços mais usados, sendo estes classificados por ordem de uso.

| Тор | Services | |
|-----|-------------|---------|
| # | Service | Bytes |
| 1 | ssh | 3.65MB |
| 2 | netbios-ns | 57.25KB |
| 3 | netbios-dgm | 10.35KB |
| 4 | tacnews | 2.93KB |
| 5 | ntp | 2.81KB |
| 6 | bootps | 1.34КВ |

Dashboard – Top Services

Top Policies

Em "Top Policies", temos uma listagem das dez políticas mais aplicadas por ordem de maior quantia de utilização e seu respectivo consumo.

| ор | Policies | |
|----|----------|---------|
| # | Policy | Bytes |
| 1 | DHCP | 1.97KB |
| 2 | NAT DNS | 266.00B |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Dashboard – Top Policies

Top Categories

Em "Top Categories", temos uma listagem das dez categorias classificadas por ordem de maior quantia de acessos e seu respectivo uso.

| Top C | ategories | |
|-------|---------------------------------------|---------|
| # | Category | Bytes |
| 1 | Uncategorized Sites | 733.00B |
| 2 | Advertisements | 139.00B |
| 3 | Information Technology | 97.00B |
| 4 | Peer-to-Peer File Sharing | 80.00B |
| 5 | Business and Economy | 74.00B |
| 6 | Professional and Worker Organizations | 45.00B |
| 7 | Web Hosting | 30.00B |
| 8 | Computer Security | 16.00B |
| 9 | Entertainment | 10.00B |
| 10 | Search Engines and Portals | 8.00B |

Dashboard – Top Categories

Top Applications

Em "Top Applications", temos uma listagem de dez tipos de aplicações mais usadas, sendo estas classificadas por ordem de uso.

| Тор А | pplications | |
|-------|---------------|------|
| # | Application | Hits |
| 1 | BitTorrent | 840 |
| 2 | QUIC | 46 |
| 3 | Doubleclick | 18 |
| 4 | Yahoo! | 14 |
| 5 | CDN | 10 |
| 6 | Tidal | 8 |
| 7 | Facebook | 6 |
| 8 | In | 5 |
| 9 | BitTracker | 5 |
| 10 | Reality Kings | 4 |

Dashboard – Top Applications

Top Attacks

Em "Top Attacks", temos uma listagem dos dez tipos de ataque cibernéticos mais recorrentes, sendo estes classificados por ordem de ocorrência.

| Тор / | Attacks | |
|-------|--|------|
| # | Attack | Hits |
| 1 | Apache Struts wildcard matching OGNL remote code executi | 28 |
| 2 | Microsoft ASP.NET bad request denial of service attempt | 4 |

Dashboard – Top Attacks

Top Threats

Em "Top Threats", temos uma listagem dos dez tipos de ameaça mais recorrentes, sendo estes classificados por ordem de ocorrência.

| Тор | Threats | |
|-----|---------|------|
| # | Threat | Hits |
| 1 | malware | 57 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Dashboard – Top Threats

Para acessar relatórios mais específicos, cheque as opções disponíveis no Analyzer.

Monitor - Live Sessions

Este recurso permite que o administrador monitore o tráfego de rede em tempo real, determinando com garantia qual acesso (ou tentativa) gerou *log.* O sistema está dividido em dois tipos: *Firewall* e *Web*, o primeiro efetua o monitoramento de todo o tráfego realizado no *firewall* e o segundo executa monitoramento de todo o tráfego *web*.

Para acessar esta tela, basta selecionar a opção "Live Sessions".



Monitor – Live Sessions

A tela abaixo será exibida:

| pe Presed () Veb (| | State State () Here | | | () IN COMP. | 346 | |
|-----------------------|--|------------------------|------|----------|---------------|--------|--|
| HER . | Soares | Deptination | Port | Protocal | THE | Policy | |
| de general i | and the second s | investments. | | | and so in the | Select | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Monitor - Live Session - Live Connections

A tela *Live Sessions* comporta as seguintes abas:

- Connections;
- Users;
- VPN.

A seguir analisaremos os componentes da aba Live Connections.

Live Sessions - Connections

Nesta aba é possível averiguar a atividade atual no firewall e na web, sendo possível filtrar por usuário, origem, destino, porta, protocolo ou política.

Para acessar, caso a aba não esteja selecionada, clique em "Connections".



Surgirá a tela "Connections", conforme demonstrado pela imagem abaixo:

| /2° D Dressail | O Web | | Status Esta | otated 🔘 New | | | View 30 (100) | - 205 | |
|---------------------|-------|---------|----------------|--------------|---------|----------|------------------|--------------------|---------|
| une : une (Educe | | Solatos | Destinat | tion - | Port | Protocol | MAC | Policy select ~ | -30 |
| (i) | User | Source | Destination | Port Prot | acol Ma | AC Byt | is i Packages i | Policy | Actions |
| | User | Source | Destination | Port Prot | acol Ma | NC Byto | es i Packages i | Policy | Actions |
| | | | | | | | | | |
| | | | | 1 | N Tarta | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Connections

Esta sessão irá abordar:

- Componentes deste painel;
- Monitoramento de todo o tráfego realizado no firewall;
- Monitoramento de todo o tráfego realizado na web.

A seguir, analisaremos os componentes deste painel.

Connections - Componentes

O painel Connections é composto dos seguintes recursos:

| pe Hrewall | Web | | Status Es | tablated 🔘 New | | | Wess 34 | 200 | |
|---------------|------|-------------|--------------|----------------|-------|----------|------------------|--------|--------------|
| se | | Source | Deutin | ation | Port | Protocol | MAC | Policy | |
| ere@dataire | | 10.44(0):40 | 164 | | 1.000 | 704 | 40.1218/9576-1 | select | - Sta |
| | | | | | | | | | |
| 6 | lser | Source | Destination | Port Prote | | ιC θyt | tes i Packages i | Policy | Actions |
| 0 | Iser | Source | Destination | Port Prote | | C Byt | es i Packages i | Policy | Actions |

- Type: Determina o tipo de monitoramento estre as opções:
 - Firewall J: Ao selecionar esta opção, se opta pelo monitoramento de todo o tráfego realizado no firewall;
 - Webl J: Ao selecionar esta opção, se opta pelo monitoramento de todo o tráfego web. Este tipo de monitoramento só verifica novas conexões, desabilitando o campo status.
- Status: Determina o tipo de estado que será monitorado entre as opções:
 - Established[]: Ao selecionar esta opção, serão exibidas as conexões TCP estabelecidas e seus detalhes. Esta opção desabilita o campo view;
 - New[]: Ao selecionar esta opção, serão exibidas as novas conexões (aceitas, rejeitadas e bloqueadas) em qual política a conexão foi tratada.
- View[]: Determina a quantia de resultados visualizados, podendo ser de 50, 100 a 200 resultados;
- User: Neste campo, é possível determinar um usuário, para ser usado como filtro durante o monitoramento;
- Source: Neste campo, é possível determinar um IP de origem, para ser usado como filtro durante o monitoramento;
- Destination: Neste campo, é possível determinar um URL de destino, para ser usado como filtro durante o monitoramento. Neste campo é necessário adicionar a URL completa do destino. Ex.: "https://www.blockbit.com/solutions/network-security/";
- Port: Neste campo, é possível determinar uma porta, para ser usada como filtro durante o monitoramento;
- Protocol: Neste campo, é possível determinar um tipo de protocolo, para ser usado como filtro durante o monitoramento;
- Policy: Nesta lista suspensa, é possível determinar uma política, para ser usada como filtro durante o monitoramento. As políticas disponíveis nesta lista são criadas em UTM - POLICIES.
- CGNAT: O Carrier Grade Network Address Translator, consiste em uma solução de NAT que opera a nível provedor, na distribuição de IPs e tradução de endereços.

Os resultados são exibidos na tabela abaixo das opções:

| Live Se | ssions | | | | | | | | | | |
|--|----------|----------------|----------------|-----------|----------|-----|----------|--------|------------|--------|---------|
| Connectio | ne Users | 977 W | | | | | | | | | |
| Type Firews | el 🔿 wee | | Status Esta | bisted | O New | | | View | 0 0 100 | 200 | |
| User | | Source | Destinat | tion | p | urt | Pretocol | MAC | | Policy | |
| integration of the second seco | risi() | iPut/Pot | 10,001 | ruf;to,o) | | | 109 | | alussum. (| Select | - Ratio |
| (8) | User | Source | Deutination | Port | Prohocol | MAC | D | fena û | Packagen 1 | Policy | Actions |
| | | 172.31,208.179 | 172.18.11.245 | 53 | UD# | 5 | 4 | 16,009 | 4 | 100 | |
| | | 172.33,200.378 | 172,13,13,245 | 52 | UDP. | | | 16,000 | - 4C | | ж |
| | | 172.31.208.339 | 172.18.13.265 | 50 | 00P | - K | | 10.008 | 4 | 342 | |
| | | 172.33.200.178 | 172.18.13.245 | 53 | 0DP | | | 14.008 | - 81 | 222 | ж |
| | | 172.34,208.379 | 172.18.13.242 | 10 | UDP. | 2 | | 14.000 | - 80 | 3.83 | |
| | | 172.31.108.178 | 172,56,13,248 | 53) | UDP. | | | 16,000 | 43 | | |
| | 100 | 172-12-508-126 | 1723613.945 | - 61 - | ine | | : | ADD IN | 11 | 122 | 120 0 |

Connections - Results

A seguir, vamos analisar cada componente desta tabela:

- User: Exibe o usuário relacionado ao acesso, caso contrário apresenta um "-";
- Source: Exibe o IP da origem do acesso;
- Destination: Exibe o IP do destino do acesso;
- Port: Exibe a porta utilizada no acesso;
- Protocol: Exibe o protocolo utilizado no acesso;
- Policy: Exibe a política aplicada ao acesso, caso não tenha nenhuma política relevante apresenta um "-";
- Actions: Permite deletar a conexão ao clicar no botão [], uma janela de confirmação será exibida conforme demonstrado abaixo:

Do you want to delete this connection?

172.16.100.144 > 172.31.240.30:98

| Cancel | Proceed |
|--------|---------|
|--------|---------|

Do you want to delete this connection

ATENÇÃO: Algumas aplicações possuem recursos para renovar ou manter a conexão, graças à essas características, essa opção não necessariamente irá interromper qualquer tipo de conexão. Para certificar-se que o bloqueio será instaurado, é recomendável criar uma política impedindo o acesso. Para mais informações sobre como criar políticas, consulte esta página.



Connections - Firewall

A seguir exibiremos alguns exemplos de como efetuar o monitoramento de conexões ativas no firewall.

Firewall - Established

Para efetuar o monitoramento, configure a aba Connections conforme demonstrado à seguir:

| Pinevili 🔿 Hida | | Materia Catalitation Intern | | Vice 10 200 | 208 |
|-----------------|---------|--------------------------------|---------------|---|-----------|
| | Sector | Deptileation | Pest Protonal | MAL | Pelky |
| | and the | Pyl Princi | 40 100 | (main section of the | 3442 - 10 |
| | | | | | |
| | | | | | |
| | | | | | |

Connections- Firewall - Established

Feito isso, clique no botão Start

Type: Selecione a opção *Firewall*; *Status:* Selecione a opção *Established*;



], os resultados serão exibidos conforme demonstrado abaixo:

| 1939 (* 11 | a dian | | Statue | | iner 1 | | 10.0 | (in 10) | 1.44 | |
|---------------|--------|------------------|---------------|------|----------|------|----------|-----------|---------|-------|
| | | Source | Intina | tion | Paint | Pept | acid MAC | | Publicy | |
| | 191 | Perille | | | | | 5.11 | | | - |
| (E) | 000 | Some | Derivative | Peri | Pretocol | MAC | Bytas 1 | Perkego 1 | Policy | Attes |
| | | 17131306136 | 1752633280 | 39 | 104 | | 40.015 | 4 | | |
| | | 111.01.018.170 | 179,26,21,219 | - 28 | 100 | | 419.308 | | | |
| | | 175.00.006.036 | 112263526 | -10 | 104 | | 416,008 | | | |
| | | 10131308170 | 10.mm240 | 24 | UD# | | 410,308 | - ÷. | | |
| | | 17131205120 | 175.56.35.549 | - 16 | 107 | | 415.218 | + | | |
| | | 17131306.070 | 17518-8341 | - 10 | 1.0* | | 414,018 | 4 | | |
| | | 125.45 (100.100) | Decourage of | | | | 1.00000 | | | |

Connections - Firewall - Established - Results

Para interromper o monitoramento basta clicar no botão Stop

Firewall - Established - Source

Também é possível realizar filtro de busca por agrupamento do tipo Source e Destination quando o status for do tipo Established. Segue um exemplo de como efetuar monitoramento de *IP* de origem:

| Elevent Steh | | Status Lockbord | | 2 58 180 | 180 |
|--------------|--------------|--------------------|-------------|----------|-------|
| sar | 56800 | pestination | Per retical | MAC | Nia |
| | 112.06.12.02 | Programme . | 4 0 | | MAC - |
| | | | | | |
| | | | | | |
| | | | 100 | | |

Connections - Firewall - Established - Source IP

- Type: Selecione a opção Firewall;
- Status: Selecione a opção Established;
 Source: Digite o IP de origem que será filtrado. Ex.: 172.16.12.62.

], os resultados serão exibidos conforme demonstrado abaixo:

| - | 4. 1/ hour | | the late | atori (| - | | 6 | 10.14 | | |
|---|------------|-------------|--------------|---------|----------|--------|----------|------------|--------|---------|
| | | Search | Distinut | dani | Peri | Pretac | d MAC | | Policy | - |
| | User | Source | Dethatlar | Pet | Protocol | MIC | Signe () | Packages 1 | Policy | Actions |
| | | 101010 | 111/03/06/79 | 14 | 309 | | 40000 | 39 | | |
| | | 1/210-02-02 | 012123420 | н | 101 | | Tatiya | 4 | | |

Connections - Firewall - Established - Source IP - Results

Stop

Para interromper o monitoramento basta clicar no botão Stop

Firewall - Established - Destination

A seguir veremos um exemplo de como efetuar monitoramento de IP de destino:

| Grand C Water | | Status Constitu | andred () now | Lat. | Destroyal | Veve (a) Set [] (100.] | 220) Rođen | |
|---------------|---------|--------------------|---------------|-------|-----------|----------------------------|---------------|---------|
| | p-sona | 171.1 | 120419 | - | 12 | Carry Laboratory | Jump. | - |
| C. Stern | Source. | Destruitore | Fed Dete | an 19 | uic be | te i foctape i | Pelky | Acidoes |
| | 30,00 | (resident) | 100 000 | | | or i souperi. | hint | |
| | | | | | | | | |
| | | | | | | | | |

Connections - Firewall - Established - Destination IP

- *Type:* Selecione a opção *Firewall*; *Status:* Selecione a opção *Established*; *Destination:* Digite o *IP* de destino que será filtrado. Ex.: 172.31.208.75.

| Feito isso, clique no botão Start | Start |], os resultados serão exibidos conforme demonstrado abaixo: |
|--|-------|--|
| | | |

| P ⁴ | - | | 5545.6 | | 1.44 | | Nev = | i Santa | 144 | |
|----------------|-----|-------------|---------------|------|----------|-------------|-----------|------------|--------|---------|
| lans - | | Source | Berthu | fiet | 9 | loet Prod | Not Mad | 5 | Policy | |
| | | | | | | | | | | 1 |
| | 8 M | Spend | Derfinitie | Port | Protocol | MAC | Bytes : | Pockager 1 | Policy | Actions |
| | | 112363245 | 177.01.208.19 | 70 | 71,9 | | 24,4890 | 36 | | |
| | | L*LILAMP | 10.10.0479 | .14 | 100 | miscorrowci | E DAME | 62.A | | |
| | | 112,25,4,44 | 172.51.208.19 | 11 | 11.9 | morroace | 415 10 10 | 416 | | |
| | | 172.25.048 | 171.21.29.71 | - 32 | 107 | 00000755600 | 0. 10040 | 38 | | |
| | | 121314230 | 1223120679 | 14 | 1107 | | 1.00.000 | 10 | | |

Connections - Firewall - Established - Destination IP - Results

Para interromper o monitoramento basta clicar no botão Stop[



Firewall - New

Ao clicar sobre o status New e type Firewall, é possível realizar o monitoramento de novos acessos.

| Grout Nob | Sec. and | Staten Latakifakturi 🛞 Itom Jaurikastan | Sect Personal | 944 | |
|-------------|----------|---|---------------|------------------------|---------|
| a-Deservers | Publica | PARAME | 10 TP | looma . | - |
| tse | George C | icotination Port Posts | of the b | viez i Pacheger Polity | Actions |
| | | | | | |
| | | | | | |
| | | | | | |

- *Type:* Selecione a opção *Firewall*; *Status:* Selecione a opção *New*. •
- ٠

Start

Feito isso, clique no botão Start

], os resultados serão exibidos conforme demonstrado abaixo:

| Convections Units | 100 | | | | | | | |
|------------------------------|---------------|-------------------------|---------|-----------|------------------|------------------------|---------|---|
| type (a) Consult (C) mate | | tion () thereas a ve | 2 | | Virus (c) (c) | | | |
| User | Source | 3 extinution | Ret | Protectal | Policy | | | |
| inspired. | and the | Partnersd | - | | | | | |
| . Uner | Seuto | deades | dies . | Port | Protocol | Pulky | Actions | |
| | 101.006.79.10 | | | 10 | 127 | Vesilies NU-los -1-10 | | 1 |
| | 110,008,75,19 | 177.200. | 84.274 | 07133 | ute . | Westwee 190,059,75 [J. | | |
| | 10.00.00 | 175.200 | 9.388 | \$2584 | SEP.1 | WebCom DIL 198,75.18 | | |
| 1.00 | 10.198.75.18 | 166.232 | 25.98 | 18743 | sar | BECONTY_PSI | - 10 | |
| | 112.008,75.10 | 101.000 | 10.000 | 30031 | 75P | 00008379_900 | .0 | |
| | 101.004.79.10 | 101-101 | 100,000 | intist. | URP | 00010070_9101 | - 12 | |
| | 1012057520 | 100.02.4 | 101 | 00228 | 712 | BECORD 707, PSD | 0 | |
| | 101.000.01.00 | 109-00- | e.tes | 32238 | ver | HELLINTE, MO | | |
| | | | | | | | | |

Connections - Firewall - New - Results

Para interromper o monitoramento basta clicar no botão Stop

Para mais informações a respeito de cada campo desta tela, cheque esta página.

Connections - Web

A seguir exibiremos alguns exemplos de como efetuar o monitoramento de todo o tráfego web

Web - New

Para efetuar o monitoramento, configure a aba Live Connections conforme demonstrado à seguir:

| ratwill 🛞 tees | | Statut. | | | Were | |
|----------------|----------------|-------------------|------|----------|-------|------|
| | 10.000 | De-Official lane | P0(1 | And sold | Publy | |
| | and the second | Statistical Acade | | | Sect | - 14 |
| | | | | | | |
| | | | | | | |

Connections- Web - New

- *Type:* Selecione a opção *Web*;
- Status: A opção New será automaticamente selecionada;

Start

Feito isso, clique no botão Start

], os resultados serão exibidos conforme demonstrado abaixo:

| Considere : Dista | (/ APRI) | | | | | | | |
|----------------------------|---------------|------------------|-----------------|----------|---------------|--------------------------|---------|---|
| Type Contained the last | | Status | | | *** 11 1 1 | 14 (D 14) | | |
| ENN | Sountin | Dectication: | Fed | Protocol | Policy | | | |
| and provides (| Faire | | | | | | | |
| State 1 | BORATER. | Linal | aution - | ret | Protocal | Policy | actions | |
| 14 | 222.186.75.23 | ingo/2018.ek | strightenide. | - 85 | ne | Minutes 322 (M. 15.2) | 0 | 1 |
| 5.4 | 202.106.75.36 | Hits:/UEIBate | | .00. | YCP | Westman 302.105.75.38 | | |
| | 222.148.73.38 | https://pititum | and provide the | 00 | TOP | Minimum 202.186.75.38 | 0 | |
| | 202.188.75.30 | https://2018.akc | | | RP | WEIRING 2011/06/75-10 | - | |
| | 002.144,75.22 | 1050/0016-60 | tengtionne_ | 90. | TEP | Biosous 202.192.75.28 | | |
| | 222.186.75.23 | impligiture | arargittenite | | ne | Michlows 322 (#6.15.20 | 0 | |
| | 202.108.75.30 | His/2018 of | anarg/deexte | | TOP | Westpos 222.186.11.18 | .0 | |
| | 222.149.73.38 | hater Statute | | 00 | TOP | Million 200, 200, 75, 20 | | |

Connections - Web - New - Results

Web - New - Source

Também é possível realizar filtro de busca por agrupamento do tipo Source e Destination quando o status for do tipo New.

Segue um exemplo de como efetuar monitoramento de IP de origem:

| gei Firmidi 🛞 Pela | | Slater | 20 | | Nov | |
|-----------------------|---------------|------------------|-------|----------|--------|------|
| aw . | Seato | Overfile at loss | Pet | Protocol | Policy | |
| second descent | 130,308,75.10 | PARTIN | 1.1.1 | 1 +++ | (siz) | 1000 |
| | | | | | | |
| | | | 8 | | | |
| | | | | | | |

Connections - Web - New - Source IP

- *Type:* Selecione a opção *Web*; *Status:* A opção *New* será automaticamente selecionada; *Source:* Digite o *IP* de origem que será filtrado. Ex.: 192.168.75.10.

Start

Feito isso, clique no botão Start

], os resultados serão exibidos conforme demonstrado abaixo:

| p thread in such | | Abber (B. 1 | - | | at the second | 101 (2.44) | | |
|--|---------------|----------------|----------------|----------|---------------|--------------------------|---------|--|
| law . | Seator | Deptin at ton | Part | Prototol | Policy | | | |
| and the second s | 10.0470.0 | | 1.44 | 1.04 | | | | |
| lise. | Sona | Dead | lador | Fait | Protecti | ast ₁₀ | Artices | |
| | 101206-75-20 | Planal second | mataheiw- | 1945 | 11.9 | 100 alway 200,186 70-10 | | |
| | 182-186-71-30 | 100000-0000-0 | Sadlasschut. | 941 | TOP | Biodows 222.161.77.33 | | |
| | 101110-0530 | keppi/since | whatabolin | and i | 11,9 | #80.60w6.222.186.75.28 | - 00 | |
| 24 | 102.108.71.30 | tep/2018-etc | storg internet | 80. | 117 | #Referen 202.160.75.33 | 0 | |
| | DECOM.75.00 | https://-001.b | Galliperchat. | 1942 | YEP | Westine 20,10175.18 | .0 | |
| | 101106-75-20 | ##potsta.ec | - straitgrout | 85 | 12.9 | Intelligen 202,188,75,18 | 5 | |
| | 1011002030 | ten/hitaka | #scolaritygeng | 80 | TOP | 800-0040-322-000-TL-10 | 10 | |

Connections - Web - New - Source IP - Results

Para interromper o monitoramento basta clicar no botão Stop[

Stop

Para mais informações a respeito de cada campo desta tela, cheque esta página.

Live Sessions - Users

O painel disponível na aba Live Users tem como função efetuar monitoramento dos acessos, porém especificamente focado nos usuários.

Assim como em "Connections", é possível aplicar filtros de forma a gerar relatórios mais específicos.

| Este painel não exibe todos os usuários autenticados e sim os usuários que possuam conexões ativas ou estabelecidas com o UTM. Para visualizar todos os usuários autenticados, consulte esta página. | |
|---|--|
| Para acessar, clique na aba <i>"Users".</i> | |





Surgirá a tela "Users", conforme demonstrado pela imagem abaixo:

| | Securos | 1446 | | Zose | | |
|------|---------|-----------|------|--------|----------|------------|
| | theme | 16.011791 | | 110 | | |
| User | State | MAC | Zone | Mytes. | Fackages | connection |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Live Session - Users

Esta sessão irá abordar:

- Componentes deste painel;
- Como executar o monitoramento;

A seguir, analisaremos os componentes deste painel.

Users - Componentes

O painel Live Users é composto dos seguintes recursos:

| and the | | 00 | | 20040 | | - |
|-------------|--------|------------|-----------------|--------------------------|-----------------------------------|--|
| 11-12-11-10 | | | | - Law | | |
| Searce | HARC | Zone | Ayres 2 | Pachages 1 | Generations : | Actions |
| | | | | | | |
| | | | | | | |
| | | 2.1 | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | Soarts | Source MAC | Searce Mat Dave | Source MC Source Space 1 | Source MC Source Space Packages 1 | Source MAC Zone Open 2 Partage 2 Generations 2 |

- User: Neste campo, é possível determinar um usuário, para ser usado como filtro durante o monitoramento;
- Source: Neste campo, é possível determinar um IP de origem, para ser usado como filtro durante o monitoramento;
- MAC: Neste campo, é possível determinar um endereço físico, para ser usado como filtro durante o monitoramento;
- Zone: Neste campo, é possível delimitar o monitoramento a uma zona de rede específica.

Para efetuar o monitoramento, basta clicar em

Start

]. Os resultados são exibidos na tabela abaixo das opções:

| ne en e | and a second | | MAC. | | 1 and | | 1 |
|--|----------------|--------------|------|---------|------------|------------|---------|
| taux | Source | MAC. | Jam | Byba : | Packages : | Connection | Actions |
| conclubition del com- | 112.16.000.040 | | 1.00 | 45.534B | 454 | | |
| uner fülfstock fot zurb | 173.56.31.00 | (<u>*</u>) | LHI | 1.5446 | 101 | . 65 | |
| unit2850x80c.cm | 172.01.295/04 | | 1.44 | 1.1040 | 75 | | |
| anar Sigbbork Bit, Jory | walatenar | | 1.49 | 1.0588 | - 21 | ÷ | |
| uner Tapiblockist.com | 372.02.230.37 | | 044 | 37948 | 34 | 48 | |

Live Users - Results

A seguir, vamos analisar cada componente desta tabela:

• User: Exibe o usuário relacionado ao acesso;

- Source: Exibe o IP da origem do acesso;
 MAC: Exibe o endereço físico do usuário;
 Zone: Exibe a Zona do acesso;

- Bytes: Exibe a consumo do tráfego do acesso;
 Packages: Exibe a quantia de pacotes trocados durante o tráfego do usuário em questão;
 Connections: Exibe a quantia de conexões efetuadas pelo usuário;

Caso um monitoramento já esteja sendo executado, é possível interrompê-lo clicando em [

Users - Monitoramento

A seguir exibiremos alguns exemplos de como efetuar o monitoramento de conexões ativas dos usuários.

Monitoramento em geral

Para efetuar o monitoramento em geral não é necessário efetuar nenhuma configuração.

| anner: | Source | | N. CONTRACTOR CO. | | 20## | | 1 |
|---------|--------|--------|-------------------|----------|------------|-------------|--------|
| Lase | Searce | INC | Zana | Bytos : | Packages 1 | Connections | Action |
| Queer . | Sedece | INFC | Zone | Bytou II | Packages 1 | Connections | Act |
| | | | | | | | |
| | | | | | | | |
| | | (Notes | | | | | |
| | | | | | | | |
| | | | | | | | |

Users - Sem Filtros

Simplesmente, basta clicar em [Start] para iniciar o monitoramento.

| | a la constante de la constante | | No. of the second second | | - Lot | | 1 |
|-----------------------|--|--------------|--------------------------|----------|------------|---------------|---------|
| taux | Source | MAC. | 2 yrm | ByNa : | Packages : | Connections : | Actions |
| the laboration of | 112.16.000.042 | | 1.66 | 46.639/B | 454 | | |
| contrighted bit and | 172.96.01.00 | (<u>*</u>) | 1041 | 1.5446 | 165 | 10 | |
| 000-201000000.0079 | 172.02.295/94 | | 1.44 | 1.1040 | 78 | | |
| and Sigbook Scions | with the second | | 1.49 | 1.0588 | | ÷ | |
| uner Taxibiock/ML.com | 37232.23637 | | 044 | 37948 | 34 | 48 | |

Users - Sem Filtros - Results

ор

Monitoramento de um usuário específico

Para efetuar o monitoramento de um usuário específico, adicione os filtros desejados conforme demonstrado à seguir:

| ser | Source | MAC | | Tess. | | |
|------------------|--------|-----|------|--------|----------|-------------|
| are plained or a | 042744 | | | | | 100 |
| Unor | Starce | MAC | 7cme | liyten | Packages | Connections |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Users - Filtrado por usuário

• User: Utilizando qualquer um dos campos é possível gerar um filtro, neste caso filtraremos por usuário. Ex.: user1@blockbit.com;



| the process of the second second | 15000 | | permittents. | | UR | | 1 |
|----------------------------------|----------------|-----|--------------|---------|------------|---------------|--------|
| ume | Searce | MAC | itee | Ryber : | Fackaget : | Connections : | Action |
| una (1996) estate trave | 172.16.086.242 | | GAR | - | 104 | ŧ. | н |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Para interromper o monitoramento basta clicar no botão



Live Sessions - VPN

Este recurso permite ao administrador visualizar os status dos túneis de VPN estabelecidos, as informações disponíveis são:

| pe 1 Site-to-Site 🔄 Herberts access | | Fam. 🖬 2 | <u>a</u> (| | | | | 1.08 |
|--|-----------|----------|------------|-----------------|------------|----------|------------|---------|
| tooraction | Producted | Searco | Detivation | Vitaal Adilvess | Doration 1 | toffic + | Pockages 1 | Actions |
| | | | | | | | | |
| | | | No. Cale | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Live Sessions - VPN

- *Type:* O tipo de conexão, da *VPN* em questão. Podendo ser *site-to-site* ou *remote access; Protocol:* Define o protocolo da *VPN*. Podendo ser *IPsec* e SSL;



], os resultados serão exibidos de acordo com o tipo de conexão e o protocolo selecionado, conforme

| Ao iniciar o monitor clicando em [| |
|------------------------------------|--|
| demonstrado abaixo: | |

| Live Sessions | | | | | | | | | | |
|--------------------------------------|---|------------|-------------|-----------------|------------|----------|------------|---------|--|--|
| Type Sta-to-life C Remete account | Protocol Wein, SSL | | | | | | | - | | |
| Connection | Protocal | Searce | Destination | Virtual Address | Duration : | Tarfic 1 | Packages 2 | Actions | | |
| 0403820-052 | 094 | 1014130829 | 1010308170 | 1003024 | 101010 | 0.088 | 1.6 | ж | | |
| VPH SSL | μ. | TRALARM | ITZALINE.IN | | 82.8400 | 014700 | 1998 | н | | |
| | | | | | | | | | | |



As colunas exibem as seguintes informações:

• Connection: Nome do túnel;

- Protocol: Exibe o protocolo da VPN (IPsec ou SSL). ٠
- ٠
- Source: Endereço *IP* do gateway local do túnel; Destination: Endereço *IP* do gateway remoto do túnel; Virtual Address: Exibe o endereço *IP* virtual da VPN; •
- Durantion: Exibe durante quanto tempo corrido a conexão com a VPN está estabelecida. A data de conexão é exibida como dica da ferramenta;
- Traffic: Exibe o tráfego atual da VPN;
- Packages: Número de pacotes trafegados; •
- Actions: Exiba a opção de remoção:

• [] Essa opção serve para derrubar um túnel VPN. Atente que estes túneis não irão se reconectar sozinhos.

8 Ao derrubar um túnel VPN através da opção acima, ele NÃO irá se reconectar (Independente de estar configurado para se conectar automaticamente).

Para mais informações a respeito de como configurar um túnel VPN IPSEC, cheque esta página.

Para mais informações sobre a configuração de VPN SSL, cheque esta página.

Para interromper um monitoramento que esteja sendo executado, clique em [

106

Monitor - Traffic Monitor

Como o próprio nome indica, o *Traffic Monitor*, permite que o tráfego da rede e do *SD-WAN* seja monitorado, através deste recurso o administrador pode visualizar o tráfego de rede real ou histograma (*Network Throughput*), por interfaces, número de conexões simultâneas e o tráfego de rede por cada *PIPE* (Q.o.S). Além disso, também é possível visualizar o desempenho do *SD-WAN* de acordo com suas interfaces e índices de performance.

Para acessar esta tela, basta selecionar a opção "Traffic Monitor".



A tela abaixo será exibida:



Monitor - Traffic Monitor - Network

A tela Traffic Monitor comporta as seguintes abas:

- Network;
- SD-WAN.

Traffic Monitor - Network

Na aba Network do Traffic Monitor, é possível acompanhar em tempo real o desempenho e o tráfego efetuado na rede.





Surgirá a tela demonstrada abaixo:



A seguir vamos analisar cada componente desta tela:

Gráfico de Throughput

O gráfico de *Throughput* demonstra o histórico do desempenho da rede em tempo real. Ao passar o mouse por cima, é possível de se visualizar um resumo do período selecionado.


Traffic Monitor - Network - Throughput

Gráfico de Conexões

O gráfico Connections demonstra um histórico conexões simultâneas e o consumo que seu tráfego causa em tempo real. Ao passar o mouse por cima, é possível de se visualizar um resumo do período selecionado.



Traffic Monitor - Network - Connections

Monitoramento de Interfaces em tempo real

A barra localizada no topo da tela serve monitorar as interfaces de rede que forem selecionadas em tempo real.

É possível adicionar as interfaces que se deseja monitorar, para tanto, digite ou selecione-as à partir da lista, como demonstrado pela imagem:

| ensistic encisi encisi encisi | |
|-------------------------------|---|
| - 410 | |
| 40.64 | |
| white | 6 |
| ette | 9 |
| atts | |

| O máximo de interfaces que se pode adicionar para monitoramento em tempo real é 4. | |
|--|--|
| | |

Clique no botão Start

para iniciar o monitoramento.

Novos gráficos serão adicionados abaixo dos gráficos de *Throughput* e *Connections* e o monitoramento em tempo real será iniciado, conforme exibido abaixo:



Traffic Monitor

Start

Traffic Monitor - Network - Monitoramento de interfaces em tempo real

| | | _ |
|---|------|------------|
| | Stop | |
| Caso um monitoramento já esteja sendo executado, é possível interrompê-lo clicando em Stop [| |] . |

Traffic Monitor - SD-WAN

Na aba SD-WAN do Traffic Monitor, é possível acompanhar em tempo real o desempenho nas interfaces, índices de performance e perfis do SD-WAN.

Para monitorar o SD-WAN, é necessário antes possuir algum perfil de SD-WAN, para mais informações a respeito, cheque o capítulo: Services - SD-WAN.

Para acessar, caso a aba não esteja selecionada, clique em "SD-WAN".

| Network | SD-WAN |
|---------|--------|
| | |

Aba SD-WAN

Surgirá a tela demonstrada abaixo:

| Traffic Monitor | |
|------------------|-------------|
| + Profiles | |
| onurlasas | Balancag |
| | |
| Lawrey | |
| 10m | i line |
| .1 <i>8</i> 94 | 1.000 |
| 1979 | 139mt |
| (1996) (1997) | 1 28mg |
| Um | 1304 |
| Failler Loss | modwath. |
| 14 | 1 meta |
| n. | 4 300 Bry |
| | 1998 |
| 8 | 1.00 BA |
| | 1000 ADM 88 |
| n | 10000 |

A seguir vamos analisar cada componente desta tela:

Monitoramento de SD-WAN em tempo real

A barra localizada no topo da tela serve monitorar em tempo real o perfis de SD-WAN que for selecionado.

Para tanto, selecione-o à partir da lista, como demonstrado pela imagem:



Os gráficos serão construídos de acordo com o perfil selecionado e o monitoramento em tempo real será iniciado, conforme exibido abaixo:



Traffic Monitor - SD-WAN - Monitoramento em tempo real

Caso um monitoramento já esteja sendo executado, é possível interrompê-lo clicando em Stop

Painel de Interfaces

Após ter escolhido o perfil de SD-WAN para iniciar o monitoramento, este painel exibirá todas as interfaces referentes ao perfil selecionado.



Ao desmarcar [__] a caixa de checagem referente à interface, suas informações serão ocultas de tos os gráficos até sua caixa ser remarcada [1].

Gráfico Balancing



Este painel exibe um gráfico representando a porcentagem de balanceamento de tráfego de cada interface.

Traffic Monitor - SD-WAN - Painel Balancing

Ao passar o mouse por cima do gráfico ou das interfaces na legenda lateral, é possível visualizar um resumo referente ao período e a interface selecionada.

Gráfico Latency

Este painel exibe um gráfico demonstrando o histórico do desempenho do SD-WAN de acordo com o índice de latência em tempo real.



Traffic Monitor - SD-WAN - Gráfico Latency

Ao passar o mouse por cima do gráfico ou das interfaces na legenda inferior, é possível visualizar um resumo referente ao período e a interface selecionada.

Gráfico Jitter

Este painel exibe um gráfico demonstrando o histórico do desempenho do SD-WAN de acordo com o índice de jitter em tempo real.



Traffic Monitor - SD-WAN - Gráfico Jitter

Ao passar o mouse por cima do gráfico ou das interfaces na legenda inferior, é possível visualizar um resumo referente ao período e a interface selecionada.

Gráfico Packet Loss



Este painel exibe um gráfico demonstrando o histórico do desempenho do SD-WAN de acordo com o índice de largura de banda em tempo real.

Traffic Monitor - SD-WAN - Bandwidth

Ao passar o mouse por cima do gráfico ou das interfaces na legenda inferior, é possível visualizar um resumo referente ao período e a interface selecionada.

Para mais informações a respeito de SD-WAN, cheque o capítulo: Services - SD-WAN.

Monitor - System Status

Este recurso permite ao administrador a visualização na interface WEB de dados e informações de "Sistema", "Licença" e das bases de dados "Subscriptio ns", permitindo também visualizar e alterar o "Status dos módulos e serviços".

Para acessar esta tela, basta selecionar a opção "System Status".



A tela abaixo será exibida:

System Status



System status - Visualização de um appliance virtual

| Synai interanse | | Setur Accenta. | | | Synam Gersteen | |
|----------------------|----------------------------------|---------------------|-----------------|-------------------|---------------------------------|------|
| Rodenna | 012041 | | | | * 4.0. Same | 10.5 |
| Installation . | WHEN THE SAME AREAS | | in an | | * A.B. (Distant | 1.1 |
| 10.000 | Receiver over Log Australia | | 10.016 | | * 5-0-USP | 1.1 |
| Resultai. | 81.00 | - | | 5 | * Arth. Salter: | |
| Dista di Orice | 20-20-20 A (20-20 | 2.37% | | 08.5% | · Partner and | |
| toria. | 10 march | | | \mathbf{O} | · Anima fairmini | - 31 |
| Latriples | Proved Provide State | | 25 | 100 | · torus through | |
| Last the ball | | | | | · Inter-Suite | |
| High doublet the | - | 0.29% | | 12.0% 8/15 | · house house | |
| | | | - | | · Colomba | |
| | | | 70 | | | |
| | | | 1 24 | | | |
| | | | | | owneday | |
| | | | | | · Faller - ROP | |
| same and the barrier | | turner without | | | Feature All | |
| Inertial Materials | 7000000 0400-000-4801-40400-0040 | mescipital | List wally | N. Ann Applicants | * Press 1100 | - 21 |
| License High | 240-638-12024734 | Web Filter | 35.0000.06258 | 40073264 | di Fasiler Th | |
| Regiony from | Televis in | Application Canater | 2010/012305761 | 4 | Roma 88764 | |
| Harris Elastin Galar | 3002.43.03 | Introdet/Pergnition | 2010/012/047/01 | 1125.0 | NORE | |
| Lines of Biolog. | - | Thread Probabilism | 2010/002/06/07 | 600 | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

System status - Visialização de um appliance físico

Note que quando utilizarmos um appliance físico, a widget de exibição de temperatura será exibida juntamente com as demais.

Este painel é composto de:

- System Information: Informações gerais do dispositivo;
- System Resources: Recursos de hardware do dispositivo;
 - Utilização CPU (%);
 - Entrada e Saída (I/O) (%);
 - Disponibilidade (%);
 - Load Average (%);
 - Utilização de Disco (%);
 - Memória RAM (%);
 - Temperatura de CPU (° Celsius).
- License Information: Informações de identificação do BLOCKBIT Device Number (UUID) e da licença;
 - Subscriptions: Status das bases de atualizações;
 - Antimalware;
 - ATP Advanced Threat Protection (Aplicativos);
 - ATP Advanced Threat Protection (Reputação IP);
 - ATP Advanced Threat Protection (Ameaças);
 - IPS Intrusion Prevention System (IPS);
 - WGS (Navegadores);
 - WGS (Aplicativos);
- WGS (Categorias de sites e URLs).
 System Services: Status dos serviços e recursos.

System Status - Widgets

A seguir, analisaremos cada componente dos widgets desta tela.

System Information

O widget "Information" exibe informações do firmware do Blockbit UTM, como:

- Hostname: Nome DNS configurado no equipamento. Ex.: utm.blockbit.com;
- Description: Informa o nome da aplicação. Ex.: Blockbit UTM;
- Version: Informa a versão e a build da aplicação. Ex.: BLOCKBIT UTM 2.0.0 build 20020413;
- Model: Informa o modelo do equipamento, caso seja um appliance. Ex.: BBv-5;
- Date & Time: Informa a data e hora do sistema. Ex.: 05/02/2020 10:59:57 AM;
- Uptime: Informa o tempo em horas que o sistema está ativo. Ex.: 23:40 hour(s);
- Last Update: Determina quando foi o último update. Ex.: 11:14:56;
- · Last Backup: Determina quando foi o último backup;
- High Availability: Define se o High Availability está ativo ou não.

| System Information | | | | | |
|--------------------|-----------------------------------|--|--|--|--|
| Hostname | utm20 | | | | |
| Description | UTM20 | | | | |
| Version | BLOCKBIT UTM 2.0.0 build 20012812 | | | | |
| Model | BBv-5 | | | | |
| Date & Time | 28/01/2020 02:13:11 PM | | | | |
| Uptime | 5 day(s) | | | | |
| Last Update | 09:45:24 | | | | |
| Last Backup | | | | | |
| High Availability | Active | | | | |

Dashboard - System Information

System Resources

O widget "Resources" exibe informações do recurso de hardware do Blockbit UTM, como:

- CPU: Exibe a porcentagem de uso das CPU do sistema em tempo real. Ex.: 2,25% de utilização;
- I/O: Exibe a porcentagem de uso da capacidade de escrita e leitura dos discos do sistema. Ex.: 19,1%;
- *Idle*: Exibe a porcentagem disponível para uso de *CPU*. Ex.: 97,8%;

- Load: Informa a média de uso das CPU do sistema (load average) dos últimos 5 minutos. Ex.: 0,23%; ٠
- **Disc:** Informa a % de espaço utilizado dos discos do sistema. Ex.: 20,3%; **RAM:** Exibe a porcentagem de uso de memória *RAM* do sistema em tempo real. Ex.: 22,9% de utilização.
- Temp: Exibe a temperatura da CPU em graus Celsius. ٠



Dashboard – System Resources



License Information

O widget "License" exibe informações da licença de ativação do Blockbit UTM, como:

- Serial Number: Exibe o código de identificação única (UUID) do appliance. Esse ID é utilizado na identificação do hardware para validação da ٠ licença de uso;
- License Number: Exibe o número da licença do appliance. Ex.: D845-61F9-9CBA-8145;
- Registry date: Exibe a data que a licença foi registrada no sistema. Ex.: 2017-12-18; •
- Expire Date: Exibe a data de expiração da licença do sistema. Ex.: 2018-01-31;
- License Status: Exibe o status da licença, ativa ou inativa.



Subscriptions

O widget "Subscriptions" exibe a última modificação, assinaturas e informações das bases de assinaturas do Blockbit UTM, como:

- Web Filter;
- Application Control;
 Intrusion Prevention;
- Threat Protection.

Todas as bases são atualizadas constantemente pela Blockbit, garantindo a efetividade e segurança do ambiente.

| Subscriptions | | |
|----------------------|-------------------------|---------------|
| Description | Last Modify | Subscriptions |
| Web Filter | 04/02/2020 18:49:27 | 46948563 |
| Application Control | 04/02/2020 18:49:27 | 3182 |
| Intrusion Prevention | 04/02/2020 18:49:27 | 62507 |
| Threat Protection | 04/02/2020 18:49:27 | 6792324 |
| | | |
| | | |
| | | |
| | Doobboord Subscriptions | |

Dashboard – Subscriptions

Services

O widget "Service" exibe o status dos serviços e funcionalidades do Blockbit UTM, possibilitando reiniciá-los ou pará-los:

| System Services | | |
|------------------------------------|------------|---|
| • Firewall | (1) | ^ |
| Proxy-HTTP | (1) | |
| Proxy-FTP | \bigcirc | |
| Proxy-Email | \bigcirc | |
| Web Filter | (1) | |
| SSL Inspection | \bigcirc | |
| Application Control | \bigcirc | |
| Intrusion Prevention | \bigcirc | |
| Threat Protection | (1) | |
| SD-WAN | \bigcirc | |
| • VPN-IPSEC | \bigcirc | |
| VPN-SSL | \bigcirc | |
| • SNMP | \bigcirc | |
| DHCP-Server-v4 | (1) | |
| DHCP-Server-v6 | \bigcirc | |
| DHCP-Relay | \bigcirc | |
| DNS | (1) | |
| Auth-Server | (1) | * |

Dashboard – Services

É possível visualizar o status do serviço neste painel, sendo:

- Ativo[];
 Inativo[].

Em "Services" é possível reiniciar e parar os serviços, ao lado do nome do serviço, segue os botões:

- Iniciar [];
- Parar [¹⁰].

Não é possível interromper alguns serviços específicos.

Para interromper um serviço parado, clique em Parar [1], o painel abaixo será exibido.



Para ativar um serviço parado, clique em Iniciar [D], o painel abaixo será exibido.



Monitor - Security Events

O painel "Security Events" tem como função principal exibir todas as ocorrências de eventos de segurança do Blockbit UTM.

Este painel possui alguns recursos que permitem uma análise profunda mais detalhada: Através deste painel é possível efetuar uma busca de acordo com *queries* personalizadas, analisar incidentes e eventualidades específicas, permitindo uma administração muito mais precisa e eficiente.

A principal diferença entre os relatórios exibidos em Events e os em Analyzer é que:

Em Events, é gerado um registro da conexão com os atributos todos zerados (bytes e pacotes), após a desconexão outro evento é gerado registrando esses atributos, o tráfego e o tempo conectado.

Já os relatórios do Analyzer são sumarizados de 5 em 5 minutos gerando relatórios de tempos em tempos com dados gerados no período.

Para acessar esta tela, basta selecionar a opção "Security Events".



Monitor - Security Events

| ~ | +010 | obowo | 0050 | ovubidor |
|---|--------|---------------|------|----------|
| - | 1012 | anaixn | SPIN | PARTINUM |
| | LUCIU. | UDUINO | JULI | CAIDIGG. |
| | | | | |

| a state work | | | | | | | | | i. |
|---|-----------|------------------------|----------------------|-----------|------------|-----------|--------|---|----|
| Concerne . | | | | | | | | | |
| Oute | - inter | Source | Destruitor | Devilue | Service | roli plas | Action | | |
| C minima a mi | | B 022154.0.5070 | ME 103.74.75.46.447 | 492-495 | retai | (i | - | 2 | = |
| E 2014-10-10 15-16-5 | 1 m | NE 11222-264-4642823 | 11 18-40.111.172-402 | ers2 etc. | inter | Sweet | - | 2 | = |
| E 202-05-05 19 20 5 | e), | 🙀 372.51.554.04.54575 | ME 105.15.76.45441 | 1092-1095 | intpo | and the | - | 9 | |
| (i) 2018-0110 (ALM-5) | 82 | ME 173.21.004.00430 | | ano-anti- | hitps | and No. | | 5 | = |
| E 10+0/01209 | 6.4 | 🙀 111.11.234.43820 | (11-600107540 | #93- #85 | helps | (Reil) | | 2 | 8 |
| El 103-10-09 (n.004) | 5 A | D 30737394 66 97210 | S DAUANADAD | 402-404 | Http: | Tenel | | 9 | Ħ |
| O mana a ma | 6 e . | E1 173.21.06.00374 | C1 (12/24/02/14/168 | 483-482 | 1414 | () | - | 2 | = |
| E 189-40-0 15163 | ÷ | T1 11231.008.4554650 | 23 17235.112.1H-HE | ved | viccost as | (treet) | des. | 2 | Ħ |
| E 202-05-05-05-05-05-05-05-05-05-05-05-05-05- | 1944 - C. | [] 372.51.508 at white | CI ITELELISION MA | 102-102 | etyoeik-ts | Retail | | 0 | H |
| EI 2019-02-02 (2016-0 | No. | 11 7/2 51 (in 1964) | COLLARIT MO | 692-109 | blackgare. | (second | | 9 | ÷ |

Events

ATENÇÃO: Não é possível gerar *logs* detalhados sem ter aplicado uma política que efetue inspeção. Para mais informações a respeito, consulte essa página.

Esta tela contêm as seguintes abas:

- Sessions;Authentication;
- VPN.

A seguir, os componentes do painel events serão analisados.

Security Events - Sessions

Em Sessions temos um registro de todos os eventos detectados nas sessões deste device.

Para acessar, caso a aba não esteja selecionada, clique em "Sessions".



Aba Sessions

Surgirá a tela demonstrada abaixo:

| Salar Salar | and an initial | | | | | | | - | - |
|--|----------------|---------------------------------|----------------------------|---------------|------------|-------------|------|-----|----|
| 610 | Ave. | Scare | Disbrokus | andra | inche . | Lighter. | A214 | | |
| E 2014-01-01.002 | zfi - | ineecon m F1 | 12 millionesi | | 10.0010 | Taxa . | | - | a, |
| E 2014-0-01.440 | | Las des real connector | - martet beaut | 414-1410 | ings. | - | | | ÷ |
| 1 2223-51-51 Au | | Mar The Association of the | 1 10 20 40 200 200 400 400 | -0.0 -0.0 | 1.000 | | - | 1 | = |
| II DON ALLON | 014 | int 19 disk program | - 10-4-100-216-412 | 46.400 | the second | [| | 5 | |
| E 10040.01.007 | 132 | | am 110303.031 | 944 | (Selen) | | | * | 8 |
| B 2009-05-07 Lar | THE . | and the sum of the | In Planta des | 101-100 | 1984 | (Sec.) | | - | 4 |
| iii aanaa ah soo | NE | play and a second second second | im stitisten | at16_at10 | 144 | Contract of | | 191 | |
| E Distanti de la composición d | - (4) | and (Particul contract) | en stalaautt | -01 | (Brink) | (111) | | 10 | × |
| E marks at res | C+4 | 101 Feb. 201 Feb. 2011 | Contraction in the | efficientiada | . nex | - | | \$ | = |
| E march drives | n (A | are 194, hand second state | in with street | anti-delarti | 144 | - | | - | 4 |



Na barra de pesquisa, podemos alterar o "logtype" e visualizar também outros tipos de serviços e também o período que deseja verificar. Veja o exemplo a seguir.





| Date | The | Searce . | Berfratko | 0eke | Service | Ligtype | Act in | | |
|-----------------------|-----|-----------------------|--------------------|--------------------------------|---------|----------------|--------|----|---|
| H 2013-01-01 12/01/94 | | (1) 310/10.010/00-40- | E3 195144673040 | $(h_1(h_1)-h_2(h_2)-h_2(h_2))$ | 819 | - | ates | 0 | |
| 🗇 2013-68-81 12-81-54 | | TT stem is instant | P3 102.14-06.39248 | #011-1#9x21 | 009 | and the second | at the | 10 | Ξ |
| | | | | | | | Fage 1 | | |

Esse painel é composto pelo Query Editor e pelas seguintes colunas:

- *Expandir E*: Expande o evento, para mais informações cheque esta página; *Date*: Temos a data e o horário exato desse evento;
- User: O usuário que gerou este evento;
- Source: Temos a fonte desse evento, um endereço IP. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Destination: Temos o destino desse evento, outro endereço IP. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Device: Define o device que gerou esse evento. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Service: Temos o serviço atrelado a esse evento. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Log Type: Determina o tipo de registro deste evento. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro; Action: Define qual foi a ação que as políticas tomaram quanto à esse evento. Caso clique em cima deste campo é possível efetuar uma busca • utilizando-o como filtro;
- Search com ID]: Permite fazer uma busca usando o ID do evento como filtro;
- Event view [] : Permite acessar a janela Event view.

À seguir analisaremos como expandir um evento para consultar mais informações a respeito dele.

Sessions - Event View

O botão **Event View**[]] exibe detalhes mais aprofundados do evento em questão, conforme exibido na imagem abaixo:

| vent View | |
|--|-------|
| | |
| * "Erent Information" : | |
| "event_ru, + .me-drebs hrithrows. | |
| "dete" = "2020-01-15 18:48:08" | |
| "pag" ("172-33.4.E9" | |
| "det": "172.31.0.81" | |
| "service" : "ADHIN" | |
| "tibe, 1 , 104. | |
| "gestp_det.country_same": "." | |
| "georp_coo.covacry_same" : "." | |
| "goolp_det.sity_name" : mus | |
| "genip_ant.mity_same" : Milk | |
| "geotp_det.redion_name" ; with | |
| "geoip_art.regios_same" : with | |
| "box_ad" ("755ala2170chab2349054511147adTe" | |
| * "geosp_det" (D | |
| "demin" : "ettal" | |
| "aport" ("99" | |
| "logtype" ("firewall" | |
| | class |



Sessions - Expandir Sessions

Logo do lado de data do evento temos um ícone []] que ao ser selecionado irá expandir a seleção e exibir mais informações a respeito desse evento específico.

| Sessions | Authentication VPN | | |
|----------|--|---|--|
| | Information | | |
| 3.450 | ⊖ logtype⊖ firewall | ⊕ geoip_src⊖ US | ⊕ devout⊖ eth5 |
| D | → sessid → CB70A4621F4E1E9F2E2520E38ECDF39B | ⊕ dst ⊖ 103.79.78.48 | ↔ zonein→ LAN |
| + 2 | → datetime → 2020-03-03 15:18:31 | ⊕ dport | ⊕ rule_name ⊖ Control |
| + 2 | ↔ src ◯ 172.32.250.64 | ⊕ geoip_dst ⊖ US | ⊕ service⊖ https |
| + 2 | ↔ sport ○ 52161 | ⊕ devin⊖ eth2 | - |

Events - Log Events - Expandido

Ao clicar no ícone [] as informações a frente são utilizadas como filtro e uma pesquisa é efetuada. Ao clicar no ícone [] as informações são removidas do filtro e uma pesquisa é efetuada.

À seguir vamos analisar o Query Editor.

Sessions - Query Editor

Através do editor de queries, é possível criar, editar e salvar queries para efetuar uma busca aprofundada nos eventos, ao clicar no Query Editor [

| Query editor] a se | eguinte janela será exibida: | |
|------------------------|--|-------------------|
| Query Editor | | |
| Create Query | New Query | Date range |
| AN ALCOST AND A | Actions | Last 10 minutes 🏥 |
| Load query | Filter | Period |
| | malware_file V Not equals | Last 10 minutes |
| | Filterstring | Close OK |
| | logtype:"firewall" imalware_file:"" date:"last_10m" | |
| | Filter string logtype:"firewall" imalware_file:"" date:"last_10m" | Close |

Events - Query Editor

Clear

Bave Query

Cancel

A seguir analisaremos cada campo desta janela:

Events - Query Editor - Create query

Na aba "Create query" é possível configurar como a query irá atuar:

| Create Query | New Query | | Daterange |
|--------------|---------------------------|----------------|-------------------|
| | Actions | | Last 10 minutes 🕮 |
| Load query | Filter | Period | |
| | malware_file V Not equals | Last 10 minute | e) |
| | Filter string | | Close |

| | Clear | Save Query | Cancel | Search |
|-------------------------|--------------|------------|--------|--------|
| Events - Query Editor - | Create query | | | 10 |

- New query: Determina qual será o nome da query. Ex.: Last 7 days;
- Date range: Permite determinar um período para filtrar os resultados de forma mais precisa, as opções possíveis são:

| Period | |
|----------------------|---|
| Last 10 minutes | ^ |
| Last 10 minutes | |
| Last 6 hours | |
| Last 12 hours | |
| Last 18 hours | |
| Today | |
| Yesterday | |
| By Date | |
| Opções de Date Range | |

- ° Last 10 minutes: Filtra resultados nos últimos 10 minutos;
- ° Last 6 hours: Traz os resultados das últimas 6 horas;
- Last 12 hours: Filtra resultados das últimas 12 horas;
- Last 18 hours: Filtra resultados das últimas 18 horas;
- Today: Exibe resultados especificamente para a data de hoje;
- Yesterday: Exibe resultados especificamente para ontem;
- By date: Determina uma data específica;

Para mais informações a respeito dos filtros disponíveis na caixa de seleção, cheque esta página do manual do GSM.

- Filter: Esta caixa de seleção permite selecionar o tipo de filtro utilizado pela query;
 - logtype: Faz a seleção pelo tipo de log, para este filtro as opções disponíveis são: webfilter, firewall, dpi, ips, atp;
 - src: Efetua a seleção pelo IP de origem, este filtro aceita endereços IPv4 ou IPv6 como valor. Ex.: 172.16.12.171;
 - dst: Faz a seleção pelo IP de destino, este filtro aceita endereços IPv4 ou IPv6 como valor. Ex.: 172.16.12.171;
 - sport: Este filtro possibilita a seleção por uma porta de origem, portanto, portas são aceitas como valor. Ex.: 1 a 65535;

- o dport: Este filtro possibilita a seleção por uma porta de destino, portanto, portas são aceitas como valor. Ex.: 1 a 65535;
- protocol: Este filtro permite a seleção por protocolo, as opções disponíveis são: tcp, udp, icmp, ip;
- service: No caso deste filtro, é feita a seleção por serviço, os valores aceitos são baseados na tabela do IANA, para mais informações consulte esta página;
- devin: Faz a seleção pelo Device de entrada, este filtro aceita interfaces, para mais informações sobre como criá-las, consulte esta pági na;
- devout: No caso deste filtro, a seleção é feita pelo Device de saída, os valores aceitos são as interfaces criadas pelo usuário, para mais informações sobre como criá-las, consulte esta página;
- zonein: Este filtro possibilita a seleção pela zona de entrada, os valores aceitos são as zonas configuradas nas interfaces do UTM, para mais informações consulte esta página. Ex.: LAN, WAN, DMZ, etc;
- zoneout: Este filtro possibilita a seleção pela zona de saída, os valores aceitos são as zonas configuradas nas interfaces do UTM, para mais informações consulte esta página. Ex.: LAN, WAN, DMZ, etc;
- client_mac: Faz a seleção por endereço MAC, portanto, este filtro aceita endereços físicos. Ex.: 94:e6:f7:58:5d:db;
- client_user: Este filtro efetua a seleção por usuário, ele aceita e-mails como valores. Ex.: user@blockbit.com;
- client_ip: Este filtro efetua a seleção pelo IP do cliente, os valores aceitos são endereços IPv4 ou IPv6. Ex.: 172.16.9.153;
- geoip_src: No caso deste filtro, a seleção é feita pela origem do GeoIP (Geolocalização de endereço IP), os valores aceitos são siglas de país. Ex.: BR, US, CA, CN, etc;
- geoip_dst: Efetua a seleção pelo destino do GeoIP (Geolocalização de endereço IP), os valores aceitos são siglas de país. Ex.: BR, US, CA, CN, etc;
- rule_name: Este filtro efetua seleções pelo nome da regra, sendo que o nome das regras criadas no UTM são utilizadas como valor, para mais informações consulte esta página;
- rule_action: Faz a seleção baseada na ação que a regra toma, este filtro aceita como valor as opções: Allow, Alert ou Deny. Ex.: Deny;
- web_category: Este filtro possibilita a seleção por categoria web, sendo estas mesmas aceitas como valor. Ex.: Information Technology, Web Mail, Personal Network Storage and Backup, etc.
- web_site: Faz a seleção por sites, este filtro aceita URLs como valor. Ex.: https://www.blockbit.com;
- web_method: Efetua a seleção pelo métodos HTTP, este filtro aceita como valores os métodos POST e GET. Ex.: POST;
- web_mime: Este filtro permite a seleção por MIME-Type, sendo exatamente este mesmo o valor aceito. Ex.."application/octet-stream",
- ips_profile: Efetua a seleção pelo Perfil de Intrusion Prevention System, o valor aceito é o nome do perfil, para mais informações consulte esta página;
- app_name: Este filtro permite efetuar a seleção por nome do aplicativo. Ex.: Google APIs;
- app_category: Efetua a seleção pela categoria do aplicativo, sendo exatamente este mesmo o valor aceito. Ex.: web;
- malware_file: Faz a seleção pelo tipo de arquivo de malware;
- malware_md5: Seleciona através do MD5 dos malwares;
- malware_status: Seleção pelo status dos malwares;
- malware_name: Seleção pelo nome dos malwares;
- threat_class: Este filtro faz a seleção pela classe da ameaça. Ex.: Potentially Bad Traffic;
- threat_category: Efetua a seleção pela categoria da ameaça. Ex.: USER_AGENTS;
- threat_sid: Seleciona pelo SID da ameaça. Este filtro utiliza o SID da ameaça. Ex.: 2027916;
- threat_name: Estre filtro faz a seleção pelo nome da ameaça. Ex.: Poison Null Byte;
- threat_impact: Este filtro faz a seleção baseada no nível de impacto da ameaça. Ex.: High, Medium, Low;
- threat_dump: Seleção pelo dump da ameaça. Este filtro aceita o dump da ameaça;
- threat_payload: Faz a seleção pelo payload da ameaça;
- flow: Mostra juntamente com o endereço IP, a NAT aplicada e qual o endereço atribuído.
- Contain/Not Contain: Esta caixa de seleção atua basicamente como um operador lógico do filtro da query;
 - Contain: Irá exibir todos os resultados que contêm o valor da próxima caixa de seleção;
 - Not Contain: Irá exibir todos os resultados que NÃO contêm o valor da próxima caixa de seleção.
 - Equals: Irá exibir todos os resultados que são EXATAMENTE iguais ao que for adicionado no próximo campo (Value);
 - Not Equals: Irá exibir todos os resultados que NÃO são iguais ao que for adicionado no próximo campo (Value);
- Value: Esta caixa determina o valor que será utilizado para filtrar a query;
- *Filter string:* Após editar os campos anteriores, clique em [⁺] para exibir a *string* utilizada pela busca nesta caixa de texto. É possível editar manualmente essa linha de código.

| Para limpar a <i>query</i> configurada, clique no botão <i>Clea</i> i | Clear |]. Caso deseje cancelar clique no botão Cance [| Cancel |]. Para efetuar |
|---|------------|--|--------|-----------------|
| uma busca utilizando a <i>query</i> clique no botão Search [| Search |]. | | |
| Para salvar a <i>query</i> , clique no botão Save Query [| Save query |]. | | |

Events - Query Editor - Load query

Na aba "Query Editor" é possível administrar as queries salvas, este painel é composto de uma barra de busca e um botão de ação com função de deletar todos os campos selecionados, a seguir analisaremos cada componente deste painel:

| Graate query | | | <u>α</u> |
|--------------|------------------|--|----------|
| Loadquery | Name | Filter | Actier |
| | 🔅 WebCategory-La | web_rategory. ^{co} itate*iant_33* | / 0. 0 |
| | Laut t days | web_category/** date:*last_?* | / 0. 0 |
| | | | × (1) |
| | | | ×0 |

Events - Query Editor - Load Query

- Select J: Permite selecionar a query desejada;
 Name: Exibe o nome da query;
 Filter: Exibe a string utilizada pela busca;
 Actions: Exibe um conjunto de botões contextuais;

| ° [| Edit | iery; |
|-------------------|------------------------------------|--|
| ० ड | Search | ndo a <i>query</i> ; |
| ° (| Delete | |
| Caso deseje cance | elar clique no botão Cancel |]]. Para efetuar uma busca utilizando a <i>query</i> selecionada clique no botão Search [|
| Search | 1. | |

À seguir vamos analisar o Event View.

Security Events - Authentication

Em Authentication temos um registro de todos os eventos de autenticação detectados neste device.

Para acessar, clique em "Authentication".



Aba Authentication

Surgirá a tela demonstrada abaixo:

| a records | | | | | | | 9 | Query Tat |
|---------------------|--------------------|----------------|-----|-----------------|----------------|---------|-------|-----------|
| DVR: | 150 | 54940 | MAC | Platico | *** | Report. | ENORT | ACTIV |
| 1000-09-83 3245828 | over\$54x34x1xxx | 17134.006.227 | | HodRA/530(Hits. | SebultCorAp. | policy | | 9 2 |
| 1000-00-00 5666617 | 1043656383,000 | 171.16.208.317 | | Holteston | industriality. | 100 | | 9 H |
| 000-08-03317-0028 | aim (Stricture) | 11114-00-017 | 5 | | | 12 | | 5 8 |
| 0094840315928 | per@bkokkr.com | 112.04.308.237 | 51 | | | 12 | | 2 3 |
| 00010-01114049 | 044906001104 | 177.18.294.227 | | | | | | 7 # |
| 000-09-02121340204 | aan gekoektaam | 112.16.008.017 | | | | | | 9 2 |
| 1000-08-K3 17:00e34 | meditation. | 17110-096217 | | | | | | 9 # |
| 0205-08-01111-0112 | ore pression over | 113.14.228.877 | | | | | | 9.4 |
| 00048-03110029 | sim@58c681.com | (1114.696.317 | | | | | | 2 2 |
| NOVA INTO A | our Bhilychick som | 113.04.304.21T | | | | | | |

Security Events - Authentication

Esse painel é composto pelo Query Editor e pelas seguintes colunas:

- Date: Temos a data e o horário exato desse evento;
- User: O usuário que gerou este evento. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Source IP: O endereço IP de origem do dispositivo do usuário. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- MAC: O endereço físico do dispositivo do usuário. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Platform: Qual plataforma foi utilizada pelo usuário para efetuar o acesso. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Rule: Qual regra de autenticação foi aplicada no usuário, para mais informações a respeito destas regras, consulte esta página. Além disso, caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Reason: Exibe o motivo de porque esse log foi gerado. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Event: Exibe o evento que gerou esse log. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Action: Exibe os seguintes botões:
 - Session ID []: Ao clicar neste botão será executada uma busca com uma *query* utilizando especificamente o ID de sessão do evento selecionado;
 - **Description** []: Ao clicar neste botão a janela *Description* será exibida.

À seguir vamos analisar o Query Editor.

Authentication - Query Editor

Através do Query Editor, é possível criar, editar e salvar queries para efetuar uma busca aprofundada nos eventos, ao clicar no Query Editor [

| Query Editor | | | | | 3 |
|------------------------|---------|--------|--|--------------|---|
| Filterstring | | | | Date onge | |
| Filter shring country. | Today 🛅 | | | | |
| Filter | | | | Volue | |
| Select a field | | Equals | | Encold Spine | + |
| | | | | | |

- Filter string: Ao editar os campos Date Range, Filter e Value a string utilizada pela busca será exibida nesta caixa de texto. Também é possível editar manualmente essa linha de código;
 - Date range: Permite determinar um período para filtrar os resultados de forma mais precisa, as opções possíveis são:
 - By date: Determina uma data específica;
 - By period: Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
 - Today: Exibe resultados especificamente para a data de hoje;
 - Yesterday: Exibe resultados especificamente para ontem;
 - Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
 - Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
 - This month: Exibe os resultados deste mês;
 - Last month: Exibe os resultados do último mês.
- Filter: Esta caixa de seleção permite selecionar o tipo de filtro utilizado pela query;
 - src: Efetua a seleção pelo IP de origem, este filtro aceita endereços IPv4 ou Ipv6 como valor. Ex.: 172.16.12.171;
 - mac: Faz a seleção por endereço MAC, portanto, este filtro aceita endereços físicos. Ex.: 94:a5:f6:48:5d:db;
 - · login: Este filtro efetua a seleção pelo login de um usuário, ele aceita e-mails como valores. Ex.: user@blockbit.com;
 - user_agent: Este filstro se refere à plataforma que o usuário está usando em sua navegação, como valor, ele aceita a distribuição da plataforma. Ex.: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537. 36, OMNE WinAgent/3.0 (Microsoft Windows NT 6.2.9200.0) .NET Framework/2.0.50727.9044, Blockbit Client/1.2, etc;
 - rule: Este filtro efetua seleções pelo nome da regra, sendo que o nome das regras criadas no UTM são utilizadas como valor, para mais informações consulte esta página;
 - reason: Este filtro seleciona todos os usuários pelo motivo do evento. Ex.: Session timeout, Policy;
 - event: Faz a seleção por um evento específico. Ex.: Login, Logout, Session Timeout, etc;
 - ° status: Este filtro efetuar a seleção pelo estado atual da autenticação. Ex.: Allow ou Deny.

Para mais informações a respeito de quais informações devem ser exibidas por cada filtro, consulte esta página.

As informações exibidas em Description equivalem às que o filtro irá retornar, porém, com maior detalhamento e especificidade.

- Equals/Contain/Not Contain: Esta caixa de seleção atua basicamente como um operador lógico do filtro da query;
 - Equals: Irá exibir todos os resultados que são EXATAMENTE iguais ao que for adicionado no próximo campo (Value);
 - Not Equals: Irá exibir todos os resultados que NÃO são iguais ao que for adicionado no próximo campo (Value);
 - · Contain: Irá exibir todos os resultados que contêm o valor do próximo campo (Value);
 - Not Contain: Irá exibir todos os resultados que NÃO contêm o valor do próximo campo (Value).
- Value: Esta caixa determina o valor que será utilizado para filtrar a query.

| clique em | ŕ. | |
|-----------|----|--|

Após editar os campos anteriores.

] para exibir a string utilizada pela busca na caixa de texto Filter String.



À seguir vamos exibir o funcionamento do botão Description.

Authentication - Description

O botão Description[

] exibe detalhes mais aprofundados do evento em questão, conforme exibido na imagem abaixo:

| Description | 0 | |
|-------------|--|--|
| | | |
| Session ID | A5356DF4AF8DBC6238FD05389C900730 | |
| Date | 2020-08-03 18:05:25 | |
| User | qa1@local.net | |
| Source | 172.16.100.227 | |
| MAC | | |
| Action | login | |
| Event | talse | |
| Status | en | |
| Platform | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537,36 (KHTNL, | |
| | Ilke Gecko) Chrome/84.0.4147.105 Safari/537.36 | |
| Rule | Configurações Padrões | |
| Reason | policy | |
| | | |

Close

×

Sessions - Event View

- Session ID: Exibe o ID da sessão do usuário que causou o evento;
- Date: Exibe a data do evento;
- User: Identifica o usuário que gerou este evento;
- Source: Exibe o endereço IP que originou o evento;
- MAC: Define o endereço físico do dispositivo que originou o evento;
- Action: Determina qual ação tomada ocasionou o evento;
- Event: Exibe True caso o o Login tenha sido feito por SSO (Single Sign On), caso contrário, exibirá False.
- Status: Determina o estado do evento;
- Platform: Exibe informações da plataforma utilizada pelo usuário que ocasionou o evento;
- Rule: Exibe o nome da regra que foi utilizada, para mais informações consulte esta página;
- Reason: Exibe o motivo da criação do evento. Segue uma lista com a legenda das razões possíveis:
 - src: Endereço Remoto;
 - time: Horário;
 - date: Período;
 - user_agent: Plataforma;
 - user: Usuário/Grupo;
 - ° zone: Zona de Rede;
 - **no_policy:** Nenhuma política encontrada;
 - user_blocked: Usuário bloqueado;
 - timeout: Timeout de sessão;
 - policy: Afetado por uma Política.



Authentication - Rules

Esta tela tem como função administrar a função de serviço de autenticação através de políticas de controle, as quais possibilitam a permissão ou bloqueio de acesso a tal serviço com base em condições predeterminadas ou definir os parâmetros da sessão de usuários que tiveram permissão autenticada em um determinado serviço.

Estas políticas de autenticação são aplicadas em ambos o serviço de portal cativo e cliente de autenticação.

Em termos de Políticas, as mesmas são administradas por "Prioridade", e são aplicadas considerando o método "First match wins" (O primeiro entre os elementos tem a prioridade). Todavia, as políticas localizadas acima tem prioridade, enquanto aquelas abaixo tem menor prioridade e a ação é aplicada a primeira política que se enquadrar nestas condições.

Para configurar estas opções, clique na aba Regras:



A seguinte tela será exibida, conforme mostrado abaixo:

| Action Action |
|---------------|
| 1 N C) |
| |
| |

Authentication - Servers

Nesta seção analisaremos:

- Como criar, editar e apagar estas Políticas;
- Os componentes da coluna desta aba.

A seguir, cada componente desta tela será analisado.

Security Events - VPN

Em VPN temos um registro de todos os eventos de gerados pelos perfis de VPN deste device.

Para acessar, clique em "VPN".



Aba VPN

Surgirá a tela demonstrada abaixo:

| anna Aithe | eticalice | APR: | | | | | | | | |
|--------------------|-----------|---------------------|----------------|----------------|-----------|--------|-------------------|--------------|-----------|------------|
| 11eorbi | | | | | | | | | 1961 | Query time |
| sate. | Date | Teacor | Destination | 1014/440000 | types | nate | 7994 | rotool | 3000 | Action |
| 1979-19-04 12:31 | 1117 | [89:40.01.223] | 10,106,08,114 | 198.108.100.07 | 064 | - 1000 | week-along | PHO: | dormet | 9 E |
| ana ana mari | | 186.303.143.11 0 | 10,106,06,114 | 122.148.180.37 | ().Dytasi | ÷. | 1071110-00000 | F98 | Second | 9 8 |
| LADA AD ON LO-1. | 1111 | 1063/04/8229 | 191113-08113 | 101040561- | U.Bytan | 0 | other low-strike. | 100 | inerest. | 0 = |
| 1223 - Die 14 12 1 | **** | 10100636318 | - | 572.)#4.0(%8,1 | - | - | 0.0-0-0.0 | Perception 2 | shoocest | 9 # |
| 1010-02-09 11:5 | | 105,406,01114 | 171110-00101 | 110.003/05.1. | 0.0200 | | 101-12-009 | Post: | idential. | |
| 1005-00-09 12:5 | 1117 | 10.306/01/228 | 379.133.00.133 | 177.064.0/98.1 | 121. | 26 | 101-15-101 | PRC. | dormet | 9 = |
| 1225-85-04-05-4 | 1117 · | 18540/03733 | 10,154,01110 | 735.068.00035- | 0.0409 | | 1019-00251 | PRC. | orrest | 9 ≡ |
| rain-skiss nark. | 1111 | 189-201240-08 | 198106-05118 | 040.104.101.05 | 0.6µme | 0 | nergible accessi | ten: | connect | 9 E |
| 1879-16-08 OBA | 8107 | 385.306.00.138 | 3/8.133/8.115 | 10.064.056.1., | United | 0 | ista-is-asta | PMC | (const | 9 = |
| 2023-00-01 08-4 | | 181.15.171.36 | 101108-05110 | 002.068.100.00 | O Bytan | 10 | | and the | or well | 9 10 |

Security Events - VPN

Esse painel é composto pelo Query Editor e pelas seguintes colunas:

- Date: Temos a data e o horário exato desse evento;
- User: O usuário que gerou este evento. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Source: Temos a fonte desse evento, um endereço IP. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
 Destination: Temos o destino desse evento, outro endereço IP. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Virtual Address: Exibe o endereço virtual da VPN;
- Bytes: Exibe o tráfego de Bytes da VPN;
- Packets: Exibe o tráfego de pacotes da VPN;
- Type: Determina o tipo de VPN. Ex.: remote-access.
- Protocol: Define o tipo de protocolo de criptografia da VPN. Ex.: IPSEC;
- Event: Exibe especificamente qual foi o evento que gerou o *log*. Caso clique em cima deste campo é possível efetuar uma busca utilizando-o como filtro;
- Action: Exibe os seguintes botões:
 - Session ID []: Ao clicar neste botão será executada uma busca com uma query utilizando especificamente o ID da VPN do evento selecionado;
 - Description []: Ao clicar neste botão a janela Description será exibida.

À seguir vamos analisar o Query Editor.

VPN - Query Editor

Através do Query Editor, é possível criar, editar e salvar queries para efetuar uma busca aprofundada nos eventos, ao clicar no Query Editor [

| Query editor |] a seguinte janela será exibida: | | | | | - |
|--|---|---|---|--|---|-----------|
| 50 | Query Editor | | | | × | |
| | Filter styling | De | ate range | | | |
| | Pillar thing security. | | | | | |
| | #Bbar | .Vo | aite | | | |
| | Server a field w | | Egan sysae | | + | |
| | | | | | | |
| 8 | | | Cical | Cancel | South | |
| | VPN - Query Editor | | | | | |
| • By • TC • Ye • La • La • Th • La • Filter: Esta • us • sr • ds • vin • ty • pr • ev • Equals/Co • Ecc • No • Co • No • Value: Esta | y period: Exibe resultados de uma data inicial (" <i>Start date</i> ") até uma data fina oday: Exibe resultados especificamente para a data de hoje; esterday: Exibe resultados especificamente para ontem; ast 7 days: Filtra especificamente os resultados dos últimos 7 dias; ast 30 days: Filtra especificamente os resultados dos últimos 30 dias; his month: Exibe os resultados deste mês; ast month: Exibe os resultados do último mês. a caixa de seleção permite selecionar o tipo de filtro utilizado pela <i>query</i> ; ser: Este filtro efetua a seleção por usuário, ele aceita e-mails como valores. c: Efetua a seleção pelo <i>IP</i> de origem, este filtro aceita endereços IPv4 ou lpé trual_address: Faz a seleção pelo IP virtual da VPN, este filtro aceita endereços rotocolo: Este filtro permite a seleção pelo perotocolo de criptografia da VPN, vent: Faz a seleção por um evento específico. Ex.: connect, disconnect, etc. <i>ntain/Not Contain:</i> Esta caixa de seleção atua basicamente como um opera quals: Irá exibir todos os resultados que são EXATAMENTE iguais ao que for oto Contain: Irá exibir todos os resultados que NÃO são iguais ao que for adici <i>ontain:</i> Irá exibir todos os resultados que NÃO contêm o valor do próximo campo to Contain: Irá exibir todos os resultados que NÃO contêm o valor do próximo campo to Contain: Irá exibir todos os resultados que nÃO contêm o valor do próximo campo to Contain: Irá exibir todos os resultados que NÃO contêm o valor do próximo campo ta caixa determina o valor que será utilizado para filtrar a <i>query</i> . | s. Ex. Ipv6 /6 co ereço -acce s. radoi for ac for a | "End date") "user@blc como valo omo valor. E os IPv4 ou 1 ess, site-to- opções dis r lógico do dicionado r ado no pró: alue); campo (Val | pockbit.com; r. Ex.: 172.16 Ex.: 172.16.1 Ipv6 como <i>va</i> -site, etc; sponíveis são filtro da <i>quer</i> no próximo ca ximo campo d | 5.12.171; 2.171; <i>ilor.</i> Ex.: 192.168.2 p: SSL ou IPSEC; y; ampo (<i>Value</i>); (<i>Value</i>); | 200.4/32; |
| Após editar os camp | bos anteriores, clique em [] para exibir a <i>string</i> utilizada pela busca na | ia ca | ixa de texto | o Filter String | ı. | |
| Para limpar a <i>query</i> utilizando a <i>query</i> cli | configurada, clique no botão [Clear]. Caso deseje cancelar clique ique no botão [Search]. | ue no | o botão [| Cancel |]. Para efetuar un | na busca |

À seguir vamos exibir o funcionamento do botão Description.
VPN - Description

O botão Description[

] exibe detalhes mais aprofundados do evento em questão, conforme exibido na imagem abaixo:

| Description | | × |
|-------------------|---|---|
| | | |
| ID | ae4bc723ec325faaf28f6bTfa4l236a1 | |
| Connection 10 | 37 | |
| Date | 2020-08-06 12:11:45 | |
| User | VPN 4G - Home | |
| Source | 189.100.60.138 | |
| Destination | 179.113.69.125 | |
| Virtual Address | 172.16.0.0/16, 172.31.0.0/16, 192.168.254.0/24, 172.25.0.0/24 | |
| Bytes Received | 0 Bytes | |
| Bytes Sent | 0 Bytes | |
| Bytes Total | O Bytes | |
| Packages Received | 0 | |
| Packages Sent | D | |
| Packages Total | 0 | |
| Type | site-to-site | |
| Protocol | IPSEC | |
| Event | connect | |
| Time Conection | Orn | |
| | | |

Close

Sessions - Event View

- ID: Exibe o ID da sessão do usuário que causou o evento;
- Connection ID: Exibe o ID da conexão do usuário que causou o evento;
- Date: Exibe a data do evento;
- **User:** Identifica o usuário que gerou este evento; **Source:** Exibe o endereço *IP* de origem do evento; ٠
- •
- Destination: Exibe o endereço IP de destino do evento;
- Virtual Address: Exibe o endereço IP virtual da VPN; •
- Bytes Received: Exibe a quantia de Bytes recebidos;
- Bytes Sent: Exibe a quantia de Bytes enviados;
- Bytes Total: Exibe o total de Bytes enviados e recebidos; •
- Packages Sent: Exibe o total de pacotes enviados;
- Packages Total: Exibe o total de pacotes enviados e recebidos;
- Type: Exibe o tipo de VPN;
- **Protocol:** Define o tipo de protocolo de criptografia da VPN; ٠
- Event: Exibe especificamente qual foi o evento que gerou o log;
- Time Connection: Exibe por quanto tempo o usuário ficou conectado.

Close Clique em [] para fechar esta janela.] ou em [

Monitor - Diagnostics

O painel "Diagnostics" tem como função efetuar a captura de pacotes e consultar como determinado site foi categorizado.

Para acessar esta tela, basta selecionar a opção "Diagnostics".



Monitor - Diagnostics

A tela abaixo será exibida:

| Diagnostics | | | | | |
|---------------|----------------|-----|-----|---------|---------|
| PathetCapture | Campoplantag | | | | |
| | | | | | + |
| Date | Worken Filters | Tes | Sie | Program | Actions |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Diagnostics - Packet Capture

O painel Diagnostics é composto de duas abas:

- Packet Capture;
- Category Lookup.

Diagnostics - Packet Capture

Este recurso permite ao administrador coletar dump em formato PCAP, com filtros, de qualquer tráfego filtrado pelo Blockbit UTM.

Para acessar clique na aba "Packet Capture".



Aba "Packet Capture"

A tela abaixo será exibida.

| Diagnostics | | | | | | |
|-------------------------|-------------|----------|-------|-----|-------|---------|
| Rachel Capitols Company | Linkar | | | | | |
| | | | | | | + |
| Gate 600 | netas illen | | Tex : | 919 | Ридна | Actives |
| | | | | | | |
| | | | | | | |
| | | The Dava | | | | |
| | | | | | | |

Packet Capture

Para efetuar a captura de pacotes, siga os passos à seguir:

Ao clicar sobre o botão [_____], a janela abaixo será exibida.

| Capture Settings | | × |
|------------------------------|--------|------|
| Interface | | |
| eth0 | | ~ |
| Time | | |
| 1 minute(s) | | ~ |
| Address | | |
| 172.16.100.0/24 | | |
| Port | | |
| 22,98 | | |
| Protocol | | |
| 1 1,6 | | |
| Others | | |
| Berkeley Packet Filter (BPF) | | |
| Disable IPv6 | | |
| Maximum file size: 100MB | | |
| | | |
| | Cancel | Save |

Add packet capture

- Interface: Defina a interface no qual irá realizar o monitoramento. Ex.: eth0;
- Time: Definir o tempo em que irá realizar o monitoramento. Ex.: 30s; •
- Address: Definir IP ou endereço de rede no qual irá realizar o monitoramento. Ex.: 172.16.100.0/24; •
- Port: Definir a porta ou range de porta no qual irá realizar o monitoramento. Ex.: 22,98; •
- Protocol: Definir o protocolo que irá realizar o monitoramento;
 Others: Nesse campo é possível realizar filtros usando comandos baseado no Berkeley Packet Filter(BPF);
- [V] Disable ARP: Essa opção desabilita o monitoramento de ARP na interface;
- [] Disable IPv6: Essa opção desabilita o monitoramento do protocolo IPv6.

Cancel

Save]. Após preencher os campos clique no botão [

e o sistema irá iniciar o

Caso deseja cancelar, clique em [monitoramento conforme tela abaixo.

| Diagnostics | | | | | | | |
|-------------------|----------------|---------------------|-----|----------|---------|---------|------------|
| Panicates Ce | and the second | | | | | | |
| | | | | | | | * |
| Euris . | states | 78es | Tex | See | Program | | Active |
| 2010-0111-0200-05 | | BALL HE LT. AL ROOM | 20 | 200,0310 | | | 0 |
| | | | | | | - [1] - | this age - |

Packet Capture – Progress

Aguarde a barra de progresso finalizar, os dados capturados ficam disponível para *download* ao clicar sobre o botão [

| iagnostics | | | | | | | |
|------------------|------------------|--|-----|--------|----------|---|---------|
| Nocket Cophies | Category Looking | | | | | | |
| | | | | | | | |
| ante. | Juterbaa | Tillaria | Tex | Sn | Progress | | Actions |
| 1000-02-05-01100 | 446 20 | State and Distance | 12 | 45.009 | _ | - | |

Packet Capture - Download

Diagnostics - Category Lookup

Esta tela tem como função consultar a categorização de sites. Trata-se de uma base de dados SWG (Secure Web Gateway), uma base de reputação de Urls, navegadores, arquivos e aplicações web, que contempla cerca de 88 categorias e subcategorias.

Para acessar clique na aba "Category Lookup".

| Packet Capture Ca | tegory Lookup |
|-------------------|---------------|
| | |

Aba "Category Lookup"

A tela abaixo será exibida:

| Diagnostics | |
|-------------------------|---|
| PackerCartere Earlinger | Vising |
| 1000-001-001-00-00 | non-margh ene (transferen |
| Here . | Reception |
| Orestigetted Stric | Sharp the fore not registered to the class by environment. |
| Abortion | sites with the shall or had acced greener tables of the insta- |
| Pro 2% | We statewise internation about or any gammand by equivalence that a gamming a startion or that after speed or uncomposited in L. |
| Pro-Choice | The distribution with the set of an expression by represent the representation that represent well derives a that same recorded well (but of abortion). |
| Address Dryam. | Was prevently, in distribution, regulations that according the gas or spheres in ancial name, public sphere, until practice, activities |
| Adult Harrison | table during that method for the age of inspirity |
| Adult Conset | We that dipley full is partial radius is a second content, but not invited activity, and up and paraphetradic; an environmentary tasks, |
| many | structure after impactions of cause in neuronado hastanchering, angly in the groups, not avertig result in resetting effect. |
| 24 | Souther depiction graphically tracely and a trace individy, including exhibition on part, intercolliging direct links to ach other. |
| In theorem | presthill development on advection and sexuality, with na porregulation retent. |
| | |

Diagnostics - Category Lookup

É possível pesquisar a categoria que um determinado site classificado na base do WebFilter ao digita um url na barra de busca do topo da página e clicar

no botão [

 \circ

], o sistema irá consultar a base e informar em qual categoria o site se encontra.

| iagnostics | |
|--------------------------|---|
| hibitation Cengity | |
| wentiloot.com | |
| item: | Recription |
| of courses the test of y | Here sponses day or providing relations and comparise, orbites, the relevant, and related barrens. First, including station powering the same |
| | - T birdage |
| | |

Diagnostics - Category Lookup - Search

Abaixo uma tabela informando o nome das categorias e sua respectiva descrição.

Descrição das categorias

| Nome: | Descrição: |
|--|--|
| Abuso de drogas | Sites que discutem, incentivam ou fornecem informações sobre fármacos controlados, proibidos ou regulamentados de alguma forma, e sobre abuso dos mesmos; Também sobre artigos de consumo relacionados ao uso ou abuso desses fármacos. |
| Álcool e tabaco | Sites que contêm informações, promovem ou permitem a venda de bebidas alcoólicas, produtos de tabaco, e todos os artigos e acessórios associados. São excluídos os sites de grupos de autoajuda, tais como Alcoólatras Anônimos, que fazem parte da categoria Saúde. |
| Anúncios pessoais e namoros | Sites que promovem relacionamentos interpessoais, excluindo-se os específicos para gays ou lésbicas. |
| Anúncios publicitários | Sites que contêm servidores de anúncios. |
| Armas | Sites que contêm informações, promovem ou permitem, a venda de armas e artigos relacionados. |
| Armazenament o/ <i>Backup</i> pessoal em rede | Sites que armazenam arquivos pessoais em servidores de Internet, para fins de backup ou troca. Ex.: Serviços de armazenamento de álbuns e fotos digitais. |
| Ativismo relacionado a direitos reprodutivos | Sites que apresentam discussões neutras ou equilibradas do assunto são classificados na categoria principal (Ativismo relacionado a direitos reprodutivos). |
| Buscas de emprego | Sites que contêm informações sobre ou que permitem a busca de empregos. |
| Caça esportiva / Clubes de armas | Sites de clubes interessados em armas, catálogos ou listas de sites de clubes desse tipo. Esta categoria inclui sites de games de guerra e de paintball (armas de tinta). |
| Chat na Web | Sites que hospedam serviços de chat (bate-papo na Web via HTTP) ou em chat rooms (salas de bate-papo via IRC (Internet Relay Chat)), homepages dedicadas a IRC e sites que oferecem fóruns ou grupos de discussão. |
| Compartilhame nto de arquivos <i>peer- to-peer</i> | Sites que fornecem software de computador-cliente possibilitando o compartilhamento e a transferência de arquivos de modo não- hierárquico. |
| Compras | Sites nos quais se pode efetuar compras on-line de produtos de consumo, mas não de artigos de caráter sexual, relacionados a investimentos, software ou hardware de computador, suplementos nutritivos, álcool e tabaco, serviços de viagem, veículos e peças ou armas. Inclui sites dedicados exclusivamente à venda de artigos esportivos e religiosos. |
| Comunicações pela <i>Internet</i> | Sites que permitem a troca instantâneas de mensagens ou <i>e-mails</i> . |
| Conteúdo ilegal /questionável | Sites que contêm informações sobre, ou que incentivam, crime (exceto crimes relacionados a informática), comportamento antiético, desonesto, ou como evitar indiciação. |
| Conteúdo para maiores | Sites que contêm nudez parcial ou total, que representam ou definem um contexto de orientação sexual, mas que não contêm atividade sexual propriamente dita; artigos de caráter sexual; publicações eróticas e outras que apresentam ou discutem assuntos relacionados a sexo, próximas à pornografia; empresas cujos negócios são de caráter sexual, como boates, inferninhos, serviços de acompanhante, <i>sites</i> com senha/verificação. Inclui <i>sites</i> nos quais se pode adquirir tais produtos e serviços <i>on-line</i> . |
| Corretagem e negociações o <i>n-lin</i> e | Sites que possibilitam a negociação ativa no mercado de capitais e o gerenciamento de investimentos financeiros. |
| <i>Download</i> de freeware /software | Sites cuja função principal é fornecer downloads de software e freeware. |
| Educação | Sites patrocinados ou que suportam ou oferecem informações sobre educação. |
| Educação sexual | Sites que contêm informações sobre sexo e sexualidade, sem intenção pornográfica. |
| E-mail pela Web | Sites que hospedam sistemas de e-mail baseado na Web. Qualquer serviço de e-mail baseado na Web, seja por navegador ou softw are. |
| Entretenimento | Sites que contêm informações sobre, ou que promovem, filmes, rádio e televisão sem noticiários, livros, humor, música e revistas (exceto para maiores de idade, negócios, games eletrônicos, informática, álcool e tabaco, saúde, hobbies, esportes, turismo, veículo ou armas). |

| Esportes | Sites que contêm informações sobre, ou que promovem, esportes, jogos ativos e recreação. Sites dedicados a um evento atual específico que requer uma categoria própria devido a conteúdo que pode causar objeções, demanda de largura de banda ou prejuízo potencial de produtividade. Alguns desses sites simplesmente desaparecem após certo tempo; outros são revisados após 90 dias, para fins de reclassificação. |
|--|--|
| Eventos especiais | Sites dedicados a um evento atual específico que requer uma categoria própria devido a conteúdo que pode causar objeções, demanda de largura de banda ou prejuízo potencial de produtividade. Alguns desses sites simplesmente desaparecem após certo tempo; outros são revisados após 90 dias, para fins de reclassificação. |
| Gays e lésbicas | Sites que contêm informações sobre, ou que oferecem produtos e serviços para, pessoas com estilo de vida homossexual, inclusive sites nos quais se pode fazer compras <i>on-line</i> , mas não os de caráter sexual ou relacionados a tópicos específicos. |
| Gestão de largura de banda | Sites que tem alto consumo de banda. |
| Gestão de produtividade | Sites que podem prejudicar a produtividade. |
| Governo | Sites patrocinados por órgãos governamentais ou repartições públicas, de todos os níveis governamentais (ou seja, que têm o final . gov) |
| Grupos de ativismo | Sites patrocinados por, ou dedicados a, organizações que incentivam mudanças ou reformas em normas sociais, opinião pública, prática social, atividades e relações econômicas. Exclui sites comercialmente patrocinados, sites dedicados a políticas eleitorais ou legislação, à questão do aborto, sites que pregam ódio ou violência. |
| Grupos políticos | Sites patrocinados por, ou que contêm informações sobre, partidos políticos e grupos de interesses focalizados em eleições ou legislação. |
| Hacking | Sites que contêm informações ou que incentivam o acesso a ou uso ilegal, ou de caráter questionável, de software ou equipamentos de comunicação. |
| Hobbies | Sites que contêm informações sobre, ou que promovem, passatempos que são, na maior parte, de caráter sedentário, mas que não incluem jogos ou games eletrônicos, de vídeo ou <i>on-line</i> . |
| Hospedagem de <i>Web</i> | Sites de organizações que fornecem serviços de hospedagem ou páginas de domínio de nível superior de comunidades na Web. |
| Imóveis | Sites que contêm informações sobre aluguel, compra e venda de propriedades residenciais. |
| Informações sobre Segurança de Computadores | Sites que contém informações ou ferramentas orientadas à segurança de sistemas de informática. |
| Instituições culturais | Sites patrocinados por museus, galerias, teatros (mas não cinemas e outras instituições culturais). |
| Instituições educacionais | Sites patrocinados por escolas e outras instituições educacionais ou por grupos e professores ou alunos, ou que se relacionam a eventos ou atividades educacionais. |
| Jogos de azar e apostas | Sites que contêm informações sobre, ou que promovem, jogos de azar e apostas, ou que permitem fazê-lo on-line. Sites nos quais há risco de se perder dinheiro. |
| Jogos / Games | Sites que contêm informações sobre, ou que promovem, <i>games</i> ou jogos eletrônicos, de vídeo, computador, dramatização (<i>role-play on-line</i> , mas não os que contêm jogos de cartas ou de tabuleiro; também os sites que permitem jogar ou oferecer jogos <i>on-line</i> . Inclui <i>sites</i> com sorteios e concursos). |
| Leilões na <i>Inter</i> <i>net</i> | Sites nos quais se pode participar de leilão on-line, de artigos comprados e vendidos por indivíduos. |
| <i>Lingerie</i> e maiôs | Sites que contêm fotos ou imagens gráficas de modelos em roupas sugestivas, mas não indecentes ou obscenas; imagens sugestivas de nudez e seios femininos. Também inclui sites que contêm fotos e material artístico com mulheres com pouca roupa. |
| Maconha | Sites cuja função principal é fornecer informações específicas sobre a maconha ou promover seu uso. |
| Materiais de Referência | Sites que oferecem materiais de referência como atlas, dicionários, enciclopédias, dados estatísticos, (white papers) e páginas amarelas. |
| Materiais educativos | Sites cuja função principal é fornecer informações históricas, científicas, páginas sobre pesquisa, ou materiais didáticos. |
| Mau-gosto | Sites que não se conseguiu classificar em nenhuma outra categoria, mas que contêm material ofensivo, grotesco, amedrontador, lúgubre, sem conter nada apreciável. |
| Mecanismos de busca e portais | Sites que possibilitam fazer buscas na Web, em news groups, ou índices ou diretórios dos mesmos. |

| Medicamentos ou drogas (conforme definidos pela lei dos E.U.A.) | Sites patrocinados ou que suportam ou oferecem informações sobre medicamentos ou drogas. |
|---|--|
| Medicamentos sob receita médica | Sites que fornecem informações sobre fármacos aprovados e seu uso médico. |
| Monitoramento indevido e invasão de privacidade | Sites ou páginas que podem descarregar software que, sem o conhecimento do usuário, ou sem sua permissão, monitorá-lo. |
| MP3 | Sites que permitem fazer download de arquivos MP3 ou que funcionam como catálogos de sites desse tipo. |
| Negócios e Economia | Sites patrocinados por, ou dedicados a, empresas individuais que não oferecem comércio eletrônico e não firmas relacionadas ao setor de computação e comércio na <i>Internet</i> ou à venda de bebidas alcoólicas e cigarros/tabaco, a serviços de viagem, veículos ou armas. Inclui corretoras de imóveis comerciais, mas não residenciais. |
| Noticiários e mídia | Sites que contêm noticiários em tempo real, inclusive os patrocinados por jornais, revistas, revistas especializadas ou acadêmicas, estações de rádio, redes de televisão, serviços telegráficos, mas não os que fornecem cotações da bolsa de valores ou os relacionados a esportes. |
| Nudez | Sites que apresentam nudez ou seminudez humana, de indivíduos ou grupos, e que não são abertamente de caráter sexual. |
| Organizações de Serviços e Filantrópicas | Sites patrocinados ou que suportam ou oferecem informações sobre organizações dedicadas a fazer o bem como sua principal atividade. |
| Organizações de Trabalho e Profissionais | Sites patrocinados ou que suportam ou oferecem informações sobre organizações dedicadas ao desenvolvimento profissional ou interesses de trabalhadores. |
| Organizações Sociais | Sites patrocinados ou que suportam ou oferecem informações sobre organizações dedicadas. |
| Organizações Sociais e Afiliações | Sites patrocinados ou que suportam ou oferecem informações sobre organizações dedicadas primariamente a socialização ou interesses comuns diferentes de filantropia ou desenvolvimento profissional. |
| Órgãos militares | Sites patrocinados por órgãos ou organizações militares (com final .mil) |
| Pedofilia | Sites que incentivam a pedofilia ou que disponibilizam imagens ou textos com teor pedófilo. |
| Publicações alternativas | São os equivalentes on-line aos jornais de tabloide. Obs.: Esta categoria pode conter matérias de caráter sexual. |
| Quadros de mensagens e clubes | Sites de clubes sociais e de negócios, grupos de discussão pessoais ou de negócios, e servidores de listas que não estão classificados em nenhuma outra categoria. |
| Racismo/ódio | Sites que incentivam a identificação de grupos raciais, a difamação ou submissão de grupos (identificados por raça ou de outra forma, ou a superioridade de um determinado grupo. |
| Rádio e TV na <i>l</i> nternet | Sites cuja função principal é fornecer programas de rádio e TV na Internet. |
| Religião | Sites que contêm informações sobre, ou que promovem, religiões. |
| Religiões não- tradicionais | Sites que contêm informações sobre, ou que promovem, religiões que não constam na categoria 22.2 e outras religiões não tradicionais, ou tópicos semi-religiosos, inclusive sobre cultos. |
| Religiões tradicionais | Sites que contêm informações sobre, ou que promovem, budismo, bahai, cristianismo, ciência cristã, hinduísmo, islã, judaísmo, mormonismo, xintoísmo, siquismo; também, sites de ateísmo. |
| Restaurantes e gastronomia | Sites que contêm listas, resenhas e anúncios, ou que promovem serviços relacionados a gastronomia, bufês e restaurantes. |
| Saúde | Sites que contêm informações ou orientação sobre saúde pessoal ou serviços médicos, seguro-saúde, procedimentos ou dispositivos, mas que não se relacionam a medicamentos. Inclui grupos de autoajuda. |
| Serviços e dados financeiros | Sites que contêm noticiários e cotações de ações, obrigações e outros veículos financeiros, aconselhamento sobre investimentos; mas que não oferecem negociações ou corretagem <i>on-line</i> . Inclui bancos, cooperativas de crédito, cartões de crédito e companhias de seguro de vida. |
| Sexo | Sites que apresentam imagens de atos ou atividades sexuais, ou que os descrevem de forma gráfica, incluindo exibicionismo. |

| Sistemas de evitação de <i>pro</i> <i>xy</i> | Sites que contêm informações sobre como evitar as funções de servidores proxy ou como obter acesso a URLs de forma a evitar o servidor proxy. |
|--|---|
| Sistemas de troca instantânea de mensagens | Sites que permitem a troca instantâneas de mensagens. |
| <i>Sites</i> a favor da liberdade de escolha | Sites patrocinados por, ou dedicados a, organizações que incentivam a liberdade de escolha. |
| Sites de militância /extremismo | Sites que contêm informações sobre que promovem, ou que são patrocinados por grupos de ativismo que pregam ações antigovernamentais. |
| <i>Sites</i> de tradução de <i>URL</i> | Sites que oferecem tradução on-line de URLs. |
| <i>Sites</i> Maliciosos | Sites que contém código que modifica intencionalmente sistemas de usuários sem seu consentimento, ou que causa danos. |
| Sites para maiores de idade | Sites que contém conteúdo para maiores de idade. |
| <i>Sites</i> pessoais na <i>Web</i> | Sites publicados por indivíduos para uso pessoal ou intercâmbio; não são publicados por nenhuma organização. |
| Sites pró-vida | Sites patrocinados por, ou dedicados a, organizações que incentivam a vida. |
| <i>Sites</i> que pagam para surfar (<i>pay-to-</i> <i>surf</i>) | Sites que pagam o indivíduo para surfar, ou para enviar <i>e-mail.</i> |
| Sociedade e estilos de vida | Sites que contêm informações sobre assuntos relacionados ao cotidiano, excluindo-se sexo, entretenimento, empregos, esportes, e os tópicos cobertos pelas subseções abaixo. |
| Spyware | Sites ou páginas que podem descarregar software que, sem o conhecimento do usuário, ou sem sua permissão, gera tráfego HTTP (com exceção de simples identificação e validação de usuários. |
| <i>Streaming</i> mídia | Sites cuja função principal é fornecer conteúdo de mídia tipo streaming, tais como trailers de filmes. |
| Suplementos /compostos não- regulamentados | Sites que contêm informações sobre, ou que incentivam, o uso de substâncias químicas (como as existentes em compostos naturais, por exemplo não controladas pela <i>FDA</i> (<i>Food and Drug Administration</i> - Administração de Alimentos e Medicamentos do Departamento de Saúde e Serviços Humanos dos E.U.A.)). |
| Tecnologia da informação | Sites patrocinados por, ou que contêm informações sobre, empresas do setor de computação e Internet. |
| Telefonia via <i>In</i> ternet | Sites que possibilitam aos usuários fazer chamadas telefônicas através da Internet, ou obter informações ou software para esse fim. |
| Turismo | Sites que contêm informações sobre, ou que promovem, vários serviços relacionados a viagem, inclusive sites nos quais se pode fazer compras ou reservas on-line. |
| Veículos | Sites que contêm informações sobre, ou que promovem, veículos, inclusive sites nos quais se pode comprar peças ou veículos on- line. |
| Violência | Sites que contêm informações sobre, ou que promovem, atos de violência. Sites que contêm um excesso de obscenidade ou linguagem indecorosa podem ser colocados nesta categoria, se não o forem na categoria (mau-gosto). |

As categorias apresentadas aqui podem ser utilizadas na criação de perfis Web Filter, para mais informações a respeito deste processe cheque esta página

Monitor - Reports

A função desta opção é administrar a criação automática e periódica de relatórios personalizados, permitindo seleção de característica específica dos devi ces selecionados.

Para acessar e administrar a criação automática de relatórios, clique no ícone "Reports" localizado na lateral esquerda:



Analytics - Reports

A tela de reports será exibida.

| Reports | | | | | |
|---------|----------|---------|-------|------|---------|
| | | | | | |
| · | Kdwikidd | Dealery | Paikd | Mate | sations |
| | | | | | |
| | | | | | |
| | | | | | |

Reports

Nesta sessão iremos analisar:

- Como adicionar e deletar os reports;
- Detalhes das colunas desta tela;
- Exemplos de como gerar *reports* específicos.

A seguir analisaremos a função de cada componente desta tela.

Monitor - Reports - Menu de Ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



Reports - Menu de Ações

O menu é composto das seguintes opções:

- Create;
- Delete.

A seguir cada opção do menu de ações será detalhada.

Monitor - Reports - Menu de ações - Create Report

Na opção de criação de relatório é possível configurarmos de qual funcionalidade as informações serão exibidas em Monitor > Reports. Podemos configurar relatórios de Firewall, Web Filter ou mesmo de logs da VPN. Abaixo veremos como selecionar e configurar estes relatórios.

Para criar um relatório automático clique em "Create", a seguinte tela será exibida, com a aba lateral "Settings" pré-selecionada:

| Î. | * Name | |
|----------|-----------------------|--------|
| Settings | hanc | |
| Datasets | * Description | |
| | | |
| Custom | Туре | |
| | Analyzer | \sim |
| | * Scheduled | |
| | Select date | 曲 |
| | Recurrence | |
| | Unique | \sim |
| | * Period | |
| | Start date ^ End date | Ë |
| | * Device/Logger | |
| | Select Device/Logger | \sim |
| | Send Report by Email | |

Reports - Create Report

Esta janela é composta pelas seguintes abas laterais:

- Settings;
- Datasets;
- Custom.

A seguir analisaremos o conteúdo desta janela e todas suas abas.

Aba Settings

Create Report

| atasets | * Description | | |
|---------|----------------------|----------|--------|
| | | | |
| Custom | | | 1. |
| custom | Туре | | |
| | Analyzer | | \sim |
| | * Scheduled | | |
| | Select date | | 曲 |
| | Recurrence | | |
| | Unique | | V |
| | * Period | | |
| | Start date | End date | |
| | * Device/Logger | | |
| | Select Device/Logger | | N. |
| | Send Report by Email | | |
| | | | |

A seguir analisaremos cada campo deste painel:

- Name: O nome do relatório. Ex.: Firewall Report,
- Description: A descrição do relatório. Ex.: Firewall Report;
 - *Type*: Este menu suspenso determina as opções que estarão disponíveis na aba "*Datasets*", temos as seguintes opções:
 Relatório em PDF:
 - Analyzer: Cria um relatório em PDF com informações do analyzer a respeito do serviço selecionado ou das atividades de um usuário em específico.
 - Relatório em CSV:
 - Log Session: Cria um relatório CSV sobre as sessões dos usuários, contém informações como: ID de sessão, data e hora do acesso, identificação do usuário, endereço MAC, serviço utilizado e etc;
 - Log Authentication: Cria um relatório CSV com os registros dos eventos de autenticação do sistema;
 - Log VPN: Cria um relatório CSV sobre todos os acessos utilizando VPN, contém informações como: ID da VPN, data e hora do acesso, IP de destino e de origem, informações de tráfego dos pacotes, bytes recebidos e enviados e etc.

| Analyzer | ~ |
|--------------------|---|
| | |
| PDF | |
| Analyzer | |
| CSV | |
| Log Session | |
| Log Authentication | |
| LOS VPN | |

Reports - Create Report - Type window

- Top Hits: Gera um relatório de Top Hits, sendo que na aba Datasets é determinado a quantia de hits a ser amostrado e os filtros a serem utilizados;
 - Top Bytes: Gera um relatório de Top Bytes, sendo que na aba Datasets é determinado a quantia de bytes a ser amostrado e os filtros a serem utilizados;
 - Log: Permite a criação de um relatório personalizado, em Datasets é possível utilizar-se de Queries personalizadas e determinar os 0 filtros a serem utilizados.
- Scheduled: Exibe a data de agendamento para quando esse relatório será executado;
- Recurrence: Periodicidade na qual o relatório será executado, escolha entre daily (diário), weekly (semanal) e monthly (mensal);

| Unique | ~ |
|---------|---|
| Unique | |
| Daily | |
| Weekly | |
| Monthly | |

Reports - Create Report - Recurrence window

- Period: Determina o período de quando os dados serão analisados pelo logger nos UTMs Ex.: Ao selecionar de 1 de janeiro de 2019 a 05 de ٠ fevereiro de 2020, todos os dados que existirem fora desse período, não serão exibidos no "*Report*". **Device/Logger:** É selecionado o device de onde os dados serão analisados para gerar o relatório.



É importante salientar que para receber os relatórios é necessário fazer as configurações de e-mail.

A seguir vamos analisar o conteúdo da aba lateral Datasets;

Aba Datasets

A aba "Datasets" determina os tipos de dados que serão utilizados na criação dos relatórios, conforme mencionado anteriormente, os componentes dela são determinados pela caixa de seleção "Type" da aba "Settings". Caso tenha selecionado a opção "Analyzer", a aba "Datasets" poderá ser configurada conforme as opções abaixo:

| ^ |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |

- Firewall: Exibe informações equivalentes ao Analyzer Firewall, para mais informações consulte esta página;
- Web Filter: Exibe informações equivalentes ao Analyzer Webfilter, para mais informações consulte esta página; .
- Application Control: Exibe informações equivalentes ao Analyzer Application Control, para mais informações consulte esta página; Intrusion Prevention: Exibe informações equivalentes ao Analyzer Intrusion Prevention, para mais informações consulte esta página; ٠
- Threat Protection: Exibe informações equivalentes ao Analyzer Threat Protection, para mais informações consulte esta página;
- User Behavior: Exibe informações equivalentes aos acessos de um usuário em específico. Ao selecionar esta opção, o campo "Select a user" • será exibido, selecione o usuário no qual o será baseado;
- VPN: Exibe informações equivalentes ao Analyzer - VPN, para mais informações consulte esta página;

Caso tenha selecionado a opção "Log Session", a aba "Datasets" poderá ser configurada conforme as opções abaixo:

| | - | | | \sim |
|----------|---------|--------|----------|--------|
| Datasets | Filter | | Analyzer | |
| | logtype | \sim | Equals | ×. |
| | Values | | | |
| | | | | + |
| | List | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Reports - Create Report - Datasets - Log Session

Com objetivo de facilitar na configuração do *dataset* do relatório: Atente que a sintaxe usada em Security Events é a mesma utilizada nesta janela.

Por exemplo, caso o objetivo seja criar um relatório sobre VPN site-to-site onde ouve um evento de conexão, basta clicar nas colunas em Security Events - VPN e se atentar na sintaxe que será exibida na barra de busca, conforme pode ser observado abaixo:

| Date User Searce Resthantion Winial Address Bytes Paskets Type Protocol Event Action 0038-07-02 54:5 VTH-UTMML 172.31.0.1 172.31.0.0.342 0 Bytes 0 state-state Exclored 0 Excl | | event "cornect" | | | | | | 3 | 8 | Query tidits |
|---|-------------------------|--------------------|----------------|------------------|---------|----------|--------------|----------|---------|--------------|
| 2028-01-29 144 | Date User | Source | Destination | Virtual Address | Bytes | Packets | Туре | Protocol | Event | Action |
| AD24-01-091344_UTMO24 x, 385,196,600,136 365,196,800,342 0 0 yees 0 seems the end of owner. If it appendix of the set of the end of the set of the end of | 2028-07-20 \$4(3 | W., 172.31.0.1 | 172.31.200.5 | | 0.8566 | | sta-tri-sta | PERC | connect | 9 = |
| A024-07-29134a | 2024-07-29 13:4 UTM DEV | K., 185,186,60,138 | 189-108-00-142 | | 0 Bytes | ø | site-to-site | MSCC. | connect | :2 ≡ |
| Scherber 281364_ VPH-KTMM_ 112.810.1 172.81.203.3 0 Byres Veter-We Convert Image: Convert | 2028-07-20 1314 | eK 188,108,80,138 | 201.54.225.30 | | o Byses | 0 | site-to-site | PSEC | towed | 9 = |
| iso, de volta em Create Report - Datasets, replicar a mesma sintaxe utilizando as opções do painel, segue um exemplo: | 2020-07-29.334 | W., 112:31-04 | 172,31,200,5 | | 0 Bytes | 0 | 100-11-100 | REC | connect | ⊅ ≡ |
| isso, de volta em <i>Create Report - Datasets</i> , replicar a mesma sintaxe utilizando as opções do painel, segue um exemplo: | | | | | | | | | | 3X page |
| Values Values List equalitypesite-to-site equalitypesite-to-site | | Settings | event | | V. | Equila | | | | |
| Settings Filter Analyzer event vitues Values List equalitypesite-to-site equalitypesite-to-site | | Create Repo | rt | | | | | × | | |
| event tousis Values List equalitypesite-to-site equalitypesite-to-site | | Settings | Filter | | | Analyzer | | | | |
| Values Values + List equalitypesite-to-site equalitypesite-to-site = | | | event | | ×. | Squals | Y., | | | |
| List equalitypesite-to-site equalitypesite-to-site | | Datasets | Values | | | | 1000 | | | |
| equalitypeisite-to-site = | | | (let) | | | | - | | | |
| equalieventiconnect | | | enuals | types/te-to-site | | | 1 | | | |
| | | | equal: | eventiconnect | | | - | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

• Custom Queries: Permite a seleção de queries customizadas. As queries que aparecem nesse campo são as que foram criadas em Security Events, consulte esta página para mais informações;

- Filter: Determina qual filtro será utilizado. Ex.: dst;
- Analyzer: Determina qual operação será efetuada no filtro. Ex.: not equals;
- + • Values: Define o valor que será atrelado à operação e ao filtro. Clique em [____] para adicionar à lista ou selecione uma entrada já adicionada
- e clique em [_____] para remover da lista. Ex.: 1.1.1.1; *List:* Basicamente exibe as adições feitas com base nas opções anteriores. Ex.: not_equal:dst:1.1.1.1.

Caso tenha selecionado a opção "Log Authentication" ou "Log VPN", a aba "Datasets" poderá ser configurada conforme as opções abaixo:

| Sottings | Filter | | Analyzer | | |
|------------------------------------|---|---------------------|---------------------------|--------|--------|
| Setungs | protocol | \sim | Not equals | ~ | |
| Datasets | Values | | | | |
| | | | | + | |
| | List | | | | |
| | | | * | | |
| | | | | _ | |
| | | | * | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | ~ |
| | | | Cancel | Create | |
| | | | Cancel | Create | |
| | Reports – Create Report - Datase | ts - Log Authentica | Cancel tion ou Log VPN | Create | * |
| | Reports – Create Report - Datase | ts - Log Authentica | Cancel tion ou Log VPN | Create | e 1 |
| J Determina qual filtro será ut | Reports – Create Report - Dataser ilizado. Ex.: dst; | ts - Log Authentica | Cancel tion ou Log VPN | Create | * |

• List: Basicamente exibe as adições feitas com base nas opções anteriores. Ex.: not_equal:dst:1.1.1.1.

A seguir vamos analisar o conteúdo da aba lateral "Custom", ela só será exibida caso o tipo de relatório for "Analyzer";

Aba Custom

Na aba "Custom" é possível determinar o texto que ficará de rodapé em "Footer" e customizar o "Logo" que aparecerá no relatório.

| Settings | Footer Text | |
|----------|----------------|--------|
| Datasets | Customize Logo | |
| Custom | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | Cancel |

Clique no botão Cancel] para sair dessa janela ou clique em Create] para agendar o relatório. Caso queira emiti-lo imediatamente configure-o para ser executado na data de hoje.



Report added successfully

Report added successfully

Depois destes passos, o relatório terá sido criado com sucesso.

Para ver exemplos de como criar os relatórios, acesse esta página.

Caso queira mais informações sobre como deletar um relatório, consulte esta página.

Exemplos - Criação de Reports

A seguir, vamos exemplificar a criação de alguns exemplos de *reports* como forma de demonstrar de boas práticas. Os modelo apresentados visam orientar e servir como base para o usuário criar os seus próprios relatórios conforme a sua preferência e necessidade.

Efetuaremos a demonstração criando os seguintes reports:

- Exemplo 1 Relatório de *Firewall;*Exemplo 2 Relatório de *Webfilter* para destino de acesso estrangeiro que foi permitido pelas políticas;
- Exemplo 3 Relatório de conexão de VPN site-to-site com origem e destino específico.

Exemplo 1 - Relatório de Firewall



A janela "Create Report" será exibida como demonstrado abaixo:

| Settings | * Name | | |
|----------|---------------|----------|---|
| | | | |
| Datasets | * Description | | |
| Custom | | | / |
| Subcom | Туре | | |
| | Analyzer | | |
| | * Scheduled | | |
| | Select date | | 自 |
| | * Period | | |
| | Start date ~ | End date | 巴 |
| | | | |
| | | | |
| | | | |
| | | | |

Reports - Create Report

Já na aba "Settings" siga as instruções à seguir.

Settings

Complete o formulário conforme o exemplo:

| Sottings | * Name | |
|----------|-------------------------|---|
| octango | Firewall | |
|)atasets | * Description | |
| | Report - Firewall | |
| Custom | Туре | |
| | Analyzer | V |
| | * Scheduled | |
| | 2020-07-29 12:07:27 | Ē |
| | * Period | |
| | 2020-06-01 ~ 2020-07-29 | Ē |
| | 2020-06-01 ~ 2020-07-29 | Ē |
| | Cancel | |

- Name: Digite "Firewall";
 Description: Digite "Report Firewall";
 Type: Selecione o relatório do tipo "Analyzer";
 Scheduled: Selecione uma data e horário para agendar a criação do relatório;
- Period: Selecione um período inicial e um final.

Ao finalizar, acesse a aba lateral "Datasets".

Datasets

Selecione a opção conforme o exemplo:

| Settings | Analyzer | | |
|----------|----------|--------|--------|
| 0 | Firewall | | \sim |
| Datasets | | | |
| Custom | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Cancel | Crea |

Ao finalizar, acesse a aba lateral "Custom".

Custom

Esta aba depende do design do usuário. No exemplo, configuramos conforme demonstrado abaixo:

| | Create Report | | | × |
|---|--|---|---------------------|--------|
| | Settings | Footer Text | | |
| | Datasets | Customize Logo | | |
| | Custom | | | |
| | | | | * |
| | 3 | | Cancel | Create |
| | | Create Report - Aba Custom | | |
| Footer 1Custom | Text: No rodapé digite " <i>UTM</i> ize Logo: Faça o <i>upload</i> do | - Firewall Report"; logo da empresa. Neste exemplo, utilizamos o íco | one do <i>UTM</i> . | |
| Após ter configura | ado cada aba de acordo com | a definição do exemplo aplicada, clique em [| Create]. | |
| | | Report added successfull Report added successfully | У | |

2

4

Depois destes passos, o relatório terá sido criado com sucesso.

Para consultar o exemplo 2, clique neste link.

Exemplo 2 - Relatório de Webfilter para destino de acesso estrangeiro que foi permitido pelas políticas

Neste exemplo iremos criar um relatório de Web Filter para exibir todas as conexões que foram feitas para sites estrangeiros onde a política permitiu o acesso.



A janela "Create Report" será exibida como demonstrado abaixo:

Create Report

| Datasets | * Description | |
|----------|-----------------------|--------|
| C | | |
| Custom | Туре | |
| | Analyzer | \sim |
| | * Scheduled | |
| | Select date | 白 |
| | * Period | |
| | Start date ~ End date | 問 |
| | | |

2

Х

Já na aba "Settings" siga as instruções à seguir.

Settings

Complete o formulário conforme o exemplo:

172

Create Report

| Serungs | Well Files | |
|----------|-------------------------|---|
| | web Filter | |
| Datasets | * Description | |
| | Report - Web Filter | |
| | Туре | |
| | Log Session | N |
| | * Scheduled | |
| | 2020-07-29 15:59:50 | 曲 |
| | * Period | |
| | 2020-07-29 ~ 2020-07-29 | Ē |
| | | |
| | | |

Х

Create Report - Aba Settings

- Name: Digite "Web Filter";
 Description: Digite "Report Web Filter";
 Type: Selecione o relatório do tipo "Log Session";
- Scheduled: Selecione uma data e horário para agendar a criação do relatório;
 Period: Selecione um período inicial e um final.

Ao finalizar, acesse a aba lateral "Datasets".

Datasets

Selecione a opção conforme o exemplo:

| Create | Report |
|--------|--------|

.

| Settings | Custom queries | | |
|--|--|------------------------------|--|
| | | | \sim |
| Datasets | Filter | Analyzer | |
| | rule_action ∨ | Equals | |
| | Values | | |
| | | | + |
| | List | | |
| | equal:logtype:webfilter | * | |
| | not_equal:geoip_dst:BR equal:rule_action:allow | - | - |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | * |
| | | Cancel | Create |
| <i>3</i> 5 | | | · · · |
| | Create Report - Aba Datasets | | |
| Nesta aba iremos adicionar 3 condições: | | | |
| | | | |
| | | | + |
| 1. Tipo de Log Web Filter: Em Filter, selecio a adição na lista; | ne <i>logtype</i> , deixe o Analyzer como equals, em V | <i>alues</i> digite webfilte | r e clique no botão [] para fazer |
| 2. Localização geográfica de destino estrar | geira: Em <i>Filter</i> , selecione <i>geoip_dst</i> , no <i>Analyz</i> | zer selecione Not E | <i>qual</i> s, em Values digite <i>BR</i> e clique no |
| botão I para fazer a adição na lista | | | |
| | | | |

Х

3. Política permitiu o acesso: Em Filter, selecione rule_action, deixe o Analyzer como equals, em Values digite allow e clique no botão] para fazer a adição na lista;

Após ter adicionado essas condições o relatório será criado especificamente para Webfilter cujo destino de acesso foi estrangeiro e foi permitido pelas , políticas.

Após ter configurado cada aba de acordo com a definição do exemplo, clique em [





Depois destes passos, o relatório terá sido criado com sucesso.

Clique neste link para ver o exemplo 3.

Exemplo 3 - Relatório de conexão de VPN site-to-site com origem e destino específico

Neste exemplo vamos criar um relatório de conexão VPN site-to-site com objetivo de localizar todos os acessos feitos dentro de um IP de origem e de destino específico.



A janela "Create Report" será exibida como demonstrado abaixo:

Create Report

| Datasets | * Description | |
|----------|-----------------------|--------|
| Custom | | |
| | Туре | |
| | Analyzer | \sim |
| | * Scheduled | |
| | Select date | 白 |
| | * Period | |
| | Start date ~ End date | Ē |
| | | |
| | | |
| | | |
| | | |

2

Х

Já na aba "Settings" siga as instruções à seguir.

Settings

Complete o formulário conforme o exemplo:

Create Report

| cupor-turnor | | |
|--------------|-------------------------|--------|
| atasets | * Description | |
| | Report - VPN | |
| | Туре | |
| | Log VPN | \sim |
| | * Scheduled | |
| | 2020-07-29 16:30:25 | 白 |
| | * Period | |
| | 2020-07-29 ~ 2020-07-29 | 曲 |
| | | |
| | | |
| | | |
| | | |

Create Report - Aba Settings

÷.

- Name: Digite "VPN";
 Description: Digite "Report VPN";
 Type: Selecione o relatório do tipo "Log VPN";
- Scheduled: Selecione uma data e horário para agendar a criação do relatório;
 Period: Selecione um período inicial e um final.

Ao finalizar, acesse a aba lateral "Datasets".

Datasets

Selecione a opção conforme o exemplo:

Х

| | Create Report | | | | > | |
|---|--|---|--------------------------------------|---------------------------------------|-------------------------|---------------------------|
| | | | | | | |
| | Settings | Filter | | Analyzer | | |
| | | event | \sim | Equals | \sim | |
| | Datasets | Values | | | | |
| | 1.1 | | | | + | |
| | | List | | | | |
| | | contain:src:%17 | 2.31% | | | |
| | | contain:dst:%20 | 0.5% | | - | |
| | | equal:type:site- | to-site | | | |
| | | | | | | |
| | 26 | | | Cancel | Create | |
| | | Create Re | eport - Aba Datasets | | | |
| Nesta aba iremos | adicionar 4 condições: | | | | | |
| 1. O IP de origen a fazer a adição r | n começa com 172.31: Em na lista; | <i>Filter</i> , selecione <i>src</i> , no <i>An</i> | alyzer selecione Conta | <i>in</i> , em Values digite | e 172.31 e clique | no botão [+] par |
| O IP de destin a adição na lista; | o possui 200.5: Em <i>Filter</i> , s | elecione <i>dst</i> , no Analyzer | selecione <i>Contain</i> , em | <i>Values</i> digite 200.5 | e clique no botã | o [] para fazer |
| 3. O tipo de VPN fazer a adição na | l é site-to-site: Em Filter , se lista; | lecione <i>type</i> , deixe o Analy | /zer como equals, em \ | /alues digite s <i>ite-to-</i> | <i>site</i> e clique no | potão [] para |
| 4. Só queremos ara fazer a adição | eventos de conexão: Em <i>F</i> o na lista; | ilter , selecione <i>event</i> , deixe | e o Analyzer como equ | als, em Values digit | e <i>connect</i> e cliq | ue no botão [] p |

Após ter adicionado essas condições o relatório será criado especificamente para VPNs site-to-site cujo IP de origem possua "172.31" o IP de destino possua "200.5" e efetuada uma conexão.



Depois destes passos, o relatório terá sido criado com sucesso.
Monitor - Reports - Menu de ações - Delete Report

Através do botão "Delete" é possível deletar os Reports selecionados. Para deletar através do Menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Report*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *reports* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*:

| | n | | | | | |
|---|---|--|-------|--|------------|---------|
| • | taxe | Schedulad | Outer | Ancied | ibihui | Actions |
| | (9Teal) http://www. | Distance of the second se | 1010 | Hum (December 10, 2018 To Occession 108, 2018 | (Annual) | = a |
| | (94-sport). Names in coefficiently do | Canada alexandra alexanda Canada alexandra alexanda | **** | Num (December 10, 2018 An December 00, 2018 | (Annua) | = 0 |
| | (Statuaice Report | OWELLERIA INCOME | 1000 | Foreithderfor M. 2020 Re Departition (M. 2020 | - | ≡ a |

Reports - Seleção dos Reports para deletar



3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os *Reports* selecionados:

| Delete Profile | Х |
|----------------------|---------------|
| Delete Test reports? | |
| | Cancel Delete |

Reports - Mensagem de deleção do Report



Após realizar esses procedimentos, os reports terão sido deletados com sucesso.

À seguir analisaremos as colunas de exibidas na tela Monitor Reports.

Monitor - Reports - Colunas

A seguir explicaremos cada coluna da aba Reports:

| econ | ds | | | | | | R. |
|------|----------------------------------|--|---------------|---|--------------------|----------|--------|
| | Name | Schestaled | Owner | Period | Recorners | Status | Action |
| | Report 1 Intrusion Prevention | 07/03/2003 (7588:11 Oracted 97/83/2022 17:33:00 | Administrador | fishre March 66, 2002 to: March 66, 2002 | 0.241y et 10:00 | Parality | = 0 |



- Select []: Permite selecionar um report;
- Name: Exibe o nome do relatório cadastrado na opção Create do menu de ações. Logo abaixo do nome está a descrição cadastrada no mesmo menu;
- Scheduled: Exibe o agendamento para quando o relatório será executado, logo abaixo dessa data está marcada a data de quando esse processo foi criado;
- Owner: Exibe o usuário responsável por criar esse agendamento;
- *Period*: É onde está registrado o período de quando os dados serão extraídos do sistema; *Recurrence:* Frequência com a qual o relatório será gerado; •
- Status: É exibido o estado atual da produção do relatório. Podendo ser:
 - Visualize]: Sendo possível visualizar o relatório ao clicar neste botão; • Visualize
 - Download]: Sendo possível baixar o relatório PDF ou CSV ao clicar neste botão; • Download
 - Pending [Pending]: Caso o relatório ainda não tenha sido gerado, ele estará marcado com este status.
- Actions: Botões com funções essenciais para interação com os relatórios:
 - Botão Visualizar[
 - Botão Excluir[]: Exclui o relatório selecionado.

UTM - ANALYZER

Além do dashboard já apresentado, o Blockbit UTM, possui um recurso de gerenciamento de 'Relatórios" que retorna informações essenciais para a administração e gerência de eventos e informações que reúne dados SUMARIZADOS e DETALHADOS dos principais serviços. Todos os relatórios do sistema são armazenados por 7 dias no servidor.



A principal diferença entre os relatórios exibidos em Events e os em Analyzer é que: Em Events, é gerado um registro da conexão com os atributos todos zerados (bytes e pacotes), após a desconexão outro evento é gerado registrando esses atributos, o tráfego e o tempo conectado.

Já os relatórios do Analyzer são sumarizados de 5 em 5 minutos gerando relatórios de tempos em tempos com dados gerados no período.



Analyzer

Contém as opções:

- Firewall;
- Web Filter;
- Application Control;
- Intrusion Prevention;
- ٠ Threat Protection;
- User Behavior;
- VPN.

UTM - Firewall

Para acessar os relatórios de tráfego de rede, clique no ícone "Analyzer" localizado na lateral esquerda, um menu dropdown será exibido, selecione a opção "Firewall".



Firewall

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Firewall - Caixa de seleção de data

O objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- By date: Determina uma data específica;
- By period: Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
- Today: Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
- Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
- This month: Exibe os resultados deste mês;
- Last month: Exibe os resultados do último mês.
- Policy: Verifica a regra em conjunto com os filtros acima;

Selecione o período desejado:

| | Today 🋗 |
|---------|---------|
| Period: | |
| Today | ~ |
| | Cancel |

Firewall - Seleção de Data

| Para fechar esta janela, clique em Cancel [| Cancel |] ou, após selecionar a data desejada, clique em Ok [| OK |]; |
|---|--------|---|----|----|
|---|--------|---|----|----|

A tela abaixo será exibida:



Analyzer - Firewall

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- []: Serve para dar um zoom;
- []: Tem como função remover o zoom;
 []: Serve para fazer um zoom de seleção;
- [1]: Serve para mover o gráfico;
- [1]: Reseta o gráfico para a posição inicial;
- [=]: Permitir baixar este diagrama no formato svg, png ou csv.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no botão de busca [

A seguir, analisaremos em detalhes os componentes de "Firewall":

- Geolocation;

- Geolocation;
 Zone Traffic;
 Top User;
 Top Service;
 Top Source;
 Top Policies.

UTM - Firewall – Geolocation

Em "Geolocation" é exibido o destino das conexões dos usuários da rede, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários. Ao passar o mouse por cima dos países um número total de acessos é exibido, ao fazer o mesmo com a legenda é possível visualizar uma média, além disso, o país referente a esse valor é destacado no mapa.



Firewall - Geolocation

UTM - Firewall – Zone Traffic

Em "Zone Protection" temos um gráfico demonstrando a quantia de tráfego em determinada zona, através de um gráfico de linha é possível observar esses montantes sendo ilustrados ao longo de um intervalo de tempo. Ao clicar sobre o tipo de rede utilizado (por exemplo: "LAN", "DMZ", "WAN" e etc), o diagrama é alterado de forma a exibir a opção selecionada, o que permite analisar com mais detalhamento o tráfego de acordo com as datas selecionadas.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Firewall - Zone Traffic

É possível clicar nas legendas abaixo do gráfico, para ocultar alguma das linhas de forma a ilustrar as informações relevantes, conforme demonstrado abaixo:



Firewall - Zone Traffic - Linha DMZ oculta

Ao passar o mouse por cima do gráfico, um resumo de todo o tráfego do período é exibido, conforme demonstrado na imagem abaixo:



Firewall - Zone Traffic - Resumo dos resultados

UTM - Firewall – Top User

Em "*Top User*" tem-se um diagrama demonstrando por data quando houve o maior tráfego de rede e uma lista exibindo dez usuários classificados por ordem de uso de *Gigabytes*. Ao passar o mouse por cima do gráfico, o tráfego de rede em *Gigabytes* de um determinado período é exibido, conforme demonstrado na imagem abaixo. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do usuário selecionado.



Firewall – Top User

UTM - Firewall – Top Service

Em "*Top Service*" tem-se um diagrama demonstrando por data quando houve maior tráfego de rede e uma lista exibindo os dez tipos de serviços mais usados, sendo estes classificados por ordem de uso de *Gigabytes*. Ao passar o mouse por cima do gráfico, o tráfego de rede em *Gigabytes* de um determinado período é exibido, conforme demonstrado na imagem abaixo.



Firewall – Top Service

UTM - Firewall – Top Source

Em "*Top Source*" tem-se um diagrama demonstrando por data quando houve maior tráfego de rede e uma lista exibindo as dez maiores fontes de tráfego de rede classificadas por ordem de uso. Ao passar o mouse por cima do gráfico, o tráfego de rede de um determinado período é exibido, conforme demonstrado na imagem abaixo. Por fim, ao clicar em um desses *IPs*, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do *IP* selecionado.



Firewall - Top Source

UTM - Firewall – Top Policies

Em "*Top Policies*" tem-se um diagrama demonstrando por data quando houve maior tráfego de rede e uma lista exibindo os dez tipos de políticas mais usadas, sendo estas classificados por ordem de uso de *Gigabytes*. Ao passar o mouse por cima do gráfico, o tráfego de rede em *Gigabytes* de um determinado período é exibido, conforme demonstrado na imagem abaixo.



Firewall – Top Policies

NGFW - Web Filter

Para acessar os relatórios de web filter, clique no ícone "Analyzer" localizado na lateral esquerda, um menu dropdown será exibido, selecione a opção "We Filter".



Web Filter

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Web Filter - Caixa de seleção de data

O objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- By date: Determina uma data específica;
- By period: Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
- Today: Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
- Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
- This month: Exibe os resultados deste mês;
- Last month: Exibe os resultados do último mês.

Selecione o período desejado:

| | Today 🋗 |
|---------|---------|
| | |
| Period: | |
| Today | ~ |
| | Cancel |

Web Filter - Seleção de Data

| Para fechar esta janela, clique em Cancel | Cancel |] ou, após selecionar a data desejada, clique em Ok [| ОК | 1; |
|--|--------|---|----|----|
|--|--------|---|----|----|





Analyzer - Web Filter

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- []: Serve para dar um zoom;
- []: Tem como função remover o zoom;
- [^①]: Serve para fazer um zoom de seleção;
- 📢]: Serve para mover o gráfico;
- [111]: Reseta o gráfico para a posição inicial;
-]: Permitir baixar este diagrama no formato svg, png ou csv. • [=

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no botão de busca

A seguir, analisaremos em detalhes os componentes de "Web Filter":

- Total Traffic e History;
- Allowed Sites e History;
- Denied Sites e History; Users Total Traffic e Total Hits; •
- ٠ Top Users;
- History Profiles - Total Traffic e Total Hits;
- Top Profiles; •
- ٠ History Categories - Total Traffic e Total Hits;
- Top Categories;
- History Domains Total Traffic e Total Hits; •
- Top Domains;
- History Content Types Total Traffic e Total Hits;
- Top Content Type.

UTM - Web Filter - Allowed Sites e History

O painel "Allowed Sites" exibe um total de páginas que seguindo as políticas tiveram seu acesso autorizado. Logo abaixo, é mostrado o histórico em um gráfico de barras exibindo a quantia de acessos por dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Web Filter - Allowed Sites

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter - Allowed Sites - Resumo do Período

UTM - Web Filter - Denied Sites e History

O painel "Sites Denied" mostra uma somatória de todas as páginas que seguindo as políticas tiveram seu acesso negado. Logo abaixo, é demonstrado o histórico em um gráfico de barras mostrando a quantia de acessos por dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Web Filter - Denied Sites

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter - Denied Sites - Resumo do Período

UTM - Web Filter - History Categories - Total Traffic e Total Hits

Em "History Categories", temos um gráfico que exibe informações especificamente relacionadas as categorias de rede, sua função é demonstrar quando alguma categoria foi aplicada em um dos acessos. Nessa área temos "Total Traffic" onde é exibido o total de tráfego de rede em Gigabytes por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Web Filter - History Categories - Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter - History Categories - Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter - History Categories - Resumo do período

UTM - Web Filter - History Content Types - Total Traffic e Total Hits

Em "Content Type", temos um gráfico cuja função é demonstrar quando algum tipo de conteúdo foi acessado. Nessa área temos "Total Traffic" onde é exibido o total de tráfego de rede em Gigabytes por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Web Filter - History Content Type - Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter - History Content Type - Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter - History Content Type - Resumo do Período

UTM - Web Filter - History Domains - Total Traffic e Total Hits

Em "History Domains", temos um gráfico que exibe informações especificamente relacionadas ao acesso de domínios, sua função é demonstrar quando algum domínio foi acessado. Nessa área temos "Total Traffic" onde é exibido o total de tráfego em Gigabytes por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Web Filter - History Domains - Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter - History Domains - Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter - History Domains - Resumo do Período

UTM - Web Filter - History Profiles - Total Traffic e Total Hits

Em "History Profiles", temos um gráfico que exibe informações especificamente relacionadas aos profiles da rede, sua função é demonstrar quando algum profile foi utilizado em um acesso. Nessa área temos "Total Traffic" onde é exibido o total de tráfego de rede em Gigabytes por dia e "Total Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Web Filter - History Profiles - Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter – History Profiles – Total Hits

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter - History Profiles - Resumo do Período

UTM - Web Filter - Top Categories

Na lista "*Top Categories*", temos uma listagem dos nomes das dez categorias classificadas por ordem de maior quantia de acessos e seu respectivo uso em *Gigabytes*. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da categoria selecionada.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.

| Тор С | ategories | | ٩ |
|-------|----------------------------|-------|---------|
| # | Category | Hits | Traffic |
| 1 | Information Technology | 2.779 | 1.19 GB |
| 2 | Education | 381 | 0.01 GB |
| 3 | Search Engines and Portals | 1.266 | 0.01 GB |
| 4 | Web Hosting | 703 | 0.01 GB |
| 5 | Message Boards and Forums | 37 | 0.00 GB |
| 6 | Uncategorized Sites | 1.596 | 0.00 GB |
| 7 | News and Media | 224 | 0.00 GB |
| 8 | Advertisements | 384 | 0.00 GB |
| 9 | Proxy Avoidance | 21 | 0.00 GB |
| 10 | Alternative Journals | 27 | 0.00 GB |

Web Filter - Top Categories

UTM - Web Filter - Top Content Type

Na lista "Top Content Type", temos uma listagem dos nomes dos dez tipos de conteúdo mais acessados classificados por ordem de maior quantia de acessos e seu respectivo uso em Gigabytes. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito desses tipos de conteúdo.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.

| Тор С | ontent Type | | ٩ |
|-------|-----------------------------------|-------|-----------|
| # | ContentType | Hits | Traffic |
| 1 | application/vnd.ms-cab-compressed | 16 | 611.96 MB |
| 2 | application/octet-stream | 78 | 598.03 MB |
| 3 | video/MP2T | 31 | 14.80 MB |
| 4 | image/jpeg | 260 | 7.56 MB |
| 5 | image/png | 310 | 6.34 MB |
| 6 | application/javascript | 292 | 5.54 MB |
| 7 | text/html | 2.174 | 5.00 MB |
| 8 | text/javascript | 380 | 4.46 MB |
| 9 | application/json | 983 | 2.09 MB |
| 10 | text/plain | 1.874 | 1.37 MB |

Top Content Type

Na lista "Top Content Type", temos uma listagem dos nomes dos dez tipos de conteúdo mais acessados classificados por ordem de maior quantia de acessos e seu respectivo uso em Gigabytes. Por fim, ao clicar em um desses usuários ou IPs, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito desses tipos de conteúdo.

| Top Content Type | | | ٩ |
|------------------|-----------------------------------|-------|-----------|
| # | ContentType | Hits | Traffic |
| 1 | application/vnd.ms-cab-compressed | 16 | 611.96 MB |
| 2 | application/octet-stream | 78 | 598.03 MB |
| 3 | video/MP2T | 31 | 14.80 MB |
| 4 | image/jpeg | 260 | 7.56 MB |
| 5 | image/png | 310 | 6.34 MB |
| 6 | application/javascript | 292 | 5.54 MB |
| 7 | text/html | 2.174 | 5.00 MB |
| 8 | text/javascript | 380 | 4.46 MB |
| 9 | application/json | 983 | 2.09 MB |
| 10 | text/plain | 1.874 | 1.37 MB |

Top Content Type

UTM - Web Filter - Top Domains

Na lista "Top Domains", temos uma listagem dos nomes dos dez domínios classificadas por ordem de maior quantia de acessos e seu respectivo tráfego em Megabytes. Por fim, ao clicar em um desses endereços, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do domínio selecionado.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.

| Top D | omains | | ٩ |
|-------|----------------------------------|------|---------|
| # | Domain | Hits | Traffic |
| 1 | 2.au.download.windowsupdate.com | 29 | 1.10 GB |
| 2 | database.clamav.net | 10 | 0.06 GB |
| 3 | 11.au.download.windowsupdate.com | 1 | 0.03 GB |
| 4 | www.google.com | 920 | 0.01 GB |
| 5 | tpc.googlesyndication.com | 89 | 0.00 GB |
| 6 | s0.2mdn.net | 85 | 0.00 GB |
| 7 | conteudo.imguol.com.br | 51 | 0.00 GB |
| 8 | augmentation.osi.office.net | 4 | 0.00 GB |
| 9 | lpcres.delve.office.com | 32 | 0.00 GB |
| 10 | blogdoiphone.com | 115 | 0.00 GB |

Web Filter - Top Domains

UTM - Web Filter - Top Domains by Time

Na lista "Top Domains by Time", temos uma listagem dos dez domínios mais acessados classificados por ordem de maior de tempo de navegação.

| Top D | omains by time | |
|-------|--|------|
| | Domain | Time |
| 1 | https://edge.microsoft.com | 568 |
| 2 | https://umwatson.avents.data.microsoft.com | 35: |
| 3 | https://www.bing.com | TBs |
| 4 | http://cticll.windowsupdate.com | 240 |
| 5 | http://iLic.lenct.org | 200 |
| 6 | https://login.live.com | 81 |
| 7 | https://slac.update.microsoft.com | |
| 8 | https://mtadge.api.odp.mecrosoft.com | 6 |
| 9 | https://config.edge.skype.com | 6 |
| 10 | https://update.googleapis.com | 8 |

Top Domains by Time

Por fim, ao clicar em um desses domínios ou IPs, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito desses tipos de conteúdo.

| vents | | | | | | | | | |
|-------------------------|--------------------|--------------------------------|-------------------------|---------------------|------------|----------|--------|-------|------|
| Seniore Adhesion | Der, WEN | | | | | | | | |
| web_ster="ehttps://safe | trowsing googles | ps.comic lagypes webliter date | s bidge | | | | 1 | ety E | itte |
| Oute | User | Source | Destination | Device | Senice | logippe | Action | | |
| 2023-01-30 11:10:03 | 215 20 8 | 10.000100.00040 | | attis-calasti | Triffight. | - | ales: | 9 | # |
| E 3023-01-50 11:10/03 | 24 | CT 195,598,105,105,00 | . 100 542253.425.106440 | etta idelauti | 11526 | settine" | - | 9 | |
| E 2023-02-20 LE97624 | 57 | [] 201.108.109.105581. | . 📷 142.211.120.006940 | eth1-dehaitt | intera. | setter. | 100 | 9 | = |
| AS:10;21 05-10-2135 🔄 | 84 | 1 182, 188, 185, 100-01. | | aths - carlants | linga | white | alas. | 9 | - |
| E 2023-01-00 1003713 | 12 | II 192,168,165,102,60, | . ME 342-201.125-42-445 | ette - petault | (1753) | red that | (inv) | 9 | |
| E 2623-01-30 10:37E1 | 17 | []] 102.102.105.00300. | . 📹 349-251-129-425443 | with Q - contaction | inten- | - | - | 9 | - |
| 2823-01-30 L007042 | | 1 297, 1988, 1995, LOT 980, | | etto-celaut | imps | with the | | 3 | - |
| E 2433-01-90 10/0742 | 1 | [1] 192.188.165.100.60 | . 💷 142.238.216.74(44) | 0.0280-0930-0939 | inter | setting | 40.0 | 9 | 10 |
| E 2023-01-30 00:31:23 | 5.2 | [] 303.048.109.102.00 | 218.58.221.10:440 | etti - detautt | Tritps. | nation. | 101 | 2 | - |

Events - Sessions

Clicando em [ou] é possível verificar informações mais detalhadas nesse filtro. Procure a informação de "surfing time" para verificar o tempo de navegação.



Event View 20 " "Event Information" : { "date" 1 "2010-01-01 10100:00" "legtype" : "webfilter" "sessid" : "#509 118762564084012690F65200C48" "src" : "179.30.0.10" "sport" 1 "55627" "geolo_src": "UV" "client_mac" : "00:0c;20:30:bates" "dat" : "09.364.45.8" "dport" ; "BH" "geoip_dst" | "UST "Sevin" : "atal" "devout" : "default" "saneig" : "Lill" "rule_name" 1 "WEB - Iropecan" "protocol" r "tcp" "Flow" : "forward" "web_cat_lang" : "an US" "web_profile" : "Etics de Segurança"-"web_site" : "http://ctidl.windowsummatw.com/wsdowsload/update/v3/statiz/trustede/ae/authenotistl.cam/ all2f2375e3e13b1a* "web_Hethod" 1 "GET" "web_wiwe" : "application/octet-stream" "surfing_tim" : "1" "service" : "http"-"sction" : "allow" 3

Cancol


Para mais informações a respeito do menu Analyzer, cheque esta página.

UTM - Web Filter - Top Profiles

Na lista "Top Profiles", temos uma listagem dos dez profiles mais utilizados classificados por ordem de maior quantia de acessos e seu respectivo uso em Gigabytes. Por fim, ao clicar em um desses perfis, você será redirecionado para *Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do perfil selecionado.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.

| Top Profiles | | | ٩ |
|--------------|------------------------------|-------|-----------|
| # | Name | Hits | Traffic |
| 1 | Content Filtering (Wifi) | 7.894 | 688.31 MB |
| 2 | ByPass SSL (Wifi) | 2.590 | 241.46 MB |
| 3 | Block - filestreamingservice | 377 | 0 Bytes |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Web Filter – Top Profiles

UTM - Web Filter - Top Users

Assim como as outras listas "Top Users", em Web Filter temos uma listagem de dez usuários classificados por ordem de maior quantia de acessos e seu respectivo uso em Gigabytes. Por fim, ao clicar em um desses usuários ou IPs, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do usuário selecionado.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.

| Top Users | | | ٩ |
|-----------|------------------------|-------|----------|
| # | Name | Hits | Traffic |
| 1 | 172.32.250.40 | 762 | 131.6 MB |
| 2 | 172.32.250.99 | 285 | 98.94 MB |
| 3 | doliveira@blockbit.com | 1.696 | 21.28 MB |
| 4 | pisantos@blockbit.com | 243 | 20.21 MB |
| 5 | 172.32.250.46 | 405 | 18.68 MB |
| 6 | 172.32.250.5 | 553 | 7.5 MB |
| 7 | 172.32.250.49 | 1.461 | 7.26 MB |
| 8 | dsousa@blockbit.com | 310 | 5.43 MB |
| 9 | 172.32.250.53 | 67 | 4.83 MB |
| 10 | 172.32.250.47 | 181 | 4.66 MB |

Web Filter – Top Users

UTM - Web Filter - Total Traffic e History

O painel "Total Traffic" demonstra o valor total de tráfego em Megabytes. Logo abaixo, é exibido o histórico em um gráfico de barras demonstrando a quantia de Megabytes trafegados por dia.



Web Filter - Total Traffic



Web Filter - Total Traffic - Resumo do período

UTM - Web Filter - Users - Total Traffic e Total Hits

Logo abaixo dos painéis anteriormente descritos, no lado esquerdo da tela temos o gráfico disposto em "Users", que exibe informações especificamente relacionadas ao consumo de rede por parte dos usuários: Nele temos "Total Traffic" onde é exibido o total de tráfego de rede em Megabytes por dia e "Tot al Hits" que demonstra o total de acessos para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Web Filter – Users – Total Traffic

Ao clicar em cada uma dessas legendas, o gráfico será automaticamente modificado para ilustrar as informações relevantes, conforme demonstrado abaixo:



Web Filter – Traffic – Total Hits



Web Filter - Users - Total Traffic - Resumo do Período

TM - Application Control

Para acessar os relatórios do Application Control, clique no ícone "Analyzer" localizado na lateral esquerda, um menu dropdown será exibido, selecione a opção "Application Control".



Application Control

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Application Control - Caixa de seleção de data

O objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- By date: Determina uma data específica;
- By period: Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
- Today: Exibe resultados especificamente para a data de hoje;
- Yesterday: Exibe resultados especificamente para ontem;
- Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
- Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
- This month: Exibe os resultados deste mês;
- Last month: Exibe os resultados do último mês.

Selecione o período desejado:

| | Today 🋗 |
|---------|-----------|
| | |
| Period: | |
| Today | ~ |
| | Cancel OK |

Seleção de Data

Para fechar esta janela, clique em Cancel] ou, após selecionar a data desejada, clique em Ok [OK];

A tela abaixo será exibida:



A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- []: Serve para dar um zoom;
- [O]: Tem como função remover o zoom;
 [O]: Serve para fazer um zoom de seleção;
- [1]: Serve para mover o gráfico;

- [m]: Reseta o gráfico para a posição inicial;
- [=]: Permitir baixar este diagrama no formato svg, png ou csv.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no botão de busca [].

A seguir, analisaremos em detalhes os componentes de "Application Control":

- Allowed Application;
 Denied Application;

- Defiled Application;
 History;
 Top Allowed Categories;
 Top Denied Categories;
 Top Allowed Applications;
 Top Denied Applications.

UTM - Application Control - Allowed Application

Em "Allowed Application" é exibe um total de aplicações que tiveram seu acesso autorizado.



Application Control – Allowed Application

UTM - Application Control - Denied Application

Já em "Application Denied", mostra-se uma somatória das aplicações que tiveram seu acesso negado.

Denied Applications

Application Control – Denied Application

UTM - Application Control - History

Ao lado direito é possível visualizar o gráfico "*History*" que exibe um histórico de todas as aplicações que tiveram seu acesso permitido e negado, tendo como referências para seus eixos a quantia de acessos em relação com as datas previamente pesquisadas. Os itens da legenda são interativos sendo possível alterar a exibição do gráfico através deles, de modo a fazer o gráfico exibir os aplicativos que foram permitidos e os que foram negados por data. Neste diagrama temos "*Allow*" onde são exibidas as aplicações permitidas e "*Deny*" demonstrando todas as aplicações negadas para cada um dos dias pesquisados.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Application Control – History

É possível selecionar "Allow", para modificar o gráfico e ilustrar as informações relevantes, conforme demonstrado abaixo:



Application Control - History - Allow

Também é possível clicar na legenda "Deny", para modificar o gráfico, conforme demonstrado abaixo:



Application Control – History - Deny



Application Control - History - Resumo do Período

UTM - Application Control - Top Allowed Categories

No diagrama "Top Allowed Categories" temos uma representação visual das 10 categorias permitidas mais aplicadas nos acessos dos usuários, essa sessão serve para, representar de forma pragmática, a quantidade de páginas acessadas que se aplicam a cada uma dessas categorizações.

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Application Control - Top Allowed Categories

UTM - Application Control - Top Denied Categories

No diagrama "Top Denied Categories" temos uma representação visual das 10 categorias recusadas mais utilizadas nos acessos dos usuários, essa sessão serve para, representar de forma pragmática, a quantidade de páginas acessadas que caíram em cada uma dessas categorias de recusa.

Ao passar o mouse por cima do gráfico, um resumo da quantia de categorias é exibido, conforme demonstrado na imagem abaixo.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Application Control - Top Denied Categories

UTM - Application Control - Top Allowed Applications

Em "*Top Allowed Applications*" há um gráfico representando as dez aplicações que tiveram seu acesso autorizado em relação ao período de tempo previamente especificado, abaixo desse gráfico, temos uma listagem dos nomes destas dez aplicações classificadas por ordem de maior quantia de acessos e suas respectivas categorias.

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Application Control - Top Allowed Applications

UTM - Application Control - Top Denied Applications

No painel "Top Denied Applications" temos o exato oposto da sessão anterior: Um gráfico representando as dez aplicações que tiveram seu acesso negado em relação ao período de tempo previamente especificado, abaixo desse gráfico, temos uma listagem dos nomes destas dez aplicações classificadas por ordem de maior quantia de acessos e suas respectivas categorias.

Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Application Control – Top Denied Applications

UTM - Intrusion Prevention

Para acessar os relatórios de Prevenção de Intrusão, clique no ícone "Analysis" localizado na lateral esquerda, um menu dropdown será exibido, selecione a opção "Intrusion Prevention".



Intrusion Prevention

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Intrusion Prevention - Caixa de Seleção

O objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- By date: Determina uma data específica;
- By period: Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
- Today: Exibe resultados especificamente para a data de hoje;
- Yesterday: Exibe resultados especificamente para ontem;
- · Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
- Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
- This month: Exibe os resultados deste mês;
- · Last month: Exibe os resultados do último mês.

Selecione o período desejado:

| | Today 🋗 |
|---------|-----------|
| | |
| Period: | |
| Today | ~ |
| | Cancel OK |

Intrusion Prevention - Seleção de Data

| Para fechar esta janela, clique em Cancel [| Cancel |] ou, após selecionar a data desejada, clique em Ok [| ок |]; |
|--|--------|---|----|----|
|--|--------|---|----|----|

A tela abaixo será exibida:





Analyzer - Intrusion Prevention

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- []: Serve para dar um zoom;
- []: Tem como função remover o zoom;
- []: Serve para fazer um zoom de seleção;
- [. Serve para mover o gráfico;
- [m]: Reseta o gráfico para a posição inicial;
- [=]: Permitir baixar este diagrama no formato svg, png ou csv.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no botão de busca [

A seguir, analisaremos em detalhes os componentes de "Intrusion Prevention":

- Alerted, Blocked e Histórico;
 Alerts by Geolocation;
- Impact High;
- Impact Medium;
 Impact Low;
- Layer 3 Intrusion Protection; •
- ٠ Intrusion Classification;
- Top Source;
- Top Destination.

UTM - Intrusion Prevention - Alerted, Blocked e Histórico

O painel "Alerted" exibe um total de alertas de intrusão.

Já em "Blocked", é exibido um número totalizando as tentativas de intrusão bloqueadas.

Logo abaixo, é mostrado um resumo dos alertas e bloqueios em um gráfico de linhas exibindo a quantidade de eventos relacionados a intrusão dentro do período de tempo previamente selecionado. Ao selecionar uma das legendas ("*Alerted*" ou "*Blocked*") no topo do gráfico, é possível determinar que apenas uma destas sejam exibidas no gráfico.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Alerted, Blocked e Histórico

É possível selecionar "Allow", para modificar o gráfico e ilustrar as informações relevantes, conforme demonstrado abaixo:



Alerted, Blocked e Histórico - Allow





Alerted, Blocked e Histórico - Deny



Alerted, Blocked e Histórico - Resumo do Período

UTM - Intrusion Prevention - Alerts by Geolocation

Em "Alerts by Geolocation" é exibida a origem das intrusões por geolocalização, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários. Ao passar o mouse por cima dos países um número total de alertas é exibido, ao fazer o mesmo com a legenda é possível visualizar uma média, além disso, o país referente a esse valor é destacado no mapa.



Alerts by Geolocation

UTM - Intrusion Prevention - Impact - High

Em "Impact - High" temos um gráfico de rosca exibindo a porcentagem de ameaças de intrusão de alto impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de alto impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Impact - High



Intrusion Prevention - Impact - High - Resumo do Período

UTM - Intrusion Prevention - Impact - Medium

Em "Impact - Medium" temos um gráfico de rosca exibindo a porcentagem de ameaças de intrusão de médio impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de médio impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Impact - Medium



Intrusion Prevention - Impact - Medium - Resumo do Período

UTM - Intrusion Prevention - Impact - Low

Em "Impact - Low" temos um gráfico de rosca exibindo a porcentagem de ameaças de intrusão de baixo impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de baixo impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Impact - Low



Intrusion Prevention - Impact - Low - Resumo do Período
UTM - Intrusion Prevention - Layer 3 Intrusion Protection

Em "Layer 3 Intrusion Protection" temos um gráfico exibindo as dez categorias de alertas de intrusão mais detectadas na camada 3 do IPS (Intrusion Prevention System). Ao clicar em um dos IPs ou uma das categorias, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do item selecionado. Logo abaixo do gráfico, temos uma listagem dos dez IPs e as categorias mais acessadas em ordem pelo número de acessos.



Layer 3 Intrusion Prevention

Ao passar o mouse por cima do gráfico, ele exibirá um número com a quantia de alertas de intrusão, conforme demonstrado na imagem abaixo:



Layer 3 Intrusion Prevention - Quantia de alertas de intrusão

Ao passar o mouse sobre a legenda, o gráfico será destacado, conforme demonstrado abaixo:



Layer 3 Intrusion Prevention - Gráfico destacado

UTM - Intrusion Prevention - Intrusion Classification

Em "Intrusion Classification" temos um gráfico representando as dez classes de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado. Abaixo do gráfico, temos uma listagem dos nomes das dez classificações por ordem de maior quantia de acessos.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Intrusion Classification

Ao passar o mouse sobre o gráfico, ele evidenciará a data e o número de acessos da classe mais alta deste dia em específico



Intrusion Classification - Resumo das classes

UTM - Intrusion Prevention - Top Source

Em "*Top Source*" é exibido um gráfico de linha representando as dez fontes de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os *IPs* destas mesmas dez fontes previamente citadas sendo estas classificadas por ordem de maior quantia de acessos. Ao clicar em um dos *IPs* ou uma das categorias, você será redirecionado para *Events* usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da categoria selecionado

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Top Source

Ao passar o mouse sobre o gráfico, ele evidenciará a data e o número de acessos da classe mais alta deste dia em específico:



Top Source - Resumo

UTM - Intrusion Prevention - Top Destination

Em "*Top Destination*" tem-se um gráfico de linha exibindo os dez destinos de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os *IPs* dos dez destinos de maior quantia de acessos. Ao clicar em um dos *IPs* ou uma das categorias, você será redirecionado para *Ev ents* usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do item selecionado.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Top Destination

Ao passar o mouse sobre o gráfico, ele evidenciará a data e o número de acessos da classe mais alta deste dia em específico:



Top Destination - Resumo de Acessos

UTM - Threat Protection

Para acessar os relatórios de Proteção de Ameaças, clique no ícone "Analysis" localizado na lateral esquerda, um menu dropdown será exibido, selecione a opção "Threat Protection".



Threat Protection

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:



Threat Protection - Caixa de Seleção

O objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- By date: Determina uma data específica;
- By period: Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
- Today: Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
- Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
- This month: Exibe os resultados deste mês;
- Last month: Exibe os resultados do último mês.

Selecione o período desejado:

| | Today 🋗 |
|---------|-----------|
| | |
| Period: | |
| Today | ~ |
| | Cancel OK |

Threat Protection - Seleção de Data

| Para fechar esta janela, clique em Cancel | Cancel |] ou, após selecionar a data desejada, clique em Ok [| ок |]; |
|---|--------|---|----|----|
| Tala lechal esta jaliela, cique elli Gancer | | Jou, apos selecionar a data desejada, cirque em Or | | , |

A tela abaixo será exibida:





Analyzer - Threat Protection

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- []: Serve para dar um zoom;
- []: Tem como função remover o zoom;
- [] Serve para fazer um zoom de seleção;
- [1]: Serve para mover o gráfico;
- [11]: Reseta o gráfico para a posição inicial;
- [=]: Permitir baixar este diagrama no formato svg, png ou csv.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no botão de busca [

A seguir, analisaremos em detalhes os componentes de "Threat Protection":

- Threats e History;
- Malwares e History;
- Geolocation;
- Impact High;
 Impact Medium;
- Impact Medium;
 Impact Low;
 Malicious IP Classification;
 Top Threat Types;
 Top Users by Threats;
 Top Users by Malware;
 Top Melware;

- Top Malware;
- Top Infected Domains;
- Top Source;
- Top Destination.

UTM - Threat Protection - Threats e History

O painel "Threats" exibe um total de ameaças detectadas. Logo abaixo, é exibido o histórico em um gráfico de linhas demonstrando a quantia de ameaças detectadas por dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Threat Protection - Threats e History

Ao passar o mouse por cima do gráfico, um resumo das ameaças do período é exibido, conforme demonstrado na imagem abaixo:



Threat Protection - History - Resumo das ameaças

UTM - Threat Protection - Malwares e History

Já em "Malwares", é exibido um número totalizando a quantia de malwares detectados. Logo abaixo, é exibido o histórico em um gráfico de barras demonstrando a quantia de ameaças detectadas por dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Threat Protection - Malware e History

UTM - Threat Protection - Geolocation

Em "Geolocation" é exibida a origem das ameaças por geolocalização, o mapa global demonstra através de uma legenda colorida o nível de risco. Ao passar o mouse por cima dos países um número total de ameaças é exibido, ao fazer o mesmo com a legenda é possível visualizar uma média, além disso, o país referente a esse valor é destacado no mapa.



Threat Protection – Geolocation

UTM - Threat Protection - Impact - High

Em "Impact - High" temos um gráfico de rosca exibindo a porcentagem de ameaças de alto impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de alto impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection – Impact High

UTM - Threat Protection - Impact - Medium

Em "Impact - Medium" temos um gráfico de rosca exibindo a porcentagem de ameaças de médio impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de médio impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection – Impact Medium

UTM - Threat Protection - Impact - Low

Em "Impact - Low" temos um gráfico de rosca exibindo a porcentagem de ameaças de baixo impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida com as 10 ameaças de baixo impacto mais recorrentes, exibindo seu nome e listando-as por quantidade de recorrências.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection – Impact Low

UTM - Threat Protection - Malicious IP Classification

Em "Malicious IP Classification" temos um gráfico de rosca exibindo as dez categorias de alertas de IP Malicioso mais detectadas na rede, ao passar o mouse sobre cada parte do gráfico ou seu texto correspondente, ele o destacará e exibirá um número com a quantia de acessos a essa categoria de IP e sua porcentagem correspondente em relação com as outras categorias. Logo abaixo do gráfico, temos uma listagem dos dez IPs que mais acessaram essas categorias ordenados por número de acessos.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection - Malicious IP Classification

Ao passar o mouse por cima do gráfico, ele exibirá um número com a quantia de IPs maliciosos, conforme demonstrado na imagem abaixo:



Threat Protection - Malicious IP Classification - Resumo

Ao passar o mouse sobre a legenda, o gráfico será destacado, conforme demonstrado abaixo:



Threat Protection - Malicious IP Classification - Resumo

UTM - Threat Protection - Top Threat Types

Em "Top Threat Types" é exibido um gráfico de barras representando os tipos de ameaça mais recorrentes em relação a quantia de vezes que elas foram detectadas

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



Threat Protection - Top Threat Types

Ao passar o mouse sobre o gráfico ele mostrará a quantia exata de detecções:



Threat Protection – Top Threat Types - Resumo

UTM - Threat Protection - Top Users by Threats

Em "*Top Users by Threats*" temos um gráfico de linha exibindo a quantia de ameaças por dia, ao passar o mouse sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de ameaças do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez usuários que mais foram afetados por essas ameaças ordenados por quantia de acessos.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection – Top Users by Threats

Ao passar o mouse por cima do gráfico, é exibido um resumo dos resultados dentro do período selecionado, conforme demonstrado na imagem abaixo:



Threat Protection - Top Users by Threats - Resumo

UTM - Threat Protection - Top Users by Malware

Em "*Top Users by Malware*" temos um gráfico de linha exibindo a quantia de alerta de *malware* por dia, ao passar o *mouse* sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de ameaças do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez usuários que mais foram afetados por *malware* ordenados por quantia de detecções. Logo abaixo do gráfico, temos uma listagem dos dez usuários que mais foram afetados por essas ameaças ordenados por quantia de acessos. Por fim, ao clicar em um desses usuários ou *IPs*, você será redirecionado para Events us ando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do usuário selecionado.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.

| Top Users by Malwares | | ٩ |
|-----------------------|---------|------|
| 5 | | |
| 4 | | |
| 3 | | |
| 2 | | |
| 1 | | |
| 0 | | |
| 0 | | 10 |
| # Malware | User | Hits |
| | | |
| | | |
| | | |
| | No Data | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Threat Protection - Top Users by Malware

UTM - Threat Protection - Top Malwares

Em "*Top Malwares*" temos um gráfico de linha exibindo a quantidade de *malwares* detectados por dia, ao passar o mouse sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantidade de detecções do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez *malwares* mais recorrentes ordenados por quantidade de detecções.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection – Top Malwares

UTM - Threat Protection - Top Infected Domains

Em "*Top Infected Domains*" temos um gráfico de linha exibindo a quantia de domínios infectados detectados por dia, ao passar o *mouse* sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de detecções do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez domínios mais recorrentes ordenados por quantia de detecções.

Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection - Top Infected Sites

UTM - Threat Protection - Top Source

Em "*Top Source*" é exibido um gráfico de linha representando as dez fontes de ameaça mais recorrentes em relação ao período de tempo previamente especificado, ao passar o *mouse* sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os *IPs* destas mesmas dez fontes previamente citadas sendo estas classificadas por ordem de maior quantia de acessos. Ao clicar em um dos IPs ou uma das categorias, você será redirecionado para *Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da fonte de ameaça selecionada.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection – Top Source

Ao passar o mouse por cima do gráfico, é exibido um resumo dos resultados dentro do período selecionado, conforme demonstrado na imagem abaixo:



Threat Protection - Top Source - Resumo

UTM - Threat Protection - Top Destination

Em "*Top Destination*" é exibido um gráfico representando os dez destinos de ameaça mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista exibindo os *IPs* destes mesmos dez destinos previamente citadas sendo estes classificados por ordem de maior quantia de acessos. Ao clicar em um dos *IPs*, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito da fonte de ameaça selecionada.

Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Threat Protection – Top Destination

Ao passar o mouse por cima do gráfico, é exibido um resumo dos resultados dentro do período selecionado, conforme demonstrado na imagem abaixo:


Threat Protection - Top Destination - Resumo

UTM - User Behavior

Para acessar os relatórios disponíveis em "User Behavior", clique no ícone "Analysis" localizado na lateral esquerda, um menu dropdown será exibido, selecione a opção "User Behavior".



User Behavior

O relatório "User Behavior" é um resumo do comportamento de determinado usuário de um dispositivo, informando o IP do usuário, hostname da máquina, o Sistema Operacional que o usuário utiliza e uma classificação geral das ameaças (dispostas em "top 10"), sendo possível extrair um relatório dentro de um período de tempo específico. Os relatórios dispostos são um resumo das informações já anteriormente citadas, porém sendo aplicadas específicamente a esse usuário.

Para gerar um novo relatório, será necessário selecionar o *device* desejado, depois o usuário que se deseja analisar e por fim, determinar uma data. Feita a seleção desses três dados, os relatórios serão gerados.

Localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:

| today 🛗 | Select a User | ~ |
|---------------|--------------------|---|
| User Behavior | - Caixa de Seleção | |

Na caixa de seleção "Select a User" estarão listados todos os usuários do device previamente selecionado, selecione o usuário desejado.



Selecionando o usuário.

Por fim, a caixa de seleção de datas tem como objetivo permitir uma filtragem mais precisa de resultados, as opções possíveis são:

- By date: Determina uma data específica;
 By period: Exibe resultados de uma data inicial ("*Start date*") até uma data final ("*End date*");
- Today: Exibe resultados especificamente para a data de hoje;
 Yesterday: Exibe resultados especificamente para ontem;
- Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
- Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
- This month: Exibe os resultados deste mês;
- Last month: Exibe os resultados do último mês.

Selecione o período desejado:

| | | Today | # | |
|--|----------------------------------|--------------------|-------------------|----|
| | Period: Today | Cancel | ~ | |
| | Seleção de | Data | | |
| Para fechar esta janela, clique em <i>Cancel</i> [| Cancel] ou, após selecionar a d | ata desejada, cliq | ue em Ok [|)K |

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

• [+]: Serve para dar um zoom;

1:

- [^O]: Tem como função remover o zoom;
 [^O]: Serve para fazer um zoom de seleção;
 [^O]: Serve para mover o gráfico;
- [1]: Reseta o gráfico para a posição inicial;
- [=]: Permitir baixar este diagrama no formato *svg*, *png* ou *csv*.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no botão de busca [

A seguir, analisaremos cada um desses relatórios em detalhe:

- History;Analysis Panel;Geolocation Information.

UTM - User Behavior - History

Em "*History*" um gráfico de barras verticais é exibido demonstrando o consumo de tráfego em *Megabytes* em relação com os dias pré-selecionados, a flecha no meio do gráfico representa a média de consumo dos usuários em geral. Ao passar o mouse por cima de uma das colunas do gráfico é exibido a quantia exata de tráfego em *Megabytes* para cada dia.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



293

UTM - User Behavior - Analysis Panel

Em "Analysis Panel" temos um resumo de várias informações citadas nos relatórios previamente analisados, porém desta vez, aplicados especificamente ao usuário em questão.

Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.

| | Netwo | ork Traffic |
|---------------------------------|--|--|
| Tot | al Traffic | |
| (((- | 2.37 GB | |
| p S | Services | ٩ |
| # | Services | Traffic |
| 1 | https | 1.08 GB |
| 2 | admin | 548.79 MB |
| 3 | ssh | 548.9 MB |
| 4 | http | 4.06 MB |
| | | |
| 5 | rdesktop | 221.56 MB |
| 5 pp S | ource | 221.56 MB |
| 5 •p S # | Source | 221.56 MB |
| 5 p S # 1 | source Source 172.32.250.20 | 221.56 MB |
| 5 p S # 1 2 | rdesktop Source Source 172.32.250.20 | 221.56 MB 221.56 MB Traffic 48.74 KB 123 Bytes |
| 5 # 1 3 | rdesktop Source Source 172.32.250.20 172.16.13.246 172.16.102.130 | 221.56 MB Traffic 48.74 KB 123 Bytes 81 Bytes |
| 5 # 1 2 3 4 | rdesktop Source Source 172.32.250.20 172.16.13.246 172.16.102.130 192.168.254.252 | 221.56 MB Traffic 48.74 KB 123 Bytes 81 Bytes 43 Bytes |
| 5 # 1 2 3 4 5 | rdesktop Source Source 172.32.250.20 172.16.13.246 172.16.102.130 192.168.254.252 172.16.12.27 | 221.56 MB 221.56 MB Traffic 48.74 KB 123 Bytes 81 Bytes 43 Bytes 30 Bytes |

| 'P L | Destination | ٩ |
|---|---|---|
| # | Destination | Hits |
| 1 | [] 172.16.13.245 | 2.916 |
| 2 | [] 172.16.13.246 | 2.502 |
| 3 | [] 172.16.12.171 | 1.063 |
| 4 | [] 172.31.0.50 | 558 |
| 5 | 172.16.13.57 | 485 |
| | | |
| olic | Policy Usa y Tags | ge |
| elic: | Policy Usa y Tags | ge |
| olic p F | Policy Usa y Tags SSL Profiles | ge |
| p F | Policy Usa y Tags SSL Profiles Policies | ge Q Hits |
| elic; p F # | Policy Usa y Tags SSL Profiles Policies Default (Allow) (Wifi) | ge Q Hits 24.647 |
| p F # 1 | Policy Usa y Tags SSL Profiles Policies Default (Allow) (Wifi) Default (Allow) (Wifi) (Copy) | ge Hits 24.647 12.246 |
| ep F # 1 2 3 | Policy Usa y Tags SSL Profiles Policies Default (Allow) (Wifi) Default (Allow) (Wifi) (Copy) SMB | ge Hits 24.647 12.246 5.412 |
| olic; p F # 1 2 3 4 | Policy Usa y Tags SSL Profiles Policies Default (Allow) (Wifi) Default (Allow) (Wifi) (Copy) SMB FORWARD LOCAL | ge Hits 24.647 12.246 5.412 3.962 |
| lic: p F # 1 2 3 4 5 | Policy Usa sst sst Profiles Policies Default (Allow) (Wifi) Default (Allow) (Wifi) (Copy) SMB FORWARD LOCAL Content Filtering (Wifi) | ge Hits 24.647 12.246 5.412 3.962 3.138 |

| | Application Usage | |
|------------------|--|-------|
| Tot | al Application • 1.74 KB | |
| p A | pplications | ٩ |
| # | Applications | Hits |
| 1 | CDN - Content Delivery Network | 1.043 |
| 2 | Microsoft Update | 547 |
| 3 | HTTP | 50 |
| 4 | Google API SSL | 48 |
| ~ | | |
| 5 | MSN | 18 |
| 5 | MSN | 18 |
| 5 | Web Usage | 18 |
| 5 Tot | Web Usage al Traffic > 0 | 18 |
| 5 Tot Allo | MSN Web Usage al Traffic > 0 owed Sites > 0 | 18 |

| # | Categories | Hit |
|--------------------------|---|-----------------------|
| " | Information Technology | 1.62 |
| 2 | Search Engines and Portals | 76 |
| 3 | Freeware and Software Download | 52 |
| 4 | Business and Economy | 14 |
| 5 | Web Hosting | 9 |
| | | |
| op D | estination | C |
| pp [| Pestination | G |
| ор D # 1 | Pestination Ip 2.23.98.145 | G Hit 47 |
| pp [# 1 2 | Destination | Hit 47 |
| рр [# 1 2 3 | Destination Ip 2.23.98.145 201.0.217.42 13.107.4.50 | Hit 47 44 27 |

THREAT PROTECTION

111

Total Threats

奈 1,198

5 191.252.51.215







User Behavior - Analysis Panel

UTM - User Behavior - Analysis Panel - Network Traffic

Abaixo de "Network Traffic" temos:

"Total Traffic", exibindo o total de tráfego do usuário em Gigabytes, em "Top Services" é exibida uma listagem com os 10 serviços mais utilizados pelo usuário em questão, "Top source" demonstra as maiores fontes de acesso do utilizador e "Top Destination" uma listagem de IPs dos destinos mais acessados pelo usuário.

| Network Traffic |
|-----------------|
| Total Traffic |
| |

Q

| 1 | | |
|---|----------|-----------|
| # | Services | Traffic |
| 1 | https | 1.08 GB |
| 2 | admin | 548.79 MB |
| 3 | ssh | 548.9 MB |
| 4 | http | 4.06 MB |
| 5 | rdesktop | 221.56 MB |

Top Services

| Top S | ource | 2 | ٩ |
|-------|-------|-----------------|-----------|
| # | Sou | irce | Traffic |
| 1 | | 172.32.250.20 | 48.74 KB |
| 2 | | 172.16.13.246 | 123 Bytes |
| 3 | | 172.16.102.130 | 81 Bytes |
| 4 | | 192.168.254.252 | 43 Bytes |
| 5 | | 172.16.12.27 | 30 Bytes |
| | | | |

| Тор D | estination | | Q |
|-------|------------|----------|-------|
| # | Destinatio | n | Hits |
| 1 | []] 172.16 | 6.13.245 | 2.916 |
| 2 | []] 172.16 | 6.13.246 | 2.502 |
| 3 | []] 172.16 | 6.12.171 | 1.063 |
| 4 | []] 172.31 | 1.0.50 | 558 |
| 5 | []] 172.16 | 6.13.57 | 485 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

User Behavior - Analysis Panel - Network Traffic

UTM - User Behavior - Analysis Panel - Policy Usage

Em "Policy Usage" temos:

"Policy Tags" que demonstra quais as Tags de política que foram mais aplicadas a esse usuário, em "Top Policies" temos as políticas mais aplicadas a esse usuário em específico.

| Policy Usage | | | | | |
|--------------|-------------------------------|--------|--|--|--|
| Policy | Policy Tags | | | | |
| w | w SSL | | | | |
| Тор Р | rofiles | ٩ | | | |
| # | Policies | Hits | | | |
| 1 | Default (Allow) (Wifi) | 24.647 | | | |
| 2 | Default (Allow) (Wifi) (Copy) | 12.246 | | | |
| 3 | SMB | 5.412 | | | |
| 4 | FORWARD LOCAL | 3.962 | | | |
| 5 | Content Filtering (Wifi) | 3.138 | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Analysis Panel - Policy Usage

UTM - User Behavior - Analysis Panel - Application Usage

Em "Application Usage" temos:

"Total Applications" menciona o total de aplicações utilizadas pelo usuário e "Total Application" que serve para demonstrar as aplicações mais utilizadas pelo usuário e a quantia de acessos efetuados a estas mesmas.

| Application Usage | | |
|-------------------|--------------------------------|-------|
| Tot | al Application • 1.74 KB | |
| Тор А | pplications | ٩ |
| # | Applications | Hits |
| 1 | CDN - Content Delivery Network | 1.043 |
| 2 | Microsoft Update | 547 |
| 3 | НТТР | 50 |
| 4 | Google API SSL | 48 |
| 5 | MSN | 18 |
| | | |

Analysis Panel - Application Usage

UTM - User Behavior - Analysis Panel - Web Usage

Em "Web Usage" temos:

"Total Traffic" demonstrando um total do tráfego de rede do usuário, "Sites Allowed" mostrando o total de acessos a sites permitidos efetuados pelo usuário, "Sites Denied" mostrando o total de acessos a sites recusados efetuados pelo usuário, "Top Categories" uma lista de acessos do usuário por categoria e por fim, em "Top destination" uma lista de acessos do usuário por destino exibindo o IP e quantia de acessos a esse mesmo.

| Web Usage | |
|---|--|
| Total Traffic | |
| | |
| Allowed Sites | |
| Denied Sites | |
| | |
| Top Categories | ٩ |
| Top Categories # Categories | ۹ Hits |
| Top Categories # Categories 1 Information Technology | م Hits 1.628 |
| Top Categories # Categories 1 Information Technology 2 Search Engines and Portals | ۲ Hits 1.628 763 |
| Top Categories#Categories1Information Technology2Search Engines and Portals3Freeware and Software Download | ۲ Hits 1.628 763 527 |
| Top Categories#Categories1Information Technology2Search Engines and Portals3Freeware and Software Download4Business and Economy | Q Hits 1.628 763 527 145 |

| Тор 🛛 | Destination | ٩ |
|-------|--------------|------|
| # | lp | Hits |
| 1 | 2.23.98.145 | 476 |
| 2 | 201.0.217.42 | 449 |
| 3 | 13.107.4.50 | 273 |
| | | |



Analysis Panel - Web Usage

UTM - User Behavior - Analysis Panel - Threat Protection

Em "Threat Protection" temos:

"Total Threats" exibindo o total de ameaças, "Total Malwares" exibe o número total de malwares detectados nesse usuário, no gráfico "Impacts" são exibidos os níveis de impactos das ameaças previamente citadas, "Malicious IP Classification" exibe um gráfico demonstrando um resumo da classificação dos IPs mal-intencionados acessados pelo usuário, na listagem "Top Threats" são exibidas as 5 ameaças mais recorrentes a esse usuário e a quantia de acessos feitos e em "Top Malware" é exibida uma lista com os 5 malwares mais detectados no usuário em questão.



| 1 | Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1) | 308 |
|---|--|-----|
| 2 | TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5) | 298 |
| 3 | TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4) | 275 |
| 4 | PUA-P2P BitTorrent transfer | 176 |
| 5 | PUA-P2P Bittorrent uTP peer request | 88 |

| op Malwares | C. C |
|-------------|--|
| # Malwares | Hit |
| 6 | <u>à</u> |
| No Da | ita |
| | |
| | |

Analysis Panel - Threat Protection

UTM - User Behavior - Analysis Panel - Intrusion Prevention

Em "Intrusion Prevention" temos:

"Total Alerts" exibindo o total de alertas referentes a esse usuário, em "Impacts" temos os níveis de impacto dos alertas previamente citados, "Intrusion Protection" exibe um gráfico de rosca onde é possível de se ver os tipos de invasão detectados pelo sistema e por fim, em "Top Alerts" temos uma listagem dos 5 alertas referentes a esse usuário e quantas vezes eles ocorreram.



| | Unreachable host Unreachable | |
|---|---|-------|
| 4 | PROTOCOL-ICMP Destination Unreachable Host Unreachable | 8.511 |
| 5 | GPL ICMP_INFO PING | 2.081 |
| | | |
| | | |
| | | |
| | Analysis Panel - Intrusion Prevention | |

UTM - User Behavior - Geolocation Information

Em "Hits by Geolocation" é exibido o destino das conexões desse usuário em específico, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários para cada país.



User Behavior - Geolocation

Ao passar o mouse por cima dos países um número total de acessos é exibido, ao fazer o mesmo com a legenda é possível visualizar uma média, além disso, o país referente a esse valor é destacado no mapa.



User Behavior - Geolocation - Resumo de acessos em um país

UTM - VPN

Para acessar os relatórios de VPN, clique no ícone "Analyzer" localizado na lateral esquerda, um menu dropdown será exibido, selecione a opção "VPN".





A função principal deste recurso é fornecer informações sólidas sobre as VPNs da rede, possibilitando ter uma visão holística da estrutura, facilitando um gerenciamento integrado e resposta rápida em caso de alguma eventualidade. Neste painel temos os seguintes relatórios estatísticos das VPN:

- Tráfego nas VPN;
- · Consumo dos usuários remotos;
- 100 VPNs Site-to-site mais usadas;
- 100 usuários remotos mais ativos.

Além disso também são exibidas as informações gerais de tráfego das Top 100 (cem) VPNs e Usuários Remotos:

- Identificação da Conexão VPN ou Usuário;
- Tipo de protocolo de segurança utilizado;
- Consumo de Banda (Bandwidth);
- Tempo ativo (Em horas em minutos);
- Quantidade de Pacotes;
- Tráfego.

Para gerar um relatório, localize a caixa de seleção que está posicionada no topo direito da tela, conforme ilustrado a seguir:

today 🋗

VPN - Caixa de seleção de data

O objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

- By date: Determina uma data específica;
- By period: Exibe resultados de uma data inicial ("Start date") até uma data final ("End date");
- Today: Exibe resultados especificamente para a data de hoje;
- Yesterday: Exibe resultados especificamente para ontem;
- Last 7 days: Filtra especificamente os resultados dos últimos 7 dias;
- Last 30 days: Filtra especificamente os resultados dos últimos 30 dias;
- This month: Exibe os resultados deste mês;

• Last month: Exibe os resultados do último mês.

Selecione o período desejado:

| | Today 🛗 |
|---------|-----------|
| Period: | |
| Тодау | ~ |
| | Cancel OK |

VPN - Seleção de Data

| | Cancel | | OK | |
|---|---------|---|----|----|
| Para fechar esta janela, clique em Cancel | contect |] ou, após selecionar a data desejada, clique em Ok | |]; |

| PN | | | | | | | | | | lide 2 | 5 |
|---|---|--|--|-------------------|----------|---|----------------|---------------------|-----------------------------------|----------------------|--|
| 100.000 | | | | | | Sentence - | | | | | |
| 112 (0) 111 (0) 112 (0) 112 (0) 112 (0) 112 (0) 112 (0) | | | 1 | 001 | C.A.I | | | | 11. | | |
| (Red) | Della Meridian | | | 176 (66-706-00 | A BAR DA | | ilian dan jak | rin parise de 11,18 | -10.10010-100 | 11-10-10-2 | 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 |
| (11-0) (31)-5 (01) | Dece sumon | 10 M (N / M / M / M / M / M / M / M / M / M / | 10-10-10-10 | (Ta (No. 100-10 | | f mein st | in de line de | C 1000 - 20 10 10 | -10.1 (0.1 (0.1 (0.1 | 11-10-10-2 | nd'n 24 de |
| tons a mo | Dece Burners Constantion Type | Bandadato | Duality | Packages | Talle Co | A Second | | nin paula de 19,18 | ela (p. (d. 14) | faile and | ndis In in |
| land market land land land land | ana anna | Anna an | Contest | Autogra | | Approximate Approx | 7,00 | Danie (Mr. | ela specia da Locales Mil | Parlages Tatlages | ni n ta in |
| tere i see i see i see | nandanı Anel | and a second sec | Contraction of the last of the | Packages (1) | 14. | Spinster Spi | Type Type | Cambride de 1114 | rin on its in London | Parlages Textures | 1.12 (1.12) |
| Appendix Second | non honor Tope Come honor Come honor Come honor Come honor | Brokeniko | Dootee = | Pacinges = | 14 | National Control of Co | Type 1000 o | Dents (Mr. | rin (polite in Ensities (s) | Parlages Barbages | |

Analyzer - VPN

A maioria dos gráficos desta aba possui um menu de navegação e uma barra de busca.

O menu de navegação possui os seguintes botões:

- [+]: Serve para dar um zoom;
 [-]: Tem como função remover o zoom;
 [-]: Serve para fazer um zoom de seleção;
 [-]: Serve para mover o gráfico;
- [m]: Reseta o gráfico para a posição inicial;
- [=]: Permitir baixar este diagrama no formato svg, png ou csv.

A barra de busca permite pesquisar um item específico e modificar os diagramas de acordo com os resultados da pesquisa.

Para efetuar uma pesquisa, digite um termo na barra de busca e clique no botão de busca [

A seguir, iremos analisar cada painel desta página.

- Traffic Usage;
 Remote User;
 Top Site-to-Site;
 Top Remote User.

UTM - VPN - Traffic Usage

Este painel tem como função exibir o consumo do tráfego nas VPNs IPSEC e SSL. O eixo vertical é referente ao consumo em Megabytes e o horizontal se refere ao período selecionado (podendo ser horas ou dias).



Analyzer - VPN - Traffic usage

Ao passar o mouse por cima do gráfico, um resumo de todo o tráfego do período é exibido, conforme demonstrado na imagem abaixo:



Analyzer - VPN - Traffic usage - Detalhes

UTM - VPN - Remote User

Este painel tem como função exibir informações a respeito dos usuários remotos. O eixo vertical é referente a quantia de usuários remotos e o horizontal se refere ao período selecionado (podendo ser horas ou dias).



Analyzer - VPN - Remote user

Ao passar o mouse por cima do gráfico, um resumo de todos os usuários ativos no período é exibido, conforme demonstrado na imagem abaixo:



Analyzer - VPN - Remote user - Detalhes

UTM - VPN - Top Site-to-Site Connections

O painel "Top Site-to-Site Connections" tem como função exibir as informações estatísticas referentes aos túneis VPNs Site-to-Site mais utilizadas na rede.

| | Name | Туре | Bandwidth | Duration | Packages | Traffi |
|---|------------|---------|-----------|----------|----------|-----------|
| 1 | user_bb2 | [IPSEC] | 61 | 5m | 9K | 3.49 MB |
| 2 | VPN1 | 551 | | -8m | 814 | 116.26 KB |
| 3 | teste_qa2 | IPSEC | | 4m | 2 | 722 Bytes |
| 4 | VPN Site t | IPSEC | | 8m | 0 | 10 |

Analyzer – VPN - Top Site-to-Site Connections

Para que o painel "*Top Site-to-Site*" exiba as informações referentes a uma *VPN* específica, defina o nome dela na barra de busca e clique em **Search** [o sistema irá filtrar e exibir os relatórios relevantes de acordo com o que foi buscado.

| | andwidth Duration Packages Traffic |
|----------------------|------------------------------------|
| user_bb2 IPSEC 5m 9K | 5m 9K 3.49 MB |

Analyzer - VPN - Top Site-to-Site Connections Search

O relatório é dividido pelas colunas abaixo:

- Name: Nome do túnel VPN;
- Type: Exibe o tipo de protocolo utilizado na VPN;
- Bandwidth: Mostra a largura de banda;
- Duration: Exibe durante quanto tempo corrido a conexão com a VPN está estabelecida. É exibido em horas e minutos;
- Packages: Número de pacotes trafegados. É exibido em Kilobytes;
- Traffic: Exibe o tráfego atual da VPN. É exibido em Megabytes.

UTM - VPN - Top Remote User

O painel "Top Remote User" tem como função exibir as informações estatísticas referentes aos usuários remotos.

| Top Re | emote Users | | | | | Q |
|--------|-------------|------|-----------|----------|----------|---------|
| # | Name | Туре | Bandwidth | Duration | Packages | Traffic |
| 1 | 1 | SSL | | 9h 26m | 58 | 6.34 KB |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Analyzer - VPN - Top Remote User

Para que o painel "*Top Remote User*" exiba as informações referentes a um usuário remoto específico, defina o nome dele na barra de busca e clique em **Search** [] o sistema irá filtrar e exibir os relatórios relevantes de acordo com o que foi buscado.
| Top Re | emote Users | | | 1 | | Q |
|--------|-------------|------|-----------|----------|----------|---------|
| # | Name | Туре | Bandwidth | Duration | Packages | Traffic |
| 1 | 1 | SSL | | 9h 26m | 58 | 6.34 KB |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Analyzer - VPN - Top Remote User Search

O relatório é dividido pelas colunas abaixo:

- Name: Nome do usuário remoto;
 Type: Exibe o tipo de protocolo utilizado na VPN;
 Bandwidth: Mostra a largura de banda;
 Duration: Exibe durante quanto tempo corrido a conexão com a VPN está estabelecida. É exibido em horas e minutos;
 Packages: Número de pacotes trafegados. É exibido em *Kilobytes*;
 Traffic: Exibe o tráfego atual da VPN. É exibido em *Megabytes*.

UTM - POLICIES

Todos os recursos de gerenciamento dos serviços UTM, 'Filtro de conteúdo *Web*", 'Filtro e controle de aplicativos da *WEB* 2", 'Interceptação *SSL*", *"Deep Inspection"*, 'Roteamento", 'Controle *QoS (Traffic Shaping)*", 'Garantia e prioridade de tráfego", "Controle de Cota de tráfego e tempo", 'Controle de tamanho de arquivos", 'Filtros de cabeçalho e conteúdo", 'Balanceamento de *link*", 'Múltiplos serviços", *"NAT" e "Proxy*", são aplicados através das políticas.

A definição das regras e políticas de segurança integram em uma mesma interface interativa todos esses recursos, e é possível aplicar em uma mesma política um conjunto de filtros que componham os recursos integrados. A interface permite rastrear todas as políticas a partir de *TAGs* que possibilitam agrupar as regras por finalidade o que facilita os filtros às pesquisas das políticas. As *tags* são adicionadas automaticamente pelo sistema ou o administrador pode definir uma.

- 1. Em apenas uma interface de configuração, a integração dos recursos em uma política:
- · Categoria WEB;
- Controle de Aplicativos;
- Controle de Banda;
- Múltiplos Serviços;
- QoS;
- Cota de Tempo e Tráfego;
- Escolha de perfil de link;
- Escolha de perfil de inspeção profunda;
- Controle de vírus e Malware.

2. A configuração ou habilitação dos serviços e recursos, não implicam em criação de uma política de segurança;

3. As políticas de segurança não são aplicadas individualmente em cada serviço.

À Exceção dos serviços "SD-WAN" e "Firewall", que contemplam regras ou políticas exclusivas no próprio módulo. Estas não se aplicam as políticas de segurança e sim exclusivamente ao serviço;

4. As políticas de segurança integram [N] condições de análises, que interagem com os diversos recursos de cada serviço, e isso tudo em uma mesma política de segurança.

O que torna o gerenciamento das políticas muito mais fácil e dinâmico para o administrador;

5. As políticas atuam em camadas e o seu comportamento de análise atua no modo "First Match Wins". (Literalmente quer dizer... O 1º entre os concorrentes VENCE);

6. As políticas de segurança são cadastradas em grupos e por prioridade e suportam reordenação.

Através da avaliação de *logs* e relatórios estatísticos, é possível reavaliar as prioridades e reordenar as políticas de segurança, de acordo o volume ou importância do tráfego. Por consequência melhora no desempenho do servidor;

- 7. As ações das políticas de segurança são:
- Permitir;
- Negar;
- Rejeitar.

Estes são os primeiros conceitos básicos que você deve conhecer.

Recursos das políticas de compliance

- Método de operação:
 - First-match wins;
 - ° Ordenação por prioridade.

Relação direta com o desempenho do *firewall* suporta a funcionalidade *multithread* que disponibiliza o máximo proveito dos processadores. Permite ordenar as regras, de modo que as políticas ou regras mais utilizadas sejam colocadas acima das políticas menos utilizadas, resultando em mais velocidade para as análises.

A definição das regras e políticas atendem as seguintes especificações e conjunto de filtros e condições para as tomadas de ação.

Abaixo lista das "Ações" VERSUS "Condições das regras":

| A | ções |
|--------|----------|
| Allow | Permitir |
| Deny | Negar |
| Reject | Rejeitar |

Tabela 1 - Ações de uma Política

VERSUS

Tabela 2 - Condições das Regras

| Condição POR: | Condições das políticas: |
|---------------|---|
| Servidor | Uma mesma regra pode ser aplicada para múltiplos servidores; Configurada em uma mesma tela. |
| Properties | Name; Description; Tags; Action; Policy Group; Position; Enable traffic logging; Time/Period/Date. |
| Connection | Source Network Zone; Network Interface; IP Address; MAC Address; Destination IP Address; Service. Identification Authenticated (Users/ Groups); |

| Content | Web Proxy FTP; HTTP; HTTPS; SSL Inspection; Validate SSL certificate; SSL Common Name; Malware Scanning; Explicit Proxy. Web Filter Web Categories; Applications; URL Filter, Browsers; HTTP method; Email Protection SMTP; POP3. |
|----------|--|
| Control | Surfing Control Content-Type Filter, HTTP Filter Header, Filter, Surfing Quotas Maximum Time; Maximum Traffic; Max Download Size; Max Upload Size. |
| Security | Deep Inspection Sensor. Threat Blocking Compromised Addresses; Geolocation. Packet Filter TTL; Package Type; Packet Content; TCP MSS. |
| Routing | Gateway NAT; SD-WAN. QoS Traffic Shaping; Flag packets (TOS); Flag packets (DSCP). |

As definições são idênticas para IPv4 e IPv6, sofrendo alterações somente em seus endereçamentos e algumas características proprietária de cada versão do protocolo.



Policies

Contém as opções:

- IPv4;IPv6.

Políticas IPv4

Esta seção irá demonstrar o processo de criação de políticas IPv4, além de explicar com profundidade os conceitos de como elas atuam no UTM.

Caso não esteja já selecionado, clique na opção "IPv4";



Surgirá a Tela de "Policies IPv4", conforme demonstrado pela imagem a seguir:

| | 8 |
|------|---|
| ntie | |

IPv4

Esta seção irá se aprofundar em:

- Criação de grupos de políticas;
 Cadastro e Remoção de políticas.

A seguir, vamos analisar cada componente deste painel.

IPv4 - Menu de ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



IPv4 – Menu de ações

O menu é composto das seguintes opções:

- Create Group;
- Delete Groups;
- Create Policy;
- Delete Policies;
- Expand All e Collapse All.

A seguir cada opção do menu de ações será detalhada.

| IPv4 - Menu de ações - C | reate Group |
|--|--|
| Através da opção " <i>Create Group</i> " é possível criar um novo grupo 1. Clique na opção " <i>Create Group</i> "; | b. Para acessar, clique no menu de ações []. |
| | Q 🗸 |
| | Create Group |
| | Delete Groups |
| | Create Policy |
| | Delete Policies |



2. A tela "Create Group" será exibida. Adicione o nome do grupo desejado:

| | Create Group X |
|--------------------------------|---|
| | * Name |
| | Cancel Save |
| | IPv4 – Create Group |
| Após nomear o gr Save]. | upo, caso deseje cancelar clique no botão <i>Cancel</i>]. Para concluir a criação do grupo clique no botão <i>Save</i> |
| | Group created successfully Group created successfully |

O grupo foi criado com sucesso.

Create Group - Exemplos - Criação de Grupos

A seguir, vamos exemplificar o cadastro de grupos de modo a orientar a demonstrar as melhores práticas para modelagem de grupos e políticas.

Efetuaremos a demonstração criando os seguintes grupos:

- Block;
- Forward;
- Masking (NAT);
 Web Filter.

Grupo: Block

Finalidade: Definir as políticas para aplicar o "bloqueio" imediato e definitivo de tráfegos específicos já conhecidos como INAPROPRIADOS. Sem a intervenção de "proxies".

| Para adicionar os grupos de políticas, acesse o menu de ações[|] e selecione a opção [Create Group]. |
|--|---------------------------------------|
| | ۹ 🗸 |
| | Create Group |
| | Delete Groups |
| | Create Policy |
| | Delete Policies |
| | Expand All |
| | Collapse All |
| IPv4 - | Menu de ações - <i>Create Group</i> |

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:

| | Create Group | × |
|------------|--|------|
| | * Name | |
| | Block | |
| | Cancel | Save |
| digitado o | Create Group - Criando o grupo Block Save nome indicado, clique no botão []; | |
| | Group created successfully Group created successfully | |

O grupo foi criado com sucesso.

Após ter

Grupo: Forward (FW)

Finalidade: Definir as políticas de gerenciamento do tráfego entre as redes/ subredes internas.

Neste grupo vamos definir políticas de "bloqueio" do tráfego não autorizado, para detecção e geração de "log" e políticas de "Greylist", ou seja, permitir o tráfego inicialmente classificado como "confiável", no entanto com a condição de "Inspecionar" o tráfego e validar a sua legitimidade e aplicar o descarte dos pacotes identificados com conteúdo "inapropriado ou malicioso".

Para adicionar os grupos de políticas, acesse o menu de ações[

× .

] e selecione a opção [Create Group].

IPv4 - Menu de ações - Create Group

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:

| | Create Group | × |
|---------------------|--|------|
| | * Name Forward (FW) | |
| Após ter digitado c | Cancel Create Group - Criando o grupo Forward | Save |
| | Group created successfully Group created successfully | |
| O grupo foi criado | com sucesso. | |

Grupo: Masking (NAT)

Finalidade: Definir as políticas de gerenciamento do tráfego para a rede WAN (Internet) para servidores e serviços específicos sem intervenção do "proxy".

Neste grupo vamos definir políticas de "Greylist", ou seja, permitir o tráfego inicialmente classificado como "confiável", para os servidores e serviços específicos, no entanto com a condição de "Inspecionar" o tráfego e validar a sua legitimidade e aplicar o descarte dos pacotes identificados com conteúdo "Inapropriado ou malicioso".

| Para adicionar os grupos de políticas, acesse o menu de ações[|] e selecione a opção [Create Group]. |
|--|---------------------------------------|
| | ۹ 🗸 |
| | Create Group |
| | Delete Groups |
| | Create Policy |
| | Delete Policies |
| | Expand All |
| | Collapse All |

IPv4 - Menu de ações - Create Group

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:

| | Create Group | | | Х |
|--|-------------------------|---|--------|------|
| | * Name Masking (NAT) | | | |
| | | | Cancel | Save |
| | - | Create Group - Criando o grupo Masking (I | VAT) | |
| Após ter digitado o nome indicado, clique no botão [Save]; | | | | |
| | | 😡 Group created successfull | y | |

Group created successfully

O grupo foi criado com sucesso.

Grupo: Web Filter

Finalidade: Definir as políticas de gerenciamento do tráfego para a rede WAN (Internet) via "Proxy".

Neste grupo vamos definir políticas de 'bloqueio' do tráfego não autorizado, para detecção e geração de "log", políticas de "Greylist", ou seja, permitir o tráfego inicialmente classificado como "confiável", no entanto com a condição de "Inspecionar" o tráfego para validar a sua legitimidade e aplicar o descarte dos pacotes identificados com conteúdo "inapropriado ou malicioso".

| Para adicionar os grupos de políticas, acesse o menu de ações[| e selecione a opção [Create Group]. |
|--|-------------------------------------|
| | ۹ 🗸 |
| | Create Group |
| | Delete Groups |
| | Create Policy |
| | Delete Policies |
| | Expand All |
| | Collapse All |

IPv4 - Menu de ações - Create Group

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:

| Create Group | × |
|--------------|-------------|
| * Name | |
| Web Filter | |
| | Cancel Save |

Create Group - Criando o grupo Web Filter



O grupo foi criado com sucesso.

Isso conclui o processo de criação dos grupos que serão utilizados para o exemplo, será possível visualizá-los na página inicial em *IPv4* abaixo de "*Local Rules*", conforme exemplificado pela imagem abaixo.

| an trine | |
|--------------------|---------------|
| Lacy Relat | |
| = 2 Book | . /1 |
| II > raward (ref | . / 8 |
| = > meeting (mart) | () / * |
| -) metrins | |

IPv4 – Policy Groups

Para ver o cadastro de algumas políticas básicas, acesse Policies IPv4 - Exemplos - Criação de Políticas.

IPv4 - Menu de ações - Delete Groups

Através do botão "Delete Groups" é possível deletar vários grupos instalados ao mesmo tempo. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) grupo(s) deseja deletar clicando no *checkbox*[___], como demonstrado pela imagem abaixo:



IPv4 - Menu de ações - Delete Groups

3. Surgirá a mensagem se deseja realmente deletar os pacotes selecionados:



Após realizar esses procedimentos os grupos terão sido excluídos com sucesso.

IPv4 - Menu de ações - Create Policy

O botão "Create Policy" cria as políticas no grupo de políticas selecionando, para que ele esteja disponível, é necessário que um grupo tenha sido criado previamente (cheque esta página para mais informações).

Para criar uma política, siga os passos:

1. No menu de ações [], clique na opção "Create Policy"; Create Group Delete Groups Import Template Save Template Create Policies Expand All Collapse All

IPv4 - Menu de Ações - Create Policy

2. Surgirá a tela Policy Form;

| Properties | General | | |
|------------|----------------------------------|----------|--|
| Convection | • Name | | |
| Impection | Description | | |
| Routing | | 245 | |
| 3321-04 | * Action | Taga | |
| Advanced | Alize | | |
| | Policy Group | | |
| | | | |
| | Traffic Monitor | | |
| | Truffic Logging | | |
| | Schedule | | |
| | Time | Schedule | |
| | | | |

Esta janela é organizada pelas seguintes abas:

- Properties;
 Connection;
 Inspection;
 Routing;
 Advanced.

A seguir explicaremos cada um dos campos desta janela.

Create Policy - Aba Properties

Na aba [Properties] é obrigatório definir um nome e descrição para a política e opcionalmente podem ser definidas Tags que auxiliam na organização e facilitam a busca de políticas.



IPv4 - Abas Laterais - Properties

Nesta aba estão contidos os painéis:

- General;
- Schedule.

A seguir analisaremos a função de cada campo dos painéis.

General

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [General]:

- Name: Definir nome para política;
- Description: Definir descrição para política;
- Action: Determina o comportamento da política em questão, tendo como possibilidades:
 - · Allow: Como o próprio nome diz, a ação Allow serve para conceder acesso e deixar o tráfego livre de bloqueios;
 - Deny: A ação Deny bloqueia o tráfego mas não informa ao endereço de origem que o serviço está sendo bloqueado. Ou seja, neste cenário, para o endereco da origem da conexão, não é possível saber se tem um firewall interceptando a conexão ou simplesmente o serviço não está ativo;
 - Reject: A ação Reject notifica ao endereço de origem que o serviço foi bloqueado por um Firewall, sendo que este envia um pacote ICMI indicando que o serviço está inacessível.
- Tags: Esta opção permite definir Tags de forma que o administrador consiga usá-las como "Filtro" para suas pesquisas tomando-as como base em suas definições. Por padrão o sistema define um "nome" para as *Tags* por tipo de recurso em uso habilitado na política; *Policy Group*: Através dessa opção é possível incluir a política em questão dentro de um grupo de políticas;
-], as informações das sessões que derem "match" com a política criada, serão coletadas pelo • Traffic Monitor: Com esta opção checada[serviço de monitoramento.
- Traffic Logging]: Essa caixa de checagem, caso seja habilitada fornece a opcão de gerar o relatório de uma determinada política. As opções de Traffic Loging são configuradas nesta página.

Caso pretenda utilizar Netflow, ele precisa ser habilitado opcionalmente pelo administrador nas configurações de Traffic Logging do sistema. Para mais informações, consulte esta página.



Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Schedule]:

| Schedule | | |
|----------|------------------------------|--|
| Time | Schedule | |
| | | |
| | IPv4 – Properties - Schedule | |

- *Timel* J: Caso a caixa de seleção estiver selecionada, determina se a regra se aplicará em dias úteis ("*Business*"), finais de semana ("*Weekenc*") ou em algum outro objeto do tipo "*Time*" que tenha sido criado previamente;
- Schedule]: Caso a caixa de seleção estiver selecionada, permite determinar se a regra se aplicará em relação a um objeto "Period/Date" que tenha sido criado previamente.

A seguir analisaremos o conteúdo da aba Connection.

Demais abas:

- Inspection;Routing;Advanced.

Create Policy - Aba Connection

A aba [Connection] fornece diversos filtros para especificar o escopo de origem e destino, sendo obrigatório a escolha de pelo menos um filtro.



IPv4 - Abas Laterais - Connection

Nesta aba estão contidos os painéis:

- Source;
- Destination;
- Identification.

A seguir analisaremos a função de cada campo dos painéis.

Source

O painel [Source] oferece vários filtros com função de determinar o escopo de origem, como já mencionado anteriormente, é necessário selecionar ao menos um filtro. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Source]:

| Source | | |
|--------------|-------------------|---------|
| Network Zane | Network Interface | Country |
| v | | |
|] IP Address | MAC Address | |
| | | |

IPv4 - Connection - Source

Network Zone Signature Signature

| Network Zone | |
|--------------|---|
| | ^ |
| CLUSTER3 | |
| DMZ | |
| LAN | |
| WAN | |

IPv4 - Connection - Source - Network Zone

• Network Interface []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar interface de rede para serem utilizadas como filtro de origem. As interfaces que aparecem nesse menu são criadas em Network - Interfaces;

| Network Interface | |
|-------------------|---|
| | ^ |
| eth0 | |
| eth1 | |
| eth2 | |
| eth3 | |
| tun0 | |

IPv4 – Connection - Source - Network Interface

• IP Address Z: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de Endereço IP (IPs,

redes ou conjuntos) para serem utilizados como filtro de origem. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar um ou mais objeto de endereço que irá compor a regra. Os endereços que aparecem nesse menu são criados em Settings - Objects;

| Add IP A | ddress | × |
|----------|--------------------|-------------|
| All | ~ | ۹ 🗸 |
| | Item | |
| | 172.16.102.181/32 | |
| | 172.31.0.1/32 | |
| | 192.168.254.174/32 | |
| | 199.99.99.99/32 | |
| | 20.0.0.2/32 | |
| | Class A network | |
| | Class B network | |
| | Class C network | |
| | IP eth0 | |
| | IP eth0 | |
| | | < 1 2 > |
| | | Cancel Save |

IPv4 – Connection - Source - IP Address

• MAC Address []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de Endereço Mac

Address para serem utilizados como filtro de origem. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar um ou mais objeto de MAC address que irá compor a regra. Os endereços que aparecem nesse menu são criados em Settings - Objects;

| Add MAC | Address | | × |
|---------|-----------------------|--------|-------|
| All | ~ | | ۹ 🗸 |
| | Item | | |
| | Mac Address Example 1 | | |
| | Mac Address Example 2 | | |
| | | | < 1 > |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Cancel | Save |

IPv4 - Connection - Source - Mac Address

• Country

filtro de origem. Ao clicar sobre o botão [🗮], a tela abaixo será exibida para selecionar um ou mais país que irá compor a regra.

Add Country

r.

| All | |
|-----|------------------|
| | Item |
| | Argentina |
| | Armenia |
| | Aruba |
| | Australia |
| | Austria |
| | Marta Azerbaijan |
| | 🛌 Bahamas |
| | Bahrain |
| | Bangladesh |
| | Barbados |
| | < 1 2 3 4 5 26 > |
| | Cancel Save |

IPv4 - Connection - Source - Country

Destination

 $E^{(2)}$

O painel [Destination] fornece diversos filtros para especificar o escopo de destino, sendo obrigatório a escolha de pelo menos um filtro. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Destination]:

1

| IP Address | Service | | Country | |
|------------|---------|-------|---------|-----|
| | | 1 = 1 | | 113 |

- IPv4 Connection Destination
- IP Address

redes ou conjuntos) para serem utilizados como filtro de destino. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar um ou mais objeto de endereço *IP* que irá compor a regra. Os endereços que aparecem nesse menu são criados em *Settings - Objects*;

| Add IP A | ddress X |
|----------|--------------------|
| All | ✓ |
| | Item |
| | 172.16.102.181/32 |
| | 172.31.0.1/32 |
| | 192.168.254.174/32 |
| | 199.99.99/32 |
| | 20.0.2/32 |
| | Class A network |
| | Class B network |
| | Class C network |
| | IP eth0 |
| | IP eth0 |
| | < 1 2 > |
| | Cancel Save |

IPv4 - Connection - Destination - IP Address

• Service []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de serviços (protocolos e

portas) utilizados como filtro de destino. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar um ou mais objeto de serviço que irá compor a regra. Os endereços que aparecem nesse menu são criados em *Settings* - *Objects*;

| Add Sen | vice | × |
|---------|--------|-----------------|
| All | V | ۹ 🗸 |
| | Item | |
| | AH | |
| | AOL | |
| | BGP | |
| | DHCP | |
| | DHCPV6 | |
| | DNS | |
| | ESP | |
| | FTP | |
| | GRE | |
| | H323 | |
| | | < 1 2 3 4 5 6 > |
| | | Cancel Save |

IPv4 - Connection - Destination - Service

Country : Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Países para serem usado como filtro de destino. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar um ou mais país que irá compor a regra.

Add Country

r

| All | ✓ Q ¥ |
|-----|------------------|
| | Item |
| | T Argentina |
| | Armenia |
| | Aruba |
| | 🔛 Australia |
| | Austria |
| | 📼 Azerbaijan |
| | 🛌 Bahamas |
| | Bahrain |
| | Bangladesh |
| | Barbados |
| | < 1 2 3 4 5 26 > |
| | Cancel |

17

X





 E^{γ}

O painel [Identification] permite habilitar o recurso de autenticação para a política. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Identification]:

| Identification | | |
|----------------|--------|--|
| Authenticated | | |
| C Vsers | Groups | |
| | | |

Policies IPv4 - Connection - Identification

- Authenticated
- Users []: Este campo só fica disponível ao marcar a caixa de checagem e a opção Authenticated. Permite especificar usuário(s) aos quais a política será aplicada. Ao clicar sobre o botão [

| Add User | Х |
|----------|--------|
| All V | ۹ 🗸 |
| Item | |
| No Data | |
| | |
| | |
| | |
| | |
| | Cancel |

IPv4 - Connection - Destination - Users

• Groups

política se aplica. Ao clicar em [📜], a tela abaixo será exibida para selecionar um ou mais grupos que irão compor a regra.

| Add Group | | Х |
|-----------|---------|-------------|
| All V | | ۹ 🗸 |
| Item | | |
| | No Data | |
| | | |
| | | |
| | | |
| | | |
| | | Cancel Save |

IPv4 - Connection - Destination - Groups

A seguir analisaremos o conteúdo da aba Inspection.

- Routing; Advanced.

Create Policy - Aba Inspection

Na aba [Inspection] é possível selecionar vários recursos para inspeção do tráfego afetado pela política.



IPv4 - Abas Laterais - Inspection

Inspection

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Inspection]:

| × |
|---|
| |
| |
| |
| |
| |
| |
| |

IPv4 - Inspection - Inspection

- SSL Inspection S: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite interceptar o tráfego SSL permitindo a inspeção do seu conteúdo. As opções que aparecem nesse menu são criadas em Proxy SSL Inspection;
- Intrusion Prevention []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite aplicar IPS nas políticas. Os perfis exibidos nesse menu são criados em Services Intrusion Prevention;
- Threat Protection []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite aplicar IPS nas políticas. Os perfis exibidos nesse menu são criados em Services Threat Protection;
- Application Control [1]: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar um perfil para aplicar controle de acesso à aplicações. Os perfis exibidos nesse menu são criados em Services Application Control;

Sempre que um Application Control for adicionado em uma política o Web Filter é habilitado nesta política, mesmo que um Web Filter propriamente dito não se tenha sido selecionado.

• Web Filter []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar um perfil para efetuar a filtragem de conteúdo. Os perfis exibidos nesse menu são criados em Services - Web Filter.

A seguir analisaremos o conteúdo da aba Routing.

• Advanced.

Create Policy - Aba Roteamento

Na aba [Roteamento] você configura o NAT, perfil de SD-WAN, CGNAT, QoS e Roteamento de Aplicativos. A seguir analisaremos a função de todos os campos da aba Roteamento.



IPv4 - Abas Laterais - Roteamento

Nesta aba estão contidos os painéis:

- Gateway
- Roteamento de Aplicativos.
- QoS

A seguir analisaremos a função de cada campo dos painéis.

Gateway

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Gateway]:

| Gateway | | |
|----------------------------|--------|---|
| NAT NAT | SD-WAN | |
| Orteway Dehallt Mancaradat | ×] | 4 |
| COMAT | | |
| Eur.200003000 | | |



• NAT Permite ativar o NAT e a escolha do endereço para tradução de origem, por padrão é configurado o IP do link do Gateway Padrão;

| Gateway Default (Máscarado) | |
|-----------------------------|--|
|-----------------------------|--|

• SD-WAN

| SD-WAN | |
|--------------------------------------|---|
| | ^ |
| Load Balance | |
| Failover | |
| IPv4 – Roteamento - Gateway - SD-WAN | |

• CGNAT [2]: Permite configurar o uso de CGNAT na política, ou seja, uma solução de NAT a nível de provedor, onde o mesmo IP local pode ser atribuído a diferentes hosts ao mesmo tempo, porém com tráfego em portas distintas. As portas disponíveis para o uso de CGNAT devem ser a partir da 2000 (TCP e UDP).



IPv4 - Roteamento - Gateway - CGNAT

QoS

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [QoS]:

| Controle de Banda | | Marcar Pacotes (TOS) | |
|-----------------------|--|----------------------|--|
| | | to research inst | |
| Marcar Pacotes (DSCP) | | | |
| NE (Best 155xt) | | | |

IPv4 - Roteamento - QoS

• Controle de Banda [>]: Permite ativar e selecionar a prioridade do tráfego, os valores podem ser ajustados em Configurações >> Rede >> C ontrole de Banda;
- Marcar Pacotes (TOS) Ao ativar permite a marcação do pacote conforme as opções: Espera mínima, Processamento máximo, Confiança máximo, Custo mínimo e prioridade normal;
- Marcar Pacotes (DSCP) [. Ao ativar permite a marcação do pacote conforme as opções.

Roteamento de Aplicativos

O painel [Roteamento de Aplicativos] serve para aplicar balanceamento de rotas em determinadas aplicações, é necessário selecionar ao menos um perfil de SD-WAN e ativar a Inspeção SSL. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Roteamento de Aplicativos]:

| Roteamento de aplicativos | |
|---|--|
| III Apilications | Perfil SD-WAN |
| 12 | . v. |
| IPv4 – Roteamento - QoS | r - Roteamento de Aplicativos |
| Para que as opções deste painel fiquem disponíveis para edição, é n | ecessário ativar a Inspeção SSL na aba Inspeção. |
| | |
| Ao aplicar o roteamento por aplicação, o tráfego desta mesma seguir conexão original. | á um outro caminho independente do que foi definido no <i>Gateway</i> da |

• Aplicativos []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar aplicações para que seja feito o roteamento de solicitações recebidas através do perfil de SD-WAN que for selecionado no campo à seguir, deste modo é possível obter maior

controle sobre o consumo e a prioridade de banda consumida pelas aplicações que forem selecionadas. Ao clicar sobre o botão [=], a tela abaixo será exibida para selecionar um ou mais objeto de endereço *IP* que irá compor a regra;

| 묘 | D Sustress | | allaborative | llem | |
|----------|------------|----------|--------------|----------------|---|
| | a | | CED | 24/7 Media | |
| dourient | srul | 204 | nitit | Ad Master | |
| P | 0 | | T | Co/e Audience | |
| 144 | yutal | protocoj | phony | Doubleclick | |
| P | | 8 | * | Galladity | |
| | | storage | steating | Google Advance | |
| 00 | | 0 | | OpIND | |
| Hodele: | yobi | und . | | Webtrendic | |
| | | | | | 1 |
| | | | | | |

IPv4 - Roteamento - QoS - Roteamento de Aplicativos - Aplicativos

• Perfil SD-WAN: Este campo é obrigatório. Ele é utilizado para determinar qual perfil de SD-WAN será utilizado para efetuar o balanceamento das rotas utilizadas pelas aplicações selecionadas. Os perfis exibidos nesse menu são criados em Services - SD-WAN.

Seguiremos para a aba Advanced.

Create Policy - Aba Advanced

Na aba [Advanced] é possível configurar os parâmetros limite dos pacotes por segundo em uma conexão.



Advanced

Abaixo segue uma descrição da função dos campos do formulário Advanced:

| Packet Pate (packets/seconds) | Puret Data | |
|-------------------------------|------------|--|
| Packet Rate (packets/seconds/ | Duist Rate | |
| 2000 | 1 | |
| Options | | |
| | | |
| TCP MSS | | |
| | | |
| | | |

IPv4 - Inspection - Advanced

DoS Protection: Com a caixa de DoS Protection checada () é possível limitar a quantidade máxima de pacotes por segundo no Firewall, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede.

- Packet Rate: A opção Packet Rate configura o Firewall para limitar as conexões a um valor máximo de pacotes por segundo.
- Burst Rate: A opção Burst Rate configura o Firewall para permitir inicialmente uma quantidade máxima de pacotes por segundo sem validar o Pa cket Rate, permitindo assim flexibilizar o controle de tráfego para picos de tráfego ocasionais.

Options:

• TCP MSS [

A seguir vamos analisar alguns exemplos de criação de políticas IPv4.

Exemplos - Criação de Políticas

A seguir, vamos exemplificar o cadastro de alguns exemplos de políticas como forma de demonstrar de boas práticas. O modelo apresentado visa orientar a modelagem de grupos e políticas baseado no conceito fundamental de ordenação e tratamento das políticas "First match Wins".

Efetuaremos a demonstração criando as seguintes políticas:

- Exemplo 1 Política de Navegação via *Proxy* com *Deep Inspection* habilitado para *ATP*;
 Exemplo 2 Política de Filtro de conteúdo *WEB* Bloqueando categorias de improdutividade;
- Exemplo 3 Política de Filtro de aplicativos Bloqueando aplicativos WEB 2;
- Exemplo 4 Política de NAT Para o Servidor MS Windows AD >> com destino >> Base UPDATE WSUS sem autenticação e com inspeção IPS
- Exemplo 5 Política de *NAT* para todos os protocolos com *DPI* e *Proxy*.

Exemplo 1 - Política de Navegação via Proxy habilitado para ATP

Definição da política:

- [Properties]: Web Navigation Users, Action: Allow; Enable traffic logging; Policy Group=Web Filter;
- [Conditions]: Zona=LAN, Autenticado, Serviços (HTTP; HTTPS);
- [Inspection]: SSL Inspection, Threat Protection e Web Filter;
- [Routing]: Prioridade Média (Reserva 50% link) e TAG = Manter as Tags geradas pelo sistema.

| Para adicionar uma política de segurança, no menu de ações [|], clique na opção "Create Policy"; |
|---|-------------------------------------|
| | ۹ 🗲 🗸 |
| | Create Group |
| | Delete Groups |
| | |

| ۹ 🗲 🗸 | | | | | |
|-----------------|--|--|--|--|--|
| Create Group | | | | | |
| Delete Groups | | | | | |
| Import Template | | | | | |
| Save Template | | | | | |
| Create Policy | | | | | |
| Delete Policies | | | | | |
| Expand All | | | | | |
| Collapse All | | | | | |

IPv4 - Menu de Ações - Create Policy

Configure cada aba de acordo com as definições demonstradas à seguir.

Properties

Na aba [Properties], em Name nomeie como: "Web Navigation Users";

Em Description digite "Web Navigation Users";

Em Action selecione a opção "Allow";

Em Policy Group selecione "Web Filter";

Marque a caixa de seleção Traffic Logging

| iky Form | | | | × |
|------------|-----------------------|----------|-------|---|
| Poperties | Betesi | | | |
| Conditions | * Name | | | |
| | mob Namgation Visits. | | | |
| inspection | Description | | | |
| liciting | mob Namgabon Viges. | | | |
| | + Action | Tags | | |
| | athe | | | |
| | * Policy broup | | | |
| | Web Film | | | |
| | 💟 Traffic Lagging | | | |
| | Schehrle | | | |
| | Time | Schedule | | |
| | | | tunit | - |

Create Policy - Ex. 1 - Properties

Selecione a próxima aba, [Conditions].

Conditions

Na aba [Conditions], em Network Zone selecione: "LAN";

Em Service selecione HTTP e HTTPS;

Marque a caixa de seleção Authenticated [



| Popertes | # Source | | | | | |
|------------|----------------|------|---------------------|--------|---------|----|
| Cinetana 1 | Network Zone | | Robusorik Interface | · | Country | |
| | LAN | 1.91 | | | | |
| inspection | W Address | | WAC Ad threat | | | |
| likiting | | | | | | |
| | Destaution | | | | | |
| | IF Adelross | | Sarvice | | Country | |
| | | | | | | 14 |
| | identification | | | | | |
| | Authenticated | | | Groupt | | |

Create Policy - Ex. 1 - Conditions

Selecione a próxima aba, [Inspection].

Inspection

Na aba [Inspection], marque a caixa de seleção SSL Inspection [

Marque a caixa de seleção Threat Protection z e adicione o perfil com as verificações de malware e bloqueios desejados (Para mais informações, consulte esta página);

Marque a caixa de seleção Web Filter [] e adicione o perfil com as categorias que deseje filtrar (Para mais informações, cheque esta página);

| licy Form | | |
|------------|------------------------|------------|
| Properties | Impetion | |
| Conditions | SSL happertine | |
| | TeleVacipation III. | |
| Insection | Intrusion Presentation | |
| Raiding | Depart Protection | |
| | Init Incipitor ATP | |
| | Application Control | |
| | 🖸 Web Filter | |
| | Hobidolycom | |
| | | |
| | | Canot Sole |

Create Policy - Ex. 1 - Inspection

Selecione a próxima aba, [Routing].

Routing

Na aba [*Routing*], marque a caixa de seleção *Traffic Shaping* [

| ucy Harm | | | |
|---------------|--------------------------|--------------------|--|
| Properties | - Boleway | | |
| Conditions | TAN . | SIS-WAN | |
| | and a farming the second | | |
| inpetion. | | | |
| Tables 1 | Qu5 | | |
| in the second | Traffic skaping | Plag Packets (PDS) | |
| | Hadium | - | |
| | TCP MSB | PlagPackets (DSOP) | |
| | | Without Street | |
| | Application Rowling | | |
| | appRotes | SD-WWV Profile | |
| | | | |
| | | | |

| | | | Add | Policy – E> | k. 1 – Routing | g | | | | |
|----------------------------------|--|-----------------------------------|----------------------------|-------------------------------------|----------------------------|-------|------------|----------------|---------------|-------------|
| Após ter config | jurado cada aba de acordo | com a definição | o da política | a aplicada, | clique em [| Save |]. | | | |
| | | | 🕑 Po | olicy save | d successfu | ully | | | | |
| | | | Poli | icy Saved | Successfully | | | | | |
| A tela ilustrada | na imagem a seguir será e | xibida: | | | | | | | | |
| | | | | | | | | | | |
| | Me was bacquised over | - | 31 | - | лана 1. теке 1. теке | | | | 191 | |
| | | | Add Poli | icy – Web | Navigation U | lsers | | | | |
| | | | | | | | | | | |
| Após salvar, pa informações a | ara que a política entre em a respeito da fila de comando | ação será nece os acesse a pág | ssário aces gina: UTM - | ssar a fi la e Fila de co | de comando mandos. | os [|] e aplica | ar as alteraçô | ies efetuadas | . Para mais |
| Após realizar e | esses procedimentos a políti | ca terá sido co | nfigurada c | om sucess | 60. | | | | | |

No exemplo 1 definimos e adicionamos uma política para acesso web com inspeção, no entanto, sem restrições ou qualquer tipo de filtro.

Exemplo 2 - Política de Filtro de conteúdo WEB -Bloqueando categorias de improdutividade

Vamos adicionar uma política aplicando um filtro de conteúdo, iremos definir os parâmetros para esta política e considerar o filtro à URLs que compreende-se como categorias de "Improdutividade". Para definir esta lista de categorias é interessante consultá-las antes em Diagnostics - Category

Lookup, ou mesmo navegar nos perfis em Services - Web Filter em Web Categories, clique em [

| Add Category | | × |
|--|--------------|-----|
| All V | ٩ | ~ |
| Uncategorized Sites | Allow 🗸 | ^ |
| - Abortion | Allow 🗸 | |
| Pro-life | Allow 🗸 | |
| Pro-Choice | Allow 🗸 | |
| Activism Groups | Allow 🗸 | |
| ✓ Adult Material | Allow 🗸 | |
| Adult Content | Allow 🗸 | |
| Nudity | Allow 🗸 | |
| Sex | Allow 🗸 | |
| Sex Education | Allow 🗸 | |
| Lingerie and Swimsuit | Allow 🗸 | |
| Business and Economy | Allow 🗸 | |
| Financial Data and Services | Allow 🗸 | |
| ▼ Drugs | Allow 🗸 | |
| Abused Drugs | Allow \vee | |
| Prescribed Medications | All | ¥ |
| Custom | Cancel | ave |

Services - Web Filter - Web Categories

Lista das categorias identificadas como improdutivas.

- Entretenimento;
- MP3;
- Jogos de azar e apostas;
- Jogos /Games;

- Gestão de largura de banda;
- Rádio e TV na Internet,
- Streaming mídia; ٠
- Sociedade e estilos de vida;
- Anúncios pessoais e namoros;
- Sites pessoais na Web;
- · Esportes;
- Turismo.

Abaixo um resumo do que será configurado na regra:

- [Properties]: Productivity Loss, Enable traffic logging; Policy Group=Web Filter; TAG = Block;
- [Conditions]: Zona de rede *IP* = *"LAN"*; Serviços (*HTTP*; *HTTPS*); Autenticado; [Inspection]: SSL Inspection e Web Filter; ٠
- ٠
- [Routing]: Sem controles.

Para adicionar uma política de segurança siga os passos:

| Para adicionar uma política de segurança, no menu de ações [|], clique na opção "Create Policy"; |
|--|-------------------------------------|
| | ۹ 🗲 🗸 |
| | Create Group |
| | Delete Groups |
| | Import Template Save Template |
| | Create Policy |
| | Delete Policies |
| | Expand All |
| | Collapse All |

IPv4 - Menu de Ações - Create Policy

Configure cada aba de acordo com as definições demonstradas à seguir.

Properties

Na aba [Properties], em Name nomeie como: "Productivity Loss";

Em Description digite "Productivity Loss";

Em Action deixe a opção "Allow", você efetuará o bloqueio através do perfil de Web Filter,

Em Policy Group selecione "Web Filter";

Em Tags digite "Block";

Marque a caixa de seleção Traffic Logging

Você terá chego no resultado ilustrado pela imagem abaixo:

| and the second second | 122.536 | | |
|-----------------------|--------------------|----------|--|
| Pallade | General | | |
| Conditions | * Marrie | | |
| | Productivity Linus | | |
| Inspection. | Description | | |
| | Productivity loss | | |
| - Boding | | 1 | |
| | Action | Mp | |
| | - Alter | Block (/ | |
| | * Pelicy Group | | |
| | Tako Mitur | | |
| | Traffic Logging | | |
| | Schedule | | |
| | Time | Scheikle | |
| | | | |

Create Policy - Ex. 2 - Properties

Selecione a próxima aba, [Conditions].

Conditions

Na aba [Conditions], em Network Zone selecione: "LAN";

Em Service selecione os serviços HTTP e HTTPS;

Marque a caixa de seleção Authenticated [

Você terá chego no resultado ilustrado pela imagem abaixo:

Quando for selecionar os serviços HTTP e HTTPS, agilize simplesmente digitando "HTTP" no campo de busca, por padrão surgirá apenas os serviços HTTP e HTTPS, aí basta selecionar ambos.

| Projectes | # Source | | | | |
|-----------|---------------|-------------------|------|-------------|--|
| | Retwork Zane | Network Interface | | Eeunopy | |
| Canddian | Les | | | -tailentet. | |
| icspec5an | IP Ackdrone | MNC Adictions | | | |
| Rading | | | | | |
| | Dectinution | | | | |
| | IP Address | Service | | Ennoy | |
| | | 2 Margari | = | | |
| | Mentification | | | | |
| | Authenticated | 5 | 0.85 | | |
| | | | (M) | | |

Create Policy – Ex. 2 – Conditions

Selecione a próxima aba, [Inspection].

Inspection

Na aba [Inspection], marque a caixa de seleção SSL Inspection [

Marque a caixa de seleção **Web Filter** [] e selecione o perfil relacionado as categorias de improdutividade (Para mais informações, cheque a esta pági na);

| | authorau | |
|------------|----------------------|--------|
| Conditions | SSL importion | |
| | Well Therapping SSL | |
| impaction. | Intrusion Prevention | |
| 740000 | | |
| seeing. | Threat Prideation | |
| | | |
| | Application Control | |
| | | |
| | Web Filter | |
| | Polarity cos | |
| | | |
| | | |
| | | |
| | | |
| | | Carcol |

Selecione a próxima aba, [Routing].

Routing

Na aba [Routing], nenhum controle será ativado, conforme exemplificado pela imagem a seguir:

| ky Form | | | |
|------------|--|---------------------|-------|
| Properties | Batteries | | |
| Contrios | MAT | SID-WHIM | |
| | | | |
| inspection | | | |
| 10000 | Q06 | | |
| hooing | mattic Stoping | Plag Packets (108) | |
| | And the second sec | The second second | |
| | TOP HSS | Plag Packars (DSCP) | |
| | | All Date Street. | |
| | Application Routing | | |
| | Appileations | SD-WWI Profile | |
| | | | |
| | | | tanto |

Create Policy – Ex. 2 – Routing

| Após ter configurado cao | ida aba de acordo cor | n a definição da | a política aplicada, | clique em [|]. | |
|---|--|------------------------------------|--|--------------------------------|-------------------------|--------------------------|
| | | | Policy save Policy Saved S | d successfully Successfully | | |
| A tela ilustrada na image | em a seguir será exib | ida: | | | | |
| 1. 10. | Roberty Law | e . | 8. e | 0 ees | - | |
| | | | Create Policy – P | roductivity Loss | | |
| Após salvar, para que a informações a respeito o | política entre em açã da fila de comandos a | io será necessá acesse a página | irio acessar a fila c I: UTM - Fila de col | de comandos [mandos. |] e aplicar as alteraçõ | ies efetuadas. Para mais |

Após realizar esses procedimentos a política terá sido configurada com sucesso.

No exemplo 2 definimos e adicionamos uma política de bloqueio para algumas categorias de sites de conteúdo improdutivo.

Exemplo 3 - Política de Filtro de aplicativos - Bloqueando controle de aplicação em nuvem

Vamos adicionar uma política aplicando filtros de aplicativos. Vamos considerar o filtro a *Urls* ou *sites* que executam aplicativos que compreendam as ações de improdutividade ou risco de segurança. Vamos conhecer a lista de aplicativos que podemos filtrar nos perfis localizados de *Services - Application*

Control, em Applications clique em [], este painel tem o intuito de identificar aplicações em nuvem que se enquadram neste tipo de classificação.



Application Control - Add application

Lista dos aplicativos identificados como improdutivos ou de risco de segurança.

- Baidu Movies;
- CDN Content Delivery Network (mensageiros);
- Dropbox;
- Facebook (all);
- Google Drive;
- Google Drive Upload;
- Google Mail;
- Google Photos / Google + Photos;
- One Drive;
- Skype Call Start,
- Skype Call End.

Abaixo um resumo do que será configurado na regra:

- [Properties]: WEB APP Block, Action: Allow; TAG = Block;
- [Conditions]: Zona = LAN, Autenticado;
- [Inspection]: SSL Inspection, Application Control e Web Filter;
- [Routing]: Sem controles.

 \sim

Para adicionar uma política de segurança, no menu de ações [

], clique na opção "Create Policy";

IPv4 - Menu de Ações - Create Policy

Configure cada aba de acordo com as definições demonstradas à seguir.

Properties

Na aba [Properties], em Name nomeie como: "WEB - APP Block";

Em **Description** digite "WEB – APP Block";

Em Action deixe a opção "Allow", você efetuará o bloqueio através dos perfis de Web Filter e Application Control;

Em Policy Group selecione "Web Filter";

Em Tags digite "Block";

Marque a caixa de seleção Traffic Logging

| | (11) (11) | | |
|------------|--|-----------|--|
| Pagetidi | General | | |
| Conditions | * Harne | | |
| | WEB - APP Stock | | |
| Tropec5 ar | Description | | |
| Sacing | WEB - AFP Block | | |
| | * Action | Tap | |
| | Alter | diade (i) | |
| | · Policy Oreap | | |
| | Tido Piter | | |
| | Tuffic Logging | | |
| | Schedule | | |
| | Time | Scheikvie | |
| | | | |
| | Policy Orcup Twit Film Traffic Logging Schudule Time | Schebule | |

Create Policy - Ex. 3 - Properties

Selecione a próxima aba, [Conditions].

Conditions

Na aba [Conditions], em Network Zone selecione a opção: "LAN";

Em Identification marque a caixa de seleção Authenticated

| Properties | + Seerce | | | | |
|------------|----------------|-------------------|-----|---------|--|
| Constants | Metwork Jone | Betwork Interface | | Lountry | |
| | Safe . | | | | |
| Inspection | iD Adalesia | NVCAddress | | | |
| Raby | | | | | |
| | Declarition | | | | |
| | 0 40 Adelyess | Service | | Country | |
| | | | | | |
| | identification | | | | |
| | Authentituted | Gr | oum | | |
| | | | | | |

Create Policy – Ex. 3 – Conditions

Selecione a próxima aba, [Inspection].

Inspection

Na aba [Inspection], marque a caixa de seleção SSL Inspection [] e adicione um perfil que inspecione HTTPS (Para mais informações, consulte a pá gina);

Marque a caixa de seleção Application Control

Marque a caixa de seleção **Web Filter** e selecione o perfil relacionado as categorias de improdutividade ou de risco (Para mais informações, consulte a página);

| Tiopersea | sufficient | |
|------------|-----------------------|--------|
| Conditions | 331. impaction | |
| | Weld Navigation 555 | |
| impaction. | Intruska Prevention | |
| 749005 | | |
| strend. | Threat Protection | |
| | | |
| | Application Control | |
| | Relations and Landral | |
| | Web Filter | |
| | Tark Security | |
| | | |
| | | |
| | | |
| | | |
| | | Carcol |

Selecione a próxima aba, [Routing].

Routing

Na aba [Routing], nenhum controle será ativado, conforme exemplificado pela imagem a seguir:

| TOMPORT | Caterony | | | |
|------------|--------------------------|-------|-------------------|--|
| Conditions | I HAT | [] s | D-WMPy | |
| | Salarit (princip States) | | | |
| respection | | | | |
| 1000 | Qx6 | | | |
| Builting | Traffic Shaping | (C) # | ag Patkits (705) | |
| | | 1.11 | Pro 8 1997 | |
| | TUP MSS | - F | ag Packeta (05CP) | |
| | | | loss of the st | |
| | Application Routing | | | |
| | Application | 50-W | NN Profile | |
| | | | | |

| Create Policy – Ex. 3 – Routing | |
|---|------|
| Após ter configurado cada aba de acordo com a definição da política aplicada, clique em [Save]. | |
| Policy saved successfully Policy Saved Successfully | |
| A tela ilustrada na imagem a seguir será exibida: | |
| | |
| Create Policy – WEB - APP Block | |
| Após salvar, para que a política entre em ação será necessário acessar a fila de comandos [] e aplicar as alterações efetuadas. Para m informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos. | nais |

Após realizar esses procedimentos a política terá sido configurada com sucesso.

No exemplo 3 definimos e adicionamos uma políticas de bloqueio de "categorias e aplicativos" de conteúdo inapropriado ou improdutivo.

Exemplo 4 - Política de NAT- Para o Servidor MS Windows AD com destino à Base UPDATE WSUS - sem autenticação e com inspeção IPS

Vamos adicionar uma política aplicando de "NAT (Network Address Translation)" para serviços diversos. Vamos considerar o exemplo:

Mascaramento do servidor Windows para o serviço WSUS. Com o intuito de permitir o UPDATE automático sem a exigência de autenticação.

Link com a documentação da MS - Como configurar uma conexão de rede para o MS WSUS

https://technet.microsoft.com/en-us/library/cc708602(v=ws.10).aspx

Para casos específicos definir e configurar antes os objetos que serão utilizados na política.

Abaixo um resumo do que será configurado na regra:

- [Properties]: NAT: MS-WSUS Servers, Action: Allow; TAG = NAT;
- [Conditions]: Zona = WAN;
- [Inspection]: Intrusion Prevention;
- [Routing]: Habilitar [Nat]; SD-WAN= Performance BB; Traffic Shaping= Very high.

| Para adicionar uma política de segurança, no menu de ações (| ~ | 1 clique na oncão "Create Policy". | |
|---|---|------------------------------------|--|
| r ara autoinar uma pontica de segurança, no menu de ações [| | | |

| ۹ 🗲 🗸 |
|-----------------|
| Create Group |
| Delete Groups |
| Import Template |
| Save Template |
| Create Policy |
| Delete Policies |
| Expand All |
| Collapse All |

IPv4 - Menu de Ações - Create Policy

Configure cada aba de acordo com as definições demonstradas à seguir.

Properties

Na aba [Properties], em Name nomeie como: "NAT: MS-WSUS Servers";

Em Tags inclua "NAT";

Em Policy Group selecione "Masking (NAT)";

Você terá chego no resultado ilustrado pela imagem abaixo:

| Properties | General | | |
|------------|---------------------|-----------|--|
| Conditions | * Nerse | | |
| | NAT MS-WSUS Servers | | |
| Insection | Description | | |
| Rousing | | | |
| | * Action | Tep- | |
| | Wine | 647.1 | |
| | · Palicy Group | | |
| | Hashing (197) | | |
| | Tariffic Logging | | |
| | Schedule | | |
| | - Dire | Schethale | |
| | | | |

Add Policy - Ex. 4 - Properties

Selecione a próxima aba, [Conditions].

Conditions

Na aba [Conditions], em Network Zone selecione "WAN";

IP Address selecione: "Server Windows AD/LDAP" (Caso seja necessário adicionar um novo objeto, consulte esta página);

Em Service selecione "Services UPDATE MS WSUS" (Caso seja necessário adicionar um novo objeto, consulte esta página);

| Properties | S Among | | | | | |
|------------|----------------|---|--------------------|---|---------|--|
| - Meridan | | | | | | |
| Conditions | Metaanik Zone | | Retwork hitseffice | | Deentry | |
| | - tanay - | | | | | |
| Inspection | IP Addamse | | NVC Address | | | |
| Rouding | | | | | | |
| | Dectivation | | | | | |
| | S P Address | | Service | | Ceertry | |
| | | = | 14 | 注 | | |
| | Identification | | | | | |
| | Authenticated | | | | | |
| | | | | | | |

Create Policy – Ex. 4 – Conditions

Selecione a próxima aba, [Inspection].

Inspection

Na aba [Inspection], habilite a caixa de seleção de Intrusion Prevention 2] e selecione um perfil para efetuar Deep Inspection (Para mais informações, cheque a página);

| olicy Form | | x |
|------------|-----------------------------|--------|
| Properties | Imperiod | |
| Conditions | 551 Augustian | |
| Impection | 💽 Intrusian Premettion | |
| Routing | - BAARDA Sarrow, Inspection | |
| | Application Control | |
| | | |
| | Neb Hider | |
| | | |
| | | |
| | | |
| | | Canord |

Create Policy - Ex. 4 - Inspection

Selecione a próxima aba, [Routing].

Routing

Na aba [Routing], marcar a caixa de seleção NAT[

Marcar a caixa de seleção de **SD-WAN** e selecionar a opção "Performance BB";

Em Traffic Shaping selecione a opção "Very High";

| | | | | XC. |
|---|------------------------------------|---|--|--------|
| | 22.225 | | | |
| | subtacts | Carponents | 100 (ST 100) | |
| | Conditions | NAT NAT | SD-WWN | |
| | 19.19 | Televis States, States, | Aprila manual SE | |
| | 101062000 | 065 | | |
| | Baring | Coeffic Shoping | Fing Pardists (705) | |
| | | seg-sign | A DESCRIPTION | |
| | | TCP MSS | Flag Packets (05CP) | |
| | | | R Section 1 | 19 |
| | | Application Routing | | |
| | | E Informa | SD-WAN Profile | |
| | | | | |
| | | | | |
| | | | | |
| | | | | Caseri |
| | | | Save | |
| s ter configurado | o cada aba de a | cordo com a definição da polít V F | tica aplicada, clique em [Save] Policy saved successfully Policy Saved Successfully | |
| s ter configurado la ilustrada na in | o cada aba de a nagem a seguir | cordo com a definição da polít V F será exibida: | Save | |
| s ter configurado la ilustrada na in | o cada aba de ad nagem a seguir | cordo com a definição da polít P será exibida: | Save | |
| ós ter configurado | nagem a seguir | cordo com a definição da polít F será exibida: Create Polic, | Save Save Policy saved successfully Policy Saved Successfully Policy Saved Successfully y – Ex. 4 – NAT: MS-WSUS Servers. | |

Após realizar esses procedimentos a política terá sido configurada com sucesso.

Observar a necessidade de ordenar/reordenar as políticas.

Neste caso não vamos precisar reordenar.

۲

As políticas estão bem definidas, a regra de NAT do servidor Windows AD/LDAP bem específica considerando "Origem/Destino", inclusive as portas de serviço.

As políticas de acesso e filtros WEB com inspeção e ordenadas de forma que aplicam 1º os bloqueios, depois a permissão.

Dessa maneira "não conflitante" com outras políticas, atendendo as especificações do modelo de políticas apresentadas e as considerações e "Dicas Importantes" mencionadas no capítulo anterior.

Ex.: Objeto endereço "Servidores Wsus" ver lista de endereços na documentação em nota;

Objeto serviços "Service UPDATE MS WSUS". Ver lista de portas na documentação em nota;

No exemplo 4 definimos uma políticas de redirecionamento para efetuar update sem precisar de autenticação.

Exemplo 5 - Política de NAT para todos os protocolos com IPS e Proxy

Neste exemplo iremos configurar uma política que engloba todos os protocolos para usuários autenticados com inspeção ATP e Proxy para as portas de navegação HTTP e HTTPS com Inspeção SSL.

Abaixo um resumo do que será configurado na regra:

- [Properties]: Allow all with IPS + PROXY, TAG = IPS, NAT, PROXY;
- [Conditions]: Zona de rede "LAN", Autenticado;
- [Inspection]: SSL Inspection, Intrusion Prevention;
- [Routing]: Habilitar [Nat], QOS: Prioridade Média (Reserva 50% link).

| Para adicionar uma política de segurança, no menu de ações [| ~ |], cl | lique r | na o | pção | "Create F | Policy | v "; |
|--|------|-------|---------|------|------|-----------|--------|-------------|
| | ٩ | | ÷ | | ~ |] | | |
| | Crea | ate (| Grou | ıp | | | | |
| | Del | ete (| Grou | ıps | | | | |
| | Imp | ort | Tem | pla | ate | | | |
| | Sav | e Te | mpl | ate | 2 | | | |
| | Crea | ate I | Polic | y | | | | |
| | Del | ete I | Polic | ies | 3 | | | |
| | Ехр | and | All | | | | | |
| | Col | laps | e All | l | | | | |

IPv4 - Menu de Ações - Create Policy

Configure cada aba de acordo com as definições demonstradas à seguir.

Properties

Na aba [Properties], em Name nomeie como: "Allow all with IPS + Proxy";

Em Description digite "Allow all with IPS + Proxy";

Em Tags inclua "IPS", "NAT" e "PROXY";

Em Policy Group selecione "Masking (NAT)";

Você terá chego no resultado ilustrado pela imagem abaixo:

| Properties | General | | |
|------------|-----------------------------|------------------------|--|
| Conditions | * Serve | | |
| | Mow all with IPS # Prove | | |
| Insection | Description | | |
| Routing | Millow all with IPS + Prosy | | |
| | * Action | Tep | |
| | Alas | -PE 1 - 447 1 - PR07 1 | |
| | · Policy Group | | |
| | Masking (1971 | | |
| | Forth: Legging | | |
| | Schedule | | |
| | 1 Dire | Schether | |
| | | | |
| | | | |

Create Policy - Ex. 5 - Properties

Selecione a próxima aba: [Conditions].

Conditions

Na aba [Conditions], em Network Zone selecione: "LAN";

Marque a caixa de seleção Authenticated.

| Romantias | | | | | |
|------------|----------------|-------------------|--------|---------|--|
| autheriota | + 2011/08 | | | | |
| Conditions | Network Zone | Retwork hiterface | | Deenkry | |
| | LAH | | | | |
| Impection | IP Addamse | NAC Address | | | |
| Reading | | | | | |
| | Dectrotion | | | | |
| | 10 Aduleuro | Service | | Ceerby | |
| | | | | | |
| | identification | | | | |
| | Authenticated | - 32 | Snoups | | |
| | | | | | |

Create Policy – Ex. 5 – Conditions

Selecione a próxima aba: [Inspection].

Inspection

Na aba [Inspection], habilite a caixa de seleção de SSL Inspection []] e selecione um perfil para inspecionar SMTP, POP3, FTP, HTTP, HTTPS e SS L (Para mais informações, consulte esta página);

Habilite a caixa de seleção de Intrusion Prevention [

Marque a caixa de seleção Web Filter [] e selecione o perfil desejado (Para mais informações, consulte esta página);

| Properties | Ingetion | |
|------------|-----------------------|--|
| Conditions | SSL impection | |
| | Welt Assess Filtering | |
| importion. | 🛃 Intruska Prevantion | |
| 10000 | Aduar Termin | |
| | Tivest Protestiev | |
| | Application Control | |
| | | |
| | 🔄 Web Filter | |
| | acaty en | |
| | | |
| | | |
| | | |
| | | |

Selecione a próxima aba: [Routing].

Routing

Na aba [Routing], marcar a caixa de seleção Nat,

Marcar a caixa de seleção de SD-WAN e selecionar a opção "Load Balance BB";

Em Traffic Shaping selecione a opção "Medium";

| Policy Form | | × | |
|--|---|--|--------|
| | | | |
| Properties | Sisteway | | |
| Conchiona | tran 🔤 | SD-WAY | |
| | Interfaces (noted | sala lanatas kii 🦿 👘 | |
| Inspartion | Quố | | |
| Reality | Truffic Shaping | Plag Padvets (T06) | |
| | miker v | WORKS AND IN THE OWNER AND INTERPORT AND INTER | |
| | TCP MSS | Fing Pedvets (DSCP) | |
| | | a bilan | |
| | Application Reading | | |
| | Ambraian | SD WAN Profile | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Contrast. Contrast. Contrast. | |
| | Create Policy – Ex. 5 – | Routing | |
| | | | |
| | | | |
| | | Save | |
| Após ter configurado cada aba de ac | ordo com a definição da política aplicada, clique | em []. | |
| | | | |
| | Policy saved succ | sesfully | |
| | Policy Saved Succes | set ully | |
| | | Grany | |
| | | | |
| A tela ilustrada na imagem a seguir s | erá exibida: | | |
| | | | |
| - Barris di alta di a | | | |
| | F 8 F 9 | | |
| | Create Policy – Ex. 5 – Allow all v | vith IPS + PROXY | |
| | | | |
| | | | |
| | | 0 | |
| Após salvar, para que a política entre | em ação será necessário acessar a fila de con | nandos [] e aplicar as alterações efetuadas. Para | a mais |
| informações a respeito da fila de con | nandos acesse a página: UTM - Fila de comando | S. | |
| | | | |
| Após realizar esses procedimentos a | política terá sido configurada com sucesso. | | |
| | - | | |
| Prontol Agora é só anlicar alguns te | stes | | |
| | | | |
| Para tanto, use uma estação de traba | alho devidamente configurada e navegue na WE | B. | |

Depois verifique os registros de Tráfego no Dashboard.

IPv4 - Menu de ações - Delete Policies

O botão "Delete Policies" deleta as Políticas selecionadas. Para deletar, siga os passos:

1. Selecione a(s) Política(s) que deseja deletar. Para selecionar, clique com o *mouse* no *checkbox*. Nos pacotes selecionados o *checkbox* mudará da cor cinza para azul []]. Ex.: *Test 1* e *Test 2*;

| ar or Groun 1 | | | | | | | | |
|------------------------------------|---------------|---------------|-----------|-----------------|---------|------|---------|-------|
| 1 44 241 | | | - | | - | | E3CD G1 | 0/200 |
| | ÷. | 10 | | 0 | 3 | 140 | 888 | -110- |
| 100 Test 5. | 365 | 100 | 199 | 0 | - | 1140 | | 0/800 |
| | Po | líticas selec | ionadas p | ara serem de | letadas | | | |
| | | | | | | | | |
| | | | | | | | | |
| ~ | | | | | | | | |
| 2. No menu de ações [], clique na | opção "Delete | e Policies"; | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | ٩ | $\mathbf{\sim}$ | | | | |
| | | | Create Gr | roup | | | | |
| | | | Dalata Gr | 0000 | | | | |
| | | | Delete Of | oups | | | | |
| | | | Create Po | olicy | | | | |
| | | | Dalata Pr | licies | | | | |
| | | | Deleteri | Jucies | | | | |
| | | | Expand A | AII | | | | |
| | | | | | | | | |
| | | | Collapse | All | | | | |

Policies IPv4 - Menu de Ações - Delete Policies

3. Surgirá a tela perguntando se deseja deletar os itens:

| Are you sure? | × |
|---|--------|
| Are you sure you want to delete the following policys ? • Test 1 • Test 2 | |
| Cancel | Delete |

Policies IPv4 - Are you sure you want to delete the following policies



As Policies foram removidas com sucesso.

IPv4 - Menu de ações - Expand All e Collapse All

O botão "Expand All" tem como finalidade expandir o grupo de políticas. Para expandir o grupo de políticas, siga os seguintes passos:

1. No menu de ações, clique na opção "Expand All" para expandir os grupos de políticas expandidas;



Policies IPv4 - Menu de ações - Expand All

2. Ao clicar em "Collapse All" no menu de ações acontece justamente o contrário.



Policies IPv4 - Menu de ações - Collapse All
IPv4 - Menu de ações - Validate Policies

O botão "Validate Policies" serve para verificar a existência de Políticas redundantes, em duplicidade, ou em condição de ofuscamento (sobreposição).





1. No menu de ações, clique na opção "Validate Policies" para que o sistema verifique conflitos e redundâncias entre as Políticas vigentes;



Policies IPv4 - Menu de ações - Validate all policies

Ao fazer a validação, é importante checar as notificações no canto superior direito da tela para verificar o resultado. Logo após, devemos também atualizar a página, clicando no botão refresh da página de seu navegador.

A validação de políticas pode retornar os seguintes status das políticas:

Parâmetros iguais com ações diferentes: Em caso de duas Políticas nominarem a mesma origem e o mesmo destino, mas as ações serem contra dizentes. Por exemplo, ação liberar navegação em uma Política e restringir a navegação em outra, mas para a mesma origem e o mesmo destino.

Duplicidade: Ocorre quando duas políticas compreendem as mesmas ações, origem e destino.

Ofuscamento: Ocorre quando uma Política sobrepõe a outra em termos de ação, ou seja a ação descrita já é feita por uma anterior.

É importante lembrar que a priorização das regras é top-down dentro do Firewall.

Deste modo, pudemos analisar as opções disponíveis no menu principal de Políticas IPv4.

IPv4 - Colunas

A tela Policies - IPv4 exibe informações mais detalhadas das políticas criadas.

| LA Pilet | | | | | | | | |
|---|------|----|-----------|-------|------------------------|-----|-----|-------|
| 1.11.1 | | | | | | | | |
| n Ros | | | | | | | | 1.41 |
| c is forward (FR) | | | | | | | | 0.23 |
| o v Hanking (HAD) | | | | | | | | |
| , The block of an entry | - | | - | : | 1.4 | - | 8.0 | 0/0 |
| THE APPLICATION OF | | = | ing toget | | Server, Partiel Web | - | - | 0/81 |
| -WARNEY | | | | | | | | 121 |
| THE OWNER WATER | | - | - | | | 1.1 | | 0701 |
| tion (19.4: Area- | | 10 | | S. 44 | Suist, No. 1 | - | 888 | 4.000 |
| INT Performance | 1.00 | 12 | | ° | - | | - | |
| In the barry service of the service | - | | | ÷ | - | | - | 0/81 |

IPv4 - Policies

O topo do painel Policy contém:

- Nome do Pacote: Apresenta o nome do Pacote de Políticas cadastrado;
- Versão do Sistema []: Apresenta a versão na qual o Pacote de Políticas foi criado. É de extrema importância criar Pacotes de Políticas da mesma versão que o UTM, caso contrário, o pacote não será compatível;
- IP[]: Representa o tipo de IP utilizado nos Pacotes de Políticas criados. Ex.: "IPv4"; Barra de Busca: Tem como função possibilitar a localização de itens específicos, é possível clicar em alguns campos das colunas dentro do grupo de política para servir como filtro em uma busca mais específica, para mais informações cheque esta página.

- Menu de Ações []: Apresenta o seguinte conjunto de opções contextuais:
 - Create Group;
 - Delete Groups;
 - Create Policy;
 - Delete Policies;
 - Expand All e Collapse All;
 - Validate Policies.
- · Pre Rules: Caso um GSM esteja vinculado a este UTM, representa todos os grupos de políticas que foram colocadas para atuar antes das políticas locais do UTM, portanto elas possuem prioridade sobre as políticas criadas no próprio UTM;
- Local Rules: Representa as regras dos grupos de política criadas no próprio UTM;
- Post Rules: Todos os grupos de políticas criadas que serão irão entrar em vigor somente depois das políticas locais do UTM, portanto elas terão menor prioridade e serão instaladas abaixo dos grupos de políticas já existente no UTM.

É importante, lembrar que as políticas são ordenadas por "Prioridade", sendo que elas são aplicadas considerando o método "First Match Wins" (Que literalmente quer dizer "O 1º entre os concorrentes VENCE"). Logo, as políticas localizadas acima tem prioridade enquanto as abaixo possuem menor prioridade.

Cada grupo de política contém os seguintes botões:

-] Ao clicar e arrastar, move a ordem do grupo e permite reorganizar a prioridade de acordo com qual grupo está acima (First Match Wins);
- [2] Expande para exibir as políticas criadas no grupo;

- [1] Informa quantas políticas existe no grupo;
- [Permite editar as configurações adicionadas na opção Create Group do menu de ações;
- [Deleta o grupo inteiro;
- [-] Seleciona o grupo de modo a interagir com o menu de ações.

As colunas de dentro de cada grupo de política são divididas em:

- Move [:]: Ao clicar e arrastar, move a ordem da política e permite reorganizar a prioridade de acordo com qual política está acima (First Match Wins);
- Id [#8]: Exibe o número de identificação da política, é possível clicar nele para servir como filtro no campo de busca;
- Rule: Exibe o nome da política;
- User: Determina quais usuários são afetados pela política, é possível clicar neste campo para servir como filtro no campo de busca;
- Source: Exibe se a origem desta regra será a Zona de rede, endereço *IP*, interface de rede, *Mac Address* ou qualquer um destes, é possível clicar neste campo para servir como filtro no campo de busca;
- Destination: Determina o destino da regra, o endereço IP ou serviço, é possível clicar neste campo para servir como filtro no campo de busca;
- Schedule: Exibe caso a regra depende de um período de tempo ou agendamento, é possível clicar neste campo para servir como filtro no campo de busca;
- Services: Exibe os serviços que a regra afeta, é possível clicar neste campo para servir como filtro no campo de busca;
- Tags: Exibe as tags que foram adicionadas à essa regra, é possível clicar neste campo para servir como filtro no campo de busca;
- Modules: Determina com quais módulos do UTM a regra irá interagir, é possível clicar neste campo para servir como filtro no campo de busca;
 Action: Exibe alguns botões contextuais e qual ação a regra executa.
 - Enabled[] ou Disabled[]: Através deste seletor, ativa ou desativa a regra;
 - Edit[]: Permite editar as configurações adicionadas na opção Create Policy do menu de ações;
 - Clone[^C]: Copia a política. Atente que ao usar essa opção, a política copiada usará o mesmo nome da política original, porém adicionará um número na frente (por exemplo, se eu copio a política "Test" a cópia se chamará "Test (1)") e ficará automaticamente abaixo da política original, portanto, levando em consideração o "First Match Wins", é importante mover a política de acordo com a prioridade desejada;
 - **Delete**[**1**]: Remove a política;
 - Select[]: Permite a seleção das políticas de modo a interagirem com o menu de ações;
 - Action: Determina o comportamento da política em questão, tendo como possibilidades:



A seguir analisaremos as políticas de IPv6.

Políticas IPv6

Esta seção irá analisar cada componente da interface de criação de políticas *IPv6*. As definições são idênticas para *IPv4* e *IPv6*, sofrendo alterações somente em seus endereçamentos e em algumas características proprietária a cada versão do protocolo.

Caso não esteja já selecionado, clique na opção "IPv6";



Surgirá a Tela de "Policies IPv6", conforme demonstrado pela imagem a seguir:

| ♦ 2.0 1 ^j ipv6 | |
|---------------------------|--|
| V Local Rulics | |
| | |
| | |
| | |
| | |

IPv6

Esta seção irá se aprofundar em:

- Criação de grupos de políticas;
- Cadastro e Remoção de políticas.

A seguir, vamos analisar cada componente deste painel.

IPv6 - Menu de ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



n vo mena ac açe

O menu é composto das seguintes opções:

- Create Group;
- Delete Groups;
- Create Policy;
- Delete Policies;
- Expand All e Collapse All.

A seguir cada opção do menu de ações será detalhada.

| IPv6 - Menu de ações - Cr | reate Group |
|---|---|
| | |
| Atraves da opção "Create Group" e possível criar um novo grupo Clique na opção "Create Group"; | . Para acessar, clique no menu de ações []. |
| | ۹ 🗸 |
| | Create Group |
| | Delete Groups |
| | Create Policy |
| | Delete Policies |



2. A tela "Create Group" será exibida. Adicione o nome do grupo desejado:

| | Create Group X |
|---------------------------------|---|
| | * Name |
| | Cancel Save |
| | IPv6 – Create Group |
| Após nomear o gri Save]. | upo, caso deseje cancelar clique no botão <i>Cancel</i>]. Para concluir a criação do grupo clique no botão <i>Save</i> [|
| | Group created successfully Group created successfully |

O grupo foi criado com sucesso.

IPv6 - Menu de ações - Delete Groups

Através do botão "Delete Groups" é possível deletar vários grupos instalados ao mesmo tempo. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) grupo(s) deseja deletar clicando no *checkbox*[___], como demonstrado pela imagem abaixo:



IPv6 - Menu de ações - Delete Groups

3. Surgirá a mensagem se deseja realmente deletar os pacotes selecionados:



Após realizar esses procedimentos os grupos terão sido excluídos com sucesso.

IPv6 - Menu de ações - Create Policy

O botão "Create Policy" cria as políticas no grupo de políticas selecionando, para que ele esteja disponível, é necessário que um grupo tenha sido criado previamente (consulte esta página para mais informações).

Para criar uma política, siga os passos:

1. No menu de ações [], clique na opção "Create Policy"; Create Group Delete Groups Import Template Save Template Create Policy Delete Policies Expand All Collapse All

IPv6 - Menu de Ações - Create Policy

2. Surgirá a tela Policy Form;

| Pegartai | General | | |
|------------|-------------------|----------|--|
| Connectice | + Marse | | |
| heador | Description | | |
| Surve | | | |
| | · Arthury | Taga . | |
| Adjorice# | Alleria | | |
| | * Pelles Group | | |
| | | | |
| | C Taffic Parities | | |
| | Snetuk | | |
| | Titte | Schedule | |
| | | | |

IPv6 – Policy Form

Esta janela é organizada pelas seguintes abas:

- Properties;
 Connection;
 Inspection;
 Routing;
 Advanced.

A seguir explicaremos cada campo desta janela.

IPv6 - Create Policy - Aba Properties

Na aba [Properties] é obrigatório definir um nome e descrição para a política e opcionalmente podem ser definidas Tags que auxiliam na organização e facilitam a busca de políticas.



IPv6 - Abas Laterais - Properties

Nesta aba estão contidos os painéis:

- General;
- Schedule.

A seguir analisaremos a função de cada campo dos painéis.

General

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [General]:

| Properties | General | | |
|------------|--------------------|------|--|
| Connection | * Name | | |
| Impection | Description | | |
| Routing | | | |
| | * Action | Tags | |
| Advented | Allan | | |
| | · Policy Group | | |
| | | | |
| | 📴 Traffic Mamittar | | |
| | Traffic Logging | | |

- Name: Definir nome para política;
- Description: Definir descrição para política;
- Action: Determina o comportamento da política em questão, tendo como possibilidades:
 - Allow: Como o próprio nome diz, a ação Allow serve para conceder acesso e deixar o tráfego livre de bloqueios;
 - Deny: A ação Deny bloqueia o tráfego mas não informa ao endereço de origem que o serviço está sendo bloqueado. Ou seja, neste cenário, para o endereço da origem da conexão, não é possível saber se tem um firewall interceptando a conexão ou simplesmente o serviço não está ativo;
 - Reject: A ação Reject notifica ao endereço de origem que o serviço foi bloqueado por um Firewall, sendo que este envia um pacote ICMI indicando que o serviço está inacessível.
- Tags: Esta opção permite definir Tags de forma que o administrador consiga usá-las como "Filtro" para suas pesquisas tomando-as como base em suas definições. Por padrão o sistema define um "nome" para as Tags por tipo de recurso em uso habilitado na política;
- Policy Group: Através dessa opção é possível incluir a política em questão dentro de um grupo de políticas;
- Traffic Monitor: Com esta opção checada [, as informações das sessões que derem "match" com a política criada, serão coletadas pelo serviço de monitoramento.
- Traffic Logging[]: Essa caixa de checagem, caso seja habilitada fornece a opção de gerar o relatório de uma determinada política. As opções de Traffic Loging são configuradas em Settings System Aba Logging.

Caso pretenda utilizar *Netflow*, ele precisa ser habilitado opcionalmente pelo administrador nas configurações de *Traffic Logging* do sistema. Para mais informações, consulte esta página.

Schedule

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Schedule]:

| Schedule | | | |
|----------|------------------|---------------|--|
| Time . | | Schedule | |
| | | | |
| | IPv6 – Propertie | es - Schedule | |

- Time]: Caso a caixa de seleção estiver selecionada, determina se a regra se aplicará em dias úteis ("Business"), finais de semana ("Weekenc") ou em algum outro objeto do tipo "Time" que tenha sido criado previamente;
- Schedule J: Caso a caixa de seleção estiver selecionada, permite determinar se a regra se aplicará em relação a um objeto "Period/Date" que tenha sido criado previamente.

A seguir analisaremos o conteúdo da aba Connection.

- Inspection;
- Routing;
- Advanced.

IPv6 - Create Policy - Aba Connection

A aba [Conditions] fornece diversos filtros para especificar o escopo de origem e destino, sendo obrigatório a escolha de pelo menos um filtro.



Nesta aba estão contidos os painéis:

- Source;
- Destination;
- Identification.

A seguir analisaremos a função de cada campo dos painéis.

Source

O painel [Source] oferece vários filtros com função de determinar o escopo de origem, como já mencionado anteriormente, é necessário selecionar ao menos um filtro. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Source]:

| Network Zone | Not | work interface | Country | |
|--------------|-----|----------------|---------|--|
| | | | | |
| IP Address | MA | C Address | | |
| | | | | |

Network Zone []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar interfaces de rede que podem ser sinalizadas com siglas como LAN, WAN e DMZ para facilitar a organização e criação de políticas segmentando por tipo rede. As zonas de rede que aparecem nesse menu são criadas em Network - Interfaces;

| Network Zone | |
|------------------------------------|---------|
| | ^ |
| DMZ | |
| LAN | |
| SDWAN | |
| WAN | |
| IPv6 – Conditions - Source - Netwo | rk Zone |

• Network Interface Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar interface de rede para serem utilizadas como filtro de origem. As interfaces que aparecem nesse menu são criadas em Network - Interfaces;

| Network Interface | |
|--------------------------------------|-----------|
| | ~ |
| eth0 | |
| eth1 | |
| eth2 | |
| eth3 | |
| tun0 | |
| IPv6 – Conditions - Source - Network | Interface |

• IP Address Z: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de Endereço IPv6 (IPs

, redes ou conjuntos) para serem utilizados como filtro de origem. Ao clicar sobre o botão [IIII], a tela abaixo será exibida para selecionar um ou mais objeto de endereço que irá compor a regra. Os endereços que aparecem nesse menu são criados em *Settings* - *Objects*;

Esta lista é populada especificamente por objetos de endereço IPv6. Atente-se de selecionar a opção correta em "*Type*" ao criar um novo objeto de endereço.

| Add IP Address | | × |
|----------------|--------|-----------------------|
| All 🗸 | c | • |
| Item | | |
| IPv6 | | |
| | | < 1 > |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Cancel | Save |
| | | |

IPv6 – Conditions - Source - IP Address

• MAC Address Z: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de Endereço Mac

Address para serem utilizados como filtro de origem. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar um ou mais objeto de MAC address que irá compor a regra. Os endereços que aparecem nesse menu são criados em Settings - Objects;

| Add MAC | Address | | Х |
|---------|-----------------------|--------|-------|
| All | \sim | c | • |
| | Item | | |
| | Mac Address Example 1 | | |
| | Mac Address Example 2 | | |
| | | | < 1 > |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Cancel | Save |

• Country

Add Country

٣

| All | | ۹ 🗸 |
|-----|-------------|------------------|
| | Item | |
| | 🚾 Argentina | |
| | Armenia | |
| | 🔲 Aruba | |
| | australia | |
| | 📃 Austria | |
| | Azerbaijan | |
| | 🗾 Bahamas | |
| | Bahrain | |
| | Bangladesh | |
| | Barbados | |
| | | < 1 2 3 4 5 26 > |
| | | Cancel Save |

1.7

X



Destination

 E^{-1}

O painel [Destination] fornece diversos filtros para especificar o escopo de destino, sendo obrigatório a escolha de pelo menos um filtro. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Destination]:

| IP Address | Service | 1 | Country | |
|------------|---------|-------|---------|--|
| | | 1 = 1 | | |

• IP Address Z : Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de Endereço IPv6 (IPs

, redes ou conjuntos) para serem utilizados como filtro de destino. Ao clicar sobre o botão [], a tela abaixo será exibida para selecionar um ou mais objeto de endereço *IP* que irá compor a regra. Os endereços que aparecem nesse menu são criados em *Settings* - *Objects*;

Esta lista é populada especificamente por objetos de endereço IPv6. Atente-se de selecionar a opção correta em "*Type*" ao criar um novo objeto de endereço.

| Address | | х |
|---------|-------------------------|---------|
| v | ٩ | ~ |
| ltem | | |
| IPv6 | | |
| | < | 1 > |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Cancel | Save |
| | Address Item IPv6 | Address |

IPv6 - Conditions - Destination - IP Address

• Service [:]: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de serviços (protocolos e portas) utilizados como filtro de destino. Ao clicar sobre o botão [:], a tela abaixo será exibida para selecionar um ou mais objeto de serviço que irá compor a regra. Os endereços que aparecem nesse menu são criados em Settings - Objects;

| Add Serv | vice | × |
|----------|--------|-----------------|
| All | ~ | ۹ 🗸 |
| | Item | |
| | АН | |
| | AOL | |
| | BGP | |
| | DHCP | |
| | DHCPV6 | |
| | DNS | |
| | ESP | |
| | FTP | |
| | GRE | |
| | H323 | |
| | | < 1 2 3 4 5 6 > |
| | | Cancel Save |

IPv6 – Conditions - Destination - Service

• Country []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Países para serem usado como filtro de destino. Ao clicar sobre o botão []; a tela abaixo será exibida para selecionar um ou mais país que irá compor a regra.

Add Country

٣

| All | | | | ٩ | ~ |
|-----|--------------|-------|--------|-------|------|
| | Item | | | | |
| | I Argentina | | | | |
| | Armenia | | | | |
| | Aruba | | | | |
| | 📷 Australia | | | | |
| | Austria | | | | |
| | 🔤 Azerbaijan | | | | |
| | 🗾 Bahamas | | | | |
| | Bahrain | | | | |
| | Bangladesh | | | | |
| | Barbados | | | | |
| | | < 1 2 | 345 | ••• 2 | 6 > |
| | | | Cancel | | Save |

37

X



Identification

 E^{-1}

O painel [Identification] permite habilitar o recurso de autenticação para a política. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Identification]:

| Authenticated | | |
|---------------|--------|--|
| Users | Groups | |
| | | |

- Authenticated S: Caso habilitada, esta caixa de seleção determina se a política exige autenticação;
 Users S: Este campo só fica disponível ao marcar a caixa de checagem e a opção Authenticated. Permite especificar usuário(s) aos quais a política será aplicada. Ao clicar sobre o botão [🗮], a tela abaixo será exibida para selecionar um ou mais usuário que irão compor a regra;

| Add User | Х |
|----------|-------------|
| All V | ۹ 🗸 |
| Item | |
| No Data | |
| | |
| | |
| | |
| | |
| | Cancel Save |

• Groups []: Este campo só fica disponível ao marcar a caixa de checagem e a opção Authenticated. Permite especificar grupo(s) em que a política se aplica. Ao clicar em []], a tela abaixo será exibida para selecionar um ou mais grupos que irão compor a regra.

| Add Group | Х |
|-----------|-------------|
| All V | ۹ 🗸 |
| Item | |
| No Data | |
| | |
| | |
| | |
| | |
| | Cancel Save |

IPv6 – Conditions - Destination - Groups

A seguir analisaremos o conteúdo da aba Inspection.

- Routing; Advanced.

IPv6 - Create Policy - Aba Inspection

Na aba [Inspection] é possível selecionar vários recursos para inspeção do tráfego afetado pela política.



Esta aba contém o painel

Inspection.

Inspection

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Inspection]:

| Inspection | |
|----------------------|----|
| SSL Impection | |
| | |
| Intrusion Prevention | |
| | ×. |
| Threat Protection | |
| | |
| Application Control | |
| | |
| Web Filter | |
| | |



- SSL Inspection [SSL inspection]: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite interceptar o tráfego SSL permitindo a inspeção do seu conteúdo. As opções que aparecem nesse menu são criadas em Proxy SSL Inspection;
- Intrusion Prevention []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite aplicar IPS nas políticas. Os perfis exibidos nesse menu são criados em Services Intrusion Prevention;

- Threat Protection []: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite aplicar IPS nas políticas. Os perfis exibidos nesse menu são criados em Services Threat Protection;
- Application Control [2]: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar um perfil para aplicar controle de acesso à aplicações. Os perfis exibidos nesse menu são criados em Services Application Control;
- Web Filter [1]: Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar um perfil para efetuar a filtragem de conteúdo. Os perfis exibidos nesse menu são criados em Services Web Filter.

A seguir analisaremos o conteúdo da aba Routing.

• Advanced.

IPv6 - Create Policy - Aba Routing

Na aba [Routing] você configura os NAT, perfil de SD-WAN, QoS, entre outros que serão detalhados abaixo. A seguir analisaremos a função de cada campo dos formulários.



Nesta aba estão contidos os painéis:

- Gateway
- QoS
- Application Routing.

A seguir analisaremos a função de cada campo dos painéis.

Gateway

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [Gateway]:

| altow by | |
|------------------------|--|
| NAT | |
| Salach Ratanag Printed | |

IPv6 - Routing - Gateway

• NAT Permite ativar o NAT e a escolha do endereço para tradução de origem, por padrão é configurado o IP do link do Gateway Padrão;

NAT

| Default Gateway (Masked) | ^ |
|--------------------------|---|
| Default Gateway (Masked) | |
| eth0 - 172.31.102.220 | |
| eth1 - 172.31.102.1 | |
| tun0 - 20.0.0.1 | |

IPv6 - Routing - Gateway - NAT

QoS

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel [QoS]:

| Traffic Shanlos | | Flag Packets (TOS) | |
|---------------------|----|--------------------|--|
| trout propring | | | |
| leg law, | ×. | Historian and | |
| Flag Packets (DSCP) | | | |
| 1. Dest Citato | | | |

IPv6 – Routing - QoS

Traffic Shaping []: Permite ativar e selecionar a prioridade do tráfego, os valores podem ser ajustados em System >> Network >> Traffic Shaping;

| Traffic Shaping | |
|--|---|
| Very Low | ^ |
| Very Low | |
| Low | |
| Medium | |
| High | |
| Very High | |
| IPv6 – Routing - QoS - Traffic Shaping | |

Flag packets (TOS) [Ao ativar permite a marcação do pacote conforme as opções: Espera mínima, Processamento máximo, Confiança máximo, Custo mínimo e prioridade normal;



• Flag packets (DSCP)

| | Flag Packets (DSCP) | | | | | |
|---|--|---|--|--|--|--|
| | BE (Best Effort) | | | | | |
| | BE (Best Effort) | ^ | | | | |
| | EF (Expedited Forwarding) | | | | | |
| | AF11 (Assured Forwarding) Priority Low | | | | | |
| | AF12 (Assured Forwarding) Priority Medium | | | | | |
| ł | AF13 (Assured Forwarding) Priority High | | | | | |
| | AF21 (Assured Forwarding) Immediate Low | | | | | |
| | AF22 (Assured Forwarding) Immediate Medium | | | | | |
| ļ | AF23 (Assured Forwarding) Immediate High | ~ | | | | |
| | IPv6 – Routing - QoS - Flag packets (DSCP) | | | | | |

Analisaremos a seguir a aba Advanced.

IPv6 - Create Policy - Aba Advanced

Na aba [Advanced] é possível configurar os parâmetros limite dos pacotes por segundo em uma conexão.



Advanced

Abaixo segue uma descrição da função dos campos do formulário Advanced:

IPv6 - Inspection - advanced

DoS Protection: Com a caixa de *DoS Protection* checada [1] é possível limitar a quantidade máxima de pacotes por segundo no *Firewall*, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede.

- Packet Rate: A opção Packet Rate configura o Firewall para limitar as conexões a um valor máximo de pacotes por segundo.
- Burst Rate: A opção Burst Rate configura o Firewall para permitir inicialmente uma quantidade máxima de pacotes por segundo sem validar o Pa cket Rate, permitindo assim flexibilizar o controle de tráfego para picos de tráfego ocasionais.

Options:

• TCP MSS [2]: Permite definir um valor que especifica a maior quantidade de dados, especificada em bytes, que um computador ou dispositivo de comunicações pode receber em um único segmento TCP.

Deste modo concluímos nossa análise das configurações de políticas IPv6.

IPv6 - Menu de ações - Delete Policies

O botão "Delete Policies" deleta as Políticas selecionadas. Para deletar, siga os passos:

1. Selecione a(s) Política(s) que deseja deletar. Para selecionar, clique com o *mouse* no *checkbox*. Nos pacotes selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Policy 1* e *Policy 2*;

| | 100000000 | | | | | | | | 0.00 |
|-------------|--------------------|-------------------|----------------|--|-----------------------------------|----------|---|-----------|--------|
| | + IDD makes | | 1000 | | | | | #29(2) F3 | |
| | 1910000000 | - | 10 | 100 | 0.000 | 100 | | 288 | al the |
| | 11 MB(Print 2 | - | 5 | - | | - 44 | - | 888 | |
| | | Pr | olíticas selec | cionadas p | ara serem d | eletadas | | | |
| | | FU | Jinicas selet | Jonauas p | | elelauas | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| No money de | | a na anaña "Dalat | ha Daliaiaa". | | | | | | |
| No menu de | e ações [], ciiqu | e na opçao Delet | e Policies ; | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | Create G | quo | | | | |
| | | | | Create G | roup | | | | |
| | | | | Create Gi Delete Gr | roup | | | | |
| | | | | Create Gi Delete Gr | roup | | | | |
| | | | | Create Gr Delete Gr Create Po | roup roups blicy | | | | |
| | | | | Create Gi Delete Gi Create Po | roup roups blicy | | | | |
| | | | | Create Gr Delete Gr Create Po Delete Po | roup roups blicy blicies | | | | |
| | | | | Create Gr Delete Gr Create Po Delete Po | roup roups blicy blicies | | | | |
| | | | | Create Gr Delete Gr Create Po Delete Po Expand A | roup roups blicy blicies | | | | |

Policies IPv6 - Menu de Ações - Delete Policies

3. Surgirá a tela perguntando se deseja deletar os itens:

| Are you sure? | × |
|--|----|
| Are you sure you want to delete the following policy ? • Policy 2 | |
| Cancel Delet | te |

Policies IPv6 - Are you sure you want to delete the following policies



As Policies foram removidas com sucesso.

IPv6 - Menu de ações - Expand All e Collapse All

O botão "Expand All" tem como finalidade expandir o grupo de políticas. Para expandir o grupo de políticas, siga os seguintes passos:

1. No menu de ações, clique na opção "Expand All" para expandir os grupos de políticas expandidas;



Policies IPv4 - Menu de ações - Expand All

2. Ao clicar em "Collapse All" no menu de ações acontece justamente o contrário.



Policies IPv4 - Menu de ações - Collapse All
IPv6 - Colunas

A tela Policies - IPv6 exibe informações mais detalhadas das políticas criadas.

| New York | | | | | | | | |
|------------------------------|---|-------|-----|---------|-----|------|--|-------------------|
| Levelhow | | | | | | | | |
| - Bright | | | | | | | | 5 / 1 |
| ALC: NAMES OF TAXABLE PARTY. | | 20122 | | 1000 | 100 | 1.00 | and the second s | COLUMN TWO IS NOT |
| Mill Andrew Control Public | - | ÷ | 100 | (n. 100 | - | - | | 0/8 |
| 1 (http:/ | | | | | | | | 5.74 |
| 022314123 | | | | | | | | 01002 |

IPv6 - Policies

O topo do painel Policy contém:

- Nome do Pacote: Apresenta o nome do Pacote de Políticas cadastrado;
- Versão do Sistema []: Apresenta a versão na qual o Pacote de Políticas foi criado. É de extrema importância criar Pacotes de Políticas da mesma versão que o UTM, caso contrário, o pacote não será compatível;
- IP[]: Representa o tipo de IP utilizado nos Pacotes de Políticas criados. Ex.: "IPv6";
- Barra de Busca: Tem como função possibilitar a localização de itens específicos, é possível clicar em alguns campos das colunas dentro do grupo de política para servir como filtro em uma busca mais específica, para mais informações cheque esta página.
- Menu de Ações [
 -]: Apresenta o seguinte conjunto de opções contextuais:
 - Create Group;
 - Delete Groups;
 - Create Policy;
 Delete Policies;
 - Expand All e Collapse All.
- Pre Rules: Caso um GSM esteja vinculado a este UTM, representa todos os grupos de políticas que foram colocadas para atuar antes das políticas locais do UTM, portanto elas possuem prioridade sobre as políticas criadas no próprio UTM;
- Local Rules: Representa as regras dos grupos de política criadas no próprio UTM;
- Post Rules: Todos os grupos de políticas criadas que serão irão entrar em vigor somente depois das políticas locais do UTM, portanto elas terão menor prioridade e serão instaladas abaixo dos grupos de políticas já existente no UTM.

É importante, lembrar que as políticas são ordenadas por "Prioridade", sendo que elas são aplicadas considerando o método "*First Match Wins*" (Que literalmente quer dizer "O 1º entre os concorrentes VENCE"). Logo, as políticas localizadas acima tem prioridade enquanto as abaixo possuem menor prioridade.

Cada grupo de política contém os seguintes botões:

- [] Ao clicar e arrastar, move a ordem do grupo e permite reorganizar a prioridade de acordo com qual grupo está acima (First Match Wins);
- [2] Expande para exibir as políticas criadas no grupo;
- [0] Informa quantas políticas existe no grupo;
- [] Permite editar as configurações adicionadas na opção Create Group do menu de ações;
- [¹] Deleta o grupo;
- [__] Seleciona o grupo de modo a interagir com o menu de ações.

As colunas de dentro de cada grupo de política são divididas em:

- Move [1]: Ao clicar e arrastar, move a ordem da política e permite reorganizar a prioridade de acordo com qual política está acima (First Match Wins);
- Id [#8]: Exibe o número de identificação da política, é possível clicar nele para servir como filtro no campo de busca;
- Rule: Exibe o nome da política;
- User: Determina quais usuários são afetados pela política, é possível clicar neste campo para servir como filtro no campo de busca;
- Source: Exibe se a origem desta regra será a Zona de rede, endereço IP, interface de rede, Mac Address ou qualquer um destes, é possível clicar neste campo para servir como filtro no campo de busca;
- Destination: Determina o destino da regra, o endereço IP ou serviço, é possível clicar neste campo para servir como filtro no campo de busca;
- Schedule: Exibe caso a regra depende de um período de tempo ou agendamento, é possível clicar neste campo para servir como filtro no campo de busca;
- Services: Exibe os serviços que a regra afeta, é possível clicar neste campo para servir como filtro no campo de busca;
- Tags: Exibe as tags que foram adicionadas à essa regra, é possível clicar neste campo para servir como filtro no campo de busca;
- Modules: Determina com quais módulos do UTM a regra irá interagir, é possível clicar neste campo para servir como filtro no campo de busca;
 Action: Exibe alguns botões contextuais e qual ação a regra executa.
 - Enabled[] ou Disabled[]: Através deste seletor, ativa ou desativa a regra;
 - Edit []: Permite editar as configurações adicionadas na opção Create Policy do menu de ações;
 - Clone[⁴]: Copia a política. Atente que ao usar essa opção, a política copiada usará o mesmo nome da política original, porém adicionará um número na frente (por exemplo, se eu copio a política "Test" a cópia se chamará "Test (1)") e ficará automaticamente abaixo da política original, portanto, levando em consideração o "*First Match Wins*", é importante mover a política de acordo com a prioridade desejada;
 - **Delete**[**1**]: Remove a política;
 - Select Permite a seleção das políticas de modo a interagirem com o menu de ações;
 - Action: Determina o comportamento da política em questão, tendo como possibilidades:



Isso conclui a análise das políticas IPv6.

UTM - SERVICES

Através do item Services é possível efetuar o gerenciamento de todos os serviços disponíveis no BLOCKBIT UTM.

Ative um serviço através do botão [0], para desativar um serviço utilize o botão [0].

| 0 \$ | Services | ~ |
|-------------|----------------------|---|
| » | Firewall | O |
| » | Proxy | Φ |
| » | Web Cache | Φ |
| » | Web Filter | Φ |
| » | Application Control | σ |
| » | Intrusion Prevention | Φ |
| » | Threat Protection | Φ |
| » | SD-WAN | Φ |
| » | DHCP | Φ |
| » | DNS | Ο |
| » | DDNS | Ο |
| » | VPN IPSEC | Ο |
| » | VPN SSL | σ |
| | Services | |

Services

Contém as opções:

- Firewall;
- Proxy; Web Cache;
- Web Filter,
- Application Control;
- Intrusion Prevention;
- Threat Protection;
 SD-WAN;
- DHCP;
- **DNS**;
- DDNS;
- VPN IPSEC,VPN SSL.

UTM - Services - Firewall

O Blockbit UTM habilita a proteção para segmentos internos da rede ou para ambientes externos, como perímetros de borda, datacenters, redes híbridas e aplicações em nuvem.

O Blockbit UTM foi projetado para proteger as informações confidenciais da sua organização através de controles de segurança utilizados para impedir a invasão de programas maliciosos na rede.

Esses controles contêm permissões de acesso a serviços e portas, que por padrão são configurados para proibir todos os parâmetros de segurança e conexões, integrado com as políticas de segurança, Interceptação SSL, filtros de pacotes e NAT.

O Firewall opera no modo "Stateful" e dispõe de ferramentas que parametrizam os "Níveis de segurança" e os "Controle das conexões", além das pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento" – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de pellicas de "Filtros de Pacotes" e "Redirecionamento" – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de contros de Trátego.

O serviço é pré-configurado para permitir acesso aos serviços locais do Blockbit UTM.

Para acessar esta tela, basta selecionar a opção "Firewall'.



Services - Firewall

A tela abaixo será exibida:

| Firewall | | | | | |
|---------------------------------|-----------------|---------|-------|-------------|-------|
| Zora Pretschart Pertificienting | lare of latings | | | | |
| | | | | | + - |
| Asseiption | Service | action | 2010 | Arbertistel | |
| II miny | 1119-140323 | the | (100) | | 0/0 |
| H WHISH | UTM APPESS | 1304 | UNC | | 0/0 |
| # Pacture | 10* | the . | 100 | | 0/0 |
| H Pres GARAN | (Sister | itten | 0.00 | | e / a |
| H FrechW7.1 | MAT-T | 8304 | 101 | | 0/0 |
| III Administration 524 | 534 | 4304 | 144 | | 0/0 |
| II Ami moration met | LTM-ADMIN | 1201 | 101 | | e / 0 |
| III Authentication Radius | 640.65 | Allow | 101 | | e / a |
| II schencescriptei | UTM PORTAL | silon . | 101 | | C / 0 |
| # ADM STOP | 1044 | 2010 | 100 | | 0/8 |
| | | | | | |

Firewall

A tela Firewall comporta as seguintes abas:

- Zone Protection;
 Port Forwarding;
 General Settings.

A seguir analisaremos os componentes da aba Zone Protection.

Firewall - Zone Protection

Através desta aba é possível configurar políticas de entrada para as portas e serviços locais do Blockbit UTM quando requer uma política de acesso específica.

As políticas de Zone Protection por definição são caracterizadas por perfil de acesso, por "Zona de rede" e pelas "Ações" de tratamento do pacote que permite inclusive "Inspecionar" o tráfego de [Entrada].

As políticas de Zone Protection tratam os pacotes de "Entrada" por análise condicional que inclui: "Zona de rede", "IP de origem", "IP de destino", com suporte endereçamento [IPv4/IPv6], "horário" e "Autenticação por usuários e grupos", são cadastradas por "Prioridade" e suportam "Reordenação".

As Políticas de entrada do tipo "Zone Protection" aumentam de forma significativa o grau de segurança no acesso aos serviços do dispositivo Blockbit UTM.

Para abrir a tela "Zone Protection", basta selecionar a opção "Firewall" no menu vertical à esquerda.

Caso a aba não esteja selecionada, clique em "Zone Protection".



Aba Zone Protection

Surgirá a tela "Zone Protection", conforme demonstrado pela imagem abaixo:

| Blockb | it | = | | | | | | | и А ⁰ н ⁰ л. |
|-------------------------|------|----------|---------|---------------|-------------------|-------|------------------|-----------------------|--|
| | | Fires | llew | | | | | | |
| B Marrier | - 92 | - Darest | need to | Tel benefitig | Deces Terrary | | | | |
| i⊉ Autjan | | | | | | | | | |
| New | - 22 | | | | | | | | |
| 🛋 tovin | | | | Desciption | Brida | (here | Buffer is buffer | Segretar. | Attieve |
| a const | | | - | DNS-Lacel | CHIL | LAN | | 000 | |
| | | | | WT THE Local | UTW-WWWITES: | ALL. | | NUMBER OF STREET, ST. | 10 A A A A A A A A A A A A A A A A A A A |
| • Welsen | • | | - | 9PH 551-uscal | UTINI-VENSIA. | ALL | | and size was | |
| a matter | • | | - | 9000 | A characteristics | 411 | | EXCLUSION OF | |
| · restaurchase | | | | and date | | | 12 | 100 | |
| a statute Processor | • | | | Addres Yes | STRADES | 441 | v. | 100 100 100 | |

Zone Protection

A área de Zone Protection conta com uma barra de pesquisa que permite localizar objetos e conteúdos nestes objetos.

Esta sessão irá abordar:

- Cadastro, Edição e Remoção de política de firewall do tipo Zone Protection;
- Ativação e Desativação destas mesmas;
- Exemplos de cadastro.

A seguir, analisaremos as funções localizadas no topo deste painel.

Zone Protection - Botão de Criação

Para criar uma política de firewall do tipo Zone Protection específica, clique no botão localizado no canto superior direito:



Ao clicar neste botão a janela abaixo é exibida:

| Conditions | Policy | General | |
|---|------------|-------------------------|-----------------|
| Service Zone Service Zone Service ALL Time Action Service Action | Conditions | Enabled Description | |
| Select ALL Time Action Index All Index All Intraction All Intraction Traffic Logging | | • Service | Zone |
| Time Action Induit V Alam Traffic Monitor Intrusion Prevention Intrusion Prevention Intrusion Prevention Intrusion Prevention Intrusion Prevention Intrusion Prevention | | Select | ALL |
| Indext V Allow Traffic Monitor Traffic Logging Impettion Intrusion Prevention | | Time | Action |
| Traffic Monitor Traffic Logging Intrusion Prevention Intrusion Prevention Threat Blocking Intern | | Telest | Allan |
| Intrusion Prevention | | Traffic Monitor | Traffic Logging |
| Intrusion Presention | | lingection | |
| Their Their Blocking | | Intrusion Prevention | |
| Threat Blocking | | Delect | |
| falser | | Threat Blocking | |
| | | Aaleen | |

O menu é composto pelas sessões:

- Policy;
- Conditions.

Abaixo analisaremos cada uma destas sessões em detalhes.

Policy

Em "Policy" configuramos todas as opções relacionadas à como a política do Zone Protection funcionará:

| and a local state of the second state of the s | Correct | | | | | |
|--|---|---|------------------------------------|--|--|--|
| Conditions | Enabled Description | | | | | |
| | • Service | Zone | | | | |
| | Time | Action | | | | |
| | Traffic Monitor | Traffic Logging | | | | |
| | Inspection | | | | | |
| | Intrusion Presention | | | | | |
| | Threat Blocking | | | | | |
| | | | | | | |
| | | Cancal | Same | | | |
| | Zone Protection – Pol | icy | | | | |
| bled[]: Determina se estará o scription: Define uma descrição p vice: Determina o serviço que se | com o status ativado[] ou desativad para identificação; rá utilizado na criação da política, os serv | lo[]; iços que aparecerem neste camp | oo são criados em <i>Objects</i> - | | | |
| ie: Determina o tipo de agrupame | ento de <i>interfaces</i> que será utilizado. Estes | s agrupamentos são criados em | Network - Interfaces; | | | |

- Traffic Monitor: Ao checar a caixa Traffic Monitor [2], as informações das sessões que dão match na política localizada deverão ser coletadas pelo serviço de monitoramento e enviadas ao serviço de sumarização em tempo real (Reporter).
- Traffic Logging: Ao checar a caixa Traffic Logging [], serão gerados Logs referentes as informações coletadas pelo serviço de monitoramento.

- Intrusion Prevention: Com a caixa de checagem marcada, determina que será o IPS será utilizado, além disso ativa a lista suspensa, que permite a seleção de qual perfil será utilizado. Os perfis que aparecem, são criados em Services Intrusion Prevention;
 Threat Blocking: Ao ativar esta caixa de seleção, será feito um bloqueio de todas as ameaças listadas (como tag) no campo de texto. Caso tags
- sejam adicionadas sem ativar a caixa de checagem, ela será ativada automaticamente ao salvar.

| Isso conclui a configuração, caso não seja necessária nenhuma " <i>col</i> essa janela, clique em [] para cancelar todas as configurações e v | ndition", salve as alterações clicando em Save], caso deseje fechar oltar a tela anterior. |
|---|---|
| Após salvar, será necessário acessar a fila de comandos [|] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de |
| Caso haja a necessidade de configurar "condition", cheque a sessão |) à seguir. |

Conditions

Em "Conditions" configuramos todas as condições sobre como o Zone Protection funcionará:

| Policy | identification | | | |
|------------|----------------|----|--------------|---|
| Conditions | Authenticated | | | |
| | Users | | Group | |
| | | = | | = |
| | | | | |
| | Source | | | |
| | iPv4 Address | | iPv6 Address | |
| | | Ξ | | Ξ |
| | Destination | | | |
| | IPv4 Address | | IPv6 Address | |
| | | := | | = |
| | | | | |
| | | | | |
| | | | | |

Zone Protection - Conditions

- Authenticated *J*: Esta caixa de checagem determina se a política exige autenticação (caso esteja ativada) ou não (caso esteja desativada). Além disso, ao habilitar essa caixa de checagem os campos *Users* e *Groups* ficam disponíveis para edição;
- Users: Clique em [=] e selecione todos os usuários aos quais a política será aplicada. Os usuários que aparecem nesta janela são criados em Settings Authentication Aba Users;
- Groups: Clique em [] e selecione todos os grupos de usuários aos quais a política será aplicada. Os grupos de usuário que aparecem nesta janela são criados em Settings Authentication Aba Settings Authentication Aba Users Groups Add Group;
- IPv4 Source IP: Clique em [=] e selecione todos os endereços IPv4 de origem aos quais a política será aplicada. Os endereços IPv4 que aparecem nesta janela são criados em Objects Addresses;
- IPv6 Source IP: Clique em [=] e selecione todos os endereços IPv6 de origem aos quais a política será aplicada. Os endereços IPv6 que aparecem nesta janela são criados em Objects Addresses;
- Destination IPv4: Clique em [:=] e selecione todos os endereços IPv4 de destino aos quais a política será aplicada. Os endereços IPv4 que aparecem nesta janela são criados em Objects Addresses;
- Destination IPv6: Clique em [] e selecione todos os endereços IPv4 de destino aos quais a política será aplicada. Os endereços IPv4 que aparecem nesta janela são criados em Objects Addresses;



Para ilustrar melhor os procedimentos listados acima, à seguir, analisaremos alguns exemplos:

- Exemplo 1 Acesso a interface Web Blockbit UTM (VPN Client);
- Exemplo 2 Acesso remoto SSH pela WAN "Internet" (Suporte Blockbit).

Para mais informações sobre como efetuar a remoção, clique nesta página.

Exemplo 1 - Acesso a interface Web - Blockbit UTM (VPN **Client**)

Segue uma demonstração de como criar uma política para permitir acesso à interface de administração do "Firewall", pela Rede VPN Client:

Neste exemplo iremos adicionar uma política de "Permissão" para a porta Blockbit Admin [98/TCP]. Somente para os usuários membros do grupo Suporte e autenticados.

| 1000000 | | | | | |
|------------|------------------------------------|--|--------|--|--|
| Policy | General | | | | |
| Conditions | Enabled * Description | | | | |
| | Blockbit Admin Access - VPN Client | | | | |
| | * Service | | Zone | | |
| | UTM-ADMIN | | wan | | |
| | Time | | Action | | |
| | Select | | Allow | | |
| | Inspection | | | | |
| | Intrusion Prevention | | | | |
| | Select | | | | |
| | Threat Blocking | | | | |
| | Griffet | | | | |
| | | | | | |

Zone Protection - Access interface admin for VPN client - Policy

Complete especificamente os campos à seguir:



- Enabled []: Habilitado;
 Zone: Selecione "WAN";
- Action: Selecione "Allow"; •
- Service: Informe e selecione da lista "UTM-ADMIN";
- Descrição: "Acesso Blockbit Admin VPN Client".

A seguir analisaremos as configurações que são necessárias em "Conditions".

Conditions

| Policy | Identification | | | |
|------------|----------------|---|--------------|----|
| Conditions | Authenticated | | | |
| COMMENTS | Users | | Group | |
| | | Ξ | | 1 |
| | Source | | | |
| | IPv4 Address | | IPv6 Address | |
| | | Ξ | | = |
| | Destination | | | |
| | IPv4 Address | | IPv6 Address | |
| | 3 Selected | E | | 12 |
| | | | | |
| | | | | |

Complete especificamente os campos à seguir:

- Authenticated [2]: Habilitar para exigir a autenticação;
 IPv4 source IP: Selecione o IPv4 de origem "192.168.31.0". Caso seja necessário, adicione o objeto de endereço, para mais informações consulte esta página.

| | Save | |
|--------------------------|------|--|
| Por fim, clique em Save[| | , caso contrário, clique em [^] para cancelar todas as configurações e voltar a tela anterio |

Após salvar, será necessário acessar a **fila de comandos [** comandos acesse a página: UTM - Fila de comandos.



] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de

Isso conclui o exemplo 1.

Exemplo 2 - Acesso remoto SSH - pela WAN "Internet" -(Suporte Blockbit)

Segue uma demonstração de como criar uma política para permitir o acesso remoto a console SSH pela internet.

Neste exemplo iremos adicionar uma política de "Permissão - com inspeção IPS" para a porta SSH [22/TCP]. Somente para o IP de origem do suporte Blockbit.

| Create | | | | | | |
|------------|--------------------------------------|--|--------|---------|--|--|
| Policy | General | | | | | |
| Conditions | CondRiens Enabled | | | | | |
| | SSH Remote Access - Blockbit Support | | | | | |
| | * Service | | Zone | | | |
| | 55H | | wan | <u></u> | | |
| | Time | | Action | | | |
| | Select | | Altow | | | |
| | Inspection | | | | | |
| | Intrusion Prevention | | | | | |
| | IDM Defect | | | | | |
| | Threat Blocking | | | | | |
| | Gillet | | | | | |
| | | | | | | |

Zone Protection - SSH Remote Access - Policy

Complete especificamente os campos à seguir:



- Enabled []: Habilitado;
 Zone: Selecione "WAN";
- Action: Selecione "Allow"; •
- Service: Informe e selecione da lista "SSH";

- Intrusion Prevention []: Marque a caixa de checagem e selecione o IPS desejado, para mais informações cheque o capítulo Intrusion Prevention;
- Description: "SSH Remote Access Blockbit Support".

A seguir analisaremos as configurações que são necessárias em "Conditions".

Conditions

| Conditions | Authenticated | | | |
|------------|---------------|------------|--------------|----|
| | Users | | Group | |
| | | | | |
| | | | | |
| | Source | | | |
| | IPv4 Address | | IPv6 Address | |
| | 1 Sciented | : : | | 12 |
| | Destination | | | |
| | IPv4 Address | | IPv6 Address | |
| | | | | 1 |

Zone Protection - SSH Remote Access - Conditions

Complete especificamente o campos à seguir:

 IPv4 de origem: Selecione da lista o IP que pretende dar acesso remoto a console SSH pela internet, neste exemplo usaremos o objeto de enredeço "Blockbit Support", para mais informação sobre como criá-los, cheque esta página.

As configurações de entrada para os serviços Blockbit UTM no item [Zone Protection] visa melhorar os níveis de segurança no acesso aos serviços e recursos do firewall.



], caso contrário, clique em [X] para cancelar todas as configurações e voltar a tela anterior.



Após salvar, será necessário acessar a **fila de comandos [** comandos acesse a página: UTM - Fila de comandos.

] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de

Isso conclui o exemplo 2.

Por fim, clique em Save[

Zone Protection - Colunas

A seguir, explicaremos cada coluna da aba Zone Protection:

| er leven automb | Fire | await. | | | | | |
|--------------------|------|---------------|---------------------|--|-------------|---|----------------|
| Contract (| 1 2 | eithean Anton | ing (Sections) | | | | |
| e noise | 3 | | | | | | |
| Print (| | | | | 14.00 | | |
| Careton | | Desciption | Investor | in the second se | Agreets and | Ingention | datara |
| | | - Dhi-Land | 24 | LAN | | 879.623.628 | A |
| | • | E WEPBE-G | und UTRYPOPED | (61 | | 1001020-018 | 2000 (P Z 5) 8 |
| a matter | • | - 94.95ive | u universe. | 41 | | 122.02 (22 | 30 X EL 201 |
| e sheliter | • | E 300 | Automotion | 41 | | 000 | |
| a Andrew Street of | • | 1.000 1.00 S | UTALIDEA | | | and the second | DV NA |
| | | | 1.5500 | | 1.1.1 | and the second second | |
| | | — Alex 218 | 3.00 | - 126 | | 0,0140 | |
| - | | E bok | STER - LIT M PHELIP | 1.49 | | ENGINES. | 10 × 0 × 0 × |
| | | - Wess | data-unterphota. | 441 | | 010202 | 100 C 2 6 4 |
| | | 1. T. PM | coul-size-whereas: | 161 | | 636363 | 100 C 2 11 1 |
| | ė. | E 001 | 004-045 | LH | | Children of the local division of the local | ETE C284 |
| | 6 | - | The second second | | | | |

- Zone Protection
- Select []: Permite selecionar uma política do Firewall;

Movel I: Permite movimentar a política do *Firewall* e determinar sua prioridade, a regra que estiver mais à cima terá maior prioridade; *Description:* Exibe a descrição da política que foi cadastrada no Botão de Adição; Movel •

- Service: Determina qual é o serviço utilizado pela política do Firewall;
- Zone: Exibe a zona cadastrada no Botão de Adição, por padrão, pode ser LAN, WAN ou DMZ;
- Action: Exibe qual será a ação aplicada pela política: [Allow], Deny] ou Reject]
- Authenticated: Determina se a autenticação será necessária ou não, caso seja necessário este ícone: [] será exibido; ٠
- Inspection: Exibe caso a política tenha ativado Intrusion Prevention [IPS], Threat Blocking [ATP] ou Log[ATP], Actions Menu: Disponibiliza as seguintes ações essenciais:



• Botão Clone 1: Permite clonar uma das políticas.

Zone Protection - Coluna Services

A coluna Service é configurada juntamente na criação de um perfil de Zone Protection. Nesta seção, analisaremos a habilitação do acesso SSH (Secure Shell) via serviço Telnet, em específico.

É importante lembrar que a regra vem desabilitada de fábrica, e com a ação "deny" por default.

| Blockb | it | = | | | | | | | | e = 4 | | A. |
|--|----|------|------|------|----------------|------------------|------|---------------|-------------|-------|---------|----|
| ALTHORN LLT. HTT | | Fire | wa | u | | | | | | | | |
| 6 Marrier | 10 | 249 | Pres | 1000 | Periformation | General Gallerge | | | | | | |
| et maijaar | 12 | | | | | | | | | | - Q., | 4 |
| • folia: | 14 | | | | Description | Service | Done | Arthenticated | Impetitory | | Actions | |
| d inven | | | | | Nonel Access | TRIMET | UNH | | | | + 41 1 | |
| * Donal | - | | | ÷. | may | UTM PHILING | DAM | | 888 | | 1 15 1 | 0 |
| * Perij | | | | ÷ | VPNDBL | UTM APAGSL | LAN | | 13030 | | 100 | 0 |
| . wette | | | | = | (bec | UTM-VPMPSEE | LAN | | 100 000 000 | - | 1 10 1 | 0 |
| * Applacent Control | - | | | = | DNS | 045 | LAN | | E2 (2) (2) | | 1 12 3 | 0 |
| Internet Presenter Tread Presetter | 8 | | | 3 | Administration | Administration: | 645 | | 000 | | 100 | 8 |

Firewall - Zone Protection



Primeiramente devemos criar a regra em Zone Protection, para tal clique em [_____] e na opção create. A seguir devemos selecionar a Zona e a ação:

| Pattag | General | |
|----------|--------------------------|--------|
| nditions | Enabled • Description | |
| | TelhotAccesi | |
| | * Service | Jone |
| | TUNT | 4.00 |
| | Tirm | ALL |
| | 2641 | 942 |
| | Traffic Vipritor | 1.4.14 |
| | | WOR |
| | impettion | |

Zone Protection - Create - Zone

| distance - | Cashied 🔽 | | |
|------------|----------------------|---------|--|
| 000000 | * pescription | | |
| | Telnet Access | | |
| | * Service | Zorw | |
| | TELUIET | - A4 | |
| | Time | Action | |
| | Marc. | 17 1 mm | |
| | Traffic Monitor | Allow | |
| | Marris Constants | Dany | |
| | inspection | Rejett | |
| | intrusion Prevention | 1.0 | |

Zone Protection - Create - Action

Após criar, a regra será exibida na tela principal da seguinte maneira:

| Firewall | | | | | | | | |
|-----------------|----------------|------------------|------|---------------|------------|-------|---------|---|
| Zane Protection | PartForwarding | General Settings | | | | | | |
| | | | | | | | 9 | ~ |
| | Description | Service | Zene | Authenticated | Inspection | | Edd ans | |
| | Telinet Access | TELNET | ALL | | 000 | Alich | | a |
| | Proxy | UTM-PROOV | LAN | | | Aller | 010 | ä |

Zone Protection - Telnet Rule

Abaixo vemos os comandos que podem ser utilizados para gerenciar a função:

| admın > admin > admin >admin-over-telnet Usage: admin-over-telnet <enable disable s< th=""><th>status></th></enable disable s<> | status> |
|---|--------------|
| enable: Enables service disable: Disables service status: Check service status | |
| Copyright BLOCKBIT® (<u>http://www.blockbit.c</u> All rights reserved <info@blockbit.com></info@blockbit.com> | <u>com/)</u> |
| admin > | |

CLI Interface - Telnet Management Commands

Utilizando o comando "admin-over-telnet --enable" habilitamos o serviço Telnet pela porta 23:



Enabling Telnet

Para desabilitar, devemos utilizar o comando "admin-over-telnet --disable":



Disabling Telnet

A regra com o serviço habilitado estará visível na tela principal, a regra com o serviço estará desabilitada na tela principal, também é importante lembrar que deve-se alterar a ação para "allow" e habilitar a regra:

| Blockb | it | ≡ | | | | | | | .e. = | • = | 1- |
|--|------|-------|--------|----------------|----------------|--------|---------------|---|-------------------|---------|-----|
| нетнови ассняти | j | Firev | vall | | | | | | | | - |
| n inste | 11 | Sheer | viette | n nitrout | e sneihtrgi | | | | | | |
| E Arabite | 11 | - | | | | | | | | 1 | |
| • room | 11 | | | 2003-00-01 | | 1.000 | 1.000.000.000 | and the second se | | | |
| OC Services | 1 | | | Description | Service | 1946 | Autorstated | Inspectice | | Actions | ŧ., |
| to Prevail | | | 1 | Televit Accimi | TD, MCT | ALL | | CC CC CC | | 2010 | |
| Contractory of the second seco | • | | 1.1 | Proty | UTM-P9000 | LAN | | RC9 C3 C1 | | 10 | .0 |
| * WebCarler | - | | 1.0 | VENSSL | VTH-VTHOS. | LAN | | 62 63 53 | - | 200 | |
| · | C | | | iPier - | UTMARMINE | LAN | | 10000 | - | 120 | |
| a spintener | - 21 | | - | | -Calence are | - 77.0 | | | the second second | | |
| · manthematica | 0 | | | 045 | DHS | LAN | | 000 | | 0.00 | |
| E Three Protectory | a | | 1 | Administration | Administration | ALL. | | 6383 C | | 212 | |
| · TELANS | 19 | | = | Authorscason | Automistice | LAN | | 63453 53 | - | 10 | |

Zone Protection com Telnet Habilitada

As regras com o serviço Telnet habilitado podem ser visualizadas em Security Events:

| Date | User | Source | Destination | Device | Service | Log type | Action | | |
|-----------------------|------|------------------------|----------------------|------------|----------|----------|--------|---|---|
| E 2022-04-11 11:02:51 | (†) | 172.32.0.108:50245 | [1] 177.31.175.2923 | etto | teinet | freval | slow | 9 | |
| E 2022-06-11 11-01-25 | (÷) | [] 192.108.79.10:55908 | 172.16.13.24252 | atin1-ath0 | danam | fresal | alize | 9 | ш |
| E 2022-04-11 11-01-22 | 2 | Mg 172.22.0,100:53072 | 172.31.175.29-29 | atho | tainet | Second | slow. | 9 | = |
| E 2022-04-11 11:00:50 | ÷. | C] 192.108.29.14:55926 | []] 172.16.15.246.53 | eth1-eth0 | clomain. | brevit | allen | Э | = |
| E 2022-04-11 10:59:08 | 9 | 117.32.0.108.56916 | 172.31.175.2823 | etho | temet | trevel | aline | Э | = |

Enabled Telnet

Utilizando o Query editor, podemos pesquisar também as regras com Telnet ativo:

| ssions Authentical | teo VPN | | | | | | | |
|---------------------------|------------|--------------------|---------------------|---------|----------|---------|--------|-----|
| oervice:"beinet" date "ta | st_30m* | decision in | | | | 0 | 9 | =γŧ |
| Date | Uner | Source | Destination | Device | Service | logtype | Action | |
| 2022-04-11 11.02/51 | 2 9 | 172.32.0.108.50248 | LT 172.03.575.29(23 | ethili | telost | Irowit | cline | 9 |
| j 2022-04-11 11:01-22 | 61 | 172.32.0.109-53072 | 172.33.375.29-23 | inth 0 | tabut | freed. | start | Э |
| 2022-04-11 10:59-00 | | T72.32.0.100.50915 | FT 172.11.171.2923 | attra . | Salitat. | house | dire. | 5 |

Security Events - Query Editor

Ao clicar sobre o botão de mais [+] é possível obter mais informações sobre da regra:

| | Information | | | | | | | | | |
|---|---|--------------------------------|---|---------|--------|---------|----------|--------|--------|------|
| ~ | | ⊖ na ⊕ beatrai | (i) steats (i) WAN | G atter | | | 0 | Q | uary E | cito |
| e | ⊕ biştiyen ⊜ firment | ⊕ thet.rec ⊙ 0034:21:st76.N | (i) misurem (i) Televit Access | | Device | Service | Log type | Action | | |
| - | ⊕ scold ⊕ 60603CE17333472EE5681AL5070/E300 | | teetere ① | | ath0 | tubat. | Scenal. | alow | 0 | = |
| 1 | ⊙ ML ⊙ 177.59.0.188 | i annt i cont | (i) ten (i) input | | eth0. | tidost | frekel | #.m | 3 | = |
| 2 | ⊕ +p+++ ⊖ 90246 | () and () ath | (i) service (ii) scinet | _ | 0414 | tainet | freval | Mex | 3 | = |



Em Live Sessions também podemos conferir a regra em funcionamento:

| Type (8) Honoral (1) Ands | | Status Calabilistani 🕘 New | Harbard 👜 Week | | | Manu # 24 (0 100 (0 200 | | | |
|------------------------------|---------------|-------------------------------|----------------|----------|----------|----------------------------|---------|------|--|
| Liser | Source | Destination | Port | Protocol | Policy | | | | |
| (milicante | | Participation | 10 | THP | NUT | | 1 | up 👘 | |
| User | Source | Desthatio | 90. | Port | Protecol | Policy | Actions | | |
| (H) | 152.168.29.10 | 172.16.13.2 | 46 | 53 | UDP | NAT - DNS e FING | ۲ | 1 | |
| | 172.32.0.308 | 172.31.175 | 29 | 23 | TCP | Telnet Access | | | |
| | 172.32.0.108 | 172.31.175 | .29 | 98 | TCP | Administration | ۲ | ÷ | |

Live Sessions

Deste modo conseguimos habilitar e verificar o funcionamento do serviço Telnet.

Zone Protection - Remove

Através deste botão é possível deletar vários itens ao mesmo tempo. Siga o exemplo abaixo:

1. Selecione os itens que deseja deletar clicando no ícone de seleção[___];

| • | | meaniption | terator | 2244 | action | Administra | nqetter | AC\$905 |
|---|----|---------------|-------------------|--------|-------------------------|------------|---------|---------|
| 3 | Ξ | hat. | 2017 | 1.046 | Concession in which the | | 10100 | C/ 1 |
| | Ξ. | 100 | 859 | 04 | Alter | | 60.00 | 071 |
| | = | Attravelation | Administration | (A) | Color. | | 101100 | 011 |
| | Ξ | Advetication | Forther Kitch Int | 0.00 | A Alexand | | - | |
| | Ξ. | Arryve SARAP | See. | SAM | C Aller 1 | | 8100 | 0121 |
| | = | VPMILL. | Little orregine | LAN | (CARDING) | | - | 0.29 |
| | = | Posq | 1010-05200 | LAN | (Common States) | | 6363 | 0.43 |
| | | 100 | 001 | DM. | C. Allow | | 10010 | 0.2.8 |
| | - | 154 | UNIVERSES. | C LARC | A Allen a | 1.140 | 100 000 | 071 |



2. Clique no botão [_____], surgirá uma tela perguntado se deseja deletar o item selecionado:



Zone Protection - Remove itens



O item foi deletado com sucesso.

Firewall - Port Forwarding

Como o próprio nome indica, o *Port Forwarding* efetua um encaminhamento, permitindo que uma porta em particular seja determinada para endereços *IP* específicos em uma *LAN*. Isso possibilita por exemplo, a conexão a um outro appliance ou serviço através de uma rede privada, independente do *appliance* estar atrás de um roteador.

O Port Forwarding é composto de regras de filtros de pacotes com a opção de tradução de endereços, possibilitando modificar o endereço de destino das máquinas clientes. Através dos seus recursos é possível efetuar o encaminhamento do tráfego entre os barramentos e configurar mascaramento do tipo DNAT, sendo este último especialmente útil no redirecionamento de portas.

As regras de Port Forwarding são carregadas de cima para baixo, assim sendo, as regras que estiverem no topo da tabela possuem prioridade sobre as abaixo (sendo possível até que elas sobreponham as configurações das regras de baixo).

Para abrir a tela, clique na aba "Port Forwarding".



Aba Port Forwarding

Surgirá a tela abaixo:

| are Protection | Port Forwarding | Configurações Ge | ran | | | | |
|----------------|------------------|------------------|------------|--|--|-----------|--------------|
| | | | | | | | ٩ |
| Des | criçãe | Permitidas | Bloqueadas | Interface | Destino | Controles | Ações |
| □ = 188 | # 1 | | | 172.31.130.24640/70P 172.31.130.24740/70P | 10.46 190.001 £380-709 | | 0 / @ |
| () ≡ Teg | s2 | | | 17221-30244-00758 | 17531.03654062/7C# 572/0.03654066/7C# | - | () |
| | sa regra 1 | | | 10.40.150.44.00/TCP 172.01.150.244.80/TCP | 10.46.196.201.8483/709 171.31.350.44.8383/709 | | 0 /10 |
| E Nos | sa regra | | | 11.40.150.44.0011/707 071.31.463.00231/709 17231.150.3458081/709 | ETELLOISEACHITCH ETELLOISEACHITCH | | ••• |
| E Bak | anca-MEB port_80 | | | 171.31.350.344.60/10# 173.31.110.44.60/10# 173.31.150.345.60/10# | 00-40.158.00366/TCF 00-40.158.001050/TCF 172.11.0.381.8041/TCF | 128 | •• |

Port Forwarding

A aba Port Forwarding conta com uma barra de pesquisa que permite buscar objetos e conteúdos inclusos nestes mesmos objetos.

O botão Clone [2] permite replicar as políticas individualmente.

Esta sessão irá abordar:

- Cadastro, Edição e Remoção de políticas de redirecionamento;
 Ativação e Desativação destas mesmas;
 Exemplos de políticas de redirecionamento
 Detalhes das colunas desta tela.

A seguir, analisaremos as funções localizadas no topo desta tela.

Port Forwarding - Botão de Adição

Através desta janela é possível criar um Port Forwarding e configurar as permissões de mascaramento e redirecionamento de tráfego entre os barramentos.

Para criar um Port Forwarding, clique no botão localizado no topo superior direito:



Port Forwarding - Botão de Criação

Ao clicar neste botão a janela abaixo é exibida:

| Policy | General | | | |
|------------|--------------------------|---|----------------------|----|
| Conditions | Description | | | |
| Advanced | Traffic Monètor | | Traffic Logging | |
| | Redirect To | | | |
| | * Protocol | | | |
| | 109 | | | 2 |
| | Interface | | Port / Range | |
| | Columi | | Gic 9696 (5590;6000 | |
| | • IP | | * Port/Range | |
| | Telect | 1 | Ex west 1 moderato | |
| | | | | |
| | | | | 11 |
| | 10 | | | |
| | SNAT | | | |
| | Carlock Catalog: 1144440 | | | |

Port Forwarding - Criando um novo Port Forwarding

O menu é composto por várias sessões e painéis:

- Policy;
 General;
 Redirect to.
- - Cópia de Port Forwarding Botão de Adição#Authentication;
 Cópia de Port Forwarding Botão de Adição#Sources;
 Cópia de Port Forwarding Botão de Adição#Schedule.
- Advanced;

Abaixo analisaremos cada uma destas sessões em detalhes.

Policy

Em "Policy" configuramos todas as opções relacionadas à política de como o Port Forwarding atuará:

| Policy | General | | | | |
|-----------|---------------------|---------------------|--|--|--|
| onditions | * Description | | | | |
| Advanced | Traffic Monitor | | | | |
| | Redirect To | | | | |
| | * Protocol | | | | |
| | 109 | | | | |
| | Interface | Port / Range | | | |
| | Ghil V | Ec 9898 5590-6090 | | | |
| | • IP | * Port/Range | | | |
| | Select V | Ec weet two options | | | |
| | | | | | |
| | SNAT | | | | |
| | Carlos Conceptional | | | | |



- General;Redirect to.

Iniciaremos detalhando o painel General.

General

Este painel contém apenas o campo para adicionar a descrição da política.

| | General | | |
|--|---|---|-----------------|
| | * Description | | |
| | | | |
| | ✓ Traffic Monitor | Traffic Logging | |
| | Policy · | General | |
| • Description: D | efine uma descrição para identificação; | | |
| Traffic Monitor associadas ao | r: Com a caixa de <i>Traffic Monitor</i> checada [<mark>''</mark>], s Port Forwarding; | erão coletados dados sobre o tráfego de informações | das sessões |
| Traffic Loggin associadas ao | g: Com a caixa de <i>Traffic Logging</i> checada [<mark>?</mark>], Port Forwarding. | serão gerados logs referentes ao tráfego de informaçõ | ões das sessões |
| À seguir detalharemos o | painel Redirect to. | | |

Redirect To

Este painel contém os recursos para configuração do redirecionamento da política de Port Forwarding

| Protocol | | | |
|-----------|--------|----------------------|---|
| TCP | | | Ý |
| Interface | | * Port / Range | |
| Select | 92 - S | Exc 9898 5500:6000 | |
| * IP | | * Port / Range | |
| Select | V . | Exc 9898 5500:6000 | 4 |
| | | | • |
| SNAT | | | |

Policy - Redirect to

- Protocol: Define qual protocolo será utilizado;
- Interface: Determina qual interface de rede será utilizada. As interfaces que aparecem neste menu são configuradas em Network Interfaces;
- Port / Range: Define a porta que será usada e seu respectivo range. Para este campo ser habilitado é necessário adicionar uma interface no campo anterior;
- IP: Determina os endereços de IP que serão utilizados no redirecionamento e suas respectivas portas, atente que para eles serem exibidos

nesta lista, precisam ser do tipo "*IP* único". Clique no botão [_____] para adicionar o endereço à lista, caso queira remover algum endereço,

selecione-o na lista e clique em [_____]. Para mais informações sobre como adicionar um objeto de endereço do tipo "IP único", consulte esta pá gina.

- Port / Range: Define a porta que será usada pelo IP de redirecionamento e seu respectivo range. Para este campo ser habilitado é necessário adicionar um IP no campo anterior;
- SNAT[]: Caso a caixa de checagem seja habilitada, permite a seleção de um gateway para efetuar NAT. Para tanto, é possível selecionar o Gateway padrão ou uma interface. As interfaces que aparecem neste menu são configuradas em Network Interfaces;

À seguir vamos detalhar os componentes da aba lateral "Conditions".

Conditions

Em "Conditions" configuramos todas as condições sobre como o port forwarding funcionará:

Port Forwarding

| Conditions | Users | | Groups | |
|------------|----------|----|----------|-----------|
| Advanced | | 12 | | ÷ |
| | Sources | | | |
| | Alloweds | | Blockeds | |
| | | = | | E |
| | Schedule | | | |
| | Time | | Date | |
| | Bellect | | foliat | |
| | | | | |
| | | | | Cancel Sm |
| | | | | |

X

Esta aba é composta pelos painéis:

- Authentication;Sources;Schedule.

Iniciaremos detalhando o painel Authentication.

Authentication

Neste painel estão localizadas os recursos que permitem condicionar a ativação do Port Forward por autenticação.

| Authenticated | | | |
|---------------|------|-----|----|
| Users | Grou | aps | |
| | | | := |

• Authenticated J: Esta caixa de checagem determina se o port forwarding exigirá autenticação (caso esteja ativada) ou não (caso esteja desativada). Além disso, ao habilitar essa caixa de checagem os campos Users e Groups ficam disponíveis para edição:

| • Users: Com a c | aixa de checagem authenticated marcada, clique em [🗮] | para dete | rminar à quais | usuários o port forwarding será |
|------------------|--|-----------|----------------|---------------------------------|
| aplicado, confo | me demonstrado pela imagem abaixo. Ao finalizar a seleção, cli | ique em [| Save |] caso contrário, clique em [|
| Cancel |] para cancelar; | | | |

Users

r -

| All | Q V Q V V V V V V V V V V V V V |
|-----|---|
| • | Name |
| ~ | user1 (user1@blockbit.com) |
| | user2 (user2@blockbit.com) |
| | user3 (user3@blockbit.com) |
| | < 1 > |

Х

| | | | | | Cancel | Save | |
|-------------|---------------|----------------------|--------------------------------|------------|-----------------------|------------------|--------------------|
| L | | | Authentication - User | S | | | |
| | | | | | | | |
| • Groups: (| Com a caixa | de checagem a | uthenticated marcada, clique e | m [≔ |] para determinar | à quais grupos c | le usuários o port |
| forwarding | y será aplica | do, conforme de | monstrado pela imagem abaixo | . Ao final | izar a seleção, cliqu | le em [| e] caso |
| contrário, | clique em [| Cancel |] para cancelar; | | | | |

| Group | | |
|-------|-------------|-----|
| All | | ۹ 🗸 |
| | Name | |
| | management | |
| | development | |
| | | < 1 |

12



Sources

Neste painel estão localizadas os recursos que permitem condicionar a ativação do Port Forward de acordo com a origem do tráfego.

| | Sources | | | | |
|-----------------|--------------------------------|--------------------------|--|----------------------|-------------------|
| | Alloweds | | Blockeds | | |
| | | ≔ | | ≔ | |
| | | Conditions | - Sources | | |
| • Alloweds: Cli | ique em [🔚] para determina | ar quais endereços e IP | s de origem serão permitidos pelo port forwa | a <i>rding</i> , con | forme demonstrado |
| pela imagem | abaixo. Os objetos que aparece | em na lista, são criados | em Objects - Addresses. Ao finalizar a seleç | ão, clique | em [] |
| caso contrário |), clique em [] |] para cancelar; | | | |

IPv4 Address

 r^{-}

| | All | Q |
|------------------------------------|----------|---|
| | | Name |
| | | ADDRESS 123 |
| | | ADDRESS TEST |
| | | ADDRESS UNIQUE |
| | | test |
| | | Class A network |
| | | Class B network |
| | | Class C network |
| | | Class Group Group |
| | | Localhost |
| | | Private class network |
| | | < 1 2 > |
| | | Cancel Save |
| L | | Sources - Allowed Sources |
| ockeds: Clio la imagem a | que em [|] para determinar quais endereços e IPs de origem serão bloqueados pelo <i>port forwarding, ca</i> tos que aparecem na lista, são criados em <i>Objects - Addresses</i> . Ao finalizar a seleção, clique |

Х

caso contrário, clique em [_____] para cancelar;

IPv4 Address

.

| All | २ २ २ २ २ २ २ २ २ २ २ २ < |
|----------|--|
| • | Name |
| ~ | ADDRESS 123 |
| ~ | ADDRESS TEST |
| | ADDRESS UNIQUE |
| ~ | add test |
| | Class A network |
| | Class B network |
| | Class C network |
| | Class Group Group |
| | Localhost |
| | Private class network |
| | < 1 2 > |
| | Cancel Save |

.

4

Х

Sources - Blocked Sources

À seguir, detalharemos o painel Schedule.

Ŀ.

Schedule

Neste painel estão localizadas os recursos que permitem controlar a ativação do Port Forward em um período específico.
| Schedule | | | |
|----------|---|--------|--------|
| ſime | | Date | |
| Select | ~ | Select | \sim |

- *Time:* Determina que o *Port Forwarding* será aplicado somente de acordo com o objeto do tipo "*Time*" selecionado. Os objetos que aparecem na lista, são criados em *Objects Times*; *Date:* Determina que o *Port Forwarding* será aplicado somente de acordo com o objeto do tipo "*Schedule*" selecionado. Os objetos que aparecem na lista, são criados em *Objects Schedules*;

À seguir iremos detalhar a aba Inspection.

Advanced

Em "Advanced" configuramos quais inspeções serão aplicadas no port forwarding:

| Policy | (analysis) | | |
|------------|-------------------------------|------------|----|
| roncy | inspection | | |
| Conditions | SSI, Inspection | | |
| | 5660 | | 80 |
| Advanced | Intrusion Prevention | | |
| | Selat. | | ¥. |
| | Threat Blocking | | |
| | Select | | |
| | Do5 Protection | | |
| | Packet Rate (Packets/Seconds) | Burst Rate | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Port Forwarding - Inspection

• SSL Inspection: Permite selecionar um perfil e aplicar SSL Inspection no port forwarding. Os perfis que aparecem na lista, são criados em SSL Inspection - SSL Profile;

ATENÇÃO: Ao utilizar um perfil de Inspeção SSL, o Port Forwarding irá funcionar apenas em tráfego seguro, por exemplo, quando são utilizados os protocolos: HTTPS, POPS, IMAPS, SMTPS e outros tipos de criptografia. Atente que ao criar um Port Forwarding desta forma a seguinte mensagem de alerta será exibida:

| ALTHEOR BLILLEY | | Firewa | đi | O Patthematin | profess (ALI) SSC inspection | er will only work for said | toos puppertual by security protocolo | | | | |
|-----------------|----|----------|----------|----------------|------------------------------|----------------------------|--|-------------------------|----------|--------|---|
| B Maratar | 31 | June Pro | inclary. | PartForwarding | Grani Jetrop | | | | | | |
| et Analyse | 1 | | | | | | | | | | 4 |
| • nice | ÷. | | | Description: | Allowedb | Badech | atarteo | Destination | Controls | Actual | |
| el Service | * | | | | | Charles Discording | test and the sector from | the Aug + Decision | | | |
| · inned | • | | = | TOP NO. 1.00 | | and the | an a | The Pill Pill Pill Pill | | 01 | n |
| | • | | | | | UBM TRAFES | Distantian Constantian Pro- | 102104-1-0041-1020 | - | | |
| | 0 | | | U017851.80 | | 002000 | A | 17.8.52409.009 | 88 | 01 | 1 |
| | • | | | | | and there is | | | | | |
| | •0 | | 8. | HTTP NUMI-1.28 | | and these | | the second second | 88 | 01 | 1 |

- Intrusion Prevention: Permite selecionar um perfil e aplicar Intrusion Prevention no Port Forwarding. Os perfis que aparecem na lista, são criados em UTM - Services - Intrusion Prevention;
- Threat Blocking: Permite efetuar proteção contra as ameaças selecionadas. Cada opção é adicionada como tag, caso deseje remover alguma

opção clique em [X] ou selecione ela novamente no menu. Para limpar esse campo, basta clicar em []. Possui as opções abaixo:

- Abuse;
 Anonymizer
- Anonymizers;
- Attacks;
- Malware;
- Reputation;
 Snom
- Spam.

DoS Protection

Neste painel estão disponíveis os controles de DoS Protection:

| Packet Rate (Packets/Seconds) | * Burst Rate | |
|-------------------------------|--------------|--|
| 2000 | 1 | |



- - Packet Rate: A opção Packet Rate configura o Firewall para limitar as conexões a um valor máximo de pacotes por segundo.
 - Burst Rate: A opção Burst Rate configura o Firewall para permitir inicialmente uma quantidade máxima de pacotes por segundo sem validar o Packet Rate, permitindo assim flexibilizar o controle de tráfego para picos de tráfego ocasionais.



Para ilustrar melhor os procedimentos listados acima, à seguir, analisaremos alguns exemplos.

Port Forwarding - Exemplos

A seguir vamos exemplificar como criar algumas políticas de redirecionamento.



Exemplo I - Port Forwarding 1:1

No acesso ao formulário de configuração, vamos preencher os campos de acordo com as especificações definidas na política exemplo.

- Descrição: Nome de identificação da regra de redirecionamento;
- Origem: Interface de entrada desejada;
- Protocolo de origem + Porta/Range: Protocolo e porta de origem desejada *Redirecionar para*: Endereço de IP e porta desejada;

| Policy | General | | |
|---------|--------------------------------|-------------------|-----|
| ditions | Description | | |
| | 14 | | |
| dvanced | Traffic Monitor | Z Traffic Logging | |
| | Source | | |
| | Interface | | |
| | Met . | | - + |
| | eth0-172,31,158,44 | | [(= |
| | Source Protocol + Port / Range | | |
| | Protocol | • Port / Range | |
| | | 21 | |

| | | iP | | Port / Range | | |
|---|--|---|--|-----------------------|---------------|------------------------------|
| | | Mart. | 96 | Ext 9050 [\$360-6000 | | * |
| | | 10,40,150,100 - 4 | 43 | | * | - |
| | | SNAT | | | | |
| | | parket (Laborate (1) | 4-(k=2) | | | 10 |
| | | | Port Forwarding - Policy | /1 | Cancel | Save |
| | | | | | | |
| Depois clique em [| Save]. | | | E | • | |
| Após salvar, para q mais informações a | ue o encaminhamento respeito da fila de com | entre em ação será ne andos acesse a págir | ecessário acessar a fila na: UTM - Fila de coman | de comandos [dos. |] e aplicar a | s alterações efetuadas. Para |

Após realizar esses procedimentos a política terá sido configurada com sucesso.

Exemplo II - Port Forwarding N:1

No acesso ao formulário de configuração, vamos preencher os campos de acordo com as especificações definidas na política exemplo.

- Descrição: Nome de identificação da regra de redirecionamento;
- Origem: Interfaces de entrada desejadas;
 Protocolo de origem + Porta/Range: Protocolo e porta de origem desejada
- Redirecionar para: Endereço de IP e porta desejada;

| Policy | General | | | |
|------------|---|-----------------|-----------------------|---------|
| Conditions | Description | | | |
| | N:1 | | | |
| Advanced | Z Traffic Monitor | | Traffic Logging | |
| | Source | | | |
| | interface | | | |
| | default. | | | · + |
| | eth0-172.31.150.44 eth1-10.40.150.44 | | | |
| | Source Protocol + Port / Han | pe. | | 1 |
| | Protocol | | Port / Range | |
| | | | 21 | |
| | Redirect To | | | |
| | iP | | Port / Range | |
| | Select: | 196 | Ext 9080 [\$360+6000 | + |
| | 10.40.150.100 - 443 | | | |
| | SNAT | | | |
| | pelant listenary filadaet | | | W. |
| | | | | 1 |
| | | | Cano | el Save |
| | Port Forw | arding - Policy | 2 | |
| Save | | | | |
| ie em []. | | | | |
| | | | • | |

Após realizar esses procedimentos a política terá sido configurada com sucesso e, assim, será possível redirecionar o tráfego da porta X, em diferentes entradas/interfaces do Blockbit, para UM host da rede interna.

Exemplo III: Port Forwarding N:N

No acesso ao formulário de configuração, vamos preencher os campos de acordo com as especificações definidas na política exemplo.

- Descrição: Nome de identificação da regra de redirecionamento;
- Origem: Interfaces de entrada desejadas;
- Protocolo de origem + Porta/Range: Protocolo e porta de origem desejada
- Redirecionar para: Endereços de IP e portas desejada;

| Policy | General | | |
|-------------|---|----------------|---------------------------------------|
| | Description | | |
| Landitions: | NeN | | |
| Advanced | Traffic Monitor | 💟 Traffic Log | ging |
| | Source | | |
| | Interface | | |
| | Saturi | | · · · · · · · · · · · · · · · · · · · |
| | ethi0 - 172.31.150.44 ethi1 - 10.40.150.44 | | - |
| | | | - |
| | Source Protocol + Port / Range | | |
| | * Protocol | • Port / Range | |
| | 10 | 21 | |

| IP | Port / Range |
|--|--|
| Talact | Ex: 9898 5509:6000 |
| 10.40,150.100 10.40,150.42 - | - 443 |
| SNAT | |
| Definit Consense | Helef. V |
| | |
| | Cancel Save |
| | Port Forwarding - Policy 3 |
| Depois clique em []. | |
| Quando configurado 2 ou mais destinos a regra criad será o principal, e caso esteja indisponível o redirecio | a obedecerá o padrão "first match wins", ou seja, o primeiro IP configurado como destino onamento será feito pelos outros IPs configurados. |
| Após salvar, para que o encaminhamento entre em ação será mais informações a respeito da fila de comandos acesse a pá | a necessário acessar a fila de comandos [I e aplicar as alterações efetuadas. Para Igina: UTM - Fila de comandos. |
| Após realizar esses procedimentos a política terá sido configuentradas/interfaces do Blockbit, para N hosts da rede interna. | urada com sucesso e, assim, será possível redirecionar o tráfego da porta X, em diferentes |

No final das configurações exemplificadas, não esqueça de habilitar as políticas cadastradas, para tanto, clique em habilitar [

Isso conclui o exemplo, à seguir detalharemos o botão de remoção.

Port Forwarding - Botão de Remoção

Através do botão de remoção é possível deletar vários itens ao mesmo tempo. Siga os seguintes passos:

```
1. Selecione os itens que deseja deletar clicando no ícone de seleção[___];
```

| i fiid | Action PortParenting | Served Settings | | | | | |
|--------|----------------------|-----------------|-----------|-------------------|----------------------------------|-----------|-------------|
| | | | | | | | |
| • | Speciption | Alloweds | idischeda | aviei fiele | Institution | Gastralia | Artices |
| 2 | = 107 | | 1200.2015 | 20.01291.00101707 | 0038186970 | 88 | • •• |
| | a operator | | 1107,2458 | aut2584xaw | 20000.00000000 1210120400.009 | | |
| | | | 1101,050 | 01.41.03.07.00707 | 10110123-00717 | 109403 | - |

Port Forwarding - Seleção para deleção

2. Clique no botão de **remoção**[_____] e uma tela perguntado se deseja deletar o item selecionado:



Port Forwarding - Criar Port Forwarding

Através desta janela é possível criar um Port Forwarding e configurar as permissões de mascaramento e redirecionamento de tráfego entre os barramentos.

Para criar um Port Forwarding, clique no botão localizado no topo superior direito:



Port Forwarding – Botão de Criação

Ao clicar neste botão a janela abaixo é exibida:

| Service 1 | | | |
|-----------|-----------------------------------|-----------------|-------|
| Politica | Geral | | |
| iondições | * Descrição | | |
| Avançado | Traffic Honitor | Traffic Logging | |
| | Origem | | |
| | interface | | |
| | | | ~] + |
| | | | ÷ |
| | | | - |
| | | | |
| | Origeni Protocolo + Porta / Range | | |
| | * Protocolo | Porta / Range | |
| | 7/10 | | |

| Georgianay | | ET: UNU 1000-0000 | |
|------------------------|------|---------------------|-------|
| | | | 1 |
| | | | |
| | | | |
| | | | 7 |
| SNAT | | | |
| | | | |
| Grane Centre Hamasters | | | |
| | SMAT | SNAT | SRIAT |

Port Forwarding - Criando um novo Port Forwarding

O menu é composto por várias sessões e painéis:

- Política
 - Geral Origem

 - Origem Protocolo + Porta/Range
 Redirecionar Para
- Condições
- Autenticação
 Origens
 Agendamento
- Avançado
 - . Inspeção
 - DoS Protection

Abaixo analisaremos cada uma destas sessões em detalhes.

Política

Em "Política" configuramos todas as opções relacionadas à política de como o Port Forwarding atuará:

| Politica | Geral | | | |
|-------------|--------------------------------|-------|------------------------|---|
| and/day | * Descrição | | | |
| -united the | | | | |
| Avançado | 🛃 Traffic Honitor | | Traffic Logging | |
| | Origem | | | |
| | interface | | | |
| | | | | + |
| | | | | * |
| | | | | - |
| | | | | |
| | Origenti Protocolo + Porta / R | lange | | |
| | • Protocolo | | • Porta / Range | |
| | ΤÇΡ | - V. | Le Ime Stancood | |
| | | | | |
| | Redirectionar Para | | | |
| | • (P | | Porta / Range | |
| | Gelegister av | | Ex: 0400 \$500-\$000 | + |
| | | | | * |
| | | | | - |
| | 11000 | | | 7 |
| | SNAT | | | |
| | | | | |

Port Forwarding - Política

Esta aba é composta pelos painéis:

- Geral
 Origem
 Origem Protocolo + Porta/Range
 Redirecionar para

Iniciaremos detalhando o painel "Geral"

Geral

Este painel contém apenas o campo para adicionar a descrição da política.

| | Geral | | |
|------------------------------|---|--|------|
| | * Descrição | | |
| | Traffic Monitor | Traffic Logging | |
| | Po | lítica - Geral | |
| Descriçã | o: Define uma descrição para identificação; | | |
| Traffic M associada | onitor: Com a caixa de <i>Traffic Monitor</i> checada [|], serão coletados dados sobre o tráfego de informações das sessõe | s |
| Traffic Lo associada | ogging: Com a caixa de <i>Traffic Logging</i> checada [|], serão gerados logs referentes ao tráfego de informações das ses | sões |

À seguir detalharemos o painel "Origem"

Origem

| Drigem | |
|----------|-----|
| nterface | |
| | ✓ ↓ |
| | |
| | - |
| | * |



• Interface: Determina quais interfaces de rede serão utilizadas, já que mais de uma pode ser inserida nesse campo.. As interfaces que aparecem neste menu são configuradas em Network - Interfaces;

À seguir detalharemos o painel "Origem Protocolo + Porta/Range"

Origem Protocolo + Porta/Range

| Origem Protocolo + Porta / Range | | | |
|----------------------------------|---|----------------------|--|
| * Protocolo | | * Porta / Range | |
| тср | ~ | Ex: 9898 5500:6000 | |
| | | | |



- Protocol: Define qual protocolo será utilizado;
- Port / Range: Define a porta que será usada e seu respectivo range. Para este campo ser habilitado é necessário adicionar uma interface no campo anterior;

À seguir detalharemos o painel "Redirecionar Para"

Redirecionar Para

Este painel contém os recursos para configuração do redirecionamento da política de Port Forwarding

| IP | Porta / Range | |
|-------------|----------------------|---|
| Selectioner | Ex: 9498 5500-0000 | - |
| | | |
| | | - |
| | | * |
| | | |

Política - Redirecionar Para

• IP: Determina os endereços de IP que serão utilizados no redirecionamento e suas respectivas portas, atente que para eles serem exibidos

nesta lista, precisam ser do tipo "*IP* único". Clique no botão [____] para adicionar o endereço à lista, caso queira remover algum endereço, selecione-o na lista e clique em [____]. Para mais informações sobre como adicionar um objeto de endereço do tipo "*IP* único", consulte esta pá gina.

- Port / Range: Define a porta que será usada pelo IP de redirecionamento e seu respectivo range. Para este campo ser habilitado é necessário adicionar um IP no campo anterior;
- SNAT[]: Caso a caixa de checagem seja habilitada, permite a seleção de um gateway para efetuar NAT. Para tanto, é possível selecionar o Gateway padrão ou uma interface. As interfaces que aparecem neste menu são configuradas em Network Interfaces;

À seguir vamos detalhar os componentes da aba lateral "Conditions".

Condições

Em "Condições" configuramos todas as condições sobre como o port forwarding funcionará:

| Politice | Аслектосаção | | | |
|-----------|----------------------------|---|--|---|
| Cambles | Autorrtinado Usanie teo | | _: drupe | |
| . Anargan | Organa | | | |
| | Pennitidas | | Bloqueadas | |
| | | = | | 1 |
| | Agordamento | | | |
| | Tempo | | Data | |
| | Minister . | | and the second s | |
| | | | | |
| | | | | |
| | | | | |

Port Forwarding - Conditions

Esta aba é composta pelos painéis:

- AutenticaçãoOrigensAgendamento

Iniciaremos detalhando o painel Authentication.

Autenticação

Neste painel estão localizadas os recursos que permitem condicionar a ativação do Port Forward por autenticação.

| Autenticação | |
|---|----------------------------|
| Autenticado | |
| Usuários Grupo | |
| Condições - Autenticação | |
| Autenticado[]: Esta caixa de checagem determina se o <i>port forwarding</i> exigirá autenticação (caso esteja ativada) ou não (caso desativada). Além disso, ao habilitar essa caixa de checagem os campos Users e Groups ficam disponíveis para edição: Usuários: Com a caixa de checagem autenticadomarcada, clique em [] para determinar à quais usuários o <i>port fo</i> Save | o esteja örwarding será |
| aplicado, conforme demonstrado pela imagem abaixo. Ao finalizar a seleção, clique em [] caso contrário, Cancel] para cancelar; | clique em [|
| | |
| Autenticação | |
| ✓ Autenticado ✓ Usuários Grupo | |
| | |
| | |
| Usuários | |
| Selecion_V | |
| Nome | |
| aurora (aurora@domtniof.com) | |
| Diego (diego@clominiof.com) | |
| | |
| Autenticação - Usuários | |

| 0 | <i>Grupo</i> : Com a caixa de c | checagem autenticado marcada, o | clique em [📃] para determ | ninar à quais grup | os de usuários o port |
|---|---|--|---------------------------------|--------------------|-----------------------|
| | forwarding será aplicado, contrário, clique em [| conforme demonstrado pela imag Cancel] para cancelar; | em abaixo. Ao finalizar a seleç | ;ão, clique em [| Save] caso |
| | Autenticação | | | | |
| | ✓ AutenticadUsuários | do | ✔ Grupo | | |
| | | | | : | = |
| | ŝ | Srupo | | × | |
| | | Todos 🤄 | 9 | * | |
| | | E Name | | | |
| | | C-Portal | | | |
| | | quèas | | | |
| | | vendedores(top10) | | | |
| | | | | 1. > | |

Autenticação - Grupo

À seguir, detalharemos o painel Origens.

Origens

Neste painel estão localizadas os recursos que permitem condicionar a ativação do Port Forward de acordo com a origem do tráfego.

| Origens | | |
|------------|---------------------|----|
| Permitidas | Bloqueadas | |
| | = | ;≡ |
| | Condições - Origens | |

• Permitidos: Clique em [] para determinar quais endereços e IPs de origem serão permitidos pelo *port forwarding*, conforme demonstrado

pela imagem abaixo. Os objetos que aparecem na lista, são criados em *Objects - Addresses*. Ao finalizar a seleção, clique em [Cancel] para cancelar;

Х

IPv4 Address

| All | ✓ Q |
|-----|------------------------------|
| | Name |
| | ADDRESS 123 |
| | ADDRESS TEST |
| | ADDRESS UNIQUE |
| | test |
| | Class A network |
| | Class B network |
| | Class C network |
| | Class Group Group |
| | Localhost |
| | Private class network |
| | < 1 2 > |
| | Cancel Save |
| | Origens - Origens Permitidas |
| | |

Bloqueados: Clique em [] para determinar quais endereços e IPs de origem serão bloqueados pelo port forwarding, conforme demonstrado pela imagem abaixo. Os objetos que aparecem na lista, são criados em Objects - Addresses. Ao finalizar a seleção, clique em [Save Cancel]

] caso contrário, clique em [_____] para cancelar;

IPv4 Address

r

| All | $\mathbf{\vee}$ | ۹ 🗸 |
|-----|------------------------------|-------------|
| | Name | |
| ~ | ADDRESS 123 | |
| ~ | ADDRESS TEST | |
| | ADDRESS UNIQUE | |
| ~ | add test | |
| | Class A network | |
| | Class B network | |
| | Class C network | |
| | Class Group | Group |
| | Localhost | |
| | Private class network | |
| | | < 1 2 > |
| | | Cancel Save |
| | Origens - Origens Bloqueadas | |

À seguir, detalharemos o painel Schedule.

μ.

Agendamento

Neste painel estão localizadas os recursos que permitem controlar a ativação do Port Forward em um período específico.

7

| Agendamento | | | |
|-------------|--------|------------|--------|
| Tempo | | Data | |
| Selecionar | \sim | Selecionar | \sim |

Condições - Agendamento

- Tempo: Determina que o Port Forwarding será aplicado somente de acordo com o objeto do tipo "Time" selecionado. Os objetos que aparecem na lista, são criados em Objects - Times;
- Data: Determina que o Port Forwarding será aplicado somente de acordo com o objeto do tipo "Schedule" selecionado. Os objetos que aparecem na lista, são criados em Objects Schedules;

À seguir iremos detalhar a aba Inspection.

Avançado

Em "Avançado" configuramos quais inspeções serão aplicadas no port forwarding:

| 40414.9 | mpeçin | | |
|-----------|--|------------------|--|
| Condition | \$54. Impection | | |
| | de la como de | | |
| Avergate | Intrision Provention | | |
| | Weiner- | | |
| | Threat Blocking | | |
| | -la a su a | | |
| | Dos Protection | | |
| | Taxo de Pacete (pacetos/segundes) | Taxa de Explesão | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Port Forwarding - Avançado

Inspeção SSL

Inspeção SSL: Permite selecionar um perfil e aplicar Inspeção SSL no port forwarding. Os perfis que aparecem na lista, são criados em SSL Inspection - SSL Profile;

| Inspeção | |
|----------------------|--------|
| SSL Inspection | |
| Selecionar | \vee |
| Intrusion Prevention | |
| Selecionar | \vee |
| Threat Blocking | |
| Selecionar | |
| | |



| Blockb | it | = | | | 0 | taxed iscrematicly | | | = A | -0 | 1 |
|---------------|------|----------|---------|-----------------|----------------------------|---------------------------|--------------------------------------|-------------------------------|------------|--------|----|
| ALTHE MALER | | Firewa | di | O Pathinating | ning of the SSE inspection | e will only work for sain | too papportati ku saca ety protocijo | | | | |
| B Maratar | 30 | Zane Pro | methory | PartForwarding | Grentletrep | | | | | | |
| e notice | - 4) | | | | | | | | | | 1 |
| • value | 61 | | | | | | | | | | |
| C Service | 4 | | | Description | Altreeth | Bischerb | arlarhox | Deuterators | Controlle | Active | |
| Tranil | • | | = | TOP INE ALCO | | UMI JSEES | on accession to | 10.44113452709 | 100 | 07 | |
| | • | | | | | | | | | | |
| | œ | | | U011655.00 | | dim Tinice | SPECIFICATION | 101361Av61009 108524090009 | 88 | 0/ | 10 |
| · Westellings | • | | | | | | | | | | |
| | •0 | | | HTTP: WEWL-1.28 | | man, treest | 20140.004700709 | INCOMPTINGUES. | C2 C3 | 01 | |

- Intrusion Prevention: Permite selecionar um perfil e aplicar Intrusion Prevention no Port Forwarding. Os perfis que aparecem na lista, são criados em UTM - Services - Intrusion Prevention;
 Threat Blocking: Permite efetuar proteção contra as ameaças selecionadas. Cada opção é adicionada como tag, caso deseje remover alguma

 - opção clique em [X] ou selecione ela novamente no menu. Para limpar esse campo, basta clicar em [• Abuse;
 - Anonymizers;
 Attacks;

 - Malware;
 - Reputation;
 Spam.

DoS Protection

Neste painel estão disponíveis os controles de DoS Protection:

| | DoS Protection | | |
|---|--|--|---|
| | Taxa de Pacote (pacotes/segundos) | Taxa de Explosão | |
| | 2000 | 10 | |
| | Avançado - Configura | ções de DoS Protection | |
| • DoS Pro evitando o o | otection: Com a caixa de DoS Protection checada [dataques distribuídos ou anomalias de tráfego causadas por Taxa de Pacote : A opção Taxa de Pacote configura o Fire Taxa de Explosão: A opção Taxa de Explosão configura o segundo sem validar o Packet Rate, permitindo assim flexit | e possível limitar a quantidade máxima de pacotes por segundo possíveis <i>malwares</i> na rede. <i>ewall</i> para limitar as conexões a um valor máximo de pacotes po <i>Firewall</i> para permitir inicialmente uma quantidade máxima de pilizar o controle de tráfego para picos de tráfego ocasionais. | no <i>Firewall,</i> or segundo. pacotes por |
| Para salvar as alt voltar a tela anter | erações clique em [Save], caso contrário, clique ior. | em [X] ou em [Cancel] para cancelar todas as confi | gurações e |
| Após salvar, será comandos acesse | necessário acessar a fila de comandos [a a página: UTM - Fila de comandos. | ar as alterações efetuadas. Para mais informações a respeito d | a fila de |

Para ilustrar melhor os procedimentos listados acima, à seguir, analisaremos alguns exemplos.

Port Forwarding - Excluir Port Forwarding

Através do botão de remoção é possível deletar vários itens ao mesmo tempo. Siga os seguintes passos:

1. Selecione os itens que deseja deletar clicando no ícone de **seleção[___]**;

| Zone Protection | Part Parwarding | Configuraçãos De | ata.) | | | | |
|---------------------|------------------|------------------|----------------------------------|--|---|------------------|-------|
| | | | | | | | 8 |
| Desc | orição | Permitidas | Bioqueadas | Intertace | Destino | Controles | Ações |
| 🖂 📄 Bala | nce-WEB port_30 | | | 171.51.10034400/TCP 171.31.1004430/TCP 171.31.10024540/TCP | 13-45 100 (00 00 TCP 13-45 100 (00 00 TCP 13-45 100 (00 10 00 TCP 171 (00 00 00 00 TCP | | ्र थ |
| | | | Port Forwarding | y - Seleção para deleção | | | |
| | Excluir Po | rt Forward | ing | | | X | |
| | DNA | T: A x B | Jer excluir os s | seguintes itens? | | | |
| | | | | | | | |
| | | | | Canc | elar Confi | rmar | |
| | | | Port Forwar | ding - Remover Item | elar Confi | rmar | |
| o deseje cancelar c | lique no botão [| Cancela | Port Forwar r]. Para cond | Canco ding - Remover Item | otão [| rmar ar | |
| o deseje cancelar c | lique no botão [| Cancela | Port Forwar | Canc ding - Remover Item cluir a deleção clique no b vido com sucesso | otão [| rmar ar J. | |

O item foi deletado com sucesso.

À seguir detalharemos o conteúdo das colunas.

Port Forwarding - Colunas

A seguir explicaremos cada coluna da aba Port Forwarding:

| Firewall | | | | | | | |
|-----------------|--------------------|----------------------------------|-----------------------|------------------------|-------------------------|---------|-------------|
| 24 w Production | Fort forwarding | ianti latinge | | | | | |
| | | | | | | | n 4 |
| | Rectipilos | Alloweds | Beckedy | interter | Destination | Correst | Action |
| 5.8 | Bill level | Present Stands Reprint Stands | Areas and Class A. R. | 100.00.01.00.000.725 | TTLES AND DRAME TOP | 88 | 321 |
| 0.8 | 400 leve | | | | | 38 | 0/1 |
| 0.8 | un have | | | | | 88 | O 21 |
| 0.8 | neise | | | 100.01.8120310.009 | 171311030611/309 | 38 | (1) (1) |
| 0.4 | 913P Inglian | | | THE VERY CONDUCTION | 175-05-001,006-005-0009 | 88 | a ki |
| 민준 | WTC-inclass | | | 1010101-00120120000000 | 172.95.852.000355-859 | 28 | 0×1 |
| 12 B | | | | 126.00.01.00.00.779 | 101003430140039 | 88 | |
| | mental Bill Canada | | | annicanty. | 10110-0425-0500 | 123 123 | |

Port Forwarding

- Select []: Permite selecionar uma política de Port Forwarding;
- Movel]: Permite movimentar a política de Port Forwarding;
 Description: Exibe a descrição do Port Forwarding para identificação;
- Allowed: Exibe os objetos do tipo endereço permitidos que foram configurados em Port Forwarding Botão de Adição;
- · Blocked: Exibe os objetos do tipo endereço bloqueados que foram configurados em Port Forwarding Botão de Adição;

Nas colunas Allowed e Blocked é possível visualizar mais detalhes passando o mouse por cima dos objetos de endereço, uma lista com todos os IPs que fazem parte do objeto será exibida, segue um exemplo:

| Além disso, ao clicar no botão 🎑 exit | ido nesta janela é poss | Webex servers Image: Construction of the servers o | onstrado abaixo: |
|---------------------------------------|-------------------------|--|------------------|
| Edit Addres | ses Object | | × |
| * Name | | | |
| Webex Serv | rers | | |
| * Type | | | |
| IPv4 Address | | <pre> </pre> | Unique |
| * Address | | Mask | |
| | | 255.255.255 | · + |
| 114,29,192 | .0/255.255.0.0 | | ^ |
| 173.243.0. |)/255.255.0.0 | | - |
| 208.8.81.0 | 255.255.255.0 | | |
| 209.197.19 | 2.0/255.255.0.0 | | v |
| Description | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Cancel Import Address | Save |

Interface: Determina qual é o IP e o tipo de interface que o Port Forwarding está utilizando;
Destination: Exibe o endereço de IP de destino determinado em Port Forwarding - Botão de Adição;

- Controls: Exibe caso o Port Forwarding foi configurado para efetuar SSL Inspection [SSL], Intrusion Prevention [PS], Threat Blocking[ATP] e/ou user authentication[USR];
 Actions: Disponibiliza as seguintes ações essenciais:

• Enable[]/Disable[]: Permite ativar ou desativar uma política de Port Forwarding;

• Edit Permite editar as configurações da interface adicionada no Port Forwarding - Botão de Adição;

• Delete]: Permite remover um dos itens, é o equivalente à Port Forwarding - Botão de Remoção

Quando muitos dados são inseridos, excedendo o limite das células das tabelas e/ou na janela de detalhes dos objetos (citado acima) surgirão barras de rolagem para facilitar a navegação.

Para outras informações sobre port forwarding, acesse esta página.

Firewall - General Settings

Através desta aba é possível habilitar e configurar as políticas de entrada para as portas e serviços locais do Blockbit UTM.

Além disso, esta aba permite efetuar a configuração dos parâmetros de segurança e controles de conexão do firewall.

O item "Parâmetros de Segurança" define as configurações básicas de segurança e os parâmetros dos controles de conexão responsável em manter as informações do estado de todas as conexões e sessões do *Firewall*.

Os recursos pré-configurados referente aos itens das "Configurações de conexões" desta interface referem-se aos parâmetros de controle das conexões, a alteração destes valores implica diretamente no resultado de desempenho do servidor.

Para acessar, clique em "General Settings".



Surgirá a tela "General Settings", conforme demonstrado pela imagem abaixo:

| | | | 1 |
|--|----|---|----|
| Security Settings | | | |
| DoS Protection | | # Spoofing Protection | |
| | 12 | | 12 |
| Portscan Protection | | Jimalil Packet Protection | |
| 🛃 Alkow Ping | | Z Allows ICMP Radirect | |
| Ignore ICMP Broadcast | | Source Routing | |
| Checksoni | | inwa\$id Log | |
| Forward exonomiection | | | |
| Max Estimetions | | TCP Max Orphans () | |
| 380000 | | 365644 | |
| limatuts | | | |
| · Ganaria Timored | | * KMP Timeted | |
| 640 | | 20 | |
| | | The structure starts | |
| 1 CF Max Multians | | 10 | |
| | | 4* | |
| TCP Timeout Close Wait | | TCP Timeout Established | |
| 38 | | 180000 | |
| • TCP Timeout FIN Wait | | TCP Tineedot Last ACM | |
| н | | 30 | |
| TCP Timeout Max Retrans | | TCP Timeout SWM reck | |
| 42. | | 80 | |
| TCP Timeout SVN Sent | | * TCP Timeout Time Wait | |
| 136 | | 10 | |
| TTP applies | | Tr D movies tribes | |
| 3 | | 17 | |
| TCB 600 antrior | | • 1/ B mardelen | |
| 3 | | 3 | |
| | | | |
| 0 | | fighted | |
| | | | |
| • UDP Firecost | | * UDP Timoout Stream | |
| West and the second sec | | | |
| * TCP loose | | * Printk Messages Rate Limit/Sec | |
| 5 wheel | ×. | 19 | |
| Messages Cost/sec | | | |

General Settings

A tela "General Settings" é composta pelos seguintes painéis e recursos:

• Security Settings;

- DoS Protection;
- IP Spoofing Protection;
- PortScan Protection;
- Invalid Packet Protection;
- Allow Ping;
- Allows ICMP Redirect;
 Ignore ICMP Broadcast;
- Source Routing;
- Checksum;
- Invalid Log;
- Forward Error Correction;
- Max Connections; • TCP Max Orphans.

• Timeouts;

- Generic Timeout;
- ICMP Timeout;
- Max Connections;
- TCP Loose;
- TCP Max Retrans;
- TCP Timeout Close;
- TCP Timeout Close Wait; • TCP Timeout Established;
- Timeout TCP FIN Wait;
- TCP Timeout Last ACK;
- TCP Timeout Max Retrans;
- TCP Timeout SYN Recv;
- TCP Timeout SYN Sent;
- TCP Timeout Time Wait;
- TCP Retries;
- TCP Max Retries;
- TCP SYN Retries;
- TCP Reordering;
 TCP Enhanced Retransmission Timeout (F-RTO);
 TCP Selective Acknowledgements;
- UDP Timeout;
- UDP Timeout Stream.

A seguir detalharemos cada componente dos painéis:

Security Settings

Serve para detalhar alguns dos itens de configurações dos parâmetros de segurança.

| Das Piotection | IP Spoofing Protection | |
|-------------------------|-----------------------------|--|
| 1 Deserved | | |
| PortScan Protection | 🛃 Towalid Packet Protection | |
| 🛃 Allow Ping | Allows ICMP Redirect | |
| Ignore ICMP Broadcast | Source Roleting | |
| Checkturn | Invalid Log | |
| Forward error competion | | |
| Max Connections | * 3CP Max Orphans () | |
| 100006 | 26384 | |

General Settings - Security Settings

DoS Protection

Este recurso permite o bloqueio contra-ataques de negação de serviço (também conhecido como *Denial of Service - DoS*), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga, as técnicas suportadas são: *SYN Flood, TCP Flood, UDP Flood e ICMP Flood.*

| | 1 Selected | |
|----------------|-----------------------------------|-----------------------------|
| | Dos F | Protection |
| | := | |
| licar no botão | [🔚] a tela abaixo será exibida: | |
| | | |
| | DoS Protection | X |
| | SYN flood | |
| | Packet Rate (packets/second) | Burst Rate (packets/second) |
| | 2000 | 100 |
| | TCP flood | |
| | Packet Rate (packets/second) | Burst Rate (packets/second) |
| | 2000 | 100 |
| | VDP flood | |
| | Packet Rate (packets/second) | Burst Rate (packets/second) |
| | 2000 | 100 |
| | ICMP flood | |
| | Packet Rate (packets/second) | Burst Rate (packets/second) |
| | 2000 | 100 |
| | | |
| | | |
| | | Cancel Save |

- SYN Flood limit (per second): Determina o limite de pacotes recebidos de modo a prevenir ataques SYN Flood. O valor mínimo é 100 e o valor padrão é 2000;
- SYN Burst: O valor mínimo é 1 e o valor padrão é 100;
- TCP Flood limit (per second): Determina o limite de acesso TCP de modo a prevenir ataques TCP Flood. O valor mínimo é 100 e o valor padrão é 2000;
- TCP Burst: O valor mínimo é 1 e o valor padrão é 100;

- UDP Flood limit (per second): Determina o limite de acesso UDP de modo a prevenir ataques UDP Flood. O valor mínimo é 100 e o valor padrão é 2000;
- UDP Burst: O valor mínimo é 1 e o valor padrão é 100;
- ICMP Flood limit (per second): Determina o limite de acesso ICMP de modo a prevenir ataques ICMP Flood. O valor mínimo é 100 e o valor padrão é 2000;
- ICMP Burst: O valor mínimo é 1 e o valor padrão é 100.

IP Spoofing Protection

Este recurso habilita a proteção de IP Spoofing na zona de rede desejada.



Esta opção pode causar problemas com o serviço de SD-WAN



Este recurso é um tipo mensagem utilizada por roteadores para notificar hosts do mesmo segmento de rede, que existe um caminho (rota) melhor para um determinado destino. Recomendação: Ex: "[Desabilitar]".



Ignore ICMP Broadcast

Esse recurso ignora o tráfego *ICMP Broadcast*, usado para fazer com que servidores participem involuntariamente de ataques *DOS*, enviando grande quantidade de pings aumentando exponencialmente o tráfego *NETBIOS* da rede e tornando os serviços reais indisponíveis.

Recomendação: Ex: "[Habilitar]" Ignore ICMP Broadcast.

| Ignore | ICMP | Broad | lcast |
|--------|------|-------|-------|
|--------|------|-------|-------|

Ignore ICMP Broadcast

Source Routing

Este recurso permite aplicar testes de roteamento atrás do firewall, permitem ao emissor do pacote especificar o caminho de ida e volta do pacote. Recomendação: Ex: "[Desabilitado]".

Source Routing

Source Routing

O roteamento de origem consiste em um mecanismo de protocolo que permite o transporte de informações por um pacote IP. Informações como listas de endereços, informando ao roteador o caminho que o pacote deve seguir. Conta também com opção para gravar os saltos à medida que a rota é percorrida. O registro de rota, que lista os saltos realizados, fornece ao destino um caminho de retorno para a origem. Isso permite que a origem (o host de envio) especifique a rota, de maneira vaga ou estrita, ignorando as tabelas de roteamento de alguns ou de todos os roteadores. Permite também que um usuário redirecione o tráfego de rede para fins maliciosos. Logo, o roteamento baseado na origem deve ser desabilitado.

A opção "Roteamente de Origem" faz com que as interfaces de rede aceitem pacotes com o conjunto de opções Strict Source Route (SSR) ou Loose Source Routing (LSR). A aceitação dos pacotes roteados de origem é controlada pelas configurações do kernel. Portanto, para emitir o comando de descarte dos pacotes com o conjunto de opções SSR ou LSR, deve-se manter o checkbox desabilitado.

Checksum

Pacotes com checksums ruins ficam em estado inválido. Com esta opção ativada, tais pacotes não serão considerados para rastreamento de conexão na session tracking.



Checksum

Invalid Log

Habilita logs de pacotes com estado INVÁLIDO.

| Invalid | Log |
|---------|-----|
| | |

Invalid Log

Forward Error Correction

Consiste em um método de controle de erros em uma transmissão de dados, na qual a fonte emite dados redundantes e o destino reconhece apenas uma parte dos dados, aparentemente sem nenhum erro. Com esta opção, os pacotes de dados são recebidos duas vezes e aceitos somente com validação em ao menos uma instância.

| | Forward error correction | |
|----------------------|--------------------------------|--|
| | FEC - Forward error correction | |
| Max Conne | ctions | |
| Número máximo de cor | iexões. | |
| | * Max Connections | |
| | 300000 | |

Max connections

TCP Max Orphans

Número máximo de TCP sockets não associados a processos ou serviços, que são executados pelo OS no user space. Caso este número seja excedido, as conexões são imediatamente resetadas.

| * TCP Max Orphans 🛈 | | | | |
|---------------------|---------------------|--|--|--|
| 16384 | | | | |
| | TCP Max Connections | | | |

Timeouts

Os demais recursos pré-configurados referente os itens das "Configurações de conexões" desta interface referem-se aos parâmetros da "Session Track", a alteração destes valores implica diretamente no resultado de desempenho do servidor.
| Timouta | | | |
|---------------------------|------|--------------------------|-----|
| + Georgic Timecat | | + KHP Release | |
| 234740947 | (B) | (E | 創 |
| * Mag | | + 3CP loane | |
| 308069 | 8 | Distant | |
| * TOP Max Relyans | | * XCF Terrenal Close | |
| <u>x</u> | 8 | - 41C | 1 |
| * 107 Timeset Clese Walk | | * 707 Timmert Latablaked | |
| - 20 | (R) | | R. |
| * tro? timoral Heritak | | * 9CP TREWNET Last ACK | |
| -80 | (B): | 1 | (B) |
| + DOP Timewal Max Betrans | | · NOP Transact DVN oncy | |
| 80 | (R) | 40 | 9 |
| + ICP Tarasat SYR Aut | | • 10P General Time Wall | |
| 139 | * | 10 | 3 |
| + LEP Timenut | | * URP Timepet Streem | |
| 30 | #: | 346 | 8 |

General Settings - Timeout

Generic Timeout

Este parâmetro é usado para informar em segundos a session tracking o tempo limite genérico caso não seja possível determinar o protocolo usado e nem usar valores mais específicos. Qualquer fluxo ou pacote que entra no *firewall* que não pode ser totalmente identificado como qualquer outro tipo de protocolo receberá um tempo limite genérico definido neste parâmetro. O valor mínimo é 0 e o valor padrão é 600 segundos.

| | * Generic Timeout | | |
|------------|-------------------|----------------|--|
| | 2147483647 | * | |
| | Ge | eneric Timeout | |
| ICMP Timed | ut | | |

Usada para definir em segundos o tempo limite para os pacotes *ICMP* que resultarão no tráfego de retorno. Em outras palavras, incluir *ECHO REQUEST* and *REPLY*, *TIMESTAMP REQUEST* and *REPLY*, *INFORMATION REQUEST* and *REPLY* e *ADDRESS MASK REQUEST* and *REPLY*. Uma vez que é feito um dos pedidos, deve haver um pacote de retorno, e é quando o tempo limite do *ICMP* é contabilizado. Normalmente uma resposta *ICMP* é bastante rápida, a menos que seja utilizada uma conexão muito lenta. O valor mínimo é 0 e o valor padrão é 30.

| * ICMP Timeout | | |
|----------------|--------------|---|
| 8 | | - |
| | ICMP Timeout | |

Max Connections

Tamanho máximo da tabela de session tracking, ou seja, de conexões estabelecidas simultaneamente. O valor padrão é 300.000 segundos.

| * Max | | |
|--------|-----|--|
| 300000 | | |
| | Max | |
| | | |

TCP Loose

Habilita/Desabilita o levantamento de novas entradas de conexões já estabelecidas na tabela session tracking. O valor mínimo é 0 e o valor padrão é 1 (habilitado), para desabilitar, definir o valor 0.



TCP Max Retrans

Define o número máximo de pacotes TCP que podem ser retransmitidos sem receber um ACK aceitável do destino. O valor mínimo é 0 e o valor padrão é 3.

| * TCP Max Retrans | | |
|-------------------|---|---|
| | 3 | - |
| | | |

TCP max retrans

TCP Timeout Close

Define o valor padrão de *timeout* em segundos para conexões *TCP* no estado *CLOSE*, para serem removidas da tabela de session tracking. O valor mínimo é 0 e o padrão é 10 segundos.

| 1 | * TCP Timeout Close | |
|---|---------------------|---|
| | 8 | × |
| | TCP timeout clos | e |

TCP Timeout Close Wait

Define o valor padrão de *timeout* em segundos para conexões *TCP* com estado *CLOSE-WAIT*, para serem removidas da tabela de session tracking. O valor mínimo é 0 e o padrão é 30 segundos.

| 3 | * TCP Timeout Close Wait | |
|---|--------------------------|---|
| | 30 | - |
| | | |

TCP timeour close wait

TCP Timeout Established

Define o *timeout* em segundos para conexões *TCP* estabelecidas, para serem removidas da tabela de session tracking. O valor mínimo é 0 e o valor padrão é 180000 segundos (equivalente a 2,08 dias).

| * TCP Tin | neout Established | | |
|-----------|-------------------|-------------------------|---|
| 8 | | | • |
| | | TCP timeout established | |

TCP Timeout FIN Wait

Define o timeout em segundos para conexões TCP com estado FIN-WAIT-1 e FIN-WAIT-2, para serem removidas da tabela de session tracking. O valor mínimo é 0 e o valor padrão é 30 segundos.

| * TCP Timeout FIN Wait | | | |
|------------------------|----|--------------------|---|
| | 30 | | • |
| | Ti | meout TCP FIN wait | |

TCP Timeout Last ACK

Define o timeout em segundos para conexões TCP com o estado LAST-ACK, para serem removidas da tabela de session tracking. O valor mínimo é 0 e o valor padrão é 30 segundos.

| 3 | TCP Timeout Last ACK | |
|---|----------------------|---|
| | 8 | - |
| | | |

TCP timeout last ACK

TCP Timeout Max Retrans

Define o timeout em segundos para as conexões TCP que atingem o número máximo de retransmissões definido na opção "TCP max retrans" sem receber um ACK aceitável dos destinos. O valor mínimo é 0 e o valor padrão é 300 segundos.

| | * TCP Timeout Max Retrans | |
|---|---|---|
| | 60 | ▲ |
| | TCP timeout max retran | S |
| TCP Timeou | t SYN Recv | |
| Define o <i>timeout</i> em o valor padrão é 60 | segundos para conexões TCP com o estado SYN RECV, para seren segundos. | n removidas da tabela de session tracking. O valor mínimo é 0 e |
| | * TCP Timeout SYN recv | |
| | 60 | • |
| | TCP timeout SYN recv | |

TCP Timeout SYN Sent

Define o timeout em segundos para conexões TCP com o estado SYN SENT, para serem removidas da tabela de session tracking. O valor mínimo é 0 e o valor padrão é 120 segundos.

| * TCP Timeout SYN Sent | | |
|------------------------|----------------------|--------|
| 120 | | * * |
| | TCP timeout SYN sent | |

TCP Timeout Time Wait

Define o timeout em segundos para conexões TCP com o estado TIME WAIT, para serem removidas da tabela de session tracking. O valor mínimo é 0 e o valor padrão é 60 segundos.

| * TCP Timeout Time Wait | | |
|-------------------------|---|--|
| 30 | • | |
| | | |

TCP timeout time wait

TCP Retries

Define quantas vezes se tentará efetuar a retransmissão de pacotes TCP em uma conexão estabelecida. Quando esse limite é excedido, antes de cada nova retransmissão a camada de rede terá sua rota atualizada. O valor padrão é 3.



TCP SYN Retries

Determina no máximo quantas vezes serão retransmitidos os SYNs iniciais em uma tentativa de conexão TCP ativa. O valor padrão é 5 (equivale à cerca de 180 segundos) e o valor máximo é 255.



TCP SYN retries

TCP Reordering

Este valor define o limite máximo para que a reordenação seja efetuada em pacotes de um fluxo TCP sem que o protocolo assuma que haja perca destes pacotes e tenha o desempenho da sua inicialização reduzido. O valor padrão é 3.

| ATENCÃO: Não altere este valor sem ter completa certeza do que está fazendo. Ele atua detectando a reordenação dos pacotes e serve para |
|---|
| minimizar retransmissões (necessárias ou não) causadas pelo reordenamento dos pacotes da conexão. |

| 1 | * TCP reordering | |
|---|------------------|---|
| | 3 | • |
| | | |

TCP reordering

TCP Enhanced Retransmission Timeout (F-RTO)

F-RTO significa *Forward Retransmission TimeOut*, trata-se de um algoritmo cuja função é detectar e melhorar o limite de tempo na retransmissão ilegítima usando o protocolo TCP e SCTP (controle de fluxo).



UDP Timeout

Esse recurso define o tempo máximo que uma conexão permanece ativa em estado ocioso, ou seja, sem nenhum tráfego. Uma vez atingido o tempo limite configurado, o sistema remove todas as conexões do protocolo *UDP*, que estão no estado ocioso com o tempo limite configurado excedido. O valor mínimo é 0 e o valor padrão é 30 segundos

| * UDP Timeout | | |
|---------------|-------------|---|
| 30 | | * |
| | UDP timeout | |

UDP Timeout Stream

Define o timeout em segundos para conexões UDP STREAM (ASSURED). O valor mínimo é 0 e o valor padrão é 180 segundos.



UDP timeout stream

NGFW - Services - Proxy

A tela Proxy tem como função configurar o funcionamento dos proxies do sistema e também como a inspeção SSL atuará. A seguir analisaremos mais detalhadamente.

Para acessar esta tela, basta navegar até o menu/opção "Serviços > Proxy":

| 📽 Services 🗸 👻 | | | | | |
|----------------|----------------------------------|----------------------------|--|--|--|
| » | Firewall | | | | |
| » | Proxy | | | | |
| » | Web Cache | O | | | |
| » | Web Filter | O | | | |
| » | Application Control | O | | | |
| » | Intrusion Prevention | O | | | |
| » | Threat Protection | O | | | |
| » | SD WAN | 5 | | | |
| | SD-WAN | ω | | | |
| » | DHCP | 0 | | | |
| » » | DHCP | 9 0 0 | | | |
| » » » | DHCP DNS DDNS | 9 0 0 0 | | | |
| » » » | DHCP DNS DDNS VPN IPSEC | 9 0 0 0 0 0 | | | |

Services - Proxy

A tela abaixo será exibida:

| Naey | | | | |
|------------------|---------|---|----------------------|--|
| Pragi Intrani | - | | | |
| | | | | |
| to-ethenin | | | | |
| - Landhigter | | | | |
| Later marries | | | | |
| 9179 | | | | |
| + days | + law | | | |
| 14 | 475 | | | |
| 445 | 11 Gene | - | | |
| inglish many | | | Arthur Scatter Reels | |
| | | | | |
| | | | | |
| 100 | | | | |
| 004.12 | | | | |
| 194 | | | | |
| Peek10 | | | | |
| 1.00 | | | | |
| | | | (STERNE) | |
| No. 147 | | | figure Mine (n-10) | |
| | | | | |
| and tradition | | | | |
| | | | | |
| 1015 | | | | |
| Aug. 120 | | | C Aurola | |
| 1 CHILL CONTINUE | | | | |
| Louil Templete | | | | |
| | | | | |
| | | | | |

Proxy

Essa tela possui as seguintes opções:

- Proxy Services;
 Proxy SSH;
 SSL Inspection.

A seguir analisaremos os componentes da aba 'Proxy Services'

Proxy - Proxy Services

Vamos abordar os aspectos de segurança de rede por meio da análise dos Proxies, que são serviços de interceptação de conexões/tráfego de rede.

Os "Proxies" são sistemas ou aplicações que atuam como intermediários para as requisições clientes que solicitam recursos de outros servidores. Uma aplicação cliente conecta-se a um servidor "Proxy", solicitando algum serviço, ex.: "uma conexão", "uma página web", "um arquivo", ou "outros recursos" de outros servidores. O Proxy repassa esta requisição para o servidor remoto (normalmente na rede pública), e devolve sua resposta para o cliente interno (host da rede local).

Na maioria das vezes os Proxies são utilizados por todos os clientes de uma sub-rede e devido a sua posição estratégica, normalmente eles implementam um sistema de cache para alguns serviços. Além disso, como os *proxies* trabalham com dados das aplicações, para cada serviço é necessário um Proxy diferente.

Para configurar e habilitar os serviços de Proxy, caso já não esteja selecionado, clique na aba, conforme demonstrado abaixo:



Aba Proxy Services

A tela abaixo será exibida:

| 0xy | | | | |
|--|--------|-------|----------------------|---|
| ng bernen () må in | - | | | |
| | | | | h |
| ta-Monia | | | | |
| - cardhone | | | | |
| Long mar to | | | | |
| | | | | |
| ALL- | | | | |
| A Dest | + 1ge | | | |
| | | SIS | | |
| 445 | 11.000 | - U 8 | | |
| Inglish many | | | Appleptication Reads | |
| | | | | |
| | | | | |
| | | | | |
| 0(4)12 | | | | |
| 1011 | | | | |
| Pee 12 | | | | |
| | | | | |
| and the second s | | | | |
| Tel: (12) | | | Ref 400 | |
| | | | | |
| min bradder | | | | |
| | | | | |
| tors | | | | |
| Ave 120 | | | hereite | |
| Freed Solders | | | | |
| | | | | |
| I mult langings | | | | |
| | | | | |



O Blockbit NGFW, inclui serviços de segurança por meio de Proxies ativos, os protocolos e serviços suportados são:

- Root Certificates;
 HTTP;
 FTP;
 SSH;
 SMTP;
 POP3.

A seguir analisaremos cada painel desta tela.

Root Certificates

O Campo certificates é utilizado para a seleção de certificado de autoridade (CA) remoto para uso no serviço de proxy.

| Proxy | |
|------------------------------|---|
| Pray Services 80. Repetition | |
| | - |
| Certificade | |
| * Caritificate | |
| Canal RentTa | |

Proxy - Certificates overview

As CAs apresentadas neste campo de seleção são Certificados Remotos e devem ser importadas em "Configurações > Certificados > aba Autoridade".

Para mais detalhes de como realizar a importação, clique aqui.

Proxy HTTP

O recurso *Proxy HTTP* é fornecido integrado pelo serviço *Web Cache* que consiste em oferecer como principal recurso, entre as suas diversas funcionalidades, o acesso à Internet para usuários de uma rede ou sub-rede que não possuam acesso direto à rede pública, de forma simples, segura e eficiente.

Além disso, também contribui para controlar o uso irrestrito dos serviços web e diminuir o consumo de banda, já que possui os mecanismos de "Web caching" e integração ao serviço de "Web Filter" com controle de acesso por filtros de "Conteúdo" e "Aplicativos", e ao serviço de "Antimalware" para filtros de arquivos comprometidos, através das políticas de segurança que restringem a navegação dos usuários.

O Blockbit UTM opera com proxy nos modos:

Transparente

Neste modo de operação o proxy é configurado para permitir o tráfego Https somente sob a interceptação SSL, o que exige a importação e instalação da CA (Certification Authority) para todos os dispositivos da rede.

Para permitir o tráfego SSL no modo by-pass é necessária a configuração com filtro por "SSL COMMON NAME" para exceção nas políticas de segurança.

Explícito

Para acesso ao proxy no modo explícito é necessário configurar o navegador WEB dos dispositivos da rede para acesso ao proxy no modo configurado.

Este modo de acesso exige a configuração de uma política de segurança com permissão de acesso aos serviços WEB no modo Proxy Explícito.

Configuração

Para configuração do Proxy HTTP, analise as considerações abaixo. Neste painel você configura as portas suportadas:

| 107 I wrmi - 4 | |
|----------------|-----------------------|
| | |
| ati sma | |
| Explicit Drawy | Authorities then Mode |

Proxy HTTP

O serviço é pré-configurado para permitir acesso aos serviços web padrões "HTTP (porta 80) e HTTPS (porta 443)". As portas de serviços são configuráveis com suporte aos protocolos "HTTP e HTTPS versões 1.0 e 1.1".

Para adicionar uma nova porta, clique no botão [____]. Caso deseje remover uma porta clique no botão [____].

Em Port digite a porta desejada, em Type é possível selecionar o protocolo que será utilizado no proxy, existem 3 opções para as caixas de seleção:

- HTTP: Neste modo a porta se utilizará do protocolo HTTP;
- HTTPS: Neste modo a porta se utilizará do protocolo HTTPS;
- HTTP/HTTPS: Caso este modo seja ativado, ambos os protocolos HTTP e HTTPS serão aplicados para a mesma porta, porém, este modo fará
 com que o proxy funcione apenas em modo explícito, assim sendo, todas as regras utilizadas no proxy transparente, serão ignoradas. Por este
 motivo, a mensagem de sistema ilustrada abaixo é exibida ao selecionar essa opção:

HTTP and HTTPS detected for the same port, or functional proxy service only in explicit mode.

Proxy HTTP/HTTPS

| Atenção: Caso o modo HTTP/HTTPS seja ativado em qualquer porta, todas as regras de proxy utilizadas no modo transparente ficarão DESATIVADAS. Para reativar é necessário PARAR de utilizar o modo HTTP/HTTPS em qualquer porta. | | | | |
|---|--|--|--|--|
| Explicit Proxy : Ao checar esta caixa de checagem o proxy em modo explícito será ativado e o campo de modo de autenticação ficará disponível. Neste campo é necessário definir a porta do seu servidor de proxy, por padrão, o sistema utilizará o objeto de serviço "UTM-PROXY" com a porta <i>TCP</i> 128; Authentication Mode: Permite selecionar qual o tipo de autenticação que será efetuado, as opções são: Basic: Caso esta opção seja selecionada, um pop-up requisitando a autenticação será exibido no navegador; Captive Portal: Caso esta opção seja selecionada, a autenticação será efetuada através do captive portal, para mais informações a respeito, consulte esta página; | | | | |
| Para salvar todas as alterações, clique em [| | | | |
| Após salvar, para que o <i>proxy</i> entre em ação será necessário acessar a fila de comandos [] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos. | | | | |

A seguir analisaremos o proxy FTP.

Proxy FTP

Nesta seção vamos abordar o serviço de Proxy FTP, uma aplicação integrada ao Blockbit UTM com a finalidade de inspecionar o tráfego de transferência de arquivos entre as redes locais e a rede pública (Internet) sob o protocolo FTP de modo seguro.

A sua função básica é possibilitar ao administrador através das "Políticas de segurança" o tratamento dos pacotes e transferências de arquivos por meio do tráfego das portas FTP "20 e 21/TCP".

Configuração

Para configuração do Proxy FTP, analise as considerações abaixo:



Proxy FTP

• [1] Port 21: Ao habilitar esta caixa de checagem, a porta de conexão com os servidores FTP Remotos (21/TCP) é ativada.

Suporte:

• Modo: [FTP Ativo].

| O funcionamento do Proxy FTP requer a configuração de uma "Política de Segurança" com o filtro de conteúdo Web Proxy habilitado para o protocolo FTP. |
|---|
| Para salvar todas as alterações, clique em [|
| Após salvar, para que o <i>proxy</i> entre em ação será necessário acessar a fila de comandos []] e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos. |
| 100 |

Caso seja necessário integrar filtro Malware Scanning por meio do tráfego Proxy FTP, será necessário efetuar a habilitação e configuração do serviço Threat Protection.

Seu funcionamento depende da configuração de perfis por "Políticas de Segurança".

A seguir analisaremos os recursos de SMTP.

Proxy SSH

Nesta seção vamos abordar o serviço de Proxy SSH, e como configurá-lo no NGFW.

Na configuração do Proxy SSH, o Blockbit situa-se entre o cliente e o servidor. O Proxy SSH habilita no Blockbit a criptografia interna e externa de conexões SSH e garante que possíveis atacantes/invasores não utilizem tunelamento para aplicações e conteúdos indesejados. A criptografia SSH não requer certificados e o Blockbit NGFW automaticamente gera uma chave utilizada para a criptografia quando a conexão é iniciada. Durante o processo de inicialização, o Blockbit checa se já há uma chave, caso não, uma é gerada. O proxy utiliza a chave para descriptografar as sessões SSH em todos os sistemas virtuais configurados no Blockbit e em todas as sessões SSH v2.

O uso do SSH deve ser limitado a administradores que necessitam acessar os serviços de rede, logar todo o tráfego, e também considere configurar o Multi-Factor Authentication para garantir que somente usuários legítimos possam utilizar SSH para acessar dispositivos, ação esta que pode reduzir a probabilidade de potenciais ataques.

Configurando o Proxy SSH

No menu principal do NGFW, devemos ir para Serviços > Proxy > Proxy Services. Nesta seção, encontraremos a opção para habilitar a porta 22, inicialmente devemos marcar a opção habilitando-a:

| SSH | |
|-----------|--|
| V Port 22 | |

Serviço de Proxy SSH

A seguir devemos ir para Configurações > Autenticação > Usuários, nesta outra seção podemos criar um usuário ou editar um pré-existente. A opção "Permitir acesso ao shell (SSH)" e "Permite executar comando remoto no shell (SSH)" devem ser marcadas:

| Name | E-mail | | | |
|---|------------|-----------------|-----|--------------------|
| umr_1 | aner_1@iab | stijnel | | |
| Login | Domain | | | |
| user_1 | labeli net | | ÷ | |
| Password 介介介 | Confirm | | | |
| | | | | |
| Groups of clomain | | tearth | ۹ | |
| | | | - | |
| | | | | |
| | | | | |
| User groups | | | | |
| smartphone | | | | |
| | | | | |
| Enabled Enable shell (SSH) access for this user Enable exec remote command in shell (SSH) |) | | | |
| | | Pastword expire | Sam | |
| | | | | Pormionãon do unuá |

Na sequência, devemos ir para Serviços > Threat Protection > Perfis e configurar um perfil de Threat Protection, habilitando a "verificação de Malware" e o "Bloqueio de ameaças":

| offes Seiturgs | Threat Protection Profile | | | .) |
|----------------|---------------------------|---|-----------------|----|
| 1 mand | General | | | |
| Name | * Name | | | |
| Perfit-Ast | Perfil-AV. | | | |
| | Description | | | |
| | Test | | | 1 |
| | Threat Protection | | | |
| | Malware Scanning | | Threat Blocking | |
| | 3 liekthol | = | T Balancia | = |
| | | | | |

Configuração de perfil de Threat Protection

A seguir, devemos criar uma Política de inspeção em Políticas > IPv4 > Criar Política, e marcar a opção de Threat Protection, bem como selecionar o perfil de Threat Protection que criamos previamente:

| ;; ~ PH000 | | | | | | | 0.00 |
|----------------|--------------|---------------------|--|--|---------|---------------|----------|
| | | 1.00 | | All the second s | 1000 | No. and a | 1.00 |
| (I B) Provides | | MI . | 670 1977 | - | ib Hand | | C / 21 0 |
| | Create PoScy | | | | | ж | |
| | Papatas | rustin | | | | | |
| | Genuter | Sit mapsets | 0 | | | | |
| | Instantion. | Artistics (Pa | within . | | | | |
| | Roteing | C Treast Prote | the l | | | | |
| | Worded | Autoria and Autoria | and and a second se | | | | |
| | | | | | | | |
| | | Web Rher | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | Gamili | |

Criação de Política com Threat Protection ativado

Tendo finalizado as configurações, devemos iniciar uma conexão SSH normalmente (do host cliente para o servidor de destino). No terminal o usuário deverá inserir o login e IP/host de destino do SSH, como no seguinte exemplo: # ssh user_1@server1.blockbit.com.

Após isso, o Proxy SSH irá interceptar a comunicação, exigir uma autenticação local no Blockbit, e a verificação de segurança será executada normalmente. Assim, o usuário e senha que devemos utilizar são os que cadastramos no Blockbit, em "Configurações > Autenticação", com a opção de "Permitir SSH" habilitada.

A seguir uma imagem do terminal solicitando login do Blockbit, todavia ainda não se trata dos dados do SSH:



Após os testes do NGFW com o servidor SSH no destino final, estas informações são exibidas na tela e a opção se a conexão deve ser continuada será exibida:

```
estel@venon2: s ssh administrator@172.23.21.185
 Welcome to Block-bit 55H-Proxy *
You must login to NGFW first to access 172.23.21.185
ogin: user 1
assword:
tarting Auditing....
LIENT
gen] software: OpenSSH 8.2pl
security
cve) CVE-2821-36368 -- (CVS5v2: 3.7) trivial authentication attack to bypass FIDD tokens and SSH-ASKPASS
cve) CVE-2821-28041 -- (CVS5v2: 7.1) double free via sch-agent
cve) CVE-2820-14145 -- (CVS5v2: 5.0) information leak via algorithm negotiation
ERVER
gen) software: OpenSSH 8.9p1
gen) compatibility: OpenSSH 8.5+, Dropbear SSH 2018.76+
gen) compression: enabled (zlib@opensch.com)
                                                            - [info] available since Open55H 5.7, Dropbear 55H 2013.62
                                                            - [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
                                                                 [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
kex) sntrup761x25519-sha512gopenssh.cum -- [info] available since OpenSSH 8.5
kex) diffie-hellman-group-exchange-sha255 (2048-bit) -- [info] available since OpenSSH 4.4
                                                                [info] available since Open55H 7.3, Dropbear 55H 2016.73
[info] available since Open55H 7.3
                                                            -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
kex) diffie-heliman-group14-sha256
key) rsa-sha2-512 (3072-bit)
key) rsa-sha2-256 (3072-bit)
                                                                [info] available since OpenSSB 7.2
                                                                           using weak random number generator could reveal the k
```

Resultados da análise de vulnerabilidade

Deste modo finalizamos a configuração do Proxy SSH e acesso ao servidor.

fin) ssh-rsa: SHA256:J1Rw0IvN1x5+t2VBy60idfXMUL3diCja4H/3XKdaP/U algorithm recommendations (for DpenSSH 8.9) rec -- mac algorithm to remove rec) -hmac-shal-etm@openssh.com -- mac algorithm to remove rec) rec -umac-128@openssh.com -- mac algorithm to remove rec) rec) -umac-64-etmoopenssh.com mac algorithm to remove rec) -umac-64@openssh.com -- mac algorithm to remove

Caso haja alguma notificação indicando a troca de "fingerprint" a mesma deve ser ignorada, uma vez que o SSH está sendo conectado no Blockbit.

fin) ssh-ed25519: 5HA256:VHmMgf0td8rdNth0D2Zf9W+YRTYyjp0k8Y8uSaS2c9A

Liech spincespage

fingerprints

Continue(y/N):

The authenticity of host '172.23.21.185 (172.23.21.185)' can't be established. ECDSA key fingerprint is SHA256:nvkWoDCDznPWm3X019twocOKYOfAux2xB70p0V6jtrQ. ECDSA key fingerprint is MD5:ed:f5:63:69:3c:fd:4e:41:02:4d:8a:3d:b9:e7:49:21. Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '172.23.21.185' (ECDSA) to the list of known hosts. administrator@172.23.21.185's password:

Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86 64)

* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com

* Support: https://ubuntu.com/advantage

System information as of Tue Feb 14 10:47:29 AM -03 2023

 System load:
 0.4716796875
 Processes:
 249

 Usage of /:
 10.5% of 78.19GB
 Users logged in:
 0

 Memory usage:
 42%
 IPv4 address for ens160:
 172.23.21.185

 Swap usage:
 77%
 7%
 7%
 10.5%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

5 updates can be applied immediately. To see these additional updates run: apt list --upgradable

Last login: Mon Feb 13 15:29:26 2023 from 172.31.150.48 administrator@mail:~\$

Proxy SMTP

Nesta seção vamos abordar o serviço de *Proxy SMTP*, uma aplicação integrada ao Blockbit NGFW com a finalidade de inspecionar o tráfego de *E-mails* entre "Cliente-Servidor" e "Servidor-Servidor" sob o protocolo *SMTP* de modo seguro.

A sua função básica é possibilitar ao administrador através das "Políticas de segurança" o tratamento dos pacotes e transferências de arquivos por meio do tráfego das portas SMTP, "[25, 465, 587/TCP]".

Caso o tráfego for SSL, ao habilitar proxies SMTP e POP3 será necessário habilitar um perfil de SSL Inspection na Política IPv4 ou IPv6 de liberação do tráfego, para mais informações sobre como criar políticas IPv4 consulte esta página, sobre IPv6 consulte esta página.

Configuração

Para configuração do Proxy SMTP, analise as considerações abaixo:

| (arre) | |
|-------------------|--------------------------------|
| (1) Physics 25 | Mircls 4(0 |
| C factorier | Print at any light in (27–20). |
| | |
| Adminute relation | |
| | |
| | |

Proxy SMTP

- [Y] Porta 25: Habilitação do porta padrão de conexão com os servidores SMTP Remotos. Porta [SMTP 25/TCP]. Em conexões da porta SMTF 25 normalmente se aplica a conexões entre servidores SMTP.
- [Y] Porta 465: Habilitação da porta SMTPS de conexão com os servidores SMTP over SSL/TLS Remotos. Porta [SMTPS 465/TCP]. O tráfego SSL/TLS cliente-servidor exige que a origem possua um certificado digital que seja conhecido pelo servidor SMTP remoto.
- [1] Porta 587: Habilitação da porta SMTP Submission de conexão com os servidores SMTP Remotos. Porta [SMTP Sub 587/TCP].
- [M] Filtro de Spam: Habilita o filtro de spam. A função do filtro de spam consiste em uma variedade de técnicas como filtragem de DNS e classificação de ameaça por pontuação, analisa o conteúdo de um e-mail de acordo com o nível do filtro estabelecido pelo administrador. Procura desde quantidades excessivas de conteúdo HTML até o domínio do servidor do remetente. Basta atribuir um grau de aceitabilidade após ativar o filtro para moderar o nível de análise.

O Tráfego SMTP Submission exige a autenticação cliente-servidor no protocolo SMTP, o que dificulta o uso indevido de contas de email ou de estações máquinas "zumbis", método bastante utilizado por spammers.

Utilize esta porta nas conexões cliente-servidor por meios dos clientes de e-mail. Ex.: "Thunderbird e Outlook".

P [Adicionar Cabeçalho: Este campo contempla um recurso de "Sinalização" que devolve ao usuário um conteúdo "Informativo" quanto ao tratamento aplicado sobre o E-mail enviado no cabeçalho do respectivo E-mail. Ex.: "x-header: E-mail Infectado com vírus.".

| ž | Add Header |
|---|-----------------|
| | heiderinflicted |

Proxy SMTP - Add Header

| O funcionamento do Proxy SMTP requer a configuração de uma "Política de Segurança" com o filtro de conteúdo Email Protection habilitado para o protocolo SMTP. | | | | | |
|--|--|--|--|--|--|
| Para salvar todas as alterações, clique em [| | | | | |
| Após salvar, para que o <i>proxy</i> entre em ação será necessário acessar a fila de comandos [informações a respeito da fila de comandos acesse a página: NGFW - Fila de comandos. | | | | | |
| Caso seja necessário integrar filtro <i>Malware Scanning</i> por meio do tráfego <i>Proxy SMTP</i> , será necessário efetuar a habilitação e configuração do serviço <i>Threat Protection</i> . Seu funcionamento depende da configuração de perfis por "Políticas de Segurança". | | | | | |
| Caso haja a necessidade de verificar os bloqueios feitos pelo Proxy SMTP, é possível fazê-lo via interface de comando (CLI), para saber mais clique aqui. | | | | | |

A seguir analisaremos os recursos de POP3.

Proxy POP

Nesta seção vamos abordar o serviço de *Proxy POP*, uma aplicação integrada ao Blockbit UTM com a finalidade de inspecionar o tráfego de *E-mails* entre "Cliente-Servidor" sob o protocolo *POP* de modo seguro.

A sua função básica é possibilitar ao administrador através das "Políticas de segurança" o tratamento dos pacotes e transferências de arquivos por meio do tráfego das portas *POP*, "[110, 995/*TCP*]".

| \odot | Caso o tráfego for SSL, ao habilitar proxies SMTP e POP3 será necessário habilitar um perfil de SSL Inspection na Política IPv4 ou IPv6 de |
|---------|--|
| libera | cão do tráfego, para mais informações sobre como criar políticas IPv4 consulte esta página, sobre IPv6 consulte esta página. |

Configuração

0

Para configuração do Proxy POP, analise as considerações abaixo:

| PDP3 | | |
|----------------|---------|--|
| Part 113 | Europe. | |
| E-risitSatjett | | |
| | | |
| | | |

Proxy POP3

- 🔹 🔀 Port 110: Habilitação da porta padrão de conexão com os servidores POP Remotos. Porta [POP3 110/TCP];
- [Yort 995: Habilitação da porta POP3S de conexão com os servidores POP3 over SSL/TLS Remotos. Porta [POP3S 995/TCP]. Este recurso aumenta a segurança no tráfego POP3 cliente-servidor. O tráfego SSL/TLS, exigem que a origem possua um certificado digital que seja conhecido pelo servidor POP remoto;

| Utilize es | sta porta nas conexões cliente-servidores por meios dos clientes de e-mail. Ex.: "Thunderbird e Outlook". |
|------------|--|
| | |
| | |
| • [1] E | Email Subject: Este campo contempla um recurso de "Sinalização" que devolve ao usuário um <i>E-mail</i> de notificação do tipo "Mailer |
| Posina | |
| | |
| | |
| | |
| | 🔀 L-mail Salajost |
| | Constantizioned Anticipat |
| | Verenzielen versielen vers |
| | E Frank Salaged Werkenis Erevel Exercise Proxy POP3 – E-mail Subject |

 E-mail Template: Este campo contempla o "Conteúdo do corpo" do E-mail de notificação "enviado" para a caixa postal local do usuário final para cada e-mail identificado como "Infectado". Os valores dos campos em destaque abaixo correspondem aos dados de variáveis retornados pelo tratamento do "Antimalware".

| Virus name: %VIRUSNAME% |
|---|
| (Supposed) Sender of the email: |
| %MAILFROM% |
| Sent To: |
| %MAILTO% |
| On Date: |
| %MAILDATE% |
| Subject: |
| %SUBJECT% |
| Connection data: |
| <pre>%PROTOCOL% from %CLIENTIP%:%CLIENTPORT% to %SERVERIP%:%SERVERPORT%</pre> |
| |

| | * E-vold longuists |
|------------------------------------|--|
| | State states: *Society Section 25 Section 2 |
| | Proxy POP3 - E-mail Template |
| O funcio o protocolo P | onamento do Proxy POP requer a configuração de uma "Política de Segurança" com o filtro de conteúdo Email Protection habilitado para OP. |
| Para salvar tod | as as alterações, clique em []. |
| Após salvar, pa informações a l | ara que o <i>proxy</i> entre em ação será necessário acessar a fila de comandos []] e aplicar as alterações efetuadas. Para mais respeito da fila de comandos acesse a página: UTM - Fila de comandos. |
| Caso se serviço Threa | aja necessário integrar filtro <i>Malware Scanning</i> por meio do tráfego <i>Proxy POP,</i> será necessário efetuar a habilitação e configuração do It Protection. |

Seu funcionamento depende da configuração de perfis por "Políticas de Segurança".

Isso conclui a análise dos proxies.

Proxy - SSL Inspection

O SSL Inspection atua interceptando o tráfego SSL Inbound/Outbund e inspecionando conteúdo criptografado, utilizando-se deste recurso é possível selecionar o conteúdo que se deseja inspecionar através de políticas de conformidade.

Este recurso atua basicamente conforme os seguintes passos:

- 1. Atuando Inicialmente é efetuada a captura das comunicações HTTPS criptografadas entre cliente e servidor;
- 2. Objetivando manter a segurança, uma conexão SSL é criada;
- 3. A inspeção propriamente dita é efetuada de maneira segura permitindo filtrar conteúdo inseguro e indesejado;
- 4. Por fim, após encriptar novamente as informações, uma nova conexão SSL é criada para dar continuidade à comunicação que foi interceptada.

| O limite de perfis de SSL Inspection equivale à metade do número de CPUs do appliance. Por exemplo: Um appliance com 32 CPUs terá um limite de 16 perfis. | |
|--|--|
| | |

Clique na aba "SSL Inspection".



Surgirá a Tela de "SSL Inspection". Ela é composta pelas colunas "Name", "Description", "Mode", "Version" e "Actions". Além disso, no topo direito da tela está localizada a barra de busca e o menu de ações.

| Ргоху | | |
|--------------------------|---------------|-----------------|
| Programmer 201 Impediate | | |
| 1 month | | |
| tane . | Beactiptice | Actions |
| 🗇 minipittio | THE PROMITION | / 8 |
| | | • 1) · (40 mm · |

Proxy - SSL Inspection



A seguir, o menu de ações será analisado e posteriormente nos aprofundaremos no conteúdo das colunas do painel SSL Inspection.

Proxy - SSL Inspection - Menu de ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



SSL Inspection - Menu de Ações.

O menu é composto das seguintes opções:

• Delete Profile.

A seguir, cada opção do menu de ações será detalhada.

Proxy - SSL Inspection - Menu de Ação - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de SSL Inspection.

Analisaremos a criação de um perfil de SSL Inspection e também veremos em detalhe as seções:

- General;
- Exception.

Inicialmente, clique no menu de ações []. Após, clique na opção "Create Profile":



SSL Inspection - Create Profile

A seguir, a tela "SSL Profile" será exibida:

SSL Profile

| • Name | |
|--|--------|
| Description | |
| Number of Workers | |
| 1 | |
| Certificate | |
| Local Remote CA | |
| Protocols HTTP5 SMTP5 POP35 Block invalid certificates | |
| Exception | |
| Dictionary | |
| Web Categories | × |
| | 12 |
| | |
| | Cancel |
| | |

General

Neste painel são efetuadas as configurações gerais do perfil SSL.

X

| | - | | |
|-----|------|---------|-----|
| 200 | - Pa | 11 E I | 100 |
| | | ~ ~ ~ ~ | - |
| | | | |

| General | |
|----------------------------|--|
| * Name | |
| Description | |
| | |
| Number of Workers | |
| 1 | |
| Certificate | |
| Lacal Remote Cé | |
| Protocols | |
| I HTTPS | |
| SMTPS | |
| P0P35 | |
| Block invalid certificates | |

×



- Name: Definir um nome para o perfil. Ex.: SSL Inspection;
- Description: Definir uma descrição para o perfil. Ex.: SSL Inspection;
- Number of Workers: Permite definir o número de workers (processos) por perfil de inspeção, limitado ao número de CPUs detectadas automaticamente pelo sistema.
- Certificate: Permite a seleção do certificado CA que será utilizado pelos serviços de Proxy. Campo não obrigatório e, caso fique vazio, o certificado utilizado pelo proxy será o padrão definido na aba "Serviços do Proxy";
- Protocols: Determina em protocolos o SSL Inspection será aplicado. As opções disponíveis são: HTTPS, SMTPS e POP3S.
- Block Invalid certificates: Caso esta caixa de checagem tenha sido marcada [], todas as vezes que a inspeção SSL detectar um certificado inválido, será efetuado um bloqueio.

O Certificado CA utilizado no perfil de SSL Inspection tem prioridade sobre o certificado utilizado na seleção da aba "Serviços de Proxy".

Exception

Neste painel são configuradas as exceções do perfil SSL:

533

| Exception | |
|----------------|---|
| Dictionary | |
| | ~ |
| Web Categories | |
| | |

| Cancel | Save |
|--------|------|

SSL Inspection - SSL Profile - Exception

- Dictionary: Selecione itens pré-definidos como exceção para o Perfil SSL.
- Web Categories: Ao marcar o campo Web Categories [], será possível selecionar entre as categorias disponíveis quais serão marcadas como exceção para o Perfil SSL.

0

Se um objeto ou uma categoria for adicionado às exceções de SSL, o pacote não irá passar pelos modos de Proxy e Flow-based Inspection Engine, do novo fluxo de inspeção de pacotes da Blockbit, ou seja, o pacote será encaminhado para o modo de Egress Filtering (NAT, IPSec Compression, Traffic Shapping, Routing etc).

Para consultar o fluxo de inspeção de pacotes, consulte a arquitetura do UTM.

| Inspection Exception | | |
|----------------------|---------------|---|
| | | 0 |
| Alphanumeric | | |
| Credit Card | | |
| Email Address | | |
| IP Address | | |
| Link HTML | | |
| URG | | |
| URL Insage | | |
| | SSL Exception | |

Este recurso atende os casos de condições específicas de Aplicações e Serviços que não leem os certificados do sistema, também não tem a opção de importar o certificado em sua aplicação, casos muito comuns para serviços e aplicativos de "Bancos, instituições financeiras e Governo", e é muito útil para os casos que se pretende permitir o tráfego *bypass* destes serviços e aplicações para toda a rede;

• Web Categories: Este campo segue a mesma lógica do campo Dictionary, no Web Categories é possível selecionar categorias Web para

aplicar filtros de "Exceção". Para selecionar as categorias, clique no botão [], escolha as categorias desejadas marcando as **caixas de checagem** [] que serão consideradas como exceção, conforme demonstrado abaixo:

Add Category

٣

Ŀ.

| All V | ~ |
|---------------------------------------|-----|
| Lingerie and Swimsuit | ^ |
| 👻 🔽 Business and Economy | |
| Financial Data and Services | |
| ▼ Drugs | |
| Abused Drugs | |
| Prescribed Medications | |
| Supplements and Unregulated Compounds | |
| Marijuana | |
| ✓ Education | |
| Educational Institutions | |
| Cultural Institutions | |
| Educational Materials | |
| Reference Materials | |
| ▼ Entertainment | |
| MP3 and Audio Download Services | |
| Gambling | ~ |
| Cancel | ave |
| SSL Inspection - Add Category | |

.

4

]:

Х

Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no menu de ações [

| Q | ~ | |
|--------------|---|--|
| Select All | | |
| Deselect All | | |

SSL Inspection - Add Category - Menu de Ações



O permition chado com sucesso.

A seguir veremos como apagar um perfil em Delete Profile.

Proxy - SSL Inspection - Menu de Ação - Delete Profile

Através do botão "Delete Profile" é possível deletar os Profiles selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*:

| тоху | | | |
|----------|-----------------|---------------|------------------|
| frong (a | waa SiLmpecton | | |
| 2.000 | • | | a + |
| | Name | Decipter | Actions |
| 8 | Test | 544 - | <u>× 1</u> |
| | bia. Impeccia e | all important | / 1 |
| | | | a (1) a lationer |



| 2. Entre no menu de ações [] e clique na opção "Delete | Profile". |
|---|------------------------------|
| | ۹ 🗸 |
| | Create Profile |
| | Delete Profile |
| SSL | Inspection – Delete Profile. |

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os Profiles selecionados:

| Delete Profile | X |
|---|---------------|
| Are you sure you want to delete: Test ? | |
| | Cancel Delete |

SSL Inspection - Mensagem se deseja deletar os profiles



Após realizar esses procedimentos, os profiles terão sido deletados com sucesso.

Proxy - SSL Inspection - Colunas

A seguir explicaremos cada coluna da aba SSL Inspection:

| Marine Contractor | | |
|-------------------|-----------------|-------------|
| 1 month | | |
| New | Leastlyfiles | Actions |
| The superfee | Bill Index Tark | 23 |
| | | - [1] . 201 |



A seguir explicaremos cada coluna:

- Caixa de Seleção[]: Seleciona o profile.
- Name: Apresenta o nome do profile cadastrado;
- Description: Apresenta a descrição do profile cadastrado;
- Actions: A coluna "Actions" é composta por vários botões:

• Botão Edit []: Permite editar as configurações do profile adicionado na opção Create Profile do menu de ações;

• Botão Delete []: Deleta o profile, é o equivalente a opção Delete Profile do menu de ações.

UTM - Services - Web Cache

O mecanismo de "Web Cache" consiste em minimizar os custos de acesso à Web, reduzir a latência neste tipo de acesso é uma questão muito importante, ainda mais quando considera-se que mais de 60% do tráfego de internet atual é gerado nos acessos web (HTTP e HTTPS).

O sistema de cache armazena localmente objetos (páginas HTMLS, imagens e arquivos) da internet, esse recurso melhora significativamente a qualidade do serviço oferecido aos usuários.

A configuração do serviço Web Cache é definida pela configuração dos controles de cache e ainda conta com o recurso de redirecionamento do tráfego para um proxy hierárquico.

Para acessar esta tela, basta selecionar a opção "Web Cache".



Services - Web Cache

A tela abaixo será exibida:
| Cache | | 8 | Hierarchy | | r. |
|---|-------------|---|-------------|--------------|-----|
| star of the cache in memory | - 64 (V) PM | | Endled | | |
| maximum ear of the object rememory | 10 m | | P Address | Fiel | |
| man cashe dia | 3 🗐 🚥 | | 0 | > | 0 |
| Nitramum object solo an disk | 4 M 88 | | Arbertkated | Тури | |
| Dynamic content cache | | | Enabled | Titler Maren | 4)) |
| Featorsk Google Mapx Mith Yoloo Sourcebryge Dokenhoeth Worksen Update Romane | | 1 | Der | Paswerd | |
| Camplion cache | | | | | |
| the last | | | | | |

Web Cache

A tela Web Cache comporta os seguintes painéis:

- Cache;Hierarchy.

A seguir analisaremos os componentes do painel Cache.

Web Cache - Cache

No quadro [*Cache*] temos os recursos de gerenciamento e controle do serviço de *cache* que armazena em uma base local os documentos retornados dos servidores *WEB* requisitados, dessa forma é possível reaproveitar o acesso a esses documentos sem que haja a necessidade de estabelecer uma nova conexão com o servidor remoto.

Configuração da cache em memória e disco.

Tamanho máximo e mínimo dos arquivos referentes aos acessos Web que serão salvos/carregados em memória quando do 1º (primeiro) acesso para entrega imediata aos usuários quando requisitados novamente.

Cache de conteúdos dinâmicos.

Existem conteúdos que são disponibilizados pelos servidores WEB de forma dinâmica e distribuída, são os chamados CDN (Content Delivery Network). Esse recurso utiliza uma tecnologia que responde a requisição do usuário pelos servidores web mais próximos da sua localização geográfica.

Normalmente a resposta a requisição é atendida de forma dinâmica onde cada servidor da pilha de servidores próximos a requisição responde fragmentos do conteúdo solicitado.

Lista de serviços Web de conteúdos dinâmicos suportados:

- Facebook;
- Google Maps;
- MSN Video;
- Sourceforge Downloads;
- Windows Update, Youtube.

O Blockbit UTM possui um recurso de proxy capaz de concatenar estes fragmentos do conteúdo solicitado e guardar cache mesmo de origens diversas.

Exceção de cache, configurável por expressões regulares.

| Cache | | |
|--|----|------|
| Size of the cache in memory | 64 | и мв |
| Maximum size of the object in memory | 16 | MB |
| Disk cache size | 1 | ✓ GB |
| Minimum object size on disk | 4 | и кв |
| Dynamic content cache | | |
| Facebook Google Maps MSN Video Sourceforge Downloads Windows Update Youtube | | |
| Exception cache | | |
| Select | | |

Web Cache Settings

| Para salvar todas as alterações, clique em [| B J. | | |
|--|--|---|--|
| Após salvar, para que as alterações tenham informações a respeito da fila de comandos : | efeito será necessário acessar a fila de comandos [acesse a página: UTM - Fila de comandos. | 1 |] e aplicar as alterações efetuadas. Para mais |

Após realizar esses procedimentos as configurações de Cache terão sido configuradas com sucesso.

UTM - Services - Application Control

Através do recurso Application Control é possível controlar caso os usuários terão permissão de acesso à determinadas aplicações ou caso não estarão autorizados a utilizar alguma aplicação. As aplicações são divididas entre categorias possibilitando que o administrador determine de forma específica o acesso de cada item.

Caso um Application Control seja adicionado em uma política o Web Filter é habilitado nesta política, mesmo que um Web Filter propriamente dito não se tenha sido selecionado. Para mais informações a respeito de Web Filter, consulte esta página.

Para acessar esta tela, basta selecionar a opção "Application Control".



Services - Application Control

A tela abaixo será exibida:

| Application Control | | |
|---------------------|---------------------|---------|
| notia | | |
| | | |
| hen | Description | Actions |
| | | |
| | | |
| | | |
| | | |
| | Application Control | |

A seguir, o menu de ações será analisado e posteriormente nos aprofundaremos no conteúdo das colunas do painel Application Control.

Services - Application Control - Menu de ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



Application Control – Menu de ações

O menu é composto das seguintes opções:

- Create Profile;
- Delete Profile.

A seguir cada opção do menu de ações será detalhada.

Services - Application Control - Menu de ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de Application Control.

Analisaremos o processo de criação de um perfil em Application Control e também detalharemos as seguintes seções:

- General;
- Application Control.

| Para acessar, clique no menu de ações [| ~ |], e | selecio | ne a op | oção "Cre | eate | Profile"; | ; |
|--|---|------|---------|---------|-----------|------|-----------|---|
| | | | | | ٩ | | ~ | |
| | | | | | Create | Pro | ofile | |
| | | | | | Delete | Pro | file | |

Application Control - Create Profile

Após, a tela "Create Profile" será exibida. Neste painel é possível efetuar as configurações gerais e definir as permissões das aplicações utilizadas nesse perfil.

| reate Application Control profile | |
|-----------------------------------|---|
| General | |
| • Name | |
| Description | |
| | 2 |
| Workers | |
| 1 | |
| Application Control | |
| Applications | |
| | |
| | |

Application Control - Create Profile

General

Em "General" temos as seguintes caixas de texto:

| General | |
|-------------|--|
| • Name | |
| Description | |
| | |
| Workers | |
| 31 | |

Application Control – General

- Name: Definir um nome para o perfil. Ex.: Deny All Ads;
 Description: Definir uma descrição para o perfil. Ex.: Application Control to deny all ads.
 Workers: Definir um número de workers, ou processos, por perfil de inspeção. Note que o campo vem pré-definido como 1.

Application Control

permissões.

Em "Application Control" são determinadas as aplicações cujo acesso será permitido ou negado:

| | Application Control | | | | | | |
|----------------|----------------------------------|-----------|------------------|--------------------|----------------------------|--------------|----------------|
| | Applications | | | | | | |
| | | | | | | | := |
| | | | Application Co | ntrol - Applicatio | ons | | |
| | | | | | | | |
| a editar as ap | olicações, certifique-se que o (| heckbox [|] está habilitad | do, depois clique | e no botão list app | olications [|] para adminis |

| | T | CEAY C | | AL V | ۹. 1 |
|----------|-----------|----------|----------------|----------------------|---------|
| errail | tuoo. | | etoman | Item | Control |
| | | B | | 1000mercin | Dery 😔 |
| eda | VIND | dougs | rotherostation | 247 inc. | Deny |
| | 0; | | 09 | 24/7 Media | 0ery 🔍 |
| mobile | sodate | protocol | games | 33Across | Deny - |
| | | | 0 | Ad4enat | Deny ~ |
| Business | streaming | cloud | web | Ad Advisor | Beny 🕤 |
| 0 | P P | | | Adblade | Geny 🔍 |
| portal | pîp | download | riation | Adconion Media Group | Dery 👘 |
| | | | | AdGear | Deny |
| | | | | Adity | Gany |
| | | | | < 3 2 3 | 4 5 17 |

Application Control - Add Application

Ao selecionar um dos ícones à esquerda, as aplicações serão exibidos no painel à direita.

Para mais informações a respeito das categorias utilizadas pelo Application Control, consulte esta página.

Escolha as categorias desejadas e depois selecione *Allow, Block ou Disable*. No menu de ações [], também é possível aplicar alguma destas opções em todas as categorias em *Allow All, Block All* e *Disable All* para desabilitá-las. Segue uma breve descrição da função de cada ação:

- Allow: O acesso às aplicações classificadas com esta categoria é permitido;
- Block: O acesso às aplicações classificadas com esta categoria é bloqueado;
- Disable: Esta categoria é desabilitada, isso significa que o Application Control irá ignorá-la e considerará apenas as aplicações em categorias permitidas ou bloqueadas.

No exemplo abaixo, iremos desabilitar todas as propagandas.

Para tanto, selecione a categoria desejada, neste exemplo, selecionaremos a opção "ads":

| | T | social | Q | AL V | ٩ |
|----------|-----------|----------|---------------|----------------------|--------|
| errall | tuool. | (10007) | remote | item | Contro |
| | | e | | 1000mercin | 0ery 👘 |
| eda | VHp | quett | colisionation | 247 inc. | Deny |
| | 0 | | | 24/7 Media | 0ery |
| mobile. | sodate | protocol | games | 33Across | Deny |
| | | | G | Ad4erat | Dery |
| Business | streaming | cloud | neb | Ad Advisor | Deny 😔 |
| 0 | U P | | | Adblade | Deny |
| portal | pân | download | ciatory | Adconion Media Group | 0ery 👘 |
| | | | | AdGear | Dery |
| | | | | Adity | Deny |
| | | | | < 1 2 3 | 4 5 17 |

Application Control - Add Application - Opção "ads" selecionada

Determine a aplicação desejada e na caixa de seleção, escolha a opção **Deny** [Deny], conforme exemplificado na imagem abaixo:

| Item | Controls |
|----------------------|---------------------|
| 1000mercis | Deny V |
| 247 Inc. | Deny \land |
| 24/7 Media | Allow |
| 33Across | Deny |
| 33ACI 035 | Disable |
| Ad4mat | Allow 🗸 |
| Ad Advisor | $\fbox{Allow} \lor$ |
| Adblade | Allow 🗸 |
| Adconion Media Group | Deny V |
| AdGear | Deny V |
| Adify | Deny V |

Application Control - Add Application - Itens negados

] ou

Caso seja necessário fazer uma configuração em todos os itens de uma categoria, basta selecionar a opção desejada no menu de ações [na caixa de seleção demonstrada abaixo:

| All | ^ |
|--------|-----|
| All | |
| Allow | All |
| Deny A | All |

Application Control - Add Application - All, Allow All e Deny All

Ao ter uma aplicação com a permissão negada, a quantia de aplicações negadas e permitidas será exibida sob o ícone da sua respectiva categoria à esquerda, conforme demonstrado abaixo:



Application Control - Add Application - 7 itens negados e 99 permitidos

| | C | | Causa | |
|--|--------|---|-------|-----|
| | Cancel | | Save | |
| Por fim. caso deseie cancelar clique no botão Cancel | | Para concluir a edição das aplicações clique no botão Savel | | 1. |
| | | | | ÷., |

Após, ter efetuado os processos anteriores, um resumo de todas as aplicações permitidas e negadas serão exibidas no campo Applications, conforme exemplificado abaixo:



Criar grupo customizado de aplicações

Insira o nome do grupo a ser criado, por exemplo "Custom", e o grupo será adicionado à lista de categorias já existentes.



Custom Group Application

Após realizar esses procedimentos, as configurações terão sido finalizadas com sucesso.

Sendo assim, o grupo customizado poderá receber dinamicamente as aplicações dos demais grupos.

A seguir analisaremos como apagar perfis em Delete Profile.

Services - Application Control - Menu de ações - Delete Profile

Através do botão "Delete Profile" é possível deletar os Profiles selecionados. Para deletar pelo Menu de Ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*:

| plikas | | |
|---------------|--------------------------------------|--------|
| -cords | | 6 6 8 |
| • here | Description | Action |
| IlleryADAte : | Application Control to them all with | / 5 |
| to the | 1947 | / 0 |

Application Control - Seleção dos Profiles para deletar



Application Control – Delete Profiles.

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os Profiles selecionados:

| Delete Profile | × |
|-------------------|---------------|
| Confirm • Test | |
| | Cancel Delete |

Application Control - Mensagem se deseja deletar os Profiles



Após realizar esses procedimentos, os Profiles terão sido deletados com sucesso.

Services - Application Control - Colunas

A seguir explicaremos cada coluna da aba Application Control:

| Application Control | | |
|---------------------|------------------------------------|---------------------|
| mille | | |
| tretosis | | |
| - Note | Description | Actions. |
| C Ourș at Sch | Application Control to deep of ach | / 0 |
| | | - (1) y - History V |

Profiles - Application Control

A seguir explicaremos cada coluna:

- Caixa de Seleção[]: Seleciona o profile;
- Name: Apresenta o nome do profile cadastrado;
- Description: Apresenta a descrição do profile cadastrado; Version: Apresenta a versão na qual o profile foi criado. É de extrema importância criar profiles da mesma versão que o UTM, caso contrário, o p • rofile não será compatível;
- Actions: A coluna "Actions" é composta por vários botões:

• Botão Edit [I Permite editar as configurações do profile adicionado na opção Create Profile do menu de ações;

• Botão Delete [

Application Control - Lista de Categorias

A seguir exibiremos diversas tabelas informando as categorias e suas respectivas aplicações.

As categorias utilizadas pelo Application Control são:

- Email;
- Proxy;
- Social;
- Remote;
- Ads;
- VOIP;
- Storage;
- Collaboration;
- Mobile;
- Update;
- Protocol;
- Games;
- Business;
- Streaming;
- Cloud;
- Web;
- Portal;
- P2P;
 Download.

As categorias instant messaging e anonymizers também estão inclusas. 0

Segue as tabelas abaixo:

Email

| Category | Application |
|----------|-----------------|
| Email | 126.com |
| | AOL Mail |
| | Apple Mail |
| | Basecamp |
| | BBC |
| | Bleacher Report |
| | Comcast |
| | Comcast Mail |
| | Daily Mail |
| | Daum Mail |
| | Eudora |
| | Eudora Pro |
| | Evolution |
| | Exchange |
| | Eyejot |
| | Fastmail |
| | |

| Fox News |
|--------------------------------|
| Fox Sports |
| Gmail |
| Gmail attachment |
| GMX |
| GMX Mail |
| Google Inbox |
| Google Mail |
| Hightail |
| Hushmail |
| IL |
| IMAP |
| IMAPS |
| IMO |
| Instan T |
| Jubii |
| KMail |
| LiveGo |
| Lotus Notes |
| MailChimp |
| Maildotcom |
| Maildotru |
| MAILQ |
| Mail.Ru |
| Mail.ru Attachment |
| ΜΑΡΙ |
| Official Major League Baseball |
| Mutt |
| Naver Mail |
| NI Mail |
| ODMR |
| Open Webmail |
| Outlook |
| Outlook Express |
| PCMAIL |
| POP2 |
| POP3 |
| POP3S |
| QMTP |
| QQ Mail |
| RoadRunner |
| |

| SMTP |
|---------------------|
| SMTPS |
| Spypig |
| Squirrelmail |
| Stack Overflow |
| Thunderbird |
| T-Online |
| Verizon Email |
| Web.de |
| Windows Live |
| Wall Street Journal |
| XNS Mail |
| Yahoo! Accounts |
| Yahoo! Mail |
| Zoho Mail |
| |

Proxy

| Category | Application |
|----------|--------------------|
| Proxy | ASProxy |
| | Avoidr |
| | Browsec |
| | CactusVPN |
| | Camo Proxy |
| | CDN |
| | FlyProxy |
| | Gom VPN |
| | gpass1 |
| | Guardster |
| | Hotspot Shield |
| | I2p Reseed Request |
| | ibVPN |
| | ICAP |
| | KProxy |
| | OpenVPN |
| | Ozyman |
| | Privax |
| | ProxEasy |
| | Proxifier |
| | |

| Proxyorg |
|-------------|
| Reduh |
| Suresome |
| Surrogafier |
| Ultrasurf |
| VTunnel |
| Zalmos |
| Zen Guard |
| ZenMate |
| ZenVPN |

Social

| Category | Application |
|----------|---------------------|
| Social | 17173.com |
| | 51.com |
| | Adult Friend Finder |
| | aNobii |
| | Athlinks |
| | Badoo |
| | beRecruited |
| | Bigadda |
| | Blogger |
| | BranchOut |
| | CafeMom |
| | Classmates |
| | Cloob |
| | Cyworld |
| | Daily Horoscope |
| | Delicious |
| | deviantART |
| | Diaspora |
| | Douban |
| | eHarmony |
| | Eventbrite |
| | Facebook |
| | Facebook Apps |
| | Facebook Like |
| | Family Tree |
| | |

| Fazed |
|------------------------|
| Facebook Comment |
| Facebook event |
| Facebook Message |
| Facebook Status Update |
| Facebook search |
| Facebook video |
| Facebook video chat |
| Flixster |
| Fotolia |
| FriendFeed |
| Friendster |
| FriendVox |
| Fubar |
| Funshion |
| Gaia Online |
| Gather |
| GOLFZON |
| Habbo |
| Hatena |
| Hyves |
| iAstrology |
| Ibibo |
| iKarma |
| Imgur |
| ipernity |
| iWiW |
| Kaixin001 |
| LinkedIn |
| LinkedIn Contacts |
| LinkedIn Job Search |
| LiveJournal |
| LiveJournal Post |
| Livemocha |
| Lokalisten |
| Match.com |
| Me2day |
| MEETin |
| Meetup |
| MeinVZ |
| MetroFLOG |
| |

| Mister Wong |
|-----------------------|
| Mixi |
| Mixx |
| Mxit |
| MyHeritage |
| MySpace |
| myUdutu |
| Netlog |
| Odnoklassniki |
| Orkut |
| Pinboard |
| Ping FM |
| Pinterest |
| Plaxo |
| Plenty of Fish |
| Po.st |
| Qzone |
| Renren |
| schuelerVZ |
| Skyrock |
| spin.de |
| Squidoo |
| StayFriends |
| studiVZ |
| Sway |
| Tagged |
| The Microsoft Network |
| Tuenti |
| Tweet |
| Twig |
| Twitter |
| Twitterrific |
| Userplane |
| Viadeo |
| VKontakte |
| Weibo |
| wer-kennt-wen |
| XING |
| Yelp |
| Zoosk |
| zShare |

Remote

| Category | Application |
|----------|-----------------------------|
| Remote | 4shared |
| | ADrive |
| | Amazon Cloud Drive Download |
| | AMMYY |
| | AnyDesk |
| | ARCServe |
| | Atlassian |
| | Backblaze |
| | BigUpload |
| | Bitbucket |
| | BlazeFS |
| | Bomgar |
| | Box |
| | Boxnet Upload SSL |
| | Brothersoft |
| | Citrix IMA |
| | Citrix Licensing |
| | Citrix RTMP |
| | Citrix SLG |
| | Citrix WANScaler |
| | Clip2Net |
| | Clip2Net Upload |
| | Commvault |
| | DCE/RPC |
| | DEC LaDebug |
| | DepositFiles |
| | DivShare |
| | dl.free.fr |
| | Docstor |
| | Dropbox |
| | Dropbox Download |
| | Dropbox Share |
| | Dropbox Upload |
| | DynGate |
| | Easy-Share |
| | |

| exec | |
|--------------------|--|
| FileDropper | |
| Filemail | |
| FileServe | |
| Flickr Upload | |
| Fluxiom | |
| FTP Data | |
| FTPS Data | |
| Ganglia | |
| GoToAssist | |
| GoToMyPC | |
| HiveStor | |
| HP VMM | |
| iCloud | |
| ifile.it | |
| ImageShack | |
| Imgur | |
| IMTransferAgent | |
| lssuu | |
| Ktelnet | |
| KVM | |
| KWDB | |
| LeapFILE | |
| Linuxconf | |
| LogMeIn | |
| LogMeIn Rescue | |
| lsh | |
| MediaFire | |
| Megashare | |
| Megaupload | |
| Mendeley | |
| Microsoft Azure | |
| Mionet | |
| Multiupload | |
| NetSarang | |
| NetSight | |
| Netviewer | |
| Okurin | |
| OneDrive | |
| Onehub | |
| Online File Folder | |
| 1 | |

| OpenSSH |
|------------------------------|
| Pando |
| PAWSERV |
| PcAnywhere |
| PC-Duo |
| Phanfare |
| Photobucket |
| Putlocker |
| PuTTY |
| RADIUS-acct |
| RayFile |
| RDP |
| Remote Job Service |
| Remote Telnet |
| RJE |
| Rsupport |
| Scribd |
| Scribd Upload |
| SF MGMT |
| ShareFile Upload SSL |
| shell |
| Windows Live SkyDrive |
| Skyfex |
| SQL-NET |
| SSH |
| SShell |
| Su-Mit Telnet |
| SUPDUP |
| syslog |
| TeamViewer |
| Telnet |
| Timbuktu |
| TransferBigFiles.com |
| TurboUpload |
| TwitPic |
| TypePad |
| Uploading.com |
| vCOM |
| VMware Remote Authentication |
| VMware vCenter client |
| VNC |
| |

| RFB |
|------------|
| Webhard |
| Webshots |
| Yahoo! Box |
| yfrog |
| Yoics |
| Zannet |
| ZumoDrive |

Ads

| Category | Application |
|----------|----------------------|
| Ads | 1000mercis |
| | 247 Inc. |
| | 24/7 Media |
| | 33Across |
| | Ad4mat |
| | Ad Advisor |
| | Adblade |
| | Adconion Media Group |
| | AdGear |
| | Adify |
| | AdJuggler |
| | Ad Marvel |
| | Ad Master |
| | Admeld |
| | ADMETA |
| | Ad Mob |
| | AdNetwork.net |
| | Ad Nexus |
| | AdReady |
| | AdRoll |
| | adSage |
| | AdSame |
| | Adtech |
| | Ad Tech |
| | Adtegrity |
| | Advertising.com |
| | AdXpose |
| | |

| Amazon Ads System | |
|------------------------|--|
| Amobee | |
| AOL Ads | |
| AppNexus | |
| Atlas Advertiser Suite | |
| AudienceScience | |
| Auditude | |
| Bizo | |
| BlueKai | |
| Brightroll | |
| Brilig | |
| Burstly | |
| BV! Media | |
| Caraytech | |
| Casale | |
| Cedexis | |
| Chango | |
| Chinauma | |
| ClickBooth | |
| ClickTale | |
| CloudFlare | |
| CNZZ | |
| Cognitive Match | |
| Commission Junction | |
| Compete | |
| Compuware | |
| comScore | |
| Connexity | |
| Connextra | |
| ContextWeb | |
| contnet | |
| Conviva | |
| Core Audience | |
| CPX Interactive | |
| Criteo | |
| Crowd Science | |
| cXense | |
| DataLogicx | |
| DC Storm | |
| Dotomi | |

| DoubleVerifyDynamic LogicEffective Measureengage BDREnsightenEQ AdsEvidoneXelateExponential InteractiveeyeReturnFederated MediaGonieoGonaddyGoogle AdsenseGreystripeiAdICAInfonlineInfonlineIntegral Ad ScienceInvitemediaiArequinaiAdIteagabltLigatusKomli MediaHarketoMaxPoint InteractiveMaximiserMadudiMediaôDegreesMediaVMicrosoft AdsMilennial Media | Doubleclick |
|--|-------------------------|
| Dynamic LogicEffective Measureengage BDREnsightenEQ AdsEvidoneXelateExponential InteractiveeyeReturnFederated MediaGonaddyGoogle AdsenseGoogle AdsenseInfonlineInfonlineInfonlineIntegral Ad ScienceKuxLeadBoltLigatusKuxMarketoMaxPoint InteractiveMaxin SerMaxymiserMadataMediaMarketoMatediaMarketoMaciafiaMatediaMarketoMaxymiserMediaMediaMediaMathaMediaMediaMediaMatediaMatediaMathaMathaMathaMediaMathaMediaMatha <td>DoubleVerify</td> | DoubleVerify |
| Effective Measureengage BDRensightenEQ AdsEvidoneXelateExponential InteractiveeyeReturnFederated MediaGonieoGoDaddyGoogle AdsenseGreystripeiAdInfonlineInfonlineIntegral Ad ScienceInvitemediaiNediaIntegral Ad ScienceKomli MediaKomli MediaiAdMaxetoKanketoMaxPoint InteractiveMaxymiserMedia6DegreesMediaVMediaVMediaMathMediaVMediaVMathMediaVMathMediaVMathMediaVMediaMathMediaVMediaMathMediaVMediaVMediaVMediaVMediaVMathMediaVMediaVMediaVMathMediaVMediaVMediaVMathMediaVMathMediaVMediaVMathMediaVMediaVMathMediaVMediaNMathMediaVMathMediaVMathMediaVMathMediaVMathMathMediaVMath | Dynamic Logic |
| engage BDREnsightenEQ AdsEvidonexelateExponential InteractiveeyeReturnFederated MediaFreewheelGonaddyGoogle AdsenseGreystripeiAdICAInfonlineIntegral Ad ScienceIntegral Ad ScienceKomli MediaLiperceptionsKomli MediaLigatusLigatusLigatusMaxPoint InteractiveMaxPoint InteractiveMaxPoint InteractiveMaxibMatedoMatedoMacida Innovation GroupMediaAlnMediaVMediaVMediaVMatedoMatelaMatelaMatelaMatelaMatelaMediaMatelaMediaAlnovation GroupMicrosoft AdsMillennial Media | Effective Measure |
| EnsightenEQ AdsEvidoneXelateexponential InteractiveeyeReturnFederated MediaFreewheelGonieoGoogle AdsenseGoegle AdsenseInfonlineInfonlineInfonlineIntegral Ad ScienceInvitemediaiPerceptionsKomli MediaLeadBoltLigatusJuitMarketoMaxPoint InteractiveMaxiniserMaciafiaMediafiaMatediaInteractiveMaxiniserMediafiaMediafiaMatenMatenMatenMatenMatenMatenMatenMediafiaMatenMatenMatenMediafiaMatenMediafiaMatenMediafiaMatenMediafiaMatenMediafiaMatenMediafiaMatenMediafiaMediafiaMediafiaMatenMediafiaMatenMatenMatenMediafiaMatenMatenMatenMatenMatenMatenMatenMatenMatenMatenMatenMatenMatenMatenMatenMatenMaten< | engage BDR |
| EQ AdsEvidonexelateexponential InteractiveeyeReturnFederated MediaFreewheelGonieoGoDaddyGoogle AdsenseGreystripeiAdICAInprove DigitalInfonlineIntegral Ad ScienceInvitemediaiPerceptionsKomli MediaLeadBoltLigatusLigatusMaxPoint InteractiveMaxPoint InteractiveMaxymiserMediaôDegreesMediaVMediaVMediaVMediaVMediaVMathMediaVMediaVMathMediaVMediaVMediaVMediaVMediaVMediaVMediaVMediaVMediaVMillennial Media | Ensighten |
| EvidoneXelateeXonential InteractiveeyeReturnFederated MediaFreewheelGonieoGoDaddyGoogle AdsenseGreystripeiAdICAInfonlineInfonlineIntegral Ad ScienceiNvitemediaiPerceptionsKomli MediaLeadBoltLigatusLigatusMaxPoint InteractiveMaxymiserMadyMedia Innovation GroupMediaVMediaVMediaVMatheMatheMatheMediaVMediaVMediaMatheMediaVMediaVMediaVMediaVMediaVMicrosoft AdsMillennial Media | EQ Ads |
| eXelate Exponential Interactive eyeReturn Federated Media Freewheel Genieo GoDaddy Google Adsense Google Adsense Greystripe iAd Greystripe iAd Infonline Infonline Infonline Infonline Infonline Infonline Infonline Infore Digital Infonline Infore Digital Infor Ads Integral Ad Science Infor Ads Integral Ad Science Integral Ad Science Integral Ad Science Infor Ads Integral Ad Science Infor Interactive Infor Ads Interior Int | Evidon |
| Exponential Interactive eyeReturn Federated Media Freewheel Genieo Gonaddy Google Adsense Google Adsense Greystripe iAd ICA Infonline Infonline Infonline Infonline Infonline Infonline Infonline Infonline Inforta Infonline Inforta Infonline Inforta Infort | eXelate |
| eyeReturn Federated Media Freewheel Genieo GoDaddy GoOgle Adsense Greystripe iAd ICA ICA Infonline Infonline Infonline Integral Ad Science Integral Ad Science iNvitemedia iPerceptions Komli Media Krux LeadBolt Ligatus Ligatus Ligatus Asreoi MaxPoint Interactive Maxymiser Media6Degrees Media Innovation Group MediaV | Exponential Interactive |
| Federated MediaFreewheelGenieoGoDaddyGoogle AdsenseGreystripeiAdICAImprove DigitalInfonlineInfoskin MediaIntegral Ad ScienceInvitemediaiPerceptionsKomli MediaLeadBoltLigatusLigatusMarketoMaxPoint InteractiveMaxymiserMedia6DegreesMediaVuMediaVuMediaVuMediaVuMicrosoft AdsMillennial Media | eyeReturn |
| FreewheelGenieoGoDaddyGoogle AdsenseGreystripeiAdICAImprove DigitalInfonlineIntegral Ad ScienceInvitemediaiPerceptionsKomli MediaLeadBoltLigatusLigatusMarketoMaxPoint InteractiveMaxymiserMedia6DegreesMedia1nnovation GroupMediaVMediaVMediaVMicrosoft AdsMillennial Media | Federated Media |
| GenieoGoDaddyGoogle AdsenseGreystripeiAdICAImprove DigitalInfonlineInfonlineIntegral Ad ScienceiPerceptionsKomli MediaKruxLeadBoltLigatusLigatusMarketoMaxPoint InteractiveMaxymiserMedia6DegreesMedia1nnovation GroupMediaVMediaVMicrosoft AdsMillennial Media | Freewheel |
| GoDaddy Google Adsense Greystripe iAd ICA ICA Inprove Digital Infonline InSkin Media Integral Ad Science Invitemedia iPerceptions Komli Media Krux LeadBolt Ligatus Ligatus Ligatus Ligatus Marketo MaxPoint Interactive Maxymiser Madymiser Media6Degrees Media Innovation Group MediaV | Genieo |
| Google Adsense Greystripe iAd ICA ICA Inprove Digital Infonline Infonline Infonline Infonline Infonline Infonline Informedia Integral Ad Science Integral Ad Science I | GoDaddy |
| Greystripe iAd iAd ICA IncA Improve Digital Infonline Infonline Infonline Infonline Infonline Infonline Informedia Integral Ad Science Integral Ad | Google Adsense |
| iAd ICA Improve Digital Infonline InSkin Media Integral Ad Science Invitemedia iPerceptions Komli Media iPerceptions Komli Media Krux Krux LeadBolt Ligatus Ligatus Ligatus Ligatus Ligatus Ligatus MaxPoint Interactive MaxPoint Interactive MaxPoint Interactive Maxymiser Macia Macia Media | Greystripe |
| ICA Improve Digital Infonline Infonline InSkin Media Integral Ad Science Integral Ad Science Integral Ad Science Integral Ad Science Integral Ad Science Integral Ad Science Image Ad Science Komli Media Komli Media Komli Media Maxeto Integration MaxPoint Interactive Maxymiser Macia Innovation Group Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | iAd |
| Improve Digital Infonline InSkin Media Integral Ad Science Invitemedia iPerceptions Komli Media Krux Krux LeadBolt Ligatus Ligatus Ligatus Ligatus Ligatus Ligatus MaxPoint Interactive MaxPoint Interactive Maxymiser Maxymiser Macia Media | ICA |
| Infonline InSkin Media Integral Ad Science Invitemedia iPerceptions Komli Media Krux LeadBolt Ligatus Lijit Lotame Marketo MaxPoint Interactive Maxymiser MdottM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | Improve Digital |
| InSkin Media Integral Ad Science Invitemedia iPerceptions Komli Media Krux LeadBolt Ligatus Ligatus Ligatus Lijit Lotame Marketo MaxPoint Interactive MaxPoint Interactive Maxymiser MadotM Media6Degrees Media Innovation Group MediaMath MediaV MediaV | Infonline |
| Integral Ad Science Invitemedia Invitemedia IPerceptions Komli Media Krux LeadBolt Ligatus Ligatus Ligit Lotame Marketo MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | InSkin Media |
| Invitemedia iPerceptions Komli Media Krux LeadBolt Ligatus Ligatus Lijit Lotame Marketo Marketo MaxPoint Interactive Maxymiser MadotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads | Integral Ad Science |
| iPerceptions Komli Media Krux LeadBolt Ligatus Ligatus Lijit Lotame Marketo MaxPoint Interactive Maxymiser MadotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads | Invitemedia |
| Komli Media Krux LeadBolt Ligatus Ligatus Lijit Lotame Marketo Marketo MaxPoint Interactive Maxymiser Madia Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads | iPerceptions |
| Krux LeadBolt Ligatus Lijit Lotame Marketo MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads | Komli Media |
| LeadBolt Ligatus Lijit Lotame Marketo MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads | Krux |
| Ligatus Lijit Lotame Marketo MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads | LeadBolt |
| Lijit Lotame Marketo MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | Ligatus |
| Lotame Marketo MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | Lijit |
| Marketo MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | Lotame |
| MaxPoint Interactive Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | Marketo |
| Maxymiser MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | MaxPoint Interactive |
| MdotM Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | Maxymiser |
| Media6Degrees Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | MdotM |
| Media Innovation Group MediaMath MediaV Microsoft Ads Millennial Media | Media6Degrees |
| MediaMath Media∨ Microsoft Ads Millennial Media | Media Innovation Group |
| MediaV Microsoft Ads Millennial Media | MediaMath |
| Microsoft Ads Millennial Media | MediaV |
| Millennial Media | Microsoft Ads |
| | Millennial Media |

| Mixpanel |
|------------------------------|
| Moat |
| Mobile Theory |
| Monetate |
| Motrixi |
| MyBuys |
| Neobux |
| NetSeer |
| Neustar Information Services |
| Nexage |
| Nielsen |
| Nugg |
| OpenX |
| Optimizely |
| OptMD |
| OwnerlQ |
| PointRoll |
| Polldaddy |
| Proclivity |
| Proxistore |
| Pubmatic |
| Quantcast |
| RadiumOne |
| Resonate Networks |
| RichRelevance |
| Rocket Fuel |
| Rubicon Project |
| Scorecard Research |
| ShareThis |
| Silverpop |
| Simpli.fi |
| Siteimprove |
| SiteScout |
| Six Apart |
| Skimlinks |
| SLI Systems |
| Smart AdServer |
| Softpedia |
| SpotXchange |
| Surikate |
| Telecom Express |
| |

| The Trade Desk |
|----------------|
| TLVMedia |
| TubeMogul |
| Undertone |
| Vibrant |
| VIEWON |
| VoiceFive |
| Weborama |
| Webtrends |
| Woolik |
| Xaxis |
| XiTi |
| X Plus One |
| Yabuka |
| Ybrant Digital |
| Yieldmanager |
| Zanox |
| ZEDO |

VOIP

| Category | Application |
|----------|-------------|
| Voip | Jajah |
| | Lync |
| | SGCP |
| | Sightspeed |
| | Viber |

Storage

| Category | Application |
|----------|-----------------|
| Storage | 2Shared |
| | Badongo |
| | Beatport |
| | BitTracker |
| | Boxnet |
| | BTMon |
| | Compressed File |

| Crocko | |
|--------------------------|--|
| DB2 | |
| DDM-SSL | |
| DRDA | |
| Dropboks | |
| DropSend | |
| Egnyte | |
| Elephant Drive | |
| eSnips | |
| FileFactory | |
| FileSonic | |
| FilesTube | |
| FlipDrive | |
| Foldershare | |
| FreakShare | |
| FreeDrive | |
| GamesTorrents | |
| Informix | |
| IngresNET | |
| Lets Create | |
| LOCKSS | |
| MaxDB | |
| Mega | |
| Mini SQL | |
| Mozy | |
| MS Global Catalog Secure | |
| Microsoft Access | |
| MS OLAP | |
| MySQL | |
| NovaBACKUP | |
| Open Drive | |
| Oracle Database | |
| Oracle SQLNET | |
| PostgreSQL | |
| RapidShare | |
| RIS | |
| RoboForm | |
| Sharingmatrix | |
| SpiderOak | |
| SQL Server | |
| SVN | |

| Syncplicity |
|----------------|
| Torrent 441 |
| Torrent Hound |
| Torrent Ino |
| Torrent Leech |
| Torrent Reator |
| TowerData |
| WebLogic |
| Your File Host |
| Zenbe |
| |

Collaboration

| Category | Application |
|---------------|----------------------|
| Collaboration | Aceproject |
| | AmoebaOS |
| | Aol Answers |
| | Apple Remote Desktop |
| | Asana |
| | Atom |
| | BeamYourScreen |
| | BFGMiner |
| | BitCoin Getwork |
| | Citrix Online |
| | CVS |
| | DeskAway |
| | Dr. Watson |
| | Fengoffice |
| | Google Docs |
| | Goplan |
| | Group Greeting |
| | Groupwise |
| | iMeet |
| | IMVU |
| | Koolim |
| | Links |
| | Mavenlink |
| | Meeting Maker |
| | Mozilla |

| Octopz |
|----------------|
| Pbworks |
| PlusIM |
| Projectplace |
| Quick Base |
| RSS |
| Saba Meeting |
| Sametime |
| Schmedley |
| ScreenToaster |
| Sharepoint |
| ShowDocument |
| Slack |
| SparkPeople |
| Springpadit |
| Sumo Paint |
| TeamBox |
| Thinkfree |
| Viewpath |
| Vote Yes or No |
| Vyew |
| WebAIM |
| Webex Teams |
| Writeboard |
| Zoho Wiki |

Mobile

| Category | Application |
|----------|--------------------------|
| Mobile | 050plus |
| | 500px |
| | AdobeAIR |
| | AD-X Tracking |
| | Airbnb |
| | Alibaba |
| | Amazon Cloud Player |
| | Android browser |
| | Android Client |
| | Android Download Manager |
| | |

| Android Music |
|----------------------|
| Anipang |
| AppleCoreMedia |
| Apple Stocks |
| Avaya Live |
| BBC iPlayer |
| Bebo |
| Resilio Sync |
| Blackberry browser |
| BlueStacks |
| BlueStacks apps |
| Brewster |
| Bria |
| Buffer |
| Burnbook |
| Campfire |
| Chat |
| ConnMan |
| Crittercism |
| Dictionary.com |
| DingDing |
| Dots |
| Engadget |
| Feedly |
| Fetion |
| Flipboard |
| Foursquare |
| Game Center |
| Glympse |
| GOMTV Remote Control |
| Google Duo |
| Google Earth |
| Google Hangouts |
| GREE |
| Hello |
| НІКЕ |
| HIKE Media |
| iBooks |
| iCal |
| Infinity Blade |
| INRIX |
| |

| Instagram |
|-------------------------|
| Instapaper |
| iTunes iPad |
| iTunes iPhone |
| iTunes iPod |
| iTunes Music |
| iTunes Store |
| iTunes U |
| JetBrains |
| JetBrains feature |
| JetBrains plugins |
| KakaoTalk |
| Kik Messenger |
| Kontiki |
| Letterpress |
| Line2 |
| Linphone |
| rlogin |
| Mailbox |
| MapMyFitness |
| Mention |
| Merriam-Webster |
| Microsoft Stream |
| Mobilatory |
| Mobile Device Useragent |
| Mobile Safari |
| Nateon |
| Nest Thermostat |
| Net2Phone |
| OCS |
| Office Mobile |
| Ovi Browser |
| Parallels |
| PDF Expert |
| Periscope |
| Philips Hue |
| Photo Stream |
| Pocket |
| Pogoplug |
| Power BI |
| Pushover |
| |

| Readability |
|------------------------------|
| RealNetworks |
| RealPlayer Cloud |
| Remote Ctrl from iPhone/iPad |
| Samsung Push Notification |
| Snapchat |
| Spotify |
| ST |
| Stitcher |
| Telegram |
| Telenav |
| Tempo |
| TextMe |
| TextNow |
| textPlus |
| Tinder |
| TomTom |
| Viki |
| Vine |
| Vlingo |
| Voxer |
| We7 |
| Weather |
| WeChat |
| WhatsApp |
| WhatsApp File Transfer |
| Windows Phone Browser |
| WPS Office |
| Xunlei Kankan |
| Yahoo! Mobage |
| Yik Yak |
| Youdao Dictionary |
| Zoho Assist |
| Zoho Connect |
| Zoho Docs |
| Zoho SalesIQ Chat |
| Zoho Social |

Update
| Category | Application |
|----------|------------------------------|
| Update | Activesync |
| | Adobe Software |
| | Adobe Updater |
| | Allmyapps |
| | Apple Update |
| | BitDefender |
| | BlueStacks download |
| | BlueStacks update |
| | Eclipse |
| | Eclipse Marketplace |
| | Eclipse Updates |
| | Fedora DSGW |
| | Google Update |
| | Java Update |
| | JetBrains update |
| | ksfetch |
| | Microsoft Visual Studio |
| | Microsoft Update |
| | NVIDIA Update |
| | Python-httplib |
| | Red Hat |
| | Sophos Update |
| | SymantecUpdates |
| | Syncml |
| | Ubuntu Software Center |
| | Ubuntu Update Manager |
| | WD softwares Download/Update |
| | Windows Update |

Protocol

| Category | Application |
|----------|--------------|
| Protocol | 3Com AMP3 |
| | 3COM-TSMUX |
| | 914CG |
| | 9P |
| | ACAP |
| | ACA Services |

| AccessBuilder |
|-------------------------------------|
| Access Network |
| ACI |
| ACR-NEMA |
| Active Networks |
| ActiveSync |
| Adobe PostScript |
| AED512 |
| Aeolon Core Protocol |
| AEP |
| AFP |
| AgentX |
| Airsoft Powerburst |
| AJP |
| Alias |
| ALPES |
| AMANDA |
| AMInet |
| ANSA Notify |
| ANSA REX Trader |
| ANSI Z39.50 |
| any host |
| AODV |
| Apertus Tech Load Distribution |
| APNS |
| appleqtcsrvr |
| AppleShare |
| AppleTalk Unused 203 |
| AppleTalk Unused 205 |
| AppleTalk Unused 207 |
| AppleTalk Unused 208 |
| AppleTalk Routing Maintenance |
| AppleTalk Zone Information Protocol |
| ApplianceWare Managment Protocol |
| Applix ac |
| ARCISDMS |
| Argus |
| Ariel |
| Ariel2 |
| Ariel3 |
| ARIS |

| ARNS |
|-----------------------------------|
| Asipregistry |
| AS Server Mapper |
| AUDIT |
| Aurora |
| Aurora CMGR |
| AURP |
| Avian |
| Avocent |
| AX.25 |
| BACnet |
| banyan-rpc |
| Banyan VIP |
| BBN RCC |
| BFTP |
| BGMP |
| BGP |
| bgs-nsi |
| BH611 |
| BHEVENT |
| BHFHS |
| BHMDS |
| BITS |
| Blackjack |
| bmpp |
| BNA |
| Bnet |
| Boingo |
| Borland DSJ |
| Britton Lee IDM |
| BitTorrent |
| Bundle Discovery Protocol |
| Cableport AX |
| Cabletron Management Protocol |
| CAB Protocol |
| CadLock |
| CAICCI |
| CA Intl License Server |
| Call of Duty |
| campaign contribution disclosures |
| САР |

| СВТ | |
|---------------------------------|--|
| CDC | |
| CDDB | |
| CFDP | |
| cFTP | |
| CHAOSNet | |
| Chshell | |
| CIMPLEX | |
| Cisco DRP | |
| Cisco FNATIVE | |
| Cisco GDP | |
| Cisco NAC | |
| Cisco SYSMAINT | |
| Cisco TNATIVE | |
| Citrix Static | |
| CL1 | |
| Clearcase | |
| CLOANTO | |
| CMIP/TCP Manager | |
| Coda Auth | |
| Collaborator | |
| Combat Radio Transport Protocol | |
| Combat Radio User Datagram | |
| Common Trace Facility | |
| Compaq-Peer | |
| CompressNET | |
| COMSCM | |
| con | |
| connendp | |
| contentserver | |
| Corerjd | |
| Courier Mail Server | |
| Covia | |
| CP Heart Beat | |
| CP Network Executive | |
| cpq-wbem | |
| Cray Network Semaphore server | |
| Cray Unified Resource Manager | |
| Creative Partner | |
| Creative Server | |
| Cross Net Debugger | |

| CRYPTOAdmin |
|-------------------------------|
| CSNET Mailbox Name Nameserver |
| CSTA |
| CU-SeeMe |
| Customer Ixchange |
| cvc_hostd |
| CVS pserver |
| CVSup |
| Cybercash |
| cycleserv |
| cycleserv2 |
| DAAP |
| DASP |
| DataRampSrvSec |
| DataRamp Svr |
| DATEX-ASN |
| dBase |
| DCAP |
| DCCP |
| dcLINK |
| DCN Measurement Subsystems |
| DCP |
| dctp |
| DDM |
| DDM DFM |
| DDM RRDA |
| DDP |
| DDS |
| decap |
| DEC Auth |
| Decbsrv |
| DEC DLM |
| DECVMS |
| DEI-ICDA |
| Desknets |
| device |
| DGP |
| DHCP |
| DHCP Failover |
| DHCP Failover 2 |
| DHCPv6 |

| Diameter |
|----------------------------|
| digital-vrc |
| D-II |
| DirectPlay |
| DirectPlay8 |
| Direct TV Software Updates |
| Direct TV Tickers |
| DirecTV Data Catalog |
| DirecTV Webcasting |
| Discard |
| distcc |
| DIXIE |
| DLS |
| dls-mon |
| DN6-NLM-AUD |
| DNA-CML |
| DNP3 |
| DNSIX |
| DOOM |
| DPSI |
| Dropbear |
| DSFGW |
| DSP |
| DSP3270 |
| DSR |
| DTAG |
| ОТК |
| DTLS |
| DWR |
| eDonkey Static |
| EGP |
| EIGRP |
| EMBLNDT |
| EMC SmartPackets |
| EMFIS-CNTL |
| EMFIS Data |
| Emission Control Protocol |
| Encapsulation Header |
| entomb |
| entrust-aaas |
| entrust-aams |
| |

| Entrust Administration Service Handler |
|--|
| Entrust-KMSH |
| Entrust SPS |
| EntrustTime |
| Epic |
| Epmap |
| ERPC |
| errlog copy/server daemon |
| ESCP |
| eSignal |
| ESP |
| ESRO |
| ESRO-EMSDP V1.3 |
| EtherIP |
| ETOS |
| Eudora Set |
| FastCGI |
| FastTrack |
| Fatmen |
| FCP |
| FDSSDP |
| FileMaker |
| Finger |
| Fink |
| FLEXIm |
| FLN-SPX |
| X font server |
| FTP |
| FTP Active |
| FTP Passive |
| FTPS |
| FTP Software Agent System |
| Fujitsu Device Control |
| FXP |
| GACP |
| gdomap |
| GDS DataBase |
| Genie |
| GENRAD |
| GGP |
| ginad |
| 1 |

| GIOP |
|------------------------------------|
| GIST |
| GKrellM |
| Glide |
| Glype Proxy |
| GMTP |
| GNU Generation Foundation NCP 678 |
| GoBoogy |
| Gopher |
| GotoDevice |
| GPFS |
| Graphics |
| GraphOn Login |
| GRE |
| Groove |
| GSI-FTP |
| Gss X License Verification |
| GTP User |
| GVFS |
| ha-cluster |
| Hamachi |
| НАР |
| Hardware Control Protocol Wismar |
| Hassle |
| HDAP |
| HELLO Port |
| HEMS |
| Heroix Longitude |
| Hitachi Universal Storage Platform |
| HL7 |
| HMMP Indication |
| HMMP Operation |
| HMP |
| Hostname server |
| HP Network Management Center. |
| HP Perf |
| НТТР |
| HTTPMGT |
| HTTP RPC Ep Map |
| HTTPS |
| Hybrid Point of Presence |

| пурег-О | |
|---|--|
| Hyperwave-ISP | |
| iafdbase | |
| IAFServer | |
| IASD | |
| IATP | |
| IAX | |
| ІВМ Арр | |
| IBM Director | |
| IBM NetView DM | |
| IBM NetView DM/6000 Server/Client | |
| IBP | |
| ICAD | |
| ICL coNETion locate server | |
| ICL coNETion server info | |
| ICMP | |
| ICMP for IPv6 | |
| ICP | |
| Ident | |
| idfp | |
| IDP | |
| IDPR | |
| IDPR Control Message | |
| IDRP | |
| IDXRad | |
| IEC 60870-5-104 | |
| IEEE-MMS-SSL | |
| iFCP | |
| IFMP | |
| IGMP | |
| IGRP | |
| IMGames | |
| IMP Logical Address Maintenance | |
| IMSP | |
| InBusiness | |
| i-nlsp | |
| Intecourier | |
| Integra Software Management Environment | |
| Internet Configuration Manager | |
| Internet telephony tool | |
| intrinsa | |

| ipcd |
|--|
| IPComp |
| IPCU |
| ipdd |
| IP in IP |
| IPLT |
| IP Mobility |
| IPP |
| IPv6 encapsulation |
| IPX over IP |
| IPX over UDP |
| IRC |
| IRCS |
| IRC-SERV |
| iRODS |
| IRTP |
| ISCSI |
| ISI Graphics |
| ISIS |
| ISO ILL Protocol |
| ISO IP |
| ISO MMS |
| ISO SAP |
| ISO-TP0 |
| ISO Transport Class 2 Non-Control over TCP |
| itm-mcell-s |
| ITU H.323 |
| iWARP |
| Jargon |
| Java RMI |
| JBoss Remoting |
| Kali |
| K-Block |
| Kerberos |
| Kerberos Administration |
| Key Server |
| KFTP |
| KFTPDATA |
| KIS |
| Klogin |
| KNETCMP |
| |

| Konspire2b |
|--------------------------------|
| kpasswd |
| Kryptolan |
| kshell |
| lanserver |
| LDAP |
| LDAPS |
| LDP |
| Leaf-1 |
| Leaf-2 |
| Legent |
| LEGENT-2 |
| ListProc |
| ljk-login |
| LLMNR |
| Locus ARP |
| Locus Map |
| Locus PC-Interface Conn Server |
| Loglogic |
| lpr |
| LWAPP |
| MacOS Server Admin |
| Magenta Logic |
| Mailbox-LM |
| maitrd |
| Management Utility |
| MANET |
| Masqudialer |
| MATIP |
| MATIP-TYPE-B |
| McAfee AutoUpdate |
| MC-FTP |
| McIDAS |
| mcns-sec |
| mdc-portmapper |
| Medipac |
| Memcomm |
| Meregister |
| MERIT Internodal Protocol |
| Metagram |
| Meter |
| |

| MF Cobol | | |
|--|--|--|
| MFE | | |
| MFTP | | |
| micom-pfs | | |
| MICP | | |
| Micromuse-Im | | |
| Microsoft Global Catalog | | |
| Microsoft Rome | | |
| Microsoft Shuttle | | |
| Microsoft System Center Operations Manager | | |
| mit-ml-dev | | |
| MIT ML Device | | |
| MIT Spooler | | |
| MobileIP | | |
| MobillP-MN | | |
| Mobility XE protocol | | |
| Modbus | | |
| Monitor | | |
| Moodlebot | | |
| MortgageWare | | |
| MPLS | | |
| MPM FLAGS Protocol | | |
| MPTN | | |
| MQTT | | |
| MRM | | |
| MSA | | |
| MS CRS | | |
| MSDP | | |
| MS Exchange Routing | | |
| MSG | | |
| msg-icp | | |
| MSMQ | | |
| Microsoft NCSI | | |
| MSOC File Transfer | | |
| MSP | | |
| Microsoft Web Platform Installer | | |
| Microsoft WNS | | |
| МТР | | |
| Multiling HTTP | | |
| Mylex-mapd | | |
| WINS | | |

| NARP | | |
|------------------------------------|--|--|
| NAT-PMP | | |
| NBP | | |
| NCED | | |
| NCLD | | |
| NCP | | |
| nCube License Manager | | |
| NDMP | | |
| NDS Auth | | |
| Nest Protocol | | |
| NetBackup | | |
| NetBIOS-dgm | | |
| NetBIOS-ns | | |
| NetBIOS-ssn (SMB) | | |
| NETBLT | | |
| netGW | | |
| Netinfo | | |
| Netix MPP | | |
| Netnews Administration System | | |
| Netop Remote Control | | |
| NETSC | | |
| NETSC-DEV | | |
| NetScout | | |
| netvmg-traceroute | | |
| NetWall | | |
| Netware | | |
| Network based Rev. Cont. Sys. | | |
| Networked Media Streaming Protocol | | |
| NetWorker | | |
| Network Innovations Multiplex | | |
| Network PID Checker | | |
| NetWorker Data Setup | | |
| Network Systems | | |
| New who | | |
| NeXTStep | | |
| NFA | | |
| NFS Lock Daemon Manager | | |
| NI FTP | | |
| Nintendo WFC | | |
| NIP | | |
| nlogin | | |
| | | |

| Nmap | | | | |
|-------------------------------------|--|--|--|--|
| NNSP | | | | |
| NNTP | | | | |
| NNTPS | | | | |
| Novadigm EDM | | | | |
| Novell Netware over IP | | | | |
| npmp-gui | | | | |
| npmp-local | | | | |
| NPMP Trap | | | | |
| NPP | | | | |
| NQS | | | | |
| NSFNET-IGP | | | | |
| NSIIOPS | | | | |
| NSRMP | | | | |
| NSS | | | | |
| NSSTP | | | | |
| NSW User System FE | | | | |
| NTP | | | | |
| NVP | | | | |
| NXEdit | | | | |
| OBEX | | | | |
| OCBinder | | | | |
| OCS_CMU | | | | |
| OCServer | | | | |
| OFTP | | | | |
| OFTPS | | | | |
| Ohimsrv | | | | |
| OLSR | | | | |
| Omginitialrefs | | | | |
| Omron FINS | | | | |
| Omserv | | | | |
| Onmux | | | | |
| opalis-rdv | | | | |
| OPC | | | | |
| OpenDoor | | | | |
| Openport | | | | |
| openvms-sysipc | | | | |
| Operations Manager - Health Service | | | | |
| TNS/Oracle | | | | |
| oracle | | | | |
| Oracle Business Intelligence | | | | |
| | | | | |

| Oracle coauthor | | |
|-----------------------------|--|--|
| Oracle Names | | |
| Oracle Net8 CMan Admin | | |
| Oracle Net8 Cman | | |
| Oracle Remote Data Base | | |
| Oracle TCP/IP Listener | | |
| Orbix 2000 Config | | |
| Orbix 2000 Locator | | |
| Orbix 2000 Locator over SSL | | |
| ORBIX-CFG-SSL | | |
| OSPF | | |
| OSUNMS | | |
| P10 | | |
| Packet Radio Measurement | | |
| PAPI | | |
| PARC Universal Packet | | |
| Parsec Gameserver | | |
| PassGo Technologies Service | | |
| Password Change | | |
| Path | | |
| PCoIP | | |
| PDAP | | |
| PDL data streaming port | | |
| PDRE | | |
| Personal Link | | |
| PFTP | | |
| PGM RTP | | |
| Pharos psrserver | | |
| Philips Video-Conferencing | | |
| Phonebook | | |
| Photuris | | |
| PIM | | |
| PIM-RP-DISC | | |
| PIP | | |
| PIPE | | |
| pirp | | |
| PKIX-3 CA/RA | | |
| PKIX Timestamp | | |
| Pluribus Packet Core | | |
| Plus Fives MUMPS | | |
| PNNI | | |
| | | |

| POV-Ray | | |
|-------------------------------------|--|--|
| PowerChute | | |
| PRM Node Man | | |
| PRM Sys Man | | |
| PROFILE | | |
| PROSPERO | | |
| PScribe | | |
| PTC Name Service | | |
| РТР | | |
| PTP Event | | |
| PTP General | | |
| PubNub | | |
| PubSubHubbub | | |
| pump | | |
| PureNoise | | |
| PVP | | |
| PWDGEN | | |
| Python urllib | | |
| Qbik | | |
| QFT | | |
| QMQP | | |
| QNX | | |
| qrh | | |
| QUIC | | |
| Quotad | | |
| Radio Control Protocol | | |
| RADIUS | | |
| Radmin | | |
| Rational Method Composer | | |
| RDA | | |
| RDT | | |
| RealVNC | | |
| Reliable Datagram Protocol | | |
| RemoteFS | | |
| Remote-KIS | | |
| Remote Method Invocation Activation | | |
| repcmd | | |
| repscmd | | |
| ResCap | | |
| Retrospect | | |
| RIP | | |

| RIPng | |
|-----------------------------------|--|
| RLP | |
| RLZ Dbase | |
| RMCP | |
| rmiregistry | |
| Rmonitor | |
| RMT | |
| rmtis | |
| ROHC | |
| RPC2PMAP | |
| RRH | |
| RRP | |
| RSH-SPX | |
| RSVD | |
| RSVP-E2E-IGNORE | |
| RSVP Tunnel | |
| rtip | |
| RTP | |
| RTSPS | |
| RUSHD | |
| Russell Info Sci Calendar Manager | |
| RVD | |
| rxe | |
| SAFT | |
| Sage | |
| SANity | |
| SAP | |
| SATNET | |
| SATNET and Backroom EXPAK | |
| SATNET Monitoring | |
| SCCM | |
| SCCP | |
| SCC Security | |
| Schedule Transfer Protocol | |
| SCO Desktop Administration Server | |
| scohelp | |
| Sco I2 Dialog Daemon | |
| SCO System Administration Server | |
| SCO WebServer Manager | |
| SCO Web Server Manager 3 | |
| SCPS | |

| scx-proxy | | |
|------------------------------------|--|--|
| SDNS-KMP | | |
| SDRP | | |
| Secure IRC | | |
| SecurSight | | |
| Semantix | | |
| Semaphore Sec Pro | | |
| SEND | | |
| Sender Rewriting Scheme | | |
| Service Status Update | | |
| SET | | |
| sFlow | | |
| SFS config server | | |
| SFTP | | |
| Shrinkwrap | | |
| Siam | | |
| SIFT | | |
| SILC | | |
| Silverplatter | | |
| Sitara Dir | | |
| Sitara Management | | |
| Sitara Server | | |
| SKIP | | |
| Skronk | | |
| SMAKYNET | | |
| Smart Session Description Protocol | | |
| SMID | | |
| SMP | | |
| smpnameres | | |
| SMPTE | | |
| smsd | | |
| SMSP | | |
| SNA Gateway | | |
| SNARE | | |
| SNET | | |
| SNNTP | | |
| SNP | | |
| SNPP | | |
| SNTP-HEARTBEAT | | |
| Soap | | |
| SOCKS | | |
| | | |

| SoftEther | | |
|-----------------------|--|--|
| SoftPC | | |
| Softros LAN Messenger | | |
| Sonar | | |
| Splunk | | |
| SPMP | | |
| Sprite RPC | | |
| spsc | | |
| SQLSRV | | |
| Squid | | |
| SRC | | |
| SRMP | | |
| SRP | | |
| SRVFP | | |
| srvloc | | |
| ss7ns | | |
| SSCOPMCE | | |
| SSL | | |
| SST | | |
| STMF | | |
| Stock IXChange | | |
| streettalk | | |
| STUN | | |
| STUN over TLS | | |
| Submit Protocol | | |
| SUBNTBCST_TFTP | | |
| SUNDR | | |
| Sun IPC server | | |
| SUN NDP | | |
| Sunquest | | |
| Sun RPC | | |
| Survey Measurement | | |
| SVMTP | | |
| Swipe | | |
| Sybase SQL | | |
| Synergy | | |
| Synology DSM | | |
| SynOptics SNMP Relay | | |
| SynOptics Trap | | |
| TACACS+ | | |
| Tanium | | |
| | | |

| Tapeware | | |
|-----------------------------------|--|--|
| TCF | | |
| TCPMUX | | |
| TDP | | |
| TDS | | |
| TeamSound | | |
| Technical Analysis Software | | |
| Teedtap | | |
| tell | | |
| TELNETS | | |
| TenFold | | |
| TESLA | | |
| Texar | | |
| TFTP | | |
| Thin Manager TFTP | | |
| TIA/EIA/IS-99 modem client | | |
| TIA/EIA/IS-99 modem server | | |
| TIME.com | | |
| Time | | |
| Timeserver | | |
| tinc | | |
| Tivoli | | |
| TLSP | | |
| TNS CML | | |
| tn-tl-fd1 | | |
| Tobit David | | |
| Tobit David Replica | | |
| Tomatopang | | |
| TP++ | | |
| TP4 | | |
| ТРСР | | |
| ТРІР | | |
| ТРКТ | | |
| TPNCP | | |
| Transport Independent Convergence | | |
| trin00 | | |
| Trunk-1 Protocol | | |
| Trunk-2 Protocol | | |
| TRUSTe | | |
| TTP | | |
| TURN Channel | | |
| | | |

| UAAC | | | |
|------------------------------------|--|--|--|
| UARPS | | | |
| UDP Lite | | | |
| UIS | | | |
| Ulpnet | | | |
| Ultrasurf | | | |
| Unidata LDM | | | |
| Unify | | | |
| Unix time | | | |
| UPMC | | | |
| UPnP | | | |
| UPS | | | |
| User Location Protocol | | | |
| UTI | | | |
| UTMPCD | | | |
| utmpsd | | | |
| UUCP | | | |
| UUCP-PATH | | | |
| UUCP-RLOGIN | | | |
| uuidgen | | | |
| VACDSM-APP | | | |
| VACDSM-SWS | | | |
| VATP | | | |
| vemmi | | | |
| vettcp | | | |
| Vid | | | |
| Videotex | | | |
| Virtual Presence Protocol | | | |
| VISA | | | |
| VMNET | | | |
| VM PWSCS | | | |
| VMTP | | | |
| VMware Fault Domain Manager | | | |
| vnas | | | |
| VPPS-Via | | | |
| VRRP | | | |
| vsinet | | | |
| VSLMP | | | |
| VVPS-Qua | | | |
| Wang Span | | | |
| WAP connectionless session service | | | |
| | | | |

| WAP Push |
|--|
| WAP Push OTA-HTTP port |
| WAP Push OTA-HTTP secure |
| WAP Push Secure |
| WAP secure connectionless session service |
| WAP Session Service Secure |
| WAP Session Service |
| WAP vCal |
| WAP vCal Secure |
| WAP vCard |
| WAP vCard Secure |
| War-rock |
| WCCP |
| Webfilter |
| WebSphere MQ |
| webster |
| WESP |
| whoami |
| Wideband EXPAK |
| |
| Wideband Monitoring |
| Wideband Monitoring Wii Shop Channel |
| Wideband Monitoring Wii Shop Channel WLCCP |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows xact-backup |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows xact-backup Xbone |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows xact-backup Xbone XDMCP |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows Xact-backup Xbone XDMCP |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows xact-backup Xbone XDMCP Xfer XNS |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows Xuindows Xact-backup Xbone XDMCP Xfer XINS XNS |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows Xundows Xact-backup Xbone XDMCP Xfer XINS XNS Authentication XNS Clearinghouse |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows Xact-backup Xbone Xbone XDMCP Xfer XINS XINS Authentication XNS Clearinghouse XNS Time |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion Wpgs WSDD XWindows XWindows Xact-backup Xbone Xbone Xbone XDMCP Xfer XINS XINS XINS XINS XINS XINS XINS Authentication XNS Clearinghouse XNS Time XTP |
| Wideband Monitoring Wii Shop Channel WLCCP World Fusion wpgs WSDD XWindows XWindows Xume Xbone Xbone Xbone Xbone XDMCP Xfer XINS XINS XINS XINS XINS XINS XINS XINS |
| Wideband MonitoringWii Shop ChannelWLCCPWorld FusionwpgsWSDDXWindowsxact-backupXboneXDMCPXferXNSXNS AuthenticationXNS ClearinghouseXTPxvttpXyplex |

Games

| Category | Application |
|----------|----------------------------|
| Games | 4399.com |
| | 9p.com |
| | Addicting Games |
| | Aliexpress |
| | Angry Birds |
| | AOL Games |
| | AOL Games |
| | Armagetron Advanced |
| | Armor Games |
| | Battlefield |
| | Battle.net |
| | Battle.net site |
| | Bejeweled Blitz |
| | Bejeweled Chrome Extension |
| | Bet365 |
| | Bigpoint |
| | Blizzard |
| | Blizzard Downloader |
| | Blockbuster |
| | Blokus |
| | Bubble Island |
| | Bubble Saga |
| | Bubble Witch Saga |
| | Cabal Online |
| | CanvasRider |
| | Castleville |
| | Cityville |
| | Clear Channel |
| | Destructoid |
| | Diamond Dash |
| | Doof |
| | DoubleDownCasino |
| | EA Download Manager |
| | The Escapist Magazine |
| | ESTsoft |
| | Evony |
| | Farmville |
| | Fire |
| | |

| FUX | |
|---------|--------------|
| FreeSt | reams |
| G4 | |
| Game | Front |
| Game | Informer |
| Game | Spot |
| Game | Spy |
| Game | Stop |
| Game | Frailers |
| Geewa | ì |
| GOMT | V.net |
| GTA C | Inline |
| Hanga | me |
| Hattric | k |
| hi5 | |
| lfeng.c | om |
| Isoball | |
| Joystic | 1 |
| King.co | om |
| Kongre | egate |
| Kotaku | I |
| League | e of Legends |
| Lineag | e |
| LINE G | Sames |
| Magicl | and |
| Maples | Story |
| Mesmo | Games |
| Minecr | aft |
| Minicli | þ |
| MyOnl | ineArcade |
| Neope | ts |
| Newgr | ounds |
| Nexon | |
| NFL.co | om |
| Ninten | do |
| OnLive |) |
| PartyP | oker |
| Planet | arium |
| Playdo | m |
| Playsta | ation.com |
| Playsta | ation App |

| Playstation Games |
|-------------------------|
| Pogo |
| Pool Live |
| PopCap Games |
| Premier Football |
| PSP Activity Agent |
| PS3 Community Agent |
| PS3 Downloads |
| PS3 Home Client |
| PS3 Messenger |
| PS3 Updater |
| PSP Community Agent |
| Playstation Store |
| QQ Games |
| Quake |
| Quake Live |
| Raptr |
| Rockstar Games |
| RuneScape |
| Second Life |
| Shopkick |
| Slotomania |
| Social Empires |
| Sohu.com |
| SpeedRunsLive |
| StationLauncher |
| Steam |
| Tango |
| Taringa |
| Tetris Battle |
| The Elder Scroll Online |
| Verizon |
| VMware Horizon View |
| Widget Media |
| Wii |
| Wooga |
| Words With Friends |
| World of Warcraft |
| Xbox Live |
| Xbox Live sites |
| Xfire |
| |

| | Xfire |
|--|--------------|
| | Y8 |
| | Yahoo! Games |
| | Yeti Bot |
| | Zynga |
| | Zynga Poker |

Business

| Category | Application |
|----------|--------------------------|
| Business | 1-800-Flowers |
| | 1&1 Internet |
| | 5pmweb |
| | 6.pm |
| | 7digital |
| | 99Acres |
| | Ace Hardware Corporation |
| | Acer |
| | Acrobat |
| | Adorama |
| | Airspace |
| | Alibaba |
| | Allstate |
| | Amazon |
| | AMD |
| | American Express |
| | Android.com |
| | Apple Push |
| | Apple sites |
| | Apple Store |
| | Argos |
| | Asus |
| | AutoTrader.com |
| | AutoZone |
| | Backpack |
| | Bank of America |
| | Barnes and Noble |
| | Barneys New York |
| | Best Buy |
| | |

| BitCoin |
|----------------------|
| Blackberry sites |
| Blackbox |
| Bloomingdales |
| Bluefly |
| Blue Nile |
| BonPoo |
| Booking.com |
| Boxoh |
| CamerasDirect.com.au |
| Capital One |
| CarMax |
| CC Studios |
| CDiscount |
| Central Desktop |
| Chase |
| CheapOAir |
| CheapTickets |
| Chinaren |
| Chrome webstore |
| Citi |
| Citrix |
| City Sports |
| Clarizen |
| CNET |
| CNET Download |
| CNET TV |
| Concur |
| CORBA |
| Costco |
| Craigslist |
| Crutchfield |
| Dangdang |
| David Jones |
| Deals Direct |
| Dell |
| Dicks Sporting Goods |
| Dillards |
| Discover |
| Drugs.com |
| Drugstore.com |
| |

| East Money |
|-----------------------|
| eBay Bid |
| eBay Search |
| eBay Watch |
| eBuddy |
| Edmunds.com |
| EndNote |
| E*TRADE |
| Etsy |
| Expedia |
| Fidelity |
| Fifth Third Bank |
| Flipkart |
| Fnac |
| Freee TV |
| Frys Electronics |
| FTD |
| Gateway |
| Geico |
| GoBank |
| GO.com |
| Google ads |
| Google Finance |
| Google Play |
| Google Product Search |
| Google Play Books |
| Groupon |
| Home Depot |
| House of Fraser |
| H&R Block |
| HSBC |
| IBM |
| IKEA.com |
| InstaCalc |
| Intel |
| Investopedia |
| IKE |
| it168 |
| J.C. Penney |
| Jetsetz |
| JIRA |
| |

| J.P. Morgan |
|-------------------------|
| Kaspersky Network Agent |
| Kay Jewelers |
| Kismet |
| Kiwoom |
| Kmart |
| Kogan Technologies |
| Kohls |
| Launchpad |
| Leap Motion sites |
| Liberty Mutual |
| LinkedIn Upload |
| LiteCoin |
| Lockerz |
| LOVEFiLM |
| Lowes |
| Luminate |
| Macys |
| MakeMyTrip |
| Megaproxy |
| Menards |
| Microsoft Store |
| MobileAsset |
| Mondex |
| Moneycontrol |
| Morgan Stanley |
| Morningstar |
| Motorola |
| Napster |
| NBA |
| NBC |
| Neckermann |
| Neiman Marcus |
| Newegg |
| Nike |
| Ning |
| Nordstrom |
| NSEIndia |
| Nvidia |
| Office 365 Planner |
| Office Depot |
| |

| OfficeMax |
|---------------------------|
| oo.com.au |
| Opalis Robot |
| OPC-UA |
| Orbitz |
| Overstock.com |
| PayPal |
| PC Connection |
| Pchome |
| PC Mall |
| PDBox |
| PDF |
| PerfectIBE |
| Photoshop |
| PNC Bank |
| Prezi |
| Priceline.com |
| ProFlowers |
| Publishers Clearing House |
| Quill Corporation |
| QVC |
| Raging Bull |
| Redmine |
| REI |
| RevenueHits |
| REVOLVEclothing |
| RitzCamera.com |
| Rona |
| Saks Fifth Avenue |
| Sams Club |
| Samsung |
| Schwab |
| Scottrade |
| Sears |
| Seterus |
| The Sharper Image |
| Shoplet |
| ShopNBC |
| ShopStyle |
| ShorTel Sky Communicator |
| ShowClix |
| |

| Skype for Business |
|--------------------|
| Snapdeal |
| Soribada |
| Sports Authority |
| Staples |
| Starbucks |
| State Farm |
| StubHub |
| StudentUniverse |
| SugarCRM |
| Swarovski |
| Target |
| Tchibo |
| TD Ameritrade |
| TechCrunch |
| TED |
| Tesco.com |
| Theme Forest |
| ThinkGeek |
| Ticketmaster |
| Tickets.com |
| TicketsNow |
| Tiger Direct |
| Toshiba |
| Trac |
| Travelocity |
| Travelzoo |
| TripAdvisor |
| Tripave |
| Tripwire |
| T. Rowe Price |
| Twiddla |
| UC4 |
| Unicenter |
| Urban Outfitters |
| USAA |
| Vanguard |
| Vehix |
| vente-privee.com |
| Victorias Secret |
| Voyages-sncf.com |
| |

| Wachovia |
|---------------------|
| Walmart |
| Wells Fargo |
| Wimbledon |
| Windows Phone sites |
| WiZiQ |
| Woot |
| Wretch |
| Wrike |
| Wunderlist |
| Yahoo! Finance |
| Yatra |
| Yodiz |
| Zales |
| Zappos |
| Zip.ca |

Streaming

| Application |
|------------------------|
| 4Tube |
| 56.com |
| 5by5 Radio |
| Aaj Tak |
| AccuWeather |
| ADNStream |
| Ado Tube |
| Adweek |
| Afreeca |
| AirPlay |
| AirTunes |
| AllRecipes |
| Amazon Instant Video |
| Ando Media |
| AOL Video |
| Apple Music |
| Apple Trailers |
| Apple TV |
| Apple Mobile Yahoo API |
| |

| Ask.com |
|----------------------|
| Asterisk PBX |
| Audible.com |
| AudioDocumentary.org |
| Autoblog |
| Axis Camera Stream |
| Babelgum |
| Baidu Movies |
| The Baltimore Sun |
| Bandcamp |
| BeeMP3 |
| BesTV |
| Bild.de |
| Biography.com |
| Blekko |
| blinkx |
| Blip.tv |
| Boxee |
| Break.com |
| Brightcove |
| Brighttalk |
| BuzzFeed |
| CAM4 |
| CBS |
| CBS Interactive |
| CCP Games |
| Channel 4 |
| Cheezburger |
| China Daily |
| Cisco SIP Gateway |
| Telepresence Control |
| ClearSea SIP Client |
| ClickBank |
| Cloud Browse |
| Clubbox |
| CNBC |
| CNN.com |
| Collider |
| Comedy Central |
| Сох |
| Crackle |
| |

| Crackle Video |
|----------------------|
| Crunchyroll |
| C-SPAN |
| CTV |
| CTV News |
| Cute Overload |
| Dailymotion |
| Deezer |
| DEOS |
| DeviantClip |
| Dilbert.com |
| Djpod |
| Dropcam |
| Drudge Report |
| EarthCam |
| Edge |
| eHow |
| EmpFlix |
| EngageMedia |
| Entertainment Weekly |
| ESPN |
| ESPNcricinfo |
| ESPN Video |
| Examiner.com |
| Extremeube |
| Facebook Photos |
| FFFFOUND! |
| FilmOn |
| FIOS TV |
| Flash Video |
| Food Network |
| FORA.tv |
| Fotki |
| FreeCast |
| FreeSWITCH |
| Fuq |
| Fuyin.TV |
| GG |
| GIFSoup.com |
| GOLF.com |
| GOMTV.com |
| |

| Google+ Videos |
|-------------------------|
| Google Play Music |
| Graboid |
| Grantland |
| Groove Music |
| Gyao |
| HardSexTube |
| НВО |
| HBO GO |
| HostGator |
| Hotstar |
| HTTP Video |
| Hulu |
| Hulu Video |
| The Hype Machine |
| I Catcher Cam Streaming |
| IceShare |
| iHeartRadio |
| Indiegogo |
| iTunes |
| iTunes Desktop |
| I Waste So Much Time |
| Jamendo |
| Jango |
| JoinMe |
| Justin.tv |
| KBS |
| Keez Movies |
| Kickass Torrents |
| Kodi |
| Kuaibo |
| KVOA.com |
| Last.fm |
| LA Times |
| Lequipe.fr |
| LeTV |
| Library of Congress |
| LINE |
| LINE Media |
| Live365 |
| LiveFlash |
| |

| LiveJasmin |
|---------------------------|
| Livestream |
| Lycos |
| lynda.com |
| Maestro FM |
| Manta |
| Marca |
| Mashable |
| Matsushira_Camera_Stream |
| mck-ivpip |
| Media Hub |
| Media Stream Daemon |
| MegaPorn |
| Megavideo |
| MelOn |
| Metacafe |
| MixBit |
| Mixcloud |
| MKRU Streaming |
| MobiTV |
| Mobotix Camera Stream |
| MOG |
| Movieclips |
| MovieTickets.com |
| MTv |
| Myspace Videos |
| NAMP |
| NBC News |
| NCAA |
| Nero SIP Client |
| Netcam |
| Netflix |
| Netflix stream |
| News Distribution Network |
| news.com.au |
| Newser |
| NHL.com |
| Nico Nico Douga |
| Nico Nico Douga Video |
| NOAA |
| Nokia Music |
| |
| NSPlayer | |
|-----------------------|--|
| Nuance Voice Platform | |
| NY Daily News | |
| The New York Times | |
| Ogg | |
| Ooyala | |
| Open Films | |
| OpenSIPS | |
| OSSProxy | |
| Outbrain | |
| Panasonic Camera | |
| Pandora | |
| Pandora Audio | |
| Pandora TV | |
| Paramount Network | |
| PBS | |
| Penultimate | |
| People.com | |
| Peoples Daily | |
| People Of Walmart | |
| Picsearch | |
| Piksel | |
| Plex TV | |
| PNAS | |
| POLITICO.com | |
| Pop Salad | |
| Pornhub | |
| Pornorama | |
| Pornoxo | |
| PPStream | |
| PPTV | |
| QDown | |
| Qriocity | |
| Quickflix | |
| QuickTime | |
| QVOD | |
| Rakuten | |
| RealAudio | |
| RealClearPolitics | |
| Reality Kings | |
| Realview TV | |
| | |

| Redbox InstantRediff.comRedOrbitRedTubeReutersRhapsodyRokuRTMPSBSShockwaveSHOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSlackerSlackerSlate MagazineSingboxSongzaSongzaSongCastSoundCloudSouthern LivingSpankWireSpankWireSquare Inc.StarsportsStreemoodStreemate <trtr>Str</trtr> | Redbox |
|---|--------------------|
| Rediff.comRedOrbitRedTubeReutersRhapsodyRokuRTMPRuTubeSBSShockwaveSHOUTCast RadioSHOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSIPSilackerSlate MagazineSlutloadSongsSongzaSongzaSongCastSoundCloudSouhCNINE ANYTIMESoluthern LivingSpankWireSpiagel OnlineSquare Inc.StarsportsStarsportsStarentStreemateStreemate | Redbox Instant |
| RedOrbitRedTubeReutersRhapsodyRokuRTMPRuTubeSBSShockwaveSHOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSlackerSlackerSlate MagazineSongzaSongzaSony Camera StreamSopCastSouthern LivingSpankWireSpankWireSquare Inc.StarsportsStarsportsStreamateStreamateStreamateStreamate | Rediff.com |
| RedTubeReutersRhapsodyRokuRTMPRuTubeSBSShockwaveSHOUTCast RadioShowboxSHOUTCast RadioShowboxShowboxShoUTCast RadioShowboxShoUTCast RadioShowboxShoUTCast RadioShowboxShouboxShouboxShouboxShouboxShouboxShouboxSilverlightSina VideoSlackerSlackerSlackerSlackerSlare MagazineSlingboxSongsSongsSongsSongsSongsSongaSoundCloudSouthern LivingSpankWireSpankWireSquare Inc.StarsportsStar TVStereomoodStreamateStreamateStreamate | RedOrbit |
| ReutersRhapsodyRokuRTMPRuTubeSBSShockwaveSHOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSIPSjackerSlackerSlate MagazineSlutloadSorigzaSongzaSony Camera StreamSopCastSouthern LivingSpankWireSparesSquare Inc.StarsportsStarsportsStreamateStreamate | RedTube |
| RhapsodyRokuRTMPRuTubeSBSShockwaveSHOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSIPSlackerSlackerSlate MagazineSongzaSongzaSony Camera StreamSopCastSoundCloudSOUNDROPSpakWireSpiegel OnlineSquare Inc.StarsportsStar TVStarenoodStreamateStreamate | Reuters |
| RokuRTMPRuTubeSBSShockwaveShOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSIPsipXecsSlackerSlate MagazineSlutloadSorgaSongsSongy Camera StreamSopCastSouthern LivingSpankWireSpankWireSquare Inc.StarsportsStarsportsStereomoodStreamateStreamate | Rhapsody |
| RTMPRuTubeRuTubeSBSShockwaveShOUTCast RadioShowboxSHOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSIPsipXecsSlackerSlackerSlate MagazineSorigJaSongzaSongzaSony Camera StreamSopCastSoundCloudSOUNDROPSpankWireSpankWireSquare Inc.StarsportsStarsportsStreemoodStreamateStreetFire | Roku |
| RuTubeSBSShockwaveSHOUTCast RadioShowboxSHOWTIME ANYTIMESilverlightSina VideoSIPsipXecsSlackerSlate MagazineSlutloadSongzaSongzaSony Camera StreamSoundCloudSOUNDROPSpankWireSpankWireSquare Inc.StarsportsStarsportsStarsportsStereomoodStreamateStreamateStreetFire | RTMP |
| SBS Shockwave SHOUTCast Radio Showbox SHOWTIME ANYTIME Silverlight Silverlight Sina Video SIP SipAccs SIP SipXecs Slate Magazine Slate Magazine Slate Magazine Slate Magazine Slate Magazine Slate Magazine Social-TV Songs Solutload Social-TV Songs Songza Song Song Song Song Song Song Song Song | RuTube |
| Shockwave SHOUTCast Radio Showbox SHOWTIME ANYTIME Silverlight Sina Video SIP Sina Video SIP Sing Case Slacker Slate Magazine Slate Magazine Southern Living Southern Living Southern Living Southern Living Southern Living Southern Living Southern Living Slate SpankWire SpankWire SpankWire Slate Inc. Starsports Star TV Stareomood Star TV Stereomood Stickam | SBS |
| SHOUTCast Radio Showbox SHOWTIME ANYTIME Silverlight Silav Video SIP sipXecs Slacker Slacker Slate Magazine Slingbox Slutload Social-TV Songs Song2a Sony Camera Stream SopCast SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Sipers Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate | Shockwave |
| Showbox SHOWTIME ANYTIME Silverlight Sina Video SIP sipXecs Slacker Slacker Slacker Slate Magazine Slingbox Slutload Social-TV Songs Songza Songza SongZa SongCast SoundCloud SoUNDROP Southern Living SopCast SoundCloud SOUNDROP Southern Living Spiegel Online Spiegel Online Spiegel Online Slaguare Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | SHOUTCast Radio |
| SHOWTIME ANYTIME Silverlight Sina Video SIP sipXecs Slacker Slacker Slate Magazine Slate Magazine Slate Magazine Slate Magazine Slate Magazine Slate Magazine Slate Magazine Southora Stream Songa Son | Showbox |
| Silverlight Sina Video SIP sipXecs Slacker Slacker Slacker Slate Magazine Slingbox Slutload Social-TV Songs Songa Songa Song2 | SHOWTIME ANYTIME |
| Sina Video SIP sipXecs Slacker Slacker Slate Magazine Slingbox Slutload Social-TV Songs Songza Song Camera Stream SopCast SoundCloud SoUNDROP Southern Living Soptart Illustrated Spiegel Online Spiegel Online Starsports Starsports Star TV Stereomood Stickam Streamate StreetFire | Silverlight |
| SIP sipXecs Slacker Slacker Slate Magazine Slingbox Slutload Social-TV Songs Songza Songza Sony Camera Stream SopCast SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Spiegel Online Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Sina Video |
| sipXecs Slacker Slate Magazine Slingbox Slutload Social-TV Songs Songa Song2 Sony Camera Stream SopCast SoundCloud SoUNDROP Southern Living Southern Living Southern Living SpankWire Spiegel Online Spiegel Online Spiegel Online Sports Illustrated Square Inc. Starsports Star TV Stareomood Stickam | SIP |
| Slacker Slate Magazine Slingbox Slutload Social-TV Songs Songza Songza Sony Camera Stream SopCast SoundCloud SopCast SoundCloud Southern Living Southern Livin | sipXecs |
| Slate Magazine Slingbox Slutload Social-TV Songs Songza Sony Camera Stream SopCast SopCast SoundCloud SoUNDROP Southern Living Southern Living SpankWire SpankWire Spiegel Online Sports Illustrated Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Slacker |
| Slingbox Slutload Social-TV Songs Songza Sony Camera Stream SopCast SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Spiegel Online Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Slate Magazine |
| Slutload Social-TV Songs Songza Songza Sony Camera Stream SopCast SoundCloud SOUNDROP Southern Living Southern Living SpankWire Spiegel Online Spiegel Online Sports Illustrated Sports Illustrated Square Inc. Starsports Starsports Starsports Starsports Stareamood Stickam | Slingbox |
| Social-TV Songs Songza Sony Camera Stream SopCast SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Slutload |
| Songs Songza Sony Camera Stream SopCast SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Spiegel Online Sports Illustrated Square Inc. Starsports Starsports Starsports Stareuncod Stickam Streemate StreetFire | Social-TV |
| Songza Songza Stream SopCast SopCast SoundCloud SOUNDROP Southern Living Spiegel Online Spiegel Online Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Songs |
| Sony Camera Stream SopCast SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Songza |
| SopCast SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Sports Illustrated Square Inc. Starsports Starsports Star TV Stereomood Stickam Streamate StreetFire | Sony Camera Stream |
| SoundCloud SOUNDROP Southern Living SpankWire Spiegel Online Sports Illustrated Square Inc. Starsports Starsports Star TV Stereomood Stickam Streamate StreetFire | SopCast |
| SOUNDROP Southern Living SpankWire Spiegel Online Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | SoundCloud |
| Southern Living SpankWire Spiegel Online Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streemate StreetFire | SOUNDROP |
| SpankWire Spiegel Online Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Southern Living |
| Spiegel Online Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | SpankWire |
| Sports Illustrated Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Spiegel Online |
| Square Inc. Starsports Star TV Stereomood Stickam Streamate StreetFire | Sports Illustrated |
| Starsports Star TV Stereomood Stickam Streamate StreetFire | Square Inc. |
| Star TV Stereomood Stickam Streamate StreetFire | Starsports |
| Stereomood Stickam Streamate StreetFire | Star TV |
| Stickam Streamate StreetFire | Stereomood |
| Streamate StreetFire | Stickam |
| StreetFire | Streamate |
| | StreetFire |

| Teache | rTube |
|----------|-----------------|
| Telly | |
| Tencen | t Video |
| The Atl | antic |
| The Bla | ze |
| theCHI | VE |
| The Gu | ardian |
| The Inte | ernet Archive |
| The We | eek Magazine |
| Tianya | |
| Tidal | |
| Tightro | pe Interactive |
| TMZ | |
| TNAFliz | < |
| TopTer | REVIEWS |
| Toshiba | a Camera Stream |
| Tube8 | |
| Tudou | |
| TuneIn | |
| Turntab | le |
| Tu TV | |
| Tvigle | |
| TVonlin | e.cc |
| TVU Ne | etworks |
| TwitchT | V |
| Twitter | Video |
| UltraVio | blet |
| UOL | |
| USA To | oday |
| Ustrear | n.tv |
| Vdio | |
| VDOLiv | /e |
| Veetle | |
| Veoh | |
| VEVO. | com |
| Viddler | |
| Video S | Sift |
| Videos | urf |
| Viewsu | rf |
| Vimeo | |

| VLC Media Player |
|------------------------|
| Vonage |
| Vube |
| WeatherBug |
| Weather.com |
| Weather.gov |
| WebM |
| WebM Files |
| Webs |
| wetpaint entertainment |
| wimp.com |
| Winamp |
| Windows Media |
| Windows Media Player |
| Wired.com |
| WorldstarHipHop |
| WTOP |
| Xhamster |
| Xiami.com |
| The Xinhuanet |
| Xlite SIP Client |
| XM Radio Online |
| Xnxx |
| X-PRO SIP Client |
| Xtube |
| Xvideos |
| XXX Tld |
| Yahoo! Douga |
| Yahoo! Flash |
| Yahoo! Screen |
| Yandex |
| Yellow Pages |
| You Jizz |
| Youku |
| You Porn |
| YouTube |
| YouTube Comment |
| Youtube Upload |
| yuvutu |
| Zattoo |
| Zaycev |
| |

| Zippyshare |
|------------|
| |

Cloud

| Category | Application |
|----------|--------------------------------|
| Cloud | 360 Safeguard |
| | 4chan |
| | AOL Instant Messenger |
| | AIM Express |
| | AOL Instant Messenger Netscape |
| | Aliwangwang |
| | Animoto |
| | Avast |
| | Avira Download/Update |
| | BaiduHi |
| | Chatroulette |
| | Check Point |
| | Cisco Jabber |
| | Eset |
| | F-Prot |
| | F-secure |
| | Google Talk Gadget |
| | GSS HTTP |
| | HipChat |
| | ICQ |
| | ICQ2Go |
| | imo.im |
| | ircu |
| | Jabber |
| | Kaspersky |
| | Malwarebytes |
| | Malware Defense System |
| | McAfee |
| | Mediamax |
| | Messenger |
| | Mibbit |
| | MMS |
| | МРМ |
| | |

| MSN Messenger |
|-----------------------------|
| MSNP |
| Microsoft Windows Messenger |
| NeoGAF |
| Nessus |
| Nimbuzz |
| ntalk |
| Omegle |
| Panda |
| Pinger |
| QOTD |
| QQ |
| Rypple |
| Skype Auth |
| Sophos Live Protection |
| SUPERAntiSpyware |
| Symantec System Center |
| talk |
| Tencent Cloud |
| Tinychat |
| TOC |
| Vchat |
| Web Of Trust |
| WooMe |
| xda-developers |
| Yahoo! Messenger |
| Yahoo! Messenger SMS |
| YiXin |
| Zoho Chat |

Web

| Category | Application |
|----------|-------------|
| Web | 12306.cn |
| | 2345.com |
| | 2channel |
| | 2Leep |
| | 39.net |
| | 58 City |
| | |

| Abonti |
|----------------------------------|
| About.com |
| Acoon.de |
| Acrobat.com |
| Adap.tv |
| Adcash |
| AddThis |
| AddThis Bot |
| AddToAny |
| Adenin |
| AdF.ly |
| Admin5 |
| Adobe Analytics |
| Adobe Connect |
| AhrefsBot |
| Aili |
| AIM HTTP API |
| Airtime |
| Aizhan |
| Akamai |
| Akamai NetSession Interface |
| Alipay |
| Alisoft |
| Aliyun |
| Al Jazeera |
| Allegro.pl |
| Allmusic |
| ALTools |
| Ameba |
| American Airlines |
| Ancestry.com |
| Android Asynchronous Http Client |
| Answers.com |
| AOL |
| Apache Nutch |
| Apple App Store |
| Apple Developer |
| Apple iForgot |
| Apple Maps |
| Apple PubSub |
| Apple qtpix |
| |

| Apple Syndication |
|----------------------|
| Aptean |
| ArcGIS |
| Arizona Public Media |
| Arora |
| ArtStack |
| ASA |
| ASF |
| Asia Times Online |
| Associated Press |
| Astraweb |
| AT&T |
| auditd |
| Autodesk |
| Autohome.com.cn |
| Avaya |
| Aweber |
| Amazon Web Services |
| Azure cloud portal |
| Babylon |
| Backpage.com |
| Backupgrid |
| Baidu |
| Baiduspider |
| Balatarin |
| Bazaarvoice |
| ВВ |
| BBB |
| BigBlueButton |
| Bing |
| Bing Bar |
| Bingbot |
| Bing Maps |
| BioDigital Human |
| Bitcoin Forum |
| BitGravity |
| bitly |
| Bizrate |
| Blackboard |
| BlekkoBot |
| Bloglovin |
| |

| Bloomberg |
|---------------------|
| Bluehost |
| BoldChat |
| Bootstrap CDN |
| Boxcar.io |
| Browzar |
| Business Insider |
| California.gov |
| Car and Driver |
| Carbonite |
| CareerBuilder.com |
| Catho |
| CBS Sports |
| Character Generator |
| Chartbeat |
| CheapStuff |
| Chickipedia |
| Chimera2 |
| China.com |
| China News |
| Chosun |
| Chrome |
| Cisco |
| Cisco Phone |
| CiteULike |
| Cleartrip |
| CloudFront |
| CloudMe |
| Coc Coc bot |
| Collabedit |
| CollegeHumor |
| CometBird |
| Commerce |
| Comodo Dragon |
| Conduit |
| Connexion client |
| Constant Contact |
| Convore |
| Coral CDN |
| Coupa |
| Coupons.com |
| |

| Coursera |
|--------------------|
| Crazy Browser |
| Creative Commons |
| CrossLoop |
| CSDN |
| cURL |
| CyberGhost VPN |
| The Daily Beast |
| Datei.to |
| Daum |
| Daum Blog |
| Daum Cafe |
| DCinside |
| Delta Search |
| Demandbase |
| DeNA websites |
| De Telegraaf |
| Detroit Free Press |
| DICOM |
| Digg |
| Diigo |
| DioDeo |
| DirBuster |
| Disney |
| Disqus |
| DNS |
| Dogpile |
| DomainTools |
| Dooble |
| Dragon Dictate |
| Drawbridge |
| Drupal |
| DSW |
| DuckDuckGo |
| Dwolla |
| EA Games |
| EarthLink |
| Easou Spider |
| easyMule |
| еВау |
| EdgeCast |
| |

| Edge Chromium | | | |
|-----------------------------|--|--|--|
| EditGrid | | | |
| eFax | | | |
| Egloos | | | |
| Elinks | | | |
| Enet | | | |
| Envato | | | |
| E! Online | | | |
| Epiphany | | | |
| eRecht24 | | | |
| eRoom | | | |
| Etao | | | |
| European Union | | | |
| EVE Online | | | |
| Evernote | | | |
| Exchange Online | | | |
| ezhelp | | | |
| Eznet | | | |
| Fab.com | | | |
| Fancy | | | |
| Fark | | | |
| Facebook Applications Other | | | |
| Facebook Games | | | |
| Facebook Notes | | | |
| Facebook Sports | | | |
| Facebook Utilities | | | |
| FC2 | | | |
| FedEx | | | |
| Feed43 | | | |
| FeedBurner | | | |
| Feedfetcher | | | |
| Feedly Fetcher | | | |
| Fileguri | | | |
| FileHost.ro | | | |
| FireAMP | | | |
| Firefox | | | |
| Fiverr | | | |
| Flexera Software | | | |
| Flickr | | | |
| Flightradar24 | | | |
| Flock | | | |
| | | | |

| Flurry Analytics | | |
|--------------------------------|--|--|
| FogBugz | | |
| folkd | | |
| Forbes | | |
| The Free Dictionary | | |
| Freelancer | | |
| FriendFinder | | |
| FrostWire | | |
| Funny or Die | | |
| Ganji | | |
| The Gap | | |
| Garmin | | |
| Gawker | | |
| Gazprom Media | | |
| Gbridge | | |
| Genieo Web Filter | | |
| Ghostery | | |
| Giganews | | |
| GitHub | | |
| Gizmodo | | |
| Glype | | |
| GNOME | | |
| GNU Project | | |
| Goal | | |
| GOGOBOX | | |
| Goodreads | | |
| GoodSync | | |
| Google | | |
| Google Accounts Authentication | | |
| Google Analytics | | |
| Google APIs | | |
| Google App Engine | | |
| Googlebot | | |
| Googlebot Image Search | | |
| Google Calendar | | |
| Google Code project hosting | | |
| Google Drive | | |
| Google Fiber | | |
| Google Groups | | |
| Google Maps | | |
| Google News | | |

| Google PageSpeed | | |
|-----------------------------|--|--|
| Google+ Photos | | |
| Google Remote Desktop | | |
| Google Safebrowsing | | |
| Google Sign in | | |
| Google Translate | | |
| Google URL Shortener | | |
| goo.ne.jp | | |
| GoToMeeting | | |
| GoToTraining | | |
| Gravatar | | |
| GreenBrowser | | |
| GSA Crawler | | |
| Guangming Online | | |
| Haiku Learning Systems | | |
| Hao123.com | | |
| Harvard University | | |
| Helpshift | | |
| HIP | | |
| HLN | | |
| The Hollywood Reporter | | |
| HootSuite | | |
| Hopster | | |
| Hotels.com | | |
| HotPads | | |
| HowardForums | | |
| HP Home & Home Office Store | | |
| HubPages | | |
| The Huffington Post | | |
| HugeDomains.com | | |
| Нири | | |
| iBackup | | |
| ICA Browser | | |
| IFTTT | | |
| iFunny | | |
| IGN | | |
| llovelM | | |
| Image Venue | | |
| IMDB | | |
| IMRWorldWide | | |
| Inbox.com | | |

| In.com | | |
|---------------------------|--|--|
| Indeed | | |
| Indiatimes | | |
| Info.com | | |
| InfoSeek | | |
| Infusionsoft | | |
| InsightExpress | | |
| Integromedb Crawler | | |
| Intermarkets | | |
| Internet Explorer | | |
| Intralinks | | |
| Intuit | | |
| IPFIX | | |
| iStock | | |
| Jalopnik | | |
| Java | | |
| jdistatic | | |
| JetSetMe | | |
| JikeSpider | | |
| Jimdo | | |
| Jingdong (360buy.com) | | |
| Johns Background Switcher | | |
| JonDo | | |
| Joomla | | |
| Joongel | | |
| JSTOR | | |
| JustCloud | | |
| Justdial | | |
| K9 Web Protection | | |
| Kakao Story | | |
| Kayak | | |
| Kickstarter | | |
| Konqueror | | |
| Kooora.com | | |
| Kraken | | |
| Leboncoin | | |
| Legacy.com | | |
| Level 3 | | |
| Libsyn | | |
| Libwww-Perl | | |
| Licorize | | |

| Limelight | | |
|------------------------|--|--|
| LINK | | |
| LinkedIn Inbox | | |
| LinkedIn Profile | | |
| Linux Mint | | |
| Livedoor | | |
| Livefyre | | |
| LivePerson | | |
| LiveStrong.com | | |
| LivingSocial | | |
| Localytics | | |
| Loyalty Innovations | | |
| Lynx | | |
| Mac App Store | | |
| MacPorts | | |
| MagicBricks | | |
| MagPie | | |
| MapQuest | | |
| Mathworks | | |
| MCStats | | |
| MDNS | | |
| Mediabot | | |
| Meebo | | |
| MegaMeeting | | |
| Mercado Livre | | |
| MetaCrawler | | |
| MetaFilter | | |
| MGID | | |
| Mgoon | | |
| Michigan Radio | | |
| Microsoft | | |
| Microsoft CRM Dynamics | | |
| Midori | | |
| Mikogo | | |
| Mint.com | | |
| MissLee | | |
| MJ12 Bot | | |
| MKRU | | |
| MLive | | |
| Monster.com | | |
| Mop.com | | |
| · | | |

| Motley Fool | |
|-------------------------------|--|
| Microsoft CryptoAPI | |
| MSDN | |
| Microsoft download | |
| MSN | |
| msnbot | |
| Microsoft Excel | |
| MS Office Existence Discovery | |
| Microsoft Powerpoint | |
| MS Office Protocol Discovery | |
| Microsoft Word | |
| MyLife | |
| MyPCBackup | |
| Myspace Photos | |
| MyWebSearch | |
| NAI | |
| NASA | |
| Nate | |
| NATO | |
| Naukri | |
| Naver | |
| Naver Blog | |
| Naver Cafe | |
| Naverisk | |
| ndgsa-crawler | |
| Netease | |
| Neteller | |
| Netnews | |
| NetNewsWire | |
| NetSurf | |
| Netvibes | |
| New Relic | |
| NewsNow | |
| Newsvine | |
| NextBus | |
| NIH | |
| Nokia | |
| Nokia Maps | |
| Nokia Store | |
| Norton AntiVirus | |
| NPR | |
| | |

| Nuance | | |
|------------------------|--|--|
| OCLC | | |
| OCSPD | | |
| Office 365 | | |
| Office365 Admin portal | | |
| OkCupid | | |
| Okta | | |
| OpenBSD | | |
| OpenDNS | | |
| OpenSUSE | | |
| Opera | | |
| Oracle sites | | |
| OsiriX | | |
| OverBlog | | |
| Owlinbot | | |
| PACS | | |
| PaleMoon | | |
| Panoramio | | |
| Pastebin.com | | |
| Patch.com | | |
| Paybill | | |
| Perforce | | |
| Phoca | | |
| PHP | | |
| phpBB | | |
| PHP-SOAP | | |
| Picasa | | |
| Picnik | | |
| Pingdom | | |
| Pivotal Tracker | | |
| PixelMags | | |
| Plista | | |
| Podio | | |
| PopUrls | | |
| Powermarks | | |
| Presto | | |
| Printer Pro Desktop | | |
| Progressive | | |
| PS3 web browser | | |
| Psiphon | | |
| QQ Music | | |
| | | |

| QQ Pay | | | |
|---------------------------|--|--|--|
| QualysGuard | | | |
| Quick Look | | | |
| Quora | | | |
| Quote.com | | | |
| R6 FeedFetcher | | | |
| Rackspace | | | |
| Radian6 CommentReader | | | |
| Rainmeter WebParser | | | |
| Rambler | | | |
| Real Estate ABC | | | |
| Realtor.com | | | |
| reCAPTCHA | | | |
| Reddit | | | |
| rekonq | | | |
| RetailMeNot | | | |
| Rotten Tomatoes | | | |
| rsync | | | |
| Safari | | | |
| Salesforce.com | | | |
| Salesforce.com Live Agent | | | |
| Sanook.com | | | |
| Seamonkey | | | |
| Searchnu | | | |
| Search-Result.com | | | |
| The Seattle Times | | | |
| SendSpace | | | |
| ServiceNow | | | |
| SFGate | | | |
| Shareman | | | |
| Sharepoint Online | | | |
| Shockwave Flash | | | |
| ShopAtHome | | | |
| ShowMyPC | | | |
| Show My Weather | | | |
| Shutterfly | | | |
| Shutterstock | | | |
| Silk | | | |
| simple-get | | | |
| SimplePie | | | |
| Siri | | | |
| | | | |

| Sky.com | | |
|---------------------|--|--|
| Slashdot | | |
| Slickdeals | | |
| SlideShare | | |
| Slothtrader | | |
| SM | | |
| SmugMug | | |
| Snort.org | | |
| SockShare | | |
| Softonic | | |
| Sogou | | |
| Sogou web spider | | |
| Soku | | |
| Songsari | | |
| Sony | | |
| Soso | | |
| SOS Online Backup | | |
| Soufun | | |
| Sourcefire.com | | |
| Sourceforge | | |
| Southwest Airlines | | |
| Space.com | | |
| SPC Media | | |
| Speedtest | | |
| Speedtest Upload | | |
| Sprint | | |
| SPS | | |
| SSL client | | |
| Stanford University | | |
| StatCounter | | |
| Storify | | |
| StreamWork | | |
| StumbleUpon | | |
| SugarSync | | |
| SuperNews | | |
| SurveyMonkey | | |
| Svpply | | |
| Swagbucks | | |
| Тадоо | | |
| Taobao | | |
| TechInline | | |

| Technorati | | |
|----------------------------|--|--|
| Tencent | | |
| The Independent | | |
| The Onion | | |
| The Telegraph | | |
| TikTok | | |
| TimesJobs | | |
| Times Union | | |
| TinyPic | | |
| Tiny Tiny RSS | | |
| TinyURL | | |
| TISTORY | | |
| Tmall | | |
| T Mobile | | |
| Top Gear | | |
| TOR | | |
| ToysRUs | | |
| Trend Micro | | |
| Trulia | | |
| TruuConfessions | | |
| Tumblr | | |
| TurboTax | | |
| Turner Broadcasting System | | |
| Tus Files | | |
| TV Guide | | |
| TweetDeck | | |
| Twitter Link Service | | |
| Twitter Music | | |
| Ubuntu | | |
| UltraView CCS | | |
| United Airlines | | |
| Uptobox | | |
| UpToDate | | |
| Urban Airship | | |
| URLAppendBot | | |
| urlgrabber | | |
| U.S.Bank | | |
| USPS | | |
| uTorrent | | |
| Venmo | | |
| Ventrilo | | |
| | | |

| VeriSign | | |
|--|--|--|
| Verizon Wireless | | |
| VMware Server Console | | |
| Voilabot | | |
| VPNReactor | | |
| w3schools.com | | |
| Walgreens | | |
| wApua | | |
| WarriorForum | | |
| The Washington Post | | |
| Washington Times | | |
| WDT | | |
| WeatherLink | | |
| Weather Underground | | |
| Webcrawler | | |
| WebEx | | |
| WebEx Connect | | |
| WebMD | | |
| Websense | | |
| Weebly | | |
| Western Digital | | |
| WeTransfer | | |
| WhereCoolThingsHappen | | |
| WhitePages Inc | | |
| Wikia | | |
| wikidot | | |
| Wikipedia | | |
| Wikispaces | | |
| Microsoft Windows Live Services Authentication | | |
| Windows Help client | | |
| Wolfram Alpha | | |
| Wondershare | | |
| Wood TV8 | | |
| Woopra | | |
| Wordpress | | |
| WordReference.com | | |
| Workday | | |
| WorldCat | | |
| Wow | | |
| Wyzo | | |
| Xanga | | |
| | | |

| | Xcode |
|--|------------------|
| | Xenu Link Sleuth |
| | XProtectUpdater |
| | Yahoo! |
| | Yahoo! Calendar |
| | Yahoo! Slurp |
| | Yahoo! Toolbar |
| | Yammer |
| | Yandex Bot |
| | Yandex Images |
| | Yesky |
| | YY |
| | Zamzar |
| | Zapier |
| | Zbigz |
| | Zendesk |
| | ZergNet |
| | Zhihu.com |
| | Zillow |
| | ZipCloud |
| | Zipskinny |
| | Zmags |
| | Zoho |
| | Zol.com.cn |
| | Zombo.com |
| | Zulily |

Portal

| Category | Application |
|----------|---------------------------------------|
| Portal | B&H Photo Video |
| | Black & Decker Corporation |
| | Cisco SLA |
| | Cloudnymous Login |
| | CMIP |
| | daytime |
| | echo |
| | Honeywell Experion DSA Server Monitor |
| | Fanpop |
| | |

| Fotolog |
|--------------------------------------|
| Fring |
| Google Reader |
| Google Toolbar |
| Hideman Login |
| Hide My Ass! |
| Hindustan Times |
| Hola |
| Honeywell Control Station/NIF Server |
| Hotwire |
| ibVPN Login |
| In |
| Indian Railways |
| IRCTC |
| Ivacy Login |
| J&R |
| L2TP |
| Lord & Taylor |
| Megaco |
| MGCP |
| MSN2Go |
| Munin |
| MUX |
| Ngrok |
| Opera VPN |
| RAP |
| RSVP |
| RTSP |
| SGMP |
| Sina |
| Skype |
| SMPP |
| SMUX |
| SNMP |
| Stat Service |
| Sulekha |
| Systat |
| TeamSpeak |
| Tiffany & Co. |
| Tunnelbear Login |
| Twitter4J |
| |

| UMA |
|---------------|
| USAIP |
| VyprVPN Login |
| whois |
| WX |
| Yahoo! Voice |
| Zabbix |
| Zabbix Trap |
| Zero VPN |

P2P

| Category | Application |
|----------|----------------|
| P2P | 100Bao |
| | ABC |
| | Aimini |
| | Applejuice |
| | Ares |
| | Baidu Yun |
| | BaoFeng |
| | BearShare |
| | BitComet |
| | BitTornado |
| | BitTorrent |
| | Direct Connect |
| | eDonkey |
| | ExtraTorrent |
| | Faroo |
| | FilesWire |
| | GnucleusLAN |
| | Gnutella |
| | Gnutella2 |
| | GoBoogy |
| | Hotline |
| | iMesh |
| | Joost |
| | KAD |
| | Kugou |
| | Manolito |
| | |

| Mininova |
|-----------------------|
| Mute |
| MyMusic |
| Paltalk File Transfer |
| PeerCast |
| PeerEnabler |
| Pipi |
| The Pirate Bay |
| Росо |
| PPTV |
| SoulSeek |
| TheCircle |
| BitTorrent tracker |
| Torrentz |
| Vuze |
| WinMX |
| Xunlei |
| Yet ABC |
| YoTorrent |

Download

| Category | Application |
|----------|------------------------------|
| Download | Android Marketplace Download |
| | Apple Pipeline |
| | Advanced Packaging Tool |
| | BackWeb |
| | FlashGet |
| | Microsoft AutoUpdate |
| | MyDownloader |
| | Wget |
| | Zedge |

Para mais informações a respeito de Application Control, acesse este link.

UTM - Services - Web Filter

O Web Filter funciona como uma segunda camada para filtrar a navegação dos usuários. É o responsável pelo filtro de conteúdo e só pode ser utilizado quando as requisições de acesso Web HTTP/HTTPS são repassadas por um servidor Proxy, antes de solicitar os dados ao servidor remoto, ele redireciona algumas informações da requisição (url, usuário e endereço IP do usuário) para o serviço de Web Filter.

Com base nas informações enviadas pelo *Proxy HTTP*, o serviço de *Web Filter* procura um filtro por categoria de que se aplica, através das "Políticas de segurança". Dependendo de como as políticas estão configuradas, o *Web Filter* responde ao proxy se a requisição foi permitida ou bloqueada.

Neste item podemos gerenciar o recurso através da "Atualização" da base de URLS de categorias, definir a "Mensagem de Bloqueio", aplicar "Controles de *login* por domínio para os serviços Google" e ainda habilitar a integração do serviço de busca segura "Safe Search" para os principais buscadores da w eb, "Google, Yahoo e Bing".

Para acessar esta tela, basta selecionar a opção "Web Filter".

| 0 \$ 3 | Services | ~ |
|---------------|----------------------|---|
| » | Firewall | |
| » | Proxy | Ο |
| » | Web Cache | Ο |
| » | Web Filter | Φ |
| » | Application Control | Ο |
| » | Intrusion Prevention | Ο |
| » | Threat Protection | Ο |
| » | SD-WAN | Ο |
| » | DHCP | Ο |
| » | DNS | Ο |
| » | DDNS | Φ |
| » | VPN IPSEC | σ |
| » | VPN SSL | Ο |

Services - Web Filter

A tela abaixo será exibida:

| Veb Filter | | |
|-------------------|---------------------|----------------|
| Polia Setop | | |
| 3 moords | | a (* |
| | Bearighten | ation |
| Thrusty mak | 36402.858 | 2.1 |
| Productivity Janu | Realizability Lenit | × 1 |
| . matythis | incarry tilius | × 1 |
| | | a 💽 a Utrimpro |



O UTM por padrão disponibiliza 3 Web Filters:

- Security Risk;
 Productivity Loss;
 Security Ethics.

A tela Web Filter comporta as seguintes abas:

- Profiles; Settings.

A seguir analisaremos os componentes da aba Profiles.

Web Filter - Profiles

O sistema possibilita a aplicação de vários perfis de filtro de conteúdo em um mesmo contexto de conexão (Origem, Destino, Usuário). Ou seja, ao detectar uma política onde determinado tipo de tráfego HTTP ou HTTPS é aplicável, o sistema considera o URL nos parâmetros de busca da política (Lookup).

Nos perfis de Filtro de Conteúdo é possível Permitir, Bloquear e Desabilitar as categorias. Uma política que possua Web Filter habilitado leva em consideração apenas os URLs cujas categorias foram permitidas ou bloqueadas no Perfil, se o URL estiver desabilitado, o serviço irá passar para a próxima política onde o contexto da conexão HTTP dê *match*, caso não exista nenhuma política que se aplique, o URL será bloqueado, o mesmo acontece para aplicações do tipo *web* caso o *application control* esteja ativo.

Esta tabela demonstra o comportamento caso a requisição dê match em categoria Web Filter e Application Control:

| Application Control | Categoria Webfilter | Comportamento |
|--------------------------|--------------------------|------------------|
| Sem controle de inspeção | Sem controle de inspeção | Permitir acesso |
| Sem controle de inspeção | Desabilitado | Próxima política |
| Sem controle de inspeção | Recusar | Bloquear acesso |
| Sem controle de inspeção | Permitir | Permitir acesso |
| Permitir | Sem controle de inspeção | Permitir acesso |
| Bloquear | Sem controle de inspeção | Bloquear acesso |
| Desabilitado | Sem controle de inspeção | Próxima política |
| Desabilitado | Desabilitado | Próxima política |
| Desabilitado | Permitir | Permitir acesso |
| Desabilitado | Recusar | Bloquear acesso |
| Permitir | Desabilitado | Permitir acesso |
| Permitir | Permitir | Permitir acesso |
| Permitir | Recusar | Bloquear acesso |
| Bloquear | Desabilitado | Bloquear acesso |
| Bloquear | Permitir | Bloquear acesso |
| Bloquear | Recusar | Bloquear acesso |
| Não dar match em nenhum | a política | Bloquear acesso |

Para mais informações sobre application control, consulte esta página.

Caso a aba não esteja selecionada, clique em "Profiles".

| Profiles | Settings |
|----------|----------|
| Aba P | rofiles |

Surgirá a tela "Profiles" de Web Filter, conforme demonstrado pela imagem abaixo:

Ø

Web Filter

| nine Setzegi | | 1 |
|-------------------|-------------------|-------------------|
| | Securition | Atlant |
| Tripely mix | 36.045 8.9 | 2.1 |
| Productivity Long | Readershilly land | × 1 |
| manythis | incurry Million | × * |
| | | a 💽 🖉 Altinique y |

Web Filter - Profiles

Esta sessão irá abordar como cadastrar, editar e remover os perfis de Web Filter,

A seguir, analisaremos as funções localizadas no topo deste painel.

Web Filter - Profiles - Menu de Ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



Web Filter - Menu de Ações

O menu é composto das seguintes opções:

- Create Profile;
- Delete Profile.

A seguir cada opção do menu de ações será detalhada.

Web Filter - Profiles - Menu de Ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de Web Filter. Para acessar, clique no menu de ações [

1. Clique na opção "Create Profile";



J.

Web Filter - Create Profile

2. A tela "Create Profile" será exibida. Conforme demonstrado pela imagem abaixo:

| General | | |
|--|---|--|
| * Narne | | |
| Description | | |
| | 14 | |
| Search | | |
| Restrict login domains for Google Apps | Enforce Safe Search for Google, Bing, Yahoo | |
| Filters | | |
| Web categories | File Filter | |
| | | |
| Surfing Quotas | | |
| Masimum Time | Maximum Download Size | |
| Mindeland day | 105 V | |
| Makimum Traffic | Maximum Upload Size | |
| ist presity | | |
| | | |

Nesta janela é possível efetuar as configurações gerais, configurar filtros e quotas que serão utilizados nesse perfil. A seguir analisaremos cada painel desta janela:

General

Em "General" temos as seguintes caixas de texto:

| General | |
|-------------|--|
| • Name | |
| Webfilter | |
| Description | |
| Webfilter | |



- Name: Definir um nome para o perfil. Ex.: Webfilter,
- Description: Definir uma descrição para o perfil. Ex.: Webfilter.

Search

Em "Search" é possível gerenciar como será efetuado o acesso aos serviços de busca:

| Search | |
|--|--|
| Restrict login domains for Google Apps | Enforce Safe Search for Google, Bling, Yahoo |
| Web | Filter - Search |

- Restrict login domains for Google Apps []: Esta opção permite controlar quais os domínios efetuarão o acesso aos Apps do Google;
- Enforce Safe Search for Google, Bing, Yahoo Site Search da Google que fornece a capacidade de impedir que sites com conteúdo inapropriado apareçam em seus resultados de pesquisa. Este recurso aplica um filtro de pesquisa segura direto nas ações de "Pesquisa" dos usuários na sua estação de trabalho a partir dos browsers. Este recurso de pesquisa segura se aplica aos principais buscadores da WEB (Google, Yahoo e Bing).

Filters

Em "Filters" as seguintes opções estão disponíveis:



de ações [_____], também é possível aplicar alguma destas opções em todas as categorias em Allow All, Block All e Disable All para desabilitá-las. Segue uma breve descrição da função de cada ação:
Allow: O acesso a URLs classificadas com esta categoria é permitido;
Block: O acesso a URLs classificadas com esta categoria é bloqueado;
Disable: Esta categoria é desabilitada, isso significa que o Web Filter irá ignorá-la e considerará apenas as URLs em categorias permitidas ou bloqueadas.

| All | Q | ~ |
|--|---------|----|
| Uncategorized Sites | Allow 🗸 | 1 |
| Abortion | Allow 🗸 | 1 |
| Pro-life | Allow 🗸 | 1 |
| Pro-Choice | Allow 🗸 | 1 |
| Activism Groups | Allow 🗸 |] |
| Adult Material | Allow 🗸 |] |
| Adult Content | Allow 🗸 | |
| Nudity | Allow 🗸 | |
| Sex | Allow 🗸 | |
| Sex Education | Allow 🗸 | |
| Lingerie and Swimsuit | Allow 🗸 | |
| Business and Economy | Allow 🗸 | |
| Financial Data and Services | Allow 🗸 | |
| ▼ Drugs | Allow 🗸 | |
| Abused Drugs | Allow 🗸 | |
| Prescribed Medications | All | 1. |

Para mais informações a respeito das categorias exibidas neste painel, vida a sessão Diagnostics - Category Lookup

Também é possível adicionar categorias customizadas clicando no botão Custom[



Custom

h,

Web Filter - Add Categoy - Custom

Clique no campo e selecione a categoria desejada, neste campo estarão disponíveis os objetos do tipo dictionaries, os objetos selecionados serão

| ndicionados como tags. Por fim, clique no botão Cancel | Cancel |] para sair dessa janela ou clique no botão | Save[| re] para salvar. |
|---|--------|--|--------|----------------------|
| Para finalizar a adição das categorias, clique no botão S | Save |] para salvar ou clique no botão Cancel [| Cancel |] para sair desta |

 File Filter []: Permite selecionar os tipos de arquivo adicionados em Objects - Contents (que são objetos criados com Mime-types e Extensions: doc, ppt, exe, pdf, bat, dll, ocx, wmi, jpeg, mpeg, etc) para aplicar filtros ao conjunto de políticas aplicadas, de modo a checar arquivos trafegados entre aplicações do tipo P2P, IM, SMB.

Para selecionar os objetos, clique no botão [;], e habilite as caixas de checagem desejadas. No menu de ações, também é possível clicar em **Select** All para marcar tudo ou **Deselect All** para desmarcar todas as categorias.

Controle de Transferência de Arquivos: possibilita a criação de filtros para arquivos e dados predefinidos, e identificados por extensão e assinaturas. Também conta com a capacidade de identificar e prevenir a transferência de arquivos por tipo (ex: doc, ppt, exe, pdf, bat, dll, ocx), ainda que dentro de aplicações como: P2P, IM e SMB.

Possibilita a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo destes tipos de arquivos. Conta também com a capacidade de identificar e prevenir a transferência de informações sensíveis (ex: número de cartão de crédito) possibilitando a criação de novos tipos de dados via expressão regular.

| | ۹ 🗸 |
|--------|--------|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | < 1 > |
| | |
| | |
| Cancel | Save |
| | |
| 0 | Cancel |

Surfing Quotas

Em "Surfing Quotas" o seguinte painel é exibido:
| rting Quotas | | | | |
|--------------|----------------|---|-----------------------|--|
| Maximum Time | e | | Maximum Download Size | |
| | Houro per day: | 1 | NE | |
| Maximum Traf | fic | | Maximum Upload Size | |
| | Into per dev | | HO | |

Web Filter - Surfing Quotas

• [] Maximum Time: Permite configurar uma quota de tempo em minutos ou horas por dia.

| Maximum Tim | e | |
|-------------|-----------------|-----------|
| | Hours per day | $^{\sim}$ |
| Maximum Tra | Minutes per day | |
| | Hours per day | |

Web Filter – Maximum Time

• [] Maximum Traffic: Permite configurar uma quota de tráfego em MB por dia.

| 🗹 Maximum Traf | fic |
|----------------|---------------------|
| | MB per day \wedge |
| | MB per day |

Web Filter – Maximum Traffic

• [Max Download Size: Permite configurar o tamanho máximo para download, em MB ou GB.

| Maximum Dov | wnload Size | |
|-------------|-------------|---|
| | МВ | ^ |
| Maximum Up | МВ | |
| | GB | |

Web Filter - Maximum Download Size

• [] Max Upload Size: Permite configurar o tamanho máximo para upload, em MB ou GB.

| 🔽 Maximum U | Jpload Size | |
|-------------|---------------------------|------|
| | мв | ^ |
| | МВ | |
| | GB | |
| Web | > Filter - Maximum Upload | Size |
| | | |

| As configurações efetuadas no perfil podem ser adicion | adas a uma polít | tica na aba Inspection na opção Web Filter. | | |
|--|------------------|--|------|---|
| Após finalizar todas as configurações, clique no botão Cancel | Cancel |] para voltar para o painel <i>Profiles</i> ou clique no botão Save [| Save |] |

Para visualizar um exemplo de configuração, acesse esta página.

Web Filter - Exemplo: Configuração do Safe Search

A seguir, será exemplificada a configuração necessária para o funcionamento do Safe Search na rede local. Nesse caso, foi criado um Web Filter simplesmente forçando o Safe Search.

| General | | | | | |
|--------------------------------------|------|-----------|----------------------|-----------------|-----|
| * Name | | | | | |
| Sale Search | | | | | |
| Description | | | | | |
| Web Filter to enforce Safe Search | | | | | iz) |
| Search | | | | | |
| Restrict login domains for Google Ap | ps | 🛃 Enforce | Safe Search for Goog | le, Bing, Yahoo | s |
| Filters | | | | | |
| Web categories | | File Filt | er | | |
| | | | | | |
| Surfing Quotas | | | | | |
| Masimum Time | | Maximu | m Download Size | | |
| Princip per dag | 196 | | 10. | | |
| Maximum Traffic | | Maximu | m Upload Size | | |
| int par stay | . 01 | | | | |
| | | | | | |

Na aba Properties:

- Name: Safe Search;
- Description: Web Filter to Enforce Safe Search;
- Enforce Safe Search for Goole, Bing, Yahoo []: Assegurar-se de que o checkbox está marcado.

Após efetuar a configuração acima, será necessário criar uma política como demonstrado pela imagem abaixo.

| 1 | | | |
|-------------|--------------------|---------------|--|
| Properties. | - Beneral | | |
| Conditions | * Nave | | |
| | Safe Search Policy | | |
| inpection | Description | | |
| 0.1608 | | | |
| matrig | * Action | Tags | |
| | Alter | - Sitchever A | |
| | * Pelicy Group | | |
| | WEE-549-Search | | |
| | C Traffic Logging | | |
| | Scheekale | | |
| | Tree | C Schedule | |
| | | | |
| | | | |

Web Filter - Policy - Properties

Na aba Properties:

- Name: Safe Search Policy;
 Action: Allow;
 Policy Group: WEB Safe Search;
 Tags: Safe Search.

A seguir acesse a aba Conditions:

| Properties. | * Source | | | | |
|-------------|---------------|-------------------|---|---------|--|
| Depittons | Matanak Jone | Network Interface | | Cauttry | |
| | int | | | | |
| ropection | IP Address | HAC Addm.ur | | | |
| liniting | | | | | |
| | Destation | | | | |
| | IP Address | Service | | Country | |
| | | | = | | |
| | ident/Acation | | | | |
| | Authenticated | 3.04 | | | |
| | | | | | |

Web Filter - Policy - Conditions

- Network Zone []: LAN;
- Service **]**: HTTP e HTTPS.

A seguir acesse a aba *Inspection:*

| #1500CD0/Y | | |
|---------------------|--|--|
| | | |
| Sil ingretter | | |
| bimple Departure | | |
| | | |
| Thread Protection | | |
| | | |
| Application Control | | |
| | | - |
| Web filter | | |
| and month | | |
| | | |
| | | |
| | SE Ingestion SE Ingestion Invest Protection Application Control Veb Filter Inkensor) | SE Impectary Infrasion Prevention Infrasion Prevention Thread Protection Application Commit. Web Filter Sek much |

Na aba Inspection:

• Web Filter Z: Safe Search (ou o nome do Web Filter criado logo no início).

Você terá chego no resultado demonstrado abaixo:

| IL + MED Sele Search | | | | | | | |
|----------------------------|---|---|----|-------|------|--|--|
| () (#E table has a booking | - | 1 | 17 | 1.000 | 1010 | | |

Política WEB - Safe Search

Ao finalizar este passo o Safe Search entrará em vigor.

| I Para funci UDP, pois o Pro | onamento correto xy só consegue f | no navega azer essa in | dor Google Ch Ispeção SSL n | nrome e pa no tráfego 1 | ra efetu TCP. | ıar uma p | esquisa se | gura no Goo | ogle, será neo | cessário bloquea | ar a porta |
|---------------------------------|--------------------------------------|---------------------------|--------------------------------|----------------------------|------------------|-----------|------------|-------------|----------------|------------------|------------|
| | 411 8,004 | . 411 | 340 501 | ** | e | alonga | 40.07 | Eth (area) | 888 | 6.terr | |
| | | | | Web | b UDP | 443 Block | k | | | | |

Para mais informações, a respeito de políticas, vide o capítulo Policy.

À seguir, detalharemos como remover um perfil de Web Filter.

Web Filter - Profiles - Menu de Ações - Delete Profile

Através do botão "Delete Profile" é possível deletar os Profiles selecionados. Para deletar pelo Menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul []. Ex.: *Test*:

| Veb Fil | ter | | |
|-----------------|---------------------|-----------------------------------|----------------------------|
| Profiles | Sattings | | |
| 4 records | | | (a) |
| | Namu | Description | Actio |
| | Security Risk | Security Risk | 1 |
| | Productivity uses | Productivity Lass | 1 |
| | Security Titrics | Security filmes | 1 1 |
| | Test | Test | 1 |
| | | | c 🕇 > 10 ² 2sig |
| | ~ | | |
| tre no r | nenu de ações [] e | clique na opção "Delete Profile". | |
| | | Q V Create Profile | |
| | | Delete Profile | |
| | | Web Filter – Delete Profiles | |

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os Profiles selecionados:

| Delete Profile | × |
|---|---------------|
| Are you sure you want to delete: Test ? | |
| | Cancel Delete |

Web Filter - Mensagem de deleção do Profile



Após realizar esses procedimentos, os profiles terão sido deletados com sucesso.

À seguir, iremos detalhar o conteúdo das colunas.

Web Filter - Profiles - Colunas

A seguir explicaremos cada coluna da aba Web Filter.

| | active provide the second seco | | |
|------|--|-----------------|--------|
| HONT | | | (A) |
| 1 | ume . | Description | Active |
| 1. | anothy Rok | Teratly Gai | / 1 |
| 11.1 | tala Sviy uni | Prinketnen Land | 2.3 |
| 11.1 | working the second | Secret/Lines | / 1 |

Profiles - Web Filter

A seguir explicaremos cada coluna:

- Caixa de Seleção[___]: Seleciona o profile;
 Name: Apresenta o nome do profile cadastrado;
- Description: Apresenta a descrição do profile cadastrado;
 Actions: A coluna "Actions" é composta pelos botões:

• Botão Edit []: Permite editar as configurações do profile adicionado na opção Create Profile do menu de ações; • Botão Delete [

À seguir iremos analisar o conteúdo da aba Settings.

Web Filter - Settings

Este item permite customizar a página de bloqueio que é devolvida aos usuários da rede referente aos acessos "Não Autorizados" do tráfego Web (interceptados pelo proxy).

Para configurar a página de bloqueio, clique em "Settings".

| Profiles | Settings |
|----------|----------|
| | |



Surgirá o painel "Customize Blocking Page", conforme demonstrado pela imagem abaixo:

| Veb Filter | |
|-------------------------|--|
| Valles Settings | |
| | |
| Outramite Blocking Rope | |
| New Logi | |
| | |
| Slocking reessage | |
| | |
| Retained | |
| Tablect to attend page | |
| | |
| | |

Web Filter - Settings

É possível alterar o "Logo" e redefinir a "Mensagem de bloqueio":

• New logo: É possível selecionar um novo logo para tela de bloqueio. Para fazer upload de uma imagem, basta clicar em Upload Upload],

+

após carregar a imagem, para visualizá-la, clique em Preview File 🞯 por fim, caso deseje removê-la clique em Remove File 🛄;

- Blocking message: É possível personalizar a mensagem de bloqueio que retorna para o cliente;
- Hostname: Permite definir qual será o Hostname utilizado;
- Redirect to external page: É possível redirecionar o tráfego para uma página de bloqueio externa.

| Castonias Backing Page | |
|--|----------|
| Now Loga | |
| | |
| tiloddag message | |
| Automa construit configuration prevents your request intercheng allowed at this tase. Obseus surrety your service provides (Pysscheel this is incorrect | |
| Hoodrawe: | |
| +marker/blockbit.com | |
| Reditati to oternal page | |
| | |
| | |
| Customize blocking page - Example | |
| | |
| Para os casos das tentativas de acesso WEB não autorizado, ou seja, definidos por meio das políticas de segurança com a ação de "Bloc elecionada, o sistema retornará a tela de "Bloqueio", com a mensagem especificada nas configurações acima. | queio" |
| ra salvar todas as alterações, clique em []. | |
| Cound augessefully | |
| Saved successfully | |
| Successfully Saved | |
| | |
| | |
| | |
| ós salvar, para que as configurações entrem em vigor será necessário acessar a fila de comandos [] e aplicar as alterações efetuad is informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos. | as. Para |

UTM - Services - Intrusion Prevention

O *Intrusion Prevention System* é responsável pela monitoração e análise do tráfego da rede, a fim de identificar o tráfego de códigos maliciosos, e ataques. Baseado em assinaturas; regras e sensores ele capaz de analisar o conteúdo de todo tráfego passante da rede, é o responsável em identificar aplicativos e ameaças direcionadas e persistentes e efetuar os respectivos bloqueios. Integrado a uma base de assinaturas eletrônicas atua na camada de aplicação, capaz de analisar o conteúdo dos pacotes em tempo real, identificar e efetuar o bloqueio do pacote ou mesmo o *IP* de origem.

Baseado em assinaturas, regras e sensores ele compara e analisa o conteúdo de todo tráfego Inbound/Outbound "Redirecionado" através de mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações e gera os registros de todos os pacotes identificados na sua base de assinaturas, seja a execução de aplicativos não autorizados, tentativa de intrusão de ameaças, ataques direcionados ao próprio equipamento, suportando algumas técnicas como: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.

O IPS suporta também as verificações nos protocolos de VoIP: H.323, SIP, MGCP e SCCP

Por default o IPS possui mais de 72.835 assinaturas (informação validada em 25 de Novembro de 2021).

Vale ressaltar que esta quantia total de assinaturas é dinâmicas e estas assinaturas são administradas pela equipe da Blockbit Labs, sendo periodicamente atualizadas.

Para acessar esta tela, basta selecionar a opção "Intrusion Prevention".

0

| 📽 Services 🛛 👻 | | | | | | |
|----------------|----------------------|---|--|--|--|--|
| » | Firewall | O | | | | |
| » | Proxy | Ο | | | | |
| » | Web Cache | Ο | | | | |
| » | Web Filter | σ | | | | |
| » | Application Control | σ | | | | |
| » | Intrusion Prevention | σ | | | | |
| » | Threat Protection | Ο | | | | |
| » | SD-WAN | σ | | | | |
| » | DHCP | σ | | | | |
| » | DNS | σ | | | | |
| » | DDNS | σ | | | | |
| » | VPN IPSEC | Φ | | | | |
| » | VPN SSL | σ | | | | |

Services - Intrusion Prevetion

A tela abaixo será exibida:

| Intrusion Prevention | | |
|--|---------------------|------------------|
| hale maintee binings prove invigence for | | |
| and | | |
| Anna - | Tracights | San Proven Adven |
| 11 An air frentise | Transfer Parameters | teres 1 CONS |
| | | (I) - House |

Intrusion Prevention

A tela Intrusion Prevention comporta as seguintes abas:

- Profiles;
 Allowed Addresses List;
 Blocked Addresses List;
 Quarantine;
 Custom Signatures;
 PCAP.

A seguir analisaremos os componentes da aba Profiles.

Intrusion Prevention - Aba Allowed Addresses

Na aba Allowed Addresses é possível cadastrar endereços IP tanto de origem como destino ou até mesmo importar uma lista de endereços IP para serem considerados confiáveis e darem um bypass nas assinaturas do Intrusion Prevention.

Caso a aba não esteja selecionada, clique em "Allowed Addresses".

| Intrusio | on Prevention | | | | |
|----------|-------------------|-------------------|------------|-------------------|------|
| Profiles | Allowed Addresses | Blocked Addresses | Quarantine | Custom Signatures | PCAP |
| | | | | | |

Aba Allowed Addresses

Surgirá a tela "Allowed Addresses" do Intrusion Prevention, conforme demonstrado pela imagem abaixo:

| hatles | Allowed Addoments | Tisckel Addresses | Quatavise | CurtornSignatures | PCAP | |
|-----------|-------------------|-------------------|-----------|-------------------|------|--------------------|
| 15 record | 6) | | | | | |
| | 8 - | | | | | Artissa |
| | 240,247,285,75 | | | | | |
| | 15.196328-31 | | | | | 0 |
| | 300.118.07.125 | | | | | |
| | 17236158-230 | | | | | 8 |
| | 199,171,141,29 | | | | | 8 |
| | 214.5134 | | | | | |
| | 394-197-247-385 | | | | | |
| | 10140104.000 | | | | | a |
| | 15.237-42.101 | | | | | 0 |
| | 122048439 | | | | | |
| | | | | | | (1) 2 > (strong - |

Intrusion Prevention - Allowed Addresses

Esta sessão irá abordar como cadastrar, editar e remover os IPs de Allowed Addresses do Intrusion Prevention;

A seguir, analisaremos as funções localizadas no topo deste painel.

Intrusion Prevention - Aba Allowed Addresses - Menu de Ações

No topo direito da tela temos o menu de ações:

Intrusion Prevention – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Intrusion Prevention - Allowed Addresses - Menu de Ações

O menu é composto das seguintes opções:

- Import Allowed Addresses;
- Create;
- Delete.

A seguir cada opção do menu de ações será detalhada.

| Allowed Addresses - M | enu de Ações - Create |
|---|--|
| | ~ |
| Através da opção "Create" é possível criar uma lista de IPs | s. Para acessar, clique no menu de ações []. |
| 1. Clique na opção "Create Profile"; | |
| | |
| | |
| | ۲ ک |
| | Import Allowed Addresses |
| | Create |
| | Delete |
| | |

Allowed Addresses - Menu de Ações - Create

2. A tela "Allowed Addresses" será exibida. Conforme demonstrado na imagem abaixo:

| | Allowed Address | es | | × |
|---|--|---|----------------------------|--------------------------|
| | • Version IPv4 | 6 | | |
| | * Address | | Mask | |
| | | | 255.255.255.255 | + |
| | | | | |
| Version: Determina ent Address: Neste campo | Allo are IPv4 e IPv6, qual se deve-se digitar o ende | owed Addresses rá utilizado na A ereco /P que ser | - Import Allowed Address | ancel Since |
| <i>Mask</i>: Neste campo, dig <i>List</i>: Clique no botão [| gite a máscara de rede, | remover um IP | da lista clique em [|]. |
| Caso deseje cancelar clique no t | Cancel | cel]. Para co | oncluir a adição clique no | botão Save[Save] |
| | | Addres | ss added successfully | |

As configurações foram feitas com sucesso.

Allowed Addresses - Menu de Ações - Delete

Através do botão "Delete" é possível deletar os IPs selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *IP*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *IP*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul [

| 15 record | ÷ | |
|-----------|-----------------|------------------|
| | B | Artisa |
| | 246,247,295,75 | |
| | 15.1%.28.31 | 8 |
| | 300.115.01.125 | 3 |
| 8 | 1723635130 | 3 |
| | 199,117,141,29 | |
| | 21.451.86 | |
| | 394.107.245.385 | |
| | 15145104.00 | a |
| | 15.207-82.101 | |
| | T2.21484.38 | |
| | | (1) 2 5 Million |





3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os Profiles selecionados:



Após realizar esses procedimentos, os IPs terão sido deletados com sucesso.

Allowed Addresses - Menu de Ações - Import Allowed Addresses list

Através da opção "Import Allowed Addresses" é possível importar uma Allowed Addresses list pré-criada para o UTM. Para acessar, clique no menu de



ações []. 1. Clique na opção "*Create Profile*";



Allowed Addresses - Menu de Ações - Import Allowed Addresses list

2. A tela "Import Allowed Addresses" será exibida. Conforme demonstrado na imagem abaixo:

| Import Allower | d Addresses | × |
|---|---|------|
| Select file | | |
| T. Clickto Up | oload | |
| | Cancel | Save |
| Ą | Ilowed Addresses - Import Allowed Addresses list | |
| 3. Selecione o arquivo desejado clicando no botão | 土 Click to Upload | |
| Ste botão aceita arquivos de extensão .txt | | |
| 4. Ao carregar o arquivo com sucesso, uma mensage | m de confirmação será exibida: | |
| | 15/15 item(s) imported successfully | |
| | Item(s) successfully imported | |

5. Ao finalizar a adição dos itens, a seguinte mensagem de confirmação será exibida:



6. Por fim, a tela exibirá todos os IPs adicionados:

| fler | Allowed Addresses Introduce Current Signatures PCAP | |
|----------|---|-----------------|
| S record | | (d) |
| | B | Action |
| | 240,247,235,75 | 1 |
| | 15.196.128.11 | |
| | 300.115.07.125 | 9 |
| | 1728456430 | 1 |
| • | 195.171.141.29 | 0 |
| | 21.4.54.84 | 0 |
| | 394.157.247.385 | 1 |
| | 15145164380 | 9 |
| | 15.207-42.107 | |
| | 12.21A94.39 | 1 |
| | | (1) 2 5 Million |

Allowed Addresses - IPs adicionados

Após realizar esses procedimentos, a importação terá sido efetuada com sucesso.

Intrusion Prevention - Aba Blocked Addresses list

Nesta aba é possível administrar a lista de IPs suspeitos que o Intrusion Prevention utilizará.

Para efetuar as configurações, clique em "Blocked Addresses".

| Intrusio | on Prevention | | | | |
|----------|-------------------|-------------------|------------|-------------------|------|
| Profiles | Allowed Addresses | Blocked Addresses | Quarantine | Custom Signatures | PCAP |
| | | Aba Blocked Ad | dresses | | |

Surgirá a tela "Blocked Addresses" do Intrusion Prevention, conforme demonstrado pela imagem abaixo:

| Intrusion Prevention | | | | | |
|----------------------|-------------------|----------|--------------------|------|---------|
| Pulles Neweskalesces | Elocked Addresses | Question | Catore Significant | POVP | |
| | | | | | |
| Bane | | | | | Actions |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Intrusion Prevention - Blocked Addresses list

Esta sessão irá abordar como cadastrar, editar e remover os IPs de Blocked Addresses List do Intrusion Prevention;

A seguir, analisaremos as funções localizadas no topo deste painel.

Intrusion Prevention - Aba Blocked Addresses - Menu de Ações

No topo direito da tela temos o menu de ações:

Intrusion Prevention – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Intrusion Prevention - Blocked Addresses - Menu de Ações

O menu é composto das seguintes opções:

- Import Blocked Addresses;
- Create;
- Delete.

A seguir cada opção do menu de ações será detalhada.

| Blocked Addresses - M | enu de Ações - Create |
|---|---|
| | ~ |
| Através da opção "Create" é possível criar uma lista de IPs | . Para acessar, clique no menu de ações []. |
| 1. Clique na opção "Create"; | |
| | |
| | ۹ 🗸 |
| | Import Blocked Addresses |
| | Create |
| | Delete |
| | |

Blocked Addresses - Menu de Ações - Create

2. A tela "Blocked Addresses" será exibida. Conforme demonstrado na imagem abaixo:

| | Blocked Addresses | | | × |
|---|--|--|------------------|----|
| | Version IDv4 IDv5 | | | |
| | * Address | Mask | | |
| | | 255 255 255 255 | · ·] + | |
| | | | | |
| | | | - | |
| | | | 1 | |
| | Blocked | l Addresses - Create Blocked Addresse | s list | |
| Version: Determina Address: Neste campo Mask: Neste campo | entre <i>IPv4</i> e <i>IPv6</i> , qual será u npo, deve-se digitar o endereç , digite a máscara de rede; | tilizado na <i>Blocked Addresses list;</i> o <i>IP</i> que será adicionado na <i>Blocked Ad</i> | ddresses list, | |
| List. Clique no bota | | | | |
| o deseje cancelar clique i | no botão Cancel |]. Para concluir a adição clique no bo | otão Save | ve |
| | | Address added successfully | | |

As configurações foram feitas com sucesso.

Blocked Addresses - Menu de Ações - Delete

Através do botão "Delete" é possível deletar os IPs selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *IP*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *IP*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul [

| 15 record | da . | (a.). |
|-----------|------------------------------------|-----------------|
| 1. | Name | Action |
| | 248.247(205.75 | |
| | 15.156.125.33 | |
| | 108.115.07.125 | |
| | 27.238.150.234 | 8 |
| | 294.377.143.26 | |
| | 20A5438 | |
| | 394.397.247.183 | |
| | 10.140.104.100 | |
| | 75.237.42.197 | 8 |
| | 72.254.64.36 | |
| | | < 1 2 > W/mp |
| | Blocked Addresses - Seleção dos IF | Ps para deletar |

| | ٩ | ~ |
|--------------|---------|-------|
| Import Block | ed Addr | esses |
| Create | | |
| Delete | | |

Blocked Addresses - Delete Profile

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os Profiles selecionados:

| | Are you sure? | × |
|----------------------------|--|------------------------|
| | Are you sure you want to delete: 100.115.97.125, 27.238 75.237.42.197 ? | 3.150.230, 20.4.54.98, |
| - | Blocked Addresses – Mensagem confirmando a e | Cancel Delete |
| Caso desejar cancelar clio | que no botão <i>Cancel</i>]. Para concluir, clique no botão | Delete |
| | Address removed successful Address successfully removed | illy |

Após realizar esses procedimentos, os IPs terão sido deletados com sucesso.

Blocked Addresses - Menu de Ações - Import Blocked Addresses

Através da opção "Blocked Addresses" é possível importar uma Blocked Addresses list. Para acessar, clique no menu de ações [

1. Clique no menu de ações:

| | ٩ | ~ |
|--------------|---------|-------|
| Import Block | ed Addr | esses |
| Create | | |
| Delete | | |

1

Blocked Addresses - Menu de Ações - Import Blocked Addresses

2. A tela "Import Blocked Addresses" será exibida. Conforme demonstrado na imagem abaixo:

| | Import Blocked Addresses X | |
|---------------------------|--|--|
| | Select file | |
| | Cancel | |
| | Blocked Addresses - Import Blocked Addresses | |
| 3. Selecione o arquivo de | esejado clicando no botão []: | |
| Este botão aceita | arquivos de extensão .txt | |
| 4. Ao carregar o arquivo | com sucesso, uma mensagem de confirmação será exibida: | |
| | 15/15 item(s) imported successfully Item(s) successfully imported | |

5. Ao finalizar a adição dos itens, a seguinte mensagem de confirmação será exibida:



6. Por fim, a tela exibirá todos os IPs adicionados:

| ntrusio | n Prevention | | | | |
|---------|----------------------|---------------------|--------------------------|-----|-----------|
| fotia | Alased Addresses Glo | okad Astronom Quine | tile 👘 Gutori Significie | 104 | |
| 15 reco | rde | | | | a . |
| | Name | | | | Actions |
| | 345,347,205,75 | | | | |
| | 15.156.120.33 | | | | 8 |
| | 180.225,97.125 | | | | 0 |
| | 27.138.150.230 | | | | 0 |
| | 150,171,541,20 | | | | 0 |
| | 21.4.54.98 | | | | 0 |
| | 184.291.347.183 | | | | 0 |
| | 18.146.164.180 | | | | 0 |
| | 75.227,42.397 | | | | Û |
| | 72.254.84.96 | | | | 8 |
| | | | | (12 | > 11/14ge |

Blocked Addresses List - IPs adicionados

Após realizar esses procedimentos, a importação terá sido efetuada com sucesso.

Intrusion Prevention - Aba Custom Signatures

Em Custom Signatures, é possível inserir assinaturas, que eventualmente venham a ser relevantes.

Nesta seção, veremos como configurar uma nova assinatura:

| Intrasion Prevent | iter | u- | | |
|-------------------|----------|-------------|-----|-------------------|
| | Naming | No. Langery | N/M | 1 * 85m |
| | | | | |
| | | | | |

Intrusion Prevention - Custom Signatures

| Create Signature | |
|---|----------------------------|
| Em options [] encontra-se a opção " <i>Create</i> ": | |
| | ۹ 🗸 |
| | Import Custom Signatures |
| | Create |
| | Custom Signatures - Create |

Após, a seguinte tela estará disponível:

| * SID | | | × |
|---|---|-----------------------------|----------------------------|
| . Catagoine | | | |
| All | | | ~ |
| * Risk Low Medium | 🔵 High | * Pi | rofile Client Server |
| * Custom Signatures | | | |
| #alert tcp any 21 -> \$H0 | OME_NET any (m | sg:"ET ATTACK_RESPONS | ε |
| | | | .11 |
| | | Cancel | Save |
| | Create | menu | |
| SID: É o código de identificação da assinatura er Category: Categorias disponíveis para este SID; Risk: Nível de risco de ameaça da assinatura; Profile: Permite selecionar o perfil da assinatura Custom Signatures: Permite nomear a assinatura | n questão; ; , se cliente (<i>Client</i>)ou ıra. | servidor (<i>Server</i>); | |
| Import custom signatures | | | |
| Import Custom Signate | ures | | Х |
| File | | | |
| _t_ Click to upload | | | |
| | Cancel | Download model | Import |
| | Import r | nenu | |

- *File*: Clique para fazer o upload de um arquivo contendo a assinatura a ser importada; *Download model:* Nesta opção, temos um exemplo do formato a ser utilizado na configuração da assinatura;
- Import: Botão que realiza a importação do arquivo contendo a assinatura.

A seguir, analisaremos as funções localizadas no topo deste painel.

4

Intrusion Prevention - Aba PCAP

PCAP ou Packet Capture é uma API (Application Programming Interface) que faz a captura de pacotes de dados de tráfego de rede. Por meio da leitura de pacotes de dados TCP/IP e UDP, permite a gravação de dados de tráfego de rede para monitoração e análise. Permite também a identificação de tráfego malicioso de uma fonte externa. As assinaturas são consolidadas em um arquivo contendo logs que reportam o comportamento e características das mesmas. Caso a opção (PCAP - Packet Logger) não tenha sido marcada na criação/edição de um perfil de IPS, nenhum arquivo será exibido nesta seção.

Esta aba exibe os dados das assinaturas (perfis) de IPS que estão com a funcionalidade PCAP habilitada:

| Intession | n Privention | | | | |
|-----------|--------------------------|-----------------|-------|-------|--------|
| Pathe | Statistics Statement Ser | en landigen mar | | | |
| | | | | | |
| | bar | Spotters | . ter | Pages | Anters |
| | | | | | |
| | | | | | |
| | | | | | |

Intrusion Prevention - PCAP

Date: Data na qual o arquivo contendo os logs foi gerado.

Signatures: Nomes das assinaturas encontradas.

Size: Tamanho total do arquivo.

Progress: Estado atual do arquivo (in progress, done) em termos de 0 a 100%.

Actions: Ações tomadas quanto ao manuseio do arquivo por parte do sistema.

A seguir, analisaremos as funções localizadas no topo deste painel.

Intrusion Prevention - Aba Profiles

Através desta aba é possível criar perfis de proteção contra ameaças e exploits de possíveis vulnerabilidades da sua rede.

Caso a aba não esteja selecionada, clique em "Profiles".

| Intrusio | on Prevention | | | | | |
|----------|-------------------|-------------------|------------|-------------------|------|--|
| Profiles | Allowed Addresses | Blocked Addresses | Quarantine | Custom Signatures | PCAP | |
| | | Aba Profiles | | | | |

Surgirá a tela "Profiles" do Intrusion Prevention, conforme demonstrado pela imagem abaixo:

| | | | 1 |
|--------------------|--------------------------|-------------------------------|------------------------|
| Bacigha | 34 | - | - 10 |
| Trianite Paraphine | head | 1.1 | 00.00 |
| | Tractation Tractation | Teactaine Type Traces Type | Rectifier Spec Frances |

Intrusion Prevention - Profiles

Esta sessão irá abordar como cadastrar, editar e remover os perfis de Intrusion Prevention;

A seguir, analisaremos as funções localizadas no topo deste painel.

Intrusion Prevention - Aba Profiles - Menu de Ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



Intrusion Prevention - Menu de Ações

O menu é composto das seguintes opções:

- Create Profile;
- Delete Profile.

A seguir cada opção do menu de ações será detalhada.

Intrusion Prevention - Aba Profiles - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de Intrusion Prevention. Para acessar, clique no menu de ações [

1. Clique na opção "Create Profile";



].

Intrusion Prevention - Create Profile

2. A tela "Add Profile" será exibida. Preencha-a com os seguintes dados:

| Sertem | Constant | |
|--------|---|---|
| mustr | | |
| Clart | * Kame | |
| Server | Description | |
| | Venion | |
| | | |
| | Mode | |
| | · Processes | Туре |
| | 1 | 🕛 Firesrall 🔘 Transparent 🔘 Pansive 💟 Packet Logger |
| | Øeske | 0ev/ce |
| | | |
| | 0evice | |
| | Prefixo do arquivo | Hasimum file size (M2) |
| | | |
| | Defailtions | |
| | Enable client recommended rules Enable server recommended rules Inspect all ports | |

Intrusion Prevention - Create Profile

Aba Settings

Nesta aba é possível efetuar as configurações gerais, definições e o modo de atuação do Intrusion Prevention.

General

Em "General" temos as seguintes caixas de texto:

| | х <i>г</i> |
|--------------------|------------|
| | |
| Version | |
| Block malwares | 1 |
| Description | |
| Malmore Prevention | |
| • Narse | |
| uo kan | |
| Especial | |

- Name: Definir um nome para o perfil. Ex.: Malware Prevention;
- Description: Definir uma descrição para o perfil. Ex.: Block Malwares;
- Version: Determina a versão na qual o profile foi criado.

Mode

Em "Mode" são determinadas as aplicações cujo acesso será permitido ou negado:

| * Processes | Туре | |
|---------------|---|--------|
| 1 | ● Firewall ○ Transparent ○ Passive ○ Packet | Logger |
| Device | Device | |
| | ×] | Y |
| Device | | |
| | | \sim |
| * File prefix | Maximum file size (MB) | |
| | 5 | |

Intrusion Prevention - Mode

• Processes: Selecione o número de processos simultâneos para carregamento do perfil. Cada processo refere-se a um thread. Recomendamos que este valor seja "menor ou Igual" ao número de núcleos de processamento do seu Appliance. O preenchimento deste campo é obrigatório.

- Type: Selecione o Modo de operação do IPS. Os tipos disponíveis são: Firewall, Transparent e Passive;
 - · Firewall: Este modo funciona como um sistema de "Proteção orientada a Ativos de Rede" através das "Políticas de segurança" é possível estabelecer regras de proteção contra intrusos "perfis" orientados para cada "serviço de rede", "protocolo" ou mesmo "ativo de rede" direcionando o tráfego do pacote para análise pelo IPS;
 - Transparent: Este modo funciona como sniffer aplicado diretamente na interface de rede. Utiliza-se de um sistema de "captura. filtragem e análise de pacotes em alta velocidade". Em termos simples, é um agente de aceleração que permite que os pacotes em uma única interface sejam segmentados em vários threads/núcleos, permitindo um processamento de pacotes mais eficiente. Os pacotes são inspecionados em um nível muito mais baixo do que os sniffer ou motores de pacotes tradicionais, reduzindo assim o custo dos recursos e aumentando a eficiência do seu dispositivo;

O modo transparente é suportado somente por "Appliances físicos".

- Passive: Este modo funciona monitorando a rede e gerando log "registros" de todos os pacotes identificados na sua base de assinaturas, referente as ameaças e ataques, não tomando nenhuma ação sobre o pacote malicioso. Opera no modo "bypass".
- · Packet Logger: Este modo permite a análise e captura do fluxo de pacotes de dados, e o registro destes pacotes em um relatório.
- Device (Flow): A configuração deste item somente é necessária no modo "Transparente". Seleciona o fluxo alvo de pacotes. O fluxo é determinado pelo dispositivo de entrada dos pacotes. Ex.: Eth2 : Eth3;
- Device (Flow): Esta opção também fica disponível apenas no modo "Transparente" e permite a seleção de um segundo dispositivo de entrada de pacotes.
- Device (Interface): A configuração deste item somente é necessária no modo "Passivo". Selecione o fluxo de pacotes de uma interface de rede. Ex .: Eth2.
- File Prefix: Prefixo do tipo de arquivo de saída.
- Maximum File Size (MB): Tamanho do arquivo de saída, contendo os dados do fluxo de pacotes.

Nos campos Flow e Interface, as interfaces de rede devem estar "habilitadas" e sem endereco IP. Conforme demonstrado abaixo: Interlase Address Galerer Type 200 Theirs Ø-stat. 172.01382.220/04 Physical LAB 0.002 Rhytical 0.00 Photos 0 X 8 Network Interfaces - Example Para mais informações a respeito de como configurar as interfaces, cheque esta página. Além disso, para evitar fragmentação, poderá ser necessário aumentar os valores do MTU das interfaces. Para mais informações a respeito, consulte esta página.

Definitions

Em "Definitions" são determinadas as aplicações cujo acesso será permitido ou negado:

| efinitions | | |
|---------------------------------|--|--|
| Enable client recommended rules | | |
| Enable server recommended rules | | |

Intrusion Prevention - Definitions

Enable client recommended rules 🔁 : A ativação desta opção habilita a exibição das regras ATP padrão da Blockbit. Estas regras serão exibidas aba client,
- Enable server recommended rules Z: A ativação desta opção habilita a exibição das regras IPS padrão da Blockbit. Estar regras serão exibidas na aba server,
- Inspect all ports i Habilita a inspeção independente da porta que o aplicativo esteja rodando.

A ativação da opção Inspect all Ports limita o processo do seu tráfico na rede.

Aba Client

Ao habilitar a opção Enable client recommended rules Za na aba Settings, a aba Client irá exibir as assinaturas conforme demonstrado abaixo:

| Sattings | Status | | Quatentine | filek | Catagory | Harrise / SAD | |
|----------|--------|------|------------|--------|-----------|---|-----------|
| | 11 | | Disbled - | 41 | 1.8 | | G. |
| Clerk | Status | Heck | Quarantine | fisk | Calegory | Natur | 581 |
| bion. | | CDF | Unided - | 10m | actives. | ACTIVEX 2X ApplicationServer TurSyste+ | (20)442 |
| | 0 | CB | guugal - | [line] | actives. | ACTIVES 28 Application server two system | amete |
| | | 00 | Statist - | Low | Activity: | ACTIVEX 20 ApplicationServer RosSpate | 32940 |
| | 020 | CB | minet - | (Less) | áctivax. | ACTIVES 25 Apatitations and TooSystell | antique |
| | 00 | CD | Quelet - | Low. | actives | ACTIVEX 28 Glant for RDP ClantSystem | 30940 |
| | 0 | 08 | Durier - | Low | acties | ACTIVEX 2X Client flux ROP ClientSystem | (AND |
| | 00 | CID | Ratified - | Low | actions | ACTIVEX 4000H VatDecodiar XMOyl Class | 3017011 |
| | 0.0 | CB | Build - | Lon | actives. | ACTIVEX ACTIVEX Incredition/IMMenu6- | 3007000 |
| | 00 | CD | Dootled = | Line . | actives | ACTIVEX ACTIVES Pussible Microsoft IE (_ | 3015211 |
| | (10) | 100 | Water - | Lon | actives | ACTIVEX ACTIVES Possible Microsoft (E | - 3090034 |

Intrusion Prevention - Client

As assinaturas estão divididas da seguinte forma:

- Status: Define o estado atual da assinatura, as opções são:
 - ∘ *All*;
 - Enabled;
 - Disabled;
 - Blocked;
 - Unblocked.
- Quarantine: É possível habilitar ou desabilitar a opção de quarentena informando se será validado por IP de origem ou destino. Ao habilitar a opção de quarentena automaticamente o sistema irá habilitar a assinatura com o status de block. Com isso, todo tráfego que dê match na assinatura o sistema irá dinamicamente inserir o endereço na quarentena dessa forma, mantendo bloqueado conforme o tempo que foi configurado para quarentena;
- - Medium;
 - ° High.
- Category: Define os grupos de assinaturas que possui a mesma finalidade;
- Name / SID: Este campo permite determinar o nome da assinatura no sistema ou o identificador único da assinatura (SID) ou código CVE. Também é possível pesquisar as assinaturas em quarentena, habilitadas, desabilitadas, entre outros;

• Botão Action []: É possível manipular assinaturas que foram filtradas, conforme as seguintes opções:

| | ۹ 🗸 |
|---|-------------|
| ĺ | Signatures |
| ł | Enable |
| 1 | Disable |
| 2 | Block |
| 1 | Unblock |
| 5 | Quarantine |
| ł | Disable |
| | Source |
| | Destination |
| | |

Intrusion Prevention - Ações

| Para alterar a ação de determinada assinatura da base, clique no [] de "Status" e "Bloqueio" da respectiva assinatura que deseja "H abilitar/Desabilitar". |
|--|
| |
| Ao ativar o checkbox Enable client recommended rules ou Enable server recommended rules na aba <i>Definitions</i> , alguns <i>SID</i> serão destacados, o <i>SID</i> em azul é o padrão recomendado pela Blockbit (por exemplo, ao editar algum deles, ele passará a ser cinza). |
| Vide o exemplo abaixo, onde terceiro e quarto SID estão destacados: |
| |
| |
| |
| |
| |
| |
| |
| |

| Status | Slock | Quarantine | Nisk | Category | Nation | 580 |
|--------|-------|-------------|---------|----------------|-----------------------------------|--------|
| 0 | CD | Otyobled | Tanw. | browser-chiome | BROWSER CHROME Sougle Chrome Cr | 40076 |
| 3 | 0 | Ceatled | tow | browser-chrome | BROWSER-CHROWE Google Chrome Cr | 46977 |
| 0 | | Duabled 👘 👳 | - izwe | browser-chrome | BROWSER-CHROME Google Chrome Fil- | 40,005 |
| 0 | | 0eabled = | - LOW- | browser-chrome | BROWSER-CHROME Google Chrome Ril | 49361 |
| 0 | 0 | Duebled - | Low | browser-chrome | BROWSER-CHROME Google Chrome nil | 2144 |
| œ | 0 | Otselfed 🔍 | Low | browser-chrome | BROWSER-CHROME Google Chrome Film | 21/47 |
| 0 | | Otiabled 🔍 | LOW | browser-chiome | BROWSER-CHROME Google Chrome Bo | 16750 |
| 3 | | Ctublet 🗸 | Westure | browser-chrome | BROWSER-CHROWE Google Chrome FT | 18785 |
| 00 | CB | Oisabled V | Low | browser-chiome | BROWSER CHROME Google Chrome GU | 16667 |
| 0 | CD | Ghabled | 1499 | browser-chrome | BROWSER-CHROME Google Chrome CU | 10008 |

O sistema possui um painel de pesquisa onde o mesmo poderá realizar buscas de acordo com as informações inseridas nos campos anteriormente citados, para tanto, clique em [Q].

Aba Server

Ao habilitar a opção Enable server recommended rules Z na aba Settings, a aba Server irá exibir as assinaturas IPS conforme demonstrado abaixo:

| All | | Quarantine Itaibiid | Risk 41 | Category U | Maine/SiD | a v |
|--------|-------|---|------------|------------------|---------------------------------------|-------------|
| Status | Block | Quarantine | Risk | Category | Name | 50 |
| 00 | 00 | tisailet = | 1.04 | attack_response | XTTACK_RESPONSE 4017RG Peril DDoS | 2024971 |
| CID | 0 | Deatlet - | Better | attack_response | ATTACK_RESPONSE W. BANIA id.php de | 2001858 |
| CD. | 3 | DisaVet = | Tow: | attack_response | ATTACK_RESPONSE Backdoor reDuh fit_ | 2011667 |
| CB | 00 | Datified | Matter | attack_response | ATTACK_RESPONSE 099 Modified physic | 2001654 |
| CIP. | 00 | Daalifeet ··································· | Netter | attack_response | ATTACK_RESPONSE clitical physical | 2007652 |
| CID. | 09 | DisaNet = | Hedrory | attack_response | ATTACK_RESPONSE Osco TciShell TFT | 3009245 |
| CB | 0 | Daallar - | Martin | attack_responde | ATTACK_RESPONSE Cisco TelBholl TPT- | 2008244 |
| CID | 3 | Onables = | Low | attack_response | AT VACK_RESPONSE FTP CWD to windo | 2008354 |
| OD | 00 | Disatled - | High | attack_response. | ATTACK_RESPONSE FTP imacoessible dk., | 2006540 |
| CIP | 0 | Daallar V | rear. | attack_response | ATTACK_RESPONSE FTP inaccessible di_ | 2006488 |
| | | | | tulal nems | 24029 < 1 2 5 4 5 2403 | - 10/mage - |

Intrusion Prevention - Server

Assim como na aba Client, as assinaturas estão divididas da seguinte forma:

- Status: Define o estado atual da assinatura, as opções são:

 - Enabled;
 - Disabled;
 - Blocked;
 - Unblocked.
- Quarantine: É possível habilitar ou desabilitar a opção de quarentena informando se será validado por IP de origem ou destino. Ao habilitar a opção de quarentena automaticamente o sistema irá habilitar a assinatura com o status de block com isso todo tráfego que dê match na assinatura o sistema irá dinamicamente inserir o endereço na quarentena dessa forma mantendo bloqueado conforme o tempo que foi configurado para quarentena;
- Risk/severity: Que determina qual o risco da assinatura baseado na criticidade e complexidade do ataque que pode ser dos tipos: • Low;
 - Medium;
 - High.
- Category: Define os grupos de assinaturas que possui a mesma finalidade;
- Name / SID: Este campo permite determinar o nome da assinatura no sistema ou o identificador único da assinatura (SID);

| ~ | |
|---|--|
| × | |
| | |

• Botão Action [_____]: É possível manipular assinaturas que foram filtradas, conforme as seguintes opções:



Intrusion Prevention - Ações

| Para <i>alterar</i> a ação de determinada assinatura da base, clique no [] de "Status" e "Bloqueio" da respectiva assinatura que deseja "H abilitar/Desabilitar". |
|--|
| |
| ~ |

Ao ativar o checkbox Enable client recommended rules ou Enable server recommended rules na aba Definitions, alguns SID serão destacados, o SID em azul é o padrão recomendado pela Blockbit (por exemplo, ao editar algum deles, ele passará a ser cinza).

Vide o exemplo abaixo, onde terceiro e quarto SID estão destacados:

| Status | Slock | Quarantine | tlisk | Category | Native | 580 |
|--------|-------|-------------|--------|----------------|-----------------------------------|--------|
| 0 | 0 | Otasbled | 10m | browser-chiome | BROWSER CHROME Sougle Chrome Cr | 90078 |
| œ | œ | Ceased | (low) | browser-chrome | BROWSER-CHROWE Google Chrome Cr | 86907 |
| 0 | | Dtarbleri 🤍 | inw. | browser-chrome | BROWSER-CHROME Google Chrome Fil- | 40,005 |
| 0 | | 0eabled - | - LOW- | browser-chrome | BROWSER-CHROME Google Chrome Ril | 49361 |
| 0 | | Disabled - | Low | browser-chrome | BROWSER-CHINOME Google Chrome nil | 21440 |
| œ | | Disellar 👻 | Unw | browser-chrome | BROWSER-CHROME Google Chrome Film | 21,147 |
| 0 | | Otiabled 🔍 | LOW | browser-chiome | BROWSER-CHROME Google Chrome Bo | 19730 |
| 0 | | Dturblet V | Nether | browser-chrome | BROWSER-CHROWE Google Chrome FT | 18785 |
| 00 | CB | 0isabled 🔍 | LOW | browser-chiome | BROWSER CHROME Google Chrome GU | 16667 |
| 0 | CD | Ghabled | Lane . | browser-chrome | BNOWSER-CHRONE Google Chrome CU | 10008 |

O sistema possui um painel de pesquisa onde o mesmo poderá realizar buscas de acordo com as informações inseridas nos campos anteriormente citados, para tanto, clique em [Q].

Botão Restore

Caso à qualquer momento queira restaurar o perfil e as configurações padrão da Blockbit, clique em *Restore*[______], a seguinte janela será exibida.





As configurações foram feitas com sucesso.

Intrusion Prevention - Aba Profiles - Delete Profile

Através do botão "Delete Profile" é possível deletar os Profiles selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul [2]. Ex.: *Test*:

| 1 | Analikites between larger | Interfaces the | | | | | |
|---|---------------------------|----------------|---------|---------|---|----|---|
| - | | | | | 1 | | 1 |
| | - | Too rijetov | 394 | Process | | | ę |
| | Marga Providen | Sector Sector | And and | | • | i, | 1 |
| | fac: | | · | 181 | | 1 | ì |

Intrusion Prevention - Seleção dos Profiles para deletar

| 2. Entre no menu de ações [| "Delete I | Profile". | | |
|-----------------------------|-----------|--------------|------------|---------|
| | | Q | • | |
| | | Create Pr | rofile | |
| | | Delete Pr | ofile | |
| | Intrusic | n Prevention | – Delete I | Profile |

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os Profiles selecionados:

| Are you sure? | × |
|---|---------------|
| Are you sure you want to delete: Test ? | |
| | Cancel Delete |

Intrusion Prevention - Mensagem se deseja deletar os profiles

| | Cancel | | Delete | |
|--|--------|--|--------|----|
| Caso desejar cancelar clique no botão Cancel | |]. Para concluir, clique no botão Delete | |]. |



Após realizar esses procedimentos, os profiles terão sido deletados com sucesso.

Intrusion Prevention - Aba Profiles - Colunas

A seguir explicaremos cada coluna da aba Intrusion Prevention:

| | | 121722341 | | | | |
|------|-----------------------------|-----------------|-------|---------|-----|-----|
| -144 | Strangerick Property States | Description For | | | | |
| - | | | | | | 1 |
| | them. | Too rijetor | 399.0 | Process | | - |
| | Statute Providence | Real Industry | - | | • | * * |
| | 14 | | | | • | 1.8 |
| | | | | -11 | 1.1 | - |

Profiles - Intrusion Prevention

A seguir explicaremos cada coluna:

- Caixa de Seleção[]: Seleciona o profile;
- Name: Apresenta o nome do profile cadastrado;
- **Description:** Apresenta a descrição do *profile* cadastrado;
- Type: Determina que tipo de prevenção será aplicada. As opções disponíveis são Firewall, Transparent e Passive;
- Processes: Determina que tipo de processos simultâneos para carregamento do perfil. Cada processo refere-se a um thread. Recomendamos que este valor seja " menor ou Igual" ao número de núcleos de processamento do seu *Appliance*;
 Actions: A coluna "*Actions*" é composta por vários botões:

• Botão Edit [

• Botão Delete [

Intrusion Prevention - Aba Quarantine

A aba Quarantine permite gerenciar todos os endereços IP (tanto de origem como destino) bloqueados e visualizar a configuração das assinaturas especificando a sua inserção na quarentena.

Os endereços IP contidos na Quarentena pelo período configurado são bloqueado antes mesmo de ser analisados por alguma assinatura de perfil do Intru sion Prevention.

Através das opções do Menu de Ações, é possível adicionar estes IPs à Allowed Addresses List, Blocked Addresses List, removê-los ou determinar o tempo limite para que estes sejam excluídos.

Para efetuar as configurações, clique em "Quarantine".

| Profiles | Allowed Addresses | Blocked Addresses | Quarantine | Custom Signatures | PCAP |
|----------------|-------------------|-------------------|------------|-------------------|------|
| Aba Quarantine | | | | | |

Surgirá a tela "Quarantine" do Intrusion Prevention, conforme demonstrado pela imagem abaixo:

| Introduct Prevention | • |
|----------------------|---|
| | |

Intrusion Prevention – Quarantine.

Uma vez na quarentena todo o pacote dessa origem ou destino serão bloqueados antes mesmo de chegar em uma assinatura específica, o tempo de permanência da quarentena de um determinado *IP* é configurável.

A seguir analisaremos as opções do menu de ações e a função das colunas da aba Quarantine.

Quarantine - Menu de Ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



Intrusion Prevention - Quarantine - Menu de Ações

O menu é composto das seguintes opções:

- Timeout;
- Move to Allowed Addresses List;
- Move to Blocked Addresses List;
- Remove.

A seguir cada opção do menu de ações será detalhada.

Quarantine - Menu de Ações - Timeout

O tempo de permanência da quarentena de um determinado IP é configurável através desta opção. Para acessar, clique no menu de ações [

1. Clique na opção "Timeout";



].

Intrusion Prevention - Quarantine - Menu de Ações - Timeout

| Timeout | | × |
|---------|---------|--------|
| * Time | | |
| 60 | Minutes | \sim |
| | | |
| | Cancel | Save |

Neste painel poderá ser configurado o tempo de *timeout* para remover o endereço na quarentena, por *default* o sistema vai configurado com o tempo de 60 minutos. No primeiro campo, é possível determinar o tempo, já na caixa de seleção é possível definir se o tempo será em minutos ou horas.

| Por fim, caso deseje cancelar clique no botão [| Cancel |]. Para concluir a edição das aplicações clique no botão [| Save |]. |
|---|--------|--|------|----|
|---|--------|--|------|----|

2. A tela abaixo será exibida:

Quarantine - Menu de Ações - Move to Allowed Addresses List

Através desta opção é possível mover um IP da quarentena para a Allowed Addresses list. Para tanto, siga os seguintes passos:

1. Selecione qual(is) IP(s) deseja mover. Para selecionar, basta clicar com o mouse no checkbox que fica localizado ao lado do IP. Nos itens selecionados o checkbox mudará da cor cinza para azul [2]:

| ntrusio | on Prevention | |
|----------|--|--------------|
| Voltie. | Almost Althouse. Bioloci Addresses. Quarentine Custors Spratures. PCAP | |
| £ record | s | (a) |
| | an a | Action |
| 53 | 192.108.75.15 | a a a |
| | 192.168.75.36 | |
| | 192.168.75.28 | <i>₽</i> = 0 |
| | 192.168.75.21 | |
| | 182.168.75.21 | 2 A 8 |
| | 192.168.75.24 | + + C |
| | | < 1 s0/gage |

Quarantine - Seleção dos IPs para mover para a Allowed Addresses

2. Clique na opção "Move to Allowed Addresses list";



Intrusion Prevention - Quarantine - Menu de Ações - Move to Allowed Addresses list

3. Após confirmar a mensagem de notificação questionando se deseja realmente mover os *itens* selecionados, o procedimento terá sido efetuado com sucesso.

Quarantine - Menu de Ações - Move to Blocked Addresses List

Através desta opção é possível mover um IP da quarentena para a Blocked Addresses list. Para tanto, siga os seguintes passos:

1. Selecione qual(is) *IP*(s) deseja mover. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *IP*. Nos *itens* selecionados o *checkbox* mudará da cor cinza para azul [2]:

| ntrusio | on Prevention | | |
|----------|--|------------|------|
| Profile. | Allowed Allibration Biochest Addresses. Quarteries Custom Signatures, PCAF | | |
| 4 record | | 4 | ŀ |
| | p q | h | tiot |
| - | 192.198.75.35 | e 9 | 8 |
| | 192.168.75.36 | | n |
| | 192.168.75.34 | - A | Û |
| | 192,198,75,21 | 1 B | C |
| | 102.168.75.21 | 10 A | |
| | 192.168.75.23 | | 8 |
| | | < 1 a 2077 | aje |

Quarantine - Seleção dos IPs para mover para a Blocked Addresses List

2. Clique na opção "Move to Blocked Addresses List";



Intrusion Prevention - Quarantine - Menu de Ações - Move to Blocked list

3. Após confirmar a mensagem de notificação questionando se deseja realmente mover os *itens* selecionados, o procedimento terá sido efetuado com sucesso.

Quarantine - Menu de Ações - Remove

Através do botão "Remove" é possível remover os itens selecionados. Para remover pelo Menu de ações, siga os seguintes passos:

1. Selecione qual(is) item(s) deseja remover. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *IP*. Nos itens selecionados o *checkbox* mudará da cor cinza para azul [

| records | 2 | () |
|---------|---------------|----------|
| | ι¢. | Actio |
| - | 192.168.75.15 | (a) (a) |
| | 192.168.75.38 | (#*) # (|
| | 192.188.75.31 | |
| | 102.168.75.21 | a" a (|
| | 102 168.75.71 | |
| | 192.168.75.23 | |



| 2. Entre no menu de ações [] e clique na opção " <i>Remove</i> ". | | | |
|---|----------------------|--|--|
| | ۹ 🗸 | | |
| | Timeout | | |
| | Move to Allowed List | | |
| | Move to Blocked List | | |
| | Remove | | |

Quarantine - Menu de Ações - Remove

3. Após confirmar a mensagem de notificação questionando se deseja realmente deletar os *itens* selecionados, a remoção terá sido efetuada com sucesso.

Quarantine - Colunas

A seguir explicaremos cada coluna da aba Quarantine:

| | server and an and a server of the server of | | | |
|--------|---|--------------|------|-----|
| record | | ι. E | Į | |
| | p. | Ad | ctio | ar |
| | 192.188.75.35 | e a | 1 | đ |
| | 192.168.75.76 | | 1 | 1 |
| | 192.168.75.20 | <i>₽</i> . ₽ | 113 | 8 |
| | 192168/521 | | | 8 |
| | 192 162 75.12 | £ 4 | | |
| | 192.168.75.23 | w 4 | 10 | iii |

Intrusion Prevention – Quarantine

A seguir explicaremos cada coluna:

- Caixa de Seleção]: Seleciona o item;
 Actions: A coluna "Actions" é composta pelos botões:
 - [] Ao clicar sobre o botão o sistema irá adicionar o endereço *IP* na *Allowed Addresses Lis*, é o equivalente à opção *Move to Allowed Addresses List* do menu de ações;
 - I Ao clicar sobre o botão o sistema irá adicionar o endereço IP na Blockes Addresses List, é o equivalente à opção Move to Blocked Addresses List do menu de ações;
 - [] Ao clicar sobre o botão o sistema irá remover o endereço da quarentena, é o equivalente à opção Remove do menu de ações.

UTM - Services - Threat Protection

O Threat Protection é um recurso que oferece proteção contra malwares e vírus para garantir a confiabilidade do tráfego de conteúdo dos serviços de Prox y. O recurso conta com proteção de "Downloads/Upload" de arquivos infectados, arquivos "PUA - Potentially Unwanted Application (Aplicações potencialmente indesejadas)", detecção por "Análise heurística" e proteção contra "arquivos com senhas".

Diferente da maioria dos Antimalware e Antivírus concebidos para detectar e prevenir códigos maliciosos em dispositivos de EPS "Endpoint Secure", o Blockbit UTM inclui um recurso interno de Threat Protection que é atualizado automaticamente na busca de novas ameaças que podem infectar sua rede. A primeira camada de proteção em um sistema integrado com acesso web via proxy deve ser a análise de malware e códigos maliciosos para garantir a confiabilidade no tráfego dos arquivos via Proxy.

O Blockbit UTM fornece tecnologias de Antimalware baseados em assinaturas geradas pelo nosso LAB Security Research Team e pela integração com bases de engines de Antivírus de última geração.

Responsável em proteger o servidor e a rede contra ataques de malwares contempla uma tecnologia capaz de promover uma varredura dos arquivos, diretórios, URLs e URIs para identificação e scanner item por item, para detectar a invasão de algum malware no tráfego de Proxy por Política de segurança.

Agrega a tecnologia Sandbox capaz de emular ataques APT (Advanced Persistent Threat) e Zero Day devido a capacidade de emulação de sistemas operacionais, tendo como principal o Microsoft Windows além de arquivos utilizados diariamente, como documentos do Microsoft Office. Com máquinas virtuais de diferentes SOs (Sistemas Operacionais), o Blockbit ATP analisa completamente o comportamento do Malware ou código malicioso sem a necessidade de uma base de assinaturas.

Para acessar e configurar este recurso, clique em "Threat Protection", conforme exemplificado na imagem abaixo.

| 0 8 | Services | ~ |
|------------|----------------------|---|
| » | Firewall | O |
| » | Proxy | Ο |
| » | Web Cache | Ο |
| » | Web Filter | Φ |
| » | Application Control | σ |
| » | Intrusion Prevention | σ |
| » | Threat Protection | Φ |
| » | SD-WAN | Ο |
| » | DHCP | Φ |
| » | DNS | Φ |
| » | DDNS | σ |
| » | VPN IPSEC | Ο |
| » | VPN SSL | σ |

Services - Threat Protection

A tela abaixo será exibida:

| Threat Protection | | |
|----------------------------|-----------------|--------------|
| Anter lating houses (paths | | |
| Deset | | |
| Nare | Invigilar | Attes |
| Teat Printer | These Protector | 2.1 |
| | | (II) (Frank) |

Threat Protection

A tela comporta as seguintes abas:

- Profiles;
 Settings;
 Quarantine;
 Sandbox.

A seguir analisaremos os componentes da aba Threat Protection.

Threat Protection - Aba Profiles

Através desta aba é possível criar perfis de proteção contra ameaças e exploits de possíveis vulnerabilidades da sua rede.

Caso a aba não esteja selecionada, clique em "Profiles".



Surgirá a tela "Profiles" do Threat Protection, conforme demonstrado pela imagem abaixo:

| Thread Protection | | |
|-------------------|-------------------|--------------|
| (meet) | 2.55 | |
| Total Printer | Thisse Protection | 2.8 |
| | | (III) France |

Threat Protection - Profiles

Esta sessão irá abordar como cadastrar, editar e remover os perfis de Threat Protection;

A seguir, analisaremos as funções localizadas no topo deste painel.

Threat Protection - Profiles - Menu de ações

Com os perfis de *Threat Protection*, é possível analisar arquivos para inspeção de *malware* e bloqueio de ameaças. Esta seção irá demostrar como criar perfis que posteriormente, serão instalados nas políticas.

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



Threat Protection - Menu de ações

O menu é composto das seguintes opções:

- Create Profile;
- Delete Profile.

A seguir cada opção do menu de ações será detalhada.

Threat Protection - Profiles - Menu de Ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de Threat Protection. Para acessar, clique no menu de ações [

1. Selecione a opção "Create Profile";



Threat Protection - Create Profile

2. A tela "Threat Protection Profile" será exibida. Neste painel é possível efetuar as configurações gerais do perfil, acionar scan de malwares e bloqueio de ameaças.

| General | | | | |
|-------------------|---------------|----|--------|------|
| * Name | | | | |
| | | | | |
| Description | | | | |
| | | | | - 14 |
| Threat Protection | | | | |
| | | | | |
| Malware Scanning | Threat Blocki | ng | | |
| | | | | |
| | | | | |
| | | | Cancel | Sm |

General

Em "General" temos as seguintes caixas de texto:

| General | |
|----------------------------------|---|
| * Name | |
| Web Navigation Threat Protection | |
| Description | |
| Web Navigation Threat Protection | 4 |

Threat Protection - General

- Name: Definir um nome para o perfil. Ex.: Web Navigation Threat Protection;
- Description: Definir uma descrição para o perfil. Ex.: Web Navigation Threat Protection.

Threat Protection

Em "Threat Protection" é determinado o escaneamento de malware e o bloqueio de ameaças.

| Malware Scanning Threat Blocking | |
|----------------------------------|----|
| | |
| | := |

Threat Protection - Threat Protection

A seguir, analisaremos em detalhes estes dois campos.

Malware Scanning

Para adicionar o *Malware Scanning*, certifique-se que o *checkbox* [] está habilitado, depois clique no botão *list applications* [] o seguinte painel, será exibido:

| Add Mal | ware Scanning | | | × |
|---------|---------------|--|--------|-------|
| All | ~ | | c | ~ |
| | ltem | | | |
| | ActiveX | | | |
| | Compressed | | | |
| | Executables | | | |
| | Images | | | |
| | Javascript | | | |
| | Multimedia | | | |
| | Office | | | |
| | | | | < 1 > |
| | | | | |
| | | | | |
| | | | | |
| | | | Cancel | Save |

Threat Protection - Add Malware Scanning

Marque as caixas de checagem para adicionar malware scanning, conforme demonstrado abaixo:

| Add Mal | ware Scanning | × |
|----------|----------------------------|----------------------|
| All | \sim | ۹ 🗸 |
| | Item | |
| ~ | ActiveX | |
| | Compressed | |
| | Executables | |
| | Images | |
| ~ | Javascript | |
| | Multimedia | |
| | Office | |
| | | < 1 > |
| | | |
| | | |
| | | |
| | | Cancel Save |
| | Threat Protection - Caixas | de checagem marcadas |



| Por fim, caso deseje cancelar clique no botão Cancel [| Cancel |]. Para concluir adição do <i>Malware Scanning</i> das aplicações clique no botão Save [|
|---|--------|---|
| Save]. | | |
| | | |

Threat Blocking

Para adicionar o *Threat Blocking*, certifique-se que o *checkbox* [] está habilitado, depois clique no botão *list applications* [] o seguinte painel, será exibido:

| Add Thr | eat Blocking | | | × |
|---------|--------------|--|--------|-------|
| All | ~ | | | ۹ 🗸 |
| | ltem | | | |
| | Abuse | | | |
| | Anonymizers | | | |
| | Attacks | | | |
| | Malware | | | |
| | Reputation | | | |
| | Spam | | | |
| | | | | < 1 > |
| | | | | |
| | | | Cancel | Save |

Threat Protection - Add Threat Blocking

Marque as caixas de checagem para adicionar o bloqueio de ameaças, conforme demonstrado abaixo:

| Add Thre | eat Blocking | × |
|----------|--------------|-------------|
| All | \vee | ۹ 🗸 |
| | Item | |
| ~ | Abuse | |
| <u>~</u> | Anonymizers | |
| | Attacks | |
| | Malware | |
| | Reputation | |
| <u>~</u> | Spam | |
| | | < 1 > |
| | | |
| | | |
| | | Cancel Save |

Threat Protection - Add Threat Blocking





Threat Protection - Select all e Deselect All

| Por fim, caso deseje cancelar clique no botão Cancel | ancel | . Para concluir adição do Malware Scanning das aplicações clique no botão Save[|
|--|-------|---|
| Save | | |

Após, ter efetuado os processos anteriores, um resumo de todos os itens de proteção de ameaças selecionados serão exibidos em ambos os campos, conforme exemplificado abaixo:

| | Threat Protection | | | |
|--------------------|---|------------|--------------------|----|
| | ✓ Malware Scanning | | ✓ Threat Blocking | |
| | 2 Selected | ≔ | 3 Selected | ∷≡ |
| | Threat Pro | otection - | Itens selecionados | |
| | | | | |
| Para concluir, bas | ta clicar no botão Save] novamente. | | | |

Threat Protection - Profiles - Menu de Ação - Delete Profile

Através do botão "Delete Profile" é possível deletar os Profiles selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul [2]. Ex.: *Test*:

| hreat | Protection | | |
|----------|-----------------------------------|-----------------------------------|---------------|
| native | Setting Quarterin | | |
| 2 recent | | | (a) (a) |
| | Itane | Description | Atlan |
| | Into Navigation Thread Protection | Red; Navigation Thread Protection | / 0 |
| - | tair | Test | e 0 |
| | | | - (T) it sep- |





3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os Profiles selecionados:



Threat Protection - Mensagem se deseja deletar os Profiles



Após realizar esses procedimentos, os profiles terão sido deletados com sucesso.

Threat Protection - Profiles - Colunas

A seguir explicaremos cada coluna da aba Threat Protection:

| Threat Protection | |
|--|--|
| Inter integ house june | |
| (meet) | |
| New Bergin | Anna |
| 😳 TealPlanter TealPlanter | 2.8 |
| | |
| A seguir explicaremos cada coluna: | |
| A seguir explicaremos cada coluna: | |
| Caiva da Salazãa | |
| Caixa de Seleçao[]: Seleciona o profile; Name: Apresenta o nome do profile cadastrado: | |
| Description: Apresenta a descrição do profile cadastrado; | |
| Actions: A coluna "Actions" é composta por vários botões: | |
| AT . | |
| Botão Edit [Permite editar as configurações do profile | e adicionado na opção Create Profile do menu de ações; |

• Botão Delete [

Threat Protection - Aba Settings

Nesta aba definimos as parametrizações dos "tipos de detecção", os "tamanhos de arquivos" para verificação pelo Threat Protection e o "tempo de vida dos arquivos" retidos em quarentena.

Para acessar estes recursos, clique em "Settings".

| Profiles | Settings | Quarantine | Sandbox |
|----------|----------|------------|---------|
| | | | |

Aba Settings

Surgirá a tela "Settings" do Threat Protection, conforme demonstrado pela imagem abaixo:

| | Yanania meneret | | | |
|-------------------|----------------------------|-------------------|---------|--|
| | | | | |
| General | | | | |
| 🖬 Detect poten | tla0y unwanted application | | | |
| 🛃 Block Encryp | Cort Files | | | |
| Enable Hours | stic Analysis | | | |
| Passive Mode | | | | |
| • Filesize maxim | um | • Quarantine site | | |
| 10 | ka – | 1 | 52 ···· | |
| | tine | | | |
| • Days in quarant | une | | | |

Threat Protection - Aba Settings - General

- Detect potentially unwanted application [1]: Para habilitar a detecção de arquivos maliciosos;
- Block encrypted files [2]: Para analisar arquivos bloqueados e realizar o bloqueio;
- Enable heuristic analysis [2]: Para habilitar o recurso de análise heurística melhorando a performance de análise do serviço possibilitando detectar e bloquear comportamento suspeito ou anormal na rede;
- Passive mode []: Para desabilitar o bloqueio do serviço do Threat Protection, nessa opção o sistema só gera relatórios não realizando assim o bloqueio do vírus;
- File Size Maximum : Define o tamanho máximo do arquivo que será analisado pelo Threat Protection;
- Quarantine size: Define o tamanho máximo da quarentena por usuário;
- Days in quarantine: Define os dias que o arquivo ficará em quarentena.

Para concluir este processo, basta clicar no botão Save[____] novamente.





] e aplicar as alterações efetuadas. Para mais

Após salvar, para que as alterações tenham efeito será necessário acessar a **fila de comandos [** informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Após realizar esses procedimentos as configurações terão sido efetuadas com sucesso.

Threat Protection - Aba Quarantine

Na aba Quarantine é possível permite gerenciar todas as ameaças detectadas que estão na quarentena do Blockbit UTM.

A quarentena é populada com entradas graças à ação de políticas que usem dos perfis de *Threat Protection* que em sua configuração estava especificando inserção na quarentena.

| A Para mais informações a respeito de Políticas, acesse esta página. |
|--|
| A Para mais informações a respeito de perfis de <i>Threat Protection</i> , acesse esta página. |
| |

Para acessar este recurso, clique em "Quarantine".

| Profiles | Settings | Quarantine | Sandbox |
|----------|----------|------------|---------|
| | Aba G | Quarantine | |

Surgirá a tela "Quarantine" do Threat Protection, conforme demonstrado pela imagem abaixo:

| Profiles | Settings Quarantie | e: Serribox | | | | | | | | | | |
|----------|---------------------|-------------|----------------------|-------------|------------------|----------------|------------|-----|------|---|----------|----|
| Schedule | d | User | Source | Destination | rile | Status | | Uri | | - | _ | |
| 02/02/ | 2000 - 00/03/2000 | | | | | | | | | 4 | a | ~ |
| | Dato | U: | ser | File | | | Status | | | | clkr | n¢ |
| | 3020-03-03 15:40:00 | | | din. | atps?c=00000000 | ed-Diffia | Cirat | | v. | ø | ۸ | |
| | 2120-03-03 15:39.58 | с. С | | din | aspx7s=00000000 | lem=tastéid= | Cikat | | 5 | ø | \$ | 8 |
| | 2120-03-03 15:39-39 | 3 | iser gibliockbit.com | 2015 | +94-15_10-48-16 | ea01/780a15 | Gean | | 1 | 0 | ۸ | 8 |
| | 3030 03 03 15:3824 | 3 | ne giblackbit, sam | 3010 | 0.04-25_10-11-31 | HREEEEECO | Clean | | ~ | ۵ | ۸ | 0 |
| | 2020-03-03 15:39:10 | | | dow | nloads?client=na | nclient-auto | Not found | | 9 | Ø | \$ | |
| | 2820-03-03 15:37:45 | 3 | iser@blackbit.com | 2019 | +04-25_10-13-31 | 00101394948 | Citan . | | * | 0 | ۵ | 0 |
| | 2120-03-03 13:34:52 | | | din. | nipx?s=00000000 | 0:2-1511015 | Cleate | | 10°. | 0 | ۵ | 0 |
| | 2020-03-03 15:32:18 | | uer@blackbit.com | chro | mesoggestions? | 11 | Not Tourie | | 9 | 0 | # | 8 |
| | 2020-03-03 15:21:13 | 10 | | din | stpc/%=00000000 | 849-1345818 | Olan | | 1 | ø | ۸ | π |
| | 2120-01-01 18:30.24 | | | 200 | 129-01136200,08 | and the second | Cisal | | ~ | 0 | 4 | 0 |

Quarantine - Quarentena Populada

A quarentena possui uma barra de busca que permite o uso de filtros para efetuar uma pesquisa mais efetiva.

| Scheduled | liteer. | Secret | Destination | rite | Status | Ord. | |
|-------------------------------------|---------|--------|-----------------|-------------|--------|------|-----|
| 82/82/2020 - 83/82/2020 | | | | | | | a + |
| | | (| Quarantine - Ba | arra de bus | ca | | |

Esta barra possui os seguintes campos:

- Scheduled: Determina um período para efetuar a busca entre duas datas;
 User: Neste campo, é possível determinar um usuário, para ser usado como filtro na busca;
- Source: Permite determinar um IP de origem, para ser usado como filtro na busca;
- Destination: Permite determinar um IP de destino, para ser usado como filtro na busca;
- File: Neste campo, é possível determinar o nome de um arquivo, para ser usado como filtro na busca; ٠
- Status: Permite selecionar o estado atual do item da quarentena para ser usado como filtro, as opções possíveis são:
 - Allow;
 - ° Deny;
 - ° Clean;
 - Infected;
 - Scanning;
 - Download;
 - Size Limit,
 - Not found.
- Url: Neste campo, é possível determinar um Url, para ser usado como filtro na busca.

| | X | |
|---|----------|--|
| Para efetuar uma busca, basta clicar em |]. | Os resultados são exibidos na tabela abaixo: |

| - | | Unior | . Emma | Destination | ril. | Theter | | - 114 | | | | |
|--------|---------------------|-------|-----------------------|-------------|--------------------|-----------|-----------|-------|----------------|----|-------|----|
| 12/02/ | 2000 - 80/03/2008 | | | | | | | | | | a, | 0 |
| | Dato | | User | File | | | Status | | | .6 | clier | ns |
| | 3025-03-03 13:49:00 | | 16 ¹ | dna | ips?u=00000000.ed | HIMPARE. | Circle | | × | ø | ٨ | |
| | 2120-03-03 15:39.58 | | 1 | dina | spx7s=000000006m | statiágs | Ckał | | 5 | ø | \$ | 1 |
| | 2120-03-03 10:39:39 | | user@blockbic.com | 2019 | 94-15_10-48-10-ea | 014780a15 | Gean | | 10 | 0 | ٨ | 1 |
| | 3830 03 03 15:29:24 | | uner giskockbit, nors | 2010 | 04-25_10-11-11-00 | H12x20H | Clean | | $\omega^{(i)}$ | ٥ | ٨ | 1 |
| | 2020-03-03 15:39:10 | | 12 1 | dawa | iloads1c5ent=navc1 | leot-auto | not found | | 9 | Ø | £ | 1 |
| | 2820-03-03.15:37:45 | | user@tklockbit.com | 2019 | 94-25_10-13-31-03 | td13ad9td | Gean | | 4 | 0 | ۵ | 1 |
| | 2120-03-02 13:34:52 | | 16 ⁻ | dina | nipx?s=00000000000 | -1511015 | Clean | | w. | 0 | ۵ | 1 |
| | 2020-03-03 15:32:10 | | user@blackbit.com | chris | nesoggestors?t=1 | | not found | | 9 | 0 | ± | 1 |
| | 2020-03-03 15:31:13 | | E. | din.a | sa0000000-r"xqx | H1345818 | Gean | | 4 | ø | ۸ | 1 |
| | 2020-05-05 18:30:24 | | 18 C | 2012 | NO-EVISEDOJOROM | quittenis | Chat | | ~ | 0 | 4 | 1 |

Quarantine - Resultado de uma busca

A seguir, vamos analisar cada componente desta tabela:

- Date: Exibe a data de quando o item foi colocado na quarentena;
- User: Exibe o usuário relacionado à esta entrada;
- File: Exibe o arquivo relacionado à esta entrada;
- Status: Determina o estado atual desta estrada, as possibilidades são:
 - Allow;
 - ° Deny;
 - Clean;
 - Infected;
 - Scanning;
 - Download;
 - Size Limit,
 - Not found.
- Actions: Exibe uma quantia de botões úteis:
 - Allow []: Ao clicar neste botão, o download do arquivo será permitido e seu MD5 entra em uma lista de liberados para acessos futuros. Este botão é exibido caso o status seja Infected;
 - Deny []: Ao clicar neste botão, o download do arquivo será negado, e seu MD5 entra em uma lista de liberados para acessos futuros;
 - **Download** A clicar neste botão, será iniciado o *download* do arquivo em questão;
 - *Remove*[]: Ao clicar neste botão, esta entrada será excluída da quarentena.

É importante lembrar que a liberação ou bloqueio do download do arquivo irá refletir na ação de download através do Captive Portal (porta 9803).
Threat Protection - Aba ATP Sandbox

Na aba Sandbox podemos analisar a natureza e classificação de arquivos e programas suspeitos ou maliciosos. Trata-se de um ambiente de testes seguro, que garante a integridade das aplicações do usuário, com testes fechados e classificação de ameaças abrangente.

Conforme o malware se torna mais sofisticado, monitorar o comportamento suspeito para detectar malware se torna cada vez mais difícil. Muitas ameaças nos últimos anos empregaram técnicas avançadas de ofuscação que podem evitar a detecção de produtos de segurança de rede e endpoint.

O Módulo de Threat Protection do Blockbit, tem a seguinte fluxo de verificação de samples e arquivos suspeitos:

1 - Threat Protection do Blockbit gera um Hash do arquivo suspeito;

2 - Threat Protection do Blockbit verifica o Hash gerado do arquivo se encontra na blocked list ou allowed list;

3 - Threat Protection do Blockbit verifica se o Hash gerado do arquivo foi verificado e classificado pelo Blockbit Labs, executando a ação de bloqueio ou liberação;

4 - Threat Protection do Blockbit analisa o arquivo em busca de ameaças utilizando o método tradicional (match com assinaturas de antimalware conhecidas);

5 - Se o arquivo não der match em alguma assinatura conhecida ou na base de hash alimentada pelo Blockbit labs, mas apresentar um comportamento suspeito ele é enviado para análise em Sandbox.

Uma Sandbox é um ambiente de teste isolado que permite aos usuários executar programas ou abrir arquivos sem afetar o aplicativo, sistema ou plataforma em que são executados.

Sandboxes são usados para executar códigos maliciosos com segurança para evitar danos ao dispositivo host, à rede ou a outros dispositivos conectados. Usar uma sandbox para detectar malware oferece uma camada adicional de proteção contra ameaças de segurança, como ataques furtivos e explorações que usam vulnerabilidades de dia zero.

Threat Protection > Sandbox

| Analysis | | | | | | Sea | rch tor | | | 1 |
|------------------|--------------------------------------|---------------------------------|--------------------|----------|----------------|---------|----------|---|-------|----|
| | | | | | | | | < | 1 | > |
| Submission Date | First Submission | MD5SUM | Filename or URL | Status | Classification | AV Scan | Zero Day | , | ictio | ns |
| 2018-07-19 15:58 | 2018-07-19 15:58 | c1f1ff88c54564fcd24eb7c3562cc5_ | Abrraxas | Reported | Maticious | 18/43 | NO | 0 | 0 | 1 |
| 2018-07-19 15:52 | 2018-07-19 15:52 | 4c7bbd181cb79865e144a3a7b59aca_ | VIRII.tar | Reported | Clean | 0/0 | NO | 0 | c | 18 |
| 2018-07-19 15:51 | 2018-07-19 15:51 | ea039a854d20d7734c5add48f1a51c_ | hinvoice_2 | Reported | Malicious | 61/67 | NO | 0 | 0 | (0 |
| 2018-07-19 15:36 | 2017-08-14 19:45 | b32ca307a45d3c9deb2d5a259db803_ | WannaCRY | Reported | Maticious | (51/62) | NO | 0 | 0 | 9 |
| 2018-07-19 15:26 | 2018-07-19 15:26 | c9b1c515fb350e7f6b35fbf465e95c_ | WormAca | Reported | Suspicious | 0/0 | NO | 0 | c | |
| 2018-07-19 15:25 | 2018-07-19 15:25 | 868c11d9efe0a44900d1db135d8995 | exercicio2 | Reported | Malicious | (1157) | NO | 0 | 0 | 1 |
| 2018-07-19 15:25 | 2018-07-19 15:25 | 42574a17a46f47b61074e83de42cd5 | exercicio 1 | Reported | Malicious | 3756 | NO | 0 | 0 | 10 |

Análise Sandbox



Classificação Sandbox

UTM - Services - SD-WAN

O Blockbit UTM contempla múltiplos *links* de internet, sendo capaz de segmentar e priorizar o tráfego através das interfaces de rede de acordo com os dados obtidos pelo monitoramento de diversos indicadores de performance, permitindo o roteamento do tráfego através das interfaces configuradas pelo melhor caminho disponível, este benefício é obtido através do *SD-WAN*.

A sigla SD-WAN significa Software-Defined Networking em Wide Area Network, trata-se de um meio de efetuar a distribuição dinâmica do tráfego, monitoramento e tomada de decisão de acordo com a melhor performance disponível. Graças a desassociação dos métodos de controle do hardware de rede, o SD-WAN viabiliza uma visão holística dos aplicativos em uso, o que possibilita o fornecimento de balanceamento de carga inteligente, facilitando a tomada de decisões durante o processo de criação de políticas SD-WAN.

A função de monitoramento do SD-WAN é permitir a supervisão de dados específicos da WAN, viabilizando o melhor caminho de rede de acordo com os fatores determinados pelo administrador, isso permite direcionar os recursos mais adequados conforme regras e políticas pré-determinadas ou com base no perfil específico dos usuários. O monitoramento efetua acompanhamento dos seguintes fatores:

- Latência;
- Jitter,
- Perda de Pacotes;
- Consumo de Banda.

Utilizando-se dos dados obtidos através deste monitoramento, o *SD-WAN* oferece a função de "Tolerância a falhas", possuindo um recurso de redundância (*Failover*) que permite a utilização do melhor *link* disponível no caso de alguma irregularidade no *link* primário. Além disso, o *SD-WAN* monito ra o *status* da placa de rede, caso ela seja detectada como *off* (por exemplo, em um evento de desconexão do cabo de rede), ele automaticamente marcará o *link* afetado como *down* sem esperar o tempo dos monitoramentos e trocará imediatamente para o melhor *link*.

O controlador de falhas de *link* é capaz de aplicar testes de disponibilidade em tempo real, possibilitando a realização de *Load Balance* definido por porcentagem, o que possibilita a divisão da carga entre os *links*, o que representa uma minimização no tempo de resposta, garantindo a qualidade do uso dos *links*. Por fim, o sistema contempla também os tipos *Spillover* e *Dynamic Selection*.

O SD-WAN contempla 4 modos de operação, sendo eles:

- Failover,
- Load balance;
- Spillover;
- Dynamic Selection.

Persistência de Link

A persistência de link está disponível apenas nas opções Load Balance, Spillover e Dynamic Selection.

O objetivo principal da função "persistência de *link*" é impedir a queda das conexões em aplicações que se utilizam de tráfego criptografado SSL. Com a caixa de seleção habilitada, cada endereço *IP* de origem utilizará um único *link* do perfil especificado na política que a conexão foi liberada, esta condição só é alterada após o tempo de ociosidade definido no campo "*Persistence timeout* 1-1440 *minutes*", ou ainda caso seja detectada alguma irregularidade no sindicadores de performance, apontando a uma instabilidade no *link*.

De forma resumida, cada endereço *IP* de origem utilizará apenas um *link* definido no perfil, essa configuração faz com que os protocolos de criptografia S SL não sejam mais afetados pelo balanceamento no uso de múltiplos *links* de conexão.

Para ativação da persistência de conexão, deve-se habilitar a caixa de checagem "Persistent connection" que estará disponível no painel de perfil do SD-WAN em qualquer modo de operação onde ocorra o balanceamento dinâmico (Failover não executa balanceamento).

| ~ | Persistence timeout 1-1440 min |
|---|--------------------------------|
| 3 | 0 |
| | |

Persistência de conexão

Ao habilitar a caixa de checagem no painel de perfil do SD-WAN, o administrador determina se a conexão por um único endereço de origem será persistente.

Tendo esta opção habilitada, é possível determinar um limite temporal para a atuação desse recurso, sendo que o tempo padrão é de 30 minutos após a última atividade.

Failback

O recurso Failback está disponível para todos os tipos de SD-WAN, ele é um processo que possibilita a restauração do serviço de forma que ele retorne ao seu estado funcional caso a conexão fique instável ou inoperante.

Caso um *link* pare de responder o *failback* é ativado, ele atua efetuando testes de conectividade, levando em consideração o valor do contador determinado pelo usuário, que determina o número de sucessos em sequência necessário para definir caso este *link* inativo voltou a se tornar estável. Assim sendo, o roteamento dos pacotes só será restaurado caso os testes de verificação de *failback* cheguem no limite definido pelo usuário. Caso no meio dos testes seja detectada uma nova falha na conexão com o *link*, o contador de *failback* é reiniciado.



<u>
</u>

Caso o perfil de SD-WAN tenha sido criado antes da implementação deste recurso, o valor será automaticamente 1. Perfis novos, por padrão são criados com valor 5.

Recursos do SD-WAN

- Performance Monitoring: Monitoramento de link baseado em indicadores de performance;
- Dynamic Path Selection: Priorização de tráfego baseado em indicadores de performance;
- Link Failover & Load Balance: Redundância e balanceamento de link baseado em indicadores de performance;
- Traffic Shapping & QoS: Controle de banda e definição de métricas para qualidade e priorização de serviço;
- Traffic Duplication: Duplicação de pacotes em múltiplas interfaces de rede;
- Secure SD-WAN: Controles de roteamento baseado em políticas de segurança.

Atente que graças ao encapsulamento, poderá ser necessário aumentar os valores do MTU das interfaces de modo a evitar fragmentação. Para mais informações a respeito, consulte esta página.

É possível visualizar os logs de debug do SD-WAN através do console CLI, para mais informações, cheque o capítulo a respeito da linha de comandos.

Para acessar a tela do SD-WAN, selecione a opção conforme demonstrado na imagem abaixo:

| 0 8 | Services | ~ |
|------------|----------------------|---|
| » | Firewall | O |
| * | Proxy | Ο |
| * | Web Cache | Ο |
| » | Web Filter | Ø |
| » | Application Control | Ø |
| » | Intrusion Prevention | Ø |
| » | Threat Protection | Ø |
| » | SD-WAN | Ø |
| » | DHCP | Ø |
| » | DNS | Ø |
| » | DDNS | σ |
| » | VPN IPSEC | σ |
| » | VPN SSL | Ø |

Services - SD-WAN

A tela abaixo será exibida:

| 5D-WAN | | | | |
|-------------------|-------------|------------|------------|----------|
| Profilma Destroye | | | | |
| | | | | |
| Bare | Description | Турчі | latertary. | Actronic |
| | | | | |
| | | | | |
| | | be direct. | | |
| | | | | |

SD-WAN – Profiles

A tela SD-WAN é comporta pelas seguintes abas:

- Profiles;
- Settings;

A seguir nos analisaremos cada componente da aba Profiles.

SD-WAN - Aba Profiles

A função de monitoramento do SD-WAN é permitir a supervisão de dados específicos da WAN, viabilizando o melhor caminho de rede de acordo com os fatores determinados pelo administrador, isso permite direcionar os recursos mais adequados conforme regras e políticas pré-determinadas ou com base no perfil específico dos usuários.

Caso a aba não esteja selecionada, clique em "Profiles".



Surgirá a tela a seguir, conforme demonstrado pela imagem abaixo:

| D-WAN | | | | |
|-------------------|-------------|---------|------------|--------|
| Politice Settings | | | | |
| | | | | - 0- |
| Aane | description | Зуре | Interfaces | Action |
| | | | | |
| | | | | |
| | | (miles) | | |
| | | | | |

SD-WAN

Esta sessão irá abordar como

- Cadastrar, editar e remover perfis de SD-WAN;
- Particularidades de cada modo de operação;
- Passo a passo da configuração completa de um SD-WAN.

A seguir, analisaremos as funções localizadas no topo deste painel.

SD-WAN - Profiles - Menu de ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



SD-WAN - Menu de ações

O menu é composto das seguintes opções:

- Create Profile;
- Delete Profile.

A seguir cada opção do menu de ações será detalhada.

SD-WAN - Profiles - Menu de Ações - Create Profile

Através da opção "Create Profile" é possível criar um novo perfil de SD-WAN. Para acessar, clique no Menu de ações [

1. Clique na opção "Create Profile";



].

SD-WAN - Create Profile

2. A tela demonstrada abaixo será exibida:

| Monitor | | | | | | |
|---------|--|--------------|-----------------------|-----------------------|------------------------|--|
| | Description | | | | | |
| | * Туре | • Fail | Fail ratio (1 - 100%) | | | |
| | | Load Balance | ÷. | 70 | | |
| | Monitoring Interval (sec) | | • Failback | | | |
| | 5 | | 5 | | | |
| | Persistence timeout 1-1 | 440 min | | | | |
| | | | | | | |
| | 30 | | | | | |
| | 30 Interfaces | | | | | |
| | 30 Interfaces Device Description | Load Ba | alance | Packet Duplication | Enable | |
| | 30 Interfaces Device Description ETHO - REDE LOCAL | Load Ba | alance | Packet Duplication | Enable | |
| | 30 Interfaces Device Description ETHO - REDE LOCAL ETH1 - | Load Ba | alance | Packet Duplication | Enable Call | |
| | 30 Interfaces Device Description ETH0-REDE LOCAL ETH1- ETH2- | Load Ba | alan ce | Packet Duplication | Enable Cill Cill | |

х

SD-WAN - Profile

Neste painel é possível efetuar todas as configurações referentes à atuação do SD-WAN. A seguir demonstraremos configurando o Load Balance, para mais informações a respeito de tipos de perfil de SD-WAN cheque a página SD-WAN - Tipos de Perfil.

Aba Interfaces

Nesta aba é possível configurar como o SD-WAN irá interagir com as interfaces eth.

| Monitor | * Name | | | | |
|---------|---------------------------|------------------|--------|-----------------------|-------|
| | Description | | | | _ |
| | * Туре | ratio (1 - 100%) | * | | |
| | Load Balance | | | | |
| | Monitoring Interval (sec) | | • Fail | back | |
| | 5 | | 5 | | |
| | Persistence timeout 1-1 | 440 min | | | |
| | 30 | | | | |
| | Interfaces | | | | |
| | Device Description | Load Ba | lance | Packet Duplication | Enabl |
| | ETHO-REDE LOCAL | 291 | | | a |
| | 18 ETH1- | 0% | | | a |
| | 11 ETH2- | 919 | | | a |
| | ETH3- | | | | a |
| | | | | | |

х

SD-WAN - SD-WAN Profile - Aba Interfaces

Painel General

Em "General" temos as seguintes caixas de texto:

| | 14531 | |
|---------|--------------------------------|-------------------------|
| Monitor | * Name | |
| | Description | |
| | | |
| | * Туре | * Fail ratio (1 - 100%) |
| | Load Balance \lor | 70 |
| | * Monitoring Interval (sec) | * Failback |
| | 5 | 5 |
| | Persistence timeout 1-1440 min | |
| | | |

- Name: Definir um nome para o perfil. Ex.: Load Balance;
- Description: Definir uma descrição para o perfil. Ex.: SD-WAN Load Balance;
- Type: Neste campo se define como o SD-WAN irá atuar. A seleção destas opções define quais campos de texto serão exibidos no painel General. É possível selecionar qualquer tipo, porém nesta demonstração usaremos o "Load Balance". Para mais informações a respeito dos tipos de SD-WAN cheque o capítulo Tipos de Perfil. As opções disponíveis são:
 - Load Balance;
 - Failover;
 - Spillover;
 - Dynamic Selection.
- Interfaces: É essencial para o correto funcionamento do SD-WAN definir as interfaces de link de internet que serão usadas na composição do perfil. Neste exemplo selecionaremos as interfaces: "tun0 Rede 10" e "tun1 Rede 11";
- Monitoring Interval (sec.): Definir o intervalo de monitoramento entre cada teste. É recomendável deixar como 1 segundo. Ex.: 1 segundo;
 Failback: Define o número de vezes que uma interface cuja conectividade tenha falhado será testada para ativar o roteamento através dela. Por exemplo, caso o valor seja 5 (o padrão), a interface precisará passar com sucesso em 5 testes de conectividade consecutivos para voltar a ser considerada ativa. O valor máximo de Failback é 100. Para mais informações consulte esta página. Ex.: 5;
- Fail Ratio 1-100%: Definir o valor da taxa de falha entre 1 a 100%. É recomendável deixar o padrão de 70%. Ex.: 70%.
- Persistence Timeout 1-1440 min: Impede a queda das conexões em aplicações que se utilizam de tráfego criptografado SSL. Para mais informações, cheque esta página

Painel Interfaces

Em "Interfaces" temos as seguintes opções:

| | | | Duplication | |
|----|-------------------|-------------------|-------------|--------|
| 11 | ETH0 - REDE LOCAL | 100% | | |
| | ETH1- | 096 | | |
| 11 | ETH2 - | 0% | | |
| :: | ETH3 - | 096 | | |
| | | SD-WAN – Interfac | res | Cancel |
| | | | | |
| | | | | |

- Mover[¹¹]: Clique e arraste para posição desejada, dessa forma o *link* que estiver na primeira posição de cima para baixo será usado para saída do tráfego, caso o *link* estiver desabilitado, o tráfego será redirecionado de forma automática para o *link* subsequente da lista dessa forma garantindo alta disponibilidade no acesso à internet, quando o *link* voltar a ser habilitado o sistema automáticamente irá retornar a saída para o primeiro *link* da lista;
- Interfaces: É essencial para o correto funcionamento do SD-WAN definir as interfaces de link de internet que serão usadas na composição do perfil. Neste exemplo selecionaremos as interfaces: "eth0" e "eth1";
- Load Balance: Ao habilitar múltiplas ETHs note que o Load Balance, que consiste no volume de tráfego de dados por ETH, será dividido entre as mesmas.
- Packet Duplication: Habilita o modo de duplicação de pacotes de dados por caminhos alternativos, para que em caso de queda do link principal, possa ser enviado ao link secundário uma cópia do pacote de dados perdido permitindo assim a maior integridade e disponibilidade do tráfego.

Aba Monitor

Nesta aba são configurados os indicadores de performance e alvos de monitoramento, utilizados pelo SD-WAN.

| Monitor Monitor Monitoring Targets Monitoring Targets www.blockbit.com | Jitter (ms) Jo Bandwidth (%) E1 Protocol • Attempts • Timeout |
|--|---|
| 16 Packet Loss (%) 10 Monitoring Targets • Address www.blockbit.com | Bandwidth (%) ef Protocol • Attempts • Timeout |
| Monitoring Targets Address www.blockbit.com | Bandwidth (%) Protocol Attempts Timeout |
| Monitoring Targets Address www.blockbit.com | Protocol Attempts Timeout |
| Monitoring Targets Address www.blockbit.com | Protocol Attempts Timeout |
| Address www.blockbit.com | Protocol Attempts Timeout |
| www.blockbit.com | |
| | 10MP ∨ 3 ∨ 3mc. ∨ |
| | |

Painel Performance Indicators

Em "Performance Indicators" temos as seguintes caixas de texto:

| * Performance Indicators | |
|--------------------------|---------------|
| ✓ Latency (ms) | Jitter (ms) |
| 10 | 10 |
| Packet Loss (%) | Bandwidth (%) |
| 10 | 85 |
| 10 | 85 |

SD-WAN – SD-WAN Profile - Performance Indicators

- Lattency: Determina quanto tempo leva para um pacote de dados sair da origem, chegar no destino e voltar. Ex.: 10 ms;
 Jitter: Determina a média de quanto tempo leva para um pacote de dados sair da origem, chegar no destino e voltar. Ex.: 30 ms;
 Packet Loss: Determina a porcentagem aceitável de perda de pacotes. Ex.: 75%;
 Bandwidth: Determina a porcentagem aceitável do consumo de banda. Utiliza como base os valores de download em "Traffic Shaping".Ex.: 70%; 70%.

Painel Monitoring Targets

Em "Monitoring Targets" temos as seguintes caixas de texto:



SD-WAN - SDWAN Profile - Monitoring Interfaces

Define os endereços nos quais serão realizados os testes. É recomendável que nos "Monitoring Targets" sejam colocados os IPs virtuais do outro lado do túnel de modo que se a comunicação for feita com sucesso, isso indica que o Túnel está corretamente configurado.

| Por fim. caso deseie cancelar clique no botão Cancel | Cancel | Para concluir a edição das aplicações clique no botão Savel | Save | 1. |
|---|--------|---|------|----|
| | | | | |

Para mais informações a respeito das particularidades e diferenças de cada tipo de perfil, cheque esta página.

Para um exemplo de como configurar um perfil de SD-WAN, cheque esta página.

SD-WAN - Tipos de Perfil

Nas páginas a seguir iremos analisar a fundo cada particularidade dos modos de operação do SD-WAN.

O SD-WAN contempla 4 modos de operação diferentes, para determinar qual deles será utilizado no perfil, siga as instruções abaixo:

1. Clique no botão de editar ou crie um perfil de SD-WAN selecionando a opção Create Profile no menu de ações, a tela abaixo será exibida.

| iterfaces | General | |
|-----------|---|-------------------------|
| Monitor | * Name | |
| | Description | |
| | * тура | * Fall ratio (1 - 100%) |
| | Load Batance 🔍 🔍 | 70 |
| | Monitoring Interval (sec) | • Failback |
| | 5 | <u>E</u> |
| | Persistance timeout 1-1440 min | |
| | 30 | |
| | interfaces | |
| | | |

2. Para determinar o modo de operação do SD-WAN, clique na caixa de seleção "Type" e determine a opção desejada

| * Type | |
|-------------------|---|
| Load Balance | ^ |
| Load Balance | |
| Failover | |
| Spillover | |
| Dynamic Selection | |

SD-WAN - Type

Conforme, demonstrado na imagem acima, o SD-WAN contempla os seguintes modos de operação:

- Load Balance;
 Failover;
 Spillover;
 Dynamic Selection.

A analisaremos as distinções entre cada um destes tipos.

SD-WAN - Load balance

Utilizando-se do Load balance, é possível balancear através de % as novas conexões dessa forma redirecionado o tráfego de acordo com a % definida para cada *link* a fim de otimizar a utilização de recursos, maximizar o desempenho, minimizando o tempo de resposta evitando a sobrecarga de um determinado *link*, dessa forma também é possível aumentar a confiabilidade através da redundância.

1. Para acessar, clique no **Menu de ações [**] e selecione a opção "*Create Profile*";

SD-WAN - Create Profile

Delete Profile

2. A tela demonstrada abaixo será exibida:

| | General | | | |
|----------|---|------------------------------|----------|---|
| Disation | * Name | | | |
| 0011103 | Load Balance BB | | | |
| | Description | | | |
| | SO-WAYL-Load Balance | | | |
| | • Туре | • Fall ratio (I | - 100%6) | |
| | Least Balance 🗸 🗸 🗸 | 100 | | |
| | Monitoring Interval (sec) | Fallback | | |
| | 5 | 5 | | |
| | Persistence timeout 1-1440 min | | | |
| | 30 | | | |
| | Interfaces | | | |
| | II EIHI- | | 33% | |
| | II ETH2- | | 34% | • |
| | 11 ETH3- | | 33% | |
| | | | | 0 |
| | ii veth0- | | | |
| | 11 VETH0 - 11 ETH0 - LOCAL NETWORK | | | a |

SD-WAN - Load Balance - Interfaces

- Fail ratio 1-100%: Definir o valor da taxa de falha entre 1 a 100% para que o *link* seja considerado offline. Ex.: 70%;
 Monitoring interval (sec.): Definir o intervalo de monitoramento entre cada teste. Ex.: 5 segundos;
 Failback: Define o número de vezes que uma interface cuja conectividade tenha falhado será testada para ativar o roteamento através dela. Para mais informações consulte esta página. Ex.: 5.
 Persistence timeout 1-1440 minutes [1]: Define o tempo de "timeout de persistência" para derrubar a conexão no caso de um tempo ocioso. Ex : 15 min. Ex.: 15 min;

3. Acesse a aba "Monitor":

 ${\bf x}_{i,i}$

| Interfaces | Performance Inc | heators | | | | |
|---|---|--|-------------|-----------------------------------|-----------|---------------------------------------|
| Manther | 🛃 Latency (ms) | | | itter (ms) | | |
| Monitor | 10 | | 38 | | | |
| | Packet Loss (| a) | 8 | andwidth (%) | | |
| | 30 | | | | | |
| | Monitoring Target | 9); | | | | |
| | * Address | | Protocol | * Attempts | • Timeout | |
| | www.blockbit.cr | om | CHP V | 3 V | Siec. V. | + |
| licadores de performanc | SD-1 | WAN – Load Balanc ramento que deseja | e - Monitor | | Cancel | Save |
| licadores de performanc mpos devidamente pree | SD-1 e e os alvos de monitor nchido clicar no botão | WAN – Load Balanc ramento que desejar Save | e - Monitor | | Cancel | Save |
| i licadores de performanc mpos devidamente pree SD-WAN | SD-1 e e os alvos de monitor nchido clicar no botão | WAN – Load Balanc ramento que deseja Save ; | e - Monitor | | Cancel | Save |
| ticadores de performanc mpos devidamente pree SD-WAN | SD-1 e e os alvos de monitor nchido clicar no botão | WAN – Load Balanc ramento que desejar Save | e - Monitor | | Cancel | Save |
| icadores de performanc mpos devidamente pree SD-WAN | SD-1 e e os alvos de monitor nchido clicar no botão [| WAN – Load Balanc ramento que desejar Save]; | e - Monitor | | Cancel | Save |
| licadores de performanc mpos devidamente pree | SD-1 e e os alvos de monitor nchido clicar no botão | WAN – Load Balance ramento que desejar Save]; | e - Monitor | Herbics | Cancel | Save |
| ticadores de performance mpos devidamente pree | SD-1 e e os alvos de monitor nchido clicar no botão Desogation IDestin Las Narras | WAN – Load Balance ramento que desejat Save); | e - Monitor | Mefacy whit land harmon | Cancel | Sawe Actions & B |
| ticadores de performance mpos devidamente pree | SD-1 e e os alvos de monitor nchido clicar no botão besolution | WAN – Load Balance ramento que desejar Save]; | e - Monitor | Methods white lange had read | Cancel | Sower |
| ticadores de performance mpos devidamente pree | SD-1 e e os alvos de monitor nchido clicar no botão Descutive | WAN – Load Balance ramento que desejar Save ; | e - Monitor | Mediates white lange histories | Cancel | Sawe Actions Actions Actions |

Após realizar esses procedimentos o SD-WAN Load Balance terá sido configurado com sucesso.

Ao editar o perfil cadastrado é possível visualizar o status do link conforme tela abaixo.

| erfaces | Load Balance | 100 | |
|---------|--------------------------------|------------|------|
| 1.000 | * Monitoring Interval (sec) | * Failback | |
| tor | 5 | 5 | |
| | Persistence timeout 1-1440 min | | |
| | 38 | | |
| | | | |
| | Interfaces | | |
| | II ETH1- | 34 | • |
| | II ETH2- | 39 | 6 🤇 |
| | ∰ ETH⊒- | 33 | fo 🕐 |
| | [] ETHO-LOCAL NETWORK | | 0 |
| | ті VETH0- | | a |
| | 11 WWANG - 222 | | |

SD-WAN - Edit profile - Load Balance

No exemplo acima, caso o *link* da interface eth1 ficar com *status offline*, o valor da % que foi definido para o mesmo será divido por igual entre os *links* que estão com *status online*, no nosso exemplo os 30% que foi definido para o *link* da interface eth1 seria dividido entre os 2 *links* restante com *status onli ne* deixando os 2 *links* respectivamente com 70% e 30%, dessa forma aumentando a confiabilidade através da redundância dos *links*. Uma vez que sistema detecte que *link* da eth1 retomou o *status* de *online* o mesmo irá voltar o peso de balanceamento entre todos os *links*, dessa forma no nosso exemplo voltaria para eth1 = 30%, eth2 = 55% e eth3 = 15%.

SD-WAN - Failover

Failover monitora ativamente os links de internet e age conforme a falha, sendo capaz de aplicar testes de disponibilidade do link em tempo real, dessa forma definindo uma rota alternativa em caso de falha do link principal e restabelecimento automático do roteamento dos links.

1. Para acessar, clique no Menu de ações [



SD-WAN - Create Profile

2. A tela demonstrada abaixo será exibida:

| erfaces | General | |
|---------|---------------------------|---|
| | • Name | |
| Agendor | Failover BB | |
| | Description | |
| | SD-WAN - Failnver | |
| | • Type | Fall ratio (1 - 100%) |
| | Fallover | 70 |
| | Nonitoring Interval (sec) | • Failback |
| | 5 | 3 |
| | Interfaces | |
| | II ETH1- | • |
| | H ELH5- | (C |
| | () ETH3- | • |
| | HE ETHO-LOCAL NETWORK | a |
| | Щ . VETH0 - | a |
| | ii www.ahio-222 | a |
| | | |

- SD-WAN Failover Interfaces

- Description: Definir o nome para o perfil. Ex.: Failover BB;
 Type: Definir o tipo que o perfil irá operar, que pode ser do tipo Failover, Load Balance, Spillover e Dynamic Selection. Ex.: Failover,
 Fail ratio 1-100%: Definir o valor da taxa de falha entre 1 a 100% para que o link seja considerado offline. Ex.: 70%;
 Monitoring interval (sec.) []: Definir o intervalo de monitoramento entre cada teste. Ex.: 5 segundos;
 Failback: Define o número de vezes que uma interface cuja conectividade tenha falhado será testada para ativar o roteamento através dela. Para mais informações consulte esta página. Ex.: 5;
 Interfaces: Definir as interfaces de link de interret que serão usados na composição do perfil. Ex.: eth1. eth2. eth3;
- Interfaces: Definir as interfaces de link de internet que serão usados na composição do perfil. Ex.: eth1, eth2, eth3;

3. Acesse a aba "Monitor":

| | Performance inc | licators | | | |
|---|--|--|-----------------|---|---------------------------------|
| Maglior | Latency (ms) | | Jitter (ms) | | |
| Nonitor | 10 | | 10 | | |
| | Packet Loss (| a) | Bandwidth (% | | |
| | 10 | | | | |
| | Monitoring Target | 8. | | | |
| | * Address | * Prot | ocol • Attempts | • Timeout | |
| | www.blockbit.c | ICHP | 3 0 | Ster, V | + |
| <i>1</i> 2 | S | D-WAN – Failover - Moi | nitor | Cancel | Save |
| icadores de performan mpos devidamente pre | S ce e os alvos de monitor enchido clicar no botão | D-WAN – Failover - Moi ramento que desejar. Save]; | nitor | Cancel | Save |
| icadores de performan mpos devidamente pre | S ce e os alvos de monitor enchido clicar no botão | D-WAN – Failover - Mor ramento que desejar. Save | nitor | Cancel | Save |
| icadores de performan mpos devidamente pre | S ce e os alvos de monitor enchido clicar no botão | D-WAN – Failover - Moi ramento que desejar. Save | nitor | Cancel | Save |
| icadores de performan mpos devidamente pre | S ce e os alvos de monitor enchido clicar no botão | D-WAN – Failover - Mol ramento que desejar. | nitor | Cancel | Sowe |
| icadores de performan | S ce e os alvos de monitor enchido clicar no botão | D-WAN – Failover - Mor ramento que desejar. | nitor | Cancel | Save |
| icadores de performan mpos devidamente pre | S ce e os alvos de monitor enchido clicar no botão besognes | D-WAN – Failover - Mor ramento que desejar. Save]; | nitor | Cancel | Sowe Actions (* A |
| icadores de performan mpos devidamente pre | S ce e os alvos de monitor enchido clicar no botão enchido clicar no botão la solution de la solution personat | D-WAN – Failover - Mor ramento que desejar. Save; | nitor | Cancel (aco) Natural (aco) Natural (aco) Natural | Sove |
| icadores de performan mpos devidamente pre | S ce e os alvos de monitor enchido clicar no botão becograe becograe totant factor totant factor | D-WAN – Failover - Mor ramento que desejar. Save ; Save ; Labore Labore | nitor | Cancel Licci fishook m, etil.etil, etil | Sove Acces I B I C age |

Ao editar o perfil cadastrado é possível visualizar o status do link conforme exibido na tela abaixo.

| * Туре | Fail ratio (1 - 100%) |
|-----------------------------|---|
| Fallover v | 70 |
| * Monitoring Interval (sec) | * Failback |
| 5 | 5 |
| Interfaces | |
| 11 ETH1- | |
| 11 ЕТНЯ- | • |
| [] ETHO-LOCAL NETWORK | a |
| 11 VETH0 - | a |
| WWAN0 - 222 WWAN0 - 222 | a |

O sistema no módulo *failover* irá redirecionar os pacotes para o primeiro *link* online da lista, é possível ordenar os *links* clicando em **[1]** e arrastando para posição desejada, dessa forma o *link* que estiver na primeira posição de cima para baixo será o *link* usado para saída do tráfego, caso o *link* se encontrar *offline* o tráfego será redirecionado de forma automática para o *link* subsequente na lista, dessa forma garantindo alta disponibilidade no acesso à *internet*, quando o *link* voltar a ficar *online* o sistema automáticamente irá retornar a saída para o primeiro *link* da lista.

| As potificações de "falhas e restabelecimento dos links" e do "restabelecimento automático do roteamento" são disparadas automático | mente em |
|---|----------|
| | mente em |
| | |
| tempo real e podem ser visualizadas através da interface WEB clicando no ícone [] ou por e-mail. | |

SD-WAN - Spillover

O Spillover consiste em um processo de transbordamento de tráfego baseado no limite da largura de banda configurado. Quando a banda excede o band width do link da primeira interface configurada com status online no perfil novos fluxos de tráfegos são realocados de forma "Round Robin" entre as interfaces restantes habilitada e com status online no perfil.

1. Para acessar, clique no **Menu de ações [**] e selecione a opção "*Create Profile*";

SD-WAN - Create Profile

Delete Profile

2. A tela demonstrada abaixo será exibida:

| destaces | General | |
|----------|---|--------------------------------|
| Herritor | * Name | |
| 100,000 | Spillover BS | |
| | Description | |
| | SD-WAW-Spillover | |
| | • Туре | Fall ratio (I - 100%) |
| | Spillover | 70 |
| | Monitoring Interval (sec) | Fallback |
| | 5 | 5 |
| | Bandwidth (Mbps) | Persistence timeout 1-1440 mir |
| | 10 | 30 |
| | Interfaces | |
| | II ETH2- | |
| | 11 ETH1+ | • |
| | II ETH3- | |
| | 11 ETHO-LOCAL NETWORK | a |
| | 31 VETH0 - | a |
| | 11 WWAND - 222 | 0 |

SD-WAN - Spillover - Interfaces

- Fail ratio 1-100%: Definir o valor da taxa de falha entre 1 a 100% para considerar o *link* como offline. Ex.: 70%;
 Monitoring interval (sec.): Definir o intervalo de monitoramento entre cada teste. Ex.: 5 segundos;
 Failback: Define o número de vezes que uma interface cuja conectividade tenha falhado será testada para ativar o roteamento através dela.
- Para mais informações consulte esta página. Ex.: 5; Bandwidth (Mbps): Define o limite de bandwidth (largura de banda), caso esse valor seja excedido o fluxo de tráfego será direcionado para a primeira interface com status online configurada no perfil. Ex.: 150 mbs; •
- Persistence timeout 1-1440 minutes []: Define o tempo de "timeout de persistência" para derrubar a conexão no caso de um tempo ocioso. Ex.: 15 min.

3. Acesse a aba "Monitor":

| interface | * Performar | nce indicators | | | | | |
|--|---|---|-------------------------------|-------|--|---|--------|
| | Latency | / (ms) | | 19 | litter (ms) | | |
| Monito | 10 | | | 38 | | | |
| | Packet | Loss (%) | | | landwidth (%) | £. | |
| | 10 | () | | 10 | | 5 | |
| | | | | | | | |
| | Monitoring | Targets | | | | | |
| | * Address | | * Proto | rai l | • Attemats | • Timpout | |
| | - Abbress | - | 191010 | 01 | Actempts | Titleoot | |
| | 11030000000 | 1623041683). | Lister of the | | 1.8 | 11 0304 10 | 1.1.53 |
| | | | | | | Cancel | |
| 25 | | SD-WAN – Spill | lover - Moni | itor | | Cancel | |
| s indicadores de perforn s campos devidamente | nance e os alvos de m preenchido clicar no b | SD-WAN – Spill nonitoramento que d potão [| 'over - Moni esejar.]; | itor | | Cancel | |
| s indicadores de perforn s campos devidamente | nance e os alvos de m preenchido clicar no b | SD-WAN – Spill nonitoramento que d potão [<mark>Save</mark> | over - Moni esejar.]; | itor | | Cancel | |
| s indicadores de perfor s campos devidamente | nance e os alvos de m preenchido clicar no b | SD-WAN – Spill nonitoramento que d potão [<mark>Save</mark> | 'over - Moni esejar.]; | itor | | Cancel | |
| s indicadores de perform s campos devidamente | nance e os alvos de m preenchido clicar no b | <i>SD-WAN – Spill</i> nonitoramento que d potão [Save | 'over - Moni esejar.]; | itor | | Cancel | 5 |
| s indicadores de perfor s campos devidamente | nance e os alvos de m preenchido clicar no b | SD-WAN – Spill nonitoramento que d potão [Save | 'over - Moni esejar.]; | itor | Interfaces | Cancel | |
| s indicadores de perfor s campos devidamente | nance e os alvos de m preenchido clicar no b | SD-WAN – Spill nonitoramento que d potão [Save | lover - Moni esejar.]; | itor | Interfaces | Cancel | |
| s indicadores de perfor s campos devidamente | nance e os alvos de m preenchido clicar no b | SD-WAN – Spill nonitoramento que d potão [Save | 'over - Moni esejar. | itor | Interviewes edute, edut, edut, edut, edut, | Cancel. | |
| s indicadores de perfor s campos devidamente | nance e os alvos de m preenchido clicar no b | SD-WAN – Spill nonitoramento que d potão [Save | over - Moni esejar.]; | itor | Notesting - Los and the set of th | Cancel contracts out Persest out Persest out Persest out Persest | |

Por fim, após salvar, para que o *SD-WAN* entre em ação será necessário acessar a **fila de comandos [** mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

] e aplicar as alterações efetuadas. Para

Após realizar esses procedimentos o SD-WAN Spillover terá sido configurado com sucesso.

Ao editar o perfil cadastrado é possível visualizar o status do link conforme tela abaixo.

| Monitoring Interval (sec) Failback | | |
|---|--------------------------------|--|
| tor 5 5 | | |
| Bandwidth (Mbps) | Persistence timeout 1-1440 min | |
| 160 30 | | |
| II ETH2- II ETH2- | - | |
| [] ETHO-LOCAL NETWORK | 0 | |
| 71 VETH0 - | a | |
| 11 W9/ANG - 227 | 0 | |

SD-WAN - Edit profile - Spillover Exemplo

No processo de *spillover* o sistema direciona todo o fluxo de tráfego para a primeira interface com *status online* configurado no perfil, quando o valor exceder o *bandwidth* (largura da banda) configurado, no nosso exemplo acima foi configurado com o *bandwidth* de 150 *Mb*/s (cento e cinquenta *mega bits* por segundo) os novos fluxos de tráfegos são realocados de forma *"Round Robin"* entre as interfaces restantes habilitada e com *status online* no perfil.

SD-WAN - Dynamic Selection

Em Dynamic Selection o tráfego é priorizado para o link que tiver um resultado melhor frente ao critério de qualidade, assim sendo, novos fluxos serão atribuídos a este mesmo. Assim sendo, o sistema dinamicamente distribui as % entre os links com melhor performance tendo como base o indicador de qualidade selecionado.

1. Para acessar, clique no Menu de ações [] e selecione a opção "Create Profile";

SD-WAN - Create Profile

Delete Profile

2. A tela demonstrada abaixo será exibida:

| 100 | 1.444 | 6.66 | ~ | | 64 | |
|-----|-------|------|---|----|----|----|
| 30 | ьw. | AN: | н | 10 | 20 | ē. |
| | | | | 00 | | 2 |

| Monitor | - Maline | | | | |
|---------|---|--|--|--|--|
| | Dynamic Selection BB | | | | |
| | Description | | | | |
| | SD-WAN - Dynamic Salaction | | | | |
| | * Туре | * Fall ratio (1 - 100%) | | | |
| | Dynamic Selection | ~ 70 | | | |
| | Monitoring Interval (sec) | • Failback | | | |
| | 5 | <u>E</u> | | | |
| | Quality criteria (Mbps) | Balancing Interval (min) | | | |
| | Labercy | v 5 | | | |
| | Persistence timeout 1-1440 mi | n | | | |
| | 30 | | | | |
| | interfaces | | | | |
| | 41 ETH2- | • | | | |
| | II ETHI- | | | | |
| | II ETHS | C | | | |
| | I ETHO-LOCAL NETWORK | a | | | |
| | 11 VETH0- | | | | |
| | 11 WWANG - 222 | 0 | | | |
| | | | | | |

×

SD-WAN – Dynamic Selection – Interfaces

• Monitoring interval (sec.) : Definir o intervalo de monitoramento entre cada teste. Ex.: 5 segundos;

Quando um dos links cai o intervalo de monitoramento é resetado e ele só voltará a contar depois que o link subir. Caso a queda de links esteja ocorrendo antes de passar o tempo do intervalo de monitoramento os relatórios gerados sempre apontarão as porcentagens de rede como 50 uma vez que o intervalo de monitoramento está sendo constantemente resetado pela seleção dinâmica.

- Fail ratio 1-100%: Definir o valor da taxa de falha entre 1 a 100% para considerar o *link* como offline. Ex.: 70%;
 Monitoring interval (min.): Determina o período que será calculado o valor dos valores em %, baseado na média dos critérios de qualidade dos *l* inks ativos. Ex.:5;
- Failback: Define o número de vezes que uma interface cuja conectividade tenha falhado será testada para ativar o roteamento através dela. Para mais informações consulte esta página. Ex.: 5;
- Quality criteria: Determina o indicador de performance que será utilizado pela seleção dinâmica do link. Ex.: Latency;

- Persistent connection: Para habilitar a persistência de *Link*, marque esta caixa de checagem. Ex.: *Enable*;
 Persistence timeout 1-1440 minutes[]: Definir o valor da taxa de falha entre 1 a 100% para considerar o *link* como offline. Ex.: 70%.

3. Acesse a aba "Monitor":

| Interfaces | Performance indicators | | | | | |
|---|---|-----------------------------------|--------|---------------------|-----------|--|
| 1 | Latency (ms) | | 1 | itter (ms) | | |
| Monitor | 10 | | 38 | | | |
| | Packet Loss (%) | | | andwidth (%) | Ê | |
| | 10 | | | | | |
| | Monitoring Targets | | | | | |
| | Address | * Proto | kod | Attempts | • Timeout | |
| | www.blockbit.com | ICHP | 1 | 3 V | Ster. V. | |
| | | | | | Cancel | |
| .0 | SD-WAN – Dyna | mic Selection - | - Mon | itor | Cancel | |
| dicadores de performance ampos devidamente preer | <i>SD-WAN – Dyna</i> e e os alvos de monitoramento q nchido clicar no botão (| mic Selection - ue desejar (FQ | - Mon | itor PV4, IPV6). | Cancel | |
| dicadores de performance | <i>SD-WAN – Dyna</i> e e os alvos de monitoramento q nchido clicar no botão [| mic Selection - le desejar (FQ | - Moni | itor PV4, IPV6). | Cancel | |
| dicadores de performance ampos devidamente preer | <i>SD-WAN – Dyna</i> e e os alvos de monitoramento q nchido clicar no botão [| mic Selection - le desejar (FQ | - Moni | itor PV4, IPV6). | Cancel | |
| dicadores de performance ampos devidamente preer | SD-WAN – Dyna e e os alvos de monitoramento q nchido clicar no botão [Sav | mic Selection - le desejar (FQ | - Moni | itor PV4, IPV6). | Cancel | |
| dicadores de performance | SD-WAN – Dyna e e os alvos de monitoramento q nchido clicar no botão [Sav | mic Selection - le desejar (FQ | - Moni | itor PV4, IPV6). | Cancel | |
| dicadores de performance ampos devidamente preer SD-WAN | SD-WAN – Dyna e e os alvos de monitoramento q nchido clicar no botão [Sav | mic Selection - le desejar (FQ | - Moni | itor PV4, IPV6). | Cancel | |

SD-WAN - Profiles

Por fim, após salvar, para que o *SD-WAN* entre em ação será necessário acessar a **fila de comandos [** mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Após realizar esses procedimentos o SD-WAN Dynamic Selection terá sido configurado com sucesso.

] e aplicar as alterações efetuadas. Para

SD-WAN - Profiles - Menu de ações - Delete Profile

Através do botão "Delete Profile" é possível deletar os Profiles selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) *Profile*(s) deseja deletar. Para selecionar, basta clicar com o *mouse* no *checkbox* que fica localizado ao lado do *Name*. Nos *profiles* selecionados o *checkbox* mudará da cor cinza para azul [2]. Ex.: *Test*:

| Nie. | Silling | | | | |
|-------|-----------------------|---------------------------|--------------------|---------------------------------------|-------|
| acori | | | | | 0 |
| • | (\$10100) | Description | type | recordances | 44594 |
| | 140 | 76.0 | Loochalaria | UTVE-401-Lacal Nativola | 1.1 |
| | lyneric teacter (iii) | 53-6446-Dynamic Selection | Exercise Salactory | emit, ath2, emit-Local terrory. | 1.1 |
| | Spilleer M | the same the second | failures. | etal, etal, etal-traal Network | 1.0 |
| | Galaxye Mil | 12-096-Falsee | fallow | while, while, while is constructions | 11 |
| | Los Diversiti | ST-WA Lost Marin | Lost Balance. | ethil-Local Network, #193, eDO, ethil | 10.1 |

SD-WAN - Seleção dos Profiles para deletar

2. Entre no Menu Actions e clique na opção "Delete Templates".



SD-WAN - Delete Profile.

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os profiles selecionados:

| Are you sure? | | × |
|--|--------|--------|
| Are you sure you want to delete the profile: Test? | | |
| | Cancel | Delete |

SD-WAN - Mensagem se deseja deletar os Profiles



Após realizar esses procedimentos, os profiles terão sido deletados com sucesso.

SD-WAN - Profiles - Colunas

A seguir explicaremos cada coluna da aba SD-WAN:

| otius | Settings | | | | | |
|----------|----------------------|-------------------------|-------------------|--|---|----|
| i nezeri | 0 | | | | 9 | Į. |
| | tees | Description | Type: | lette effectes | A | - |
| | kyunic Selection (A) | CD-WH-Dynamic Salaction | Byramic Selection | ethi, miz, etric - uscar tenverii | 1 | |
| | toilever 18 | REALIZE Tailowy | lpilover | arthdi, athdi, athdi - Local Mathemia | 1 | 1 |
| | Fallover DD | 10-wood-Fallerier | Factorie | or the state, while a constraint warms | 1 | |
| | Unied Selamon 982 | 52-WW-Load Balance | Unied Seller on | etd-LiealNaturek, #60.etd.al82 | 1 | 0 |

SD-WAN - Profiles

A seguir explicaremos cada coluna:

- Caixa de Seleção[]: Seleciona o profile.

- Name: Apresenta o nome do *profile* cadastrado;
 Description: Apresenta a descrição do *profile* cadastrado;
 Type: Define o tipo de SD-WAN, para mais informações cheque esta página;
- Interfaces: Exibe as interfaces que são afetadas pelo perfil de SD-WAN em questão;
 Actions: A coluna "Actions" é composta por vários botões:



SD-WAN - Aba Settings

Nesta aba é possível criar e configurar serviços de SD-WAN, através desta aba é possível configurar a saída do Firewall para algum serviço, sem haver a necessidade da criação de uma política. Para tanto, clique na aba "Settings".

| Profiles | Settings |
|----------|----------|
| Aba | Settings |

Surgirá a tela a seguir, conforme demonstrado pela imagem abaixo:

| -WAN | | | |
|--------------|---------|----------|--------|
| alia. Intege | | | |
| | | | 1 9 |
| Description | Prefilm | Draillie | fation |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

SD-WAN - Settings

Esta sessão irá abordar como cadastrar, editar e remover serviços de SD-WAN;

A seguir, analisaremos cada função deste painel.
SD-WAN - Settings - Menu de Ações

No topo direito da tela temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



SD-WAN - Settings - Menu de ações

O menu é composto das seguintes opções:

- Create Service;
- Delete Service.

A seguir cada opção do menu de ações será detalhada.

SD-WAN - Settings - Menu de Ações - Create Service

Através da opção "Create Service" é possível criar um novo serviço de SD-WAN. Para acessar, clique no Menu de ações [

1. Clique na opção "Create Service";



].

SD-WAN - Create Service

2. A tela demonstrada abaixo será exibida:

.

| SD-WAN Service | | |) |
|--------------------------|-----------------|--------|--------|
| ✓ Enable | | | |
| * Description | | | |
| * Service | | | |
| Select | | | |
| * Destination IP Address | | | |
| Select | | | |
| * Profile | | | |
| | | | \sim |
| | | | |
| | | Cancel | Save |
| | SD-WAN - Servic | e | |

A seguir demonstraremos como configurar este painel.

• [V] Enable: Ao marcar esta caixa de seleção, o serviço estará habilitado;

- Description: Neste campo é definida a descrição do serviço. Ela será utilizada para identificação nas colunas. Ex.: SD-WAN Service;
- Service: Neste campo deve-se adicionar os objetos de serviço que serão utilizados pelo SD-WAN. Para mais informações sobre como criar um objeto de serviço, cheque esta página. Ex.: AH, Administration;
- Destination IP Address: Neste campo são adicionados objetos de endereço que são utilizados como endereço IP de destino. Para mais informações sobre como criar um objeto de endereços, cheque esta página. Ex.: Class A Network, Class B Network, Class C Network, 192.168.254.13;
- **Profile:** Por fim, é adicionado o perfil de SD-WAN que será utilizado no serviço. Os objetos que são adicionados neste campo são adicionados na aba *Profiles*, para mais informações, cheque esta página. Ex.: Proxy Balance.

| | Cancel | | Save | |
|-------------------------------|--------|--|------|---|
| Para cancelar clique no botão | |]. Para concluir a edição das aplicações clique no botão [| | 1 |

SD-WAN - Settings - Menu de Ações - Delete Service

Através do botão "Delete Service" é possível deletar os Serviços selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) Service(s) deseja deletar. Para selecionar, basta clicar com o mouse no checkbox que fica localizado ao lado do Name. Nos services selecionados o checkbox mudará da cor cinza para azul [...]. Ex.: Test:

| SD-WA | AN | | | |
|--------|-------------|-------------------|-----------|------------|
| rodius | Seteg | | | |
| Terret | 4 | | | |
| | Description | rulle | Buildin . | Adam |
| 5 | rest | Valorit BB | 0 | 1 0 |
| | LOP- | Loss failures \$8 | 9 | 1 0 |
| | | | | (t) inter- |

SD-WAN - Seleção dos Services para deletar

2. Entre no Menu Actions e clique na opção "Delete Service".



SD-WAN - Delete Service

3. Surgirá a mensagem de notificação questionando se deseja realmente deletar os profiles selecionados:

| Delete Service | | × |
|---|--------|--------|
| Are you sure you want to delete: TEST ? | | |
| | Cancel | Delete |

SD-WAN - Mensagem se deseja deletar os Services

| | Cancel | | Delete | |
|--|--------|--|--------|----|
| Caso deseiar cancelar clique no botão Cancel | | Para concluir, clique no botão Deletel | | 1. |



Após realizar esses procedimentos, os services terão sido deletados com sucesso.

SD-WAN - Settings - Colunas

A seguir explicaremos cada coluna da aba Settings:

| SD-WAN | | | |
|-----------------|-----------------|--------|---------|
| mittee Settings | | | |
| t seconda | | | 3. 4 |
| Bucipion | Pullin | Easter | #atkas |
| 1234 | Load Balance #8 | 0 | 1.3 |
| | | | IN Nome |

SD-WAN - Settings - Colunas

A seguir explicaremos cada coluna:

- Caixa de Seleção []: Permite a seleção do profile.
- Description: Apresenta a descrição do profile cadastrado na opção Create Service do menu de ações; ٠
- Profiles: Apresenta a descrição do profile cadastrado na opção Create Service do menu de ações;
 Enable: Exibe o estado atual, podendo estar habilitado ou desabilitado;
- Actions: A coluna "Actions" é composta pelos botões:

• Botão Edit []: Permite editar as configurações do service adicionado na opção Create Service do menu de ações;

• Botão Delete []: Deleta o service, é o equivalente a opção Delete Service do menu de ações.

SD-WAN - Exemplo: Configuração do SD-WAN

Esta seção irá apresentar o passo a passo para configuração de um SD-WAN. Essa demonstração levará em consideração a seguinte estrutura:





Nesta estrutura serão interligadas duas unidades organizacionais com múltiplos *links* conectados através da *Internet*. Os seguintes *IPs* serão utilizados neste exemplo:

SD-WAN - Endereçamento IP

| Nome | Endereço IP LAN | Endereço IP Administração | Endereço IP Internet | Endereço IP Virtual (TUN) |
|---------------------|-----------------|---------------------------|----------------------|---------------------------|
| UTM - <i>HQ</i> | 172.18.0.0/16 | 172.31.208.40 | 10.0.0.2 | 20.0.0.1 |
| | | | 11.0.0.2 | 21.0.0.1 |
| UTM - Remote Office | 172.17.0.0/16 | 172.31.208.41 | 100.0.0.2 | 20.0.0.2 |
| | | | 101.0.0.2 | 21.0.0.2 |

Os passos que serão tomados a seguir serão:

- 1. Configurar interfaces Tunnel: Neste passo será viabilizado o encapsulamento ponto-a-ponto através da criação das interfaces Tunnel, estas serão utilizadas pela VPN, para mais informações cheque o capítulo Interfaces de Rede;
- Configurar VPN: Nesta etapa será estabelecido o túnel privado entre duas redes, permitindo que elas sejam interligadas e a comunicação seja efetuada de forma criptografada, para mais informações cheque o capítulo VPN IPSEC;
- Configurar SD-WAN: O foco desta fase é efetivamente configurar o SD-WAN, o que possibilita a segmentação de tráfego das interfaces de rede e monitoramento através dos indicadores de performance;
- Configurar Políticas: Nesta etapa, será criada uma política para a liberação do acesso, de modo a viabilizar a comunicação através da VPN com SD-WAN, para mais informações cheque o capítulo Policy;
- 5. Validação da Configuração do SD-WAN: Por fim, alguns testes serão executados para validar caso todas as configurações foram criadas com sucesso.

SD-WAN - Configurar Interface Tunnel

Inicialmente, acesse o menu Settings a aba Network:



Por fim, clique na aba Interfaces:

| Settings | Interfaces | Static Routing | Dynamic Routing | IPv6 Settings | Traffic Shaping |
|----------|------------|----------------|-----------------|---------------|-----------------|
| | | | Aba Interfaces | | |

Abaixo seguem as configurações do UTM – HQ:

| Network | | | | | |
|---------------------|----------------------------|------------------|-----------|-------|--------|
| internet intertaint | Reschaling. Systems had by | History Talk Ray | - | | |
| | | | | | + - |
| electure : | Address | Catriera | 5,90 | žarm. | Action |
| 0-chi | 172.20.200,40/06 | | Physical. | 1,000 | |
| 0 etc | 10.0.0254 | 10.8.0.1 | Physical | NHN . | 0/1 |
| O etc | 1144204 | 31.84.1 | Physical | AND. | • / = |
| 0 etc | | | Physical | | ⊕ ≠ s |
| 0 terr | 20.8.0.1798 | 30.402 | Totod | 32669 | C / 1 |
| 0 test | 21.0.0.010 | 21.8.2.1 | Tutted | 18999 | C / I |

Network - Interfaces

Para criar interfaces TUNNEL, clique em Add] e selecione a opção TUNNEL.

| | + |
|---------|---|
| VIRTUAL | |
| VLAN | |
| DSL | |
| LAG | |
| BRIDGE | |
| TUNNEL | |
| | |

Interfaces - Add Tunnel

A seguinte tela será exibida:

| terrent in the second states | ander anderen a | adalah (Calabasa | e 3892 | | + |
|------------------------------|------------------|------------------|-----------|--------|---|
| | Spoww | | | | |
| | Balwork Zone | | | | |
| | | NH. | | | |
| | becilgtion | | | | |
| | | | | | |
| | Temelizations | | | | |
| | Pagent Intertace | | | 10 | |
| | Angesto addmas | | AD | D-1979 | |
| | diverse interest | | | | |
| | 194 | | | | |
| | if block | Mark INCOLUMN | Catalogy | 0 | |
| | | | | | |
| | if address | profix 3 | Galanatay | 0 | |
| | Abaset | | | | |
| | MIL | | | | |

Interfaces - Network

A seguir analisaremos cada componente do painel e apontaremos os passos específicos para a configuração do SD-WAN, para obter informações mais aprofundadas a respeito desse tópico vide este capítulo.

Painel General

Complete o formulário conforme exemplificado a seguir:

| General | | |
|--------------|------|--|
| Network Zone | Name | |
| SDWAN | tun0 | |
| Description | | |
| Rede 10 | | |
| | | |

Interfaces - Painel General

- Network Zone: Neste campo é recomendável isolar o segmento de tráfego dos tuneis envolvidos para não conflitar com políticas de segurança que envolvem outras zonas de rede, como por exemplo LAN e WAN. Assim, sendo colocaremos "SDWAN";
- Description: Insira a descrição desejada de forma a facilitar a identificação da interface túnel posteriormente.

Tunnel Options

Complete o formulário conforme exemplificado a seguir:

| Tunnel options | |
|------------------|---------|
| Parent interface | |
| eth1 | ~ |
| Remote address | Dynamic |
| 100.0.0.2 | |
| | |

Interfaces – Tunnel Options

- Parent interface: Determinar a interface que será utilizada para estabelecimento do túnel. Ex.: eth1;
- Remote address: Neste campo é importante que seja inserido o IP real que será utilizado. Ex.: 100.0.0.2 (Endereço IP Internet do BLOCKBIT Remoto);

Complete o formulário conforme exemplificado a seguir:

| P Address | Mask | Gateway | |
|-----------|---------------|------------|---|
| 20.0.0.1 | 255.255.255.0 | ~ 20.0.0.2 | 6 |

- IP Address: Determina o IP que será utilizado pelo túnel. Neste campo o endereçamento utilizado é o IP virtual. Ex.: 20.0.0.1;
- Mask: A máscara neste campo pode ser a default. Ex.: 255.255.255.252;
- Gateway: O gateway utilizado neste campo pode ser o endereço da interface Tunnel do UTM Remoto. Ex.: 20.0.0.2;

As outras opções podem ser deixadas como estão no padrão.

Clique no botão Save[

we[____] para gravar as configurações feitas.

Após estes passos, devemos ter chego no resultado demonstrado pela imagem abaixo:

| General | | |
|--------------|------|--|
| Network Zone | Name | |
| SDWAN | tun0 | |
| Description | | |
| Network 10 | | |

| Tunnel options | |
|------------------|--------|
| Parent interface | |
| eth1 | ~ |
| Remote address | AD-VPN |
| 100.0.0.2 | |

| V IPv4 | | |
|------------|-----------------|----------|
| IP Address | Mask | Gateway |
| 20.0.0.1 | 255.255.255.252 | 20.0.0.2 |

| IPv6 | | | | |
|------------|--------|--------|---------|---|
| IP Address | Prefix | | Gateway | |
| | 36 | \sim | | 0 |
| | | | | |

| Advanced | | |
|-------------|---|--|
| MTU | | |
| 1280 - 9000 | ÷ | |

Interfaces - Configurações do tun0

Repita esses passos para criar todas as interfaces necessárias para cada link.

Em nosso ambiente, como temos 2 links e devemos criar 2 túneis, criaremos mais uma TUN, com as configurações abaixo:

Opções do Túnel

- Parent interface: Determinar a interface que será utilizada para estabelecimento do túnel. Ex.: eth2;
- Remote address: Neste campo é importante que seja inserido o IP real que será utilizado. Ex.: 101.0.0.2 (Endereço IP Internet do UTM Remoto).

IPv4

- IP Address: Determina o IP que será utilizado pelo túnel. Neste campo o endereçamento utilizado é o IP virtual. Ex.: 21.0.0.1;
- Mask: A máscara neste campo pode ser a default. Ex.: 255.255.255.252;
- Gateway: O gateway utilizado neste campo pode ser o endereço da interface Tunnel do UTM Remoto. Ex.: 21.0.0.2;

Segue as configurações finais demonstradas na imagem abaixo:

| Networ | k | | | | | |
|----------|----------------|---------------------------------|-----------------|----------------|--------|--------------------------------------|
| Settings | interfaces | Static Routing Dynamic Boulding | 0745 Self. (1g) | mattic shaping | | |
| | | | | | | + - |
| Status | interface | Address | Gatescoy | Тура | Jone | Action |
| e | O ethil | 172.31.706.43/18 | 14 | Physical | LAN | 1 2 |
| • | 0 etti. | 104.0.2/24 | 10.0.0.1 | Physical | man | $\langle \mathcal{X} \rangle \equiv$ |
| 0 | O eth2 | 11.9.0.2/24 | 13.4.0.1 | Physical | 16.4.M | (Z) (E) |
| 0 | Oetro | 8 | 21 | Physical | (±) | 2.1 |
| • | Oatha | 172.58.0.1/18 | C.2 | Physical | LAN | 1 |
| 0 | @tim2 | 20.0.0.1/30 | 20.0.0.2 | Turnet | SDWAIN | 21 |
| e | Otint | 214.0.1/30 | 210.02 | Turnel | SOWAH | 2 |

Interfaces - Configurações da Rede

Abaixo seguem as configurações da interface tun0 do UTM - Remote Office:

| General | | |
|--------------|------|--|
| Network Zone | Name | |
| SDWAN | tun0 | |
| Description | | |
| Network 100 | | |

| Opções do túnel | |
|------------------|--------|
| Parent interface | |
| eth1 | ~ |
| Remote address | AD-VPN |
| 100.0.0.2 | |

| V IPv4 | | | |
|------------|-----------------|------------|---|
| IP Address | Mask | Gateway | |
| 20.0.0.2 | 255.255.255.252 | ~ 20.0.0.1 | 8 |
| 20.0.0.2 | 255.255.255.252 | 20.0.0.1 | 1 |

| IPv6 | | | | |
|------------|--------|---|---------|---|
| IP Address | Prefix | | Gateway | |
| | | ~ | | 0 |

| Advanced | | |
|-------------|--------|--|
| MTU | | |
| 1280 - 9000 | * * | |

Interfaces - Remote Office - Configurações do tun0

As configurações do tun1 do UTM - Remote Office devem ficar conforme demonstrado na imagem abaixo:

| General | | |
|--------------|------|--|
| Network Zone | Name | |
| SDWAN | tun0 | |
| Description | | |
| Network 101 | | |

| ~ |
|--------|
| AD-VPN |
| |
| |

| sk | Gateway | |
|------------------|-------------------------|--|
| \$55.255.255.252 | 21.0.0.1 | 0 |
| | sk 255.255.255.252 ~ | sk Gateway 255.255.255.252 |

| IPv6 | | | | |
|------------|--------|---|---------|---|
| IP Address | Prefix | ~ | Gateway | • |
| | | | | |

| Advanced | | |
|-------------|---|--|
| MTU | | |
| 1280 - 9000 | ¢ | |

Interfaces - Remote Office - Configurações do tun1

Configurações finais:

| Networ | k | | | | | |
|----------|----------------|---------------------------------|------------|----------------|--------|--------------|
| Settings | interfaces | static locating Dynamic Roaming | missimity. | matter shaping | | |
| | | | | | | + - |
| Status | interface | inidreen | Gatessay | Тури | Jone | Action |
| C. | O ethil | 17231208.40/18 | 34 - C | Physical | LAN | 1 2 |
| • | 0 etti | 104.0.2/24 | 10.0.01 | Physical | TEAN | $ S \equiv$ |
| 0 | O eth2 | 11/9.0/2/24 | 11461 | Physical | 16.4N | (Z) 2 |
| 0 | Oetra | 8 | 12 | Physical | (±) | 2.1 |
| • | O athe | 172.58.0.1/18 | 12 | Physical | LAN | X = |
| 0 | @tim2 | 30.0.0.1/30 | 20.0.0.2 | Turnet | SDWAIN | X 1 |
| e | Otint | 214.0.1/30 | 31.0.02 | Turnel | SOWAH | 2 E |

Interfaces - Remote Office - Configurações do Network

Para testar a comunicação entre as duas interfaces criadas acesse via ambos os UTMs através de SSH. Utilizando o comando "ifconfig", será possível visualizar as duas interfaces túneis ativas, conforme é visualizado na imagem abaixo.





Além disso, é possível usar o comando ping para tentar efetuar a comunicação com estas interfaces, caso seja recebida uma resposta, isso indica que a comunicação foi efetuada com sucesso.

```
admin >ping 20.0.0.1

PING 20.0.0.1 (20.0.0.1) 56(84) bytes of data.

64 bytes from 20.0.0.1: icmp_seq=1 ttl=64 time=0.043 ms

64 bytes from 20.0.0.1: icmp_seq=2 ttl=64 time=0.034 ms

64 bytes from 20.0.0.1: icmp_seq=3 ttl=64 time=0.062 ms

64 bytes from 20.0.0.1: icmp_seq=4 ttl=64 time=0.071 ms

64 bytes from 20.0.0.1: icmp_seq=5 ttl=64 time=0.023 ms

--- 20.0.0.1 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 3999ms

rtt min/avg/max/mdev = 0.023/0.046/0.071/0.019 ms

admin >
```

CLI - ping

A seguir, vamos configurar as VPNs.

SD-WAN: Configurar VPN

Após ter configurado as interfaces tunnel, siga os passos à seguir:

Inicialmente, acesse Services e clique na opção VPN IPSEC:



Services - VPN IPSEC

Feito isso, selecione a aba Tunnels:

| Tunnels | Remote Access | Failover |
|---------|---------------|----------|
|---------|---------------|----------|

VPN IPSEC - Aba Tunnels

A seguinte tela será exibida:

| B lockbit | = | | W A 2 1- |
|---|---------------------------------------|--|--|
| | VPN IPSEC | | |
| | Territoria di Statemania di State | - | |
| a antipite | | | * |
| | and parts | 1944 | |
| > | Nexe 1 | 355.55.556 | 40 X X |
| a function of the | Typesid g | 10. N THE | 4. A. X |
| t per E | | | |
| 12. 3 | | | |
| e en res 🛛 | | | |
| Change / | | | |
| * (maximi | | | |
| and the second se | | | |
| | | VPN IPSEC - Tunnels | |
| | | | |
| | | | |
| + | | | |
| Clique no botão <i>Add</i> [] para ad | icionar uma nova VPN | <i>I</i> , a seguinte tela será exibida: | |
| | | | |
| F | | | 7 |
| Add tunnel | | | × |
| | | | |
| Description | | | |
| - | | | |
| | | | |
| Tino | | | |
| про | | | |
| Site-to-Site | | | ~ |
| | | | |
| | | | |
| | | | |
| | | | III) Source |
| | | | E Save |
| L | | | |
| | | VFIN IFSEC - Aud TUNNEI | |
| | | | |
| • Description: Tunnel 1; | | | |
| • Tipo: Site-to-Site. | | | |
| | | | |
| | | | |
| 🖺 Save | · · · · · · · · · · · · · · · · · · · | | |
| ilque em Save [] para | a salvar as alterações o | e apos esse passo, clique no botão <i>Edit</i> | J para dar continuidade às configuraçõ |

| | | | + |
|--|---|------------------------|--------|
| Seneral | | | ~ |
| | | | |
| Description | | HE Venilles | |
| Tarrel). | | | |
| toralbot | | Senote host | Dynami |
| P) Num | | 17 feature | |
| tocal tile | | Someta 18 | Dynami |
| Philippe International Accession (International Accession) | | White their enablement | |
| Turonel Initialization | | Cochange Hode | - 10 |
| Adouts | | and and | |
| Buthentication Method | | Sunday | |
| Prant Ny | | a second | |
| LOCAL REAL RAY | | (i) Portwist PEA Koy | |
| | | | |
| letwork | | | |
| letwork. | | | • |
| lottwark #Votien Seat | | | ^ |
| lofavork PYrsian Sett | | | • |
| loftwork PVcsien Seat | 8 | Resolution sofreedat | • |
| leftwork PVesten Seat | 8 | Resource and poolses | |
| lottavorik Prosien Seat | | Results sofreeds | |
| latiwork Presien Seat Local official | | Menore entrande | |
| latiwork * Vestien Seat Local connects | | Resolute and works | |
| latiwork Prosten Seat Deal offensels (mail | | | |

VPN IPSEC - Adicionando VPN

A seguir analisaremos cada componente do painel e apontaremos os passos específicos para a configuração do SD-WAN, para obter informações mais aprofundadas a respeito de VPN tópico vide o capítulo VPN IPSEC.

General

Complete o formulário conforme exemplificado a seguir:

| PX venice | |
|--------------------|---|
| HER. | |
| Remails tost | Dynamic |
| 140.033 | |
| #emate(D | Dynamic |
| 18(0.8) | |
| txxbarge stole | |
| No. | |
| Muned Kay | |
| | |
| 12: Revelation Noy | |
| | |
| | |
| | |
| | KOALER KOALER |

VPN IPSEC - Painel General

- Description: Insira a descrição desejada de forma a facilitar a identificação da VPN posteriormente;
- IKE Version: Determina a versão do IKE que será utilizada. Neste exemplo usaremos a versão IKEv1;
- Local Host: Determina o endereço de comunicação do ponto VPN LOCAL para estabelecer o túnel. Neste campo é necessário se adicionar IP real. Ex.: 10.0.0.2;
- **Remote Host**: Determina o endereço remoto com o qual a VPN irá tentar estabelecer a conexão. Neste campo é necessário se adicionar o IP real do host remoto. Ex.: 100.0.0.2;
- Local ID: Método de identificação da ponta VPN Local. Método de identificação da ponta VPN Local. Neste campo é necessário se adicionar IP real. Ex.: 10.0.0.2;
- Remote ID: Método de identificação da ponta VPN Remota. Neste campo é necessário se adicionar IP real. Ex.: 100.0.0.2;
- Tunnel Initialization: Determina a forma com a qual o túnel efetuará sua inicialização. Ex.: Automatic;
- Exchange Mode: Método de negociação da chave IKE. Ex.: Main;
- Authentication Method: Determina o método de autenticação que será utilizado na VPN. Ex.: Shared Key;
- Shared Key: A chave pré-compartilhada que será utilizada para autenticar a VPN;
- Local RSA Key: Caso a opção "RSA Key" esteja selecionada em "Authentication Method", este campo estará disponível. Neste exemplo não utilizaremos a opção "RSA Key";
- Remote RSA Key: Caso a opção "RSA Key" esteja selecionada em "Authentication Method", este campo estará disponível. Neste exemplo não utilizaremos a opção "RSA Key".

Network

Complete o formulário conforme exemplificado a seguir:

| dvanced: | | | | ^ |
|----------------|---------------|---------------|-------|--------|
| 63. lifetime | Result-(2) | 040 Action | | |
| jan . | | lister | | 1 |
| ny Delive | Alexandro (s) | BPD Delay | | Sec. |
| 46 | | dH | | |
| Beyling triles | | 3PD Streest | | Second |
| *. | | [<i>in</i>] | | |
| lielory marge | \$9xx8x(2) | | | |
| * | | | | |
| Ra-Auth | Fragmentation | Cumprasilan | NAT-T | |
| fa-Auth | Fragmentation | Corpression | NALL. | |

VPN IPSEC - Painel Network

- IP version: Não é necessário determinar a versão de IP, pode ser deixado no padrão;
- Local Networks: É importante para o correto funcionamento do SD-WAN que este campo fique sem ser preenchido. O próprio SD-WAN determinará os "Local Networks";
- Remote Networks: Assim como no campo de cima, é importante para o correto funcionamento do SD-WAN deixar este campo também sem ser preenchido. O próprio SD-WAN determinará os "Remote Networks".

Advanced

Complete o formulário conforme exemplificado a seguir:

| | | | | 100 |
|----------------|---------------|--------------|------|--------|
| 03. Unitera | 101.05 | 4 040 Action | | |
| - the | | lictor | | |
| nay Delive | Alberta | 9 BPD Belay | | loon |
| 44 | | (H | | |
| maying trime | | 3FD Sireest | | Series |
| | | | | |
| lielory margie | \$3este | E) | | |
| ÷ | | | | |
| Ro-Auth | Fragmentation | Cumprensian | NATT | |

VPN IPSEC - Painel Advanced

• Keying tries: Este é o número de vezes que os pontos VPN vão renegociar o túnel ou tentar reautenticação (re-key) depois que a chave expirar. No nosso exemplo usaremos o valor "0";

| Todas as outras opções | s podem ficar no padrão | , clique no botão | Save [|] para salvar as | s configurações efetuadas. |
|------------------------|-------------------------|-------------------|--------|------------------|----------------------------|
| | | | | | |

Após estes passos, devemos ter chego no resultado demonstrado pela imagem abaixo:

| Seheral | | | ^ |
|--|------------------------|---|---|
| Securiptice | | IKE version | |
| Termiti | | HEA. | 1 |
| lucal hold | | Repute host | Dynami |
| 10.032 | | 180.033 | |
| Local ID | | Remote10 | Oynami |
| 184.03 | | 181.0.8.9 | - 54 00.00 |
| Turnel lettiatistion | | twhies with | |
| distant store | R. | Main | |
| Referringing Mathew | 14 | Shand Kee | |
| Sectory. | 1 | | |
| L Harden of C | | L'essence | |
| | | | |
| fetwork #Vector see | 9 | | |
| Local networks | | Passote antiworks | |
| 1000 | * | 4241 | + |
| | in in | | |
| ryptography | | | ÷ |
| ldvanced | | | |
| | Ninste (d | 900 Action | |
| active and a | | 1.000 | |
| avitel 24 | | Southert | |
| NC History 100 | for the set | BPD Belay | 310 |
| NE Hulus IN Ny Ilaina | Manue SI | app being | (according to the second se |
| IC Helve IN wybitne is | No.4 St | IPO Setay | i de com |
| RE Hulos IN Reyllotino In Reylig Dies | Mark SI | BPD belay | Server Server |
| NE Halas IN Any Mathema An Any Mathema In Any Mathema In Ann Ann Ann Ann Ann Ann Ann Ann Ann | No.et St | BPD Second | Score Notes |
| IC Hulos IN Reyligities Reyligities * | Marcal St | BPD Belay DB BPD Second BPD Second SE | Server Server |
| RE Hinton IN Reyking Units I Halooy margin I | Mercel 24 Mercel 24 | BPD Second DFD Second 24 | Series Neces |
| BE Hinton 100 Reyking bles 0 Reyking | No.e Si Monto Si | BPD Second | Server Neuro |

VPN IPSEC - Configurações do Tunnel 1

Repita esses passos nas duas pontas da rede. O Tunnel 2 deverá ter sido configurada conforme demonstrado pela imagem abaixo:

| A DETAILS OF DEPARTMENT | |
|-------------------------|--|
| | |
| THE PARTY OF A | |
| - V F 13 5 F 40 (c) (a) | |

| | | | | + |
|--|-----------------|--|---|-------------|
| Several | | | | * |
| becaute - | | | | |
| taraiz | | P2 PATRO | | 10 |
| Incident | | A common la compañía de la compañía | | 1 |
| 0.002 | | NEEL3 | | |
| land (B) | | Interity ID (| | |
| Link | | 10.464 | | |
| Travel Mittal Volum | | tertain mile | | |
| kinet? | 10 | No. | | 10 |
| and the second second second | | | | |
| Dentifie | 0 | manning | | |
| | - P2 | | | |
| Local Ibd. Rey | | Entroite Stat, Key | | - |
| | | | | |
| Network It Westen | | | | ^ |
| Network P Versen Invert | 8 | | | ^ |
| Natiwork Provin Invert Local componen | 8 | Norsche Cathan Abd | | • |
| Network In Version Invert Local converter | 8 | Noracla centes rito | + | • |
| Network In Version Search Local service la | 8 • • | Noracto cellas rito. | • | • |
| Natiwark Protect Local convertor | 8 | Norselle Cathain Ala | | * |
| Katavorik IV Verilen Innet Local networks | 8 • • | Normal In Contrain Plac | | • |
| Katavarik If Version Invest Invest Invest Invest Invest Invest | B • • | Noracta cetajas Ala | | * |
| Katawarik Watien Instit Instit Instit Sryptography Kahanced | | Noracle consume | | • |
| Network | | Non-stis centes risc | | • |
| Natiwork | | Nonacio companio 1994 | | • |
| Network Prese Invert Inclateneed Inclassion | | Protecto consumbo 1990 SPED Action Tenter | | * * |
| Natiwork Proving Insuit Incut ontwork Cryptingraphy Netwanced Insuit I | | BPD Action BPD Dolay | | * * |
| Network P Voien Internet Cryptography Advanced REMAN Reveal Rev | | Proveto consulto Billio Billio Billio Billio Billio Billio Billio | | * * # |
| Network Version Version Version Version Crypotographiy Advanced PE Metric Im Key Before Im Key Before Im Key Before Im | | Browsto census risk | | * * |
| Network Presen Income Company Cryptography Advanced Styptography Rey Below Styptography Later Company Styptography Later Company La | | Results colourids | | * |
| Nativoris Proving Insuit Incut optionshi Cryptingraphy Netwarkced Proving Station In Keyfegithe I Keyfegithe I Keyfegithe I I | | BFD Action BFD Datus BFD Datus IIII BFD Datus IIII IIII IIII | | * * * |
| Natiwork P Vesion Invert Inve | | Proveto comunido Billio | | · · |

Indo para o outro ponto, na UTM - Remote Office o Tunnel 1 deverá ter sido configurada conforme demonstrado pela imagem abaixo:

| Jeneral | | | ^ |
|---|-----------------------|---|---|
| Description | | RC version | |
| Termit. | | HEN. | 1 |
| tural heit | | Repute hoat | Dynamic |
| 1003.03 | | 06003 | |
| Local IB | | Benete10 | Dynamic |
| 100.0.0.0 | | Lineat | - Hel 22 (27) |
| Turnelle Ridfollor | | turbures work | |
| false de | ų. | Hain | |
| Reflective Reflect | 10 | David Kee | 14 |
| Aground about Method | 1 | Source Key | |
| District | | | |
| | | | |
| lettwork IP Venton Scient Local setworks | B | Do moto naturorilo | Ŷ |
| Contract of the second s | + | 1041 | + |
| | | | |
| | | | 0 |
| ryptography | | | |
| iyptography dvanced | | | ×. |
| iyptography dvanced Ki Bidae | Starte () | \$F0 Action | * |
| dvanced in: | Black (d | - 100 Action Scient | * |
| iyptography dvanced IX Betwe IV | Binde () | 900 Action Scient BPD Indian | |
| iyptography dvanced IX Butus IX ini | Mande (d Mande (d | BFQ Action Solut BFO belay | |
| iyptography dvanced iX Bidae ix explictne ia | Nambr (d Nambr (d | BFO Action Subst BFO belay UK | |
| iyptography dvanced ix ix ix ix ix ix ix ix ix ix ix ix ix | Nuclei)) Nuclei () | BFO Action Solut BFO belay XX BFO Second | in and a second |
| iyptography dvanced III III III III III III III III III II | Neutro) Neutro) | SPO Action Solut BPO belay IS BPO Secont St | in and a second |
| ryptography dvanced IX IX IX IX IX IX IX IX IX IX IX IX IX | March () March () | 900 Action Scient BPO belay US BPO Sereest SI | in Street |
| ityptography dvancesi iti iti iti iti iti iti iti iti iti i | Minute (d | BFO Action Solut BFO Integ III BFO Integel III | in Record Name |
| ityptography dvanced RC Bethe IN Rey bletke IN Rey bletke I Rey bletke Rey | Name (d) | BFO Action Subst BFO Inday UE DFO Incost II | in a second |

Remote Office - Configurações do Tunnel 1

| As configurações do | <i>Tunnel</i> 2 do UTM - | - Remote Office | devem ficar | conforme d | demonstrado na | a imagem | abaixo |
|---------------------|--------------------------|-----------------|-------------|------------|----------------|----------|--------|
|---------------------|--------------------------|-----------------|-------------|------------|----------------|----------|--------|

| Jeneral | | | ^ |
|--|-------------|---------------------|--------|
| Securiptice | | INC version | |
| Terrell | | HER. | 1 |
| lucal fait | | Repute host | Dynami |
| (11.5.2 | | 181,0,83 | |
| Local IB | | Benete10 | Oynomi |
| 14,823 | | 181.0.8.9 | |
| Turnel initialization | | trothings Mode | |
| distant star | 9 | Ukie | |
| Autiverlication Method | | Shaved Key | |
| Disectives | 8 | | |
| Local RSA Key | 20 | Entrete RSA Key | |
| Network | | | |
| 18 ⁴ Verators | | | |
| Scient | 8 | | |
| Local networks | | Parriote nativorila | |
| And a second sec | + | 1041 | + |
| | | | |
| Tryptography | | | ÷ |
| idvanced | | | 2 |
| 92 Bulne | Minute (a) | 900 Action | _ |
| LIN | | Ratert | 1 |
| may Maticas | Nonale SI | BPO Beby | Second |
| (a) | | 01 | |
| novingbies | | PPD Second | North |
| . e. | | 34 | |
| tulory margin | Nitrate (2) | | |
| | | | |
| * | | | |
| | | | |

Remote Office - Configurações do tun2

Após salvar cada perfil, para que o VPN entre em ação será necessário acessar a **fila de comandos [** mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.



] e aplicar as alterações efetuadas. Para

A seguir efetuaremos a adição do SD-WAN propriamente dito.

SD-WAN: Configurar SD-WAN

Após ter configurado as VPNs, siga os passos à seguir:

Mais uma vez configuraremos o UTM – HQ, acessar Services>>SD-WAN.

| Палоска | BIT I | = | | | a a ⁰ = 3 - |
|-------------|-------|--------------|-----------|-------------|-----------------------------|
| · Continued | | | | | |
| # Ange | +- | SD-WAN | | | |
| Winner | +7/ | Puller Incom | | | |
| * Prime | | | | | (a) (x) |
| < 1++++ | | Breelpher . | Fyge | (configure) | Arites |
| | | Falser | Salare - | And Aret | 2.8 |
| | = | | | | |
| | . 🕿 | | | | |
| | | | | | |
| | - | | | | |
| | | | | | |
| * 3194 | | | | | |
| | | | | | |
| | - | | | | |
| | | | | | |
| 1.000 | | | | | |
| | | | 50 14/44/ | | |

Clique no botão Add[

] para adicionar um novo perfil SD-WAN.

A seguir analisaremos cada componente do painel e apontaremos os passos específicos para a configuração do SD-WAN, para obter informações mais aprofundadas a respeito desse tópico vide o capítulo dos Tipos de Perfil.

Interfaces

Complete o formulário conforme exemplificado a seguir:

| Som Gall 1 | o cricial | | | |
|------------|-----------------------------|-------------------------|--|--|
| Monitor | * Name | | | |
| | Failover | | | |
| | Description | | | |
| | Fallover | | | |
| | * Тура | * Fail ratio (1 - 100%) | | |
| | Follower | 70 | | |
| | * Monitoring Interval (sec) | * Failback | | |
| | 1 | 5 | | |
| | interfaces | | | |
| | 11 TUNO | • | | |
| | II TUNI | • | | |
| | E ETH1+LOCAL NETWORK | a | | |
| | ETH0 | a | | |
| | 1) ETH2 | 1) ETH2 | | |
| | 11 ETH3 | ٥ | | |
| | | | | |

- Description: Definir um nome para o perfil. Ex.: Failover;
- *Type*: Neste campo se define como o *SD-WAN* irá atuar. É possível selecionar qualquer tipo, porém nesta demonstração usaremos o "*Failover*". Para mais informações a respeito dos tipos de *SD-WAN* cheque o capítulo Tipos de Perfil;
- Interfaces: É essencial para o correto funcionamento do SD-WAN definir as interfaces de link de internet que serão usadas na composição do perfil. Neste exemplo selecionaremos as interfaces: "tun0 Rede 10" e "tun1 Rede 11";
- Monitoring Interval (sec.): Definir o intervalo de monitoramento entre cada teste. É recomendável deixar como 1 segundo. Ex.: 1 segundo;
- Fail Ration 1-100%: Definir o valor da taxa de falha entre 1 a 100%. É recomendável deixar o padrão de 70%. Ex.: 70%.

Depois desta etapa, clicar na aba lateral "Monitors".

2.00

Monitors

Complete o formulário conforme exemplificado a seguir:

| Interfaces | Performance indicate | жs | | | |
|-------------|----------------------|------------|---------------|-----------|------|
| Manitor | Latency (ms) | | Jitter (ms) | | |
| - Charlense | 18 | | | | |
| | Packet Loss (%) | | Bandwidth (%) | í. | |
| | 100 | | | | |
| | Monitoring Targets | | | | |
| | * Address | * Protocol | * Attempts | • Timeout | |
| | 20.0.0.2 | ICMP ~ | 3 V | 3 and 10 | + |
| | 21.0.0.2 | ICMP V | 3 0 | Said. V | |
| | | | | | |
| | | | | Cancel | Save |
| | | | | | |

• Monitoring Targets: Define os endereços nos quais serão realizados os testes. É recomendável que nos "Monitoring Targets" sejam colocados os IPs virtuais do outro lado do túnel de modo que se a comunicação for feita com sucesso, isso indica que o Túnel está corretamente configurado. Ex.: 20.0.0.2 e 21.0.0.2.

| | Save | |
|----------------------|------|---|
| Clique no botão Save | | para salvar as configurações efetuadas. |

Repita esses passos no UTM - Remote Office a aba "Interface" deverá ter sido configurada conforme demonstrado pela imagem abaixo:

| nterfaces | General | | | | |
|-----------|---|-------------------------|--|--|--|
| Monitor | * Name | | | | |
| | Failover | | | | |
| | Description | | | | |
| | Failover | | | | |
| | * Туре | * Fail ratio (1 - 100%) | | | |
| | Follover | 70 | | | |
| | Monitoring interval (sec) | • Failback | | | |
| | ī | 5 | | | |
| | Interfaces | | | | |
| | II TUNO | | | | |
| | II TUNI | • | | | |

A aba "Monitor" deve ficar conforme demonstrado na imagem abaixo:

| SD-WAN Profile | | | | | × | |
|--|---|---|-----------------------|--------------|--------------------------|--|
| Interfaces | Performance indicators | | | | | |
| Monitor | Latency (ms) | | Jitter (ms) | | | |
| | 10 10 | | | | | |
| | Packet Loss (%) | | Bandwidth (%) | andwidth (%) | | |
| | 100 | | | | | |
| | Monitoring Targets | | | | | |
| | * Address | * Protocol * Attempts | | • Timeout | | |
| | 20.0.0.1 | ichip 🗸 | 3 V | Siec V | + | |
| | 21.0.0,1 | iewe 🗸 | 3 | Same. V | | |
| | | | | Cancel | Sawe | |
| | Remote Office - | Configurações dos <i>M</i> | onitors | | | |
| pós salvar cada perfil, para que o <i>SD-WAI</i> ara mais informações a respeito da fila de | Ventre em ação será neces comandos acesse a página | sário acessar a fila de : UTM - Fila de comar | e comandos [ndos. |] e apli | car as alterações efetua | |

Por fim é necessário criar uma política de firewall para liberar a comunicação utilizando o SD-WAN.
SD-WAN: Adicionar Policies

Após ter configurado os SD-WAN, siga os passos à seguir:

Neste exemplo será criada uma política usando IP.

Para fazer uma política usando Mac Address, cheque o capítulo Regras de NAT por Mac Address.

Por fim, será criada uma política para liberar o acesso, acesse Policies >> IPv4.

| Blockbit | = | 1 L 0 ⁶ L- |
|----------|---|-----------------------|
| | Palicies inc | |
| · terim | 612 U.S. | |
| · iter | Contraction of the second s | |
| • • | 2.5 M. Mark | |
| al lavas | - | |
| 9 mm | * | |
| A braid | | |
| | | |

IPv4 – Policies

É recomendável adicionar um grupo separado chamado "SD-WAN" de modo a isolar as políticas de SD-WAN das outras de modo a facilitar o controle, para tanto clique no ícone Add group [].

| | Create Group | × |
|---------------------------|--|------|
| | * Name | |
| | SD-WAN | |
| | Cancel | Save |
| | SD-WAN – Add group policies | |
| Após esta etapa, clique e | m Add [] para adicionar uma nova política. | |

A seguir analisaremos cada componente do painel e apontaremos os passos específicos para a configuração do SD-WAN, para mais informações a respeito de políticas cheque o capítulo Policy.

Properties

Complete o formulário conforme exemplificado a seguir:

| Propertes | бнеа | | |
|------------|----------------------------------|----------|--|
| Devision | * Narse | | |
| | NPH (GUT) | | |
| Inspection | Description | | |
| Bielog | VEHICUTI | | |
| | + Action | Tagi | |
| | Alize | | |
| | Policy Group | | |
| | 35-AWI | | |
| | Truffic Logging | | |
| | Edvadule | | |
| | Time . | Schedula | |
| | | | |

IPv4 - Policies - Properties

- Name: Adicione o nome da política. Nesta demonstração usaremos "VPN (Out)";
- Description: Insira a descrição desejada de forma a facilitar a identificação da interface política posteriormente. Nesta demonstração usaremos " VPN (Out)";
- Tags: Nenhuma tag será inserida nesta demonstração;
- Action: Como esta política serve para liberar o acesso, selecionaremos "Allow";
 Policy Group: Nesta caixa de seleção será selecionado "SD-WAN", o nome do grupo que criamos posteriormente; ٠
- ٠ Traffic logging: Nesta demonstração iremos gerar relatórios e, portanto, esta caixa de seleção será marcada.

Todas as outras opções podem ficar no padrão.

Clique na aba lateral "Conditions".

Conditions

Complete o formulário conforme exemplificado a seguir:

| Network Zone | | Betweets Interface | | | |
|----------------|--|---|---|---|---|
| | | | | Louray | |
| | | | | | |
| D Adalesca | | NACAddress | | | |
| Thisse? | Ξ | | | | |
| Declaring | | | | | |
| 📰 ID Adelron | | Service | | Country | |
| Thinnel | Ξ | | | | |
| identification | | | | | |
| Authenthated | | | | | |
| CT Parts | | | 200 | | |
| | P Address Deckington Person Person Person Person Authorston Authorston Some | P Address Deckington P Address P Address | P Address MAC Address MAC Address Decidation P Address P Add | P Address P | PAddress PACAbless PAddress PAddress |

IPv4 - Policies - Connection

- Network Zone: Esta caixa de seleção pode ficar no padrão;
- Network interface: Esta caixa de seleção pode ficar no padrão;
- Source IP Address: Deve-se marcar esta caixa de seleção e selecionar o IP que foi configurado como interface de LAN. No UTM HQ será "L ٠ AN – 172.18.0.0/16";
 Source - MAC Address: Esta regra não usará endereço físico e, portanto, não lidará com MAC Address, a seleção pode ficar padrão;
- Destination IP Address: Deve-se marcar esta caixa de seleção e selecionar o IP que foi configurado como interface Remota. No UTM HQ será "Remoto – 172.17.0.0/16";
 Service: Esta regra não lidará com serviços e, portanto, a seleção pode ficar no padrão;
- Authenticated: Esta caixa de seleção pode ficar no padrão;
- Users: Esta caixa de seleção pode ficar no padrão;
- Groups: Esta caixa de seleção pode ficar no padrão.

Clique na aba lateral "Routing".

Routing

Complete o formulário conforme exemplificado a seguir:

| Properties | Gateway | | |
|------------|--|---------------------|--|
| Conditions |) NAT | SD-WARN | |
| | Status Linna Stated | - Falterer | |
| Inspection | | | |
| Sec. | QaS | | |
| | Truffic Shaping | Fig. Padota (T08) | |
| | and the second sec | The second second | |
| | TCP MSS | Fing Packets (DSCP) | |
| | 1540 | 41 (Sec) (March | |
| | Application Reading | | |
| | III Applications | SD-WAN Profile | |
| | | | |
| | | | |
| | | | |



- SD-WAN: É essencial que este checkbox esteja marcado e que o perfil adequado seja selecionado. Conforme foi criado na sessão anterior, no nosso caso selecionaremos "Failover";
- TCP MSS: Permite definir um valor que especifica a maior quantidade de dados, especificada em bytes, que um computador ou dispositivo de comunicações pode receber em um único segmento TCP. É essencial para o correto funcionamento da SD-WAN que este checkbox esteja marcado e possua o valor 1360, desta forma o tráfego é adequado de acordo com a necessidade de cada comunicação.

Todas as outras opções podem ficar no padrão.

Clique no botão save

Save

] para registrar todas as alterações feitas.

Após estes passos, teremos chego no resultado demonstrado pela imagem abaixo:

| II - SI WAN | | | | | | | |
|---------------|---------|------|------|-------|-----|------|-------|
| 101725 | | | 1000 | 12.00 | 144 | | |
| 11 ME 494 010 | and see | - | (8) | | 1.5 | 2002 | C/81 |
| | | 1000 | 0 | | | 000 | d 104 |

IPv4 - Policies - VPN (Out)

Repita esses passos no UTM - Remote Office, conforme demonstrado abaixo:

Properties

Complete o formulário conforme feito anteriormente:

| Propertes | биеа | | |
|------------|----------------------------------|----------|--|
| Conditions | * Name | | |
| | YEN KUT | | |
| Inspection | Description | | |
| Bintry | Yell IONU | | |
| | # Action | Tagi | |
| | Alize | | |
| | Palicy Group | | |
| | 35-AVA | | |
| | Traffic Logging | | |
| | Schodule | | |
| | Time . | Schodule | |
| | | | |

IPv4 - Remote Office - Properties

Connection

Complete o formulário conforme exemplificado a seguir:

| Properties | + Beerte | | | | |
|------------|----------------|---|-------------------|----------|--|
| Constant | Network Zone | | Betwork Interface | Dourstry | |
| | | | | | |
| Inspection | 🔝 40 Adalesaa | | NAC Address | | |
| Builty | (Thinne) | Ξ | | | |
| | Declarition | | | | |
| | 📰 10 Adelrees | | Service | Country | |
| | a bernet | Ξ | | | |
| | identification | | | | |
| | Authenticated | | 12 Gen | | |
| | | | | | |

IPv4 - Remote Office - Connection

- Network Zone: Esta caixa de seleção pode ficar no padrão;
 Network interface: Esta caixa de seleção pode ficar no padrão;

- Source IP Address: Deve-se marcar esta caixa de seleção e selecionar o IP que foi configurado como interface de LAN. No UTM Remote . Office será "LAN - 172.17.0.0/16";
- Source MAC Address: Esta regra não usará endereço físico e, portanto, não lidará com MAC Address, a seleção pode ficar padrão;
- Destination IP Address: Deve-se marcar esta caixa de seleção e selecionar o IP que foi configurado como interface Remota. No UTM Remo te Office será "Remota - 172.18.0.0/16";
- ٠ Service: Esta regra não lidará com serviços e, portanto, a seleção pode ficar no padrão;
- Authenticated: Esta caixa de seleção pode ficar no padrão;
- Users: Esta caixa de seleção pode ficar no padrão;
- Groups: Esta caixa de seleção pode ficar no padrão. ٠

Routing

1 ME 474 DAD

Complete o formulário conforme feito anteriormente:

| Property and | alaria) | | |
|--------------------------|-----------------------|---------------------------------------|--------|
| 110000.000 | oscewey | | |
| Conditions | hant | SD-WARN | |
| | Indust Lineage Stated | Salana | |
| Inspection | | | |
| Bastrop | ψa | | |
| | Truffic Shaping | Flag Pedecta (T0%) | |
| | | (a) consistent | |
| | TCP MSS | Fing Packets (DSCP) | |
| | 1540 | 412412701 | |
| | Application Reating | | |
| | III Applications | SD-WAN Profile | |
| | | | |
| | | | Carcal |
| | | | |
| | IPv4 – R | emote Office - Security | |
| e no botão save [| <i>IPv4 − R</i> | emote Office - Security es feitas. | |

IPv4 - Remote Office - Policies

unity Ameri

10

0/80

Após a criação dessa política, é possível criar outras controlando o acesso, de acordo com as necessidades, porém é recomendável colocá-las no mesmo grupo "SD-WAN" e levar em consideração a política de "First Match Wins", conforme exemplificado pela imagem abaixo, para mais informações cheque o capítulo Policy.

| IT & SERVICE | | | | | |
|----------------------|---|------------------|------------|------|--------------------|
| 10.75 | | 1.1.2 | 100100 | | and the second |
| 1 (IR) Aroso Sort of | - | 10/2000 (Million | 0 | | 0/20 |

IPv4 – Policies – Controle de Acesso

Isso conclui a configuração do SD-WAN.

SD-WAN Regras de NAT por Mac Address

No exemplo demonstrado em SD-WAN: Adicionar Policies, foi criada uma política de *IP*, porém, considerando que se deseja criar uma política por *mac* address, é obrigatório configurar também a zona de rede, interface ou endereço de origem (também é possível configurar mais do que apenas uma destas opções). Segue uma demonstração:

Gerando objeto Mac Address

No menu lateral acesse "Settings" e selecione a opção "Objects".



Já em "Objects", selecione a aba "Addresses".

| | Addresses | Services | Times | Schedules | Dictionaries | Contents | | |
|--------------------------------|---------------------|--------------|----------------------------------|---------------------|--------------------|---------------------|--|--|
| Settings - Objects - Addresses | | | | | | | | |
| | | | | | | | | |
| Crie um novo objeto de n | nac address clicand | lo no botão[|] a seguinte | janela será exibida | e complete o formu | llário conforme exe | | |

Create Addresses Object

| | * Name | | | | |
|--|--|--|--|-----------------------------------|---------|
| | Mac Address object | for Nat policy | | | |
| | * Туре | | | | |
| | MAC Address | | <pre></pre> | Unique | |
| | * Address | | | | |
| | | | | + | |
| | 38:15:3D:19:E2:1E | | | — | |
| | Description | | | | |
| | Mac Address object | for Nat policy | | | |
| | | Cancel | Import Address | Save | |
| L | | Novo objeto Mac A | Address | - | |
| Name: Digite o nor Mac address: Dig na lista e clique no Description: Digit | me do objeto Mac Address. ite o endereço físico e clique botão [] para remov e a descrição do seu objeto. | Ex.: Mac Address object for a no botão [] para ad er. Ex.: 38:15:3d:19:e2:1e; Ex.: Mac Address object for | Nat policy icioná-lo na lista. Caso des ^r Nat policy <i>;</i> | eje remover um Mac Address, selec | xione-o |

 \times

Para mais informações sobre como lidar com objetos, cheque o capítulo Settings - Objects.

Save Por fim, clique no botão Save [] para finalizar a operação.

Criando a política de Mac Address

No menu lateral acesse "Policies" e selecione a opção "IPv4".



Selecione o grupo onde se deseja criar a política, neste exemplo, usaremos o grupo "Default".

| S 37212 | | | | | | | 1000 |
|-------------|----------|------|----|-----|-------|-----------|-------|
| | | | | | _ | | |
| INC Details | 1.00 | 1.00 | 12 | | 11.00 | 2020232 | 0/48 |
| | | | 0 | 1.1 | | 205205205 | 4.494 |

Clique na opção Create Policy do Menu de ações para criar uma nova política. Complete o formulário conforme exemplificado a seguir:

| Propertea | 0nieal | | |
|-----------|-----------------|----------|--|
| Charliner | * Hang | | |
| | NAT-Noc.Aberes | | |
| Importion | Description | | |
| | NAT-Moc/Address | | |
| many. | * Artico | Taos | |
| | Nor | 1491 | |
| | • Policy Group | | |
| | Dehuit | | |
| | Traffic Logging | | |
| | Schodule | | |
| | Time . | Schedula | |
| | | | |
| | | | |

- Name: Digite o nome da sua política. Ex.: NAT Mac Address;
 Description: Digite a descrição da sua política: Ex.: NAT Mac Address;
- Action: Allow;
- Policy Group: Default;
- Traffic Logging: Enabled.

O resto das opções podem continuar como com os valores padrão.

Selecione a opção "Conditions" no menu lateral.

| Properties | + Seurce | | | | |
|------------|----------------|-------------------|--------|----------|--|
| Conditions | Metwork Zone | Retwork Interface | | Lountry | |
| | SAN | | | | |
| Inspection | 10 Adalescus | MACAddress | | | |
| Nativy | | | | | |
| | Declaring | | | | |
| | D IP Address | Service | | Dourstry | |
| | | | | | |
| | identification | | | | |
| | Authentikated | | George | | |
| | | | | | |

- Network Zone: LAN;
 MAC Address: Selecione o endereço físico, adicionado previamente, conforme demonstrado abaixo:

Add MAC Address



Х

| | Cancel | Save |
|--|-------------------------|------|
| Policies - New Po | olicy - Add Mac Address | |
| Neste próximo passo, é importante atentar que: | | |

Para complementar o Mac Address é obrigatório configurar também uma ou mais das opções a seguir:

- Network Zone;
- Network Interface;
- IP Address.

Dando continuidade ao nosso exemplo, simplesmente selecionaremos a opção "LAN" na caixa de seleção "Network Zone".

O resto das opções podem continuar como com os valores padrão.

Clique no **botão** [] para salvar a política.

| in v faciali | | | | | | 5.00 |
|---------------------|-----|---|---|-------|------|------|
| ALC: 100 | 100 | | | | | - |
| 1 18 Hill Jackstree | ~ | 1400 Han Address planet for Histophys | - | 2 | | 0160 |

Policy - NAT - Mac Address

Para mais informações sobre como lidar com políticas, cheque o capítulo UTM - POLICIES.

Isso conclui a criação da regra de NAT para Mac Address.

SD-WAN: Validação da Configuração do SD-WAN

Um dos testes mais simples para validar o funcionamento do *SD-WAN* é efetuar um *ping* da rede 172.31.208.40 para a 172.31.208.41, conforme demonstrado pela imagem a seguir:

admin >ping 172.31.208.41
PING 172.31.208.41 (172.31.208.41) 56(84) bytes of data.
64 bytes from 172.31.208.41: icmp_seq=1 ttl=64 time=0.214 ms
64 bytes from 172.31.208.41: icmp_seq=2 ttl=64 time=0.094 ms
64 bytes from 172.31.208.41: icmp_seq=3 ttl=64 time=0.163 ms
64 bytes from 172.31.208.41: icmp_seq=4 ttl=64 time=0.162 ms
--- 172.31.208.41 ping statistics --4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.094/0.158/0.214/0.043 ms
admin >

Validação por Ping

Além disso, é possível derrubar propositalmente o link que está sendo utilizado pelo SD-WAN com objetivo de checar se o Failover irá assumir a interface corretamente.

Conforme anteriormente configurado, no UTM - HQ a interface com prioridade no SD-WAN é a "tun1 – Rede 11", assim sendo, remova o cabo de rede de forma a interromper a comunicação do dispositivo.

Na janela de notificações, será possível observar o alerta exibido, conforme exibido na imagem a seguir.

| Noti | ifications | | | > | K |
|------|------------------|--------------|---|------|---|
| | 20-02-2019 15:09 | Link inativo | O perfil de SD-WAN Failover identificou que o link da interface tun1 está inativo (utm-a) | • 1 | ^ |
| | 18-02-2019 15:38 | Link ativo | | 0 | |
| | 18-02-2019 15:12 | Link inativo | | 0 | |
| | 18-02-2019 03:42 | Link ativo | | 0 | |
| | 18-02-2019 03:31 | Link inativo | | 0 | |
| | 16-02-2019 12:34 | Link ativo | | 0 | |
| | 16-02-2019 12:32 | Link inativo | | 0 | |
| | 16-02-2019 12:24 | Link ativo | | 0 | |
| | 16-02-2019 12:24 | Link ativo | | 0 | |
| | 16-02-2019 12:22 | Link inativo | | 0 | |
| | 16-02-2019 12:21 | Link ativo | | 0 | ~ |
| | | | C | lear | |

Notifications

Além disso, acesse Services>>SD-WAN e clique no botão edit [], será possível observar que a interface tunnel1 está com o status offline [Offline], conforme demonstrado na imagem abaixo.

| Edit profile | | | | | | |
|--------------|----------------------------|-----|--------------------|----------|------|----------|
| | Description | | | Type | | |
| interfaces | Falaner | | | fationer | | - |
| Mandran | Interfaces | | | | | Show all |
| | H Tonit - Rodo 11 | | | | (11) | 0 |
| | İİ turdi - Rodu 10 | | | | 0 | C |
| | Manitoring innerval (sec.) | | Failt ratio 1-106% | | | |
| | 1 | (B) | 78 | | | (2) |



Também é possível observar os efeitos desta alteração através da CLI utilizando o comando debug-sdwan -i results.



CLI - Tunnel 1 offline

O parâmetro "weight" demonstra um valor de 100% para tun0 e um valor de 0% para tun1, assim sendo a interface tun0 está com uma prioridade maior do que a tun1, o que comprova que o "failover" funcionou corretamente.

NGFW - Serviços - DHCP

Gerenciador do protocolo DHCP (RFC2131 IPv4 e RFC3315 IPv6) que atua sobre camada de aplicação nas portas padrões do DHCP 67/68 UDP (IPv4) e 546/547 UDP (IPv6). Numa rede de arquitetura TCP/IP, todo computador tem que possuir um endereço IP distinto. O DHCP (Dynamic Host Configuration Protocol) é o protocolo que provê um meio para alocar estes endereços dinamicamente.

O DHCP é responsável por distribuir os endereçamentos *IP* e configurações de rede para seu ambiente corporativo. É uma eficiente solução já que, por meio dele, o servidor BLOCKBIT UTM distribui endereços *IP* na medida em que os dispositivos da rede solicitam conexão. É importante frisar que, além do endereço *IP*, também atribui outros parâmetros, tais como: nome do *host, DNS*, rota *default*.

Recursos do DHCP:

(1)

- Distribuição de endereços IP por device / por servidor:
 - Ethernet,
 - Vlan;
 - Mac Vlan (device de endereçamento virtual);
- Distribuição de endereços IP por rede / sub-rede;
- Políticas para distribuição de endereço IP;
- Suporte a autenticação por servidor Radius.
- Modelos:
 - Distribuição por faixa (range);
 - Distribuição de endereços estáticos. (reserva de endereço de IP por filtro MAC).
- Filtros:
 - MAC;
 - Host.
- Parâmetros:
 - Gateway;
 - Sufixo DNS;
 - Múltiplos DNS;
 - Múltiplos Wins;
 - TTL Tempo de renovação (tempo de vida).

Para o uso do serviço de DHCP com IPv6 é necessário configurar uma regra de Zone Protection liberando as portas 546/547 UDP, permitindo que o firewall libere o tráfego de entrada.

Para acessar a tela do DHCP, selecione a opção conforme demonstrado na imagem abaixo:

| 0 8 | Services | ~ |
|------------|----------------------|---|
| » | Firewall | C |
| » | Proxy | Ο |
| » | Web Cache | Ο |
| » | Web Filter | Ο |
| » | Application Control | Ο |
| » | Intrusion Prevention | Ο |
| » | Threat Protection | Ο |
| » | SD-WAN | Ο |
| » | DHCP | |
| » | DNS | Ο |
| » | DDNS | Ο |
| » | VPN IPSEC | Ο |
| » | VPN SSL | Ο |
| | Serviços - DHCP | |

A seguinte tela será exibida:



DHCP

A seguir, explicaremos as demais abas da interface DHCP em detalhe:

- Server IPv4;
 Server IPv6;
 Relay IPv4;
 Relay IPv6;
 Leases IPv4;
 Leases IPv6;

DHCP - Aba Leases IPv4

Este recurso permite ao administrador visualizar os hostnames, MacAddress, Usuários, endereços IP e a Data do recebimento do IP distribuídos pelo servidor DHCP do Blockbit UTM.

Para visualizar esta janela, clique na aba "Leases", como demonstrado abaixo.



Aba Leases

Surgirá a tela a seguir:

| HCP | | | | |
|-------------------|-------------------|----------|----------------|--------------------|
| erver Relay Lease | | | | |
| Hostname | MAG | User | 19 | Date |
| - | 00.0C19-382CISA | | 172.16.102.113 | 27/02/2020 - 06:55 |
| utm-05 | 00:06:AB:F2:CF(74 | 8 | 173.16.102.137 | 17/02/2020 - 14:53 |
| injetor200 | 00:00:AB:04:00:10 | 8 | 172.16.142.139 | 37/03/2020 - 36:32 |
| bps_vblade | 00.00191387:00 | | 172-16-102-138 | 27/02/2020 - 17;37 |
| | 047EIEEADACE | | 172.06.100.111 | 21/02/2020 - DE114 |
| | 00:00:29:80:06:54 | | 172.10.100.191 | 27/02/2020 - 11:29 |
| | 00:0C:19:E0:C3:8E | 12 | 172.16.100.249 | 31/02/2020 - 13:42 |
| | 00:00:39:80:50:73 | £2 | 172.16.100.244 | 33/02/2820 - 12:15 |
| | 76/28/C8/C4/E7/96 | 5 | 172.16.100.242 | 27002/2920 - 12:59 |
| งหม | ORIOG2728EALISC | 100 | 172.18.100.217 | 21/02/2020 - 13545 |
| | B4:78:EB:E4:D8:C4 | 10 | 172.36.100.258 | 31002/2020 - 34:35 |
| | 8478±8FC17:54 | E. | 172.16.100.144 | 27/02/2020 - 15:00 |
| | 00194596-42586:70 | | 172.14.100.243 | 21/02/2020-15:05 |
| | BC/AE/CS/85/33/74 | 8 | 172.16.100.118 | 27/02/2020 - 15:21 |
| kati | 08:00:27:17:62:1C | b | 172.16.105.136 | 27/02/2020-15:56 |
| | 64c3Cr67:70x49;01 | | 172.16.106.173 | 21/02/2020 - 16:02 |
| bps_vblade | 00.00193989940983 | | 172.31.250.162 | 23/02/2020 - 06:00 |
| | 00:00-29:46:42:A4 | - 19 C | 172.31.290.209 | 31/02/2020 - 17:51 |
| | 00.0C/29/F3/80/05 | 6. | 17231259.211 | 27/02/2020 - 06:42 |
| localhinit. | 00:00:29:76:48:06 | <u>ی</u> | 172.31.290.138 | 21/02/2020 - Dé:58 |
| | 00:90:27;ED:62:20 | 18. | 172.31.299.108 | 27/02/2020-05:44 |
| | 00.0039.403652 | 15 | 172.31.250.215 | 27/02/2020-11:57 |
| | 00:0C-29:E7:F5FB | 8 | 172.31.286.217 | 37/03/2828-13:46 |
| | 00.0029/83/98/20 | 8 | 172.31.250.193 | 37/02/2020 - 12/53 |
| atm | 00.0029.70.13.08 | | 172.31.290.213 | 27/02/2020 - 14:55 |
| | 00:0C:19:CD:94:4F | | 172.31.259.167 | 27/02/2920 - 17:15 |
| | | | | |

DHCP - Leases

DHCP - Aba Leases IPv6

Este recurso permite ao administrador visualizar os hostnames, MacAddresses, Usuários, endereços IP e a Data do recebimento do IP distribuídos pelo servidor DHCP do Blockbit UTM.

Para visualizar esta janela, clique na aba "Leases", como demonstrado abaixo.

| Server | Relay | Leases | |
|--------|-------|--------|--|
| | | | |

Aba Leases

Surgirá a tela a seguir:

DHCP

| | and the | | |
|--------|---------|---------|--|
| Server | Heley | Leature | |

| Hostmarne | HAC | User | 19 | Date |
|-----------|--------------------|----------|----------------|--------------------|
| | 00.0C29-382C/8A | 1 K. | 172.56.102.118 | 27/02/2020 - 06:55 |
| tm-05 | 00/08:AB(F2:CF(74 | 8 | 172.16.102.137 | 17/02/2020 - 14/53 |
| ijetor200 | 00:50:A2:04:50:10 | 8 | 172.16.102.139 | 37/03/2020 - 38:32 |
| ps_vblade | 00.0029.13.87×0 | | 172.10.102.138 | 27/02/2020 - 17;37 |
| | 64/EEEEADACE | 2 | 172.16.100.111 | 21/02/2020 - 06:14 |
| | 00:00:29:83:06:34 | <u>1</u> | 172-10-100-191 | 27/02/2020 - 11:25 |
| | 00:0C:19:E0:C1:RE | 1. D | 172.16.100.249 | 31/02/2020 - 13:42 |
| | 00:00:29:60:50:73 | <u>e</u> | 172.10.101.244 | 33/02/2620 - 12:35 |
| | 76/28/C8/C4/E7/#6 | 5 | 172.16.100.242 | 27/02/2920 - 12:55 |
| ни | OEDU2735EA136C | | 172.16.101.217 | 21/02/2020 - 13545 |
| | 84:78:EBtE4:D8t(A | 19 | 172.36.100.258 | 21/02/2020 - 34:35 |
| | 84/78/EB/FC:17:F4 | E. | 172.16.100.144 | 27/02/2820 - 15:00 |
| | 00:96:56:43:88:70 | | 172.14.100.243 | 31/03/2020-15:55 |
| | BC/AE/CS/95/33/74 | 8 | 172.16.105.118 | 27/02/2020 - 15/21 |
| ali | 08:50:27:17:52:1C | <u>1</u> | 172.10.100.130 | 27/02/2020 - 15:55 |
| | 64:10:67:70:49:01 | 2 | 172.16.106.173 | 21/02/2020 - 36:02 |
| gs_vblade | 00.001299.89540303 | | 172.31.250.162 | 27/02/2000 - 06:00 |
| | 00:0C-29-0E-05-A4 | 19 19 | 172.31.290.209 | 37/02/2028 - 17:51 |
| | 00.0C(29.F3(80.05 | £2 | 172.31.250.211 | 27/02/2020 - 06:42 |
| ocalhost | 00:00:29:70:40:06 | 19 C | 172.31.290.138 | 21/02/2038 - D6:58 |
| | 00:90:27;ED:62;20 | | 172.31.259.108 | 27/02/2020 - 09:44 |
| | 00.00298.4036652 | 5) | 172.31.398.218 | 27/02/2020-11:37 |
| | 00:0C-39:67:F%FR | 10 - C | 172.31.295.317 | 37/03/2828-12:48 |
| | 00/00/20/83/98/20 | 8 | 172.31.350.193 | 17/02/2020 - 12151 |
| tern (| 00.00-29.70-15.08 | £. | 172.31.295.213 | 27/02/2020 - 34:55 |
| | 00.0C:19.CD:94.4F | 20 | 172.31.259.107 | 27/02/2920 - 17:15 |

DHCP - Leases

DHCP - Aba Relay IPv4

DHCP Relay (RFC3046) funciona como um proxy que recebe uma requisição DHCP e retransmite para um servidor DHCP real. Isso permite que múltiplas redes segmentadas em barramentos separados possam centralizar as requisições de DHCP através do Blockbit UTM.

Este recurso permite que as requisições enviadas pelos clientes DHCP via broadcast sejam encaminhados e entregues ao servidor DHCP localizado em outro segmento da rede.

Clique na aba "Relay", como demonstrado abaixo.



Surgirá a tela a seguir, conforme demonstrado pela imagem abaixo:

| mi Noky Liam | |
|---------------|------|
| | |
| terbin Serven | 4:16 |
| | |
| | |
| | |

DHCP - Aba Relay

Para adicionar uma configuração de *relay*, clique em [_____] e selecione a *Interface* de rede que o serviço irá ser carregado e o *IPv4 Servers* endereço *IF* do serviço de *DHCP*.

| - | Edtir relay × | |
|---------------------------------|--|--|
| | * Interface | |
| | eth1 ~ | |
| | * IPv4 Servers | |
| | 172.31.102.184 × Add tag | |
| | | |
| _ | 🖺 Save | |
| | DHCP - Aba Relay - Add Relay | |
| O campo / | IPv4 aceita objetos únicos de endereço, para mais informações cheque a página de criação de Address Objects. | |
| Depois clique em [• Leases. | Save para concluir as alterações . | |

DHCP - Aba Relay IPv6

DHCP Relay (RFC3315) funciona como um proxy que recebe uma requisição DHCP e retransmite para um servidor DHCP real. Isso permite que múltiplas redes segmentadas em barramentos separados possam centralizar as requisições de DHCP através do Blockbit NGFW.

Este recurso permite que as requisições enviadas pelos clientes DHCP via broadcast sejam encaminhados e entregues ao servidor DHCP localizado em outro segmento da rede.

Clique na aba "Relay", como demonstrado abaixo.



Surgirá a tela a seguir, conforme demonstrado pela imagem abaixo:

| Interface | Servers | Action |
|-----------|---------------------------------------|--------|
| eth3 | 172.16.196.2 • 2001:stafesci0.be82 | × a |
| ethi | 17216.199.2 • 2001stafeac10sbe02 | × 8 |
| ethi | 172.18.196.2 * 2001:rsfwsc10:be02 | ~ 0 |

DHCP - Aba Relay

Para adicionar uma configuração de *relay*, clique em [_____] e selecione a *Interface* de rede que o serviço irá ser carregado e o *IPv4 Servers* endereço *IF* do serviço de *DHCP*.

Edit relay • Interface • IPV6 Servers 2001ccafeac10b602 • Adicioner TAG Contros feace10b602 • Adicioner TAG Con

Depois clique em [

] para concluir as alterações .

• Leases.

🖹 Save

DHCP - Aba Server IPv4

Para configurar os servidores de DHCP, IPv4 e IPv6 selecione a aba correta:



Surgirá a tela a seguir, conforme demonstrado pela imagem abaixo:

| DHCP | | |
|---------------------------------|--|----|
| Server | Palay Launds | |
| | + | |
| | DHCP - Server | |
| Para adicionar <i>IPv4</i> . | uma política de DHCP, clique em [], e selecione um Device para distribuição de endereços IP na rede. Note que o default Type ser | rá |

| Enable DHCP | × |
|--|------------------------|
| Interfaces | |
| ethD | ~ |
| Туре | |
| IPv4 | ~ |
| | |
| | |
| | Save |
| DHC | P - Server - Edit Host |
| Após finalizar as configurações, clique no botão []. | |

Após salvar a seleção do Device para distribuição dos endereços IP, o sistema retorna a interface para configuração dos parâmetros DHCP.

| sthi - 192, 168, 6, 6, 24 | € 8 | Settings Optowey Inclination DNS Suffix Intelligent | #.(; | 0 | Rangos 1923880.10 🕈 (52,3880.11 | 0/2 |
|---------------------------|-----|---|--|---------|------------------------------------|--------|
| | | Incode y data | Fathès Nese | | | |
| | | * Receival Sine | mentostiaa | Seconds | | |
| | | Secret | | | | |
| | | Static add | esses | | | + - |
| | | and i | file and the second sec | 4007 | | 14/201 |

DHCP Server

O DHCP server é o responsável por distribuir os endereçamentos *IP* e configurações de rede para seu ambiente corporativo. É uma eficiente solução já que, por meio dele, o dispositivo BLOCKBIT UTM distribui endereços *IP* na medida em que os dispositivos da rede solicitam conexão. É importante frisar que, além do endereço *IP*, atribui outros parâmetros, tais como: nome do *host, DNS* e rota *default*.

Esta aba é composta pelas seções:

- Settings;
- Ranges;
- Radius;
- Static Addresses.

A seguir analisaremos cada uma delas.

DHCP Server - Settings

 \otimes

Para configuração dos parâmetros básicos para distribuição de endereços IP, no painel Settings configure os campos de acordo o formulário e os

| | B | |
|--|---|------|
| respectivos valores e endereços que pretende distribuir como válidos para o serviço DHCP. Depois clique em [| | J. – |

O endereço de Gateway obrigatoriamente deve estar dentro do intervalo de rede ou subnet declarada no device selecionado para configuração.

| Settings | |
|---------------------------|---------|
| Gateway | |
| 192.168.0.101/32 | 0 |
| DNS Suffix | |
| utm101.com | |
| DNS | |
| 172.16.13.246 | |
| Secondary dns IP address | |
| WINS | |
| Primary WINS IP address | |
| Secondary WINS IP address | |
| * Renewal time | Seconds |
| 86400 | |
| RADIUS Authentication | |
| IP | |
| | |
| Secret | |
| | |
| | |

DHCP - Settings

Em seguida ao clicar em salvar [_____] os parâmetros de configurações do *DHCP* o serviço pergunta se você deseja definir o *Range* de endereços que irá distribuir:

| Want to | add a range? |
|---------|--------------|
| ОК | Cancelar |

DHCP - Adding a range

OK Ao clicar em [

) você será automaticamente redirecionado para a interface de configurações do range.

A seguir, analisaremos as próximas seções:

- Ranges; Radius; Static Addresses.

DHCP Server - Ranges

Nesta parte, você define qual o "range" ou "intervalo" de endereços IP que pretende distribuir pelo serviço DHCP.

| | | F. | |
|--|---|----|-------------------------------------|
| Para adicionar um "range" ou "intervalo" de endereço IP, clique em [| _ | |], e configure os campos de acordo. |

S intervalos "inicial e final" do range ou intervalo dos endereços IP obrigatoriamente devem estar dentro do intervalo de rede ou subnet declarada no device selecionado para configuração.

| Range | * Initial range | |
|----------|----------------------|--|
| | 192.166.254.51 | |
| Settings | * Range end | |
| | 192,168.254.179 | |
| | MAC Filter | |
| | Select | |
| | * Description | |
| | Banges for all users | |
| | | |

- Initial Range: Determina o endereço do primeiro IP no intervalo do range. Ex.: 192.168.254.51;
- Range end: Define o endereço do último IP no intervalo do range. Ex.: 192.168.254.179;
- MAC Filter: Este recurso tem como função a distribuição dos endereços IP do range (que foi determinado nas opções anteriores) para todos os dispositivos que tiverem seu MAC Address listados neste campo;
- **Description:** Uma breve descrição definindo o range de IP.

| | Range | Gateway | |
|---|---|---|--------|
| | Settings | IP eth2 | 0 |
| | | DNS Suffix | |
| | | blockbit.com | |
| | | DNS | |
| | | 192.168.254.184 | |
| | | Secondary dns IP address | |
| | | WINS | |
| | | Primary WINS IP address | |
| | | Secondary WINS IP address | |
| | | * Renewal time | Second |
| | | 3600 | |
| e. | | Add Range - Settings | Save |
| Gateway: Det DNS Suffix: D DNS: Determi WINS: Define Renewal time | termina o gateway do ra Define o sufixo DNS do ina o endereço primário o endereço primário e e: Tempo em segundos | ange. Ex.: 192.168.254.190/32; range. Ex.: blockbit.com; e secundário do <i>DNS</i> . Ex.: 192.168.254.184; secundário do servidor <i>WINS</i> ; para a renovação do intervalo de <i>IPs</i> . Ex.: 3600. | |
| or fim, clique no botão | Save o Save[] pa | ara finalizar a criação do <i>range</i> . | |
| | Dam | | |

20 20

0 🖋 🛍

192.168.102.51 > 192.168.102.179

Ranges

A seguir, analisaremos as demais abas:

- Radius; Static Addresses.

DHCP Server - Radius

Autenticação DHCP por servidor RADIUS

Em termos de autenticação, também é possível configurar um servidor RADIUS para a validação de usuários.

Quando o DHCP + Radius está ativado, a Estação faz o pedido de endereço IP ao UTM no Serviço DHCP. O UTM consulta se existe entrada estática para essa Estação (através do MAC Address), em caso positivo, entrega o endereço reservado; caso contrário não o faz.

Sumarizando, o UTM consulta o Servidor Radius integrado, caso o Servidor Radius autorize, o UTM entrega o endereço IP do range; caso contrário, não fornece endereço IP e a máquina não recebe o endereço, ficando sem acesso a rede.

Esta opção pode ser habilitada em Services, Firewall na aba Zone Protection:

| HE TWORK STELLAST | Firewall | | | | | | |
|-------------------|----------------|-------------|--|------|-------------|----------|---------|
| A meter | Jone Protester | Partrenates | a Orent Streep | | | | |
| let traiger | | | | | | | |
| • Halon | | | 200 | 14 | | 1000 | |
| C Sentro - | | Description | Service | Dava | Arbentistat | mpetion | Actions |
| · reside | 0.4 | 10+12 | Direction of the second s | ALL | | STATES - | |

Para tal, é necessário criar uma política em Zone Protection e selecionar "DHCP" entre as opções:

| Conditions | * Description DHCP | | | | |
|------------|-----------------------|-----------------|-----|--|--|
| | | | | | |
| | | , briter | ALL | | |
| | Administration | Action | | | |
| | AH | Albw | 19. | | |
| | AOL Authentication | Traffic Logging | | | |
| | BGP | | | | |
| | DHCP | | | | |
| | DHCPV8 | | | | |

A seguir, devemos clicar na opção DHCP em Services e habilitar a opção RADIUS Authentication:

| Blockbit ≡ | | R 4 0 1. |
|---------------|-----------------------------------|----------|
| | Secondary With Life and Secondary | |
| A meter 1 | * Reserval three Seconds | |
| Let revisor 1 | V REEKS Antheretication | |
| 👟 felana 👘 | | |
| et james | 1 | |
| • damii 🗢 | Scott | 1 |
| e mer 🔍 | | |

Tela de inserção de usuário e senha do servidor RADIUS.

A seguinte mensagem será exibida, devemos clicar em OK:

0

Attention! Changing the DHCP server can lead to IP conflict.

ОК

É importante lembrar que o usuário no Servidor Radius (campo IP) deve ser o MAC address:

| 0 | ✓ Username | V THE time | C Total time left | V Actual crofile | |
|----------|--------------------|------------|-------------------|------------------|--|
| | 00:50:40:31:05:55 | Unimited | Linimited | DetCit | |
| 0 | 00:90:27:6F:70:F5 | betimited | lininited | DHCP | |
| <u>.</u> | 08/90129 28:38:88 | Unlimited | Unlimited. | OHCP | |
| 1 | 801471881191A51A7 | Unlimited | unlimited | DHCP | |
| 0. | 00-06:00:01:37:31 | Unimited | Unlistated | DHCP | |
| 0 | D4:60:60:1C:C0:60 | Unimited | Unlimited | DHCF | |
| 0 | BA:FE:98:FD:90:34 | Unlimited | Linlimited | DHCP | |
| 0 | 74:83:C2:40:84:2C | Unlimited | Linfanited. | 04CP | |
| 0 | 48:89/E7:C5:05:44 | Unlimited | Unlimited | DHCP | |
| 0 | 810401104101001AD | Unitrictad | Universitad | (CHO) | |
| 0 | 79-55:53:93:A7:A5 | Unlimited | Unimited | DHCP | |
| 0 | F0:0F:EC:All:EF:31 | Unimited | Unlamibed. | DHCP | |
| 07 | 56:50:32:86:25:00 | Unlimited | UnBritised | DHCP | |
| <u>.</u> | SC:CD:SB:E0:E4:BA | Unlimited | Unlimited | DHCP | |
| | P0(64)A2(14)S6(4A | Unlimited | Unlimited | IDHCP | |

Exemplo de tela inicial de servidor Radius.
| User details | × |
|---|---|
| ▲ Main | |
| Username: 00:E0:4C:11:0F:5E | |
| Password: | _ |
| Disabled: | |
| Owner: admin | |
| ✓ Constraints | |
| ▼ Wireless | |
| ✓ Private information ✓ Statistics | |
| ▼ Bill | |
| + DHCP | ~ |
| Chave accession 2 Street | - |
| Show sessions Save | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Exemplo de detalhes do usuário.

Finalmente, basta inserir o usuário e senha e a autenticação por servidor RADIUS do DHCP estará habilitada.

Próxima seção:

• Static Addresses.

DHCP Server - Static Addresses

O serviço ainda dispõe do recurso de distribuir endereços no modo estático, ou seja, fixando o mesmo "Endereço IP" para determinado "host", a partir da identificação do seu "endereço MAC".



DHCP reserve static address example 1

Host: NFS_CentOS7;
IP Address: 192.168.254.202;
MAC Address: 42:69:4C:3F:00.

| Edit Host | | | |
|--------------------|-------------------------|-------------------|--------|
| * Host | | | |
| NFS-CentOS7 | | | |
| * IP Address | | | |
| 192.168.102.202/32 | | | 0 |
| * MAC address | | | |
| 42:69:4C:9C:3F:00 | | | 0 |
| | | | B Save |
| | DHCP reserve static add | ress example 2 | |
| Static addresses | | | + |
| Host | IP Address | MAC address | Actio |
| NFS-CentOS7 | 192.168-102.202 | 42:69:4C:9C3F:00 | / 0 |
| WinXen2012 | 192,168,102,190 | 90:B1:1C:F6:2F:F2 | |

7

Static addresses definition

Importar múltiplos Hosts



| + - |
|----------------------|
| Import |
| Select Select all |
| Remove |

Import multiple hosts

Em import, teremos a seguinte tela:

Importar Endereços Estáticos

* Upload

Import Download Modelo

 \times

Em Download Model, há um modelo de como o documento contendo os múltiplos Hosts para importação deve estar. Basta inserir as informações dos Hosts de acordo com o modelo, salvar e clicar em "Select File". Por meio da navegação selecione o arquivo contendo as informações dos Hosts e clique em Import.

Para habilitar a distribuição automática dos endereços declarados no serviço DHCP, clique em habilitar [

A seguir analisaremos as demais abas:

- Relay;
- Leases.

DHCP - Aba Server IPv6

Para configurar os servidores de DHCP, IPv4 e IPv6 selecione a aba correta:



Surgirá a tela a seguir, conforme demonstrado pela imagem abaixo:

| | | | + |
|--|---|---|------------------|
| | DHCP - Server | | |
| Para adicionar uma IPv4. Abra a lista e | a política de <i>DHCP</i> , clique em [], e selecione um Device para distribuiçã selecione o IPv6. | ão de endereços <i>IP</i> na rede. Note que o default 7 | <i>Type</i> será |
| | Enable DHCP | × | |
| | Interfaces | | |
| | eth: | ~ | |
| | Туре | | |
| | Pré | ~ | |
| | | Save | |
| | 12 L | 14 | |

Após salvar a seleção do Device para distribuição dos endereços IP, o sistema retorna a interface para configuração dos parâmetros DHCP.

| 400 0.0100000 | | Settings | | | flarges | |
|---------------|-----|--|--------|--------|-----------------------------------|-------|
| NO HEIMSING | C 1 | Andresia | | | Introduction and the Introduction | 878 |
| iono anaque | 6.5 | - | ÷ | 0 | | |
| | | 045 Suffix | | | | |
| | | (a) dation | | | | |
| | | 190 | | | | |
| | | 2012/01/01 | | | | |
| | | 2012/02/02/02/02 | | | | |
| | | ** becould trive | | - | | |
| | | and . | | | | |
| | | RADA'S Automation | i din | | | |
| | | | | | | |
| | | | | | | |
| | | Secur | | | | |
| | | | | | | |
| | | | | | | |
| | | Salt: attrout | | | | + - |
| | | and the second s | PARTIE | som-ad | ins. | Aller |
| | | | | Tables | arbant. | |
| | | | | | | |

DHCP Server

O DHCP server é o responsável por distribuir os endereçamentos IP e configurações de rede para seu ambiente corporativo. É uma eficiente solução já que, por meio dele, o dispositivo BLOCKBIT UTM distribui endereços IP na medida em que os dispositivos da rede solicitam conexão. É importante frisar que, além do endereço IP, atribui outros parâmetros, tais como: nome do host, DNS e rota default.

Esta aba é composta pelas seções:

- Settings;
- Ranges;
- •
- Radius; Static Addresses. ٠

A seguir analisaremos cada uma delas.

UTM - Services - DNS

O Serviço de DNS (Domain Name System) é o responsável em fornecer o recurso de "tradução de nomes de domínios" para seus respectivos endereços la

O Blockbit UTM fornece o serviço de redirecionamento de *DNS* para outros servidores *DNS* recursivos, responsável por receber as consultas *DNS* de clientes *DNS* locais e consultar os servidores remotos ou externos, de modo a obter respostas às consultas efetuadas de qualquer domínio e responder aos clientes locais.

O serviço DNS conta com a integração ao recurso de Caching, lida com as consultas dos clientes DNS e armazena a resposta em seu cache local por um determinado tempo permitido pelo TTL dos respectivos registros dos domínios consultados. O Cache é usado como uma fonte para os próximos pedidos, a fim de otimizar o tempo de busca das próximas requisições de domínios já pesquisados.

Para acessar esta tela, basta selecionar a opção "DNS".



Services - DNS

A tela abaixo será exibida:

| 8 | Redirect | |
|---|----------|------------|
| | | |
| • | | |
| | | |
| + | | y cheta |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| + | | |
| | n + | * Redirect |

Services - Interface DNS

A interface DNS está dividida nos painéis:

- Settings;Redirect.

A seguir analisaremos os componentes da desta tela.

DNS - Settings

Nesta área você configura o serviço de redirecionamento de DNS para outro servidor DNS Recursivo "remoto" ou "externo". Você ainda pode selecionar habilitar o armazenamento de Caching local para os endereços pesquisados.

- Consultas recursivas:
 - Múltiplos servidores;
 Modo distribuído e balanceado;
 - Listen por device.

No quadro [Settings] configure os campos de acordo o formulário para o encaminhamento DNS para outro servidor DNS recursivo.

| DNS | |
|---------------------|---|
| Settings | |
| DNS Servers | |
| 8.8.8 | + |
| ✓ Interfaces | |
| eth0 | + |
| V DNS Cache | |
| 100000 | |
| SECURITY | |
| ✓ Rebind Protection | |
| ✓ Allow local | |
| Domains allowed | |
| Domains allowed | + |
| | |
| | |
| | |
| | |
| | |
| | |

DNS - Settings

Abaixo vamos especificar alguns campos:

• DNS Servers: Informe o servidor de DNS remoto no qual será feito o encaminhamento das consultas de DNS. Caso queira adicionar outros

servidores DNS, clique no botão [_____], após ter adicionado outros servidores, clique em [_____] para removê-los;

- Interface []: Seleção da interface de rede que será ativada para o modo "*Listen*". O que permite fazer as requisições *DNS* recursivo desta origem. Caso queira adicionar outras *interfaces*, clique no botão [], após ter adicionado outras *interfaces*, clique em [] para removê-las;
 DNS Cache []: Quantidade de endereços de *cache* para armazenamento no "*caching local*";
 Rebind Protection []: Esta opção desabilita a consulta de endereços de servidores de nomes que estão nos intervalos de *IP* privados
- visando deter ataques em que um navegador atrás de um firewall é usado para investigar máquinas na rede local. Através deste recurso, o UTM efetivamente filtra as respostas DNS que passam pelo firewall, efetuando o bloqueio de endereços locais indesejados e rejeitando a resolução de nomes externos atrelados a *IPs* internos;

🕖 A opção Rebinc

A opção Rebind Protection é especialmente efetiva contra DNS Rebinding. Trata-se de um tipo de ataque que visa adulterar o serviço de DNS e ignorar a política de mesma origem dos browsers fazendo com que seja feita uma comunicação com um servidor indesejável. Basicamente, isso é feito utilizando-se de um servidor DNS configurado com um TTL muito curto de modo a deter a criação de cache e possibilitar a execução de uma query que resolve para um IP alternativo indesejado, geralmente este sendo um IP local ou privado.

- Allow local [1]: Isenta as verificações para localhost. Esse intervalo de endereços é retornado por servidores maliciosos em tempo real, portanto, o bloqueio pode desativar esses serviços;
- Domains allowed: Detecta e bloqueia a vinculação de religação de DNS em consultas a esses domínios. Caso queira adicionar outros domínios,



] e aplicar as alterações efetuadas. Para

Após salvar, para que as alterações entrem em vigor será necessário acessar a **fila de comandos [** mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Após realizar esses procedimentos o DNS terá sido configurado com sucesso.

DNS - Redirect

Nesta área você pode configurar o serviço de redirecionamento das requisições DNS para "Que outros servidores DNS" sejam os "Responsáveis" em realizar as consultas recursivas "Exclusivas" para uma "lista de hosts".

O serviço permite através da distribuição e balanceamento das pesquisas para *hosts* específicos, redirecionar o serviço para outro servidor *DNS* exclusivo para os *hosts* específicados.

Ainda pode ser usado inclusive para redirecionar as pesquisas para um "DNS inválido", evitando a resolução de nomes de determinados endereços, logo bloqueando seu acesso.

- Redirecionamento DNS:
 - Múltiplos servidores;
 - Encaminhamento por host/IP e FQDN;
 - Cache.

No quadro *Redirect* clique em [_____] e configure apontando o endereço do servidor *DNS* e adicionando a lista de *hosts* que pretende redirecionar as pesquisas recursivas.

| | Add redirect × | |
|---|--|---------------------|
| | DNS Server | |
| | Redirected addresses | |
| | Address will be redirected to this DNS | |
| | | |
| | L Save | |
| | DNS - Add redirect | |
| • | DNS Server: Adicionar o servidor DNS que será utilizado. Caso queira adicionar outros domínios, clique no botão [], a | pós ter adicionado |
| • | outros domínios, clique em [] para removê-los; Redirected addresses: Adicionar os endereços para onde será efetuado o redirecionamento. Caso queira adicionar endereços botão [], após ter adicionado outros enderecos, caso seia necessário, clique em [] para removê-los. | s extras, clique no |
| | | |

Vamos exemplificar a pesquisa a uma lista de hosts em um DNS Server local, conforme demonstrado pela imagem a seguir:

r

7

| DNS Server | |
|-----------------------|----------|
| 192.168.254.245 | |
| Redirected addresses | |
| tests.blockbit.com | + |
| gitlab.blockbit.com | 1 |
| intranet.blockbit.com | D |
| www.blockbit.com | D |

🖺 Save

4

DNS - Add redirect - Example



Feitas as alterações, clique em [

Ŀ.

] para salvar todas as configurações.

| R | edirect | | | | | | + | |
|--|--|---------------------------------------|--------------------------------------|----------------------------|------------|------------------|---------------|-------------|
| | 102 169 254 245 | | | | | | â | |
| | 192.106.234.243 | | | | | | - | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | Ľ | DNS - Redirect | added | | | | |
| | | | | | 1 | | | |
| Após salvar, para que as mais informações a respo | alterações entrem em vig eito da fila de comandos a | or será necessár cesse a página: l | rio acessar a fil UTM - Fila de c | a de comandos comandos. | [| e aplicar as all | erações efeti | uadas. Para |
| Caso seja necessário edi | itar os dados adicionados, | , clique no botão | [💣] e efetue a | as configurações | necessária | as. | | |
| Caso pretenda removê-lo | os clique em [¹¹], a segui | nte mensagem se | erá exibida: | | | | | |
| | | | | | | | | |

| Remove redirection? |
|---------------------|
| OK Cancel |

Remove redirection



Após estes passos, o redirecionamento de DNS terá sido configurado com sucesso.

UTM - Services - DDNS (DynDns)

O serviço DDNS (Dynamic Domain Name System) é um gerenciador de um serviço de tradução de nomes para endereços *IP* dinâmicos. O DDNS é o método usado para atualizar a tabela de *IPs/hosts* públicos automaticamente em um servidor DNS em tempo real e isso com o propósito de manter ativo e publicado um *host* ou endereço *IP* configurado para algum serviço ou recurso através de *link* dinâmico como: *PPPOA*; *PPPOE*, (DSL - Digital Subscriber Line) para prover seu acesso remoto.

Os endereços *IP* dinâmicos representam um problema quando precisamos fazer algum acesso remoto em algum serviço da rede, tais como um serviço web (*intranet/extranet*), acesso *DNAT* (*Destination NAT*), configuração de *VPN*, entre outros.

Como os endereços *IP* de *links DSL* podem mudar com frequência, associar nomes de *hosts* e domínios a endereços *IP* dinâmicos é uma tarefa que exige um remapeamento quase que em tempo real para que os serviços continuem respondendo as requisições e acessos remotos sem a interrupção aos usuários públicos.

O DNS Dinâmico é uma característica esperada ou mesmo exigida nos nossos appliances. Alguns serviços como VPN IPSEC (site-to-site), VPN IPSEC R AS e mesmo o acesso remoto por redirecionamento do firewall (DNAT), utilizam-se deste recurso como ferramenta adicional para permitir de forma segura o acesso a recursos da rede através de links DSL (IP dinâmicos).

Acesse a interface de gerenciamento clicando na opção "DDNS".

| • | Services | ~ |
|---|----------------------|----|
| » | Firewall | ۲ |
| * | Proxy | Ø |
| » | Web Cache | Ø |
| » | Web Filter | Ø |
| » | Application Control | Ø |
| * | Intrusion Prevention | Ø |
| * | Threat Protection | Ø |
| * | SD-WAN | Ø |
| * | DHCP | Ø |
| * | DNS | Ø |
| » | DDNS | Ø |
| » | VPN IPSEC | Ø |
| » | VPN SSL | 0) |

Services - DDNS

A tela abaixo será exibida:

| Dynamic DNS | | |
|---------------------|---------------------|--------|
| itosts | | • • |
| Peak | W Address interface | Active |
| vgm Bh Mockhill zom | 30 - 3X | 11 |

Services - Interface DDNS

A seguir analisaremos os componentes da desta tela.

DDNS - Botão de Adição

Antes de adicionar o um "Dymanic DNS" vamos conhecer e identificar os recursos de configuração e como funcionam.

- Recursos DDNS.
 - Suporte aos provedores de serviço.
 - NoIP.org;
 - DynDNS.com.
 - Suporte a interfaces.
 - Ethernet,
 - Vlan;
 - MacVlan (Interface virtual).
 - Integração com os serviços
 - DNS;
 - VPN;
 - Firewall;
 - Políticas de segurança.
 - Atualização hosts/domínios (ddns) automática de 10/10 min.

O serviço DDNS pode ser habilitado para uma interface de rede específica "[EthX]" ou no modo "Automático".

- A seleção de uma interface específica considera-se como exemplo, associar o "host" ao "endereço IP do link DSL" do respectivo device físico;
- Na seleção da interface no modo "Automático", considera-se associar o "host" de forma dinâmica ao "endereço IP" em uso pelo link que estiver ativo como "Rota default", não importando qual seja.

Dessa forma é possível disponibilizar "Redundância" para os serviços VPN IPSEC (site-to-site), VPN IPSEC RAS e o acesso remoto por redirecionamento pelo firewall (DNAT). Não importa se você utiliza um link IP fixo ou um link DSL, é possível pelo recurso DDNS publicar o endereço IP de um host de forma dinâmica e permitir o uso deste host "FQDN – full Quality domain name" como um endereço de acesso e configuração nos serviços citados.

| Para adicionar un | n <i>DDNS</i> clique em []. A seguinte janela s | será exibida: | |
|-------------------|---|--------------------|--------|
| | Enable DDNS | | 3 |
| | Service | | |
| | NoIP.org | | ~ |
| | Host | Interface | |
| | | Automatic | ~ |
| | User | Password | |
| | | | |
| | | | |
| | | | 🖺 Save |
| | L | DDNS - Enable DDNS | |

Configure o formulário de acordo as especificações para conexão com o provedor conforme o exemplo dado.

- Service: Determina qual serviço de DDNS será utilizado;
- Host: Neste campo deve-se definir qual será o Host utilizado;
- Interface: Como citado anteriormente, a interface pode ser específica ou automática:
 - Interface Específica: As opções disponíveis são as interfaces cadastradas em Network Interfaces, este recurso é utilizado para associar o "host" ao "endereço IP do link DSL" de seu device físico;
 - Interface Automática: Associa o "host" de forma dinâmica ao "endereço IP" em uso pelo link que estiver ativo como "Rota default".

A interface automática é recomendada para casos onde é necessário acessar o Blockbit através de um roteador ou gateway onde este mesmo esteja fazendo NAT, ou seja, quando há a entrega de um *IP* privado.

- User: Assim como citado anteriormente, neste campo deve ser digitado o usuário utilizado para se autenticar no provedor;
- Password: Assim como citado anteriormente, neste campo deve ser digitada a senha utilizada para se autenticar no provedor.

Vamos exemplificar a configuração do "Dymanic DNS" para o host "vpn-bb.blockbit.com" para o provedor de serviços "DynDNS". Usar usuário e senha fornecidos/cadastrado no respectivo provedor.

| | Enable DDNS | | × |
|--|---|---|------------------------------|
| | Service | | |
| | DynDNS.com | | \sim |
| | Host | Interface | |
| | vpn-bb.blockbit.com | Automatic | \sim |
| | User | Password | |
| | blockbit | | |
| | | | 🖺 Save |
| | DDNS - Enable | DDNS - Example | |
| Depois de ter efetuado as configurações, clique em [] para salvá-las. | | | |
| Após salvar, para mais informações | que as alterações entrem em vigor será necessário acessa a respeito da fila de comandos acesse a página: UTM - Fil | ar a fila de comandos [] e aplicar a a de comandos. | s alterações efetuadas. Para |

Após realizar esses procedimentos o DDNS terá sido configurado com sucesso.

| PADDes | Interface | Action |
|--------|-----------|-------------------|
| | | 1 3 |
| | PANNES - | maadress sterface |

DDNS - Dynamic DNS Added

O Serviço DDNS já está configurado e o host "vpn-bb.blockbit.com" respondendo pelo endereço IP da interface de rede correspondente a rota default.

DDNS - Menu de ações

No topo direito da tela, ao lado do botão de adição temos o menu de ações:



Ao clicar neste botão o menu abaixo é exibido:



DDNS - Menu de ações

O menu é composto das seguintes opções:

- Select;
- Select All;
- Remove.

A seguir cada opção do menu de ações será detalhada.

DDNS - Menu de Ações - Select all

Ao clicar em "Select All" no menu de ações todos os itens serão selecionados.



DDNS – Select All

Isso permite que alterações que afetem todos os itens, sejam facilmente implementadas.

DDNS - Menu de Ações - Remove

Através do menu de ações é possível deletar vários itens ao mesmo tempo. Siga os seguintes passos:

| 1. | Selecione os itens o | ue deseia | deletar clicando | no ícone de | e selecão | i h | ĺ: |
|-----|----------------------|------------|------------------|-------------|-----------|-----|----|
| ••• | 00100100 00 100110 0 | 140 4000,4 | aorotar onoarrao | | | | |

| Dynamic DNS | |
|---|---------------------------------------|
| Hoista | |
| Heat. | #*Address telerlacy Action |
| **** | |
| | · · · · · · · · · · · · · · · · · · · |
| DDNS | - Seleção para deleção |
| 2. Clique no Menu de ações[] e selecione a opção " <i>Remove</i> "; | |

| | + | • |
|------------|---|---|
| Select | | |
| Select all | | |
| | | |
| Remove | | |

DDNS - Menu de ações - Remove

4. Surgirá uma tela perguntado se deseja deletar o item selecionado:

| | Want to remove the host (s) selected (s)? |
|--|--|
| | OK Cancel |
| | DDNS - Remove itens |
| Caso deseje cancelar clique no botão [| ncel]. Para concluir a deleção clique no botão [OK] |

O item foi deletado com sucesso.