Blockbit

Resource Center

Documentação

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 *QoS* 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:

 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"

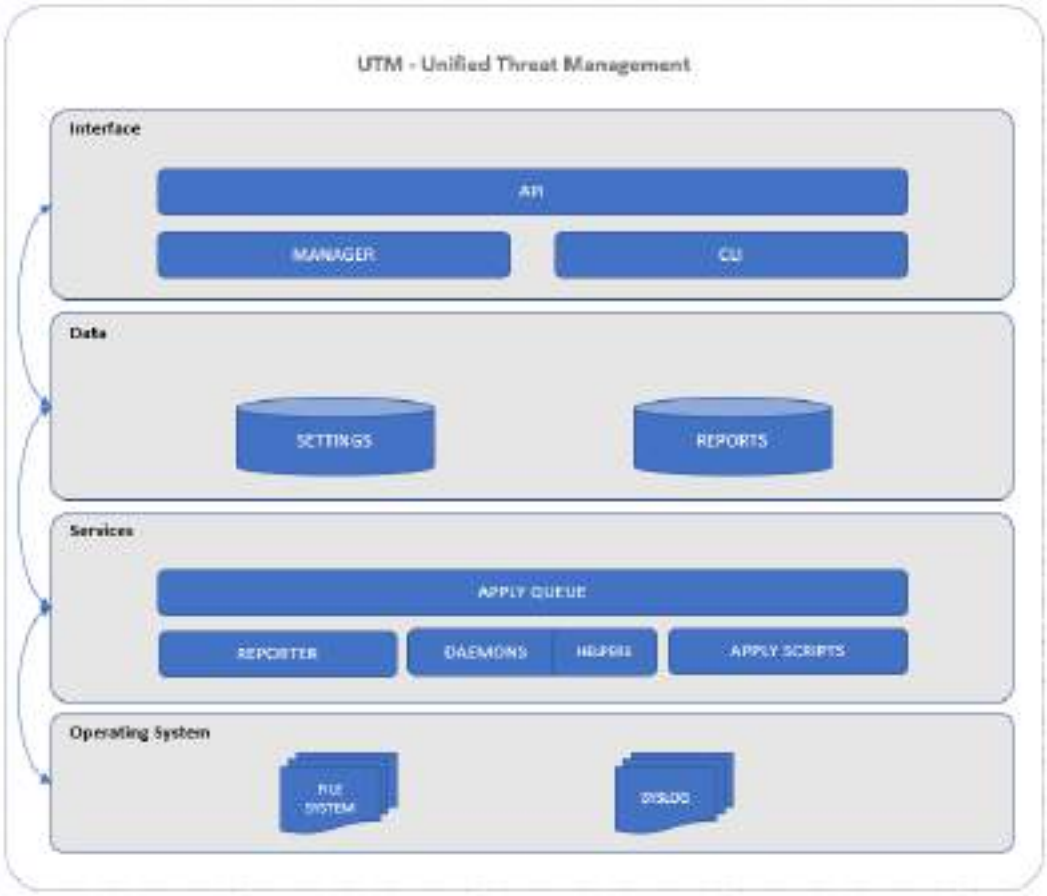
- **Informações:** Refere-se a informações adicionais a respeito do Blockbit UTM:

 Exemplo de uma mensagem de Informações.

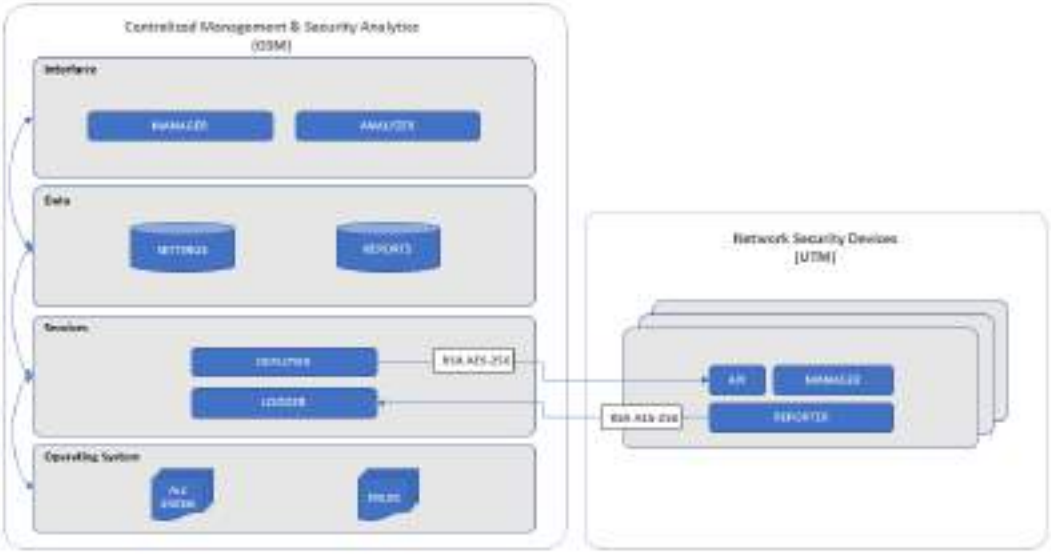
Símbolo – "Informações"

UTM - ARQUITETURA

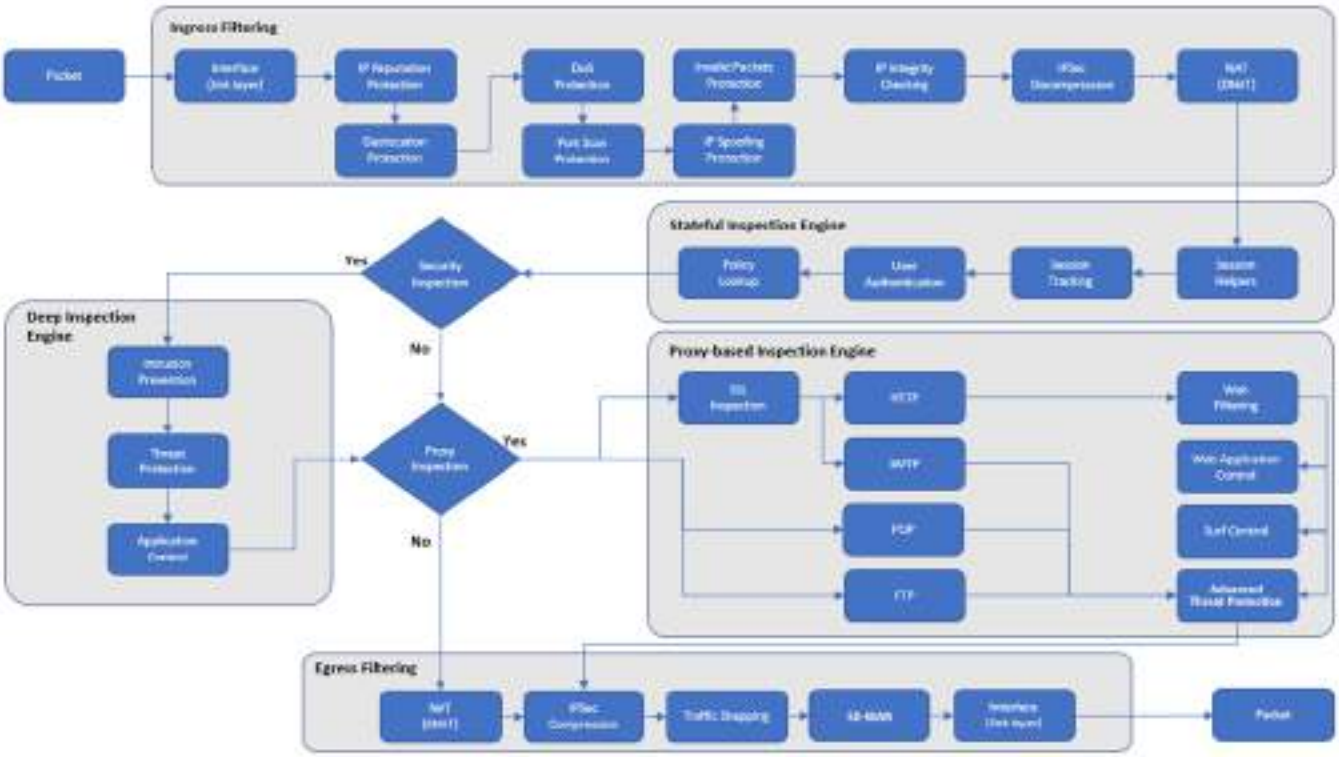
A arquitetura do BLOCKBIT UTM é apresentada por um conjunto de camadas de componentes, que integradas, definem os aspectos técnicos relativos aos serviços oferecidos pelo sistema. A imagem abaixo representa a integração dos módulos.



Arquitetura do Sistema – Gerenciamento



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*, *XenServer 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:

Tabela - Características mínimas do *Appliance Virtual*

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

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.

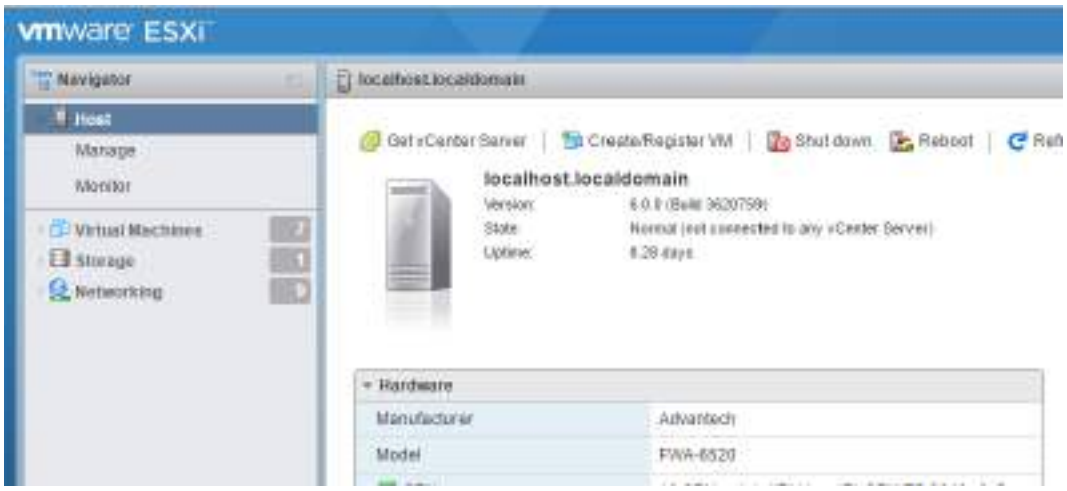
1. Usando o navegador de *internet* de sua preferência, acesse o console de gerenciamento do *VMware ESXi* no *VMware Host Client*;

2. Preencha os campos com as seguintes informações:

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

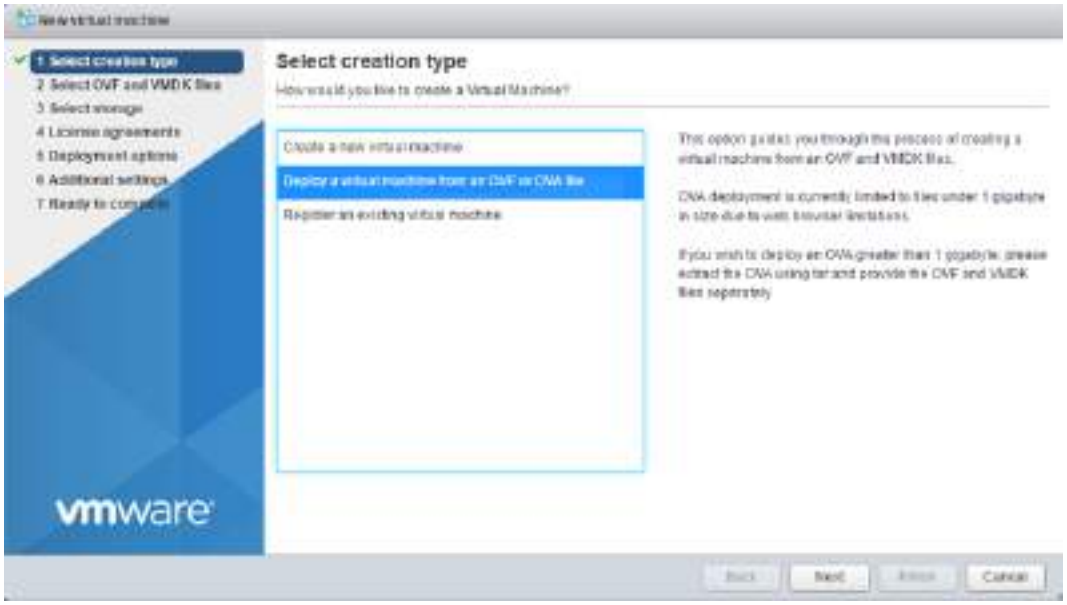
Login VMware

3. Clique em "*Create/Register VM*";



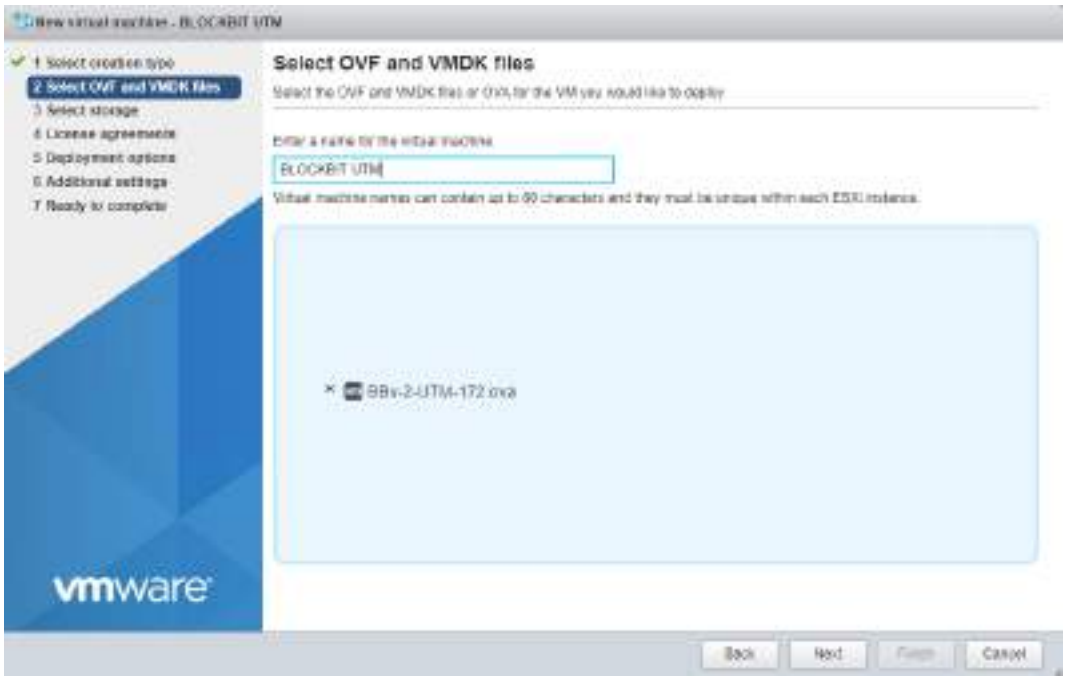
Console VMware

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



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;



Select OVF and VMDK files

- Clique no botão “*Next*”;

5. Selecione o *storage* desejado. Ex.: *datastore*1;

Select Storage

- Clique no botão “*Next*”;

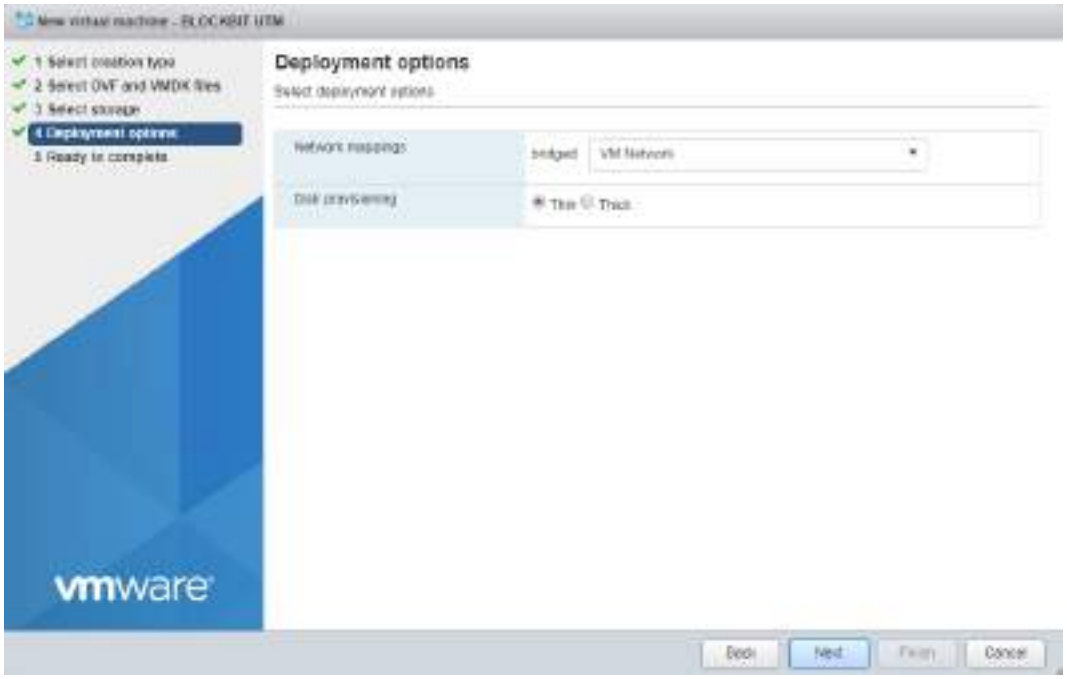
6. Aguarde o upload da *OVA*. Enquanto ocorre o *upload*, aparecerá a seguinte mensagem: “*Extracting OVA, this could take some time...*” Espere a conclusão deste processo, que deverá ocorrer automaticamente;

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.

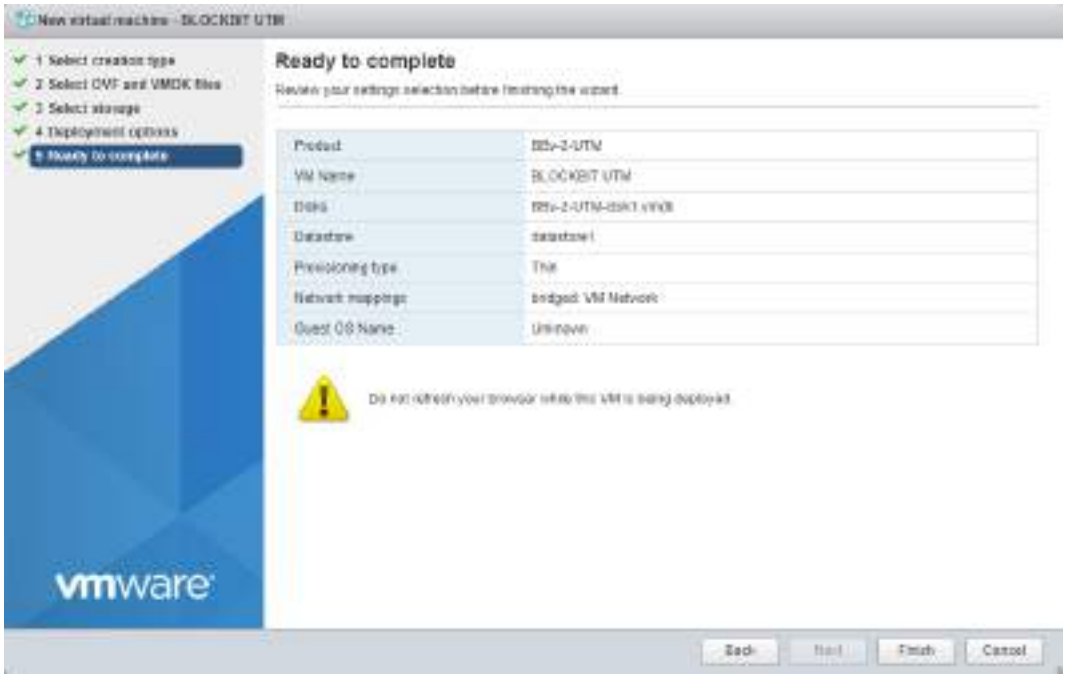
Para maiores informações consulte o manual do *VMware*. Neste exemplo será utilizado a configuração "*Disk provisioning* – Disco *Thin*".



Deployment options

- Clique no botão “*Next*”.

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 eth1 172.16.102.136/24
ifconfig eth1 down
ifconfig eth1 up
route add default gw 172.16.102.1 dev eth1
```

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

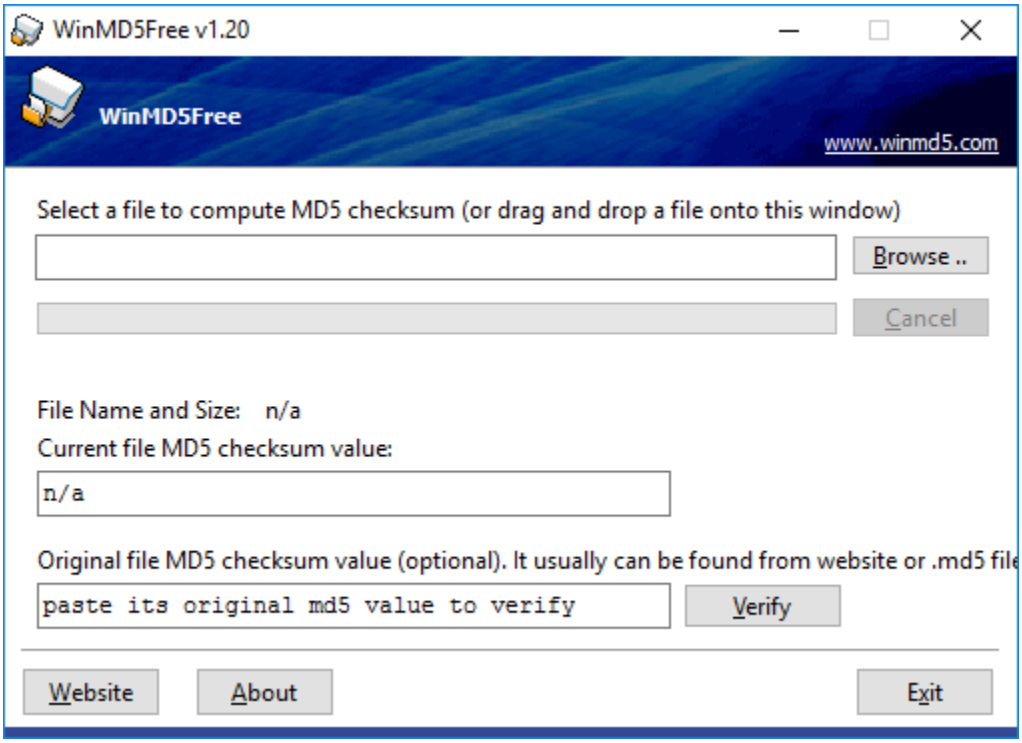
```
Digite o comando blockbit>changeip.
Tecle "Enter".
```

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:

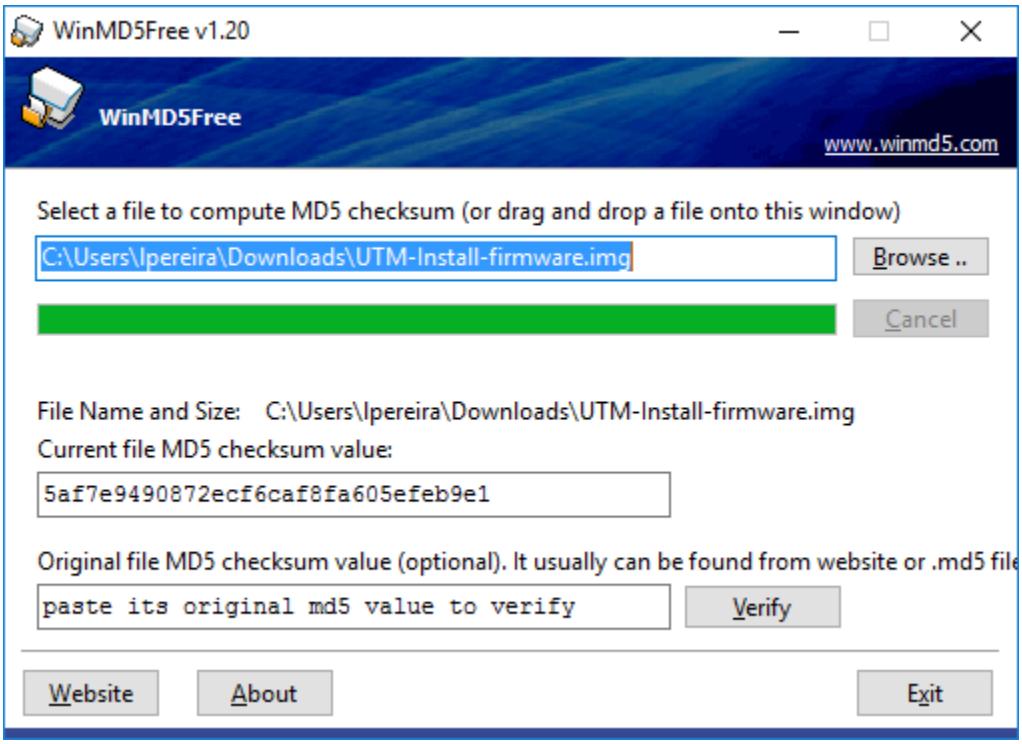
Verificação dos arquivos

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



WinMD5

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



MD5 Check

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

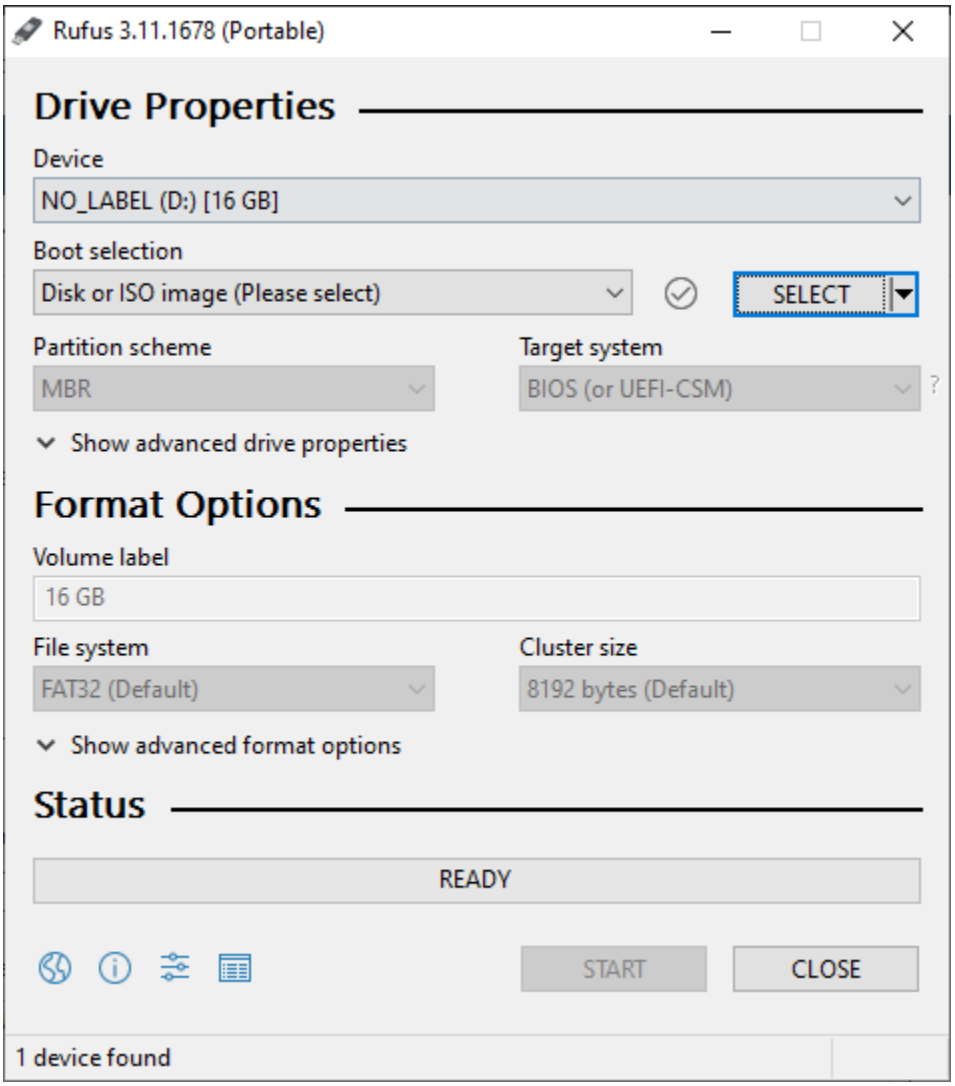
Gravando as imagens

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;

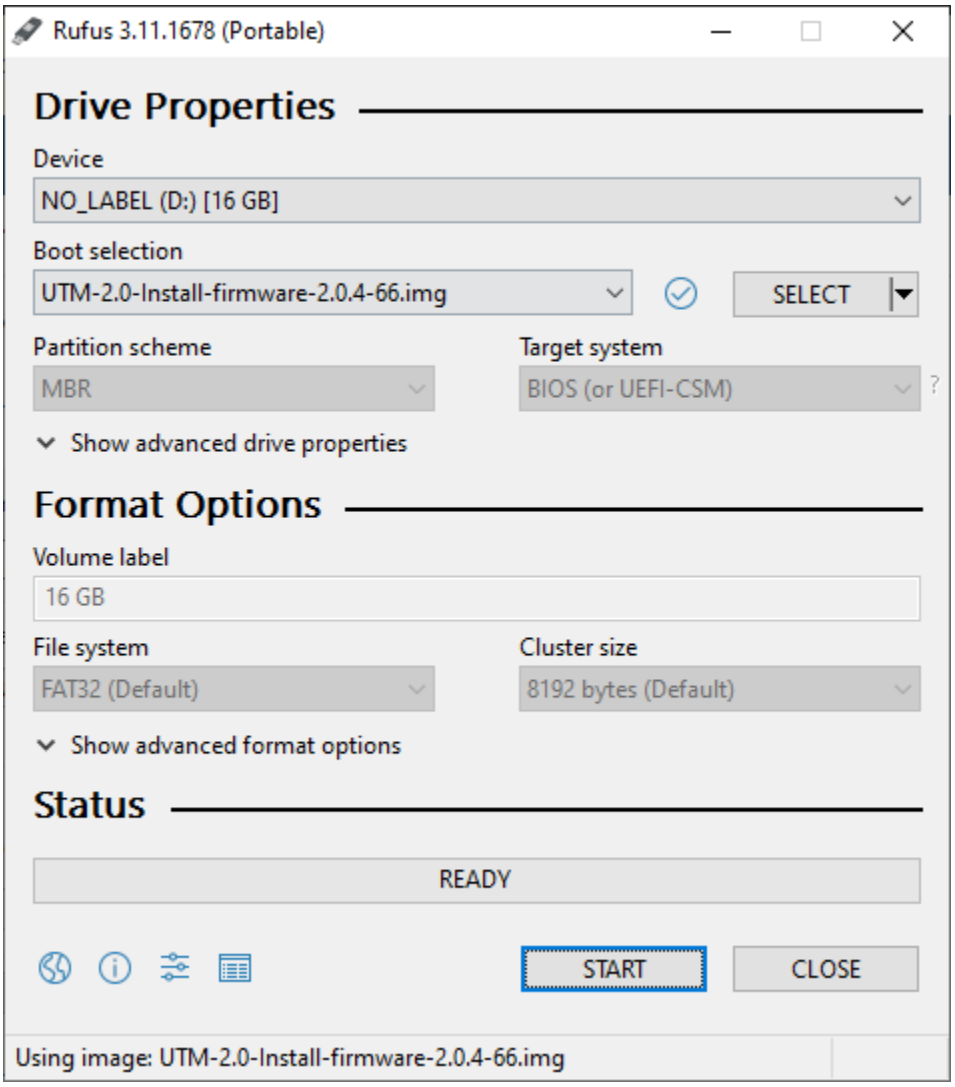
Este pendrive será usado exclusivamente para a instalação da imagem, ou seja, ele não deve possuir nenhum arquivo, caso seja necessário, faça uma formatação.

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



Rufus

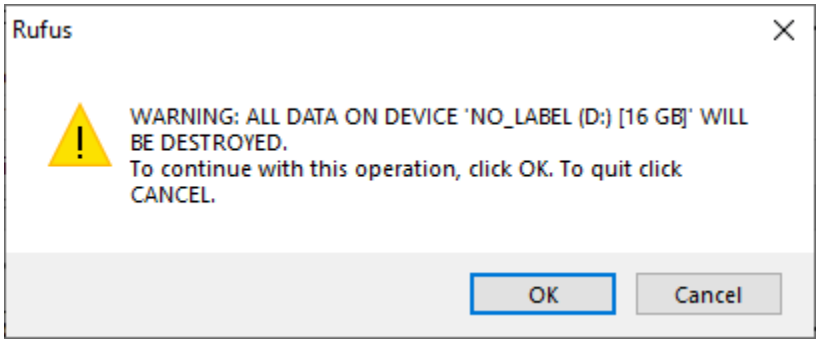
3. Clique em **[** SELECT **]** e selecione a imagem adequada a ser gravada nos *pendrives*. Ex.: UTM-Install-firmware.img;



Gravando a imagem

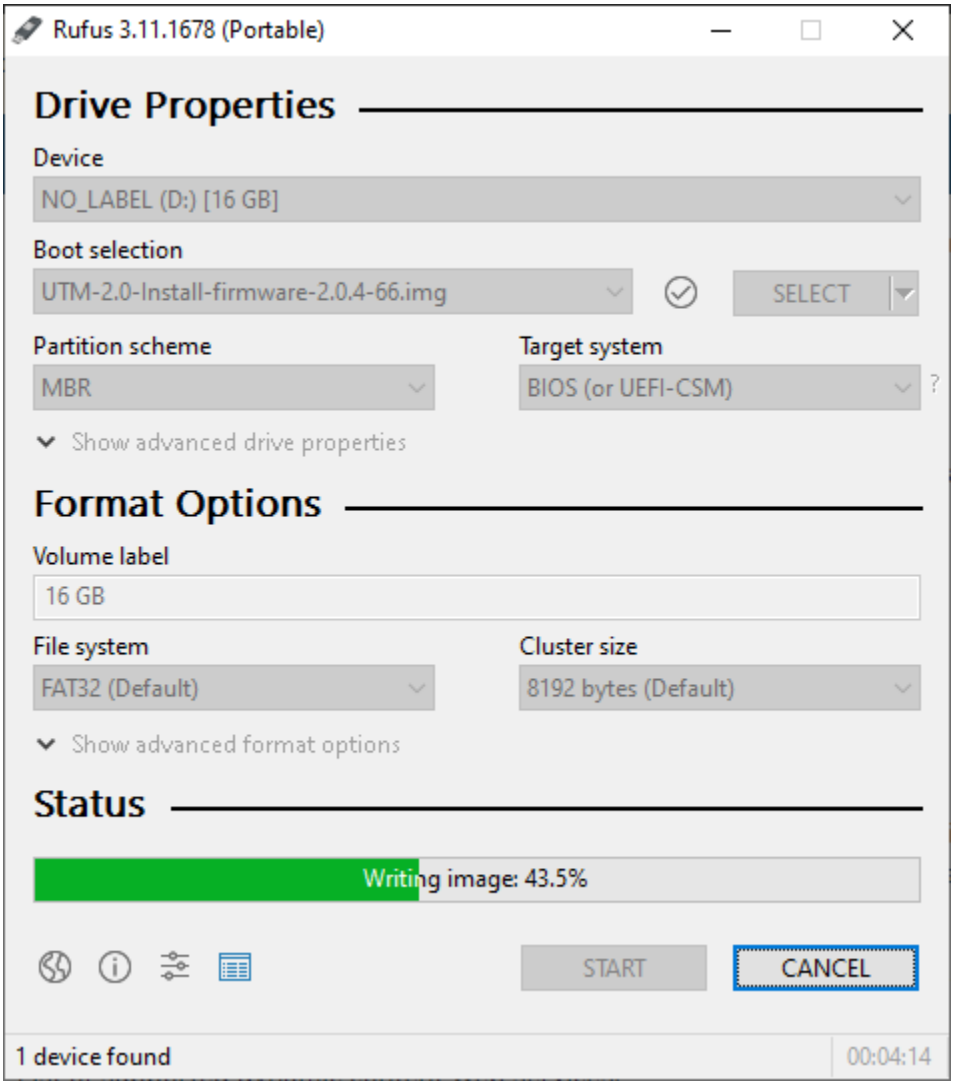
4. Caso, não esteja selecionado, selecione o *Device* correspondente ao *pendrive* que deseja gravar a imagem. *Ex*.: NO_LABEL (D:) [16 GB];

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



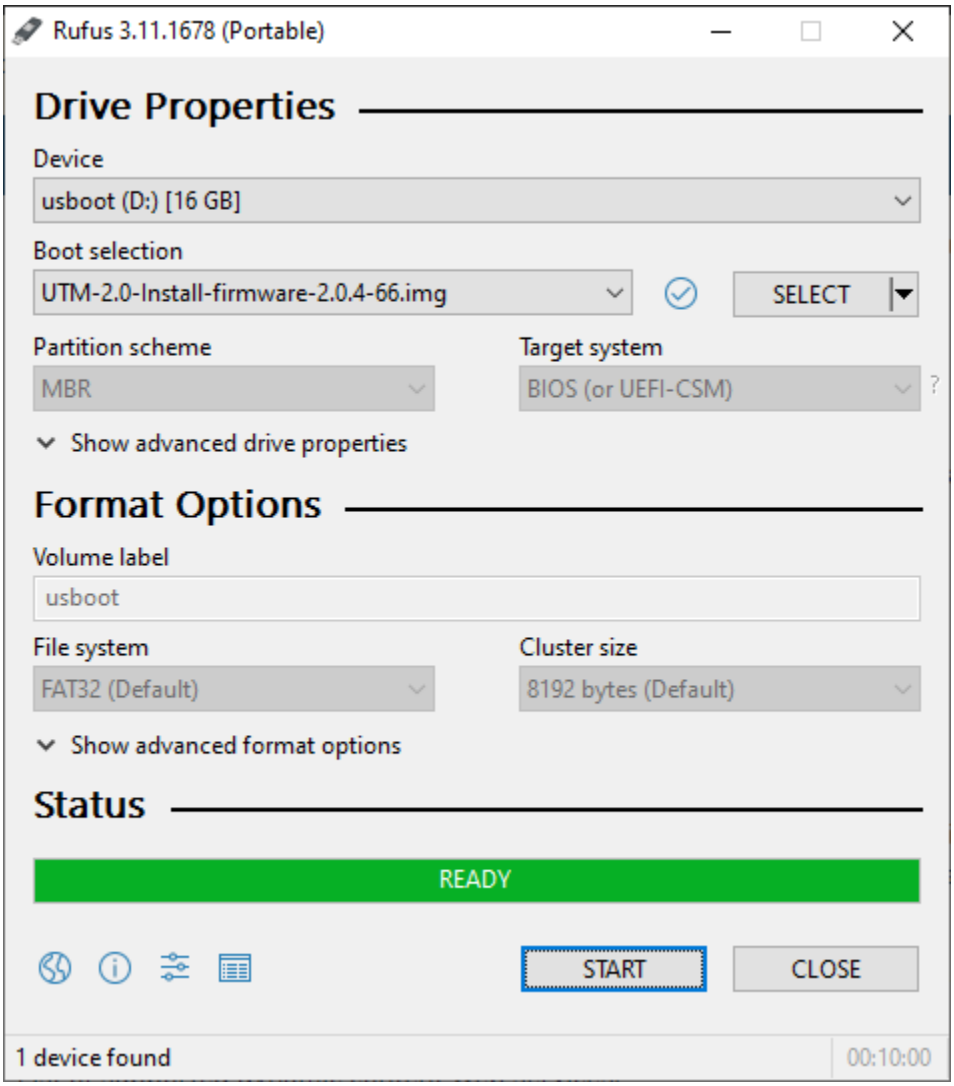
WARNING

6. Clique em **[** OK **]** e aguarde a gravação ser concluída com sucesso;



Andamento da gravação da imagem

7. Após a conclusão da barra de progresso, clique em **[** CLOSE **]** para fechar o *Rufus*.



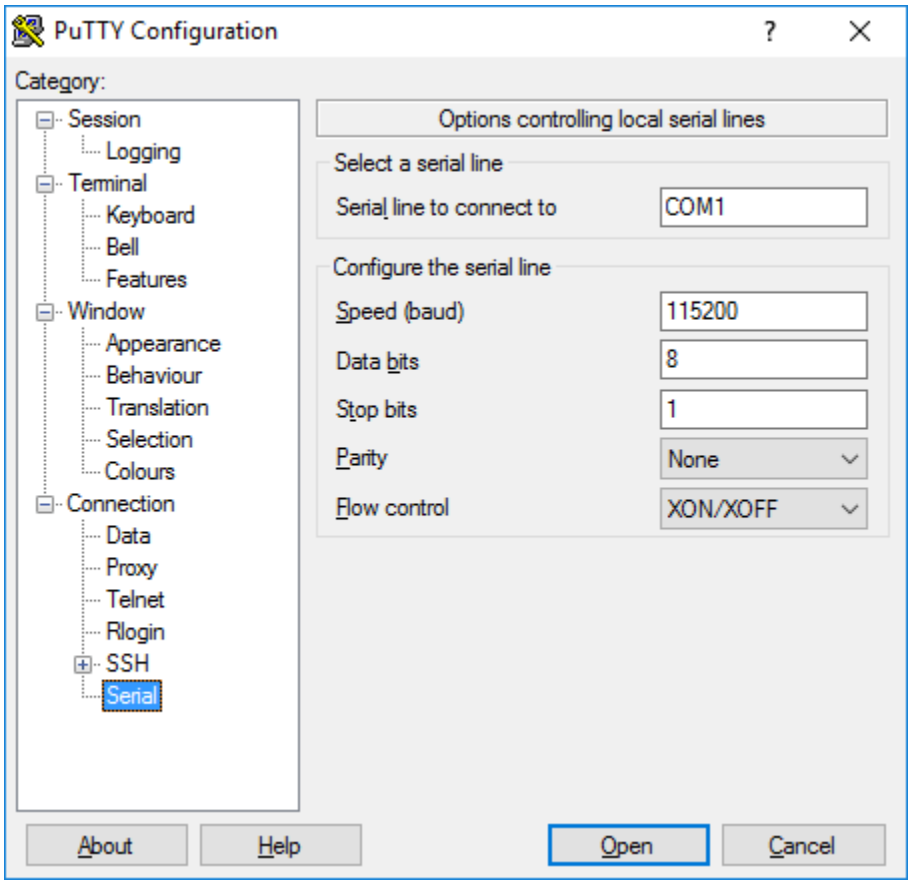
Rufus - Concluído

Acesso ao Console – *Putty*

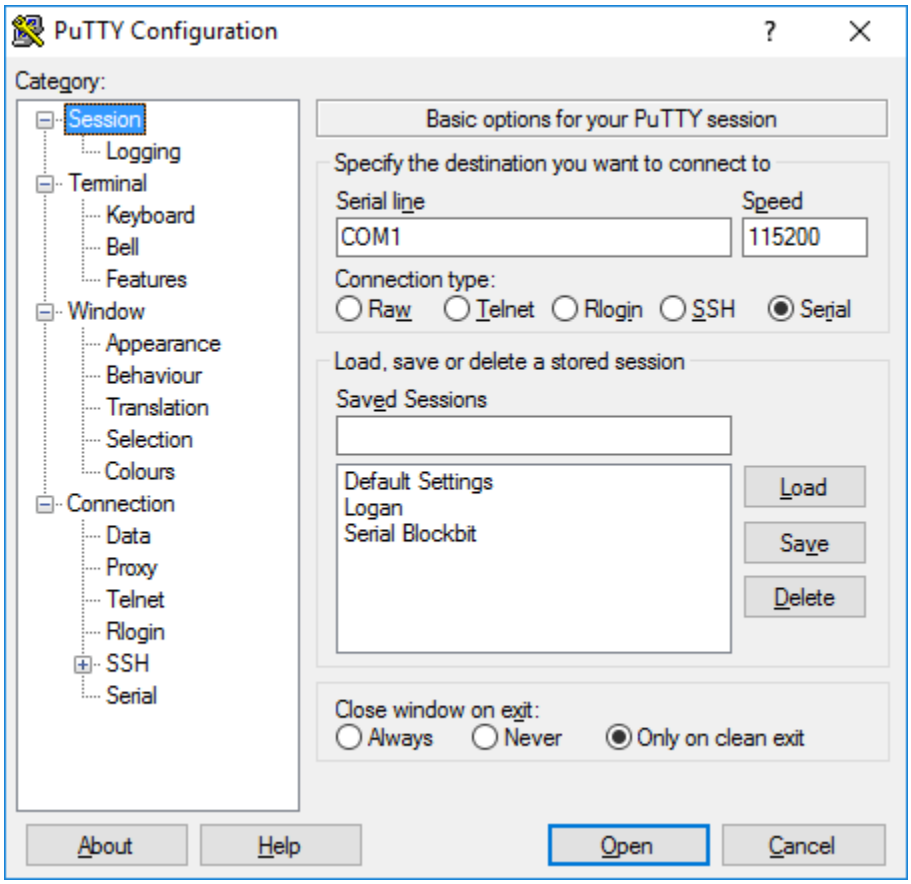
Antes de iniciar os procedimentos a seguir o aplicativo *Putty* deverá estar disponível na máquina na qual será feita a conexão ao Equipamento. O *Putty* é um *software* de emulação de *terminal* grátis e de código livre.

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;
- Paridade padrão: Nenhum.



Putty Settings



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;

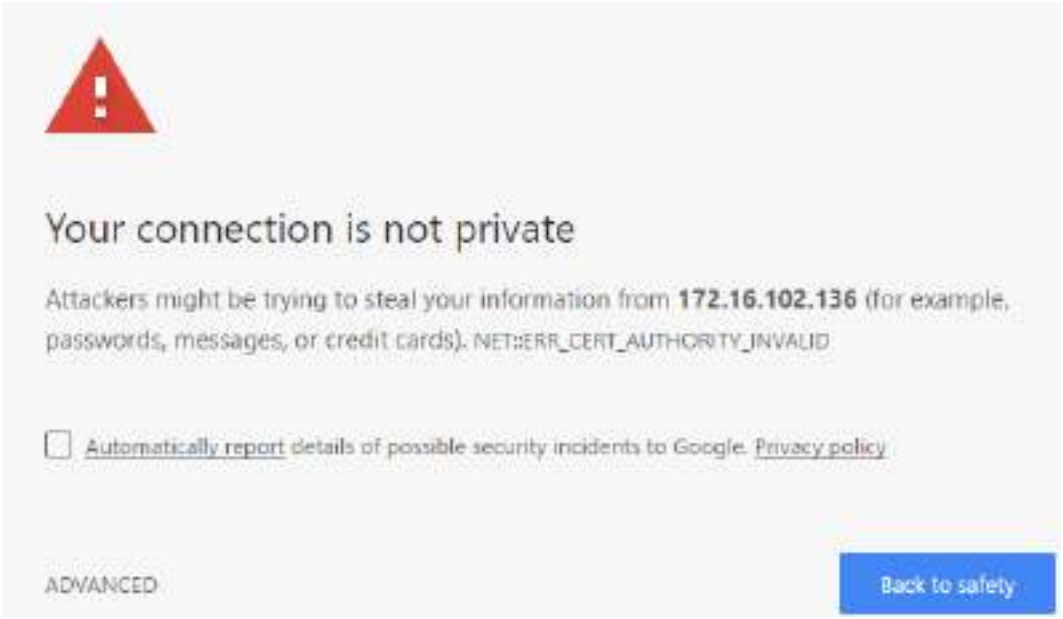
Caso o *Browser* emita um **ALERTA DE SEGURANÇA**, siga as recomendações abaixo.

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*";



Exceção *Chrome* – Botão "*Advanced*"

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

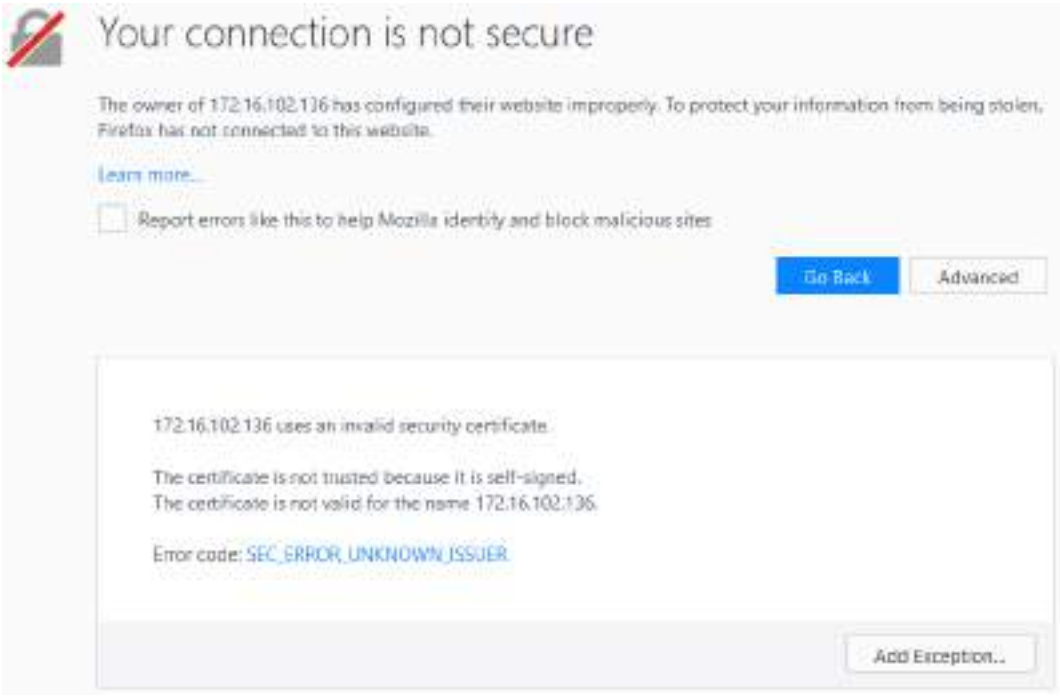
Exceção Chrome – "*Proceed to 172.16.102.136* (*unsafe*)"

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

Configurando exceção no *Mozilla Firefox*

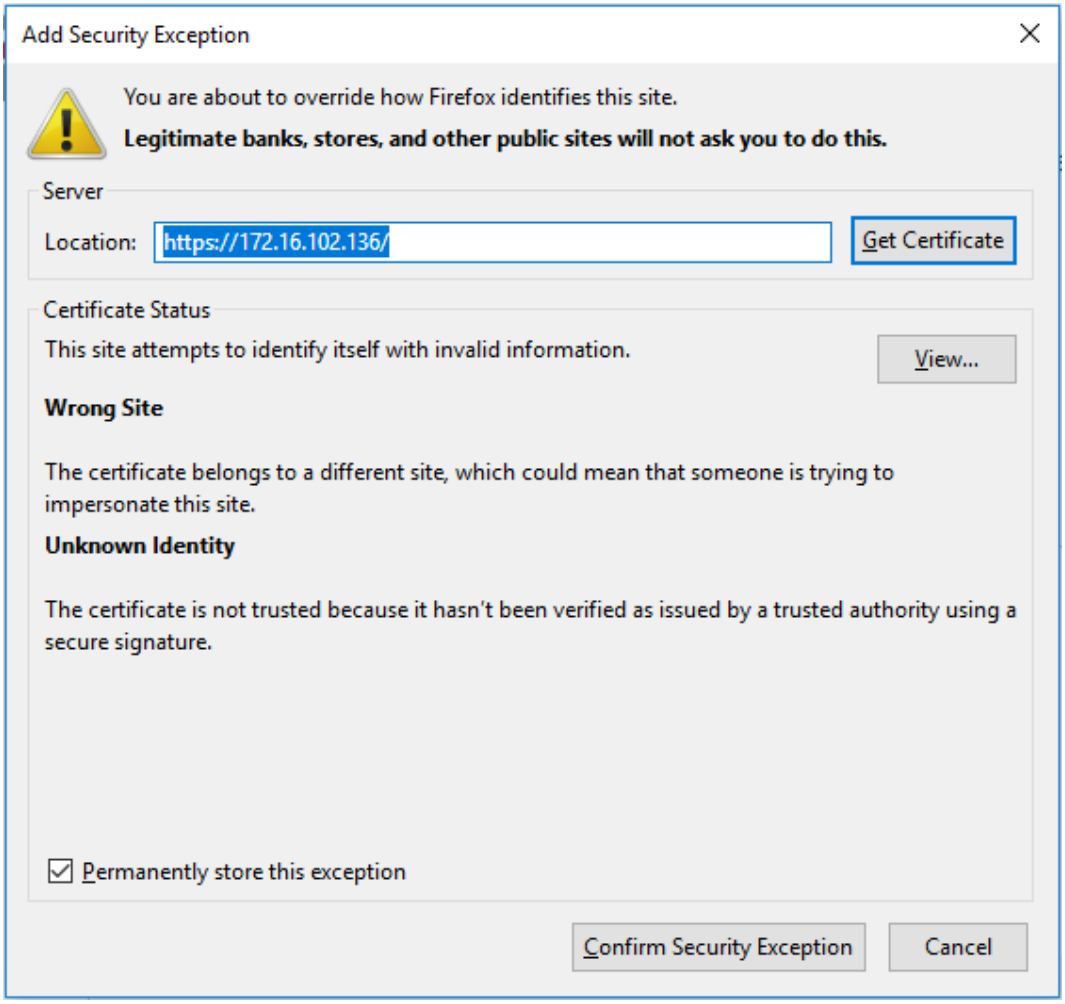
Para configurar a exceção no *Mozilla Firefox* siga os seguintes passos:

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



Exceção *Mozilla Firefox – Your connection is not secure*

3. Clique no botão "*Confirm Security Exception*".



Exceção *Mozilla Firefox – Confirm Security Exception*

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

UTM - ASSISTENTE DE INSTALAÇÃO

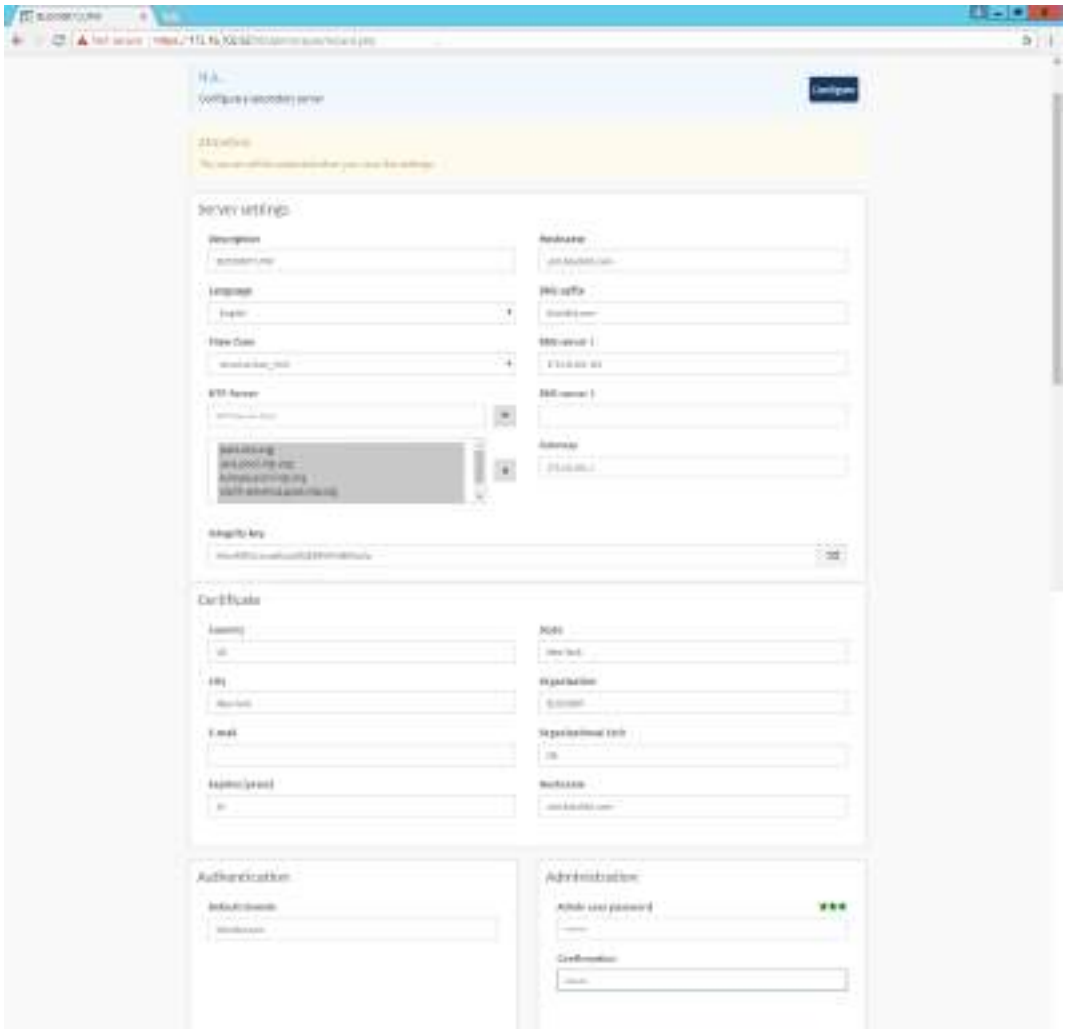
Esta seção irá apresentar como configurar o Assistente de Instalação do Blockbit UTM.

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;



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.

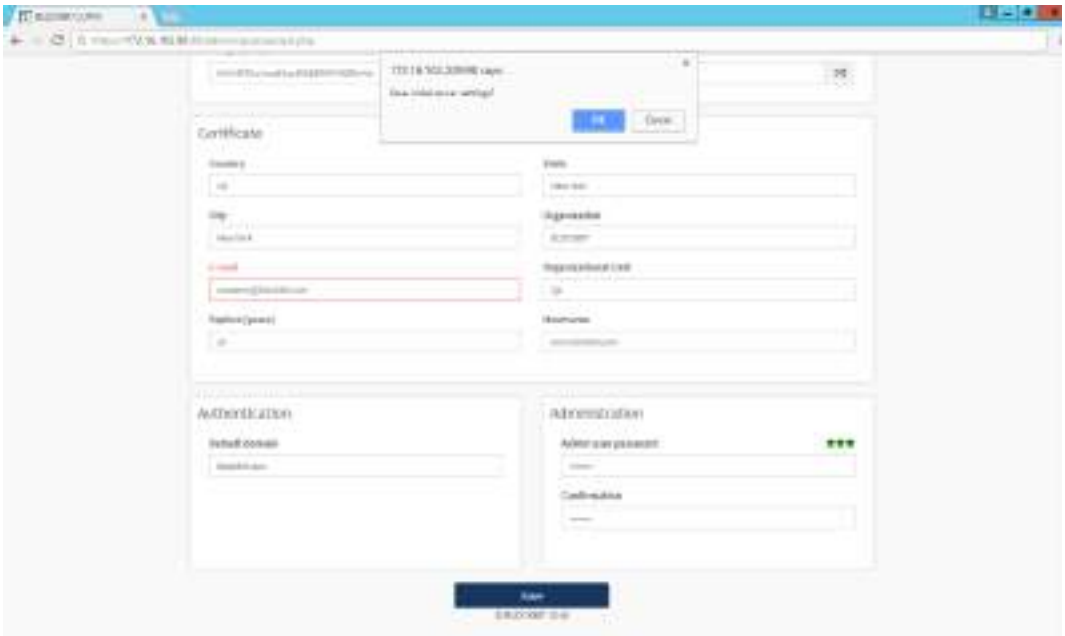
4. Digite os seguintes dados no frame "*Authentication*", define o domínio local padrão para a autenticação de usuários do Blockbit UTM.

- ***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.



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*.

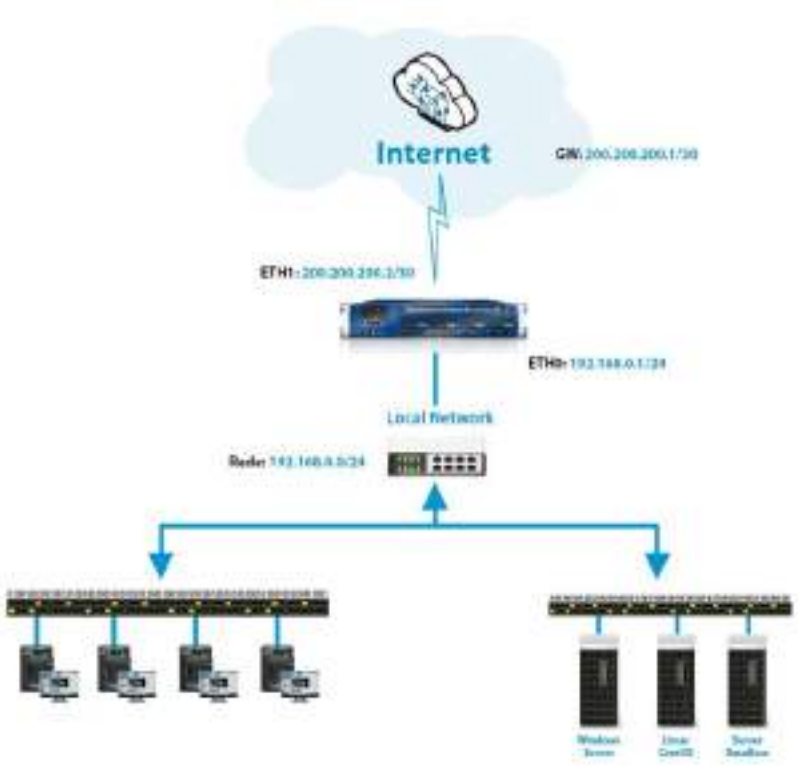
Tela de *LOGON* de administração do Blockbit UTM

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.

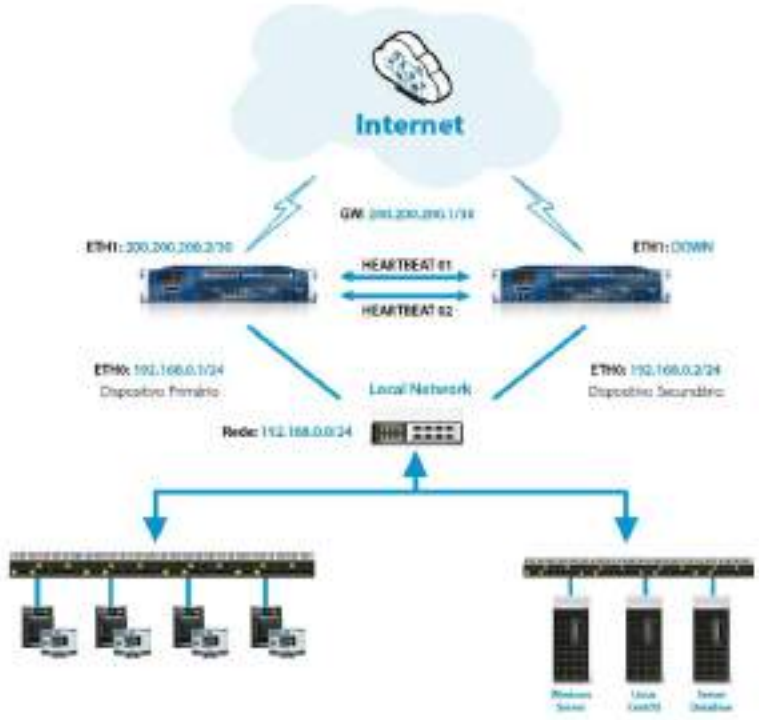


Topologia da rede – Blockbit UTM *Manager*.

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:

Tabela 1 – Endereçamento *IP*.

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

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.: *English*.

Tela de *Login* – Blockbit UTM

- Clique no botão ***Login[Login]*** para acessar a *Interface Web*.

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

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.

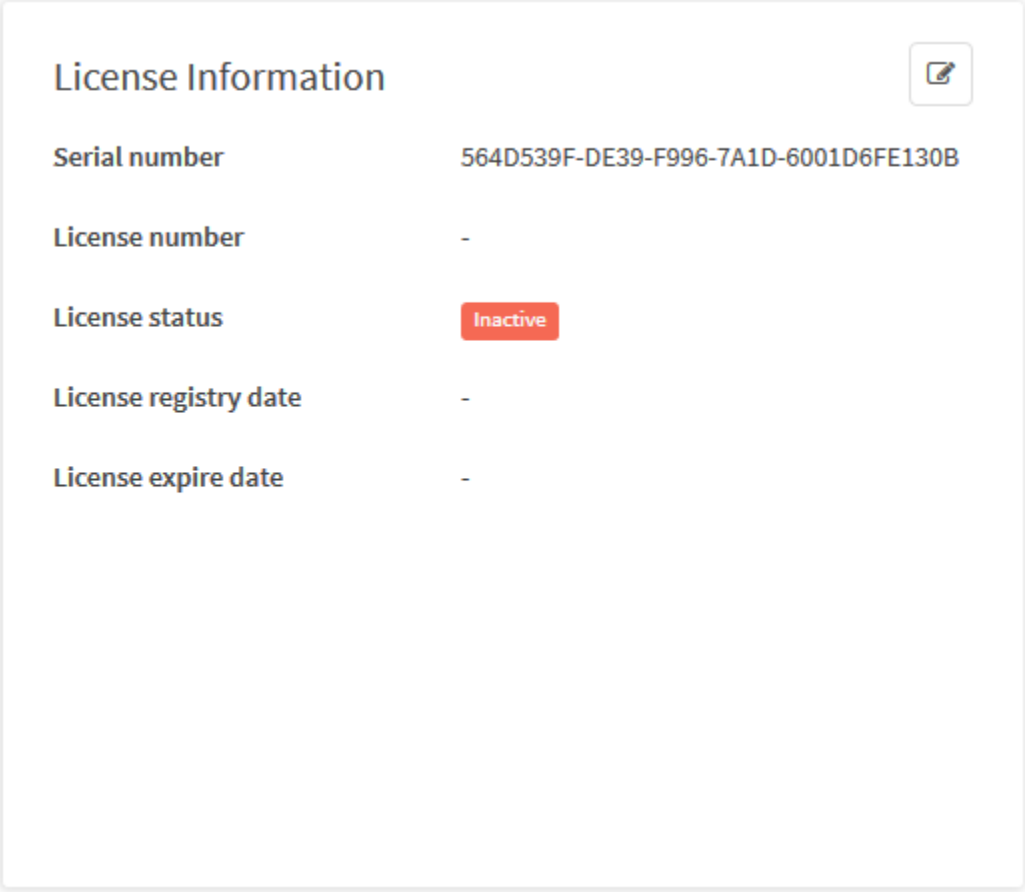
Acessando a Interface Web – Licenciamento

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*:



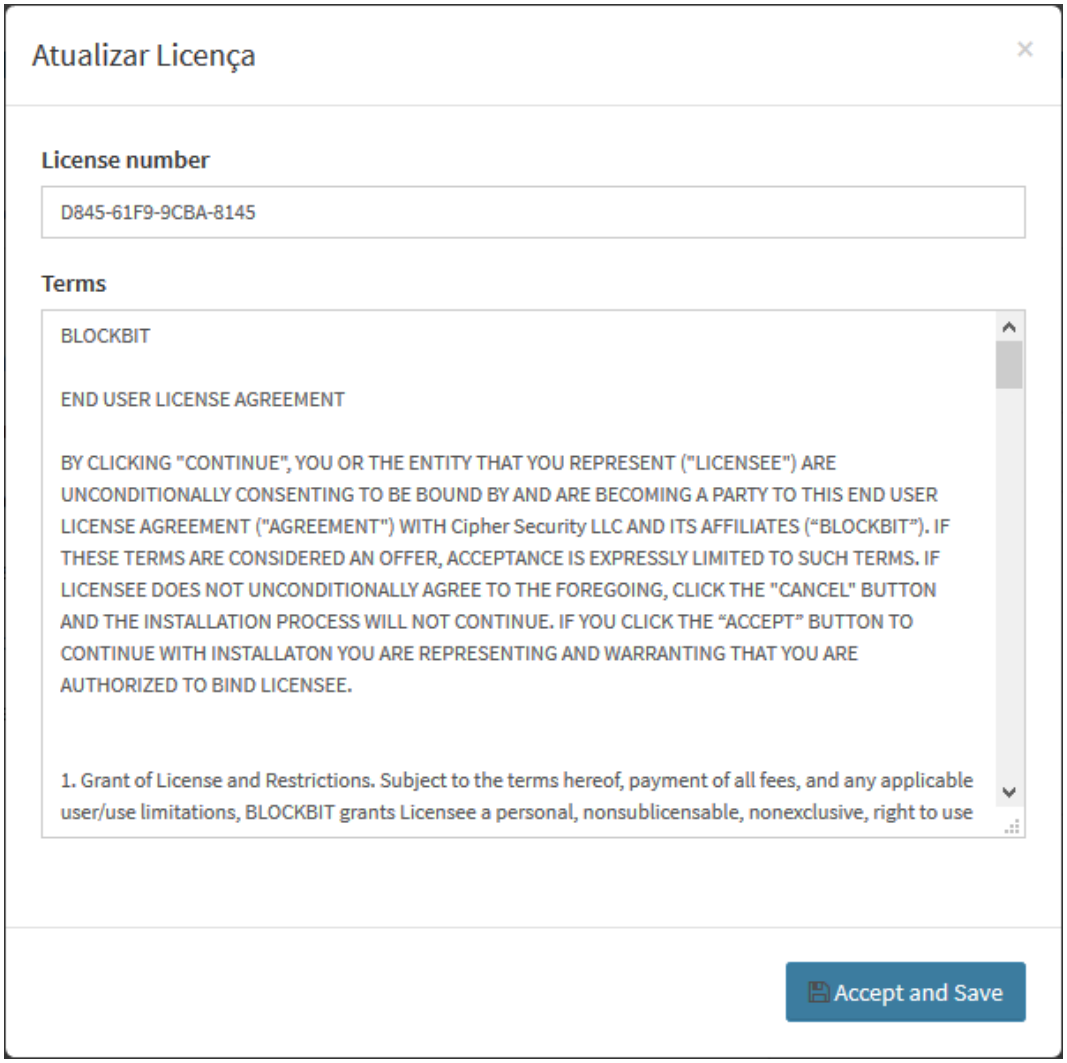
Dashboard – System

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

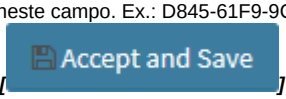
Também é possível descobrir o *UUID* usando do comando "*show-uuid"* no console. Para mais informações cheque esta página: [show-uuid].

- 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.

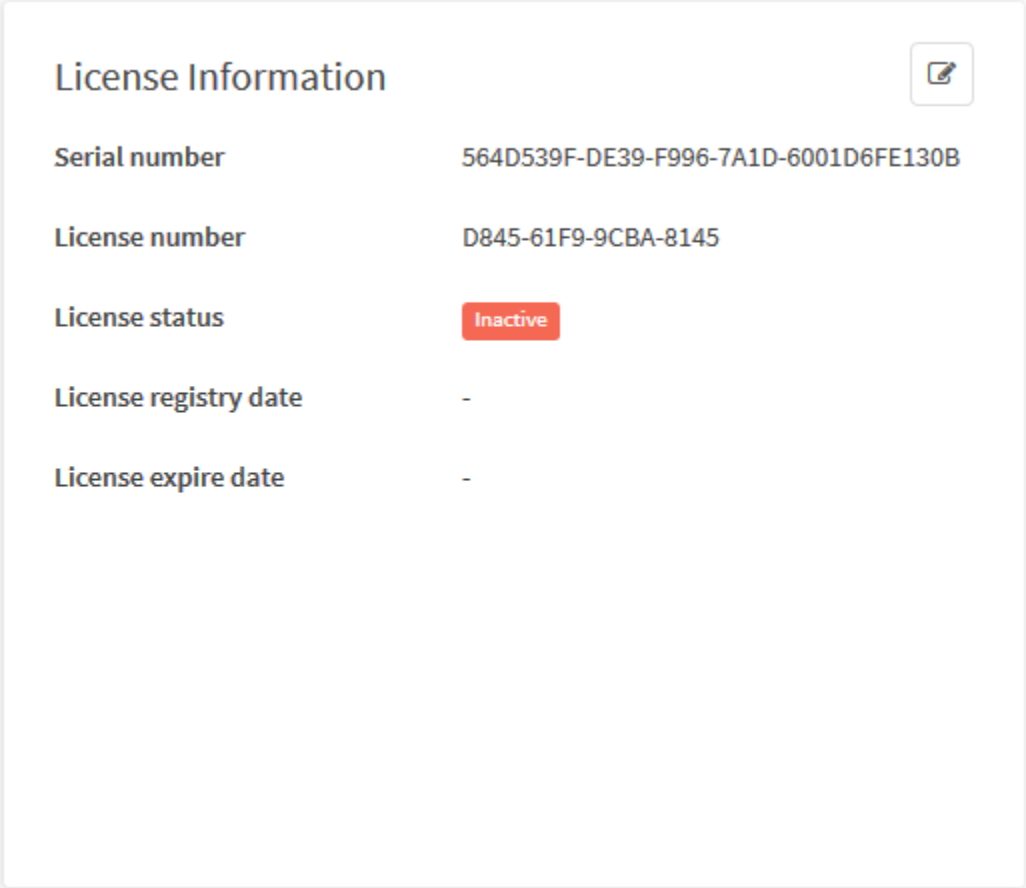
2. Clique em **[**  **]**, a tela abaixo será exibida:



Update License

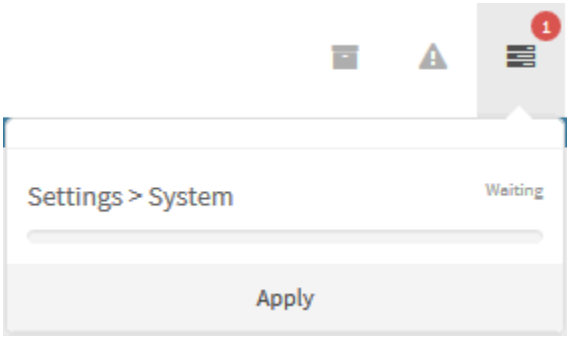
- ***Serial Number*:** Digite o número da licença neste campo. Ex.: D845-61F9-9CBA-8145;
- Após isso clique no botão ***Accept and Save[*** 

] a tela abaixo será exibida.

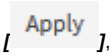


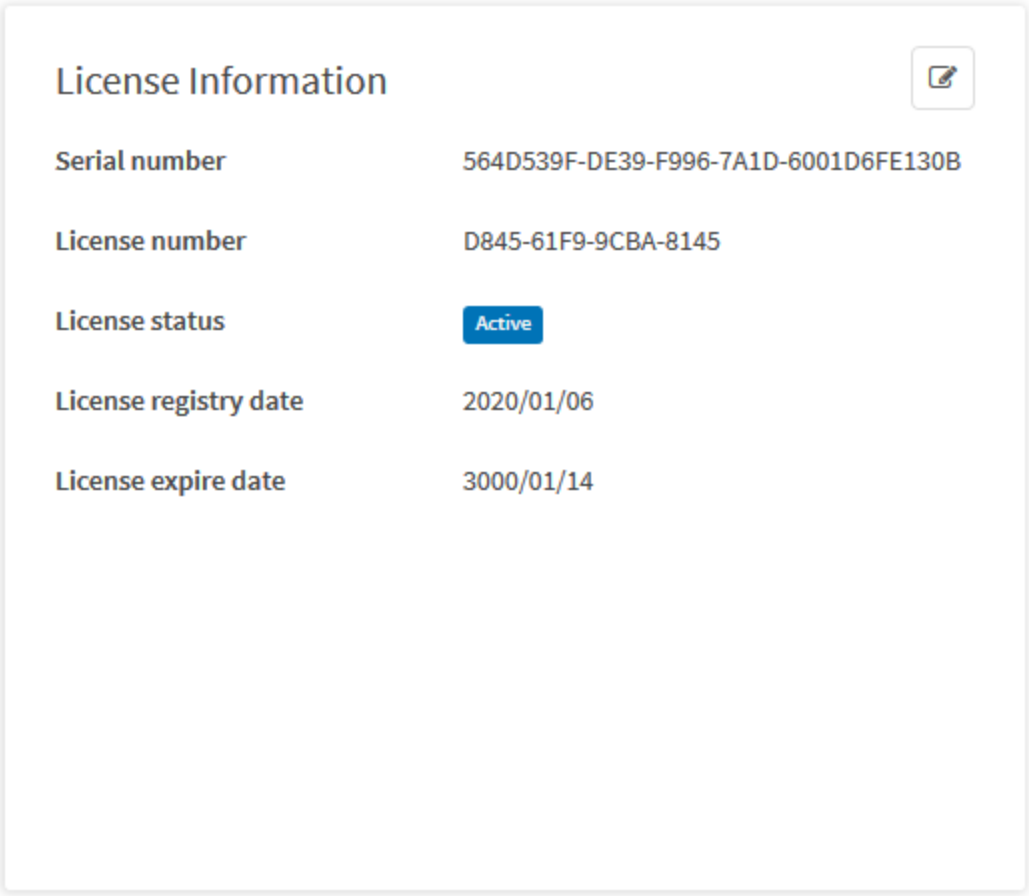
Update License - Inactive

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;



Apply queue

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



Update License - Active

Isso conclui o licenciamento do produto.

ATENÇÃO: Caso o equipamento fique 180 dias sem comunicação com o sistema de licenciamento ininterruptamente o Blockbit UTM terá suas licenças inativadas. Para reaplicar a licença é necessário entrar em contato com o canais oficiais da Blockbit e solicitar o release da licença.

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

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

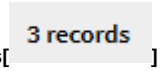
UTM - OPERAÇÃO BÁSICA

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.

Search Bar

Na **área de registros[** 

] exibido na frente da barra de busca, é exibida a quantia de registros localizados pela busca ou presentes antes de efetuar a busca.

Para remover as palavras chaves digitadas na barra de busca, clique no **botão[**  **]**, caso a barra de busca esteja em branco, clique no botão ***search*[**  **]** para voltar a tela inicial.

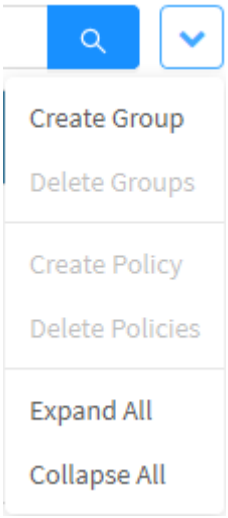
Para executar a busca, adicione a palavra chave desejada e clique no botão ***search*[**  **]**.

Menu de ações

O menu de ações fica alocado no topo direito do painel:

Botão do menu de ações

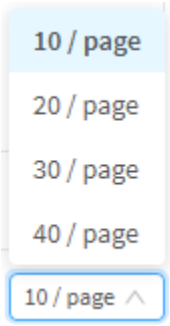
Ao clicar neste botão, um menu com um conjunto de opções contextuais ao painel onde ele estiver localizado será exibido, por exemplo:



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.

Alternar Página

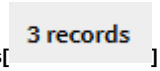
UTM - OPERAÇÃO BÁSICA

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.

Search Bar

Na **área de registros[** 

] exibido na frente da barra de busca, é exibida a quantia de registros localizados pela busca ou presentes antes de efetuar a busca.

Para remover as palavras chaves digitadas na barra de busca, clique no **botão[**  **]**, caso a barra de busca esteja em branco, clique no botão ***search*[**  **]** para voltar a tela inicial.

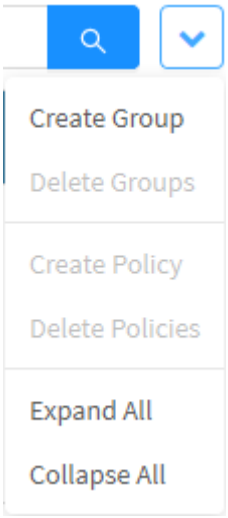
Para executar a busca, adicione a palavra chave desejada e clique no botão ***search*[**  **]**.

Menu de ações

O menu de ações fica alocado no topo direito do painel:

Botão do menu de ações

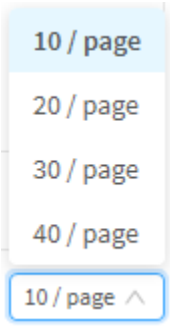
Ao clicar neste botão, um menu com um conjunto de opções contextuais ao painel onde ele estiver localizado será exibido, por exemplo:



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.

Alternar Página

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[ ]**.

Na tela abaixo o menu do usuário aparece com o nome “admin”, isso ocorre pois foi esse o nome cadastrado no item “Name” no capítulo Assistente de instalação.

Menu de perfil do usuário

O menu de perfil do usuário é composto das opções:

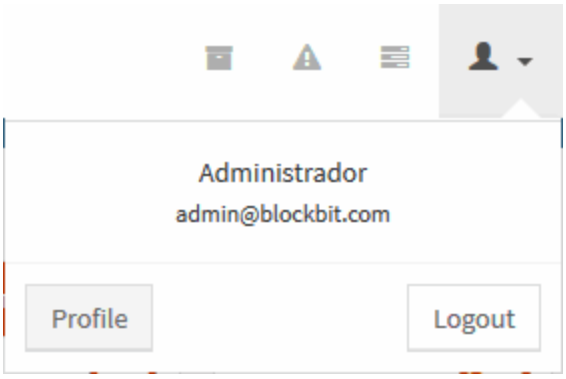
- *Profile*;
- *Logout*.

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*”;

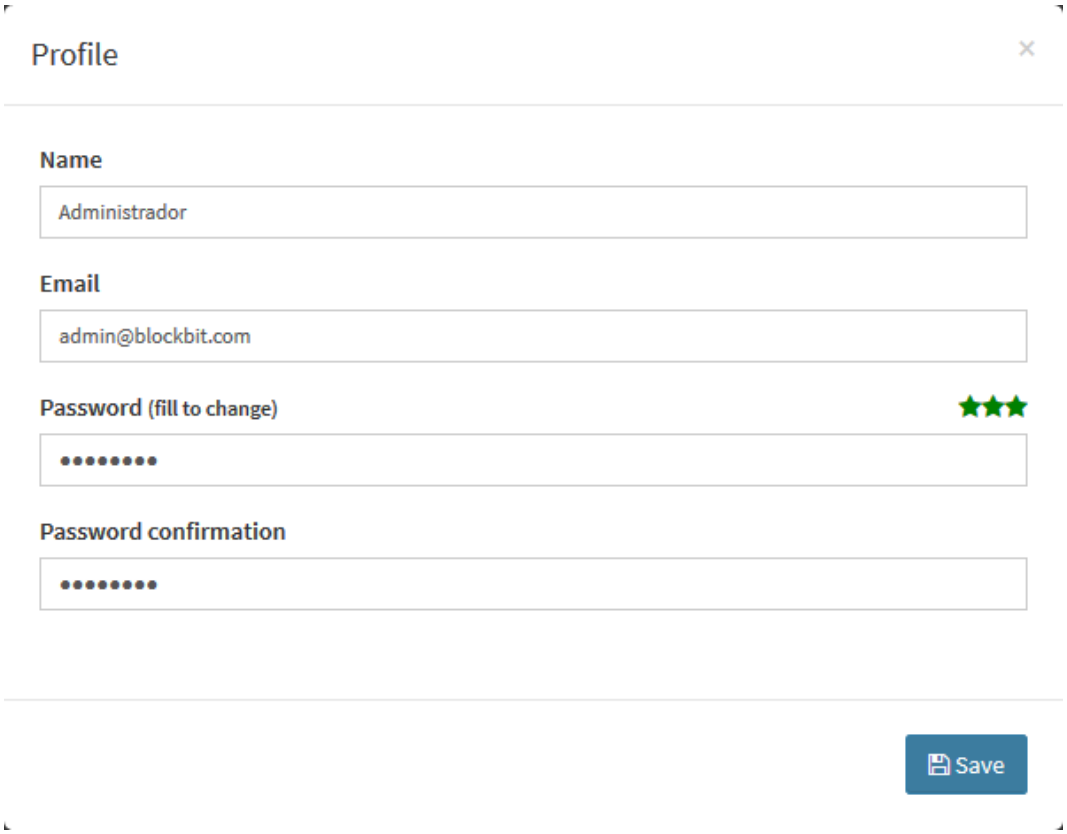


Menu do usuário – Botão “*Profile*”

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: " & | ; > < ' .



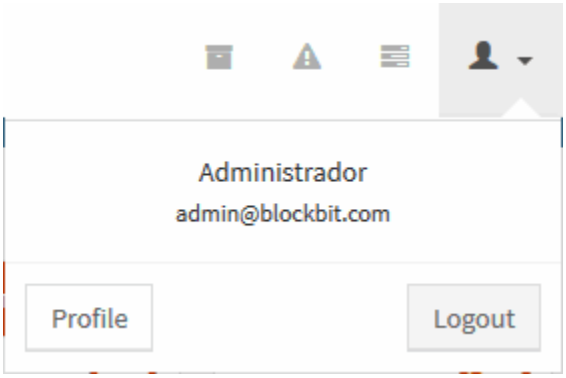
Menu do usuário – *Edit Profile*

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

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

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

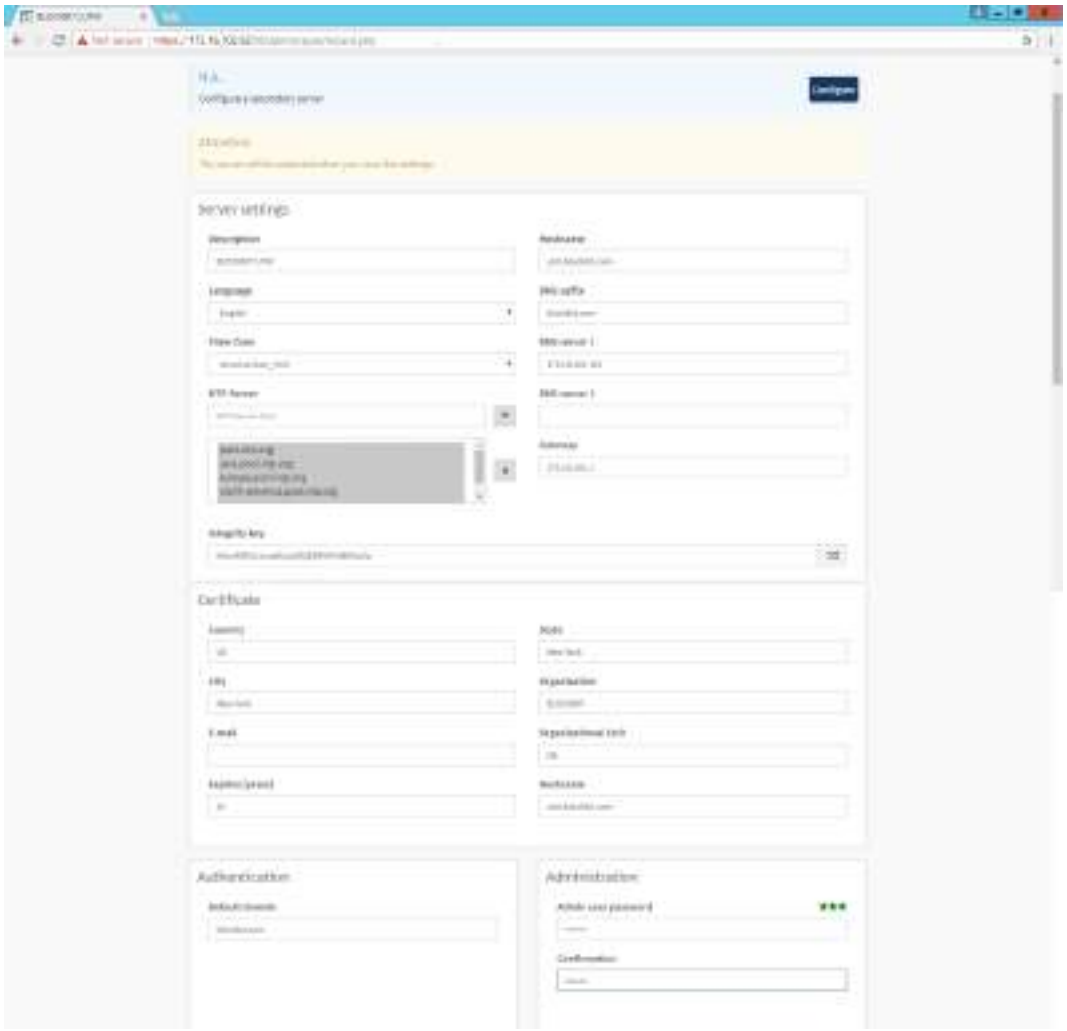
Esta seção irá apresentar como configurar o Assistente de Instalação do Blockbit UTM.

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;



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.

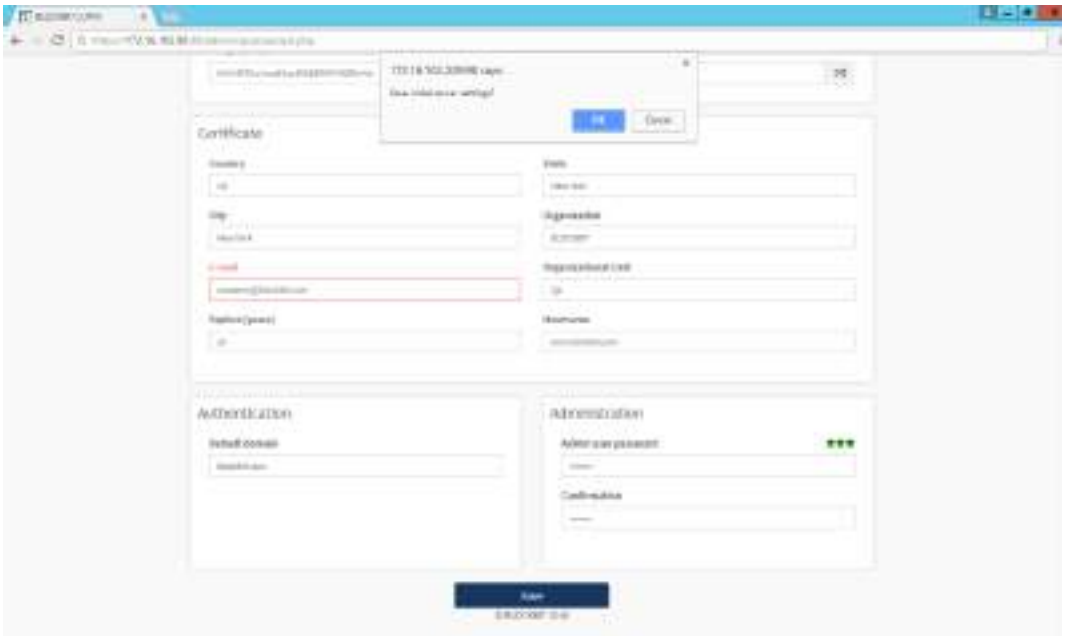
4. Digite os seguintes dados no frame "*Authentication*", define o domínio local padrão para a autenticação de usuários do Blockbit UTM.

- ***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.



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:

Fila de comandos

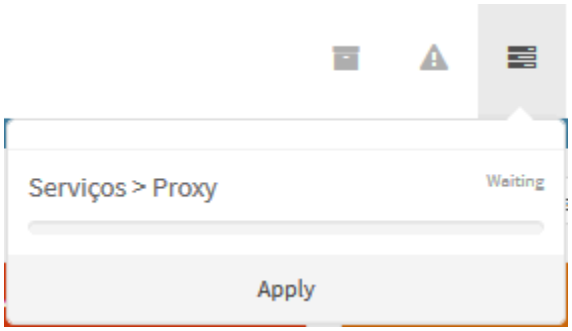
Esta seção irá demonstrar como aplicar comandos e alterações efetuadas ao Blockbit UTM.

Caso a execução de algum comando esteja pendente na fila de comandos, o ícone denotará isso exibindo com uma marcação vermelha a quantia de comandos no aguardo:

Ícone indicando comandos pendentes

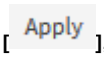
É importante salientar que: A fila de comandos sempre considera a última alteração efetuada. Assim sendo, caso tenha se arrependido de alguma configuração, basta refazê-la e aplicar a fila de comandos.

Ao clicar no ícone, surgirá uma tela listando tudo que precisa ser aplicado, conforme demonstrado abaixo:

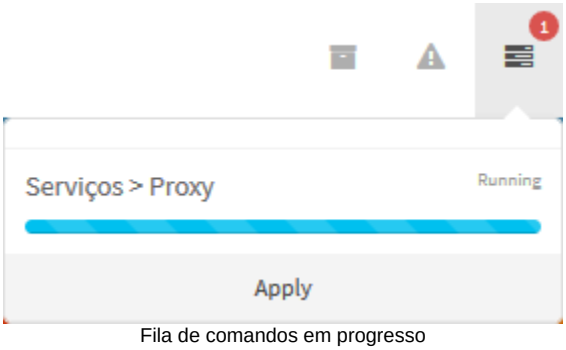


Fila de comandos pendentes

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.

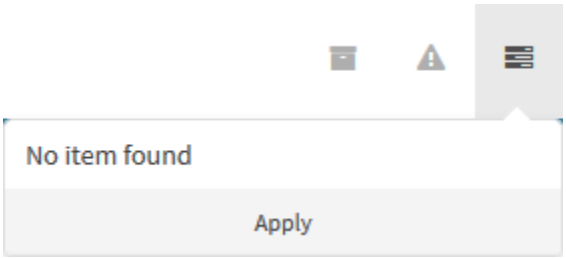
Para aplicar todos os comandos, basta clicar no botão **[** 

], o processo iniciará, como exemplificado pela imagem abaixo:



Fila de comandos em progresso

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

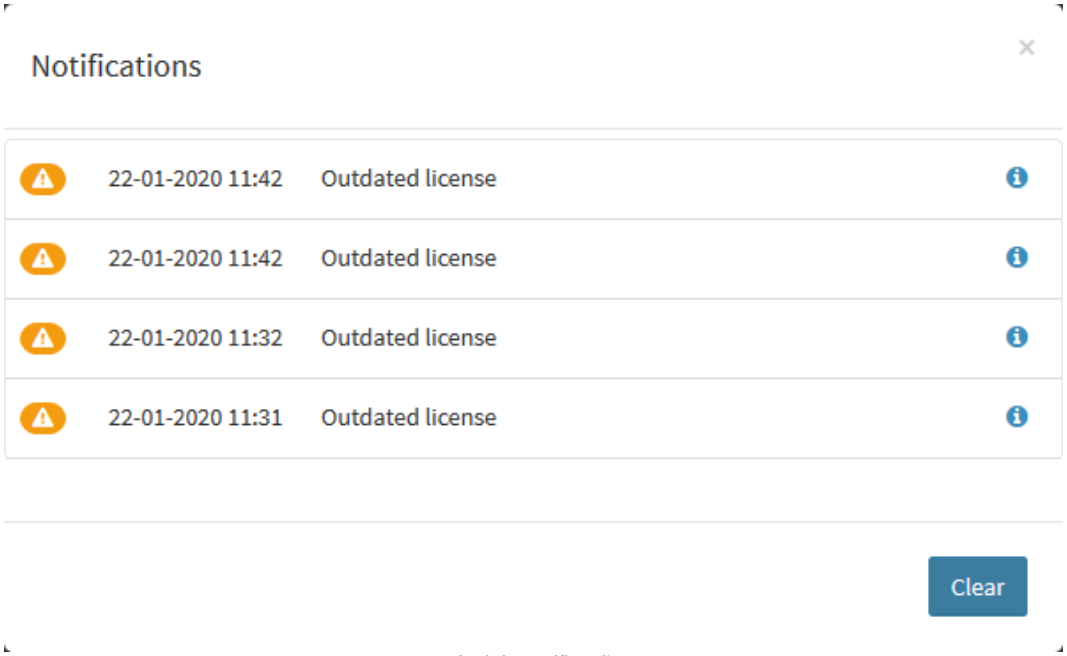


Fila de Comandos Ociosa

UTM - NOTIFICAÇÕES

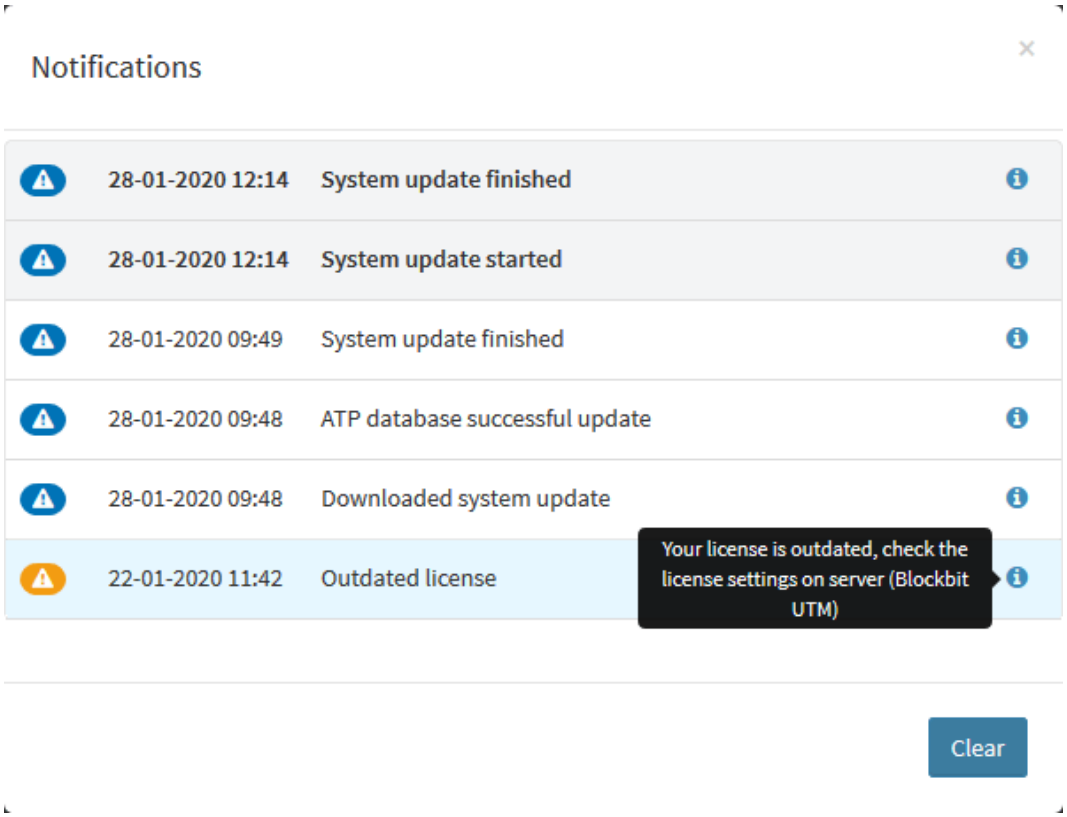
Alguns eventos que ocorrerão no Blockbit UTM irão gerar alertas, estes serão exibidos no painel de notificações, elas são configuradas na aba *Notifications* em *System* no menu *Settings*, para mais informações consulte esta página.

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

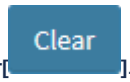


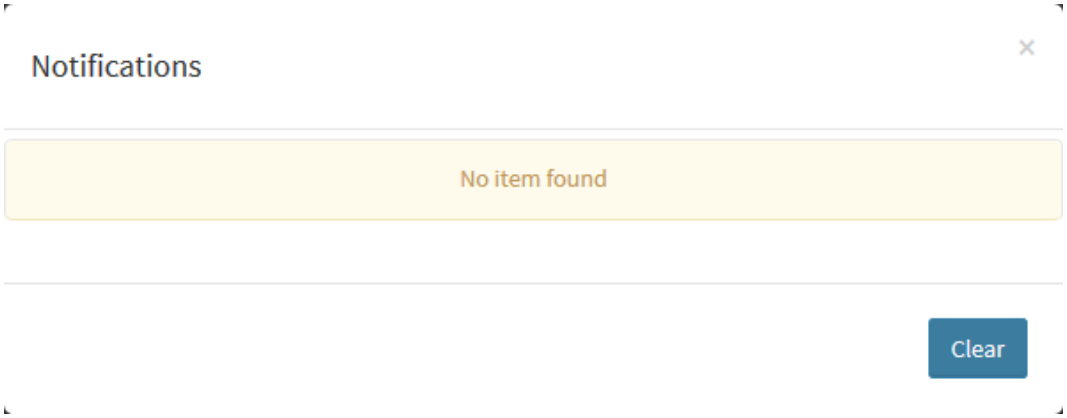
Painel de Notificações

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



Painel de Notificações - Informações

Caso deseje limpar o painel de notificações, clique no botão **Clear**[].



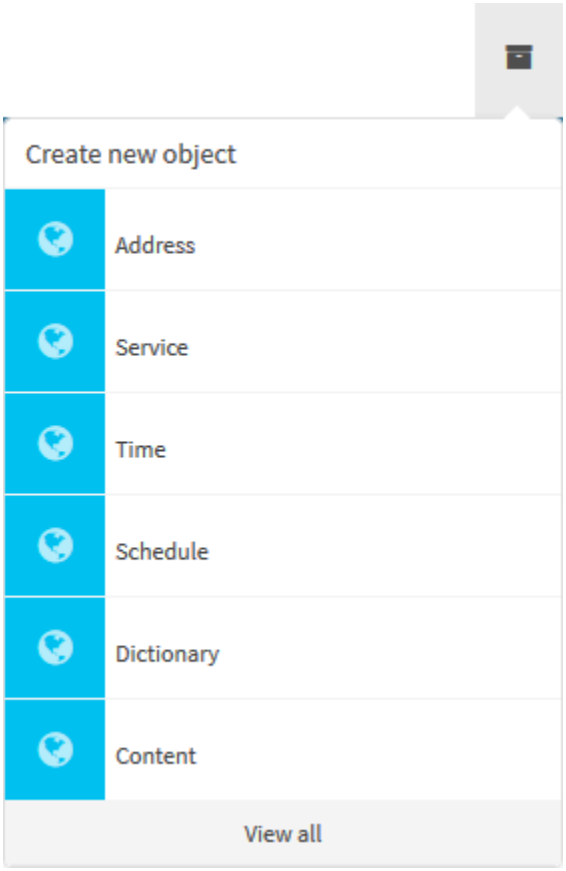
Painel de Notificações - *No item found*

Por fim, para fechar a janela clique fora dela ou no [] localizado no topo da tela.

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[ ]**.



Menu de Objetos

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:

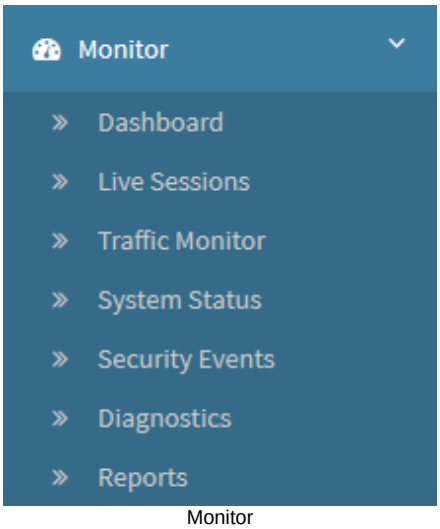
Menu de Objetos - Criando objeto de endereço

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, *web 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*;
- *Live Sessions*;
- *Traffic Monitor*;
- *System Status*;
- *Security Events*;
- *Diagnostics*;
- *Reports*.

Monitor - Dashboard

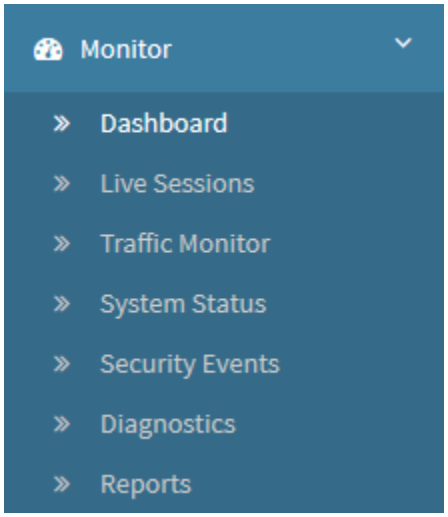
O Dashboard exibe em tempo real o estado atual do sistema de forma centralizada e consistente através de vários *logs* sumarizados os principais eventos do sistema, histórico de acesso de usuários, monitor de tráfego e diversos outros registros que podem ser utilizados para análise de risco, comportamento 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).

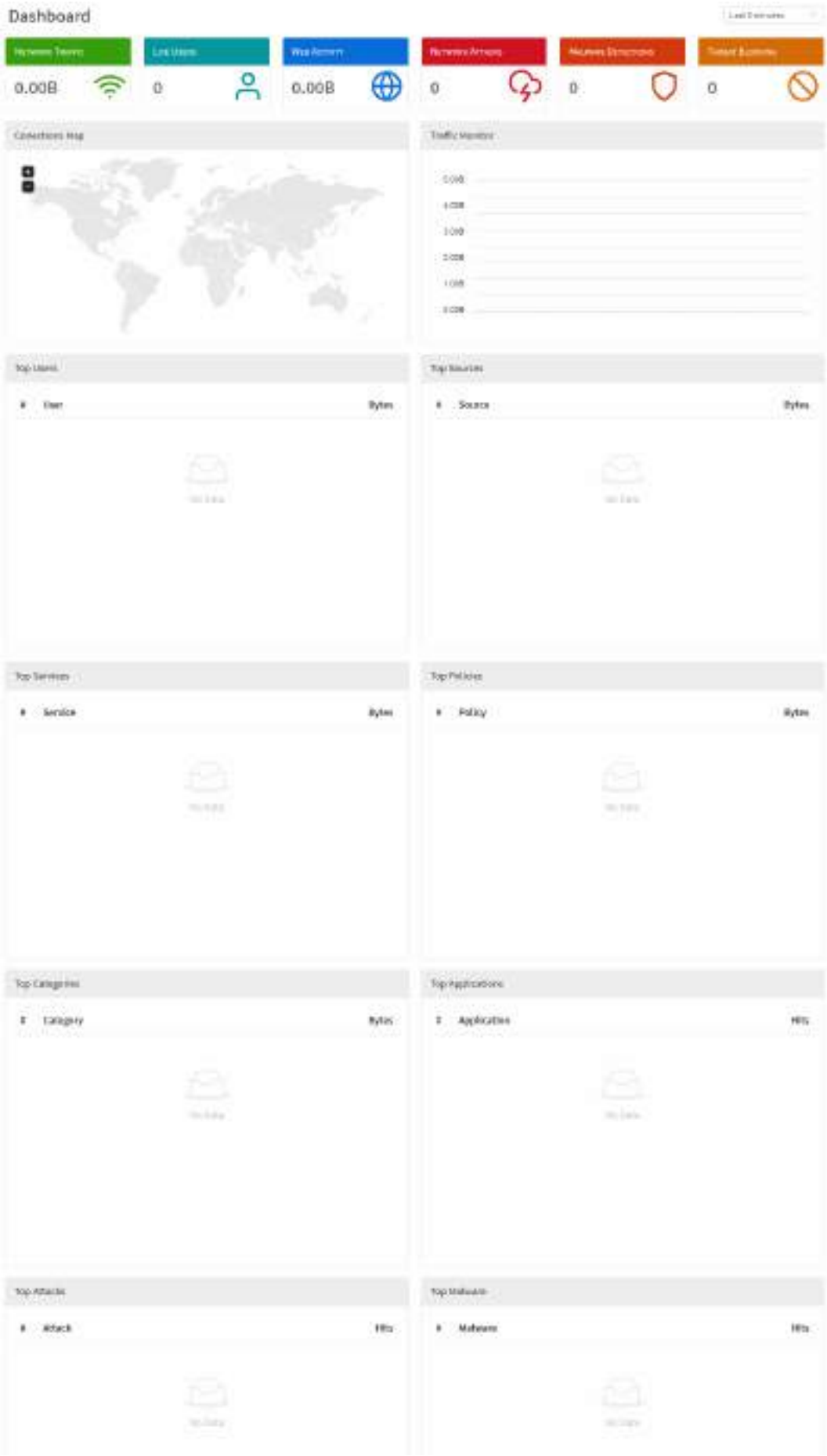
Por padrão, todas as informações dos relatórios detalhados, de todos os módulos, são armazenadas por 7 (sete) dias ou até atingir 70% de uso do disco. Caso a capacidade máxima de armazenamento seja atingida, a retenção destas informações será interrompida. Caso deseje alterar este limite de armazenamento,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



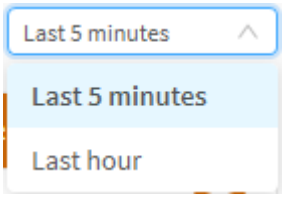
Monitor – Dashboard

A tela abaixo será exibida:


Dashboard
0.00B
0
0.00B
0
0
0
Top Users
User
Bytes
Top Sources
Source
Bytes
Top Services
Service
Bytes
Top Policies
Policy
Bytes
Top Categories
Category
Bytes
Top Applications
Application
Hits
Top Attacks
Attack
Hits
Top Malware
Malware
Hits

Dashboard – Visão Geral

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:



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.

O *Traffic Monitor* tem como função exibir informações em tempo real e sempre irá exibir os últimos 5 minutos. A seleção de 5 minutos ou 1 hora se aplica aos demais *widgets* que mostram dados sumarizados.

Os relatórios e gráficos disponíveis no *Dashboard* são:

- *Network Traffic*;
- *Live Users*;
- *Web Activity*;
- *Network Attacks*;
- *Malware Detections*;
- *Threat Blocking*;
- *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.*

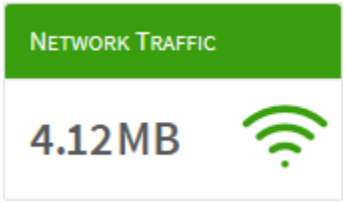
Dashboard - Widgets

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

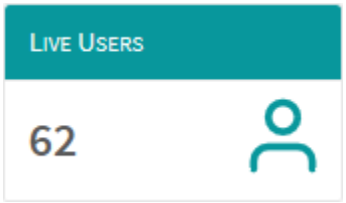
O *widget* "*Network Traffic*" exibe o volume total de todo o tráfego de rede realizado em todas as interfaces de rede do Blockbit UTM.



Dashboard – Network Traffic

Live Users

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



Dashboard – Live Users

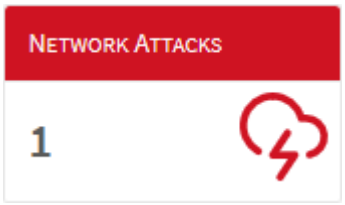
Web Activity

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

Dashboard – Web Activity

Network Attacks

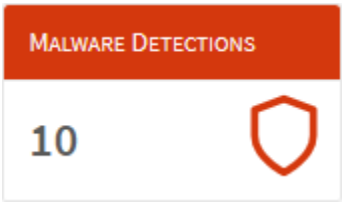
O *widget* "*Network Attacks*" exibe o volume total de tentativas de ataques realizados em todas as interfaces de rede do Blockbit UTM.



Dashboard – Network Attacks

Malware Detections

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



Dashboard – Malware Detections

Threat Blocking

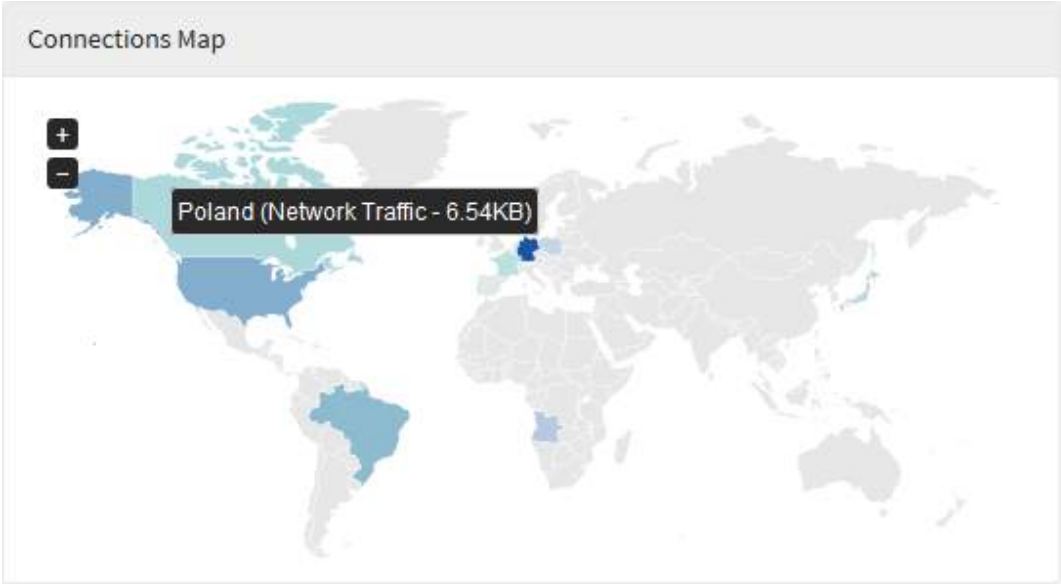
O *widget* "*Threat Blocking*" exibe o total de ameaças bloqueadas através de todas as técnicas do módulo *Advanced Threat Protection* (*ATP*) em todas as interfaces de rede do Blockbit UTM.

Dashboard – Threat Blocking

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.

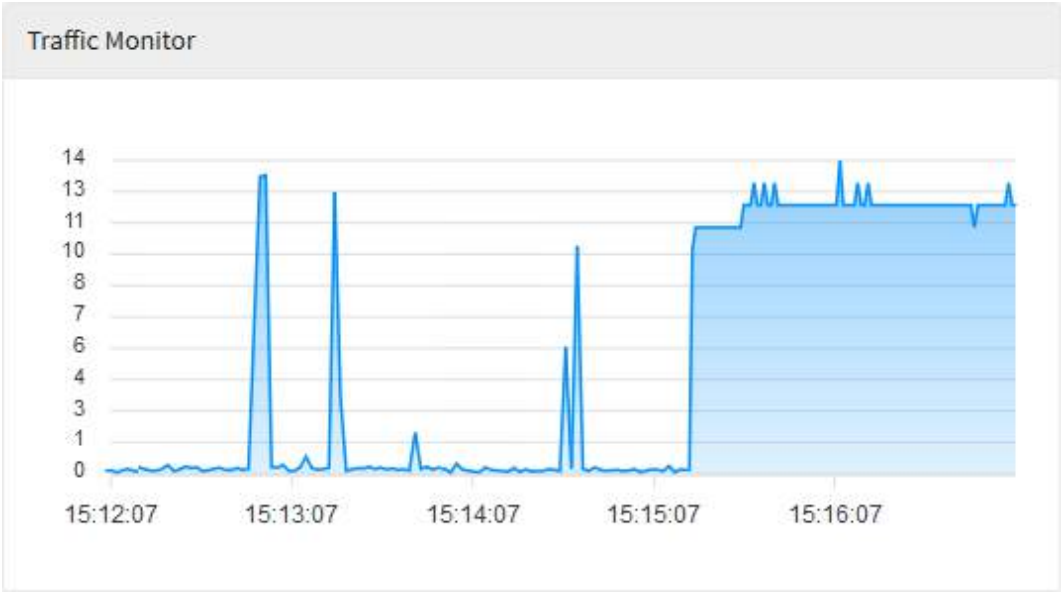
Além disso, ao passar o mouse por cima dos países, o país referente a esse valor é destacado no mapa e um número total de acessos é exibido.



Dashboard – Connections Map

Traffic Monitor

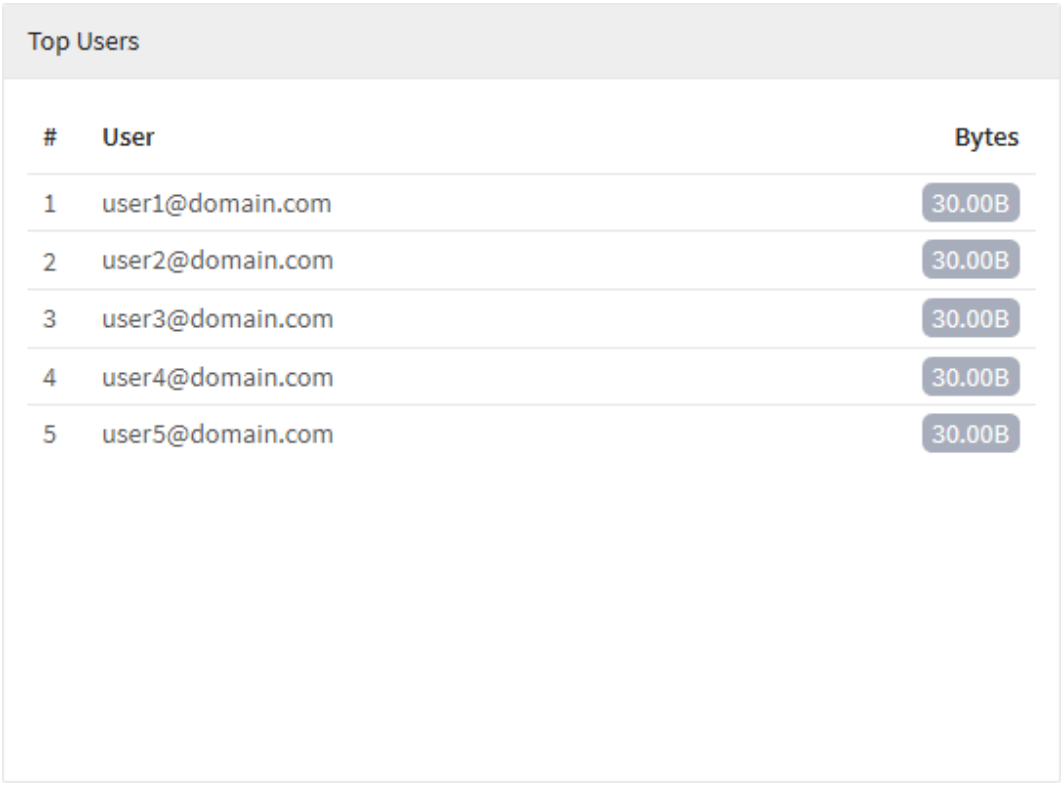
Em "*Traffic Monitor*", é possível visualizar o tráfego de rede em tempo real. Ao passar o mouse por cima do gráfico, um resumo de todo o tráfego do período é exibido.



Dashboard – Traffic Monitor

Top Users

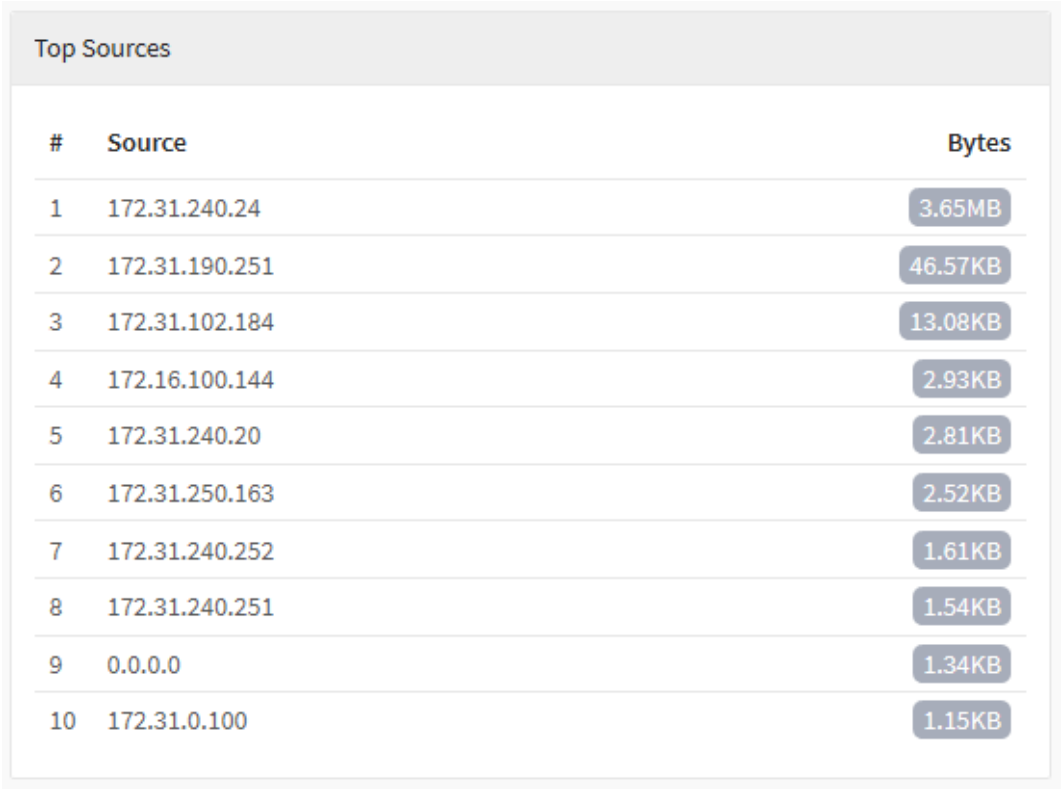
Em "*Top Users*", temos uma listagem de dez usuários classificados por ordem de maior quantia de acessos e seu respectivo consumo e seu respectivo uso.



Dashboard – Top Users

Top Sources

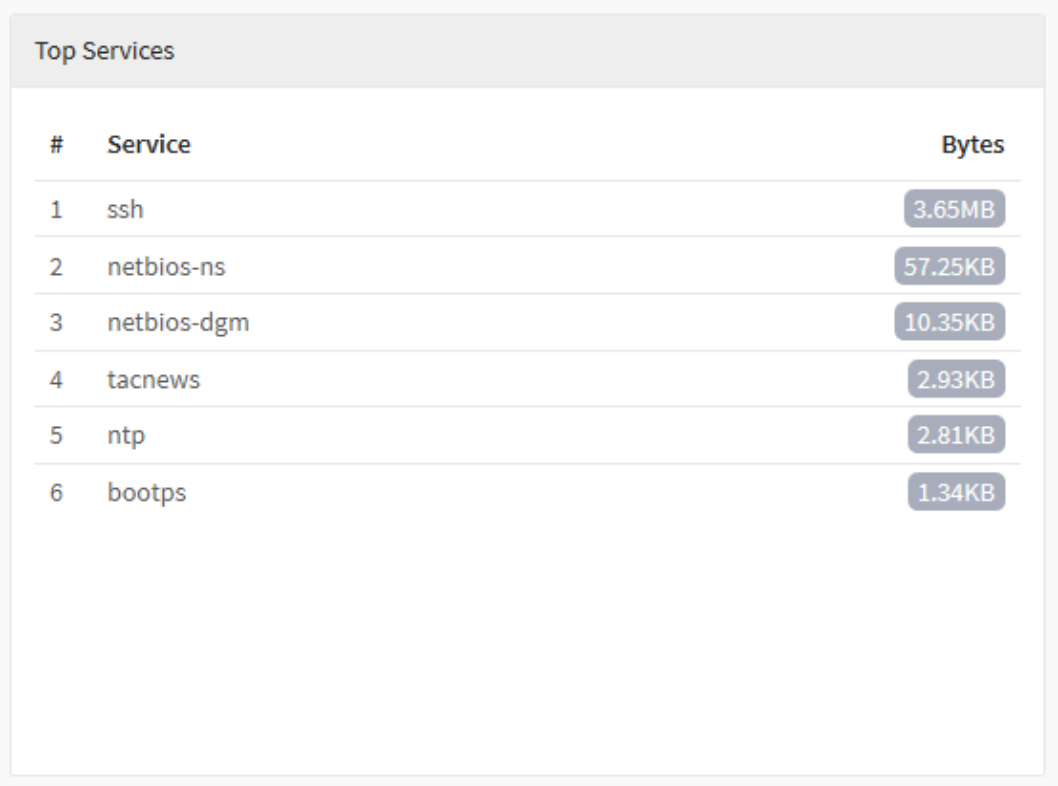
Em "*Top Sources*", temos uma listagem de dez maiores fontes de tráfego de rede classificadas por ordem de acesso e seu respectivo uso.



Dashboard – Top Sources

Top Services

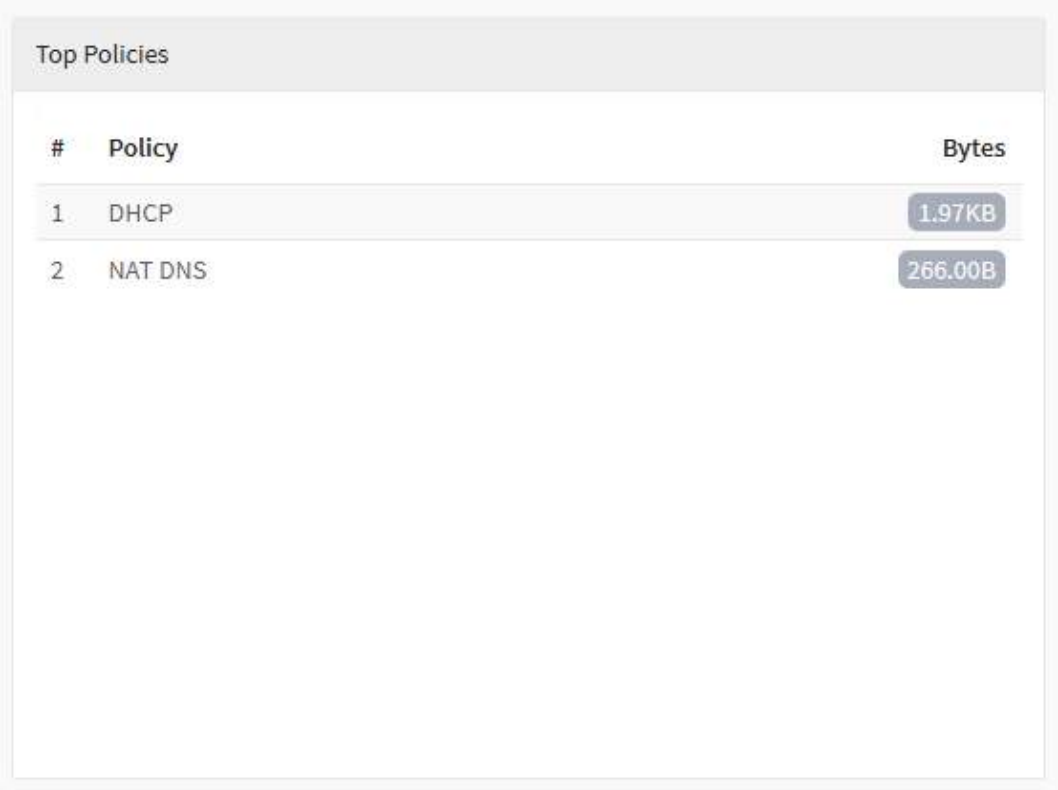
Em "*Top Services*", temos uma listagem de dez tipos de serviços mais usados, sendo estes classificados por ordem de uso.



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.



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.

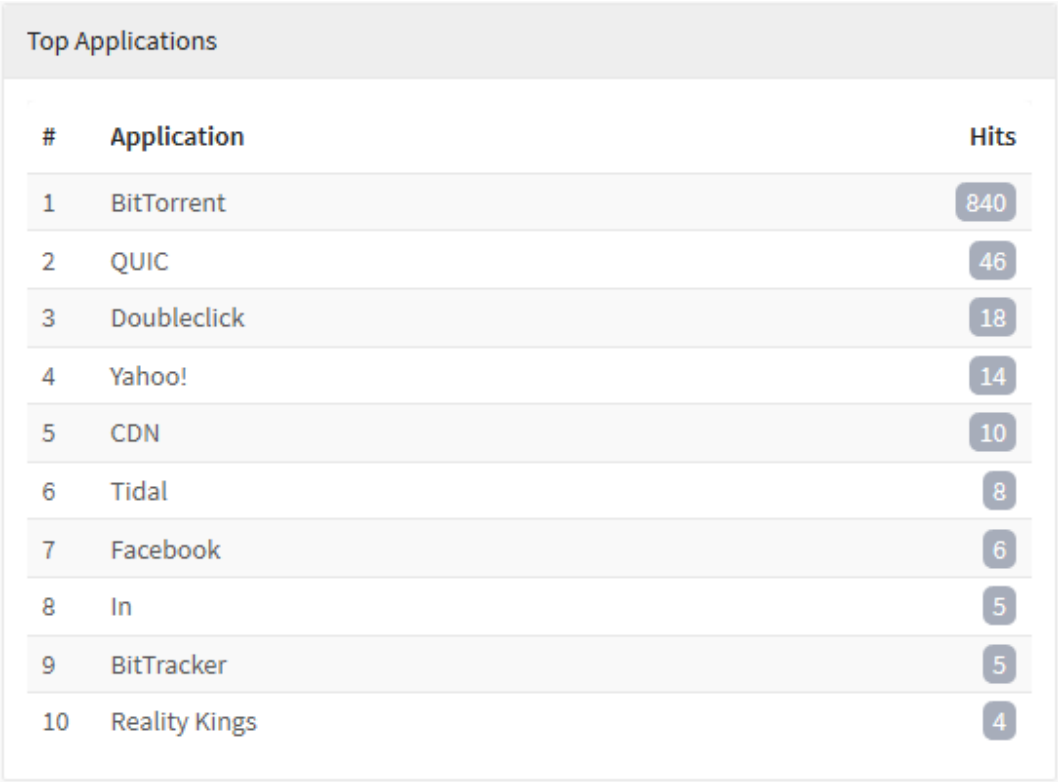
Top Categories

#	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.



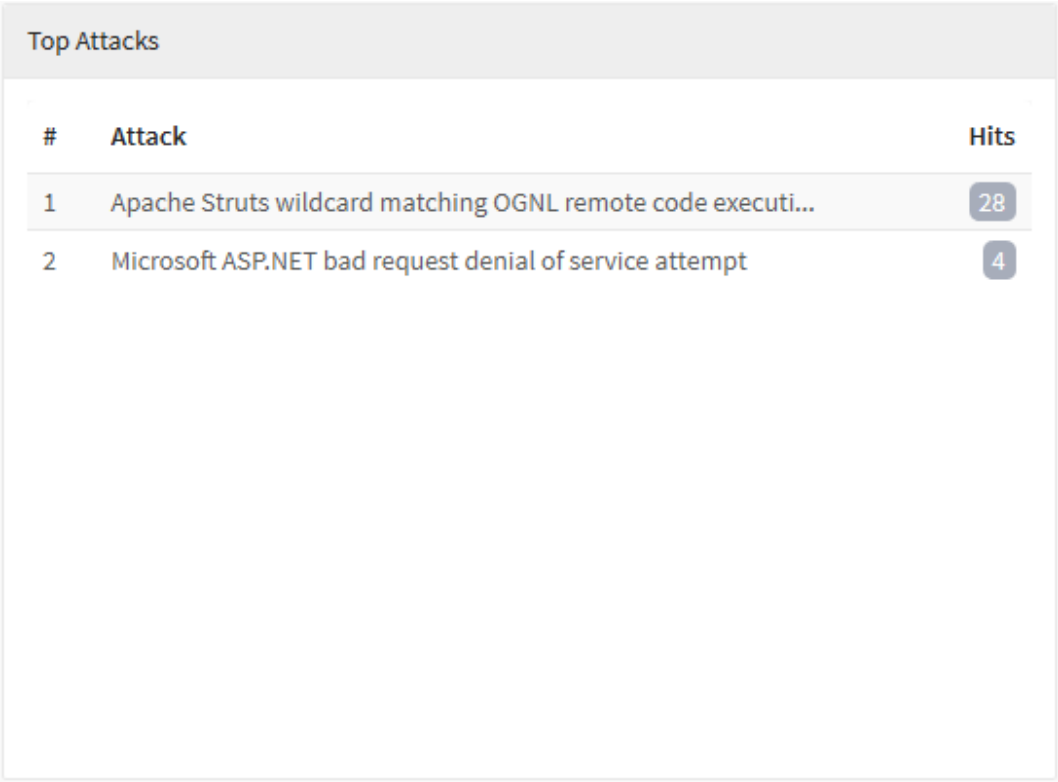
Top Applications

#	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

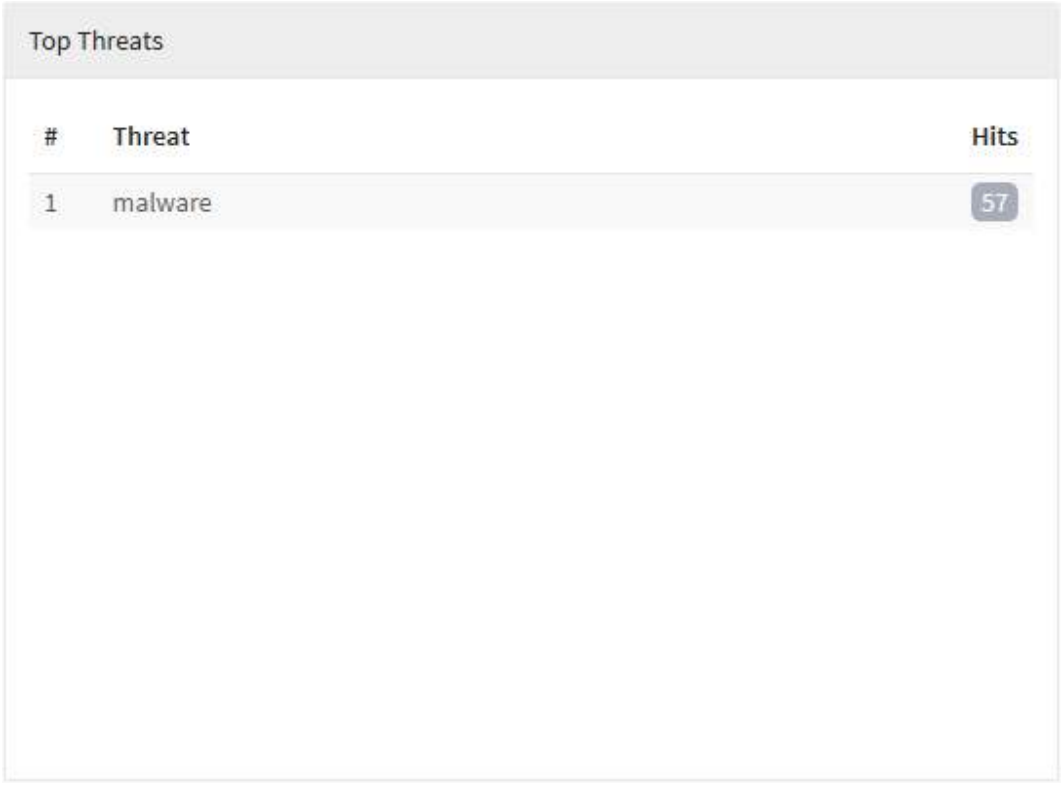
Em "*Top Attacks*", temos uma listagem dos dez tipos de ataque cibernéticos mais recorrentes, sendo estes classificados por ordem de ocorrência.



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.



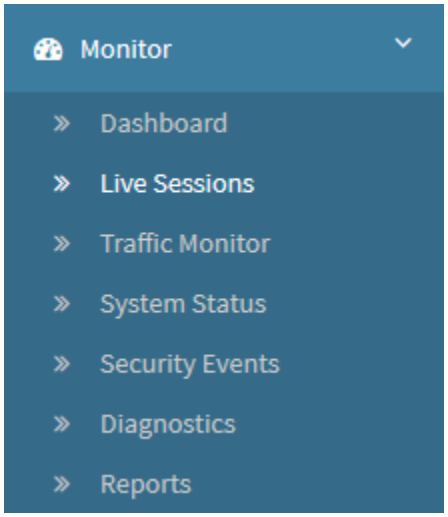
Dashboard – Top Threats

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

Monitor - Live Sessions

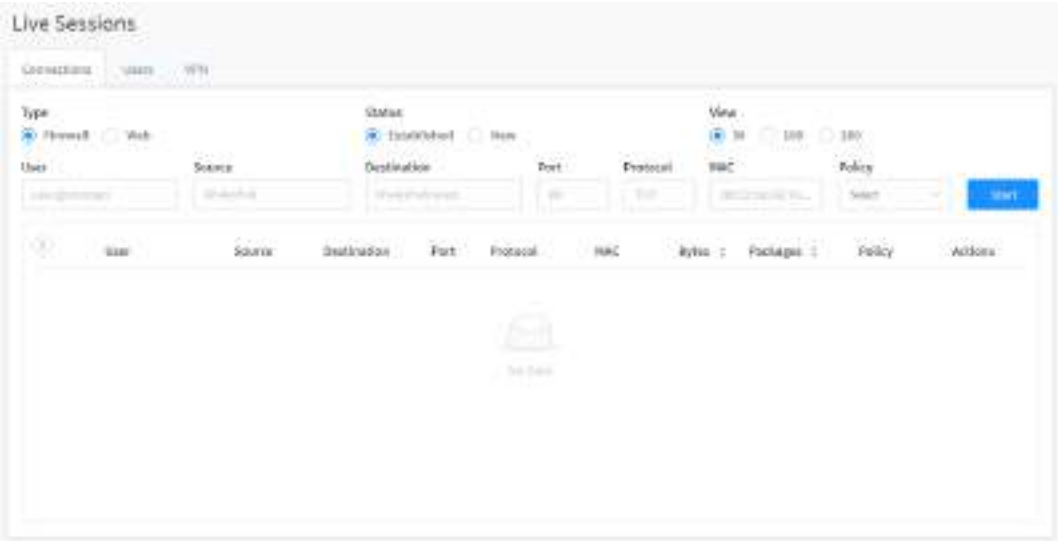
Este recurso permite que o administrador monitore o tráfego de rede em tempo real, determinando com garantia qual acesso (ou tentativa) gerou *log*. O sistema está dividido em dois tipos: *Firewall* e *Web*, o primeiro efetua o monitoramento de todo o tráfego realizado no *firewall* e o segundo executa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

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



Monitor – Live Sessions

A tela abaixo será exibida:



Monitor - Live Session - Live Connections

A tela *Live Sessions* comporta as seguintes abas:

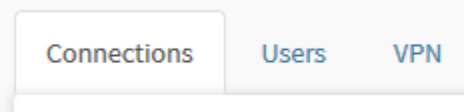
- *Connections*;
- *Users;*
- *VPN.*

A seguir analisaremos os componentes da aba *Live Connections*.

Live Sessions - Connections

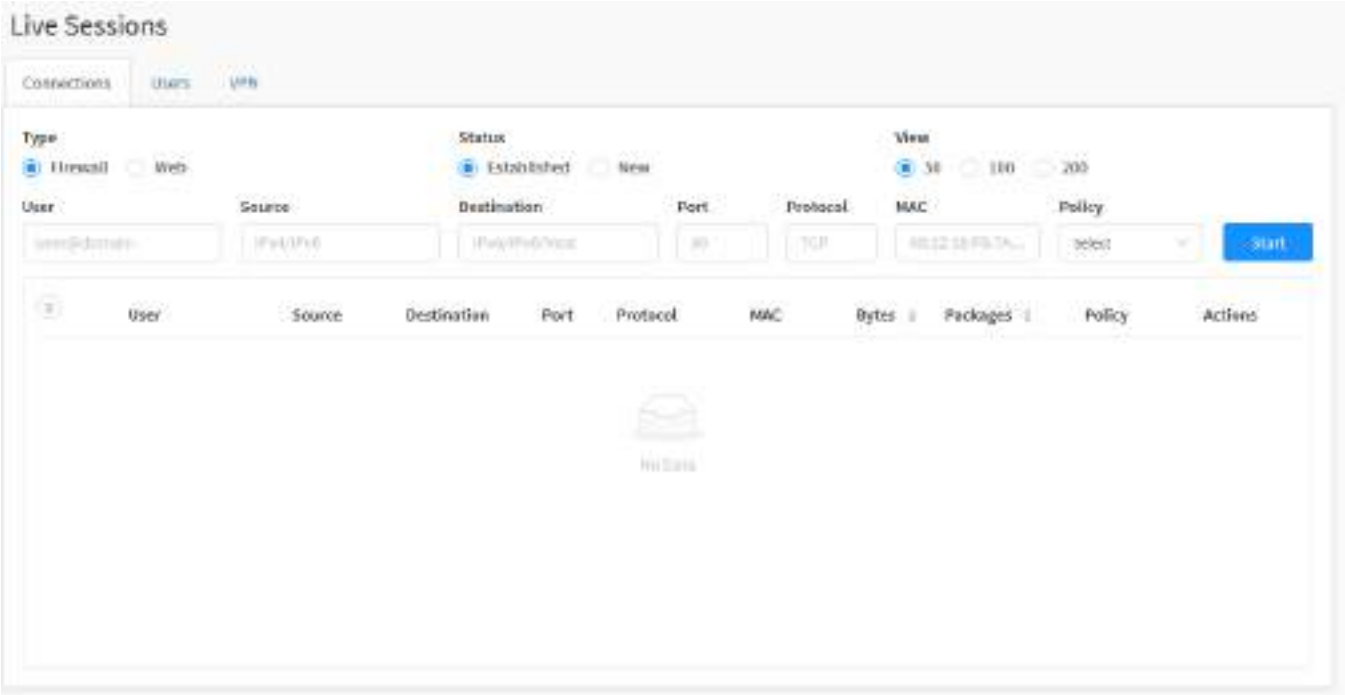
Nesta aba é possível averiguar a atividade atual no *firewall* e na *web*, sendo possível filtrar por usuário, origem, destino, porta, protocolo ou política.

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



Aba *Connections*

Surgirá a tela “*Connections*”, conforme demonstrado pela imagem abaixo:



Connections

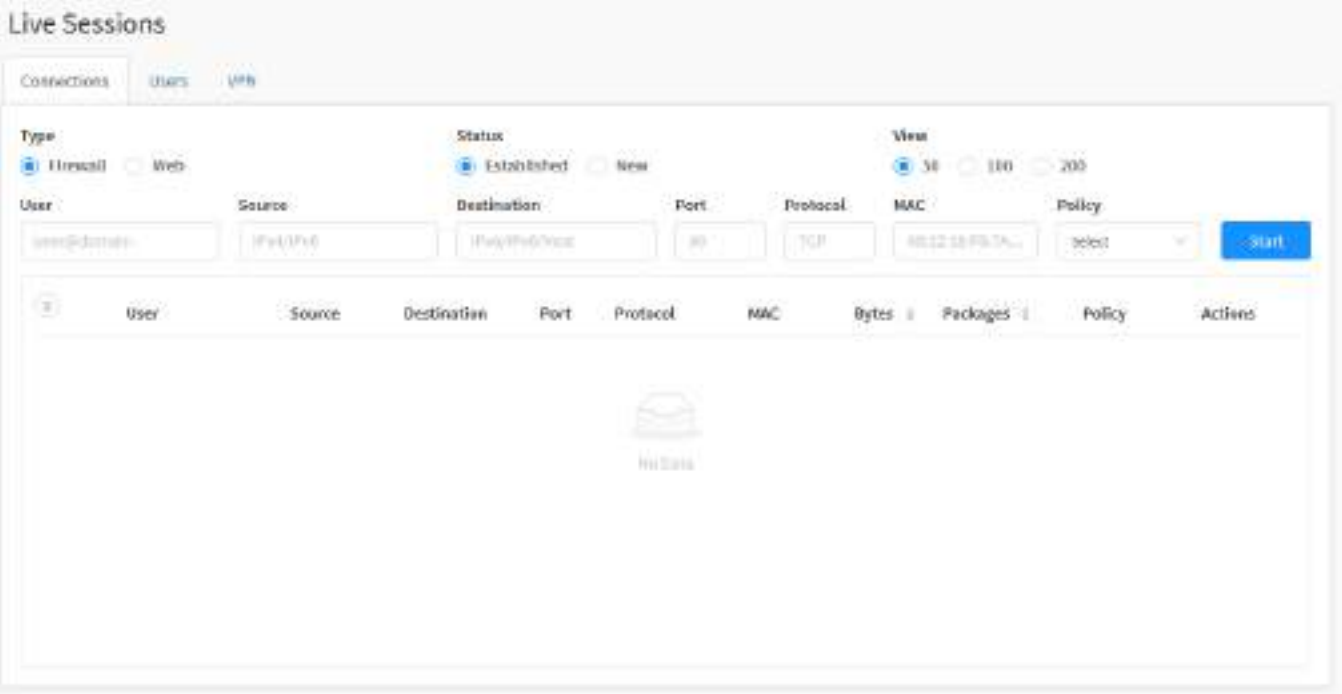
Esta sessão irá abordar:

- 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

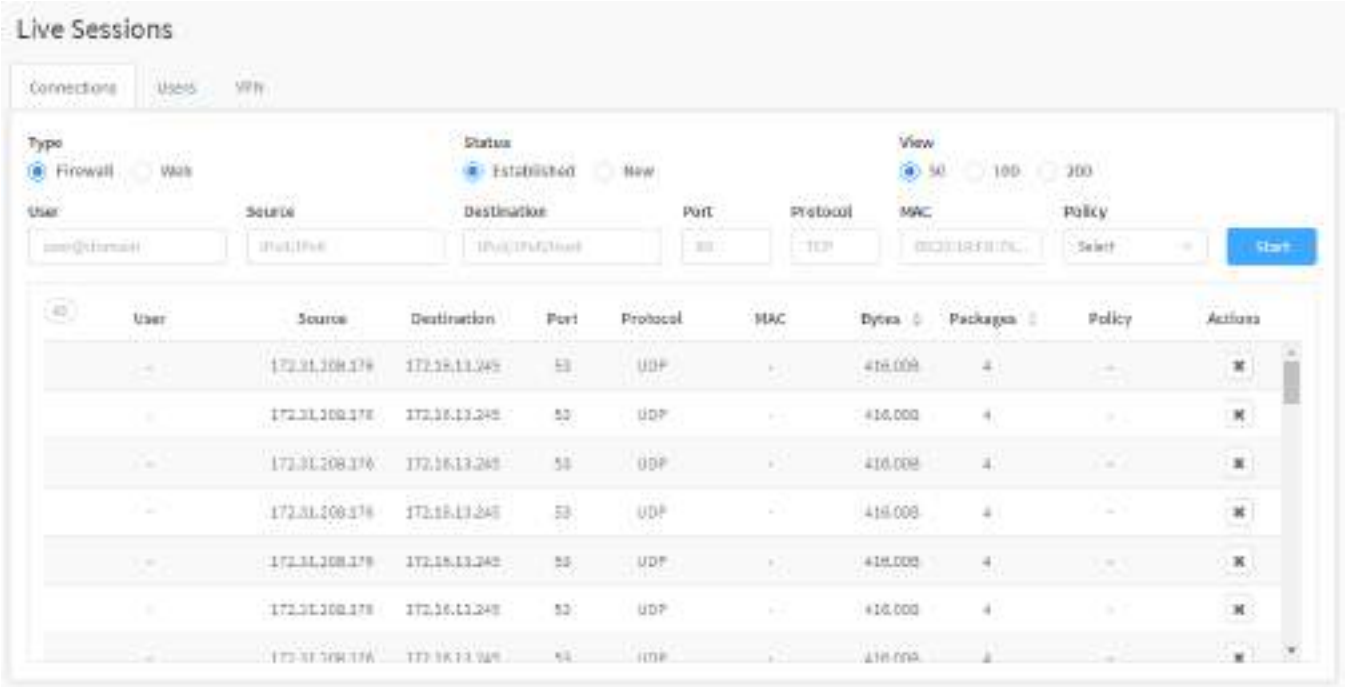
O painel *Connections* é composto dos seguintes recursos:



Connections

- ***Type:*** Determina o tipo de monitoramento estre as opções:
  - ***Firewall[ ]*:** Ao selecionar esta opção, se opta pelo monitoramento de todo o tráfego realizado no *firewall*;
  - ***Web[ ]*:** 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.

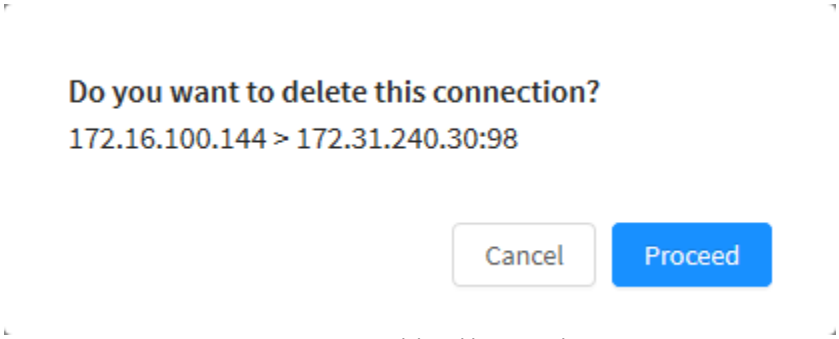
Os resultados são exibidos na tabela abaixo das opções:



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

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.

Clique no botão [Proceed] para deletar a conexão ou [Cancel] para fechar esta janela.

Connection successfully deleted

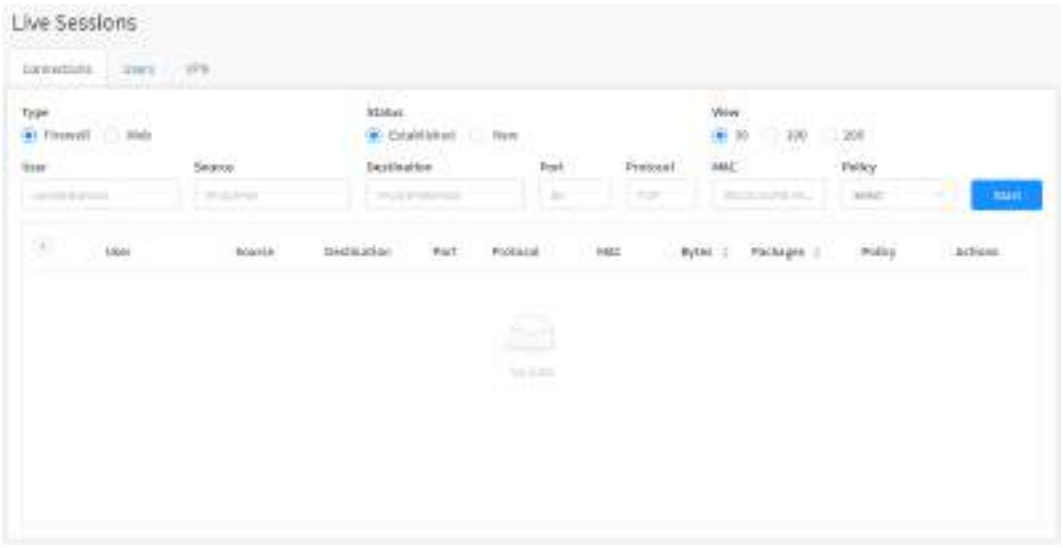
Por fim, para efetuar o monitoramento, basta clicar em [Start]. Caso um monitoramento já esteja sendo executado, é possível interrompê-lo clicando em [Stop].

Connections - Firewall

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

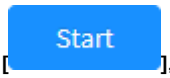
Firewall - Established

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

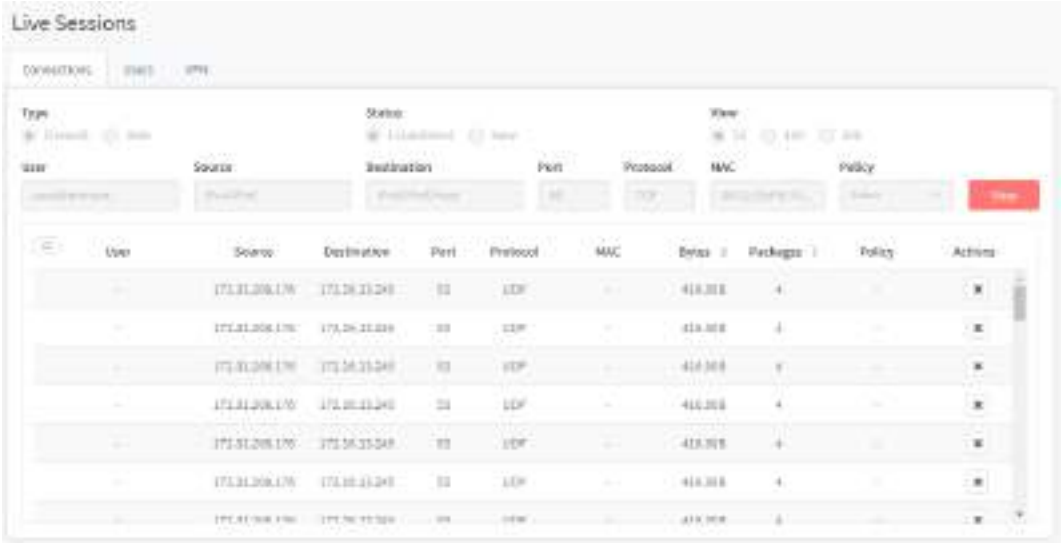


Connections- Firewall - Established

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

Feito isso, clique no botão ***Start*** [

], os resultados serão exibidos conforme demonstrado abaixo:



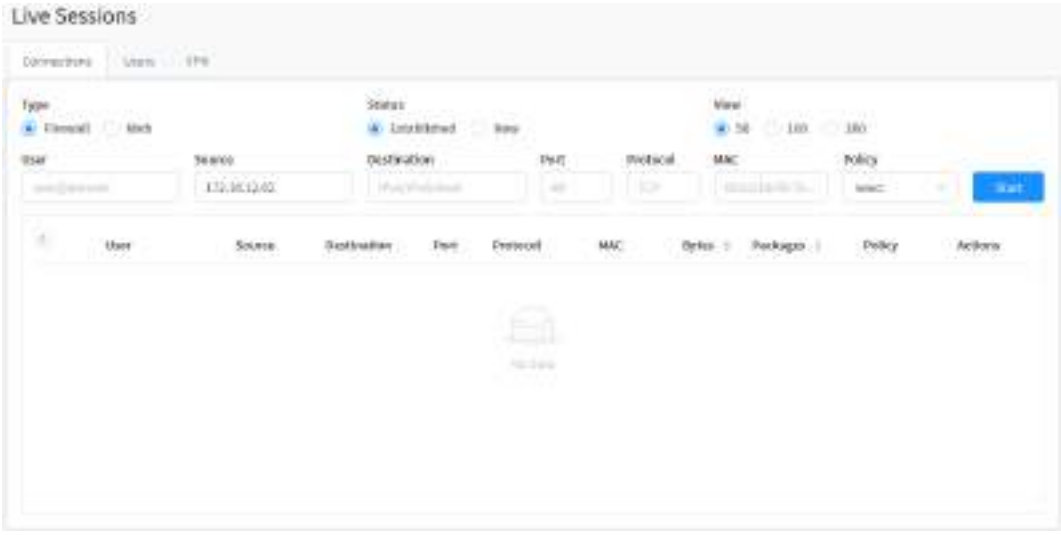
Connections - Firewall - Established - Results

Para interromper o monitoramento basta clicar no botão ***Stop***[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*.

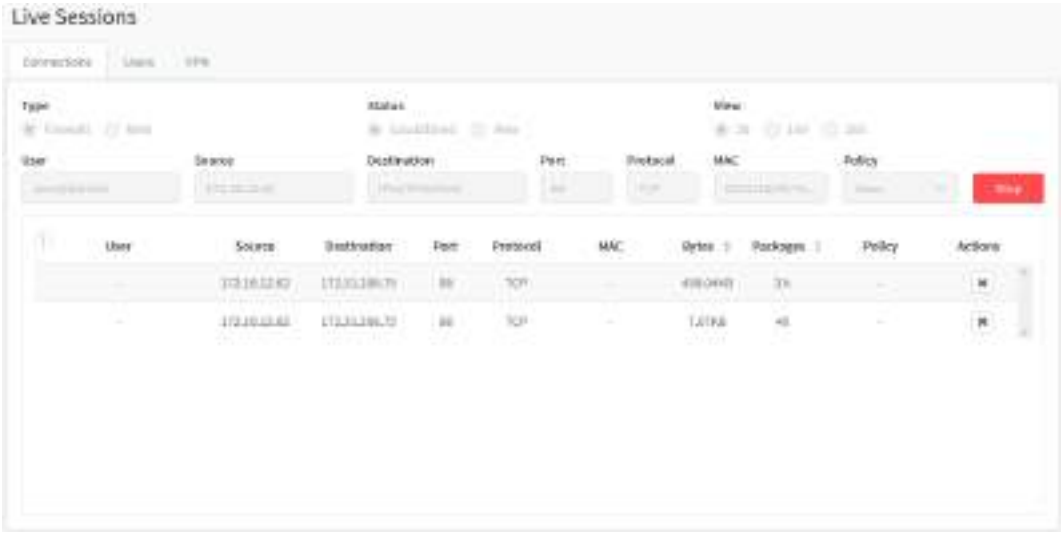
Segue um exemplo de como efetuar monitoramento de *IP* de origem:



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.

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

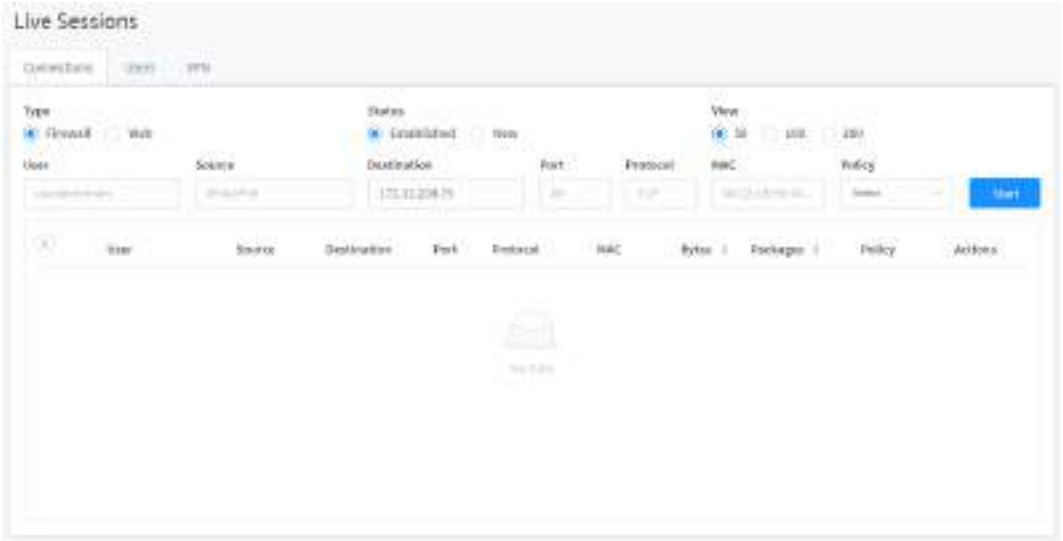


Connections - Firewall - Established - Source IP - Results

Para interromper o monitoramento basta clicar no botão ***Stop***[Stop].

Firewall - Established - Destination

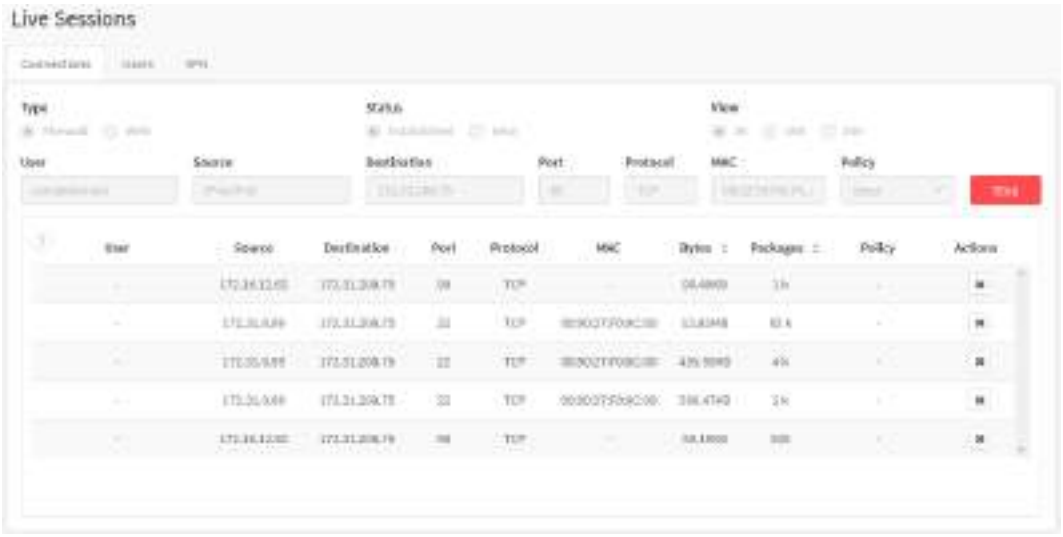
A seguir veremos um exemplo de como efetuar monitoramento de *IP* de destino:



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:

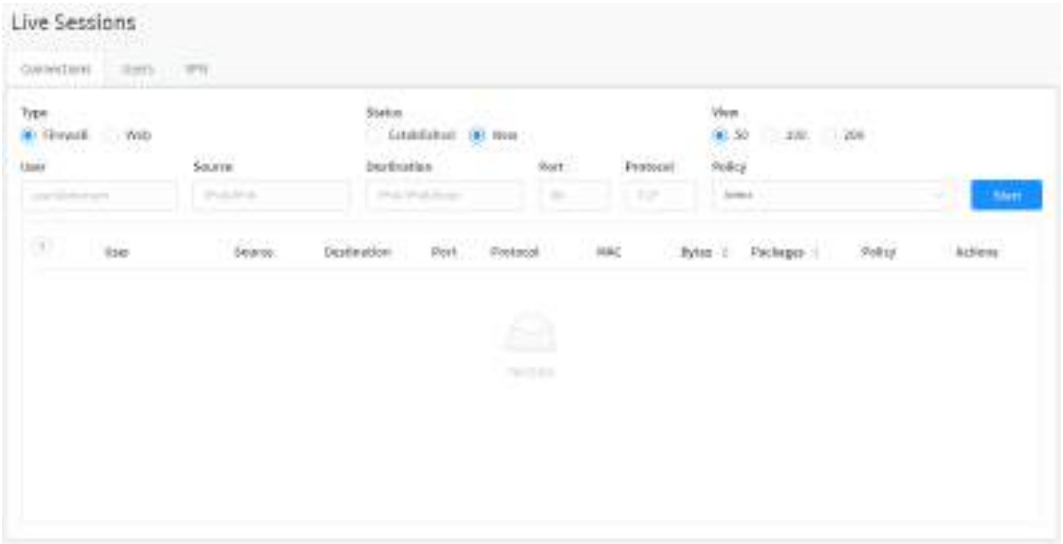


Connections - Firewall - Established - Destination IP - Results

Para interromper o monitoramento basta clicar no botão ***Stop***[Stop].

Firewall - New

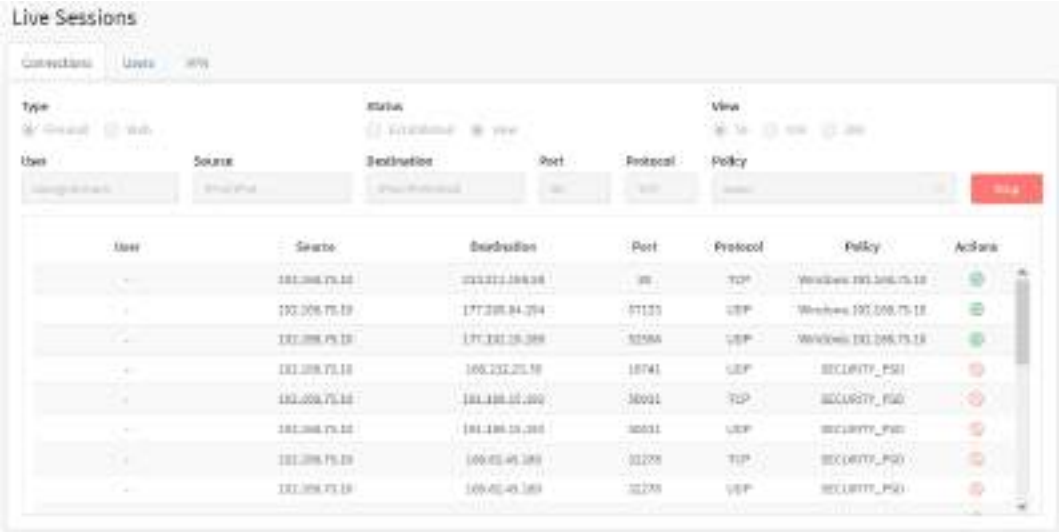
Ao clicar sobre o *status New* e *type Firewall,* é possível realizar o monitoramento de novos acessos.



Connections - Firewall - New

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

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



Connections - Firewall - New - Results

Para interromper o monitoramento basta clicar no botão ***Stop***[Stop].

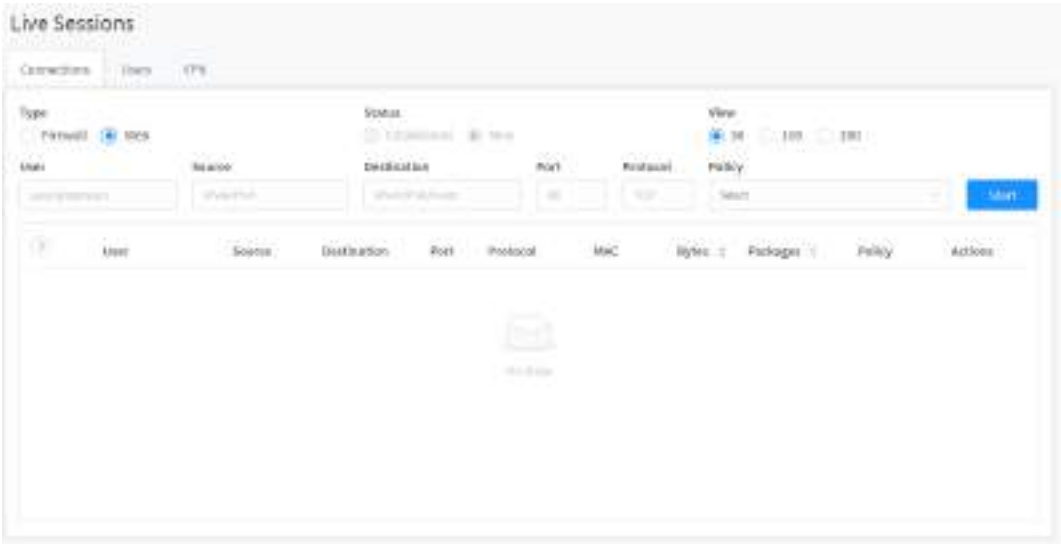
Para mais informações a respeito de cada campo desta tela, cheque esta página.

Connections - Web

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

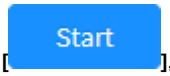
Web - New

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

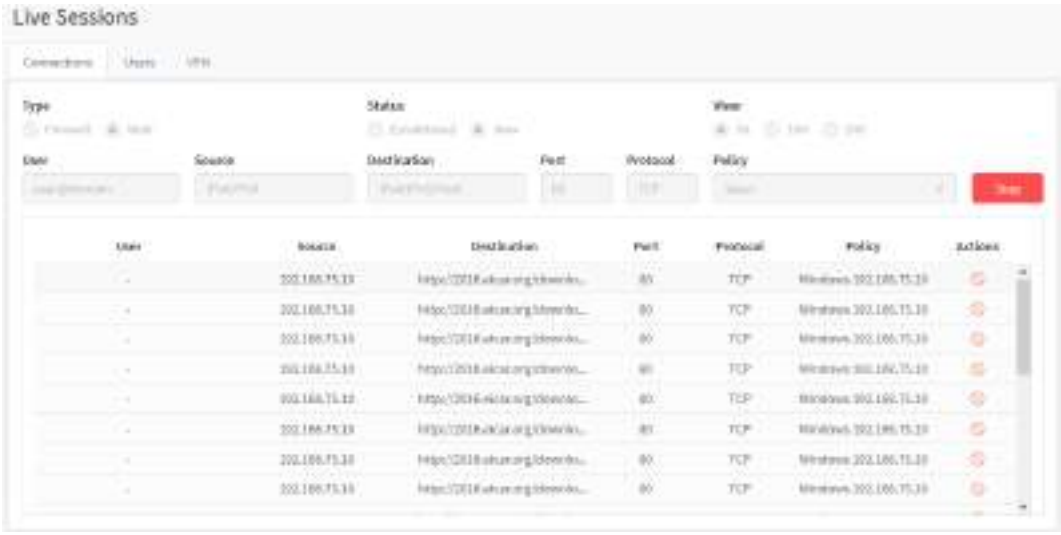


Connections- Web - New

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

Feito isso, clique no botão ***Start*** [

], os resultados serão exibidos conforme demonstrado abaixo:



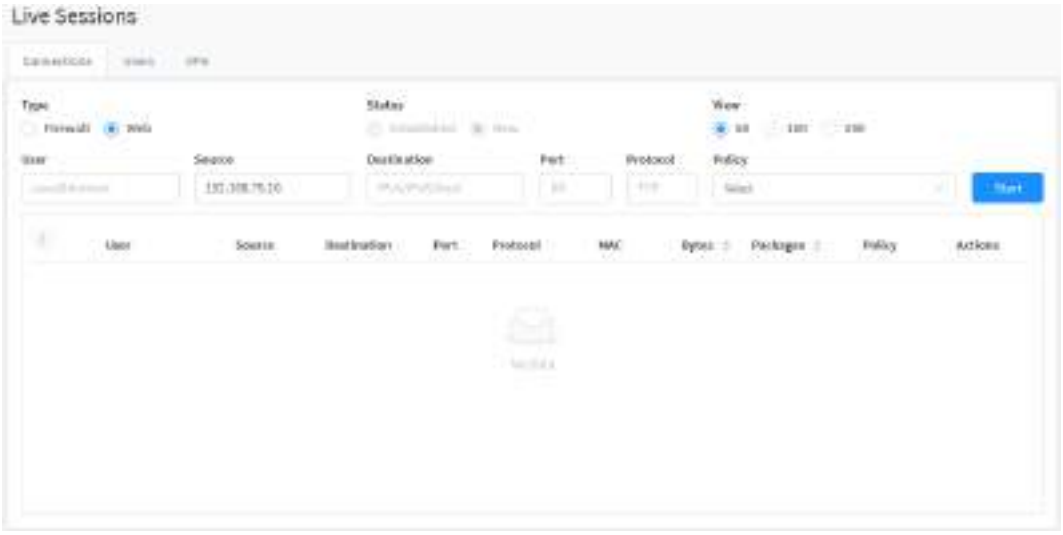
Connections - Web - *New* - *Results*

Para interromper o monitoramento basta clicar no botão ***Stop***[Stop].

Web - New - Source

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

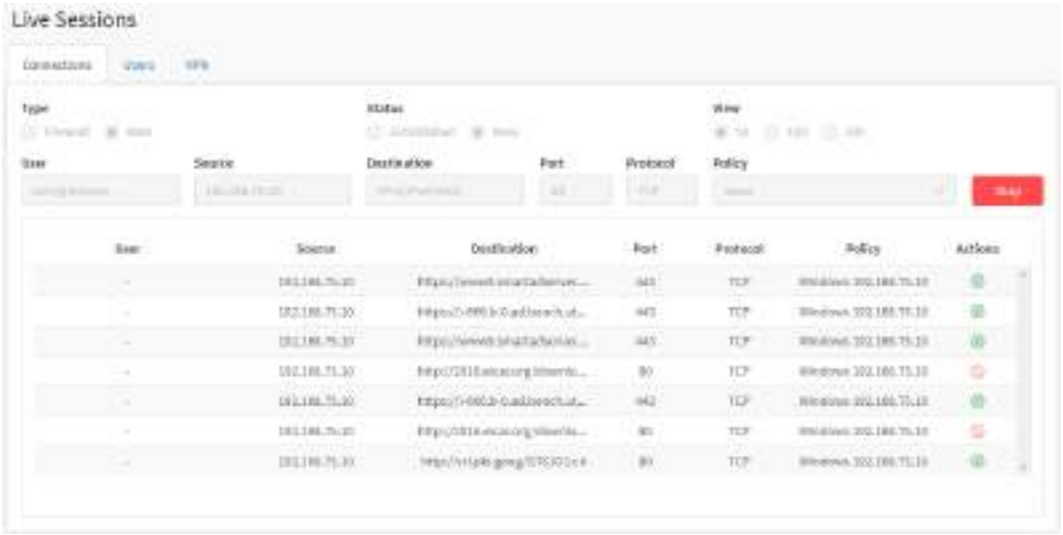
Segue um exemplo de como efetuar monitoramento de *IP* de origem:



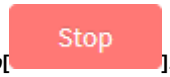
Connections - Web - New - Source IP

- ***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.

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



Connections - Web - New - Source IP - Results

Para interromper o monitoramento basta clicar no botão ***Stop***[

].

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

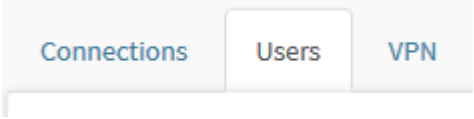
Live Sessions - Users

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 *"Users".*



Aba *Users*

Surgirá a tela “*Users*”, conforme demonstrado pela imagem abaixo:

Live Session - Users

Esta sessão irá abordar:

- Componentes deste painel;
- Como executar o monitoramento;

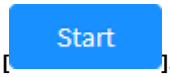
A seguir, analisaremos os componentes deste painel.

Users - Componentes

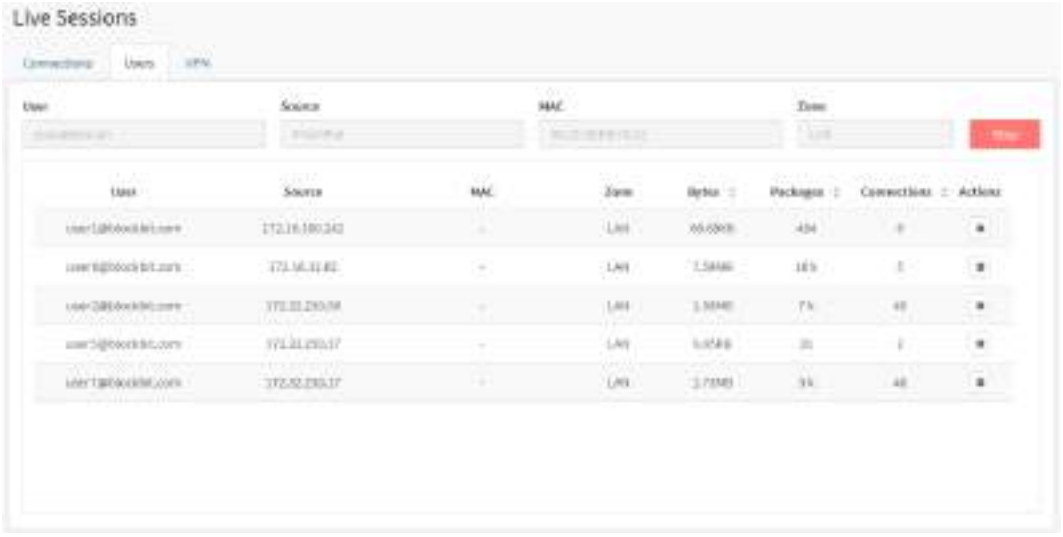
O painel *Live Users* é composto dos seguintes recursos:

Live Users

- ***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 [

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

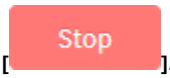


Live Users - Results

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 o 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 **[** 

].

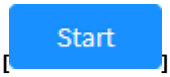
Users - Monitoramento

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

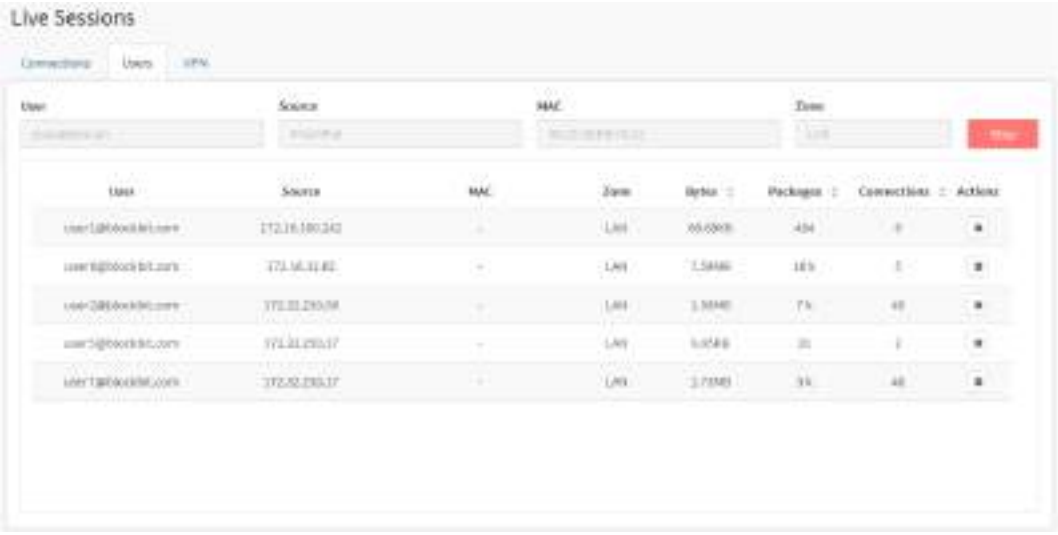
Monitoramento em geral

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

Users - Sem Filtros

Simplesmente, basta clicar em [

] para iniciar o monitoramento.



Users - Sem Filtros - *Results*

É possível interromper o monitoramento clicando em [Stop].

Monitoramento de um usuário específico

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

Users - Filtrado por usuário

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

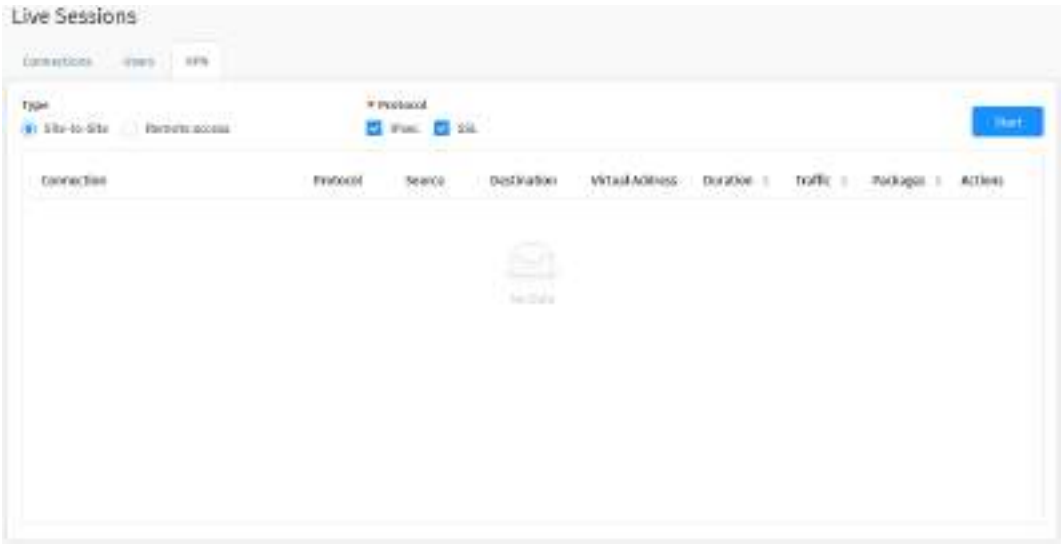
Feito isso, clique no botão [Start], os resultados serão exibidos conforme demonstrado abaixo:

Users - Filtrado por usuário - *Results*

Para interromper o monitoramento basta clicar no botão [Stop].

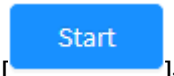
Live Sessions - VPN

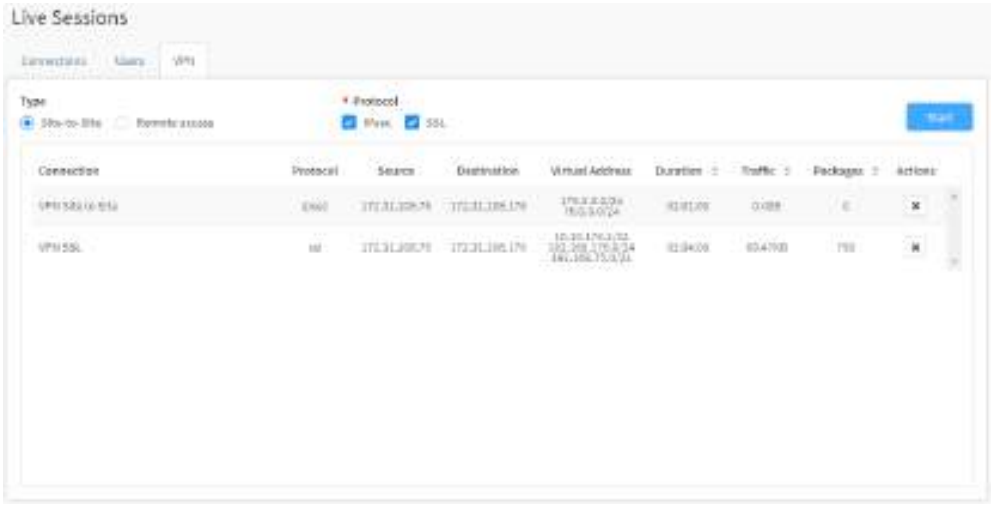
Este recurso permite ao administrador visualizar os status dos túneis de *VPN* estabelecidos, as informações disponíveis são:



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**;**

Ao iniciar o monitor clicando em **[**  **]**, os resultados serão exibidos de acordo com o tipo de conexão e o protocolo selecionado, conforme demonstrado abaixo:



Live Sessions - VPN - Resultados

As colunas exibem as seguintes informações:

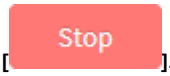
- ***Connection***: Nome do túnel;

- ***Protocol:*** Exibe o protocolo da *VPN (IPsec ou SSL)*.
- ***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.

 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.

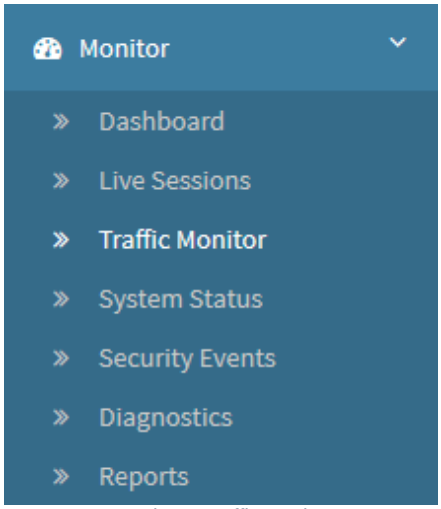
Para interromper um monitoramento que esteja sendo executado, clique em **[** 

].

Monitor - Traffic Monitor

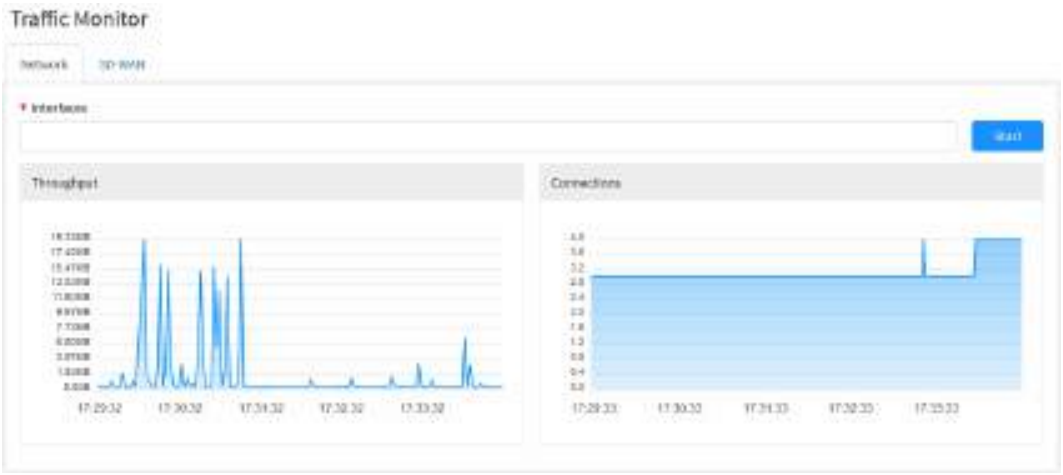
Como o próprio nome indica, o *Traffic Monitor*, permite que o tráfego da rede e do *SD-WAN* seja monitorado, através deste recurso o administrador pode visualizar o tráfego de rede real ou histograma (*Network Throughput*), por interfaces, número de conexões simultâneas e o tráfego de rede por cada *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*".



Monitor – Traffic Monitor

A tela abaixo será exibida:



Monitor - Traffic Monitor - Network

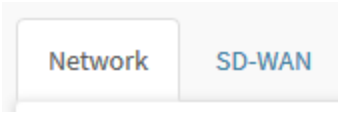
A tela *Traffic Monitor* comporta as seguintes abas:

- *Network*;
- *SD-WAN*.

Traffic Monitor - Network

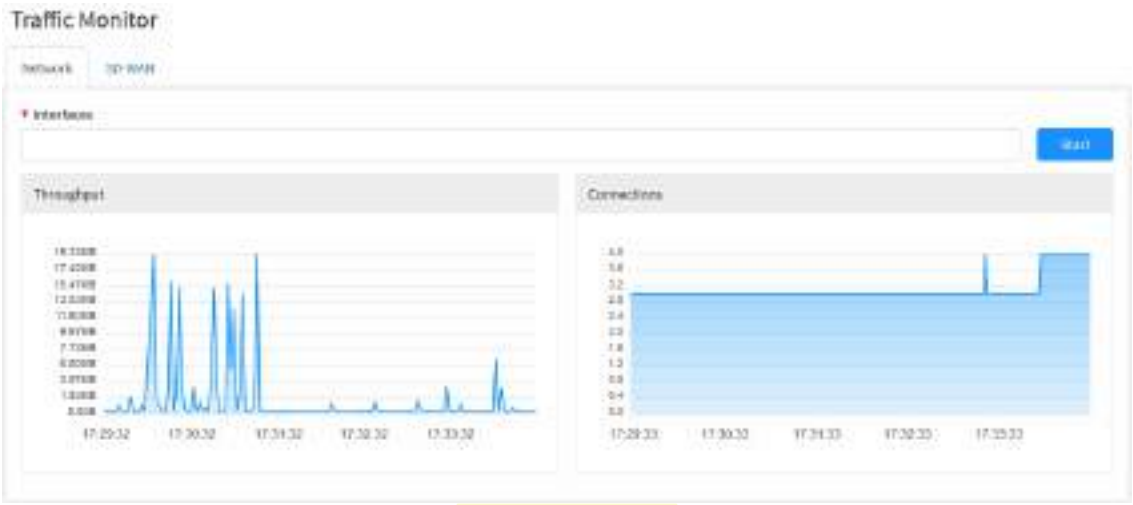
Na aba *Network* do *Traffic Monitor*, é possível acompanhar em tempo real o desempenho e o tráfego efetuado na rede.

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



Aba *Network*

Surgirá a tela demonstrada abaixo:

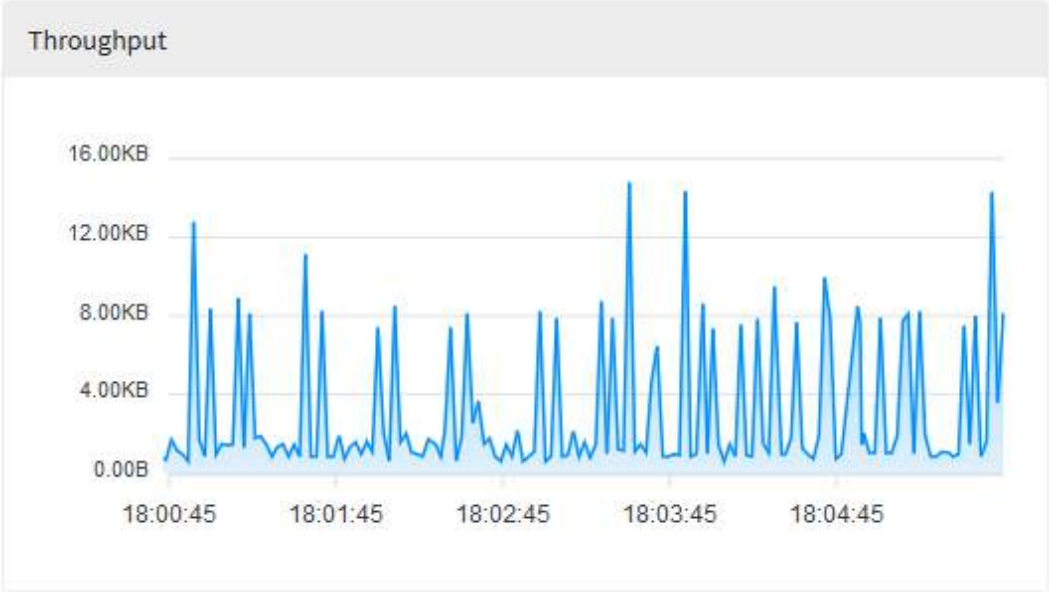


Traffic Monitor - Network

A seguir vamos analisar cada componente desta tela:

Gráfico de *Throughput*

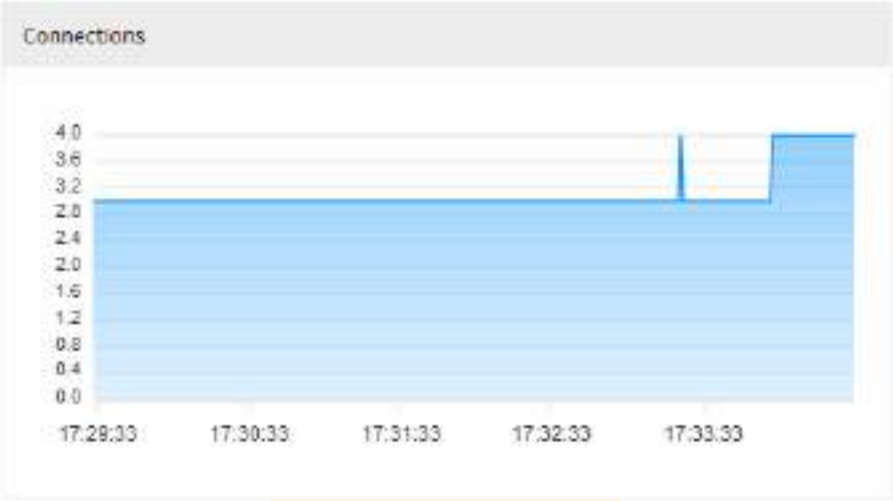
O gráfico de *Throughput* demonstra o histórico do desempenho da rede em tempo real. Ao passar o mouse por cima, é possível de se visualizar um resumo do período selecionado.



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.

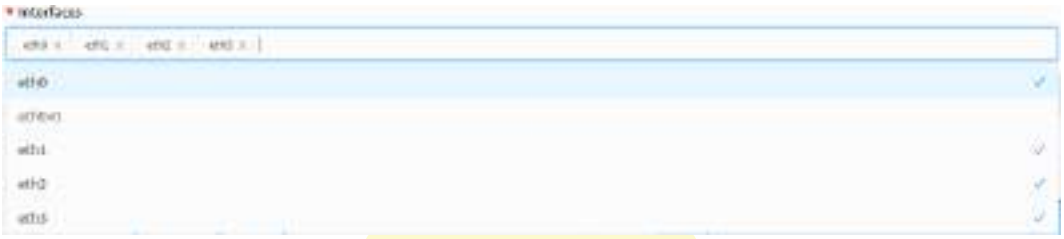


Traffic Monitor - Network - Connections

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:

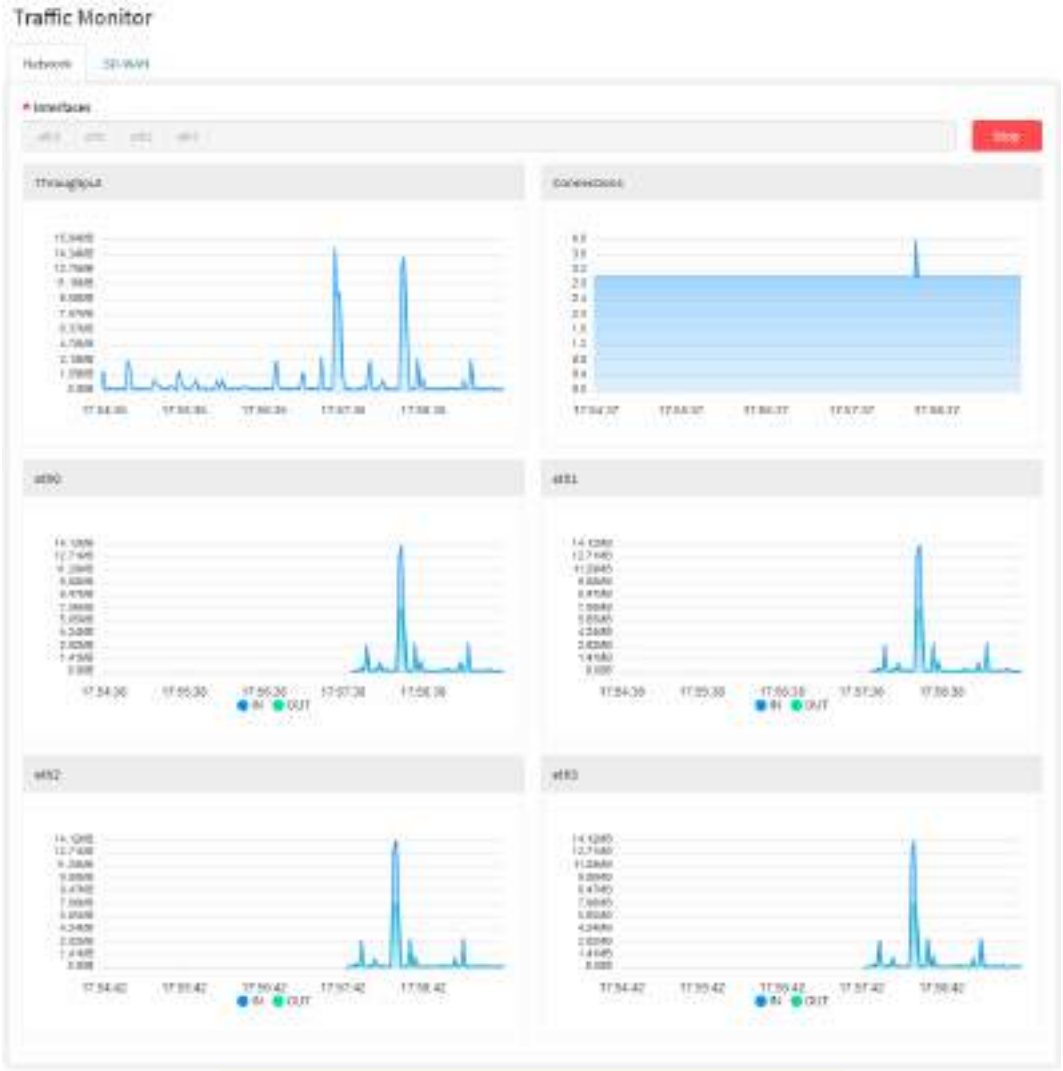


Traffic Monitor - Network - Interfaces

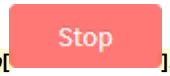
O máximo de interfaces que se pode adicionar para monitoramento em tempo real é 4.

Clique no botão ***Start*** [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 - Network - Monitoramento de *interfaces* em tempo real

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

].

Traffic Monitor - SD-WAN

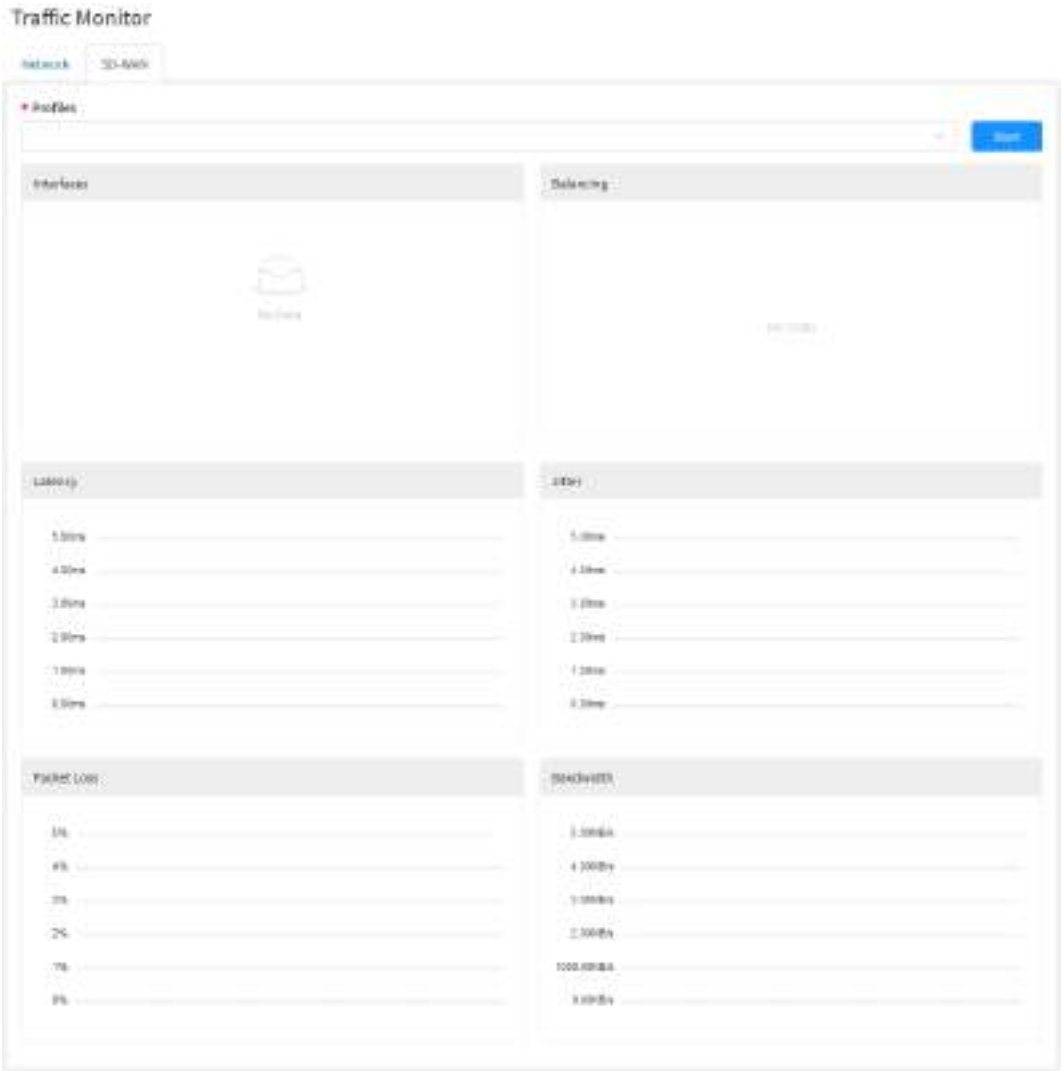
Na aba *SD-WAN* do *Traffic Monitor*, é possível acompanhar em tempo real o desempenho nas interfaces, índices de performance e perfis do *SD-WAN*.

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"*.

Aba *SD-WAN*

Surgirá a tela demonstrada abaixo:



A seguir vamos analisar cada componente desta tela:

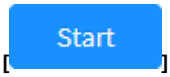
Monitoramento de *SD-WAN* em tempo real

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

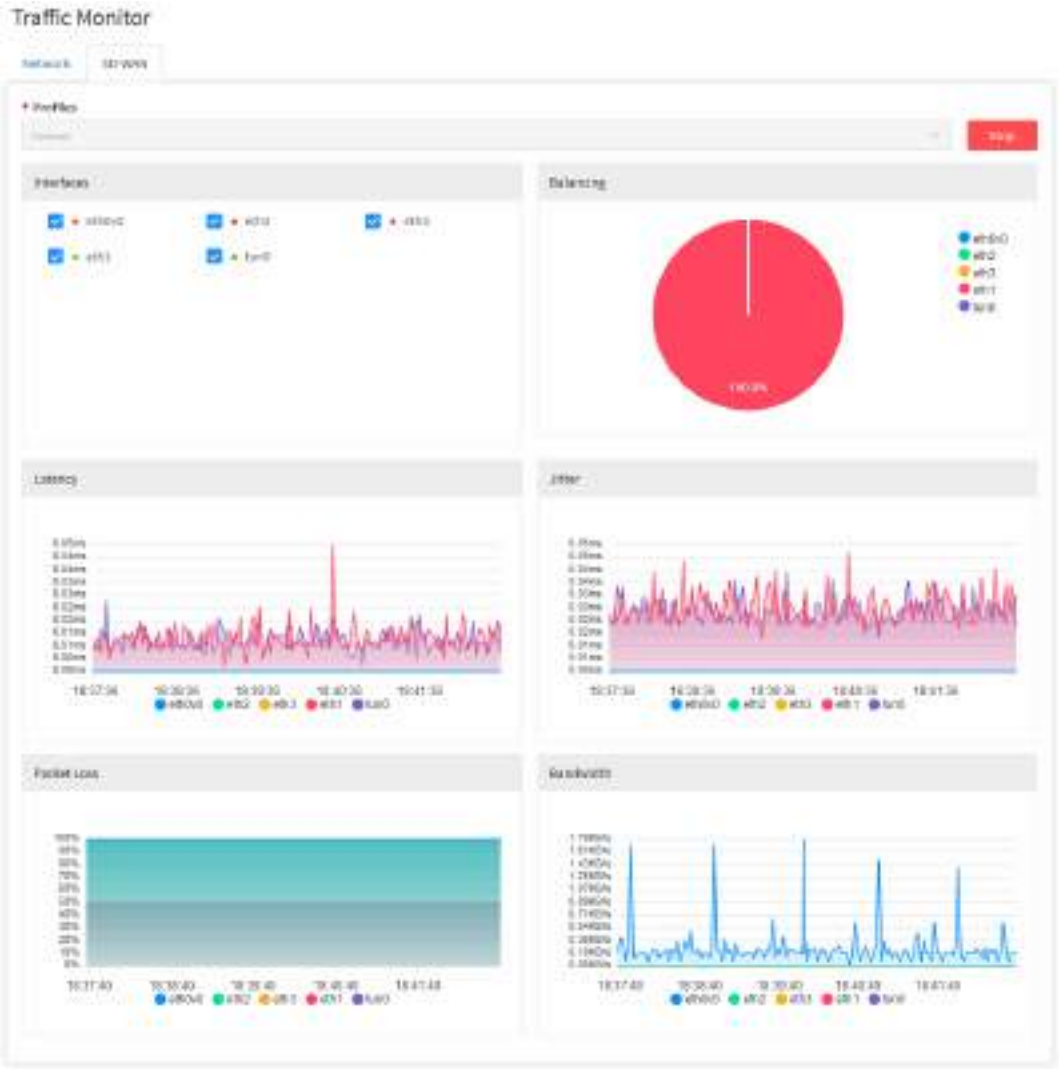
Para tanto, selecione-o à partir da lista, como demonstrado pela imagem:

Traffic Monitor - SD-WAN - Interfaces

Só é possível monitorar um único perfil de SD-WAN por vez.

Clique no botão ***Start*** **[**  **]** para iniciar o monitoramento.

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

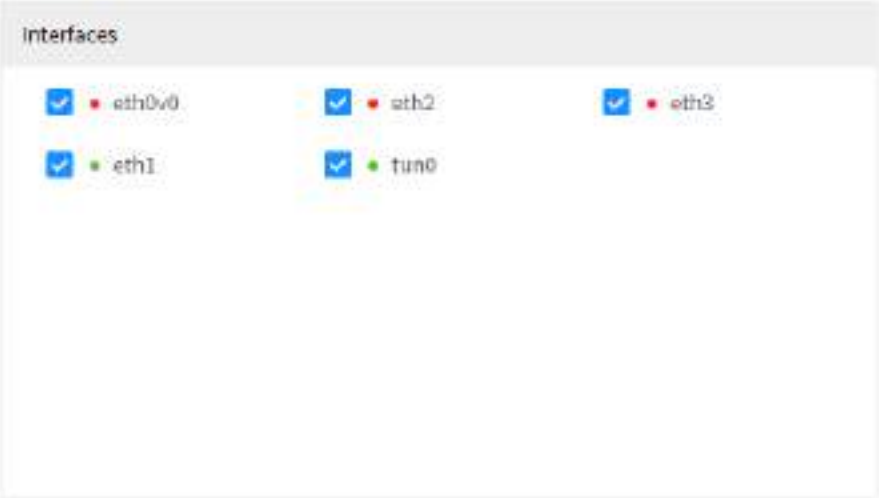


Traffic Monitor - *SD-WAN* - Monitoramento em tempo real

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

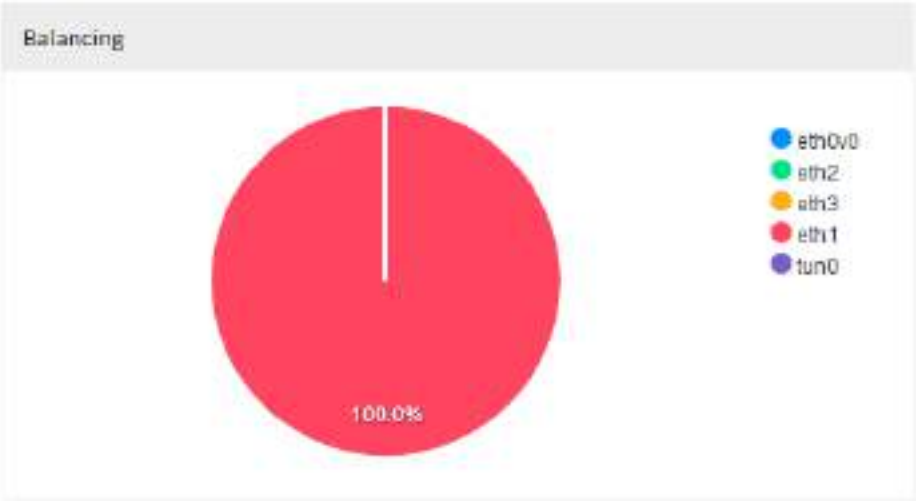


Traffic Monitor - SD-WAN - Painel *Interfaces*

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

Gráfico *Balancing*

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

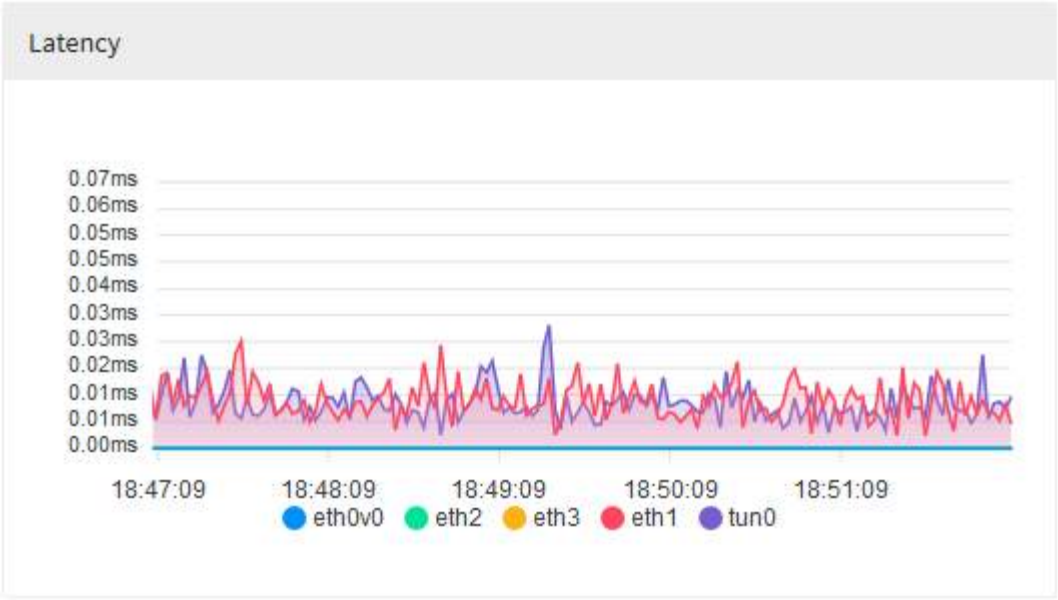


Traffic Monitor - SD-WAN - Painel *Balancing*

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.

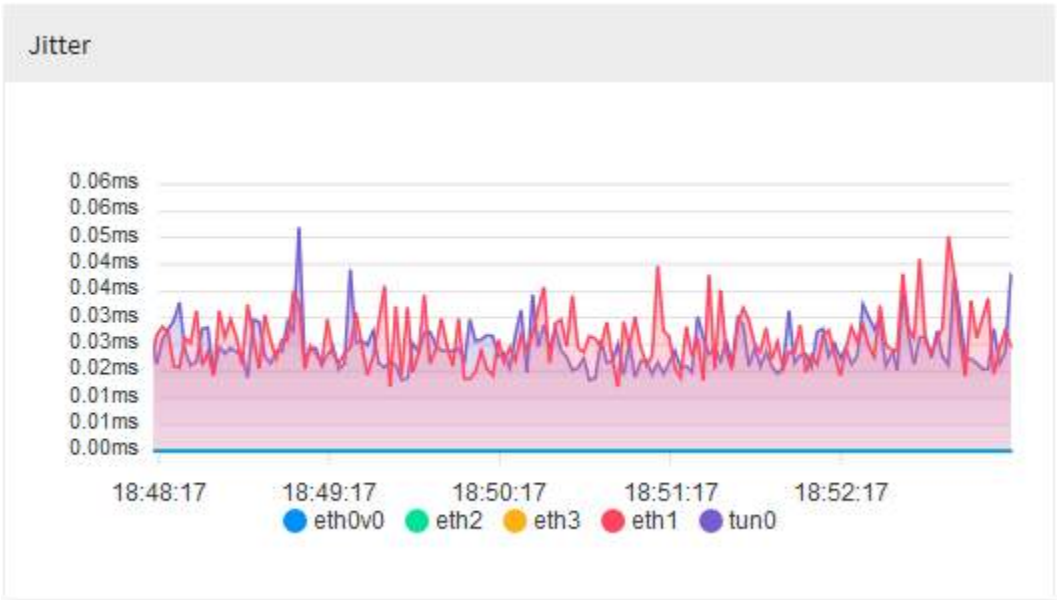


Traffic Monitor - *SD-WAN* - Gráfico Latency

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.

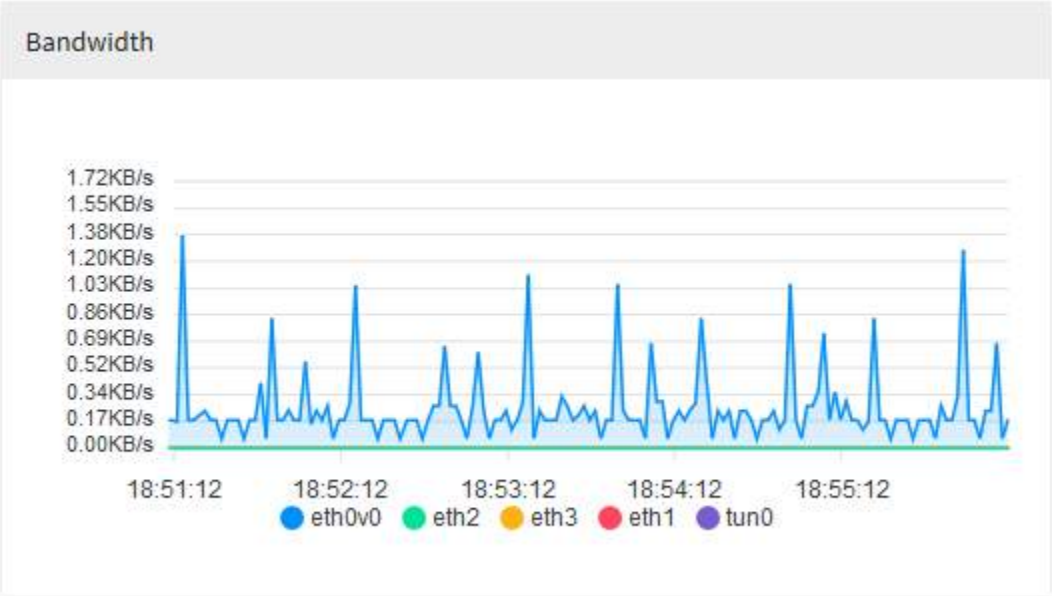


Traffic Monitor - *SD-WAN* - Gráfico *Jitter*

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

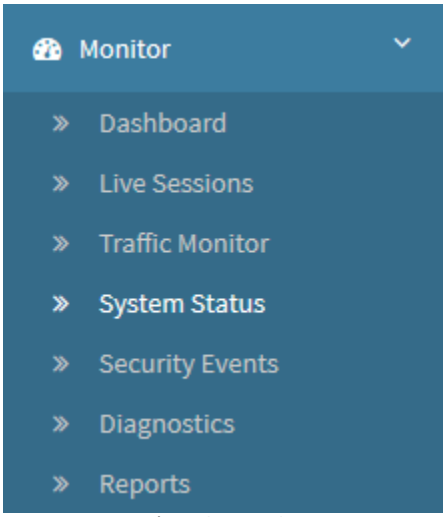
Ao passar o mouse por cima do gráfico ou das *interfaces* na legenda inferior, é possível visualizar um resumo referente ao período e a *interface* selecionada.

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

Monitor - System Status

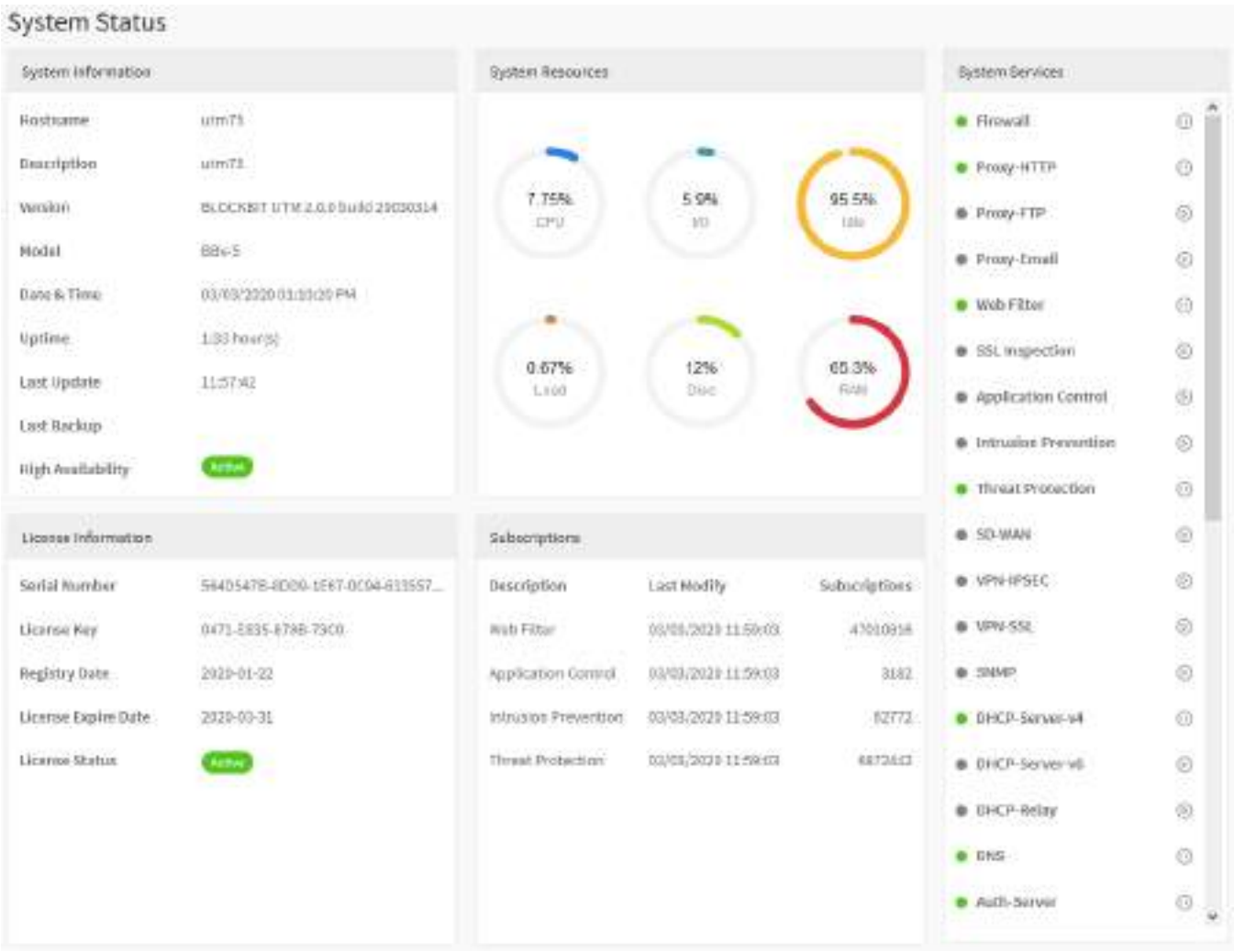
Este recurso permite ao administrador a visualização na interface *WEB* de dados e informações de “Sistema”, “Licença” e das bases de dados “*Subscriptions*”, permitindo também visualizar e alterar o “*Status* dos módulos e serviços”.

Para acessar esta tela, basta selecionar a opção “*System Status*”.

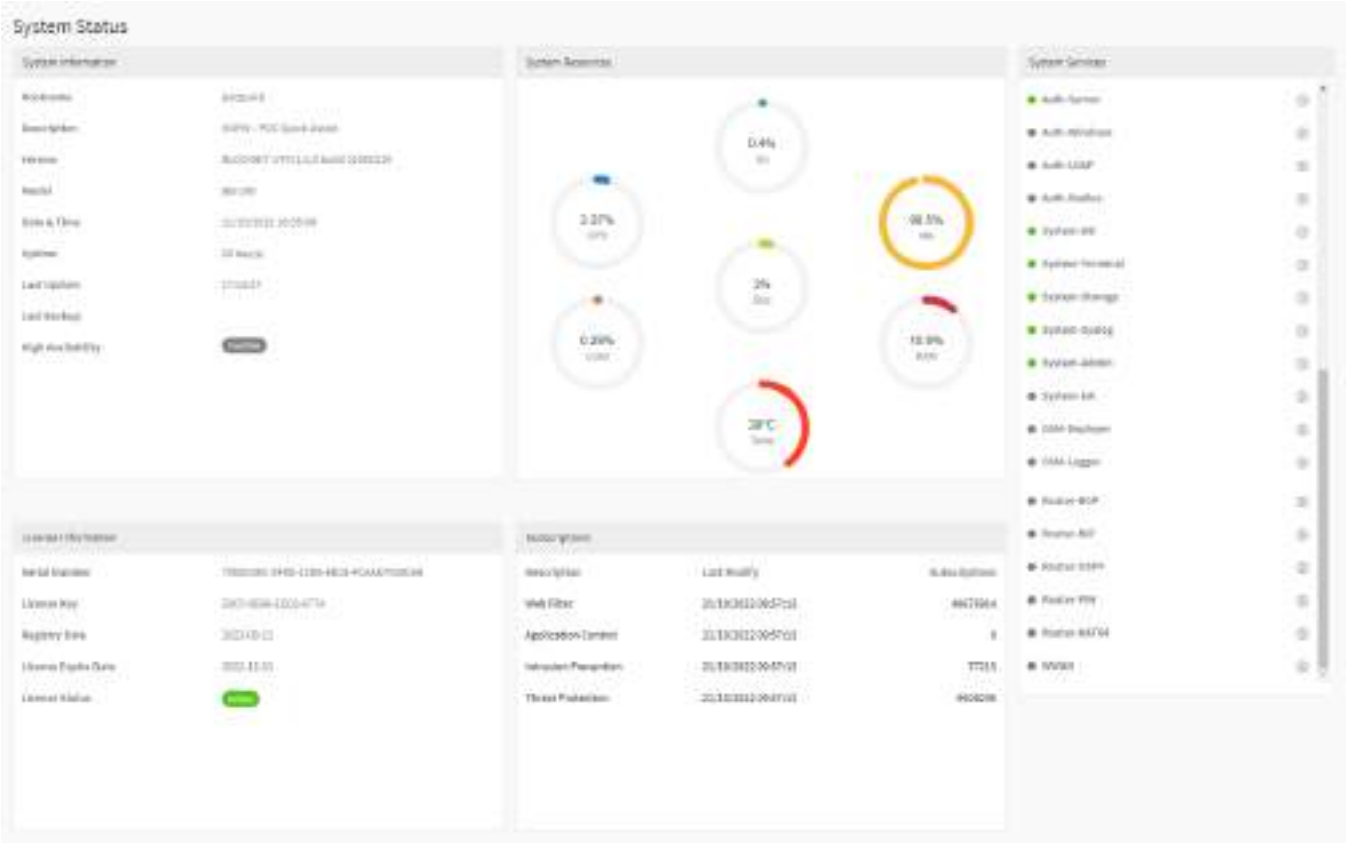


Monitor - System Status

A tela abaixo será exibida:



System status - Visualização de um appliance virtual



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.

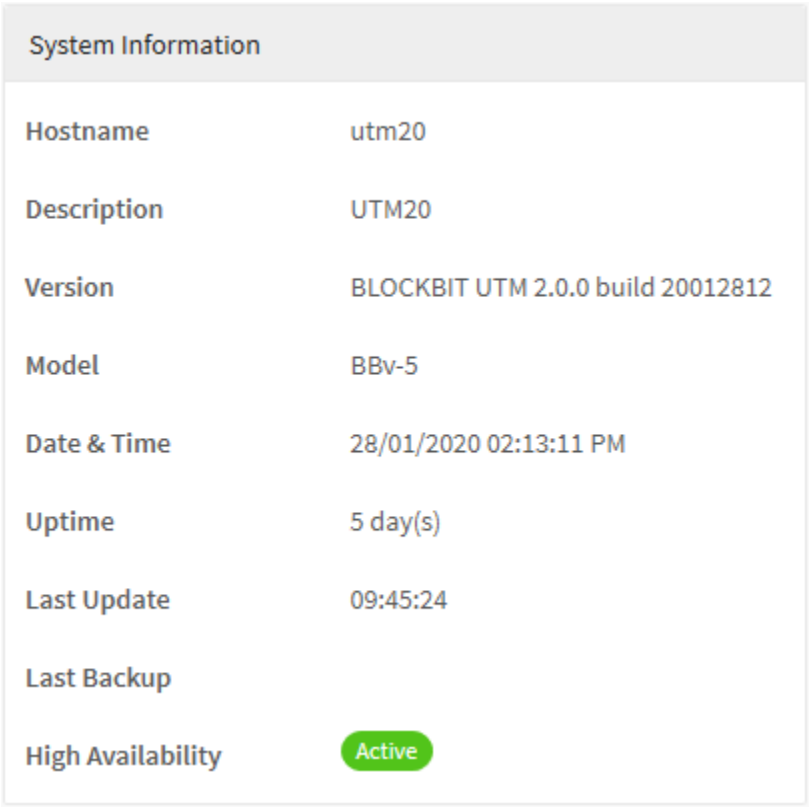
System Status - Widgets

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.



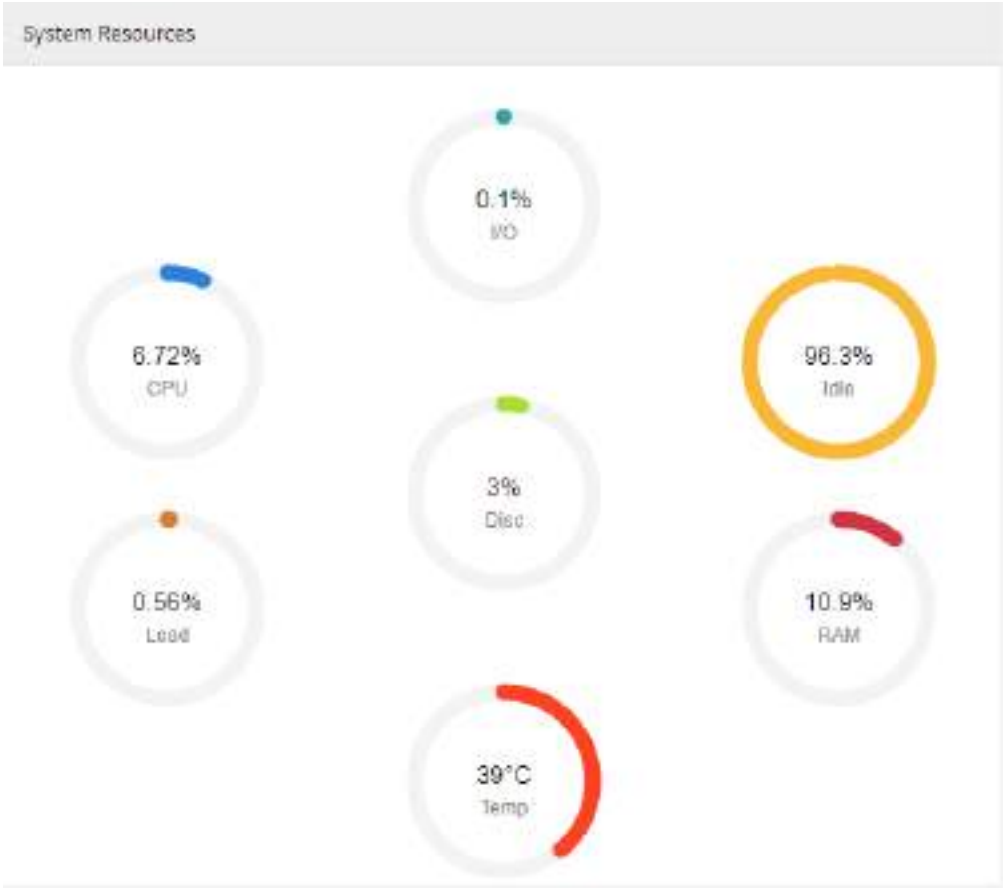
Dashboard - System Information

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%;
- ***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.



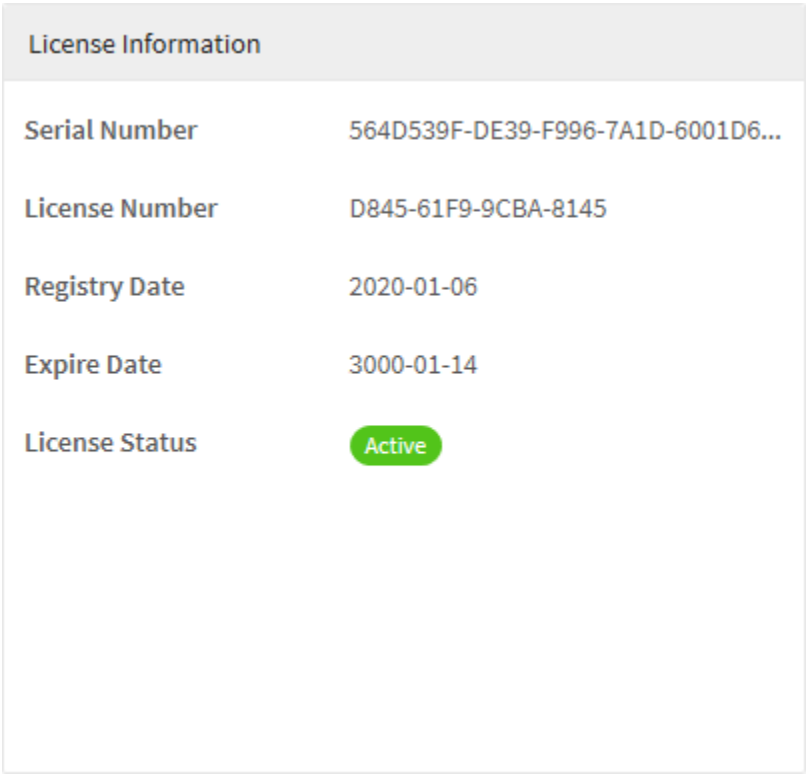
Dashboard – System Resources

Note que a widget Temp [] não será exibida em appliances virtuais. Esta funcionalidade somente estará disponível caso um appliance físico esteja sendo utilizado.

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 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.



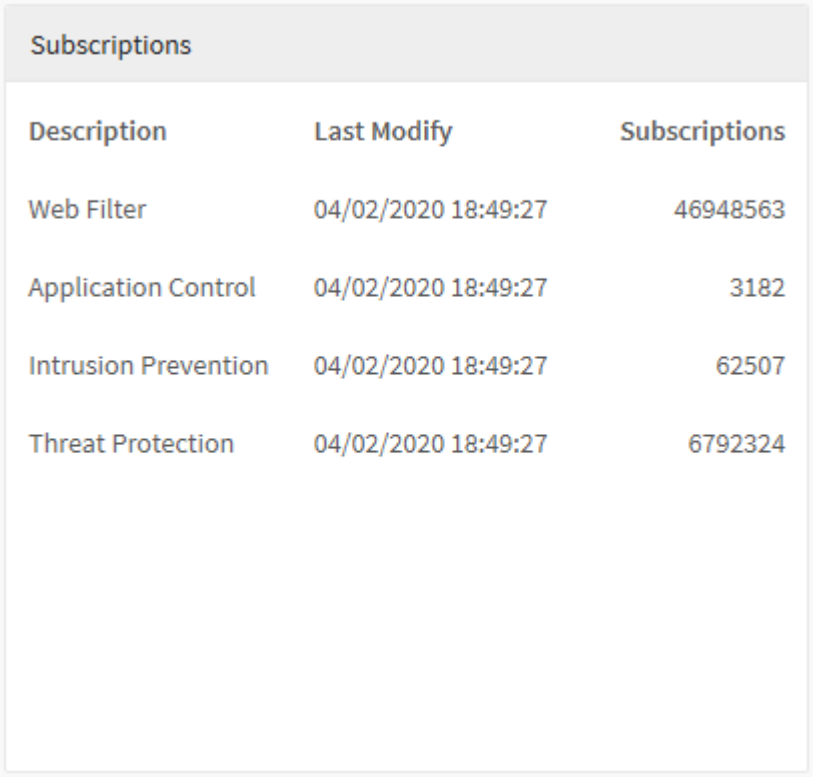
Dashboard – License Information

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***.

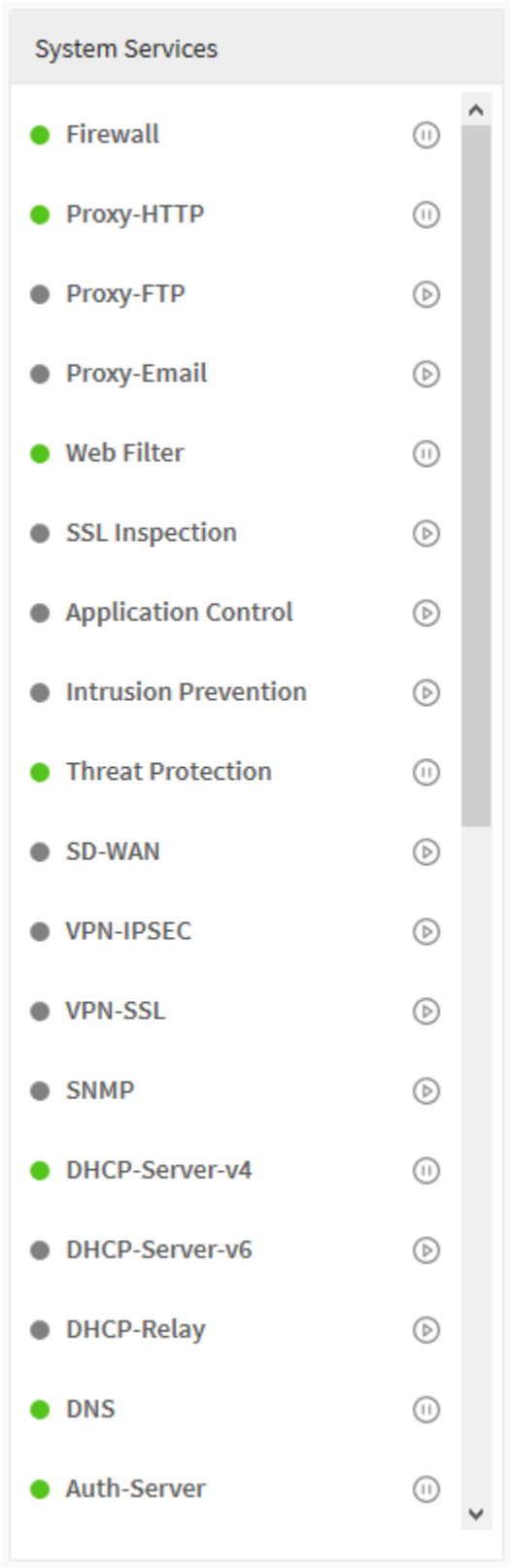
Todas as bases são atualizadas constantemente pela Blockbit, garantindo a efetividade e segurança do ambiente.



Dashboard – Subscriptions

Services

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



Dashboard – Services

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

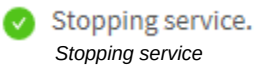
- **Ativo[ ];**
- **Inativo[ ].**

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

- **Iniciar [ ]**;
- **Parar [ ]**.

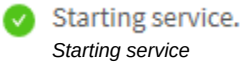
> Não é possível interromper alguns serviços específicos.

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



Stopping service

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



Starting service

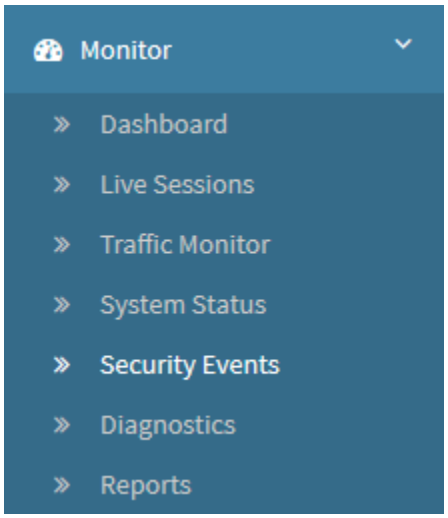
Monitor - Security Events

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.

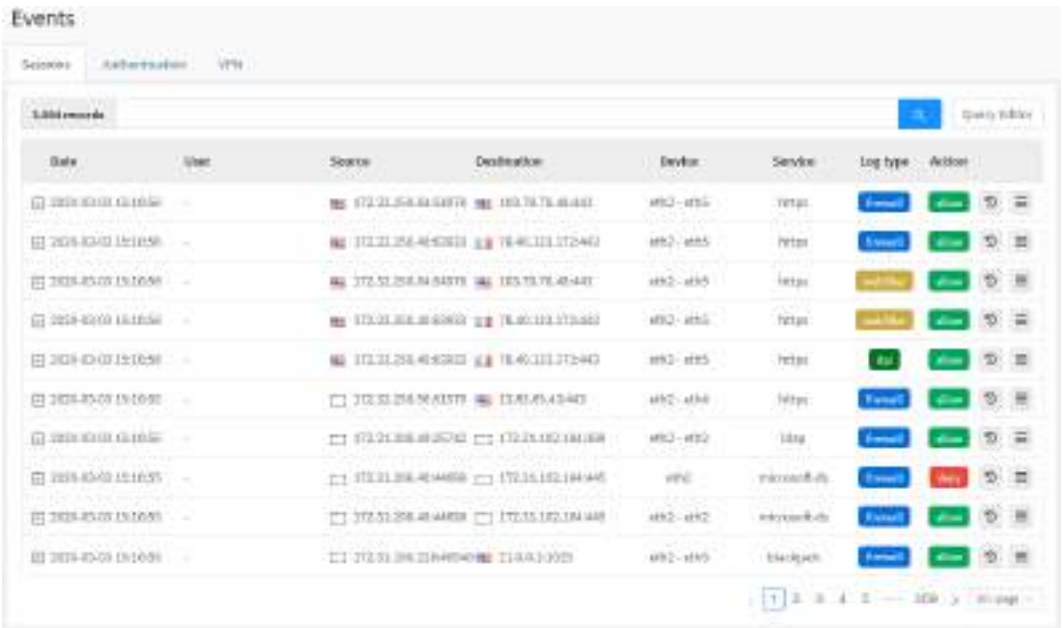
A principal diferença entre os relatórios exibidos em *Events* e os em *Analyzer* é que:
Em *Events*, é gerado um registro da conexão com os atributos todos zerados (*bytes* e pacotes), após a desconexão outro evento é gerado registrando esses atributos, o tráfego e o tempo conectado.
Já os relatórios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

A tela abaixo será exibida:



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:

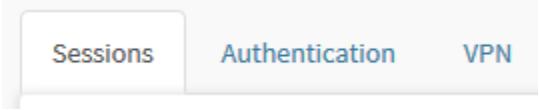
- *Sessions*;
- *Authentication*;
- *VPN*.

A seguir, os componentes do painel *events serão analisados.*

Security Events - Sessions

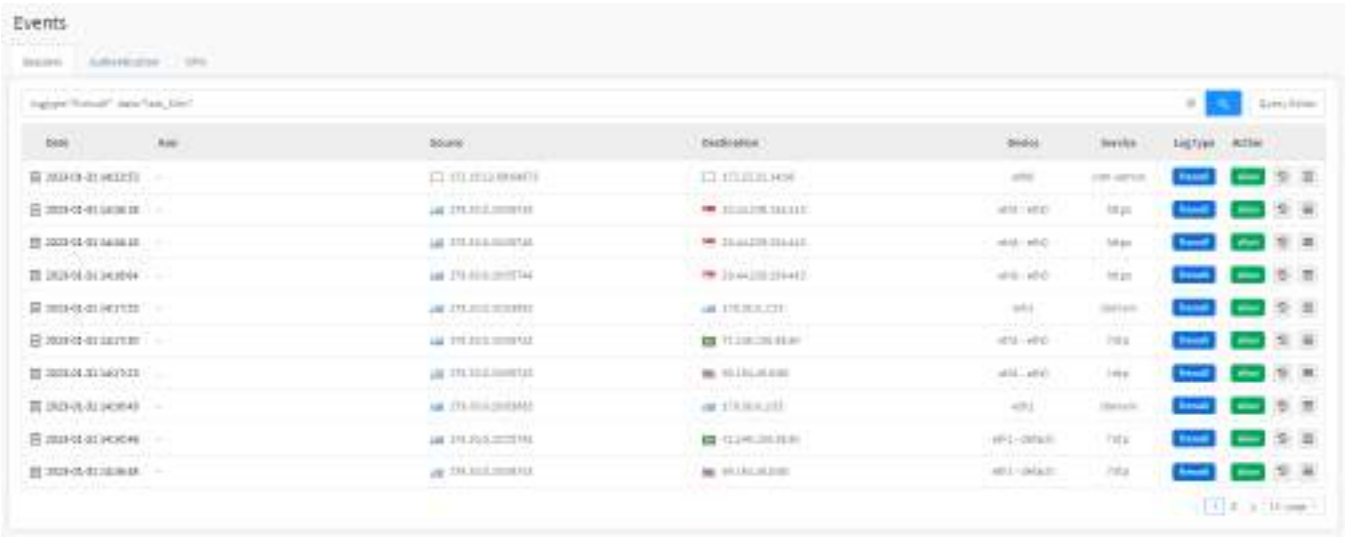
Em *Sessions* temos um registro de todos os eventos detectados nas sessões *deste device*.

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



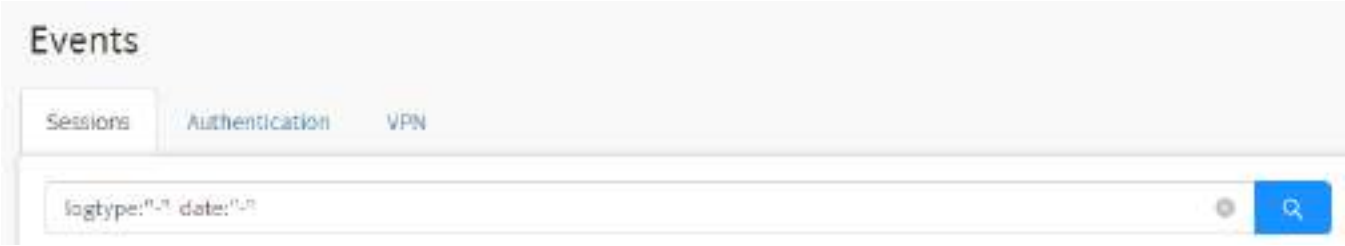
Aba *Sessions*

Surgirá a tela demonstrada abaixo:



Security Events – Sessions

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.



Events - Sessions - Barra de pesquisa

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

- ***Expandir[ ]:*** 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

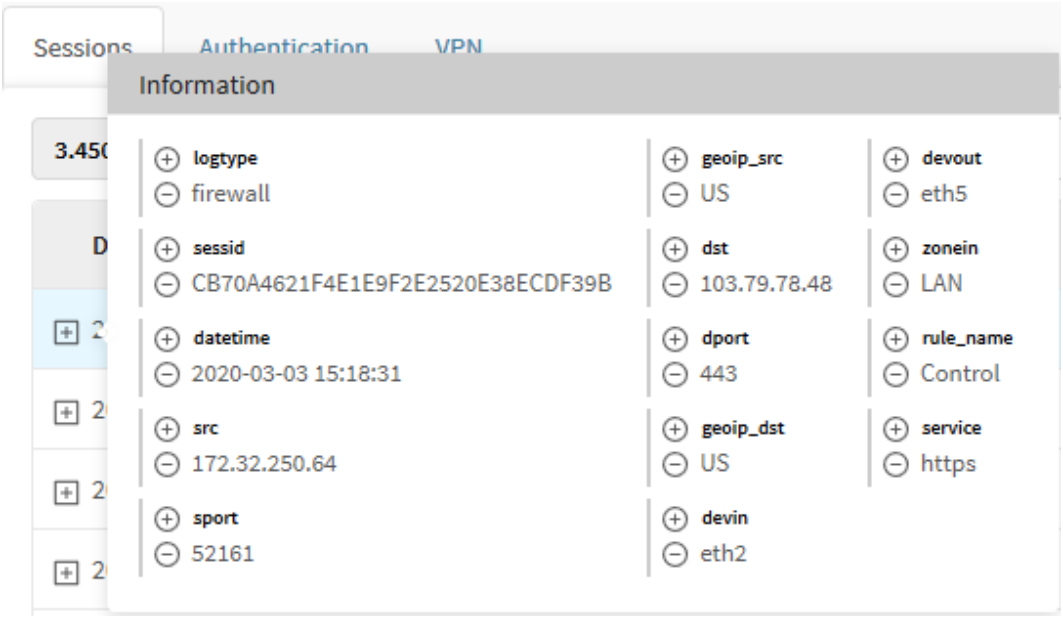
O botão ***Event View***[ ] exibe detalhes mais aprofundados do evento em questão, conforme exibido na imagem abaixo:

Sessions - Event View

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

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.



Events – Log Events – Expandido

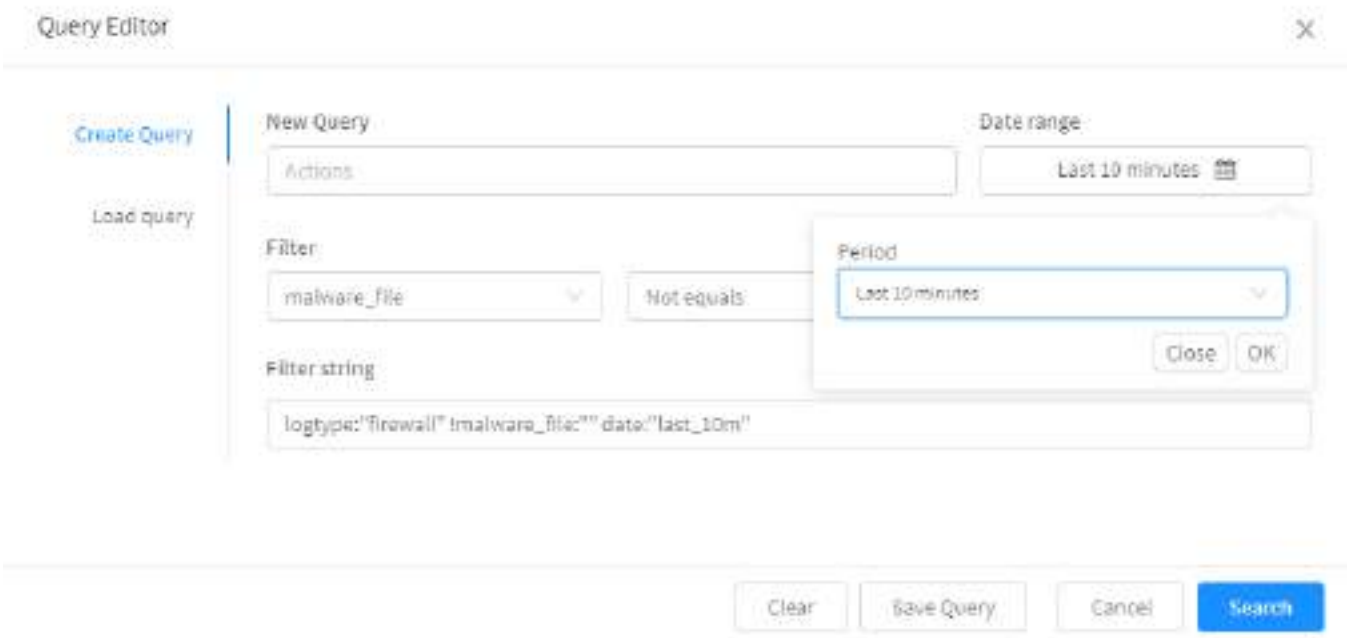
Ao clicar no ícone [⊕] as informações a frente são utilizadas como filtro e uma pesquisa é efetuada.

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 seguinte janela será exibida:

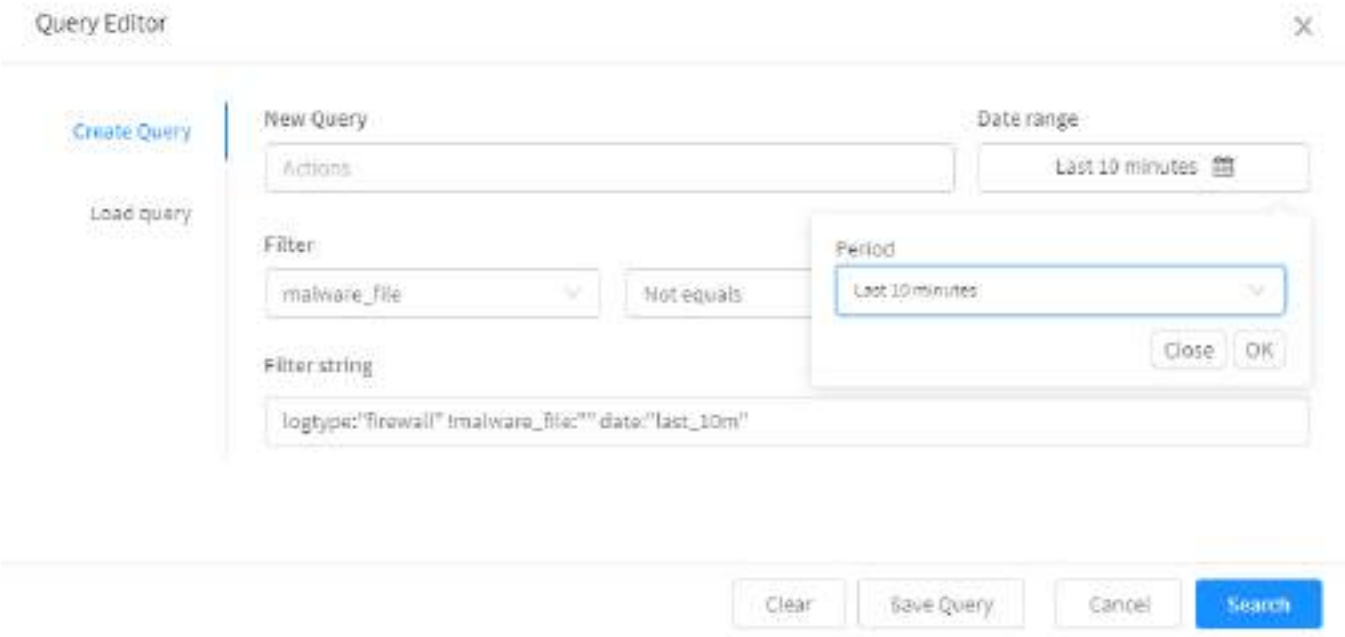


Events - Query Editor

A seguir analisaremos cada campo desta janela:

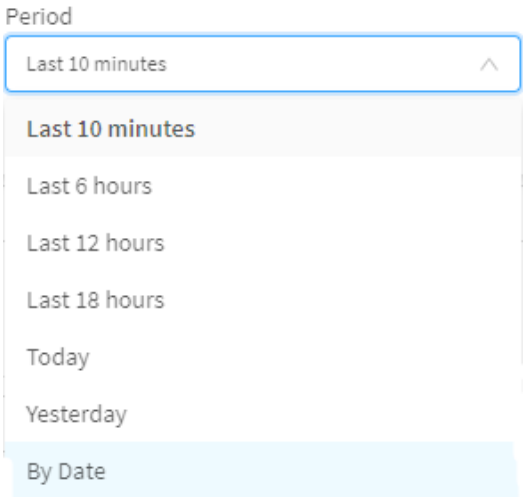
Events - Query Editor - Create query

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



Events - Query Editor - Create query

- ***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:



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;

- **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 página;
- **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 *query* configurada, clique no botão ***Clear***[Clear]. Caso deseje cancelar clique no botão ***Cancel***[Cancel]. Para efetuar uma busca utilizando a *query* clique no botão ***Search***[Search].

Para salvar a *query*, 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:

Events - Query Editor - Load Query

- ***Select[ ]:*** 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[ ]*:** Edita as configurações da *query*;
  - ***Search[ ]*:** Efetua uma busca utilizando a *query*;
  - ***Delete[ ]*:** Remove a query.

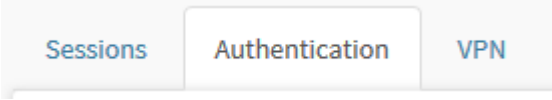
Caso deseje cancelar clique no botão ***Cancel*[** Cancel **]**. Para efetuar uma busca utilizando a *query* selecionada clique no botão ***Search*[** Search **]**.

À seguir vamos analisar o *Event View*.

Security Events - Authentication

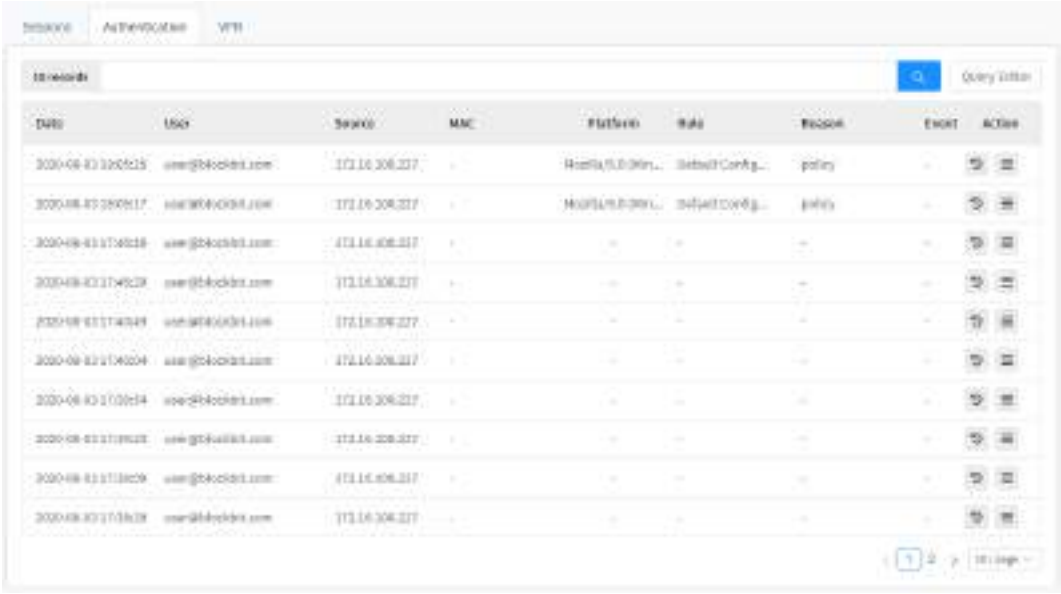
Em *Authentication* temos um registro de todos os eventos de autenticação detectados *neste device*.

Para acessar, clique em *"Authentication".*



Aba *Authentication*

Surgirá a tela demonstrada abaixo:



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 **]** a seguinte janela será exibida:

Authentication - Query Editor

- ***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.

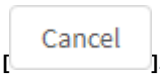
Para mais informações a respeito de quais informações devem ser exibidas por cada filtro, consulte esta página.

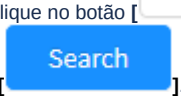
As informações exibidas em *Description* equivalem às que o filtro irá retornar, porém, com maior detalhamento e especificidade.

- ***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.*

Após editar os campos anteriores, clique em **[** + **]** para exibir a *string* utilizada pela busca na caixa de texto *Filter String*.

Para limpar a *query* configurada, clique no botão **[** 

]. Caso deseje cancelar clique no botão **[** 

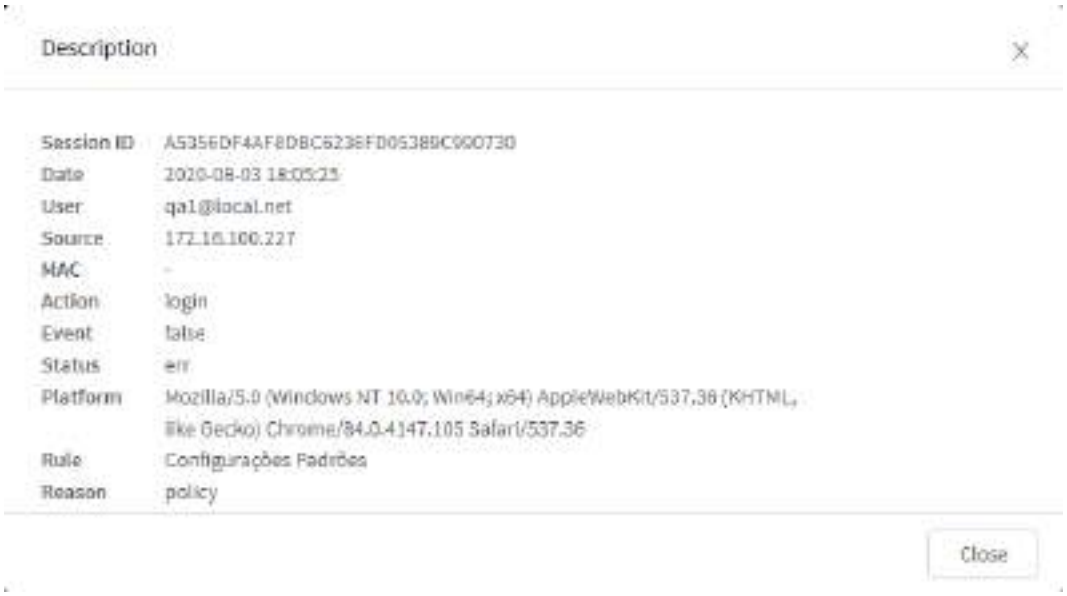
]. Para efetuar uma busca utilizando a *query* clique no botão **[** 

].

À seguir vamos exibir o funcionamento do botão *Description*.

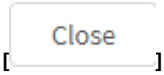
Authentication - Description

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



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.

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

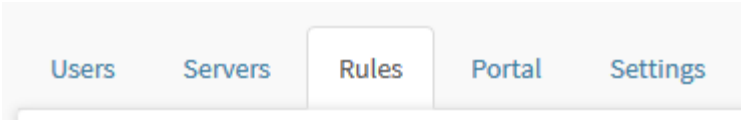
Authentication - Rules

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:



Aba Regras

A seguinte tela será exibida, conforme mostrado abaixo:

Authentication - Servers

Nesta seção analisaremos:

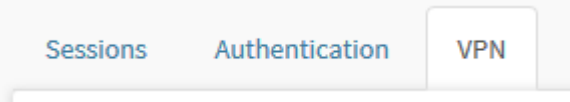
- Como criar, editar e apagar estas Políticas;
- Os componentes da coluna desta aba.

A seguir, cada componente desta tela será analisado.

Security Events - VPN

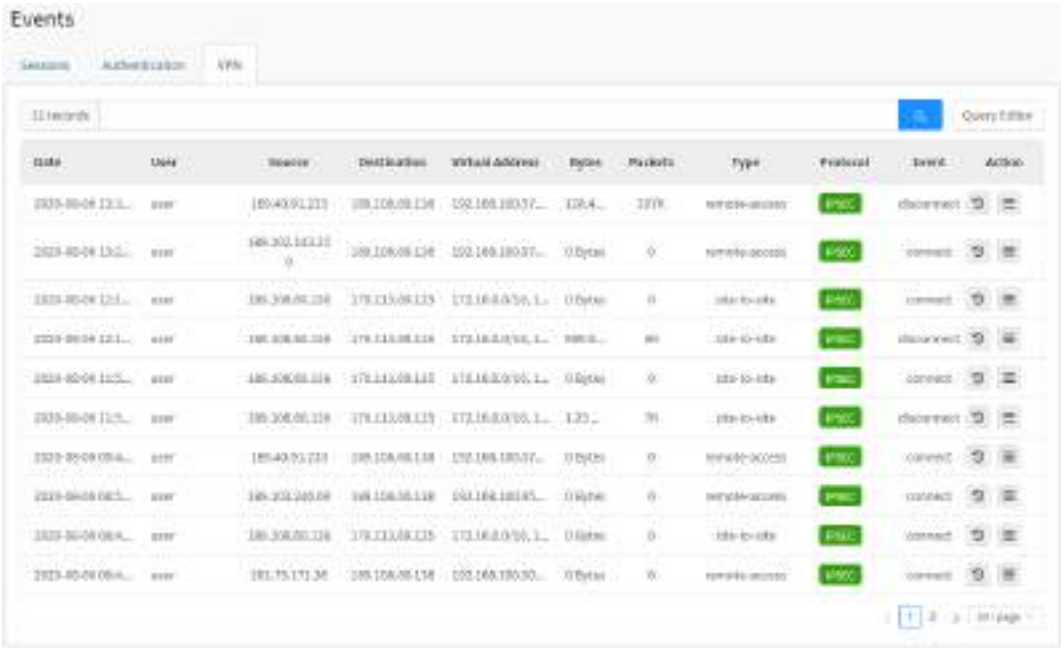
Em *VPN* temos um registro de todos os eventos de gerados pelos perfis de *VPN* deste *device*.

Para acessar, clique em *"VPN"*.



Aba *VPN*

Surgirá a tela demonstrada abaixo:



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:

VPN - Query Editor

- ***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;*
  - **user:** Este filtro efetua a seleção por usuário, ele aceita e-mails como valores. Ex.: user@blockbit.com;
  - **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;
  - **virtual_address:** Faz a seleção pelo IP virtual da VPN, este filtro aceita endereços IPv4 ou Ipv6 como *valor*. Ex.: 192.168.200.4/32;
  - **type:** Efetua a seleção baseada em no tipo de conexão da VPN. Ex.: remote-access, site-to-site, etc;
  - **protocolo:** Este filtro permite a seleção pelo protocolo de criptografia da VPN, as opções disponíveis são: SSL ou IPSEC;
  - **event:** Faz a seleção por um evento específico. Ex.: connect, disconnect, etc.
- ***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.*

Após editar os campos anteriores, clique em **[** + **]** para exibir a *string* utilizada pela busca na caixa de texto *Filter String*.

Para limpar a *query* configurada, clique no botão **[** Clear **]**. Caso deseje cancelar clique no botão **[** Cancel **]**. Para efetuar uma busca utilizando a *query* clique no botão **[** Search **]**.

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:

Sessions - Event View

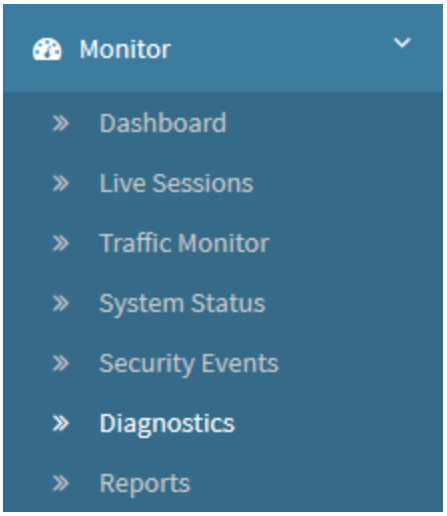
- ***ID*:** Exibe o *ID* da sessão do usuário que causou o evento;
- ***Connection ID*:** Exibe o *ID* da conexão do usuário que causou o evento;
- ***Date*:** Exibe a data do evento;
- ***User*:** Identifica o usuário que gerou este evento;
- ***Source*:** Exibe o endereço *IP* de origem do evento;
- ***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;*
- ***Event*:** Exibe especificamente qual foi o evento que gerou o *log*;
- ***Time Connection*:** Exibe por quanto tempo o usuário ficou conectado.

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

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 - Packet Capture

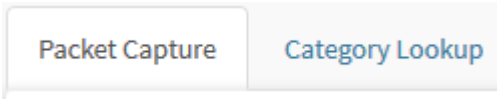
O painel *Diagnostics* é composto de duas abas:

- *Packet Capture*;
- *Category Lookup*.

Diagnostics - Packet Capture

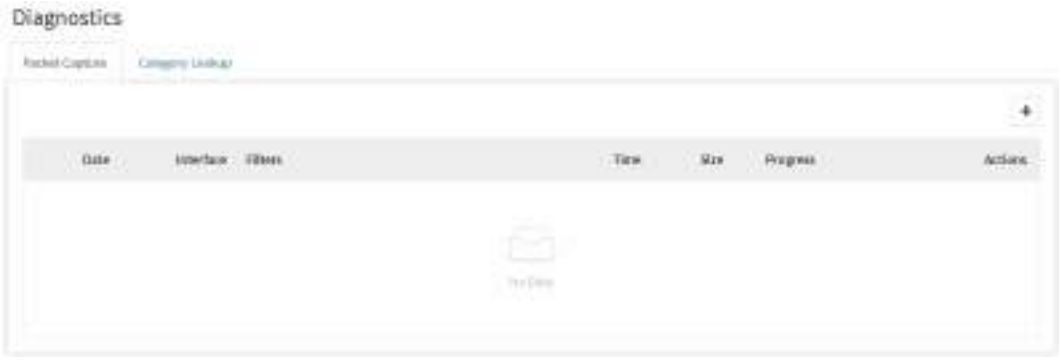
Este recurso permite ao administrador coletar *dump* em formato *PCAP*, com filtros, de qualquer tráfego filtrado pelo Blockbit UTM.

Para acessar clique na aba "*Packet Capture*".



Aba "*Packet Capture*"

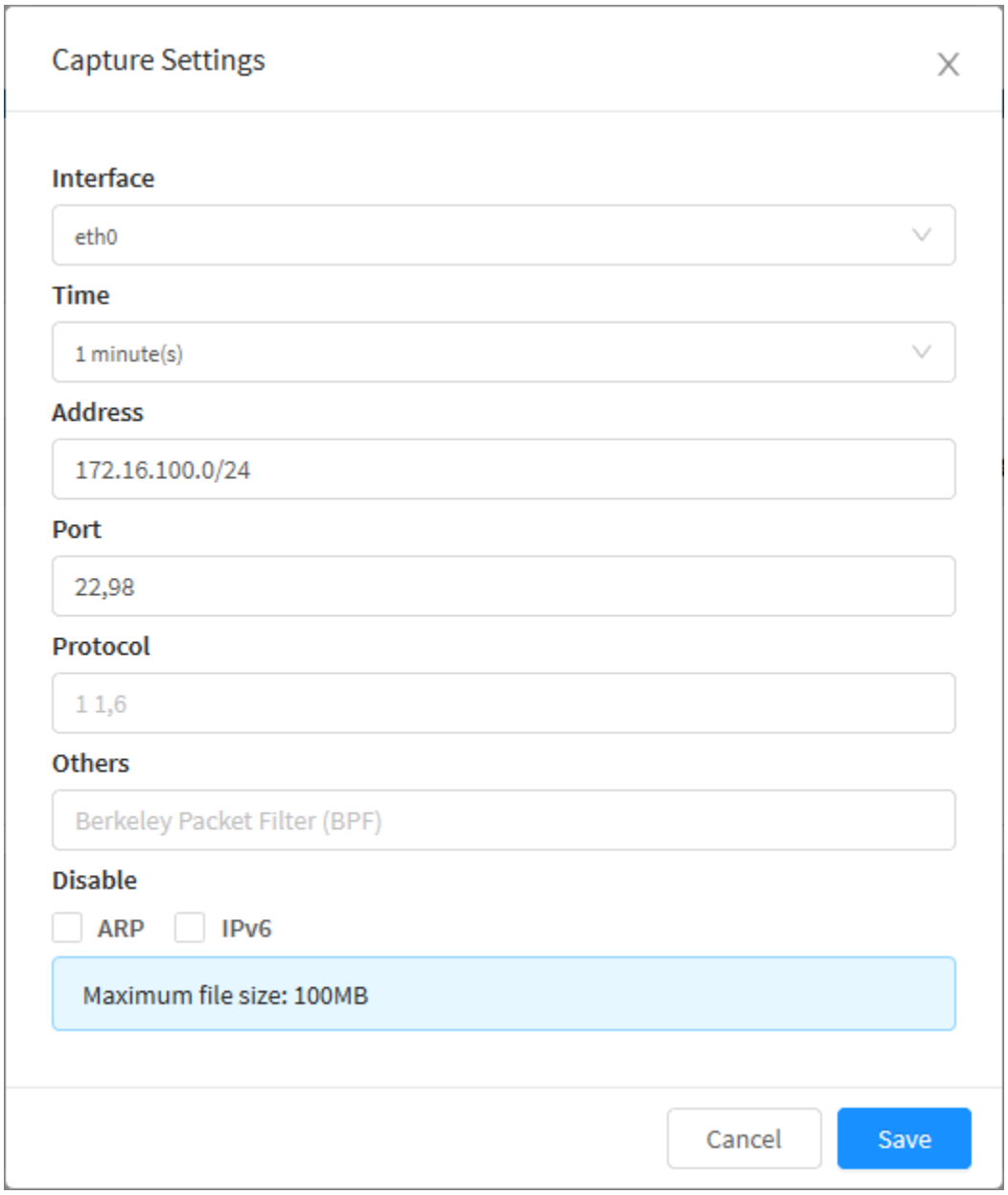
A tela abaixo será exibida.



Packet Capture

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

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



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*)**;
- [☑] ***Disable ARP*:** Essa opção desabilita o monitoramento de *ARP* na interface;
- [☑] ***Disable IPv6*:** Essa opção desabilita o monitoramento do protocolo *IPv6*.

Caso deseja cancelar, clique em [Cancel]. Após preencher os campos clique no botão [Save] e o sistema irá iniciar o monitoramento conforme tela abaixo.

Packet Capture – Progress

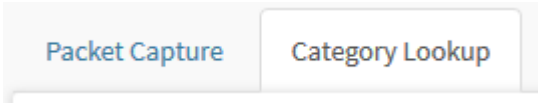
Aguarde a barra de progresso finalizar, os dados capturados ficam disponível para *download* ao clicar sobre o botão **[ ]** para ser analisado posteriormente.

Packet Capture – Download

Diagnostics - Category Lookup

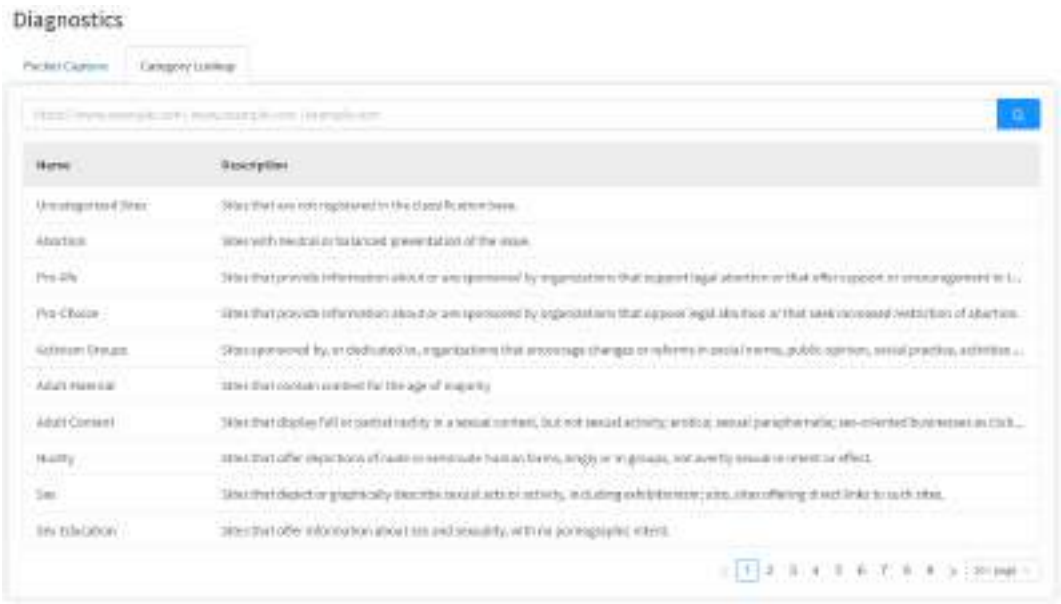
Esta tela tem como função consultar a categorização de sites. Trata-se de uma base de dados *SWG* (*Secure Web Gateway*), uma base de reputação de Urls, navegadores, arquivos e aplicações *web*, que contempla cerca de 88 categorias e subcategorias.

Para acessar clique na aba "*Category Lookup*".



Aba "Category Lookup"

A tela abaixo será exibida:



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

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.
Armazenamento/*Backup* 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.
Compartilhamento de arquivos *peer-to-peer*	*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 *Internet*	*Sites* que permitem a troca instantâneas de mensagens ou *e-mails*.
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, *sites* com senha/verificação. Inclui *sites* nos quais se pode adquirir tais produtos e serviços *on-line*.
Corretagem e negociações *on-line*	*Sites* que possibilitam a negociação ativa no mercado de capitais e o gerenciamento de investimentos financeiros.
***Download* 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 *software*.
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 *on-line*, 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 *on-line*.
Hospedagem de *Web*	*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, *games* ou jogos eletrônicos, de vídeo, computador, dramatização (*role-play on-line*, mas não os que contêm jogos de cartas ou de tabuleiro; também os sites que permitem jogar ou oferecer jogos *on-line*. Inclui *sites* com sorteios e concursos).
Leilões na *Inter net*	*Sites* nos quais se pode participar de leilão *on-line*, de artigos comprados e vendidos por indivíduos.
***Lingerie* 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 *Internet* 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 *Internet*	*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 *on-line*. 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.

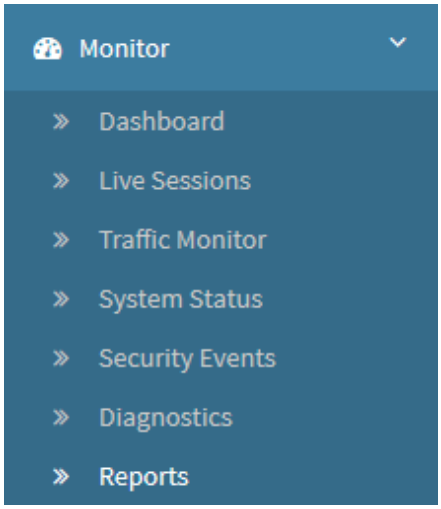
Sistemas de evitação de *proxy*	*Sites* que contêm informações sobre como evitar as funções de servidores *proxy* ou como obter acesso a *URLs* de forma a evitar o servidor *proxy*.
Sistemas de troca instantânea de mensagens	*Sites* que permitem a troca instantâneas de mensagens.
***Sites* a favor da 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.
Sites* de tradução de *URL	*Sites* que oferecem tradução *on-line* de *URLs*.
***Sites* 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.
Sites* pessoais na *Web	*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.
***Sites* que pagam para surfar (*pay-to-surf*)**	*Sites* que pagam o indivíduo para surfar, ou para enviar *e-mail*.
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.
***Streaming* 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 *FDA* (*Food and Drug Administration* - 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 *Internet*	*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 págin
.

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

Nesta sessão iremos analisar:

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

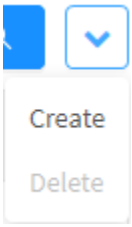
A seguir analisaremos a função de cada componente desta tela.

Monitor - Reports - Menu de Ações

No topo direito da tela temos o menu de ações:

Reports – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Reports – Menu de Ações

O menu é composto das seguintes opções:

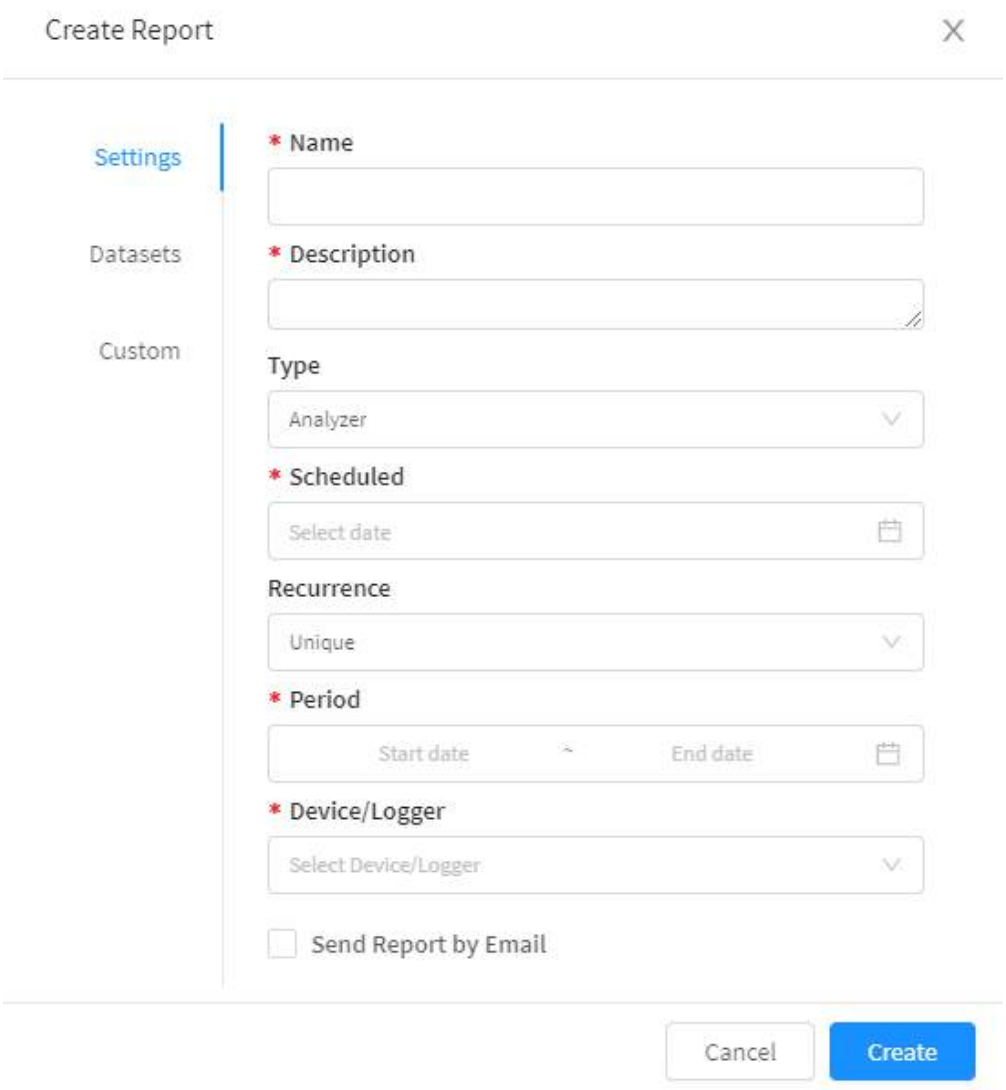
- *Create*;
- *Delete*.

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:



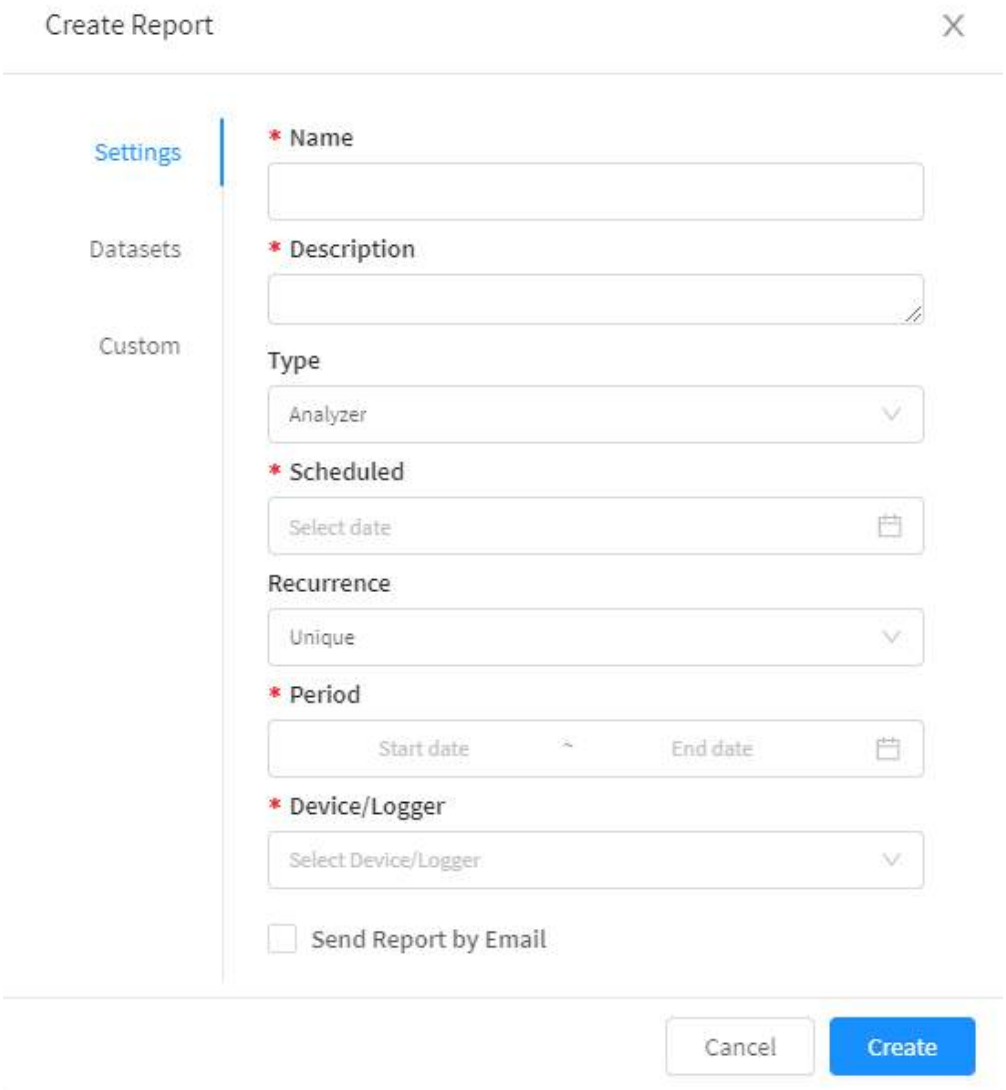
Reports – Create Report

Esta janela é composta pelas seguintes abas laterais:

- *Settings*;
- *Datasets*;
- *Custom*.

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

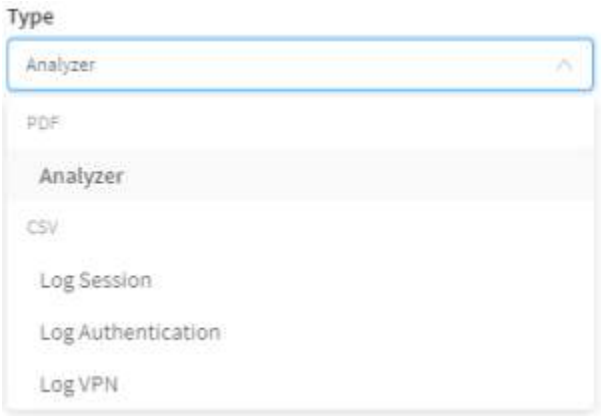
Aba *Settings*



Reports – Create Report - Settings

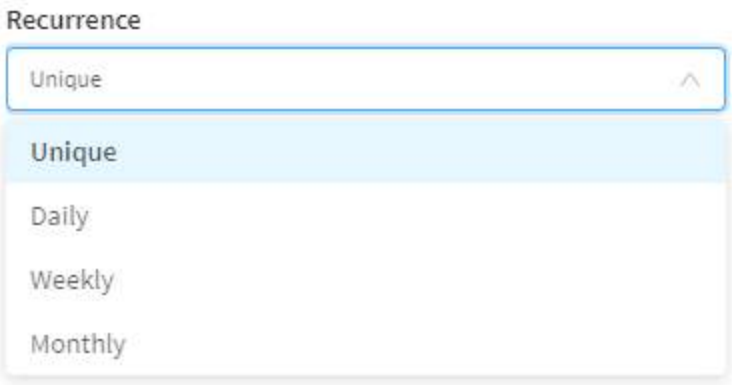
A seguir analisaremos cada campo deste painel:

- ***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.

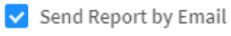


Reports - Create Report - Type window

- ***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 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);



Reports - Create Report - Recurrence window

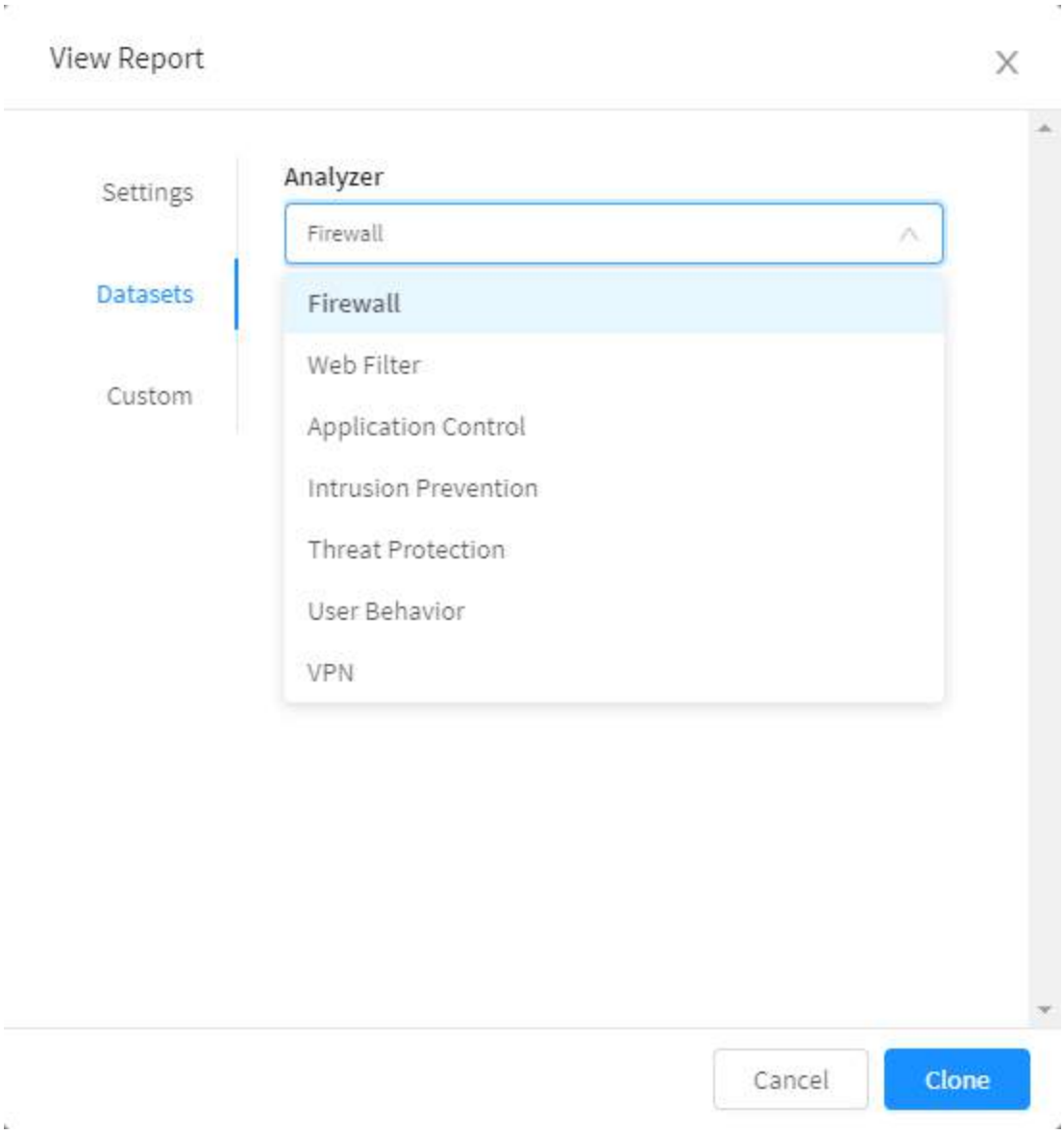
- ***Period*:** Determina o período de quando os dados serão analisados pelo *logger* nos UTMs Ex.: Ao selecionar de 1 de janeiro de 2019 a 05 de fevereiro de 2020, todos os dados que existirem fora desse período, não serão exibidos no "*Report*".
- ***Device/Logger*:** É selecionado o device de onde os dados serão analisados para gerar o relatório.
- ***Send report by e-mail:*** Marque esta opção [] para receber os relatórios gerados em analytics por e-mail, na periodicidade determinada para que os mesmos sejam gerados.

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*

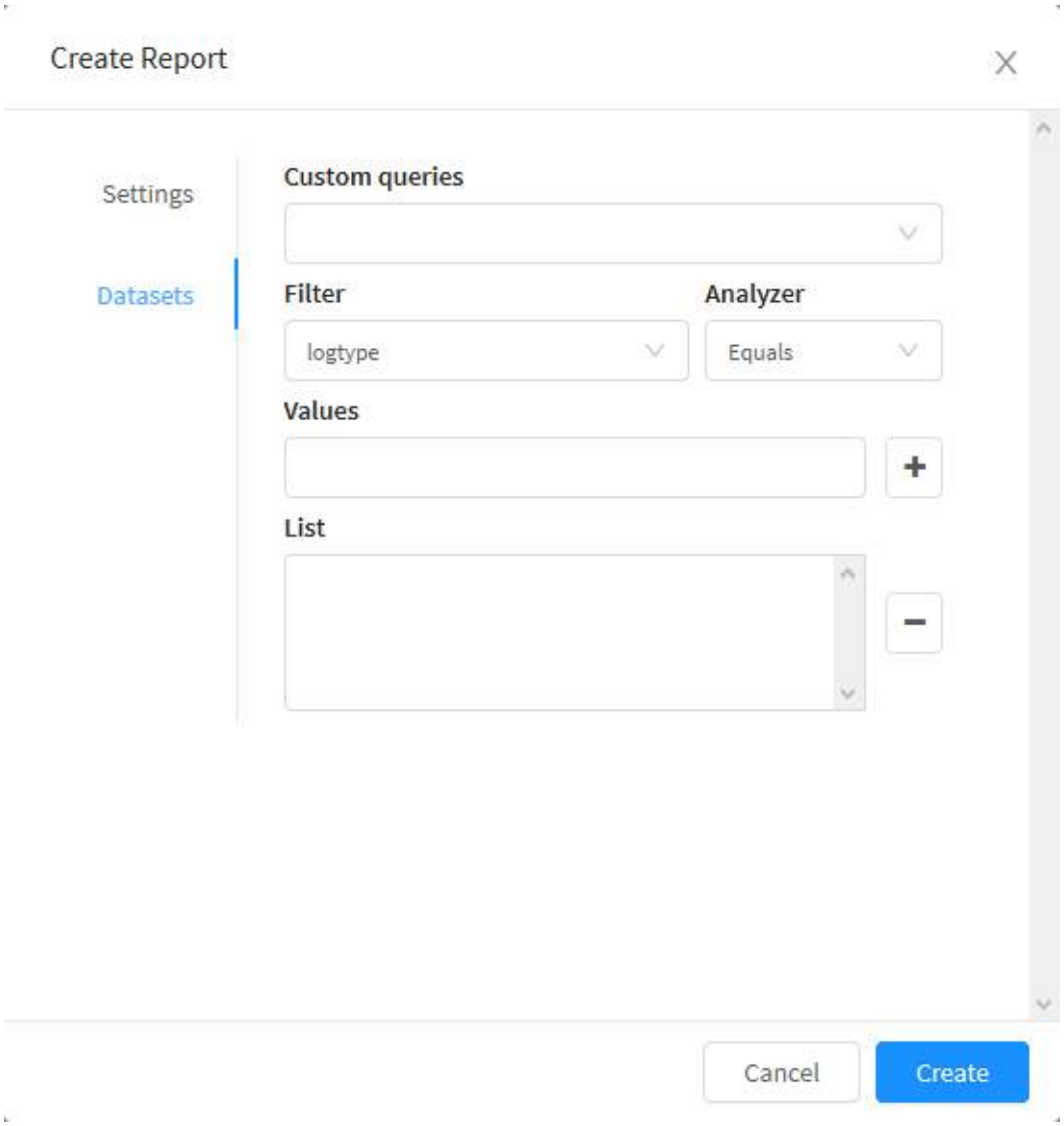
A aba “*Datasets*” determina os tipos de dados que serão utilizados na criação dos relatórios, conforme mencionado anteriormente, os componentes dela são determinados pela caixa de seleção “*Type*” da aba “*Settings*”. Caso tenha selecionado a opção "Analyzer", a aba "*Datasets"* poderá ser configurada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



Reports – Create Report - Datasets - Analyzer

- ***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;
- ***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;

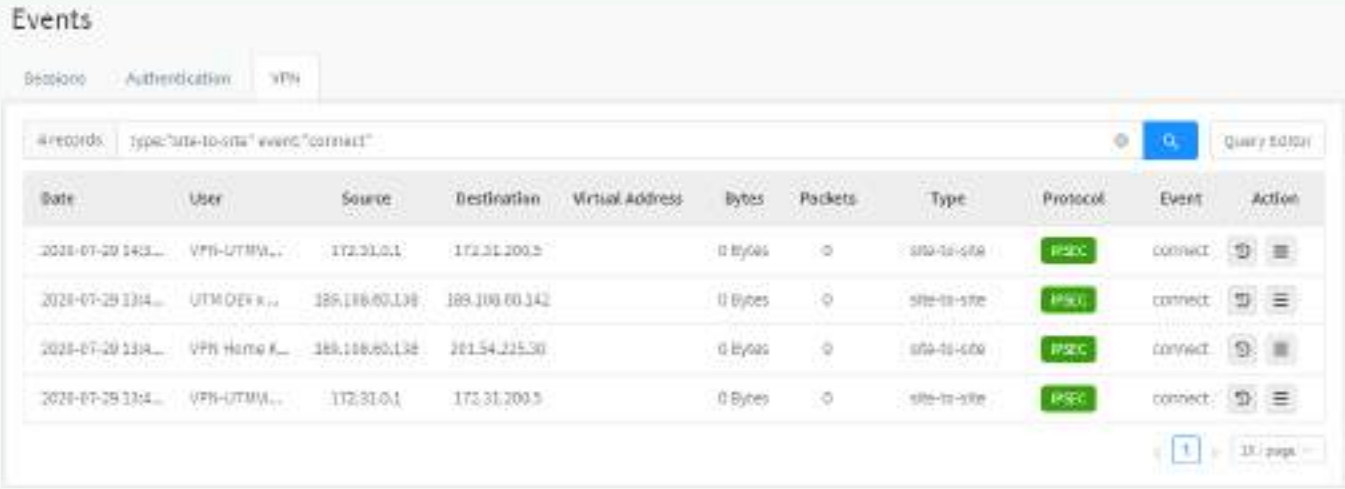
Caso tenha selecionado a opção "Log Session", a aba "*Datasets"* poderá ser configurada conforme as opções abaixo:



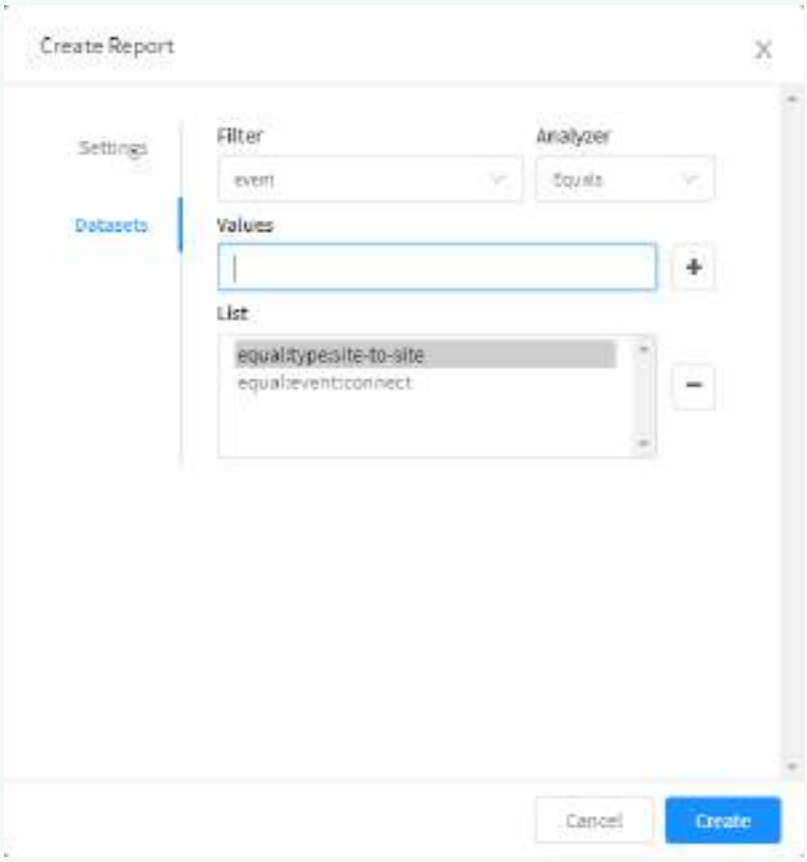
Reports – Create Report - Datasets - Log Session

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:



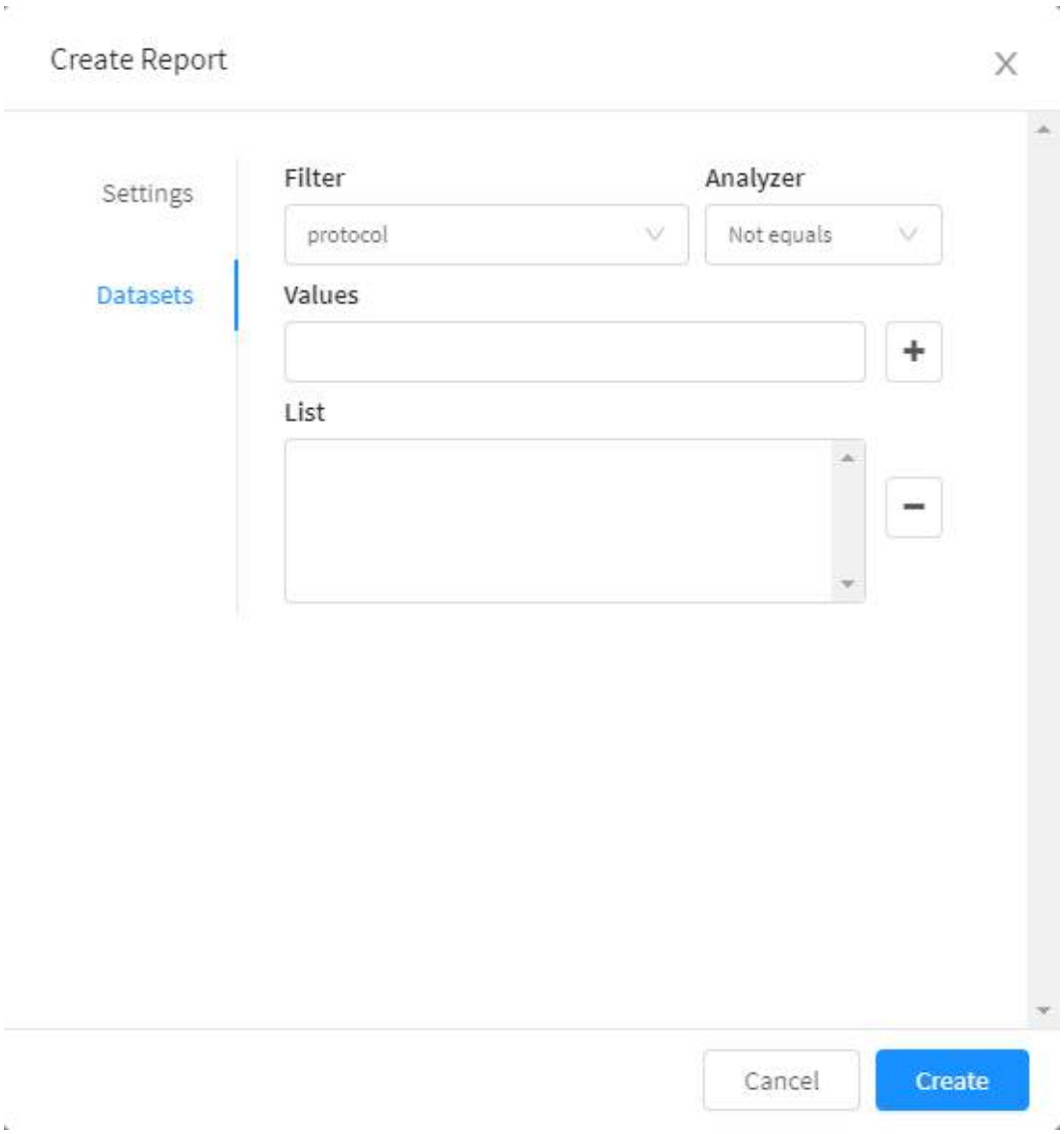
Feito isso, de volta em *Create Report - Datasets,* replicar a mesma sintaxe utilizando as opções do painel, segue um exemplo:



- ***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:



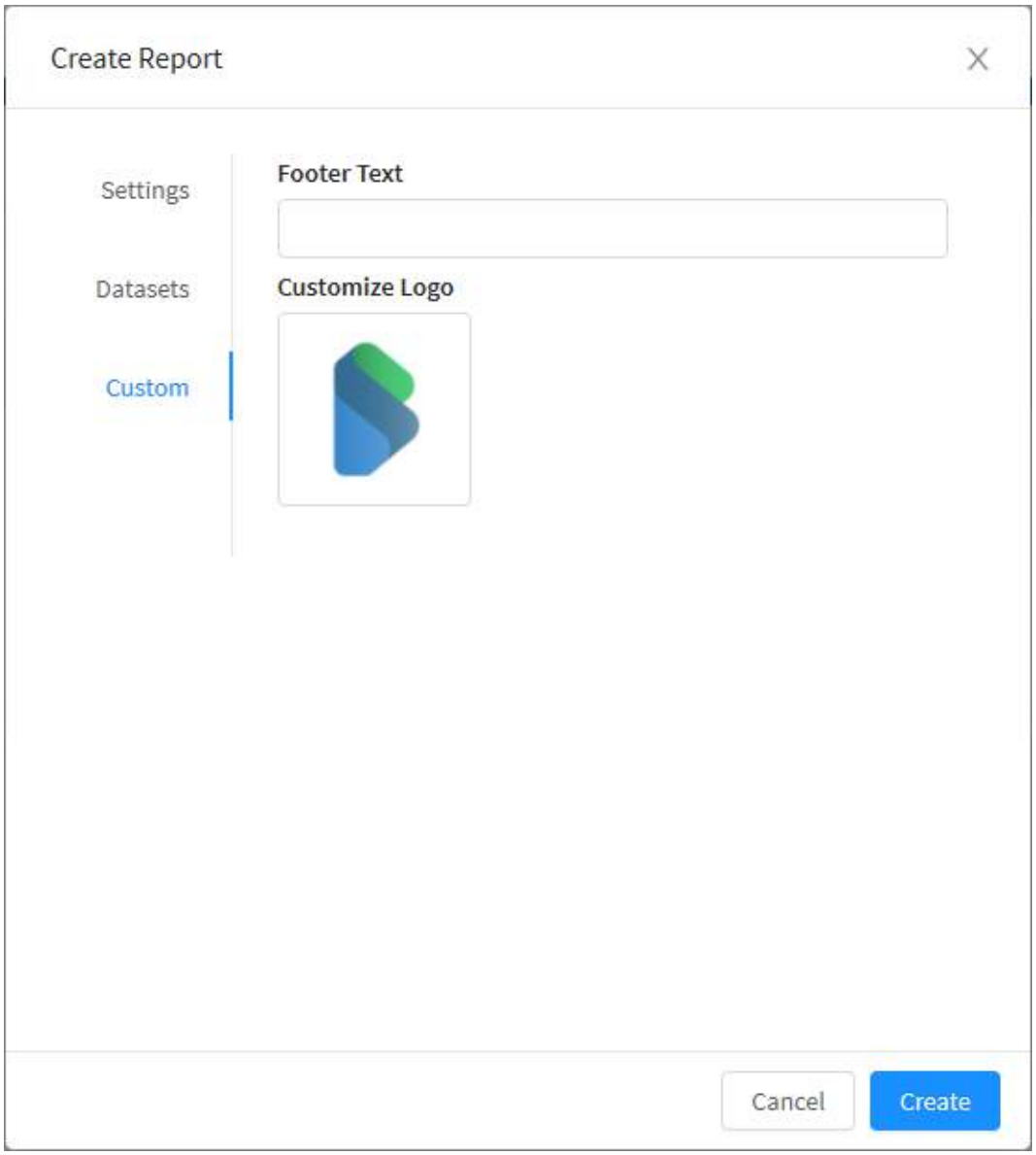
Reports – Create Report - Datasets - Log Authentication ou *Log VPN*

- ***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.

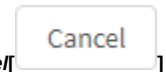
A seguir vamos analisar o conteúdo da aba lateral "*Custom"*, ela só será exibida caso o tipo de relatório for "*Analyzer"*;

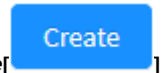
Aba *Custom*

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

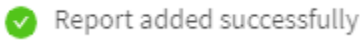


Reports – Create Report - Custom

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

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

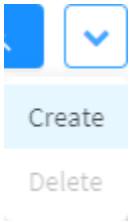
A seguir, vamos exemplificar a criação de alguns exemplos de *reports* como forma de demonstrar de boas práticas. Os modelo apresentados visam orientar e servir como base para o usuário criar os seus próprios relatórios conforme a sua preferência e necessidade.

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.

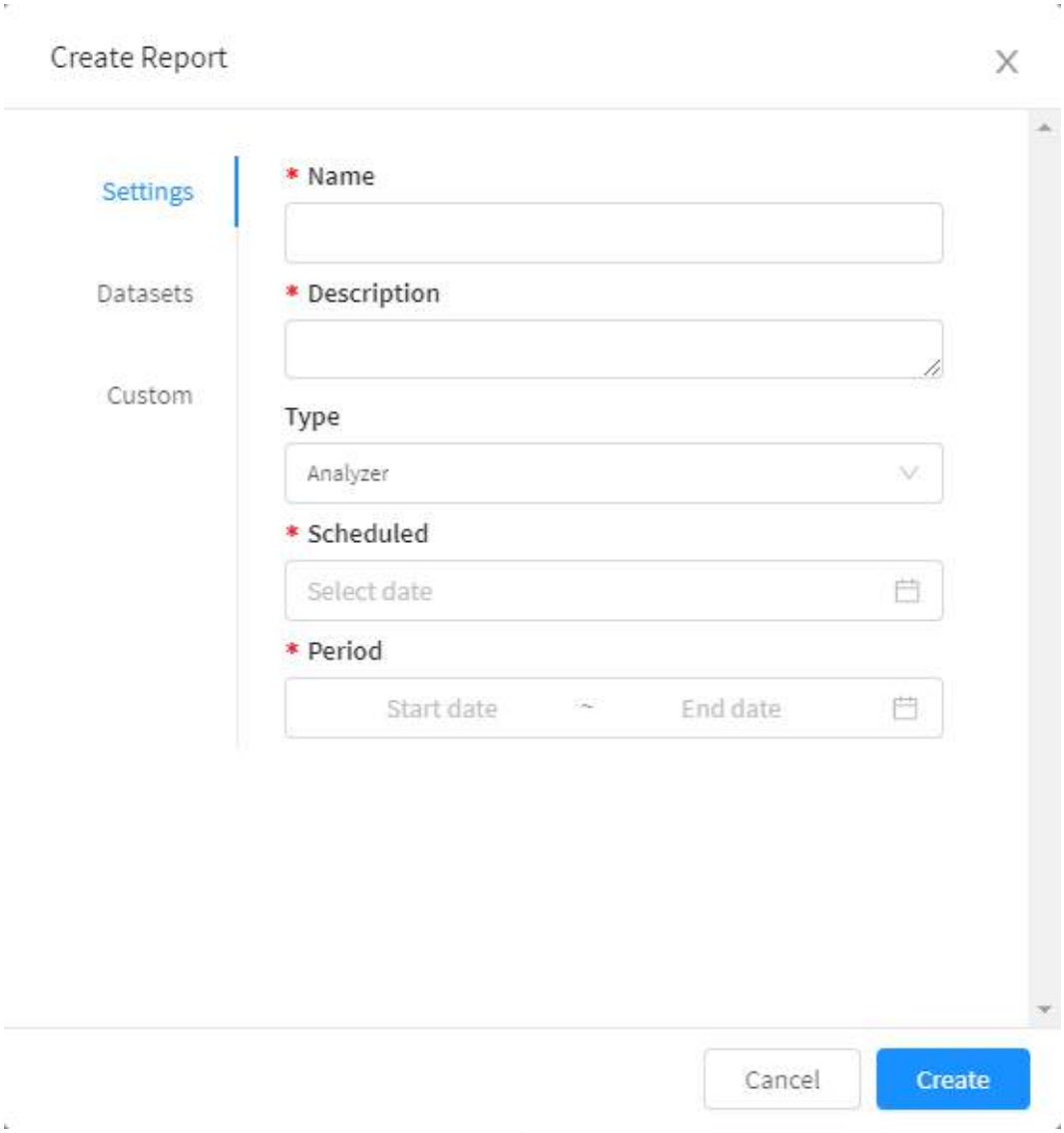
Exemplo 1 - Relatório de Firewall

Para gerar um relatório de *firewall*, primeiramente clique no menu de ações **[**  **]** e selecione a opção "*create"*:



Menu de ações - *Create*

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

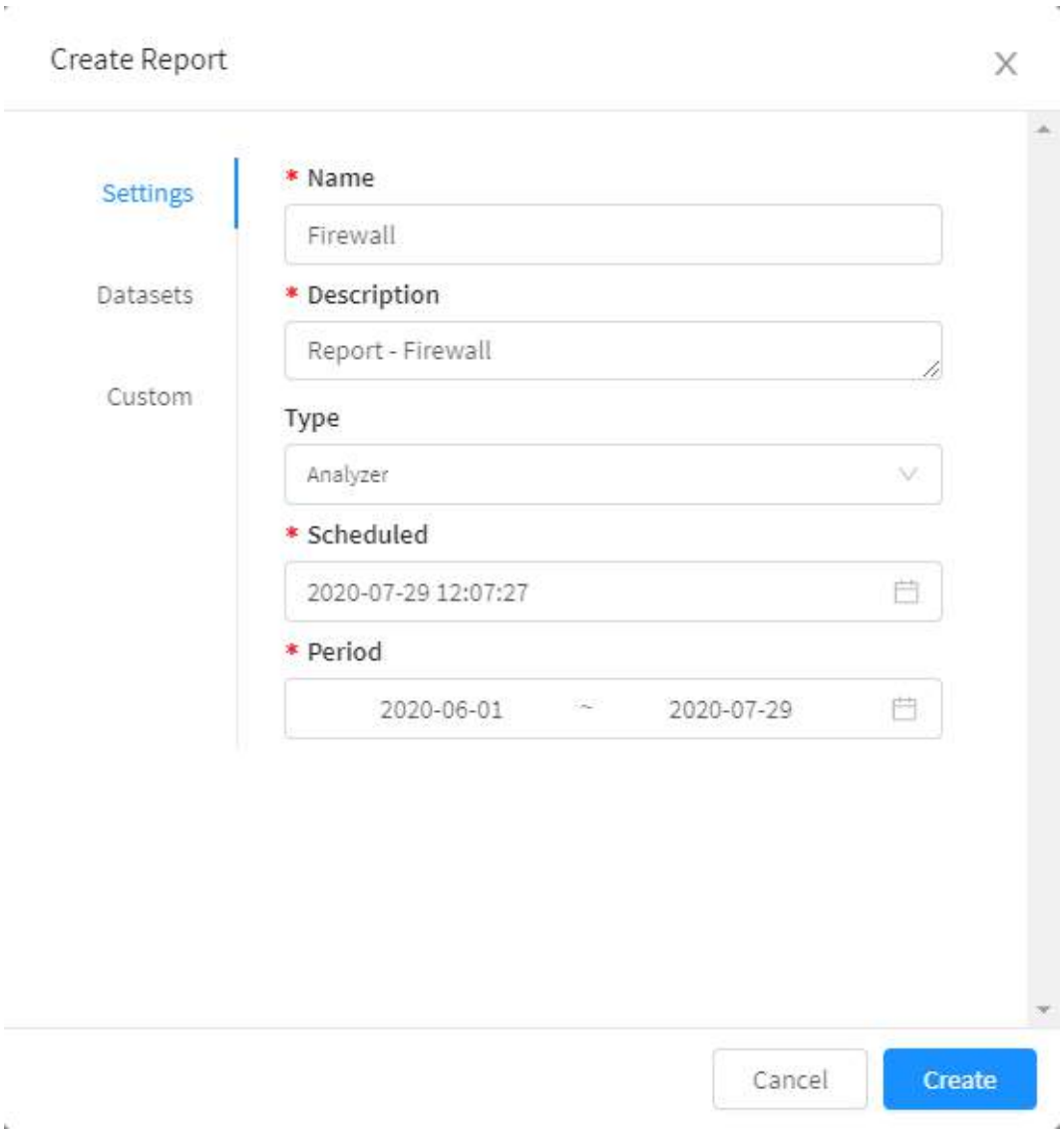


Reports - Create Report

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

Settings

Complete o formulário conforme o exemplo:



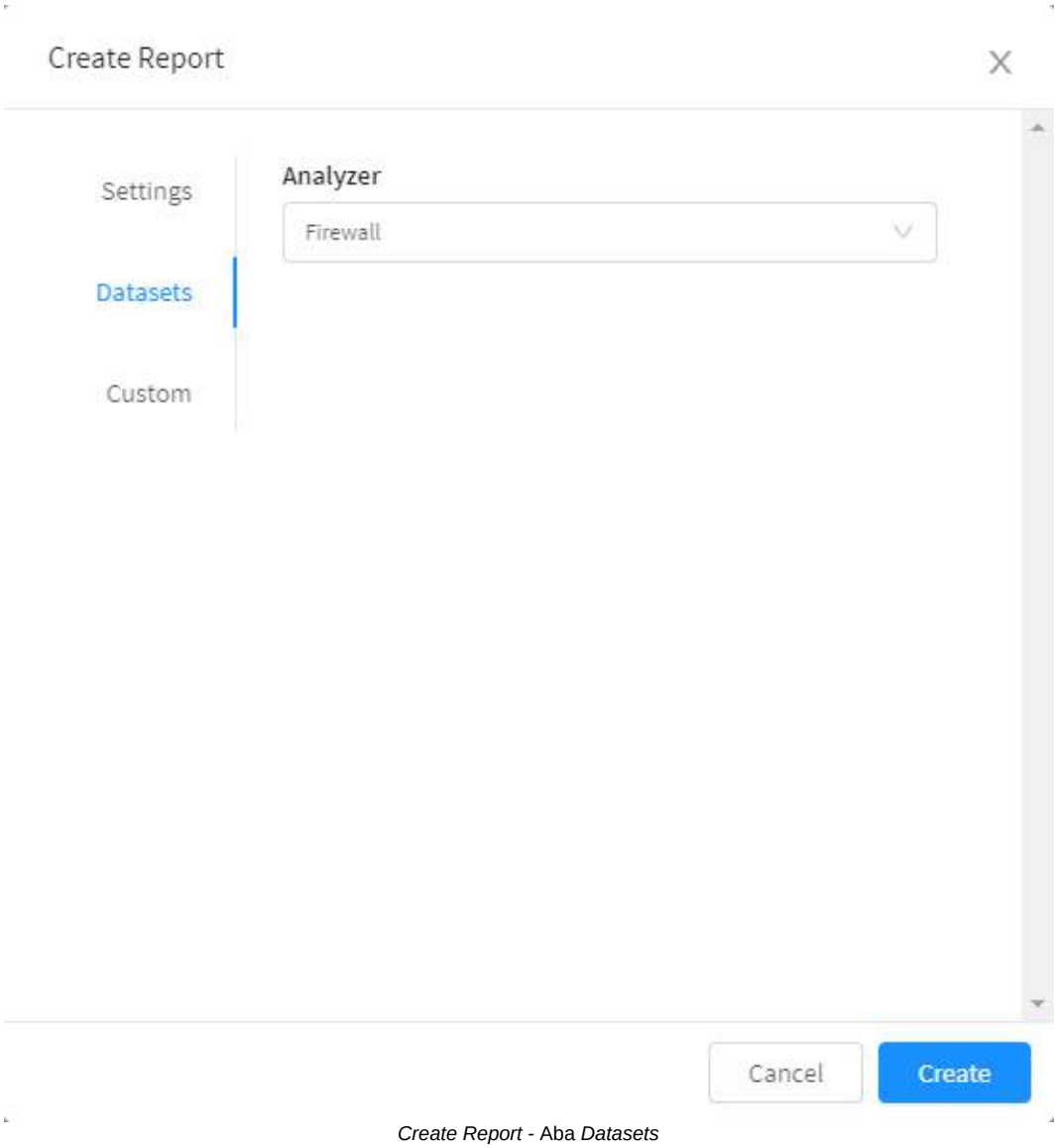
Create Report - Aba *Settings*

- ***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:



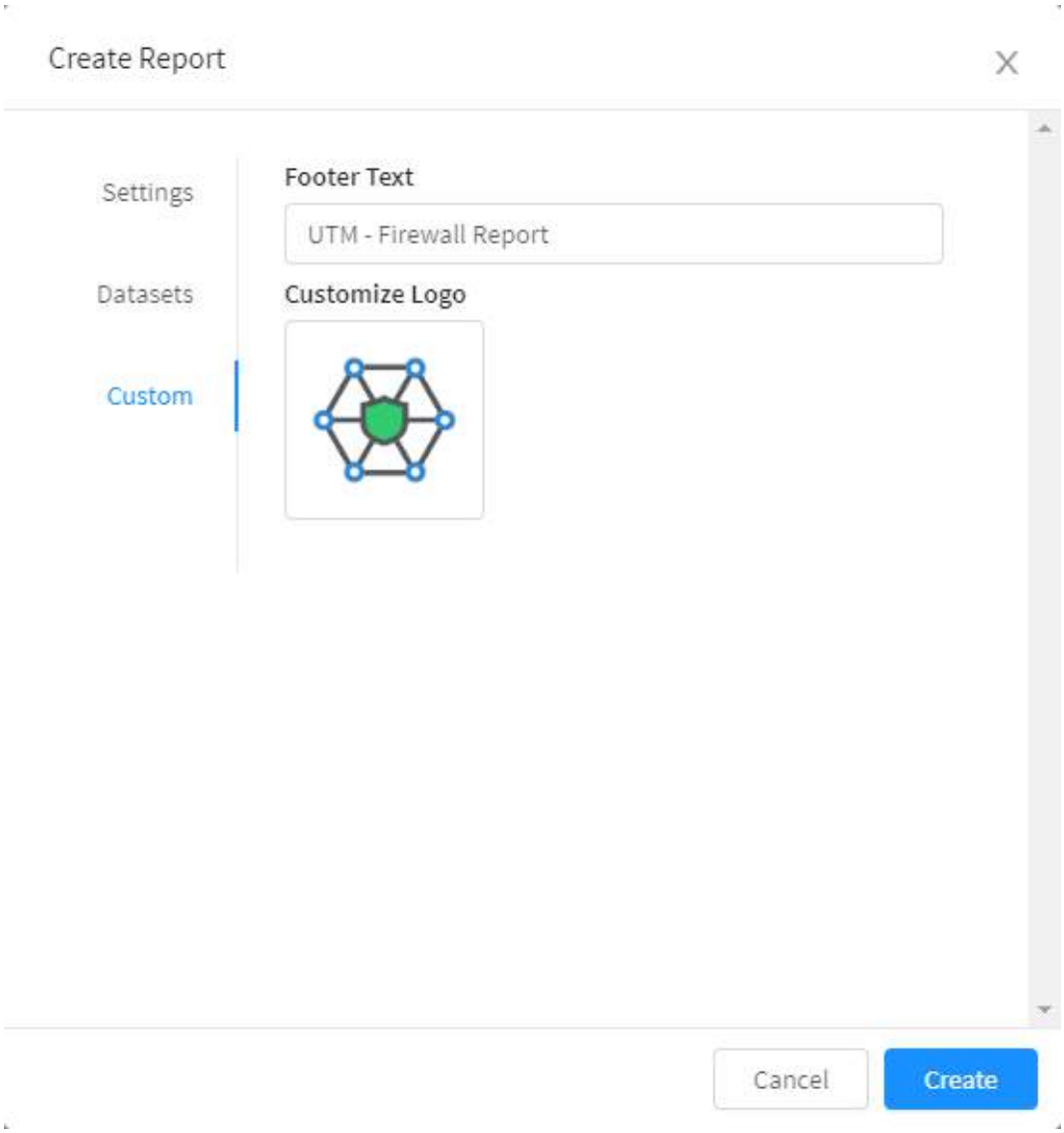
Create Report - Aba *Datasets*

- ***Analyzer*:** Selecione a opção "*Firewall*".

Ao finalizar, acesse a aba lateral "*Custom".*

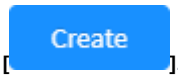
Custom

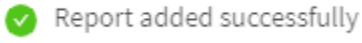
Esta aba depende do *design* do usuário. No exemplo, configuramos conforme demonstrado abaixo:



Create Report - Aba Custom

- ***Footer Text*:** No rodapé digite "*UTM - Firewall Report*";
- ***Customize Logo*:** Faça o *upload* do logo da empresa. Neste exemplo, utilizamos o ícone do *UTM*.

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



Report added successfully

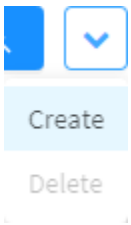
Depois destes passos, o relatório terá sido criado com sucesso.

Para consultar o exemplo 2, clique neste link.

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

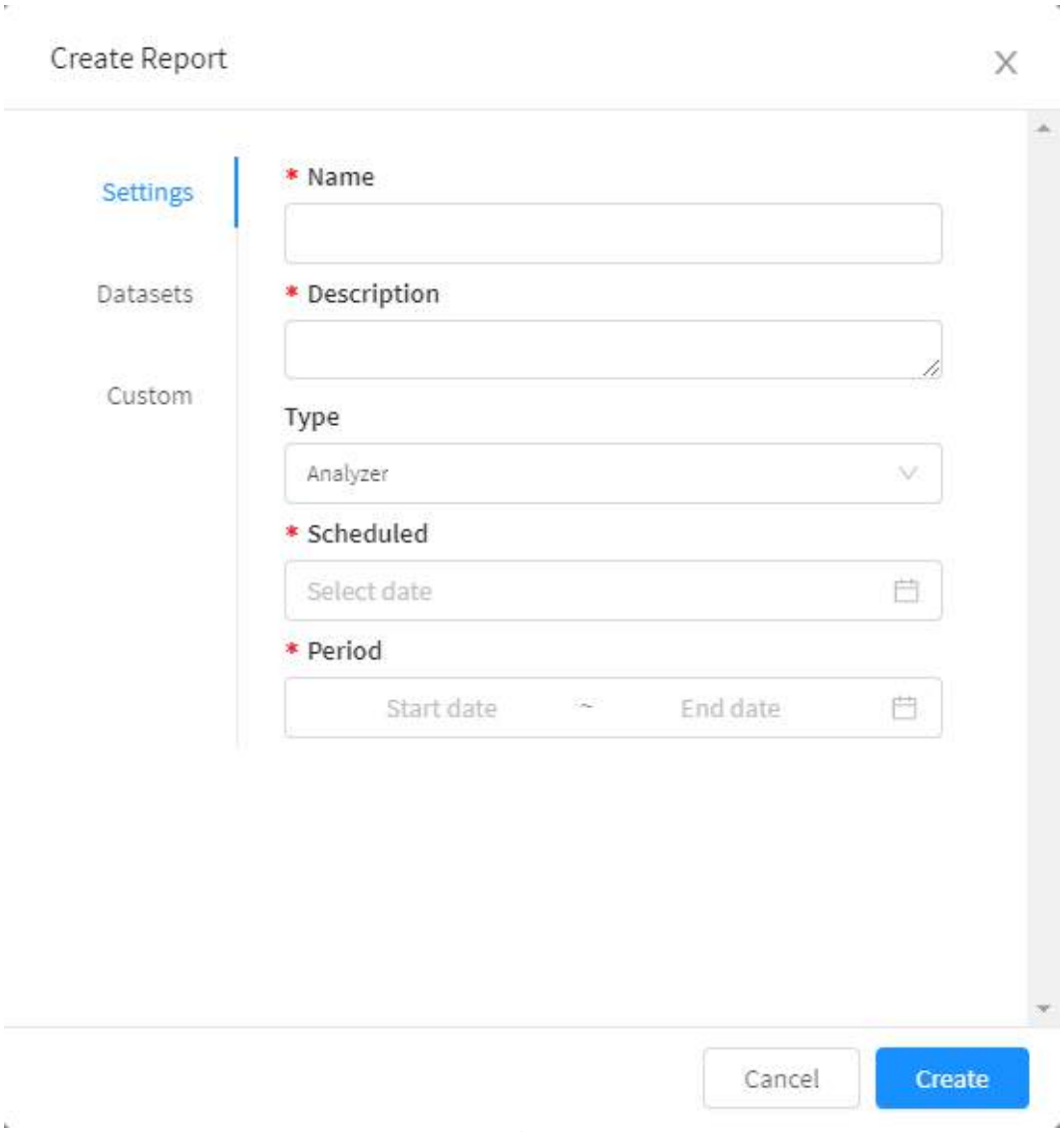
Neste exemplo iremos criar um relatório de *Web Filter* para exibir todas as conexões que foram feitas para sites estrangeiros onde a política permitiu o acesso.

Para gerar um relatório de *Web Filter*, primeiramente clique no menu de ações **[**  **]** e selecione a opção "*create"*:



Menu de ações - *Create*

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

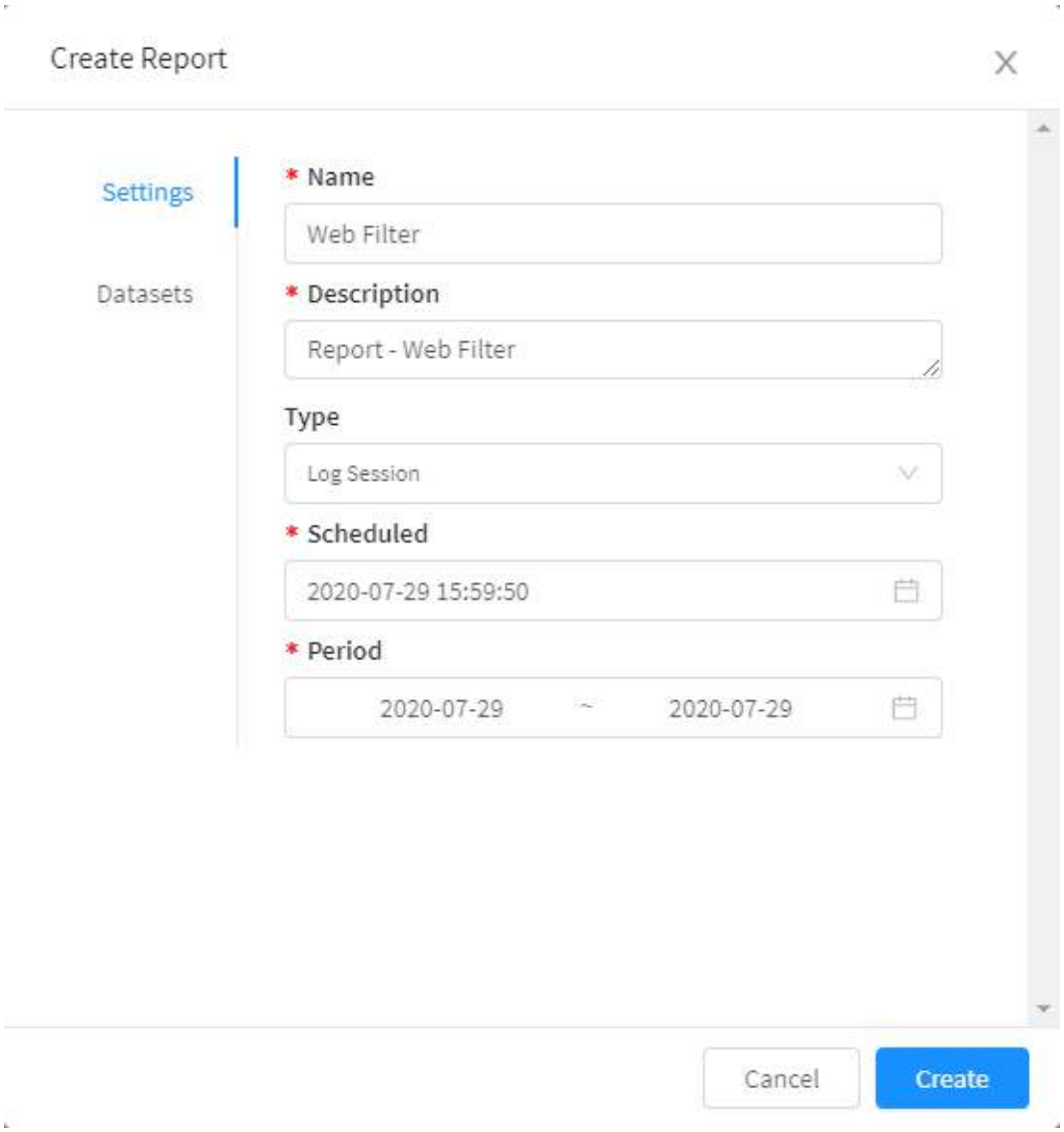


Reports - Create Report

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

Settings

Complete o formulário conforme o exemplo:



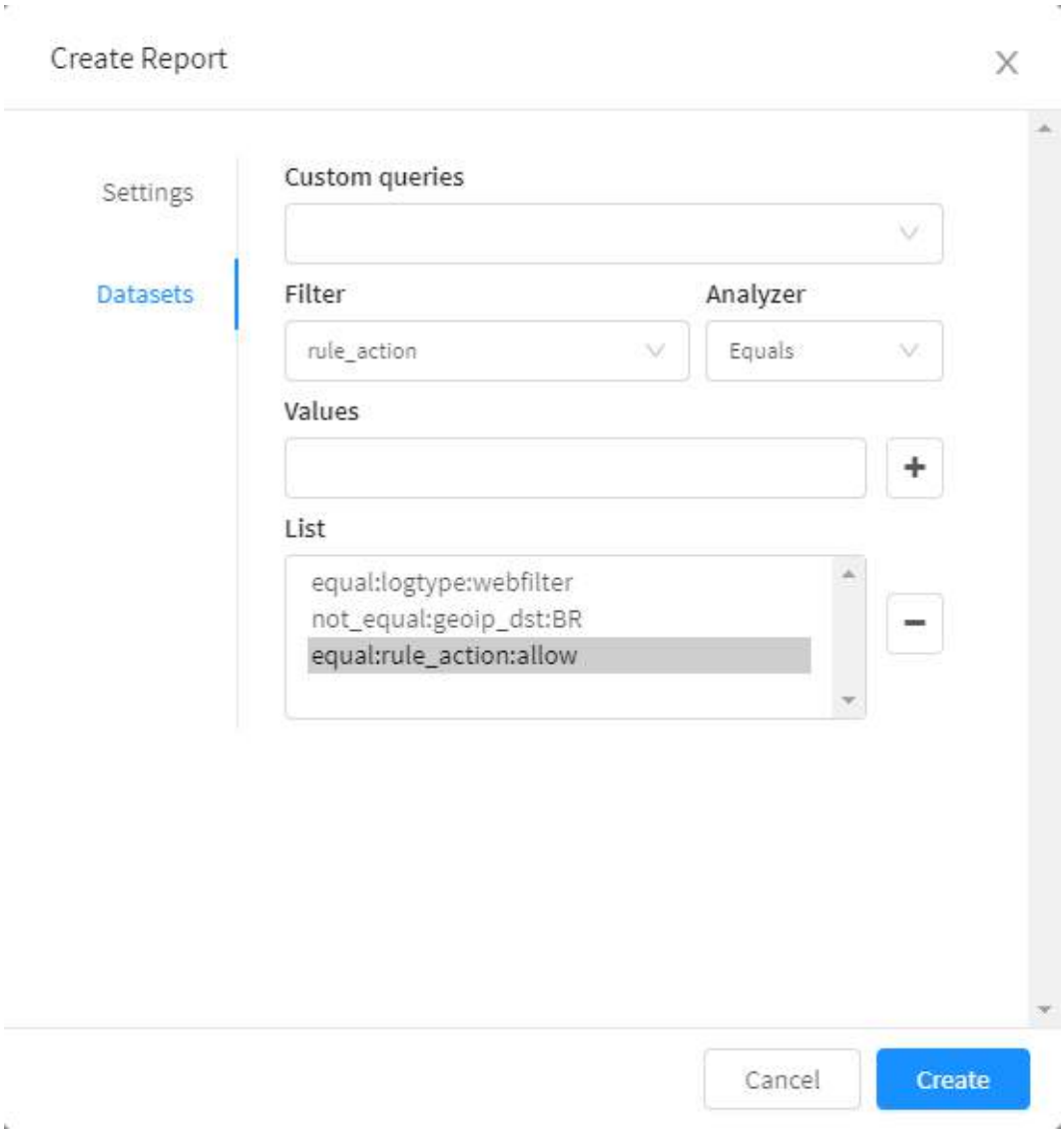
Create Report - Aba *Settings*

- ***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 - Aba *Datasets*

Nesta aba iremos adicionar 3 condições:

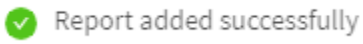
1. Tipo de *Log Web Filter*: Em ***Filter***, selecione *logtype*, deixe o ***Analyzer*** como equals, em ***Values*** digite webfilter e clique no botão **[+]** para fazer a adição na lista;

2. Localização geográfica de destino estrangeira: Em ***Filter***, selecione *geoip_dst*, no ***Analyzer*** selecione *Not Equals*, em ***Values*** digite *BR* e clique no botão **[+]** para fazer a adição na lista;

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 **[Create]**.



Report added successfully

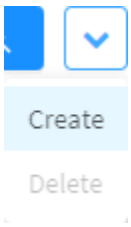
Depois destes passos, o relatório terá sido criado com sucesso.

Clique neste link para ver o exemplo 3.

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

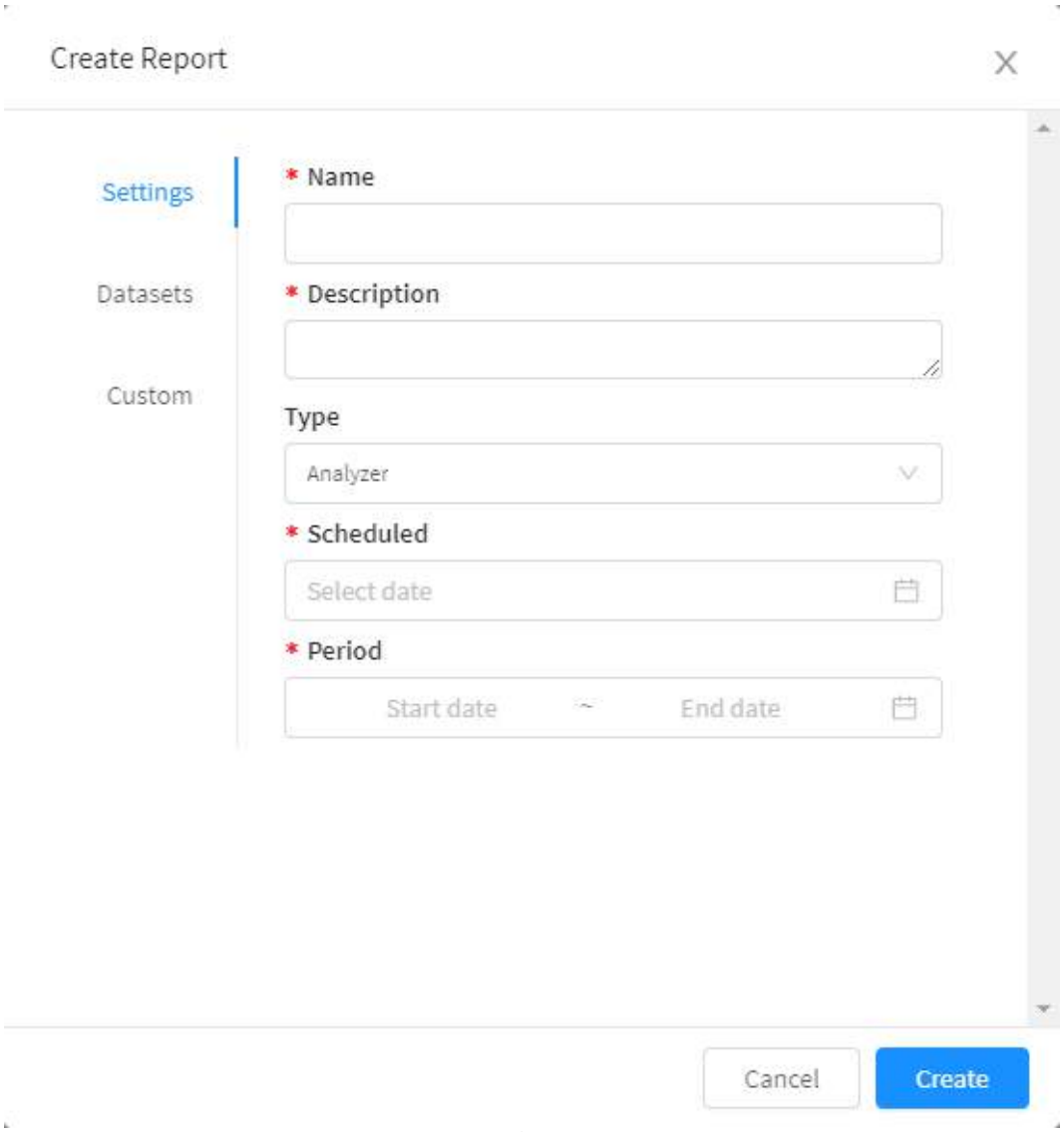
Neste exemplo vamos criar um relatório de conexão *VPN site-to-site* com objetivo de localizar todos os acessos feitos dentro de um *IP* de origem e de destino específico.

Para gerar um relatório de *VPN*, primeiramente clique no menu de ações **[**  **]** e selecione a opção "*create"*:



Menu de ações - *Create*

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

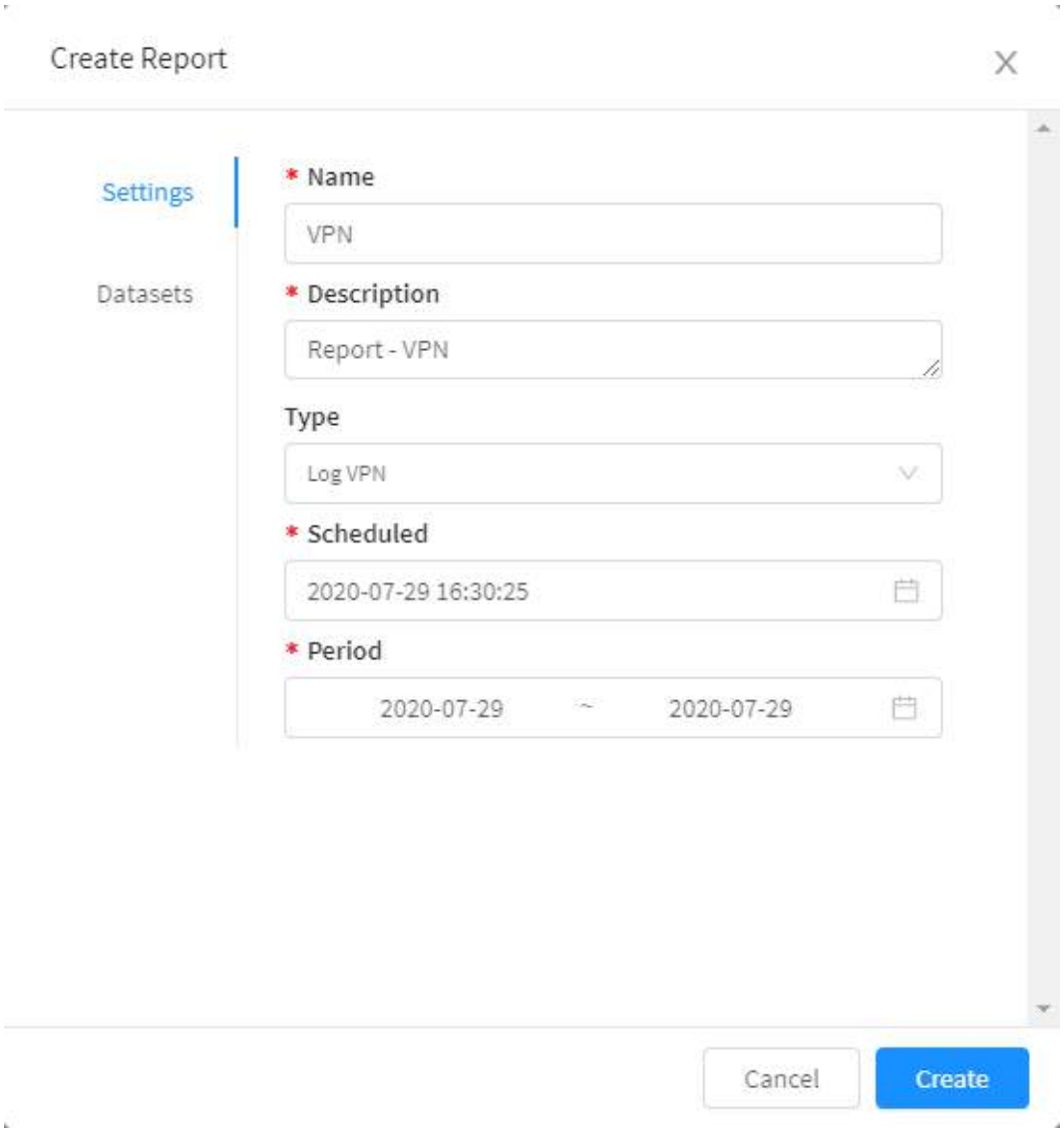


Reports - Create Report

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

Settings

Complete o formulário conforme o exemplo:



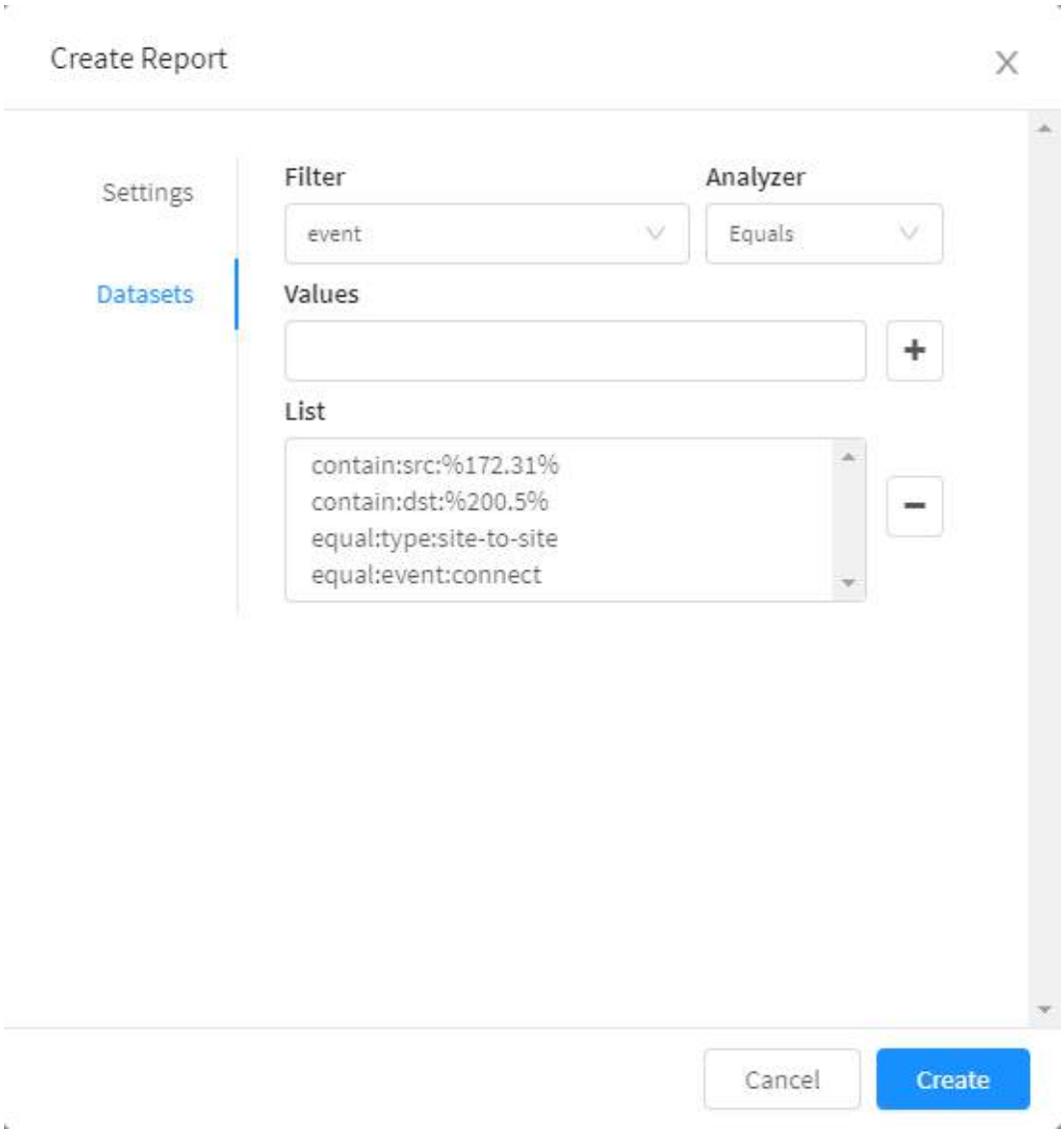
Create Report - Aba *Settings*

- ***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:



Create Report - Aba *Datasets*

Nesta aba iremos adicionar 4 condições:

1. O IP de origem começa com 172.31: Em ***Filter***, selecione *src*, no ***Analyzer*** selecione *Contain*, em ***Values*** digite 172.31 e clique no botão **[+]** par a fazer a adição na lista;

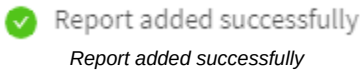
2. O IP de destino possui 200.5: Em ***Filter***, selecione *dst*, no ***Analyzer*** selecione *Contain*, em ***Values*** digite 200.5 e clique no botão **[+]** para fazer a adição na lista;

3. O tipo de VPN é site-to-site: Em ***Filter***, selecione *type*, deixe o ***Analyzer*** como equals, em ***Values*** digite *site-to-site* e clique no botão **[+]** para fazer a adição na lista;

4. Só queremos eventos de conexão: Em ***Filter***, selecione *event*, deixe o ***Analyzer*** como equals, em ***Values*** digite *connect* e clique no botão **[+]** p ara fazer a adição na lista;

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.

Após ter configurado cada aba de acordo com a definição do exemplo aplicada, clique em **[** Create **]**.



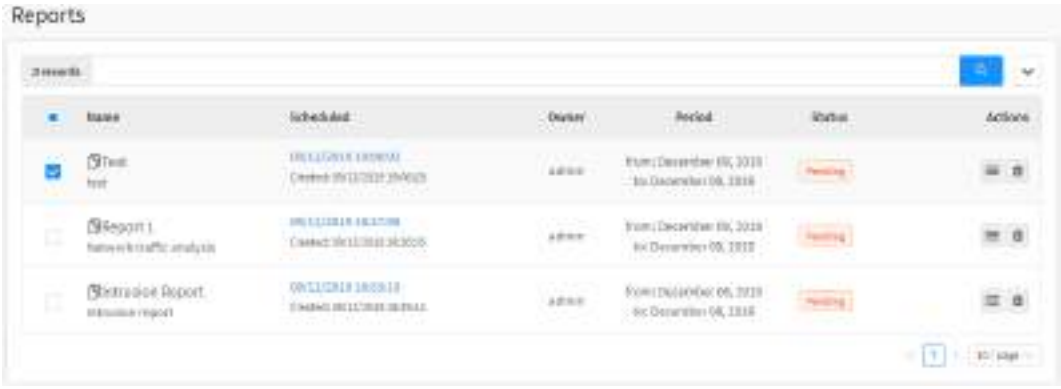
Report added successfully

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

Monitor - Reports - Menu de ações - Delete Report

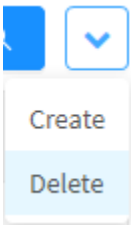
Através do botão “*Delete*” é possível deletar os *Reports* selecionados. Para deletar através do Menu de ações, siga os seguintes passos:

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*;



Reports – Seleção dos *Reports* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete*”.



Reports – Delete

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

Reports – Mensagem de deleção do *Report*

Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].

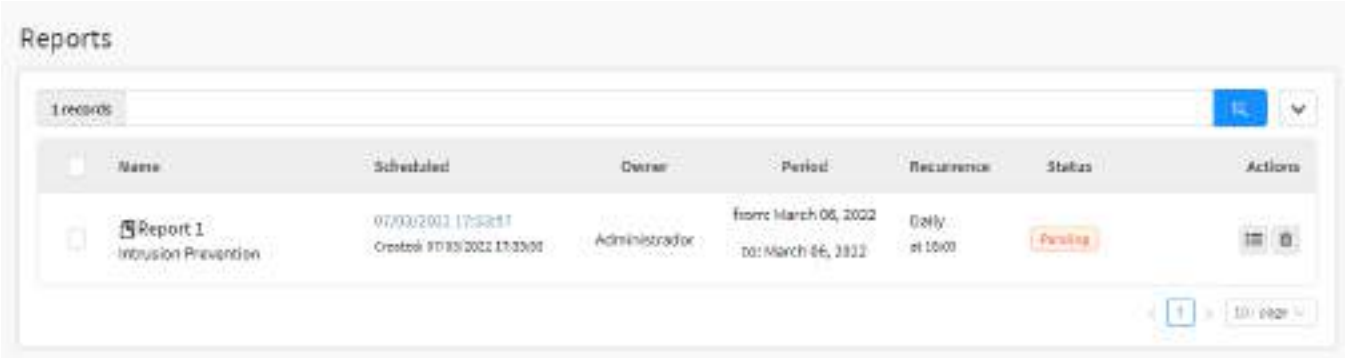
Profile deleted successfully

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*:



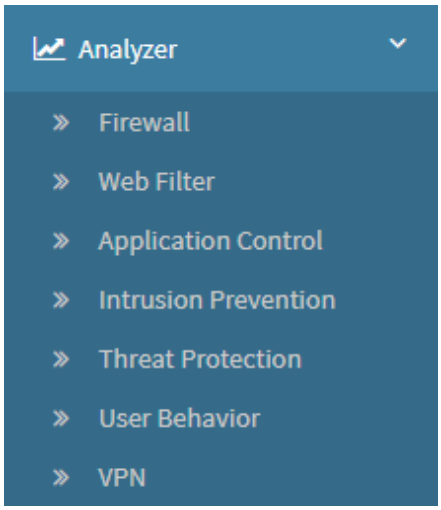
Reports

- **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*[Visualize]:** Sendo possível visualizar o relatório ao clicar neste botão;
  - ***Download*[Download]:** Sendo possível baixar o relatório PDF ou CSV ao clicar neste botão;
  - ***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[ ]:** Permite editar as configurações do *Report* adicionado na opção *Create* do menu de ações;
  - **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.



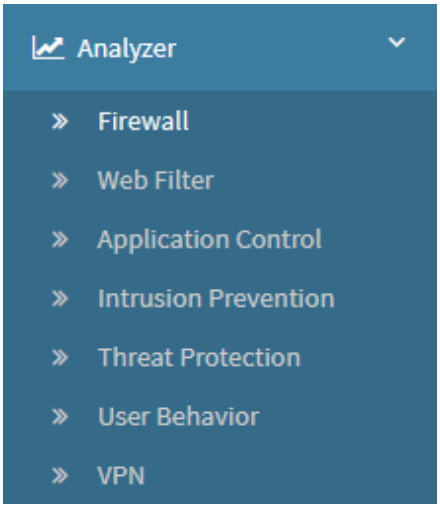
Analyzer

Contém as opções:

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

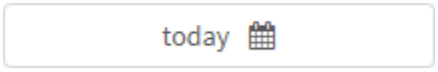
UTM - Firewall

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:

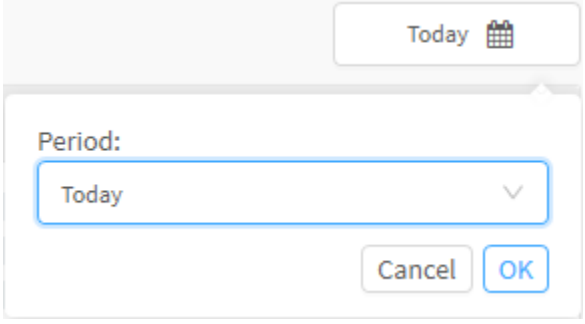


Firewall - Caixa de seleção de data

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;

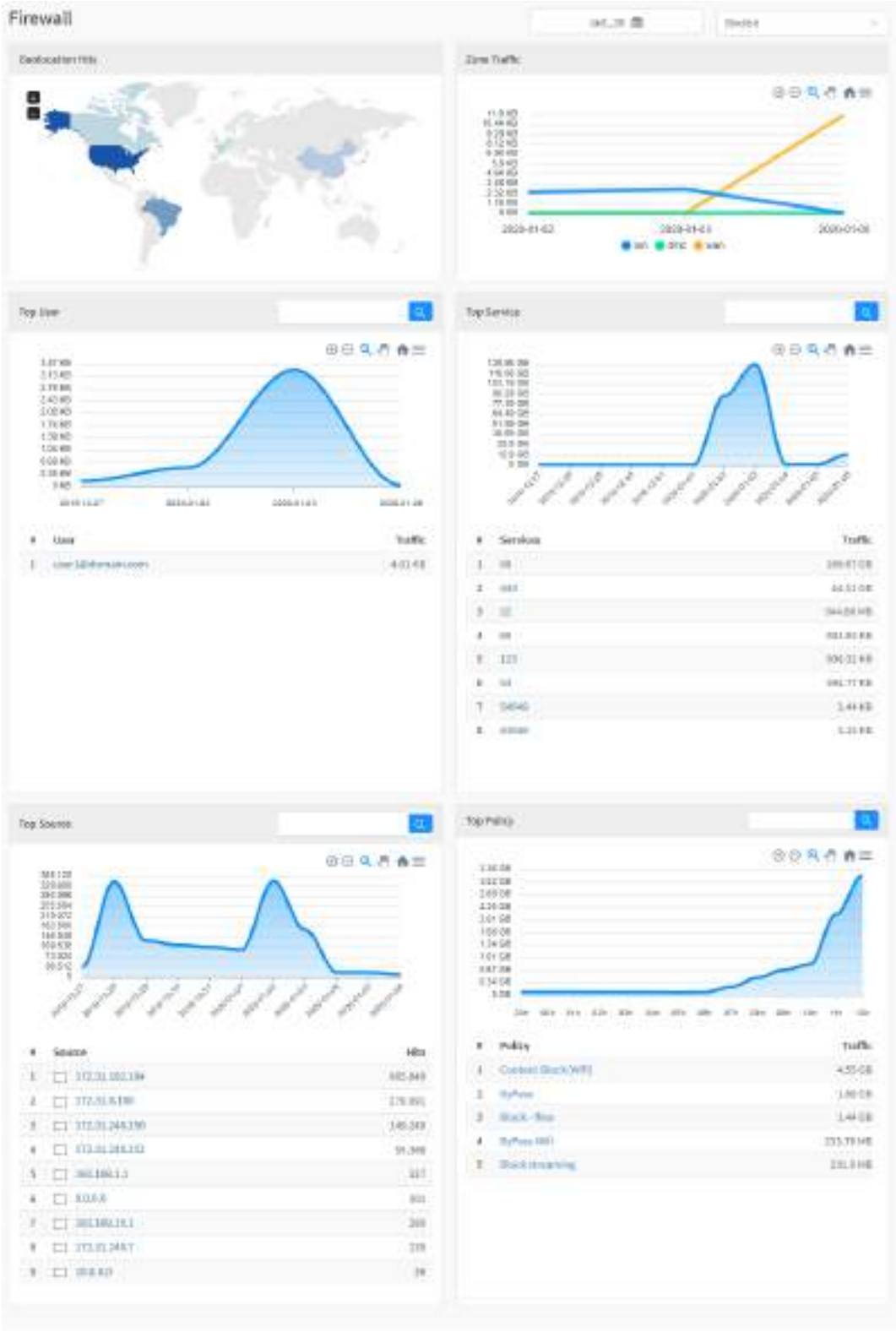
Selecione o período desejado:



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;
- []: Serve para mover o gráfico;
- []: 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*;
- *Zone Traffic*;
- *Top User*;
- *Top Service*;
- *Top Source*;
- *Top Policies*.

UTM - Firewall – Geolocation

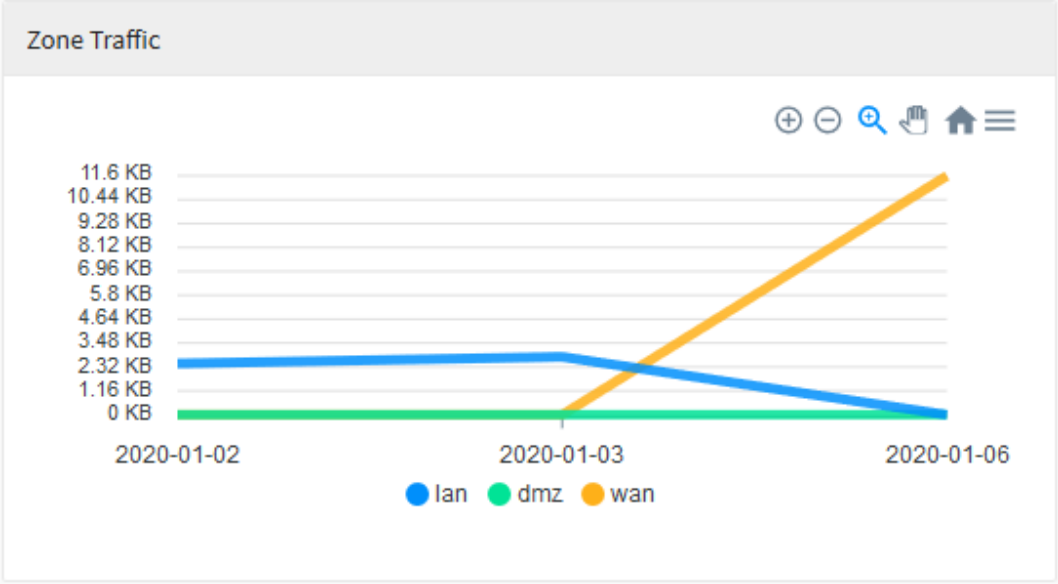
Em “*Geolocation*” é exibido o destino das conexões dos usuários da rede, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários. Ao passar o mouse por cima dos países um número total de acessos é exibido, ao fazer o mesmo com a legenda é possível visualizar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

Firewall – Geolocation

UTM - Firewall – Zone Traffic

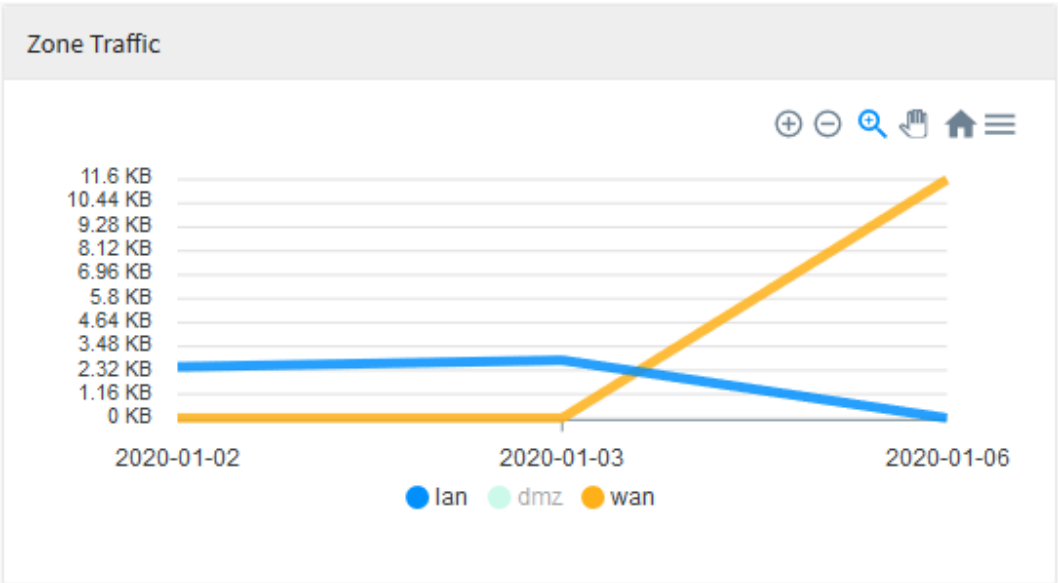
Em “*Zone Protection*” temos um gráfico demonstrando a quantia de tráfego em determinada zona, através de um gráfico de linha é possível observar esses montantes sendo ilustrados ao longo de um intervalo de tempo. Ao clicar sobre o tipo de rede utilizado (por exemplo: “*LAN*”, “*DMZ*”, “*WAN*” e etc), 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.



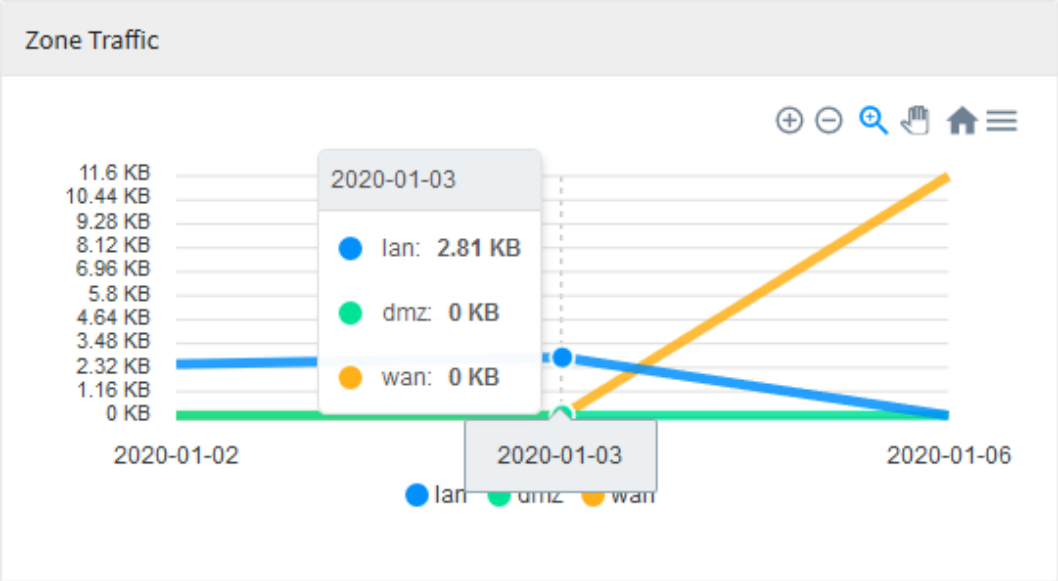
Firewall – Zone Traffic

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:

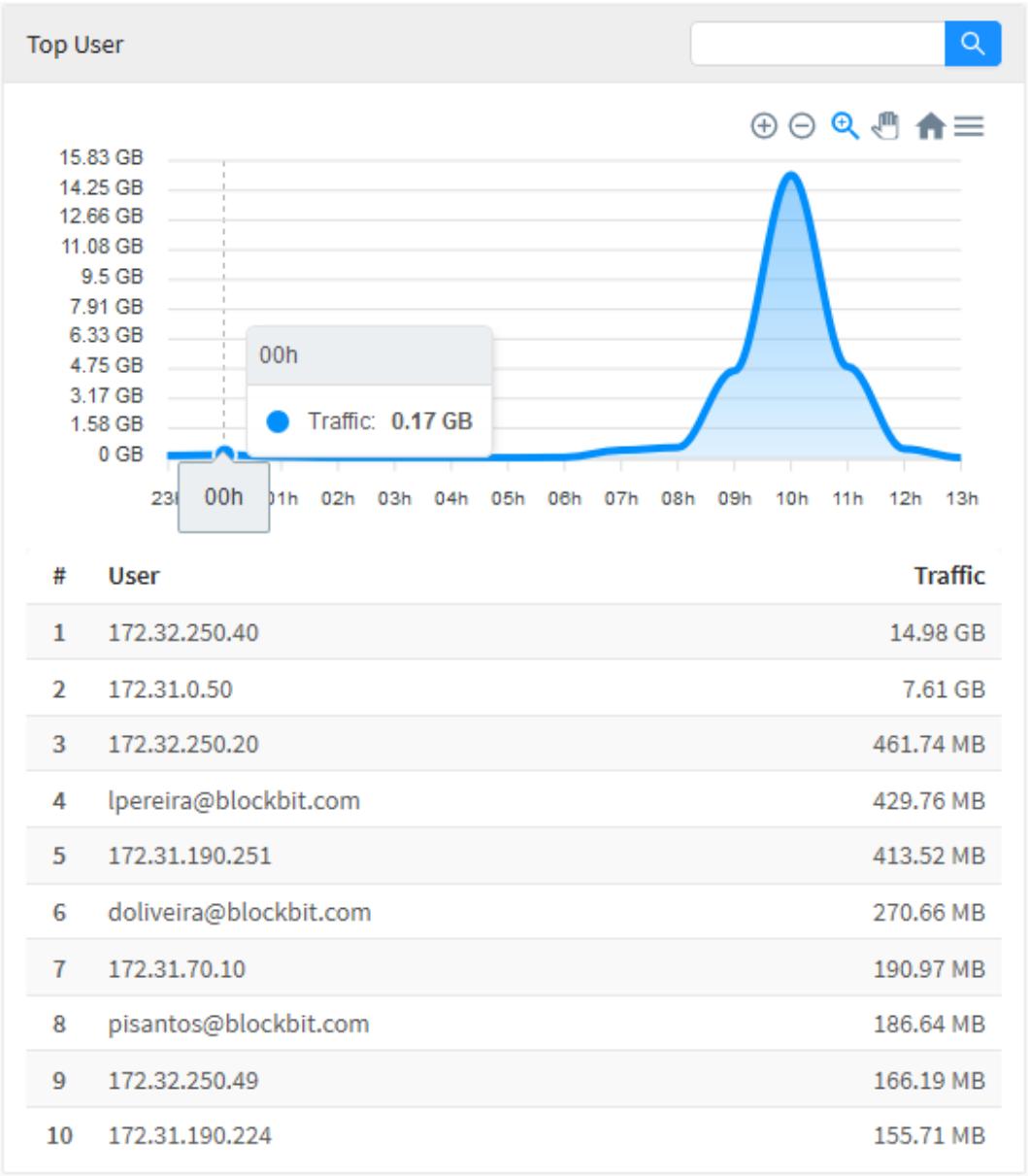


Firewall – Zone Traffic - Resumo dos resultados

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.

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



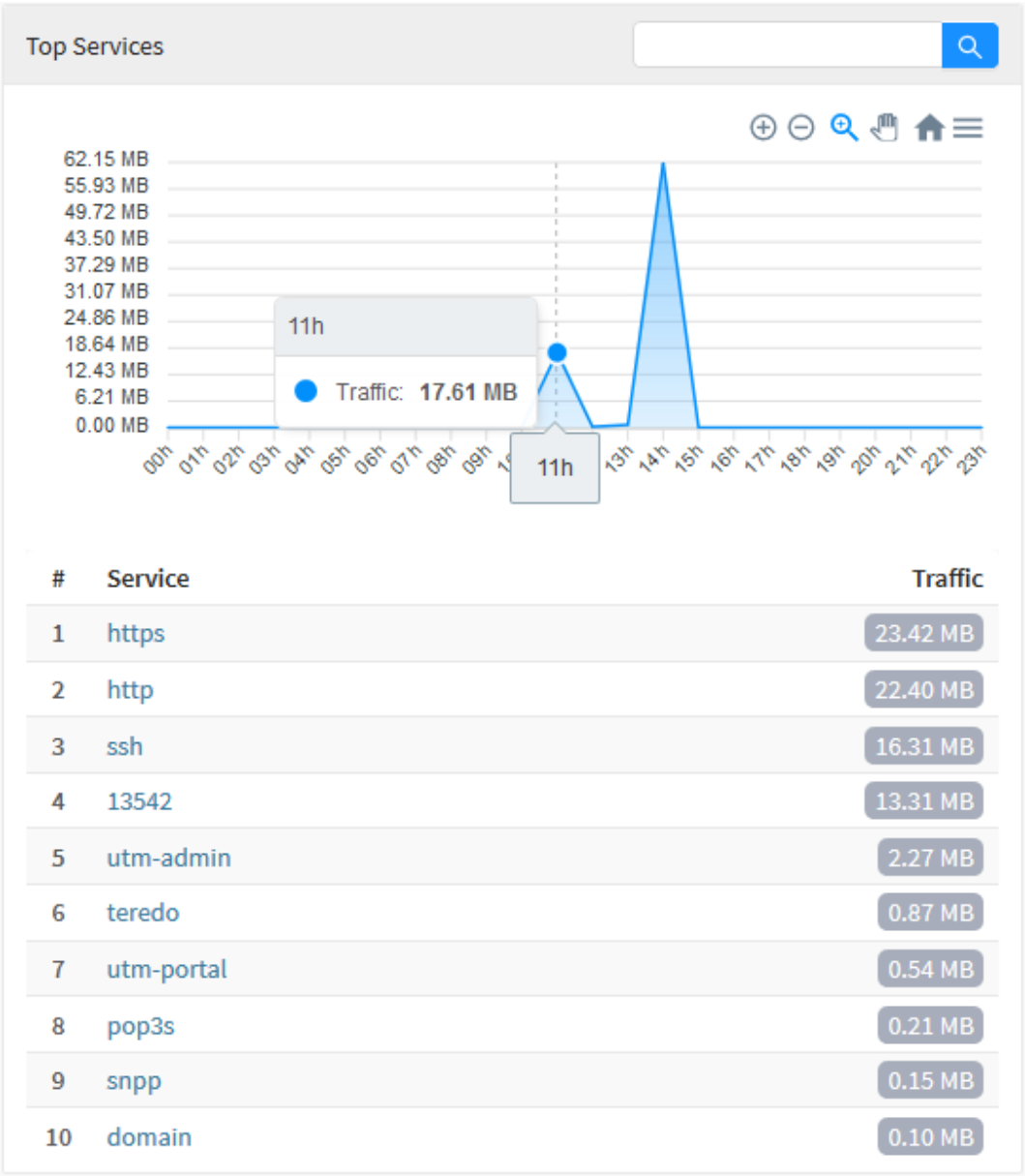
#	User	Traffic
1	172.32.250.40	14.98 GB
2	172.31.0.50	7.61 GB
3	172.32.250.20	461.74 MB
4	lpereira@blockbit.com	429.76 MB
5	172.31.190.251	413.52 MB
6	doliveira@blockbit.com	270.66 MB
7	172.31.70.10	190.97 MB
8	pisantos@blockbit.com	186.64 MB
9	172.32.250.49	166.19 MB
10	172.31.190.224	155.71 MB

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.

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

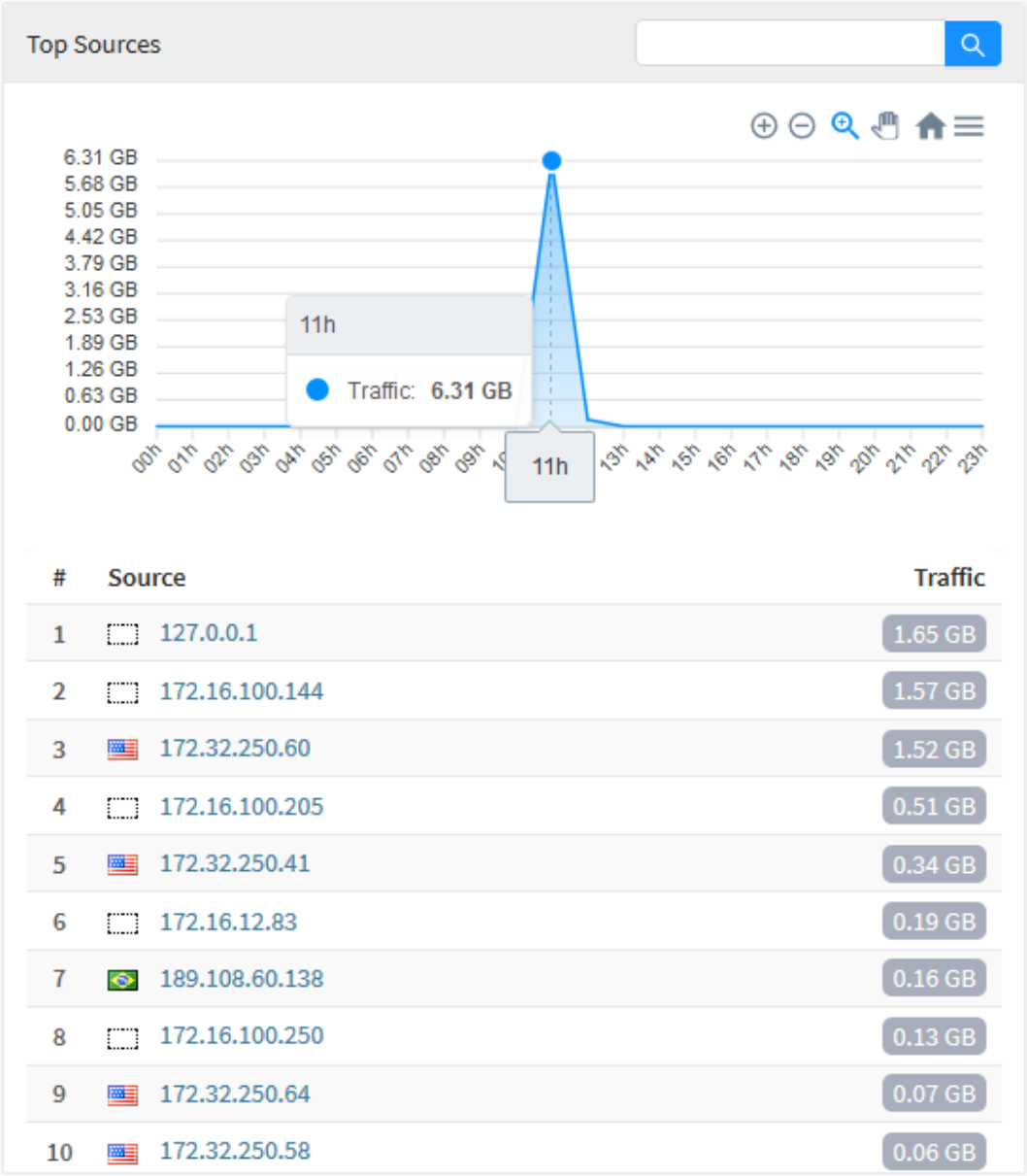


Firewall – Top Service

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.

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

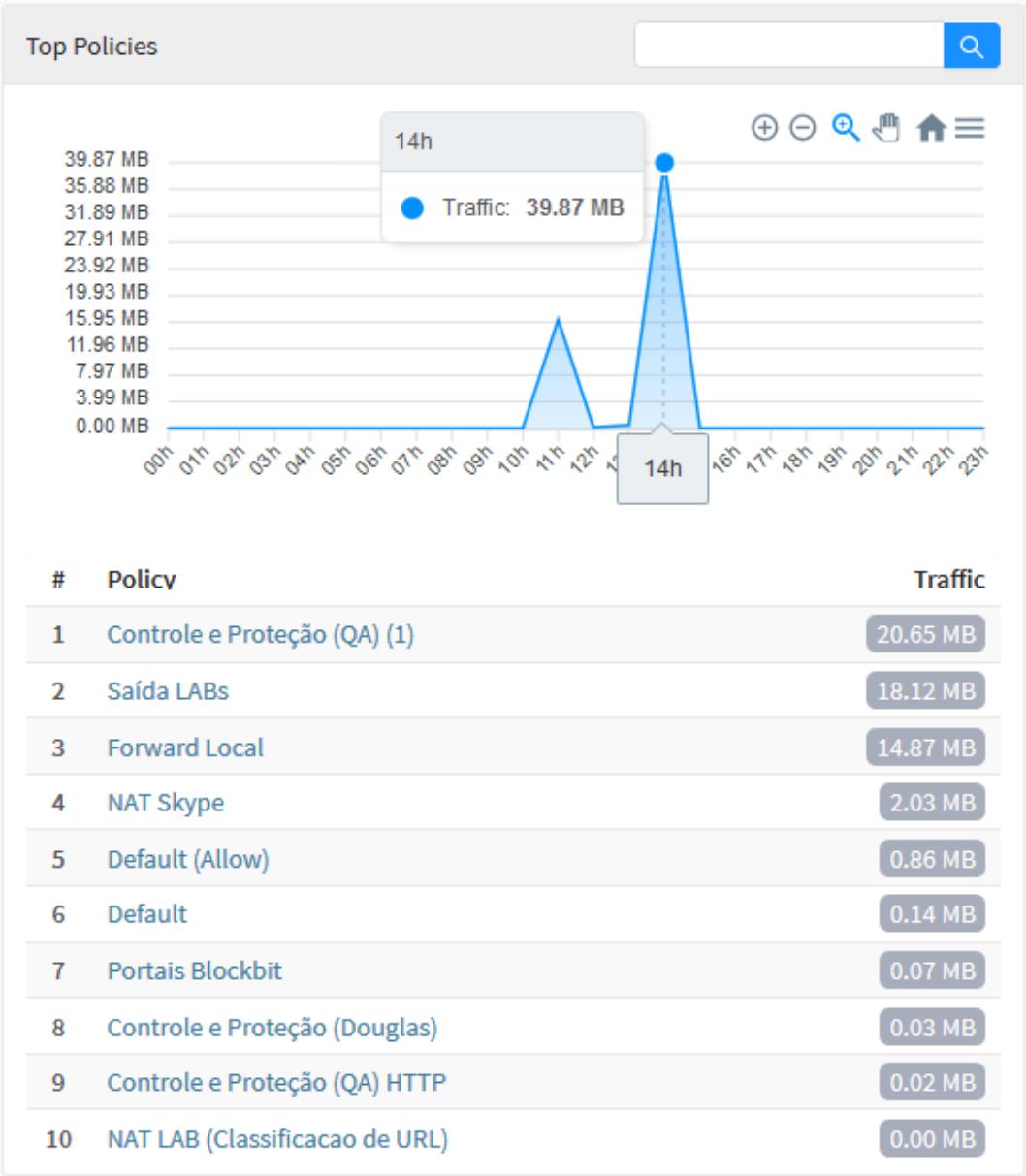


Firewall – Top Source

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.

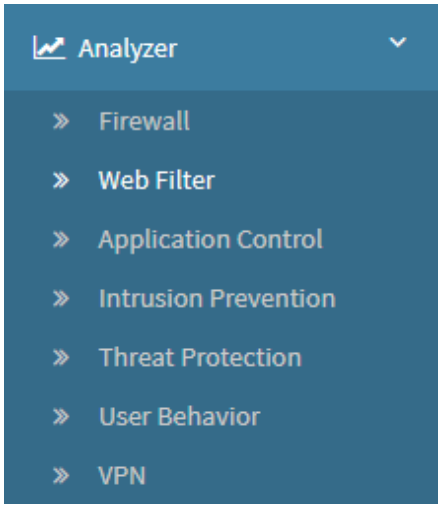
Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Firewall – Top Policies

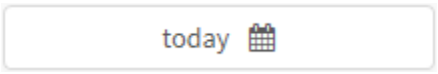
NGFW - Web Filter

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:

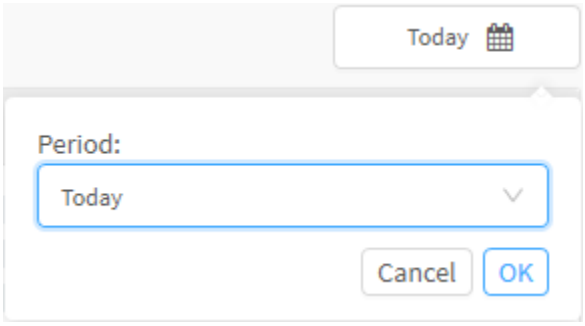


Web Filter - Caixa de seleção de data

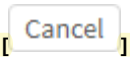
O objetivo desta mesma é basicamente permitir uma filtragem de resultados ainda mais precisa, as opções possíveis são:

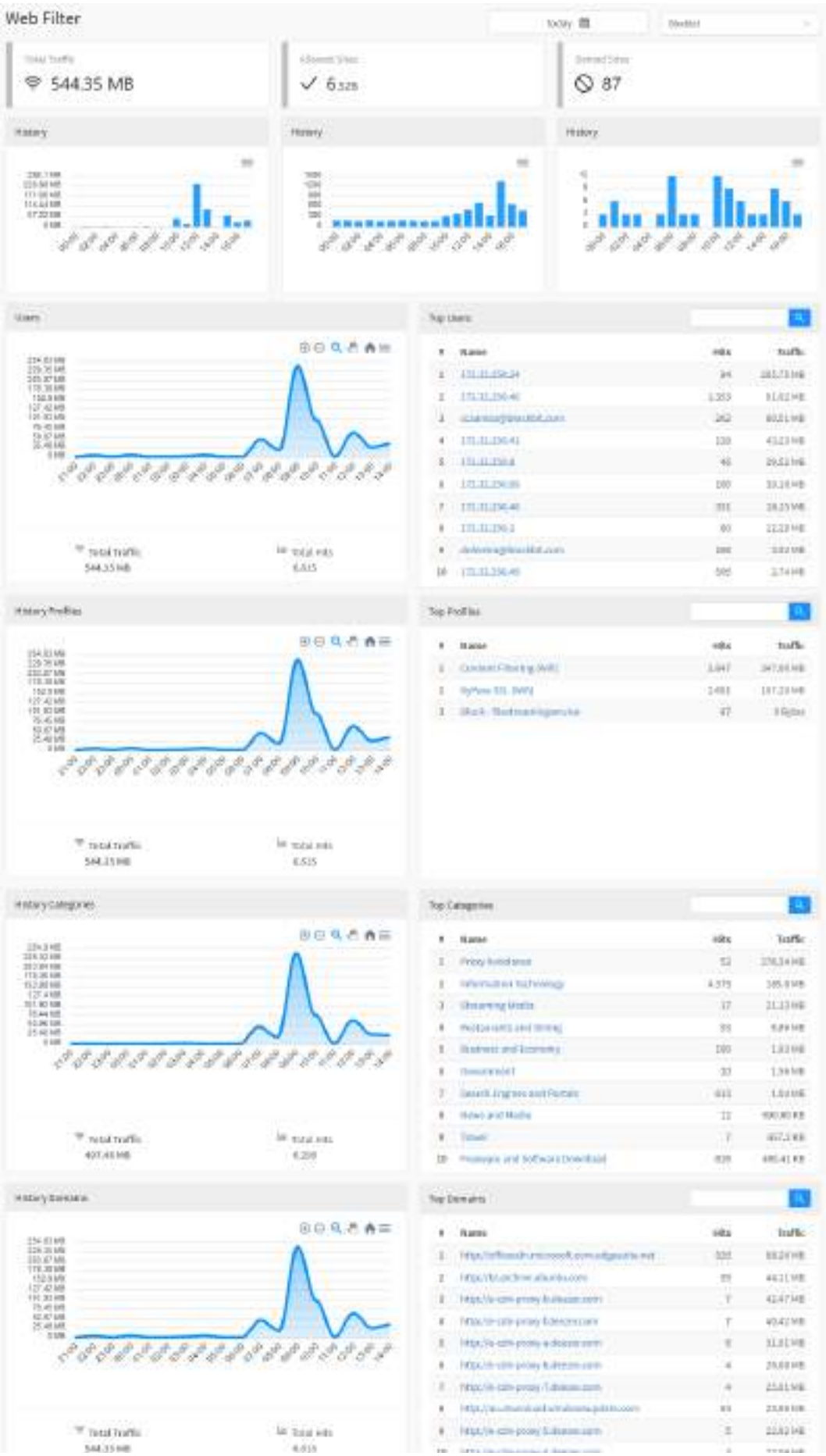
- **By date:** Determina uma data específica;
- **By period:** Exibe resultados de uma data inicial (“*Start date*”) até uma data final (“*End date*”);
- **Today:** Exibe resultados especificamente para a data de hoje;
- **Yesterday:** Exibe resultados especificamente para ontem;
- **Last 7 days:** Filtra 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.

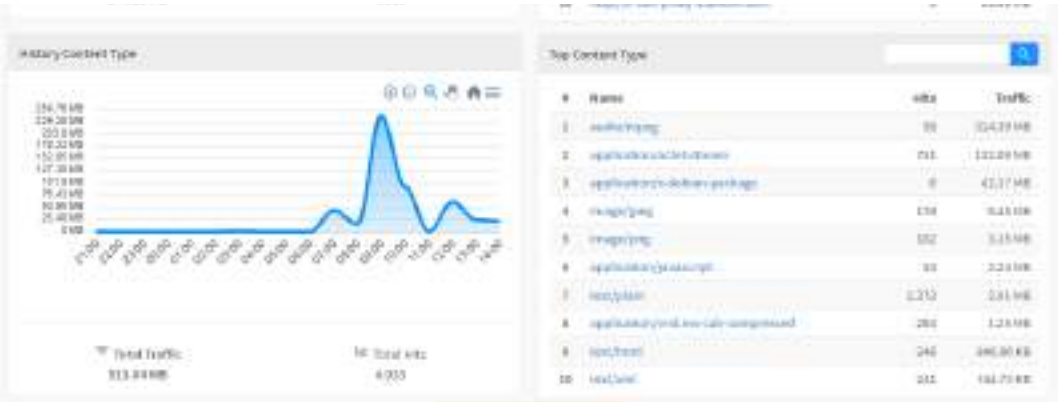
Selecione o período desejado:



Web Filter - Seleção de Data

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


Web Filter
544.35 MB
87
Top Users
Top Profiles
Top Categories
Top Domains



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;
- [ ]: Serve para fazer um zoom de seleção;
- [ ]: Serve para mover o gráfico;
- [ ]: 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 [ ]**.

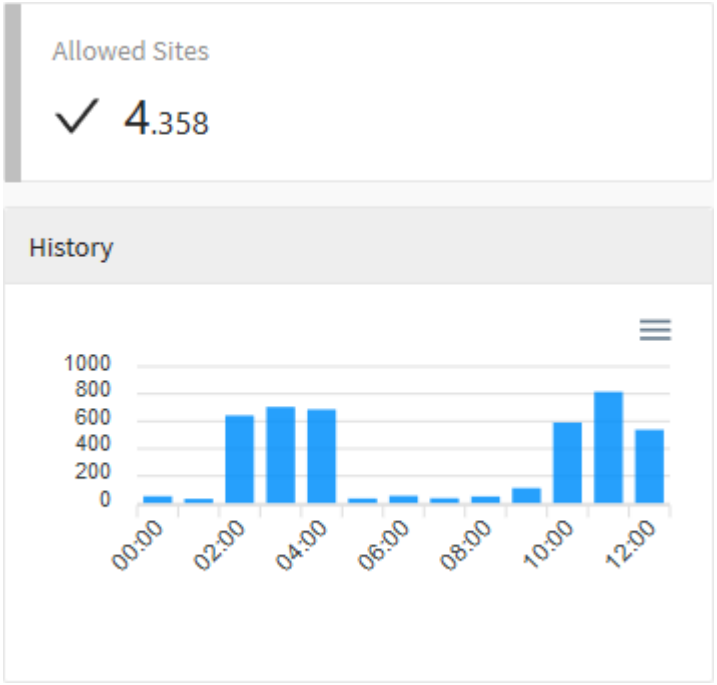
A seguir, analisaremos em detalhes os componentes de "*Web Filter*":

- *Total Traffic* e *History*;
- *Allowed Sites* e *History*;
- *Denied Sites* e *History*;
- *Users - Total Traffic* e *Total Hits*;
- *Top Users*;
- *History Profiles - Total Traffic* e *Total Hits*;
- *Top Profiles*;
- *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

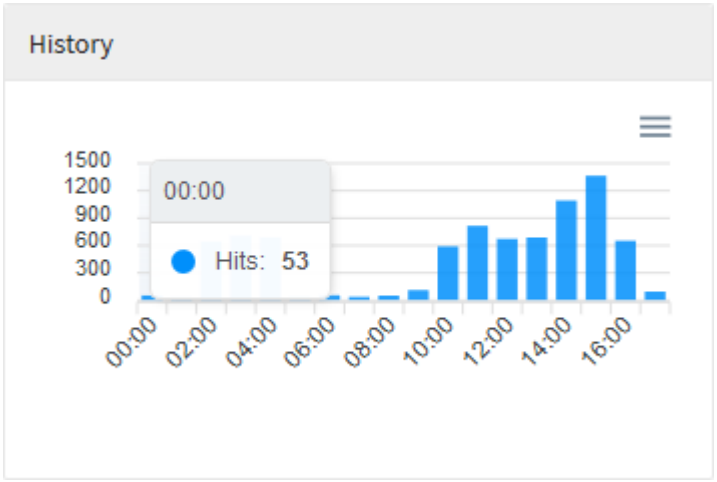
O painel “*Allowed Sites*” exibe um total de páginas que seguindo as políticas tiveram seu acesso autorizado. Logo abaixo, é mostrado o histórico em um gráfico de barras exibindo a quantia de acessos por dia.

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:

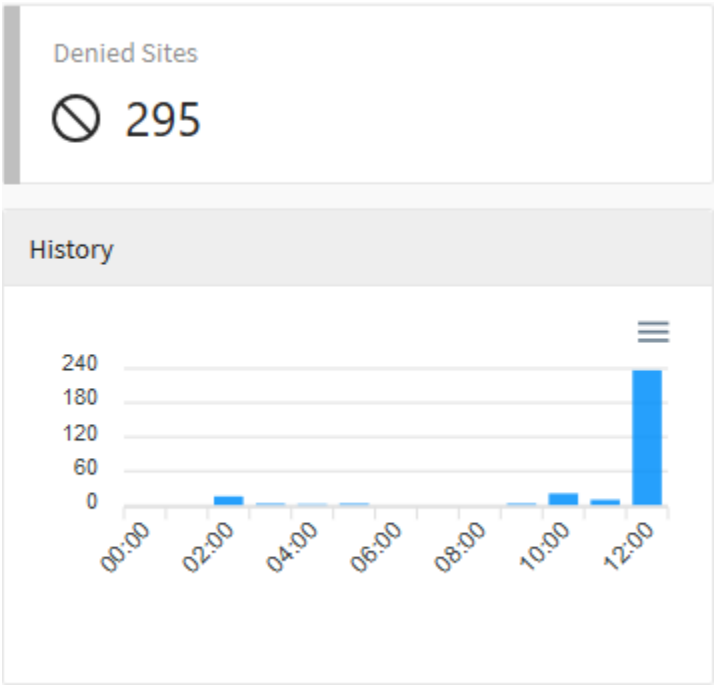


Web Filter – Allowed Sites - Resumo do Período

UTM - Web Filter - Denied Sites e History

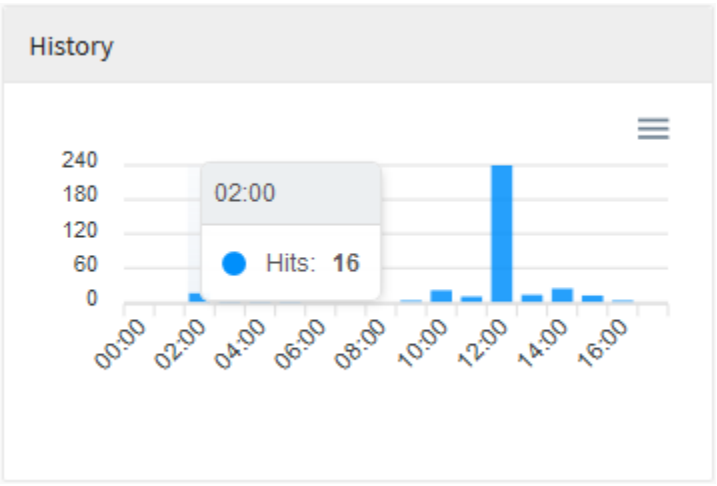
O painel “*Sites Denied*” mostra uma somatória de todas as páginas que seguindo as políticas tiveram seu acesso negado. Logo abaixo, é demonstrado o histórico em um gráfico de barras mostrando a quantia de acessos por dia.

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:

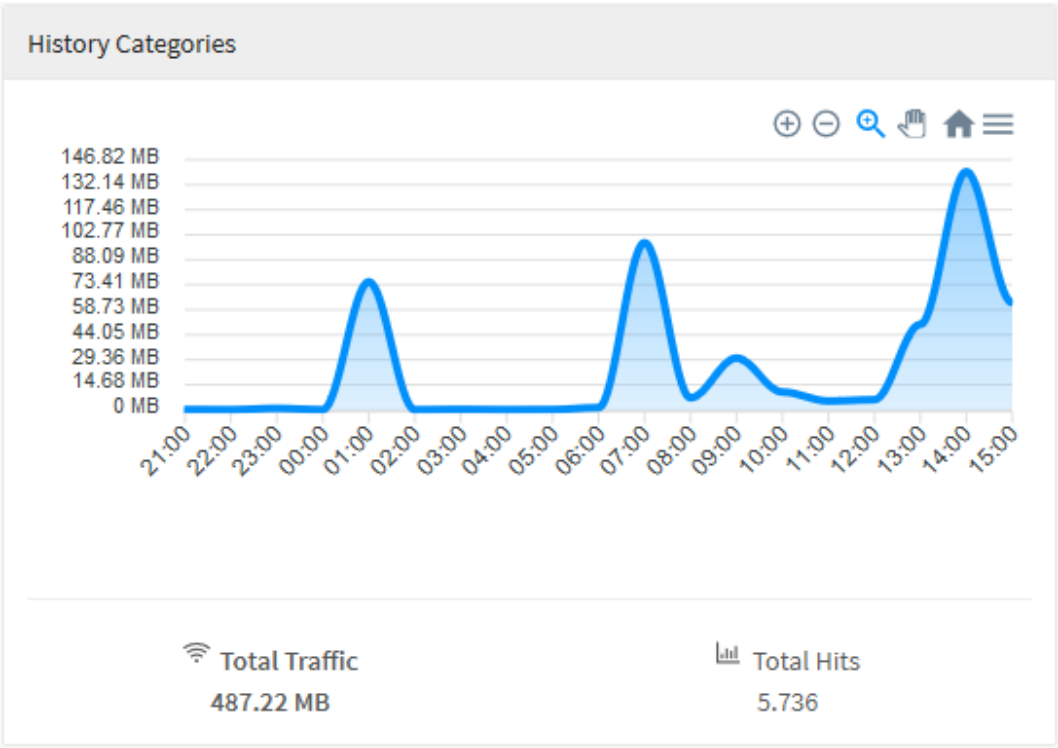


Web Filter – Denied Sites - Resumo do Período

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

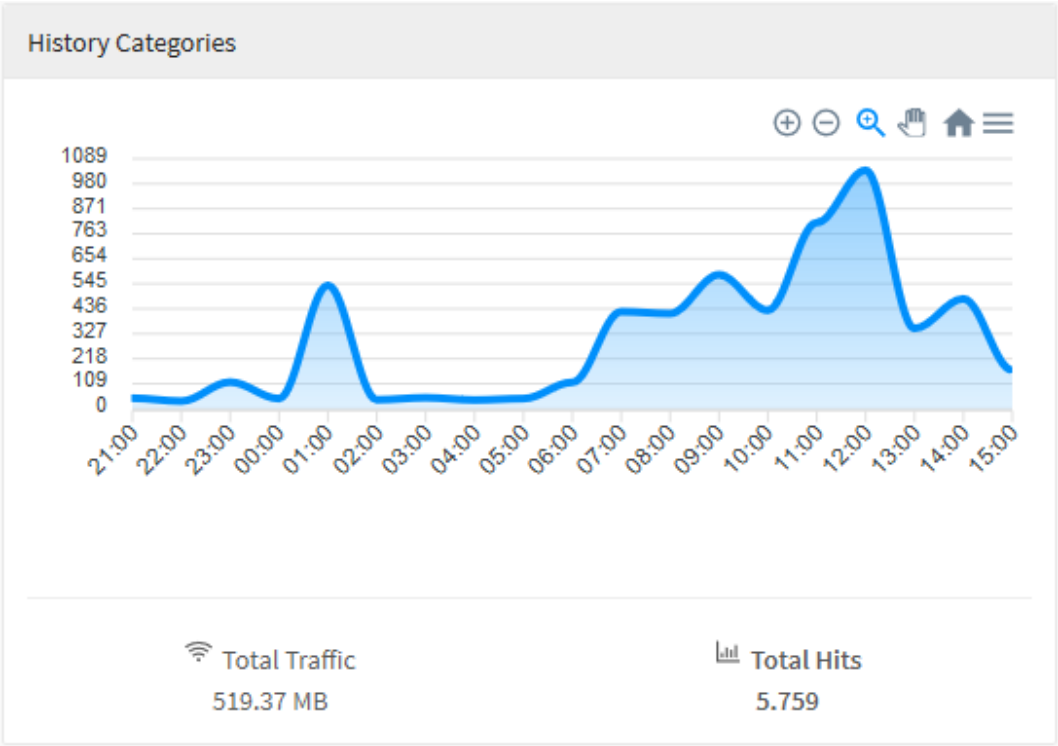
Em “*History Categories*”, temos um gráfico que exibe informações especificamente relacionadas as categorias de rede, sua função é demonstrar quando alguma categoria foi aplicada em um dos acessos. Nessa área temos “*Total Traffic*” onde é exibido o total de tráfego de rede em *Gigabytes* por dia e “*Total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



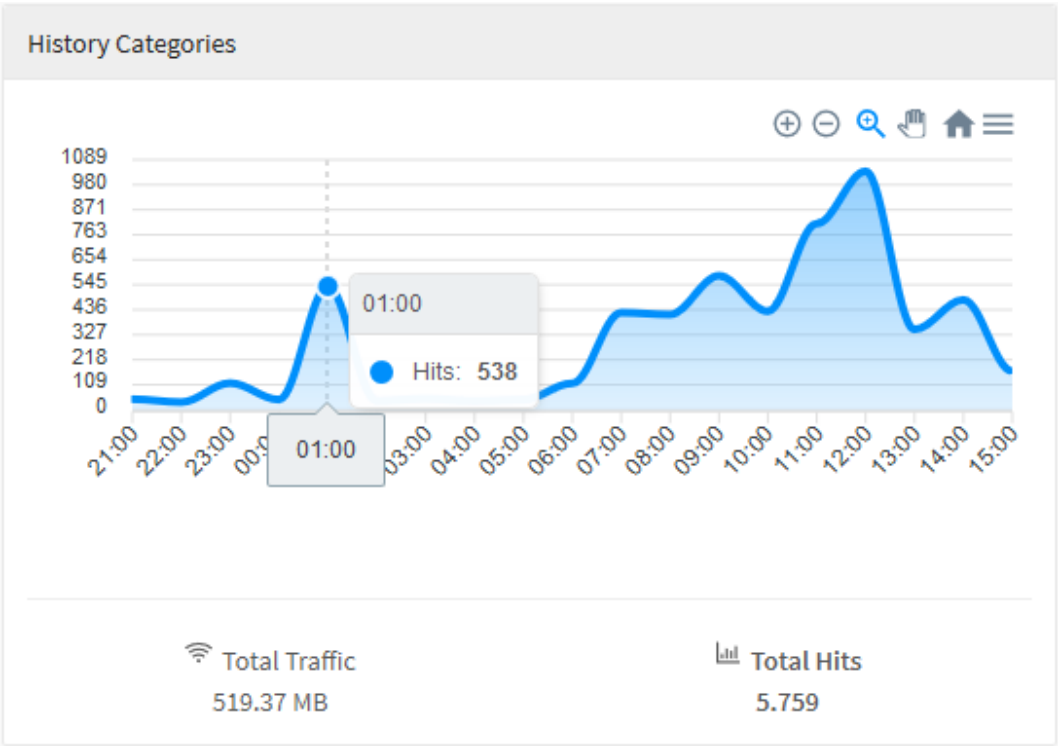
Web Filter – History Categories – Total Traffic

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:

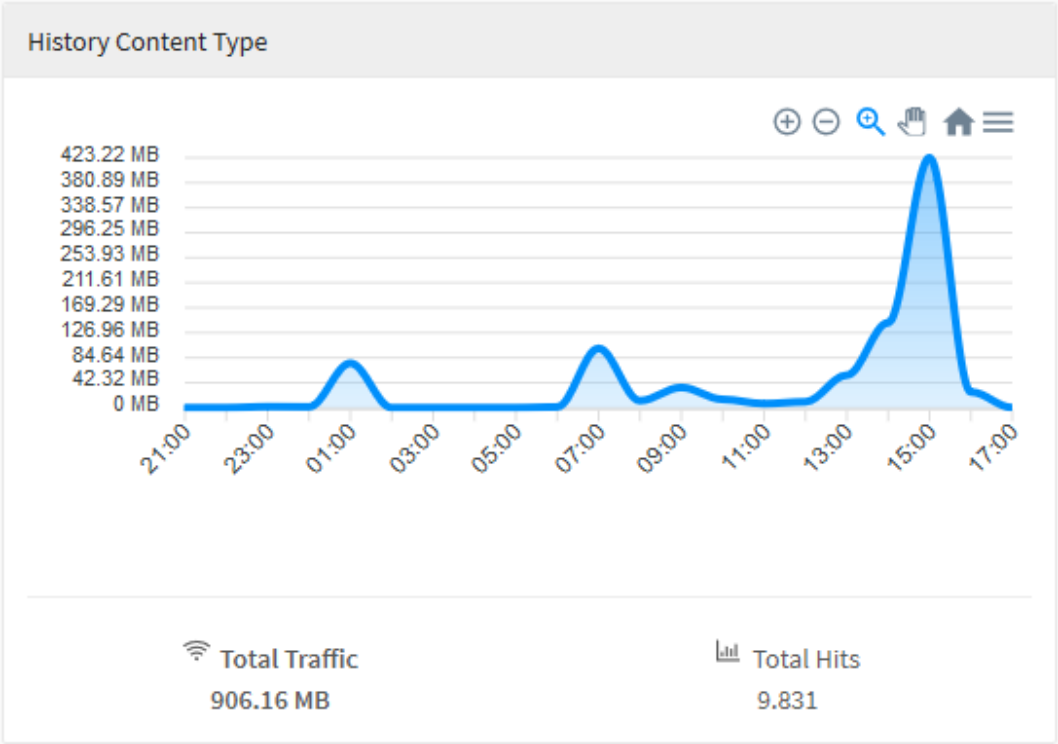


Web Filter – History Categories – Resumo do período

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

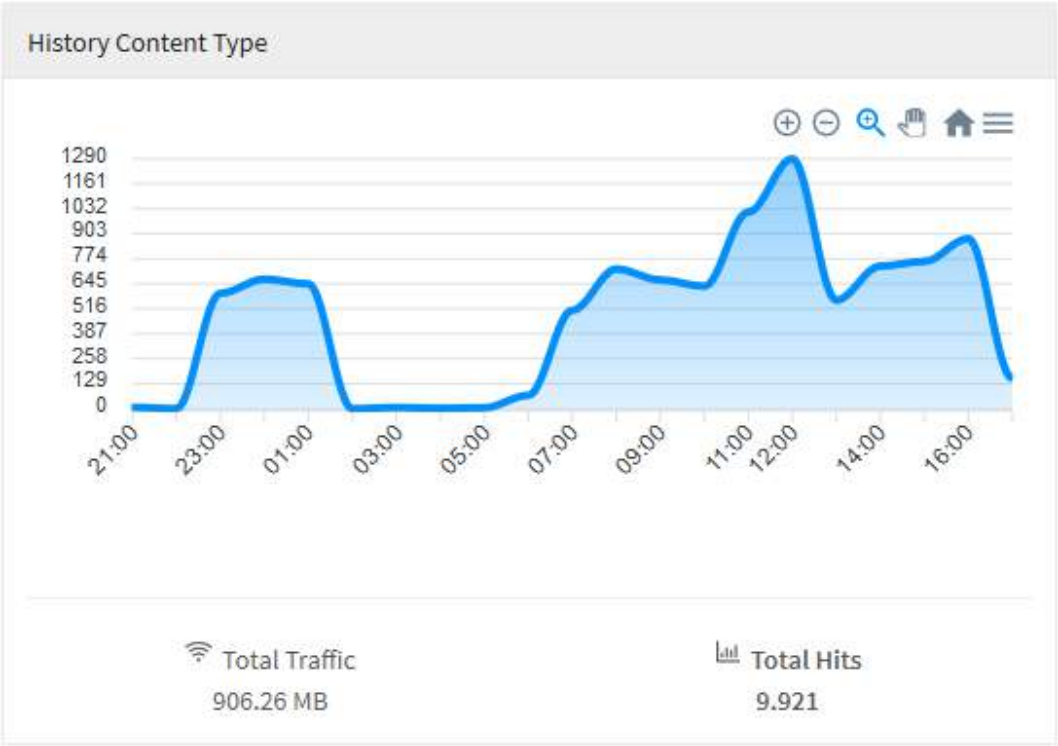
Em “*Content Type*”, temos um gráfico cuja função é demonstrar quando algum tipo de conteúdo foi acessado. Nessa área temos “*Total Traffic*” onde é exibido o total de tráfego de rede em *Gigabytes* por dia e “*Total Hits*” que demonstra o total de acessos para cada um dos dias pesquisados.

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



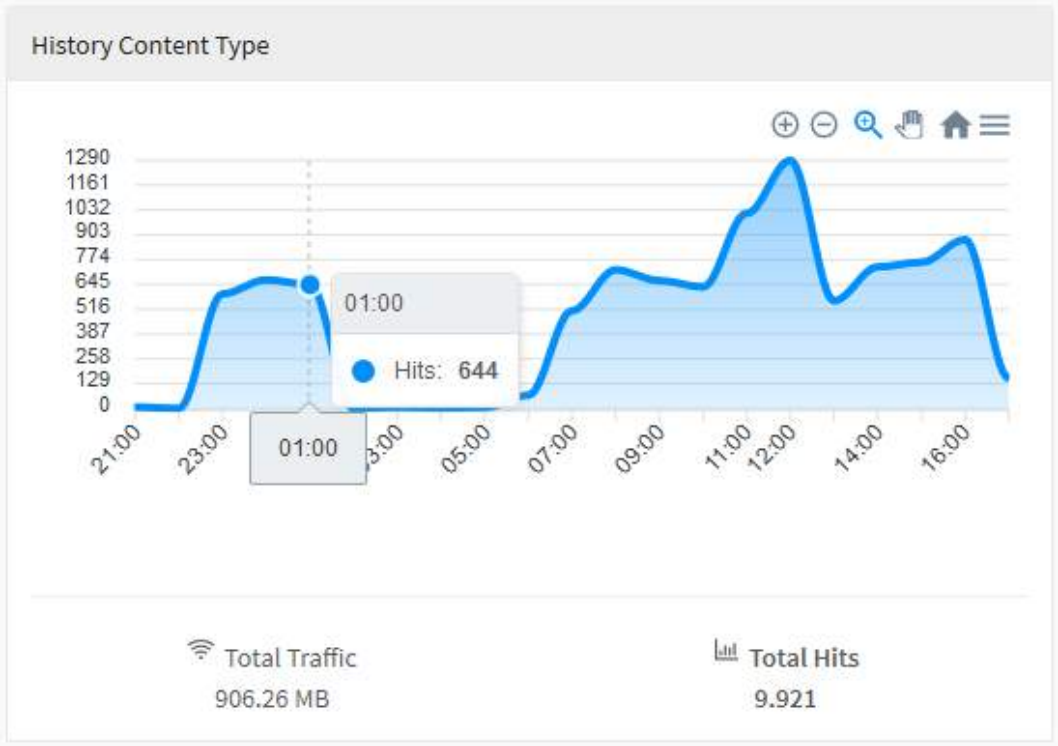
Web Filter – History Content Type – Total Traffic

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:

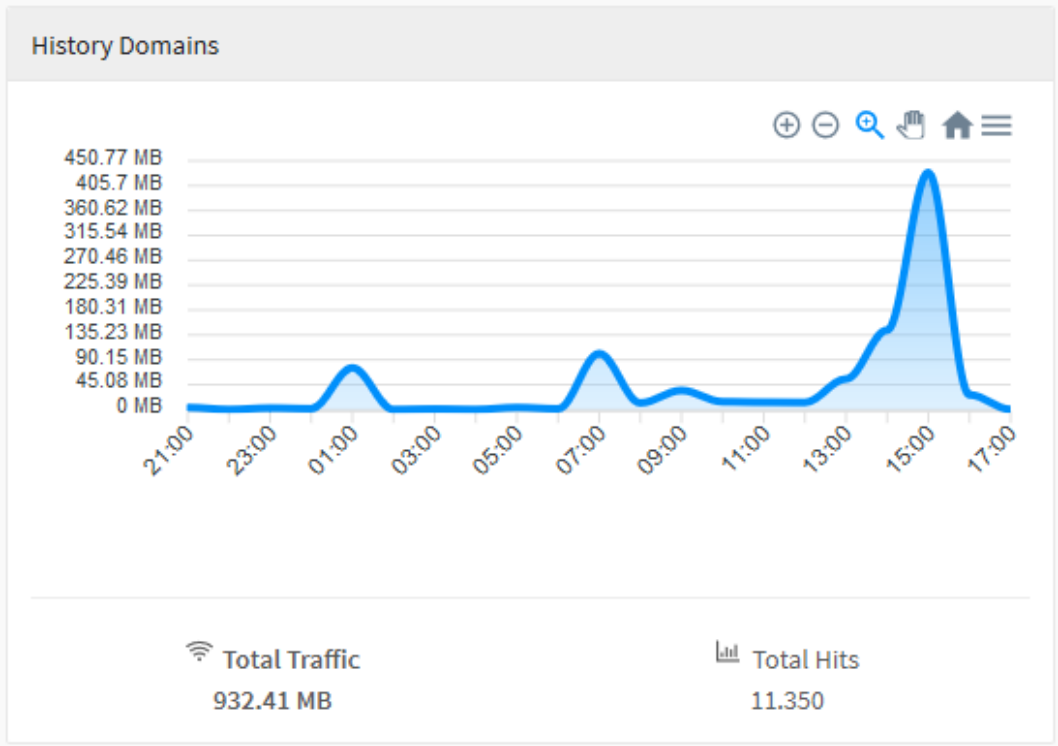


Web Filter – History Content Type - Resumo do Período

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

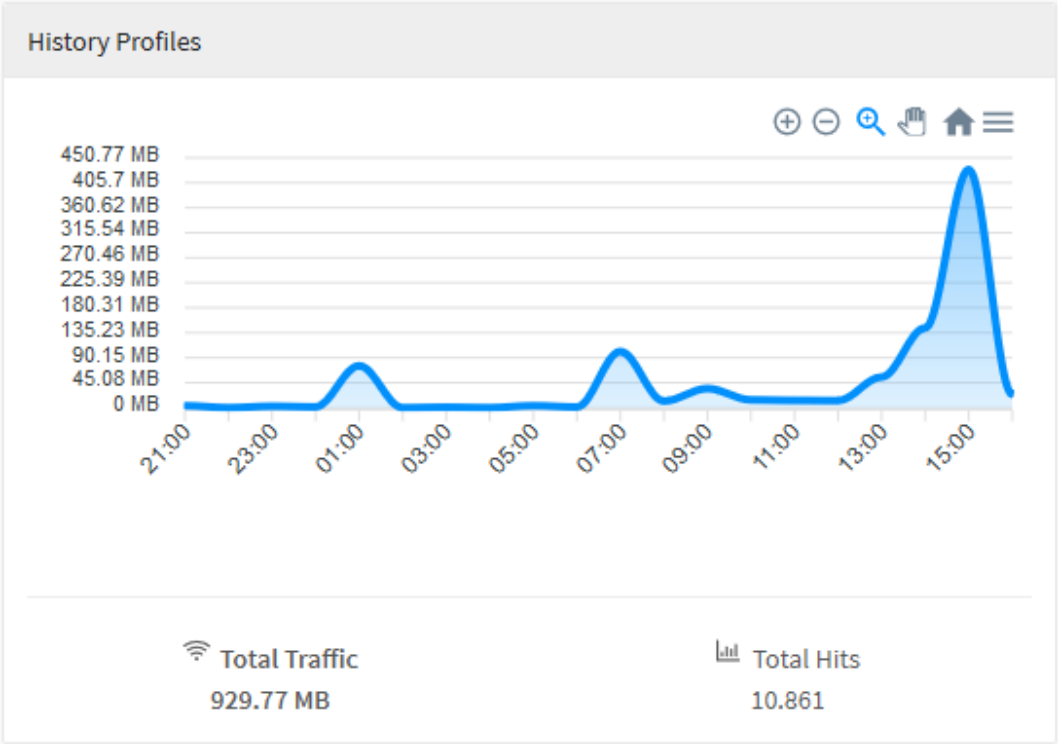
Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

Web Filter - History Domains - Resumo do Período

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

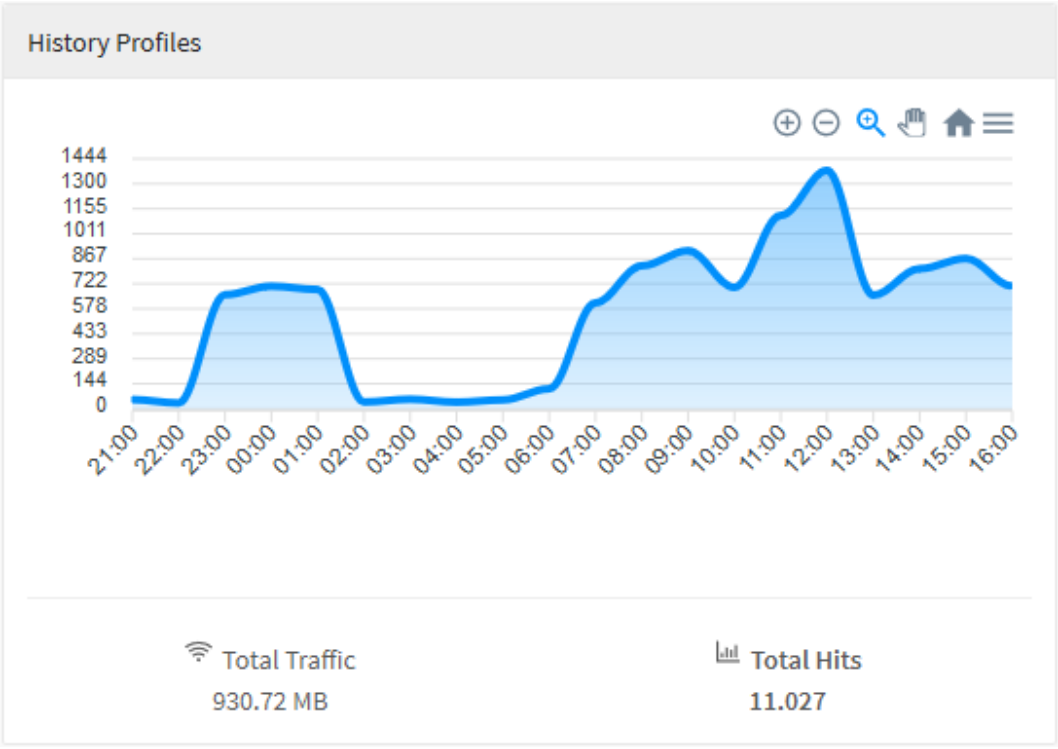
Em “*History Profiles*”, temos um gráfico que exibe informações especificamente relacionadas aos *profiles* da rede, sua função é demonstrar quando algum profile foi utilizado em um acesso. Nessa área temos “*Total Traffic*” onde é exibido o total de tráfego de rede em *Gigabytes* por dia e “*Total Hits*” 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

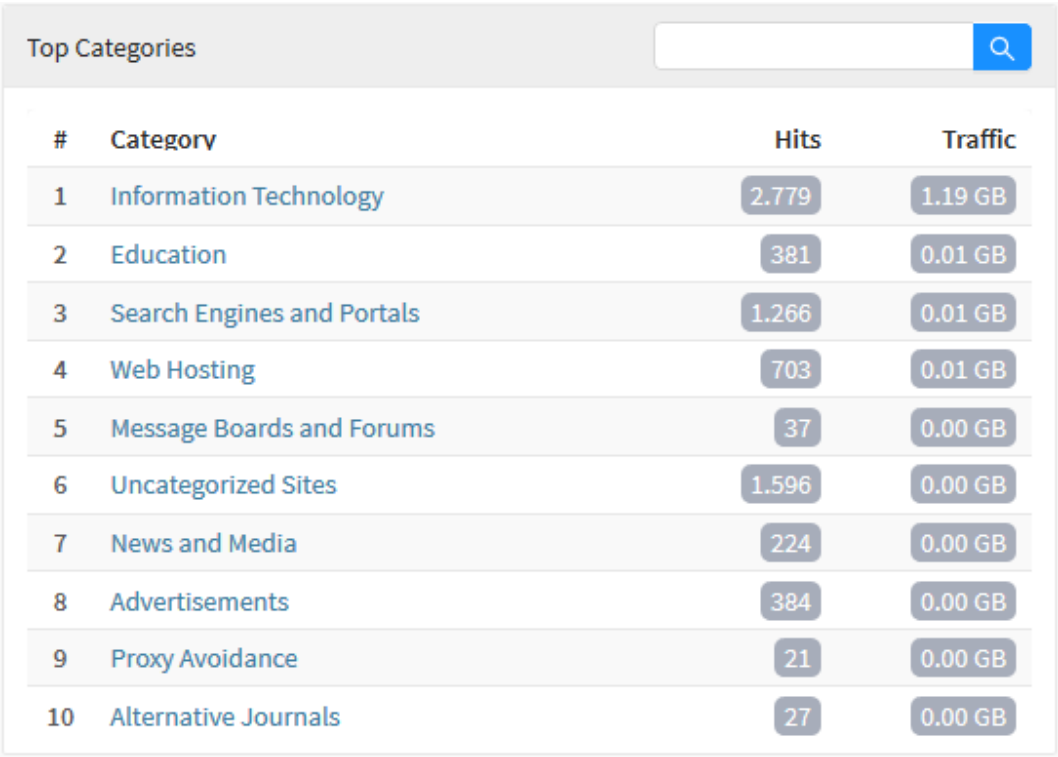
Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:

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.



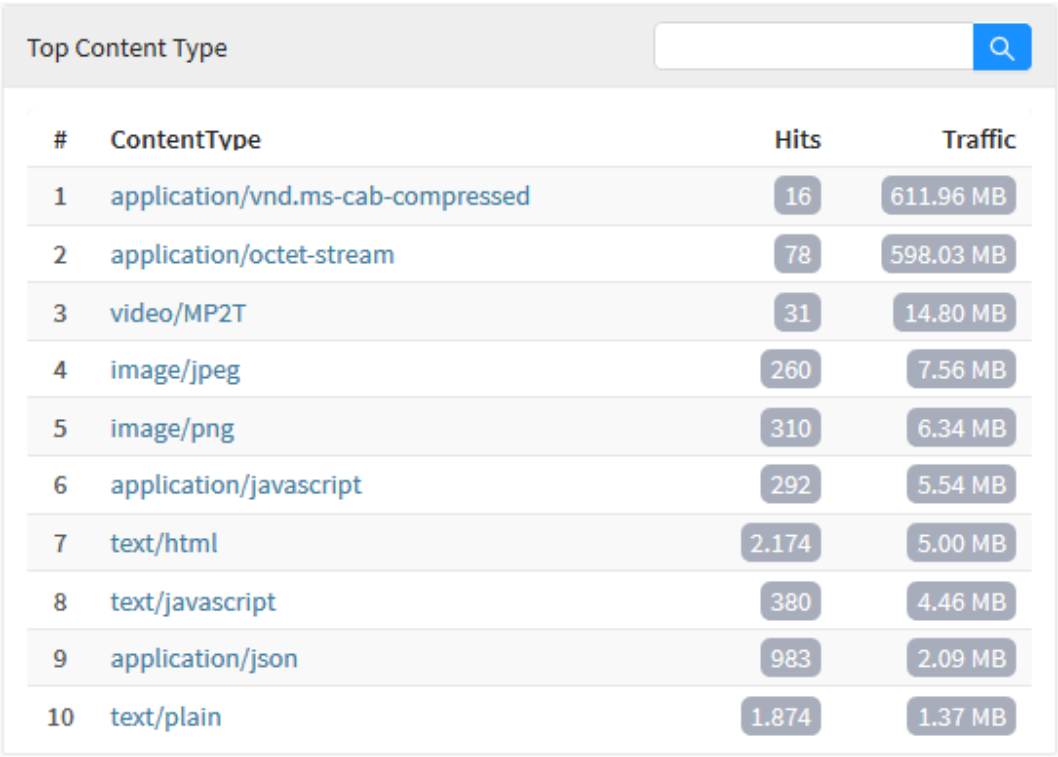
#	Category	Hits	Traffic
1	Information Technology	2.779	1.19 GB
2	Education	381	0.01 GB
3	Search Engines and Portals	1.266	0.01 GB
4	Web Hosting	703	0.01 GB
5	Message Boards and Forums	37	0.00 GB
6	Uncategorized Sites	1.596	0.00 GB
7	News and Media	224	0.00 GB
8	Advertisements	384	0.00 GB
9	Proxy Avoidance	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.



#	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.

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

Top Content Type

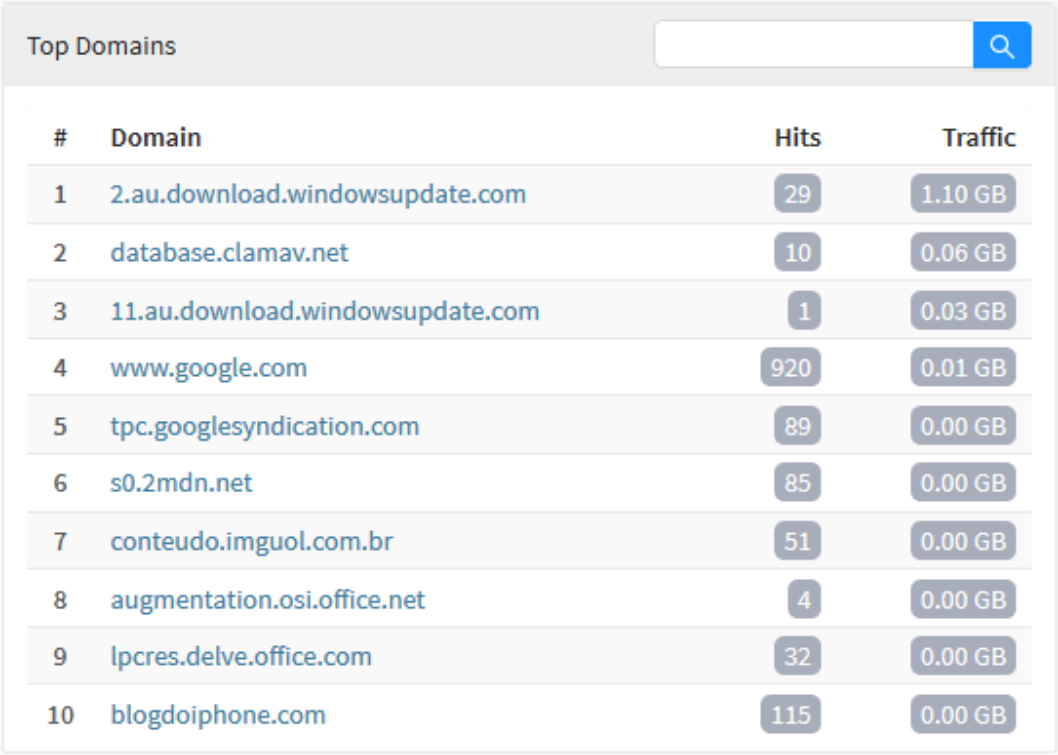
#	ContentType	Hits	Traffic
1	application/vnd.ms-cab-compressed	16	611.96 MB
2	application/octet-stream	78	598.03 MB
3	video/MP2T	31	14.80 MB
4	image/jpeg	260	7.56 MB
5	image/png	310	6.34 MB
6	application/javascript	292	5.54 MB
7	text/html	2.174	5.00 MB
8	text/javascript	380	4.46 MB
9	application/json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

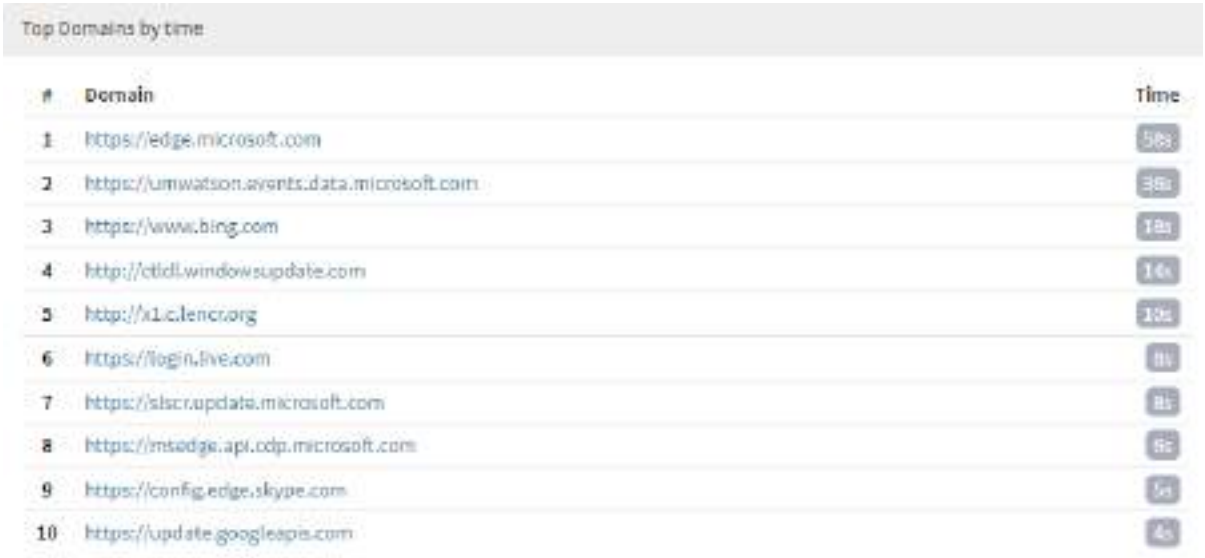


#	Domain	Hits	Traffic
1	2.au.download.windowsupdate.com	29	1.10 GB
2	database.clamav.net	10	0.06 GB
3	11.au.download.windowsupdate.com	1	0.03 GB
4	www.google.com	920	0.01 GB
5	tpc.googlesyndication.com	89	0.00 GB
6	s0.2mdn.net	85	0.00 GB
7	conteudo.imguol.com.br	51	0.00 GB
8	augmentation.osi.office.net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

Web Filter – Top Domains

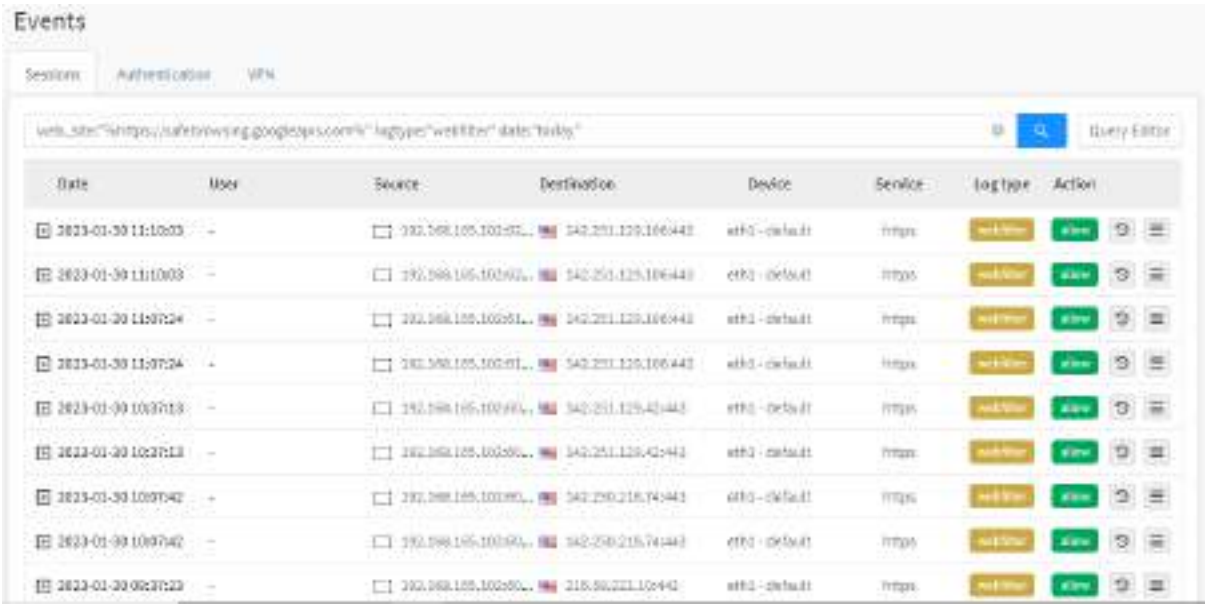
UTM - Web Filter - Top Domains by Time

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



Top Domains by Time

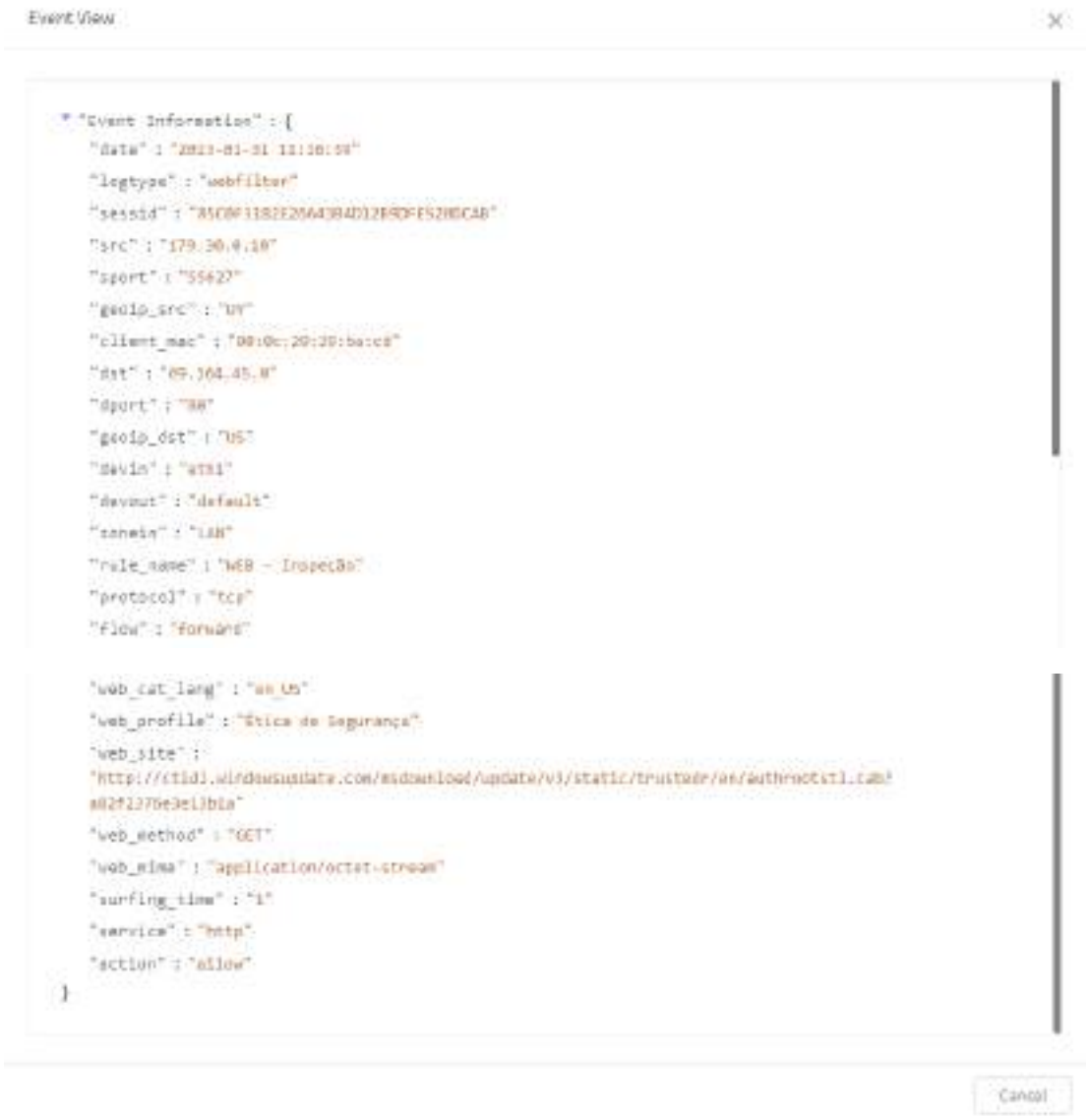
Por fim, ao clicar em um desses domínios ou IPs, você será redirecionado para Events usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito desses tipos de conteúdo.



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.

Events - Sessions - [ ] Information



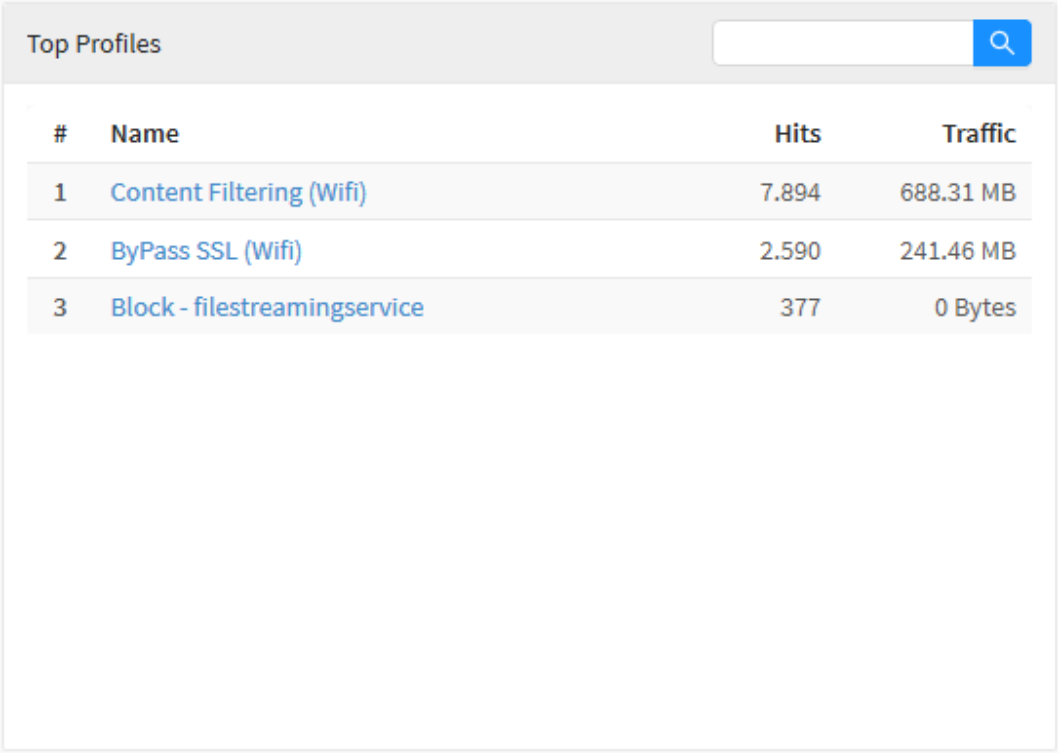
Events - Sessions - [] Event View

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.

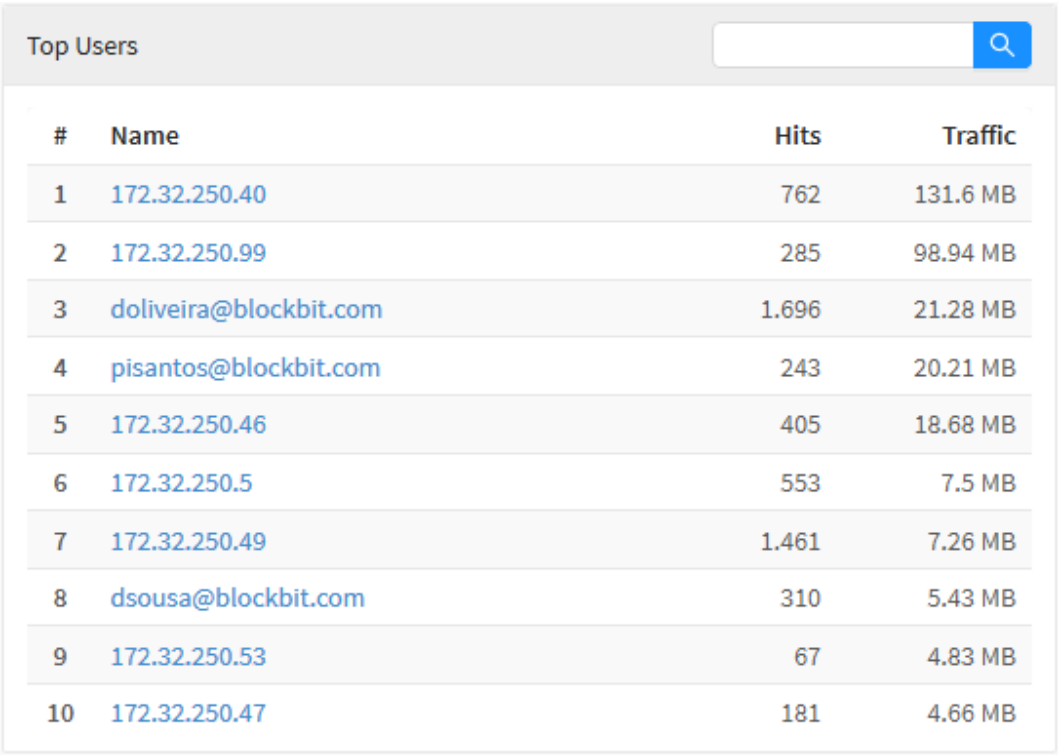


Web Filter – Top Profiles

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.

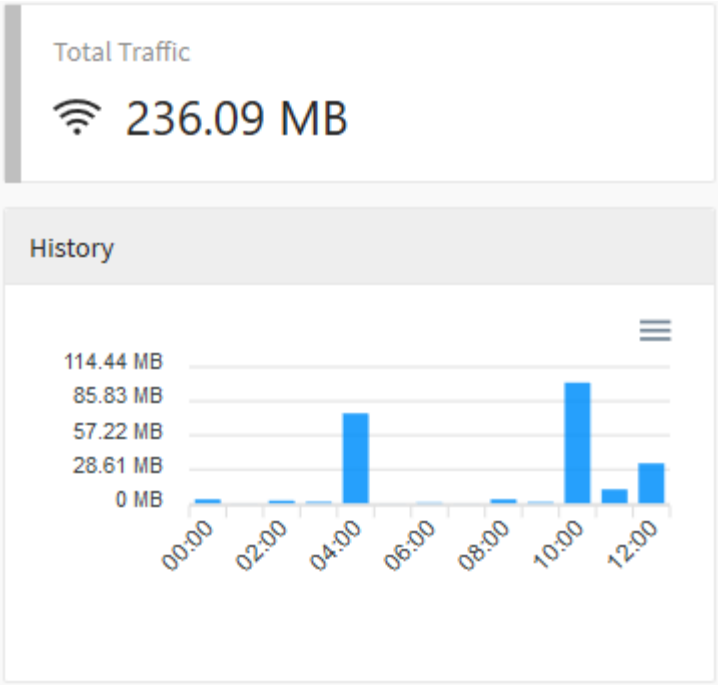


#	Name	Hits	Traffic
1	172.32.250.40	762	131.6 MB
2	172.32.250.99	285	98.94 MB
3	doliveira@blockbit.com	1.696	21.28 MB
4	pisantos@blockbit.com	243	20.21 MB
5	172.32.250.46	405	18.68 MB
6	172.32.250.5	553	7.5 MB
7	172.32.250.49	1.461	7.26 MB
8	dsousa@blockbit.com	310	5.43 MB
9	172.32.250.53	67	4.83 MB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

Web Filter – Top Users

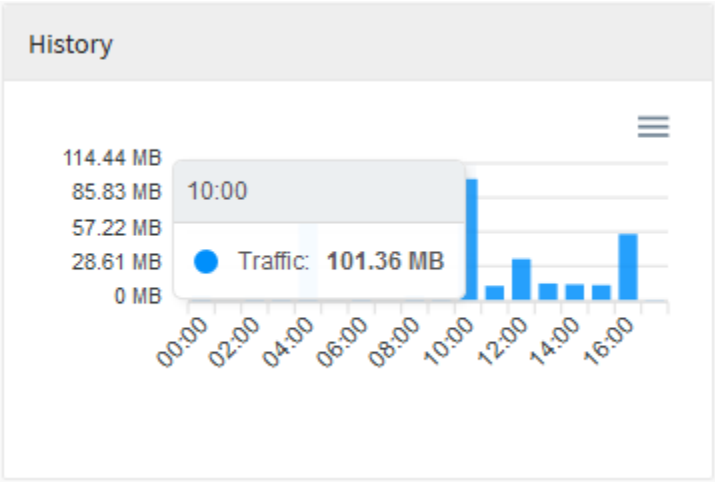
UTM - Web Filter - Total Traffic e History

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



Web Filter – Total Traffic

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

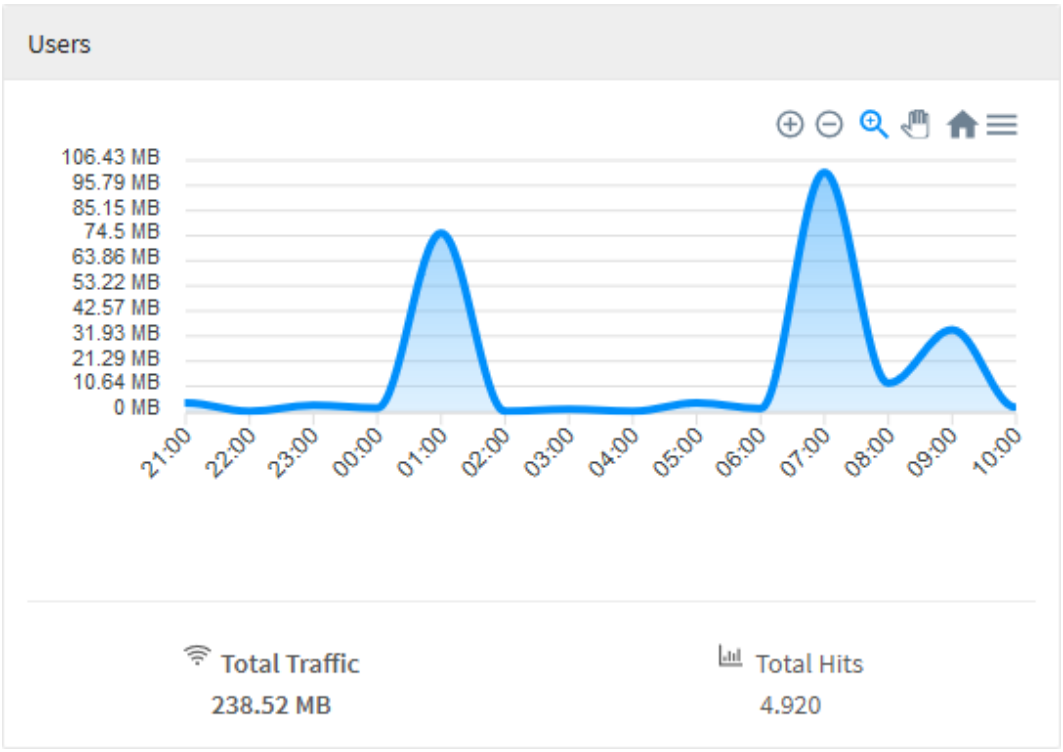


Web Filter – Total Traffic - Resumo do período

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

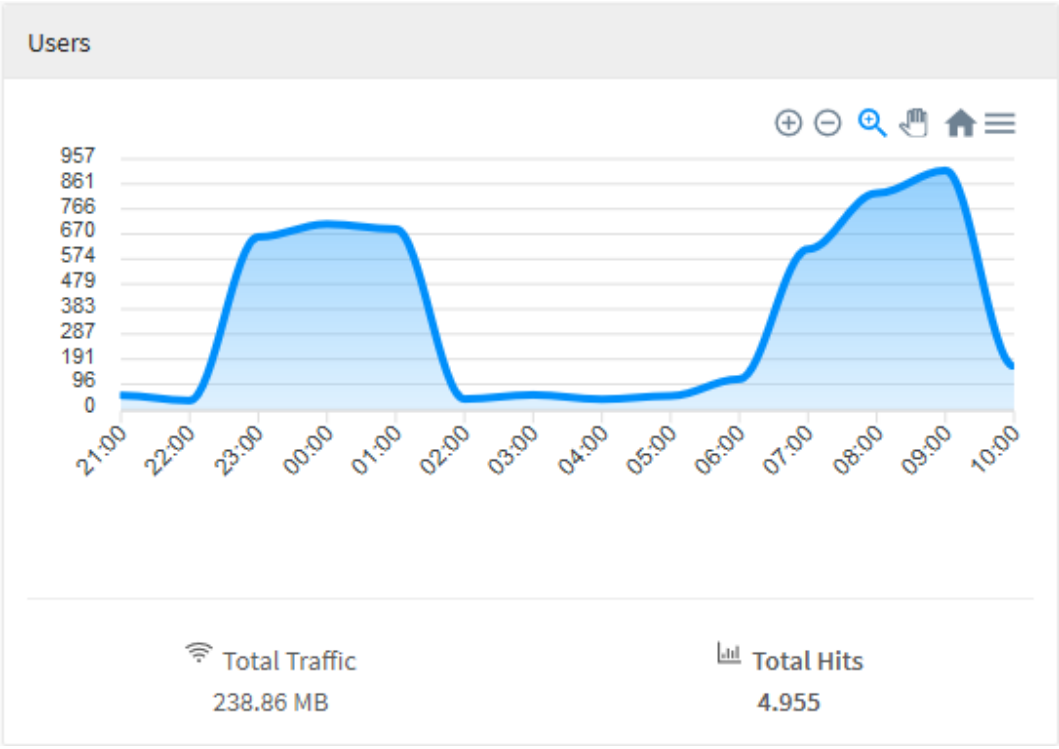
Logo abaixo dos painéis anteriormente descritos, no lado esquerdo da tela temos o gráfico disposto em “*Users*”, que exibe informações especificamente relacionadas ao consumo de rede por parte dos usuários: Nele temos “*Total Traffic*” onde é exibido o total de tráfego de rede em *Megabytes* por dia 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.



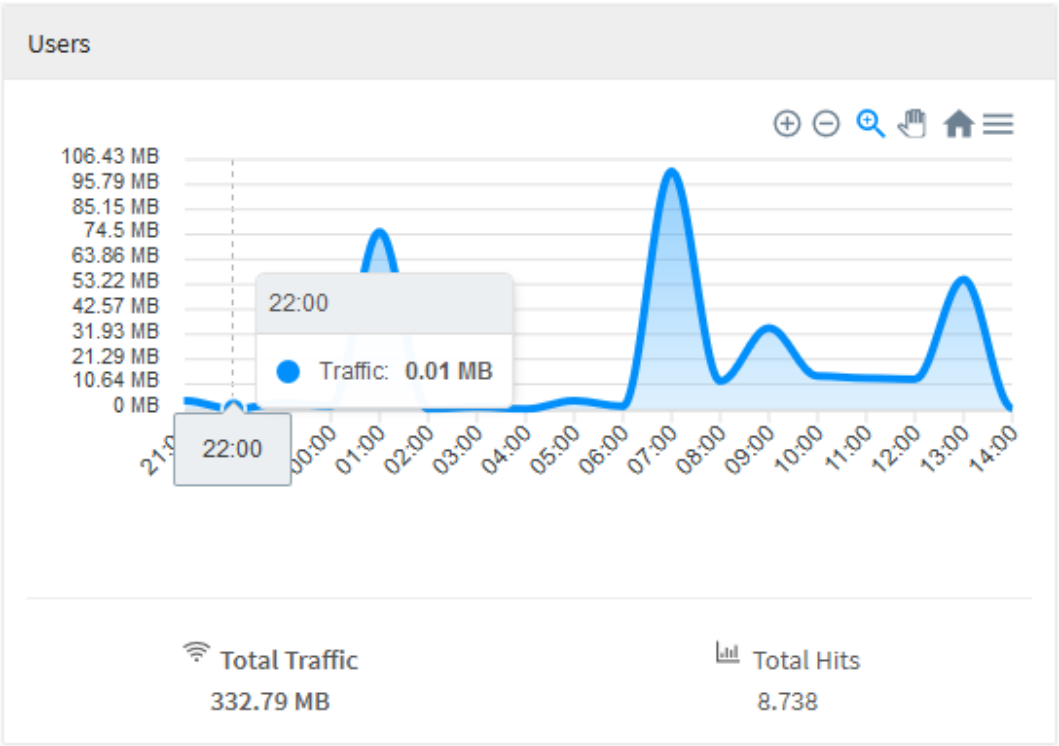
Web Filter – Users – Total Traffic

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

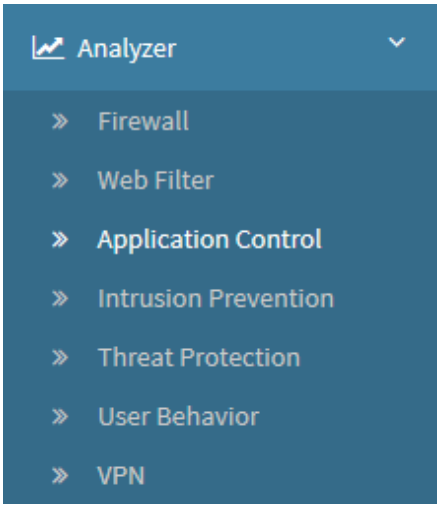
Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



Web Filter – Users – Total Traffic - Resumo do Período

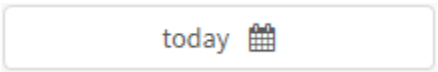
UTM - Application Control

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:

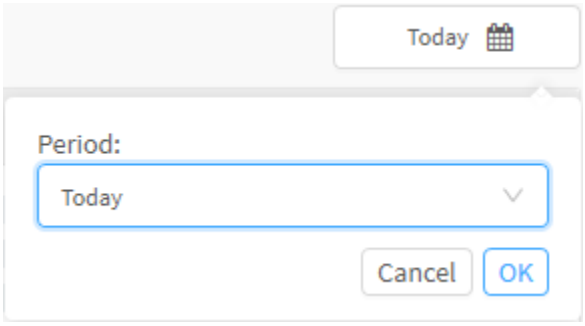


Application Control - Caixa de seleção de data

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:



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 - Application Control

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;

- **[ ]:** 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.

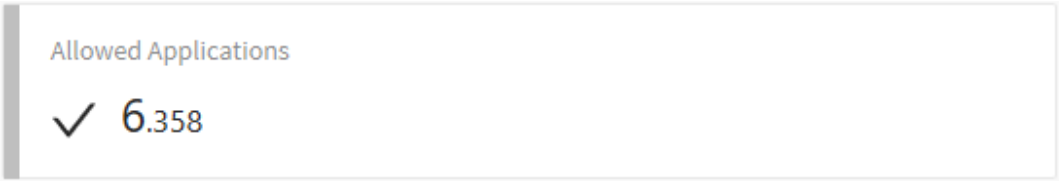
Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca [ ]**.

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

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

UTM - Application Control - Allowed Application

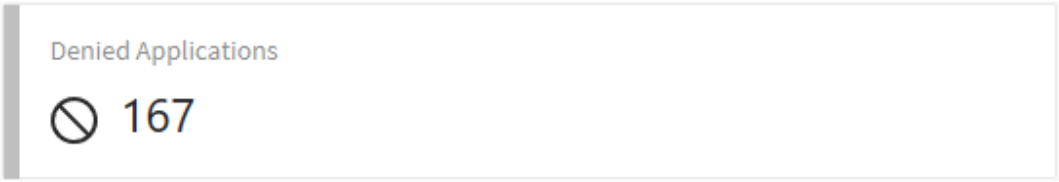
Em “*Allowed Application*” é exibe um total de aplicações que tiveram seu acesso autorizado.



Application Control – Allowed Application

UTM - Application Control - Denied Application

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

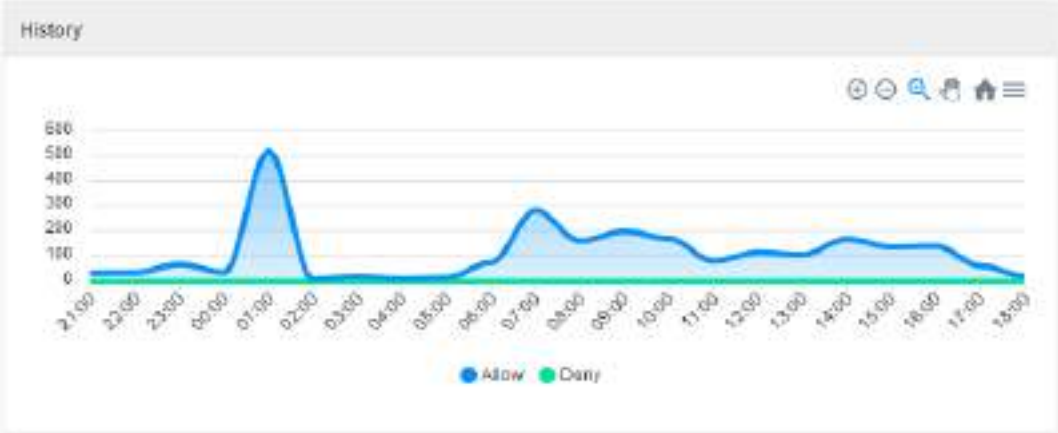


Application Control – Denied Application

UTM - Application Control - History

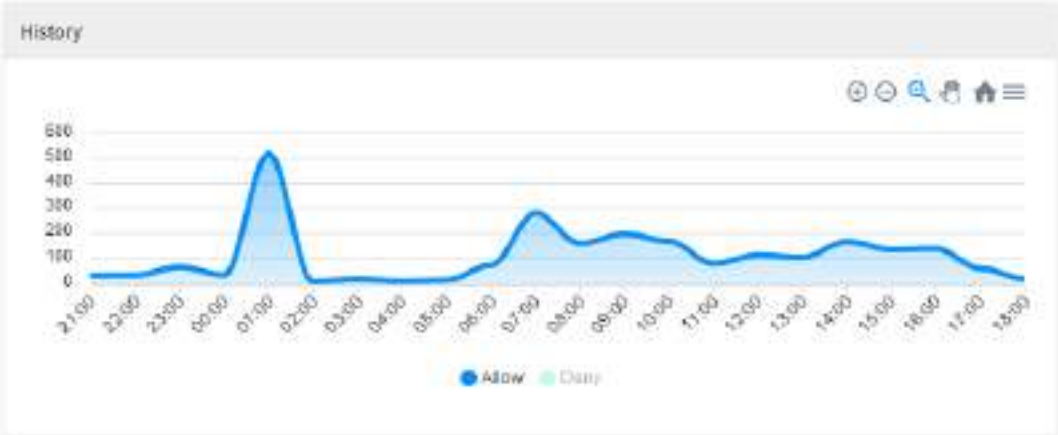
Ao lado direito é possível visualizar o gráfico “*History*” que exibe um histórico de todas as aplicações que tiveram seu acesso permitido e negado, tendo como referências para seus eixos a quantia de acessos em relação com as datas previamente pesquisadas. Os itens da legenda são interativos sendo possível 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.



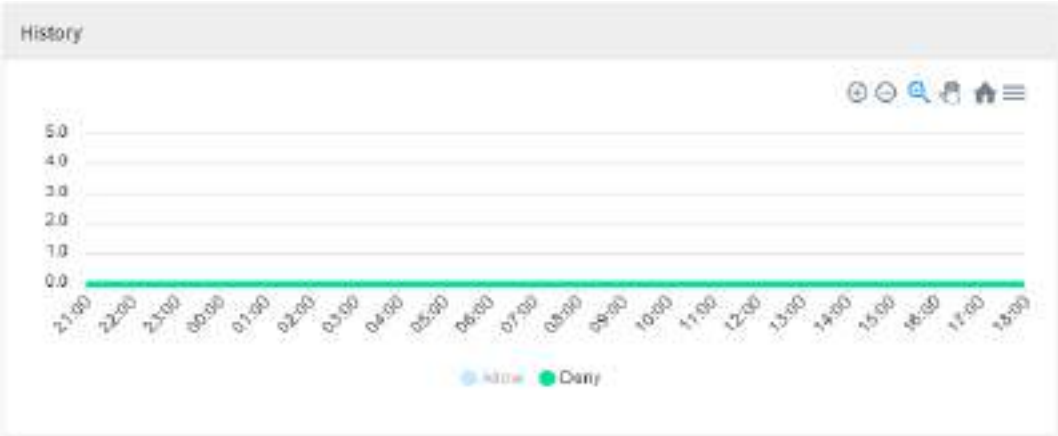
Application Control – History

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

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

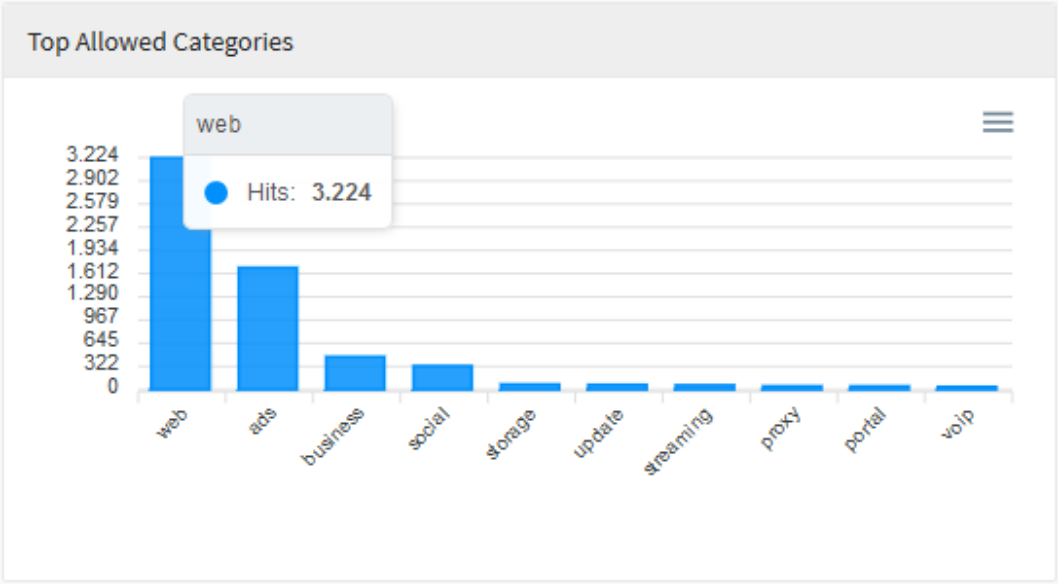
Application Control – History - Resumo do Período

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.



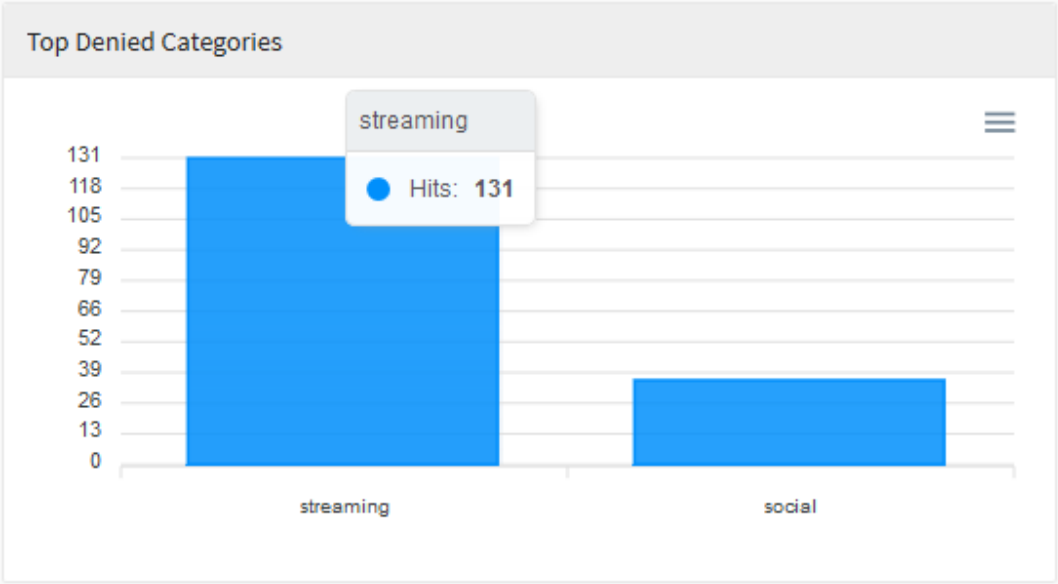
Application Control – Top Allowed Categories

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.



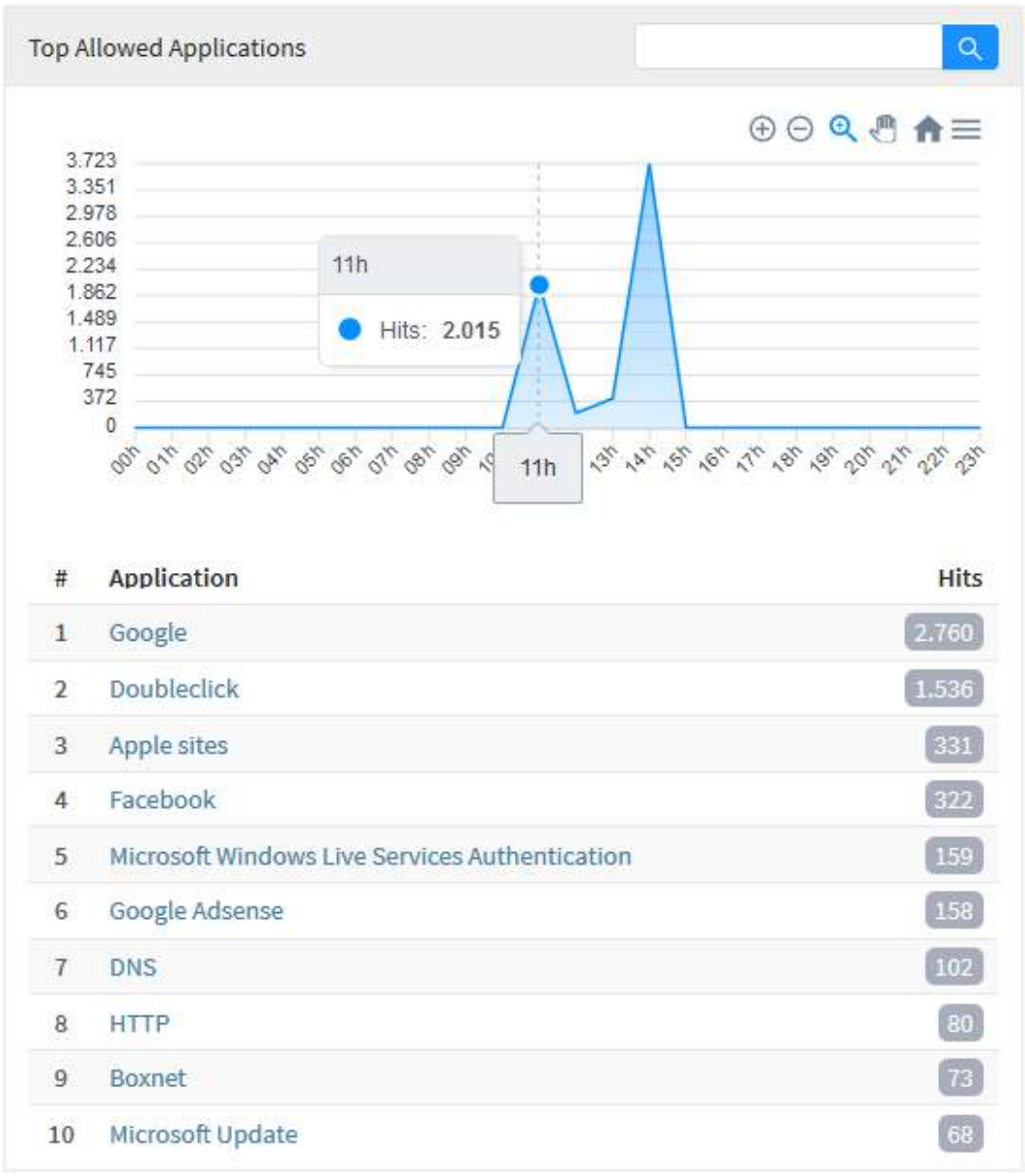
Application Control – Top Denied Categories

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.



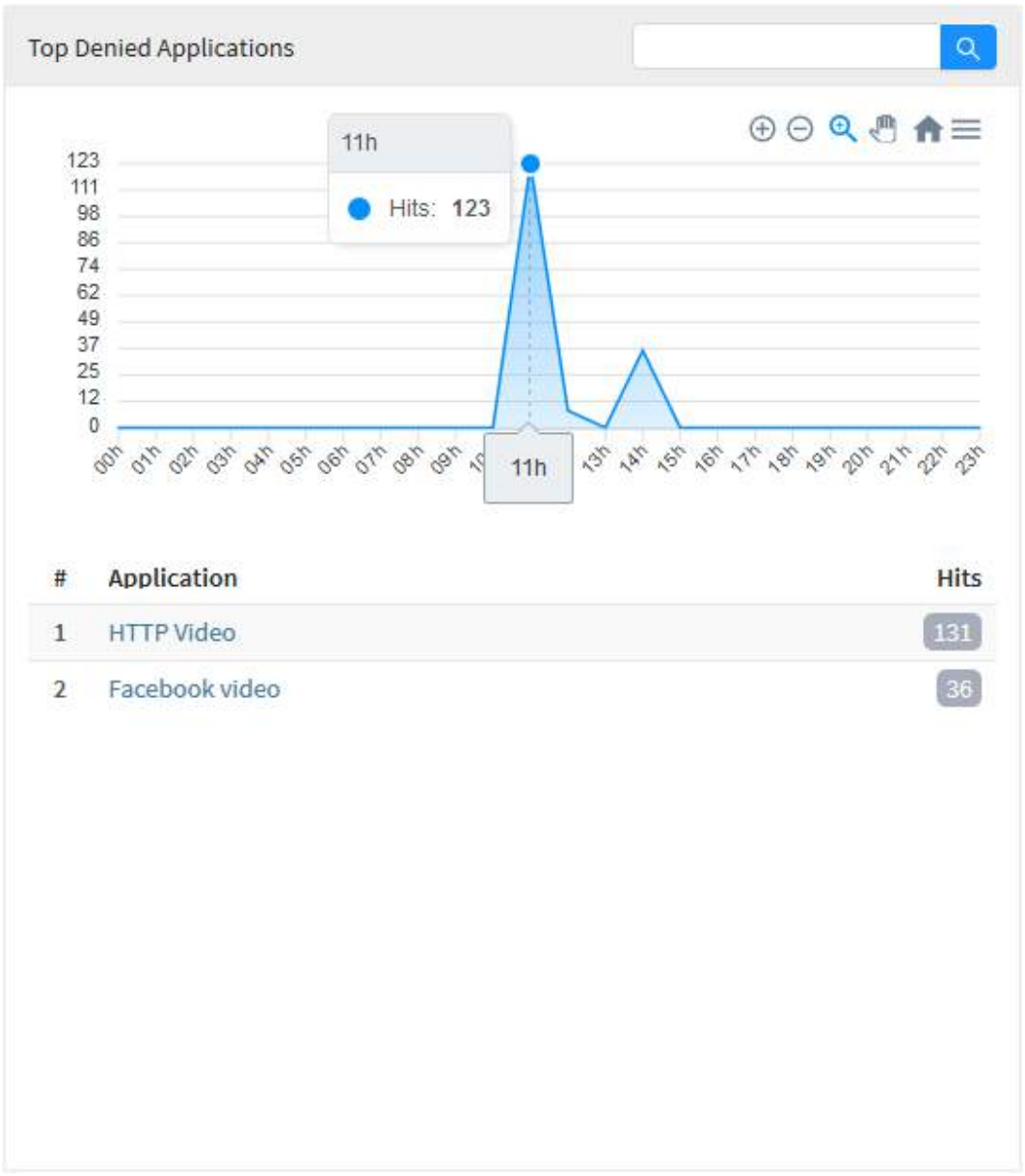
Application Control – Top Allowed Applications

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.

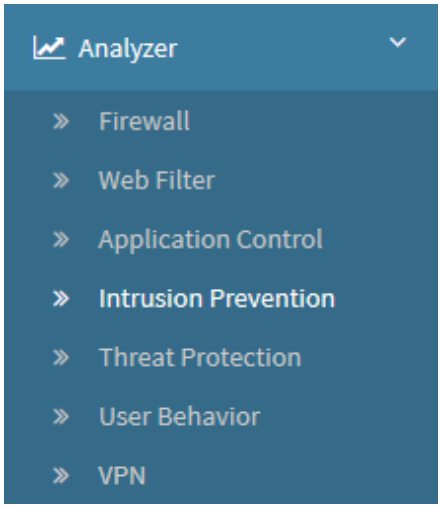
Para mais informações a respeito do menu de navegação e da barra de busca presente no topo deste gráfico cheque esta página.



Application Control – Top Denied Applications

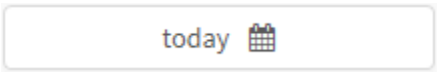
UTM - Intrusion Prevention

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:

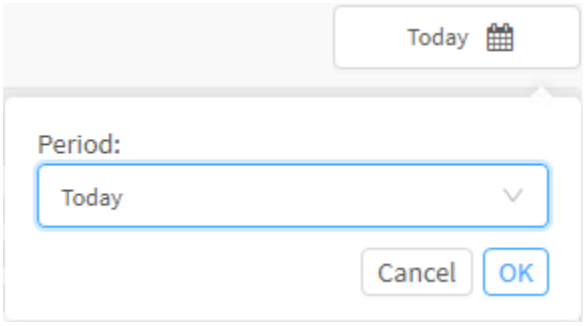


Intrusion Prevention - Caixa de Seleção

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:

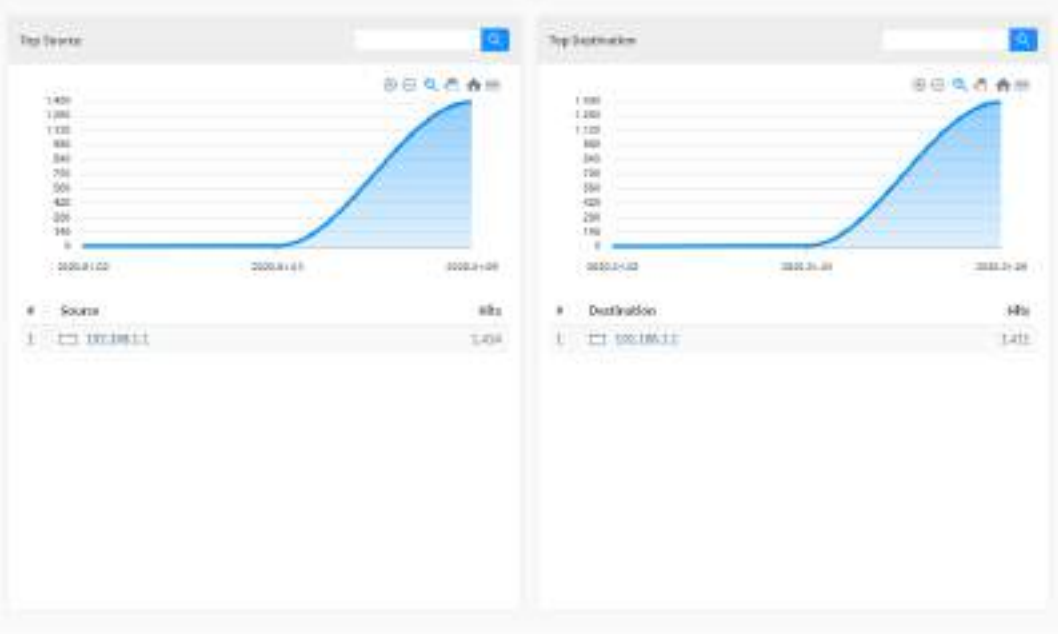


Intrusion Prevention - Seleção de Data

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

A tela abaixo será exibida:


Intrusion Prevention
12
7,000
Geolocation
History
Impact - High
Impact - Medium
Impact - Low
Layer 3 Intrusion Prevention
Intrusion Classification



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;
- **[ ]:** 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*;
- *Intrusion Classification*;
- *Top Source*;
- *Top Destination*.

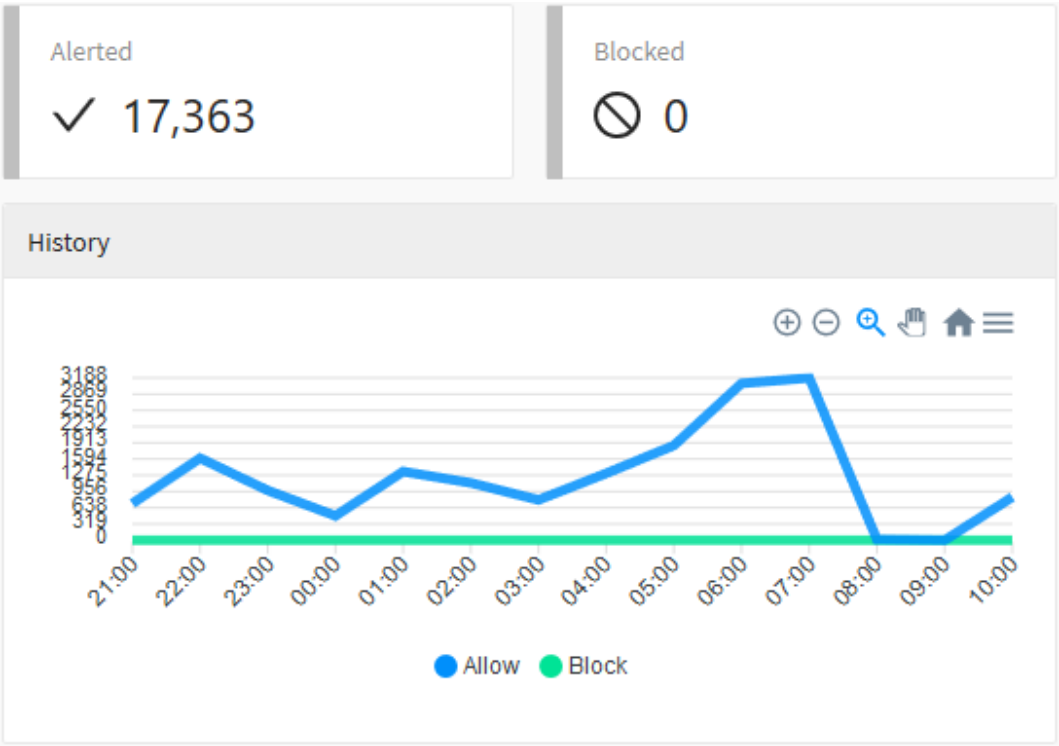
UTM - Intrusion Prevention - Alerted, Blocked e Histórico

O painel “*Alerted*” exibe um total de alertas de intrusão.

Já em “*Blocked*”, é exibido um número totalizando as tentativas de intrusão bloqueadas.

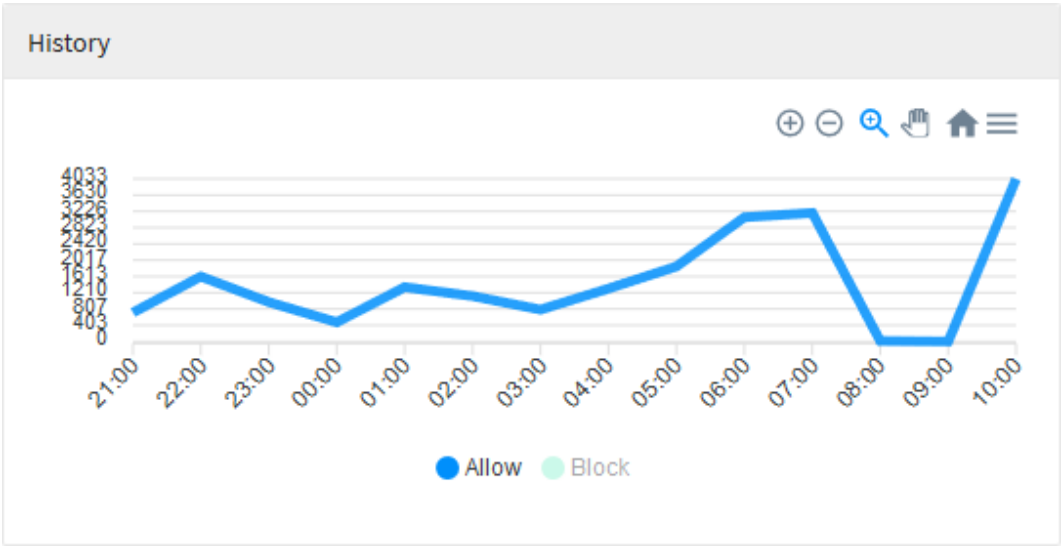
Logo abaixo, é mostrado um resumo dos alertas e bloqueios em um gráfico de linhas exibindo a quantidade de eventos relacionados a intrusão dentro do período de tempo previamente selecionado. Ao selecionar uma das legendas (“*Alerted*” ou “*Blocked*”) no topo do gráfico, é possível determinar que apenas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

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



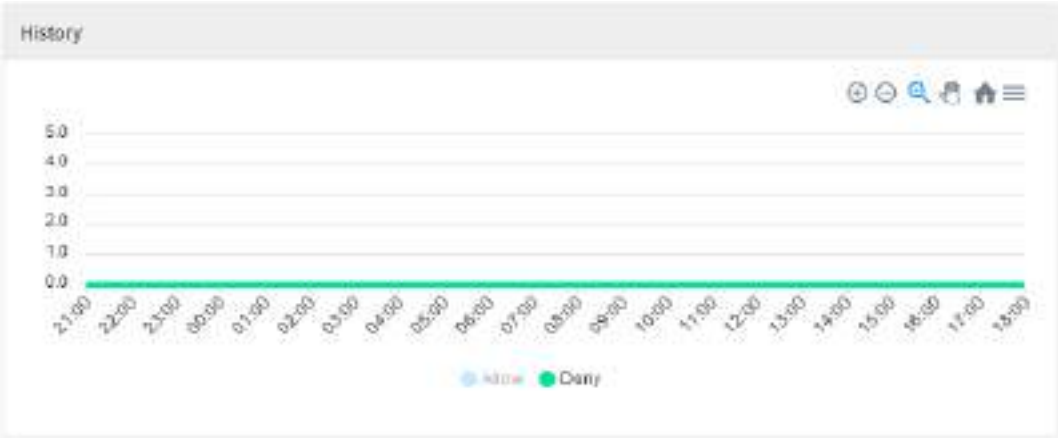
Alerted, *Blocked* e Histórico

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



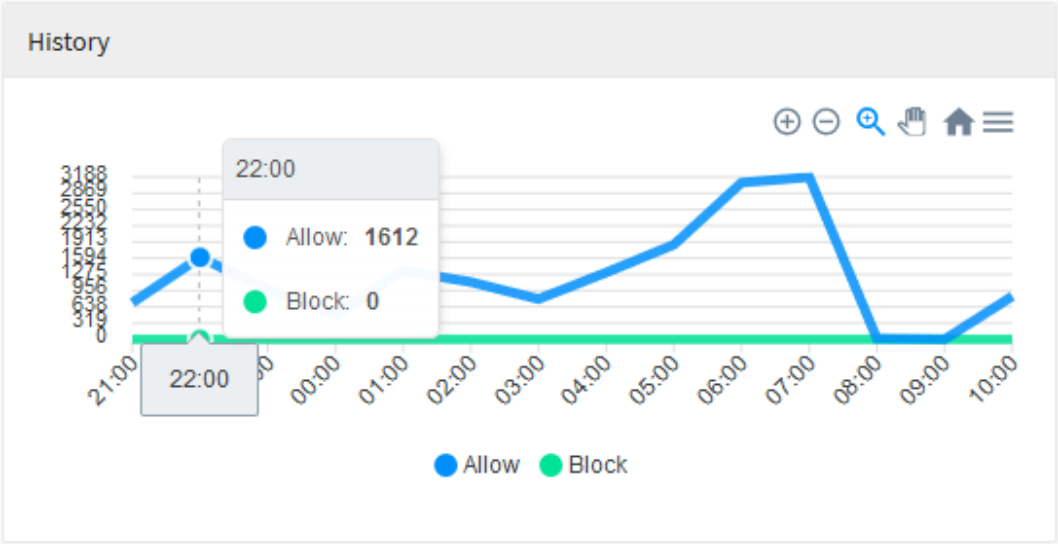
Alerted, Blocked e Histórico - *Allow*

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



Alerted, Blocked e Histórico - *Deny*

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



Alerted, *Blocked* e Histórico - Resumo do Período

UTM - Intrusion Prevention - Alerts by Geolocation

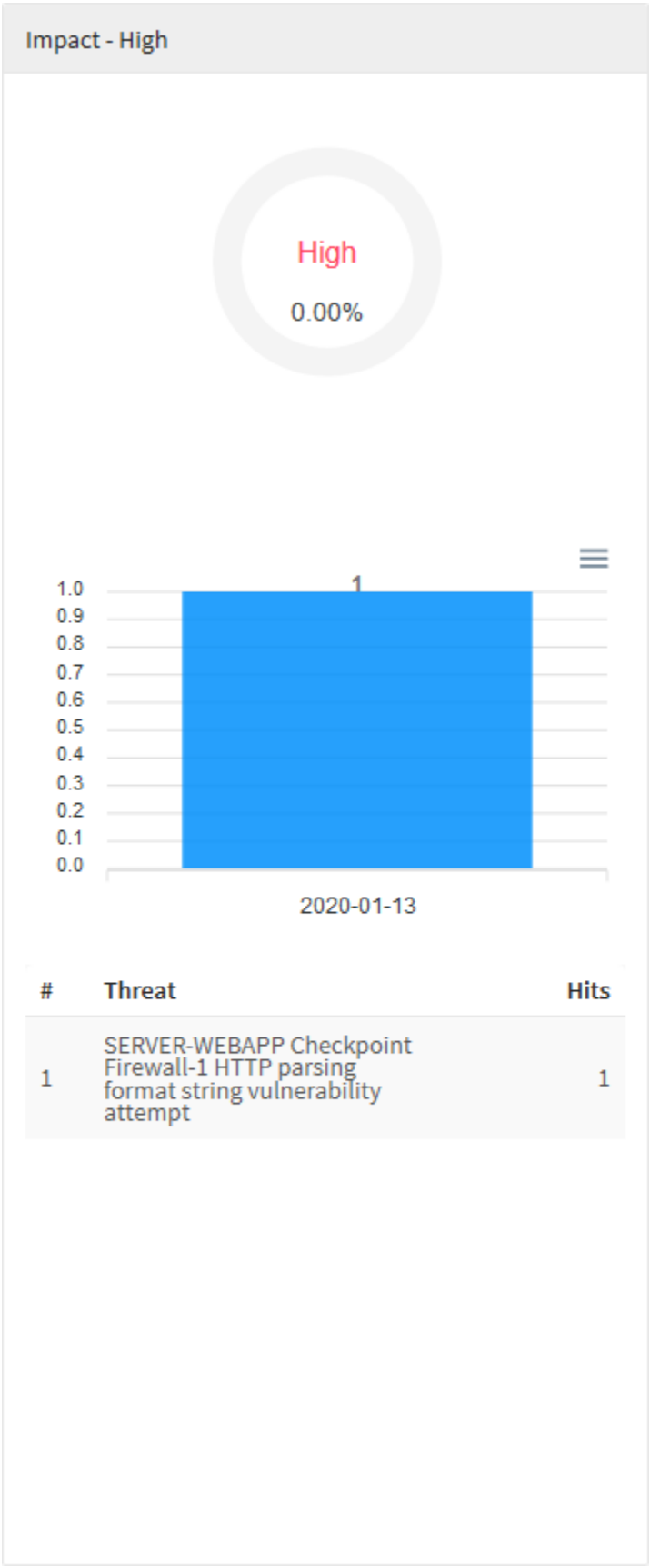
Em “*Alerts by Geolocation*” é exibida a origem das intrusões por geolocalização, o mapa global demonstra através de uma legenda colorida a quantia de acessos feitos pelos usuários. Ao passar o mouse por cima dos países um número total de alertas é exibido, ao fazer o mesmo com a legenda é possível visualizar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

Alerts by Geolocation

UTM - Intrusion Prevention - Impact - High

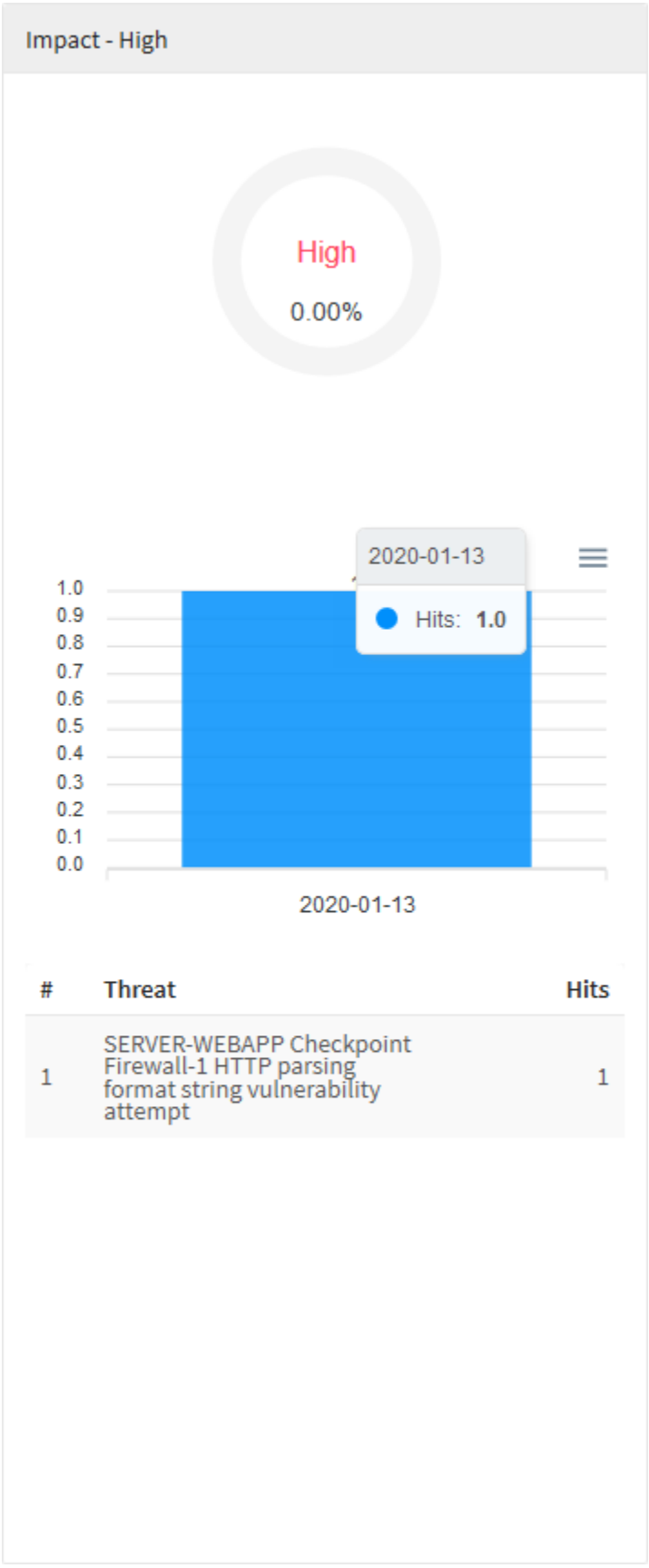
Em “*Impact - High*” temos um gráfico de rosca exibindo a porcentagem de ameaças de intrusão de alto impacto, seguido de um diagrama de colunas exibindo quantas destas mesmas ocorreram dentro do prazo previamente selecionado em comparação com o tráfego de rede do dia. Além disso, uma lista é exibida 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
High
0.00%
1
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
2020-01-13
Threat Hits
1 SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt 1

Impact - High

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

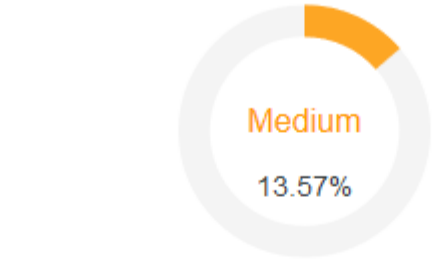


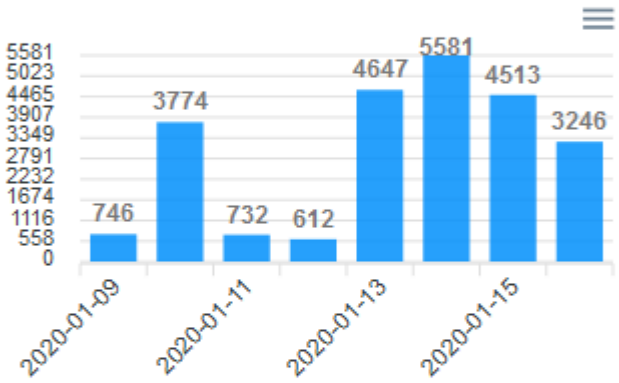
UTM - Intrusion Prevention - Impact - Medium

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

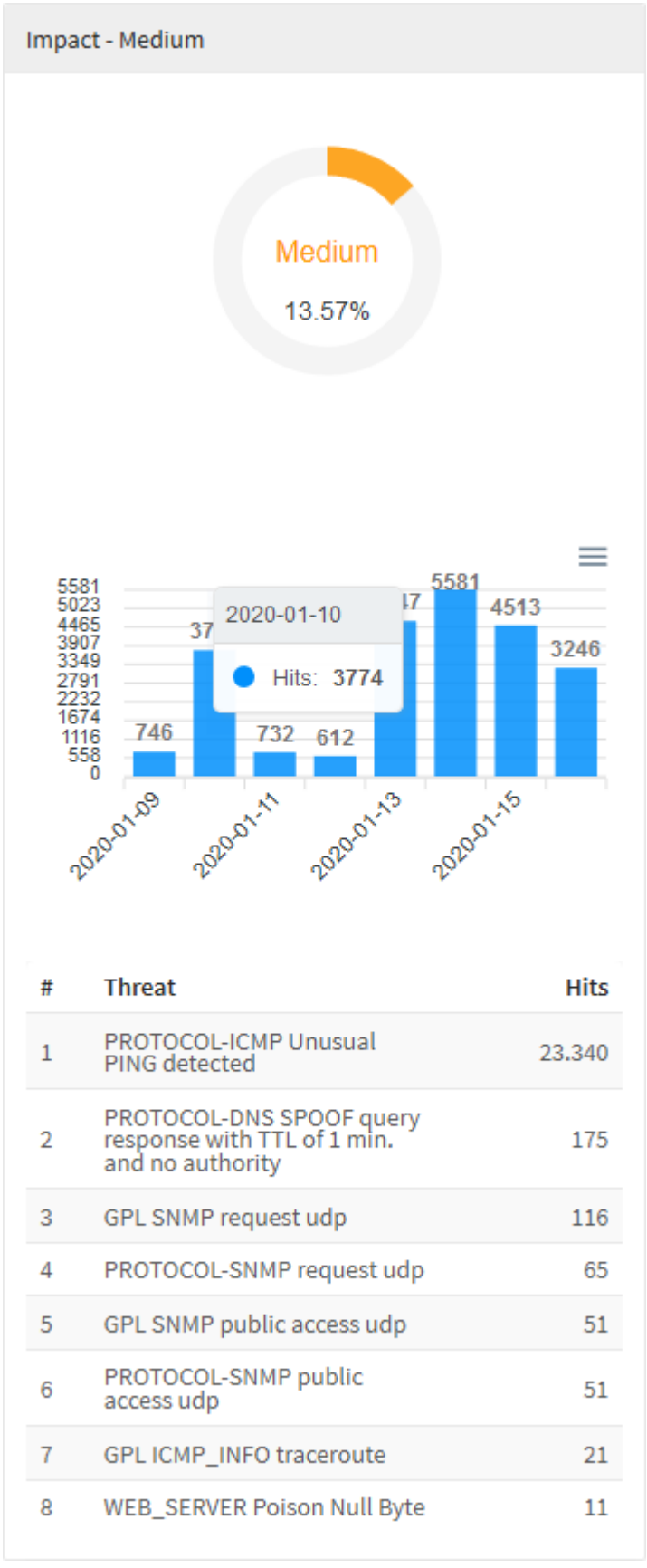




#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	23.340
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	175
3	GPL SNMP request udp	116
4	PROTOCOL-SNMP request udp	65
5	GPL SNMP public access udp	51
6	PROTOCOL-SNMP public access udp	51
7	GPL ICMP_INFO traceroute	21
8	WEB_SERVER Poison Null Byte	11

Impact - Medium

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



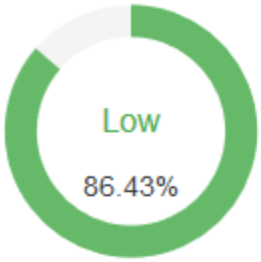
#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	23.340
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	175
3	GPL SNMP request udp	116
4	PROTOCOL-SNMP request udp	65
5	GPL SNMP public access udp	51
6	PROTOCOL-SNMP public access udp	51
7	GPL ICMP_INFO traceroute	21
8	WEB_SERVER Poison Null Byte	11

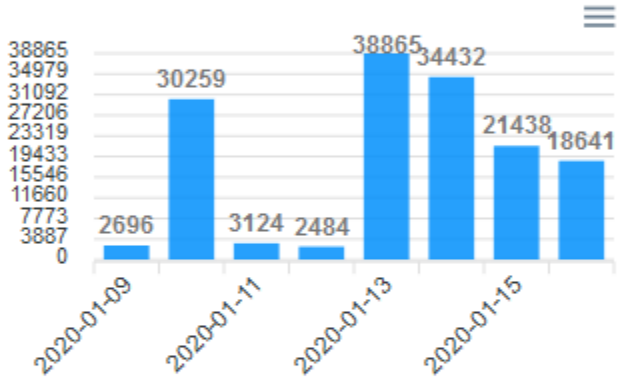
UTM - Intrusion Prevention - Impact - Low

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

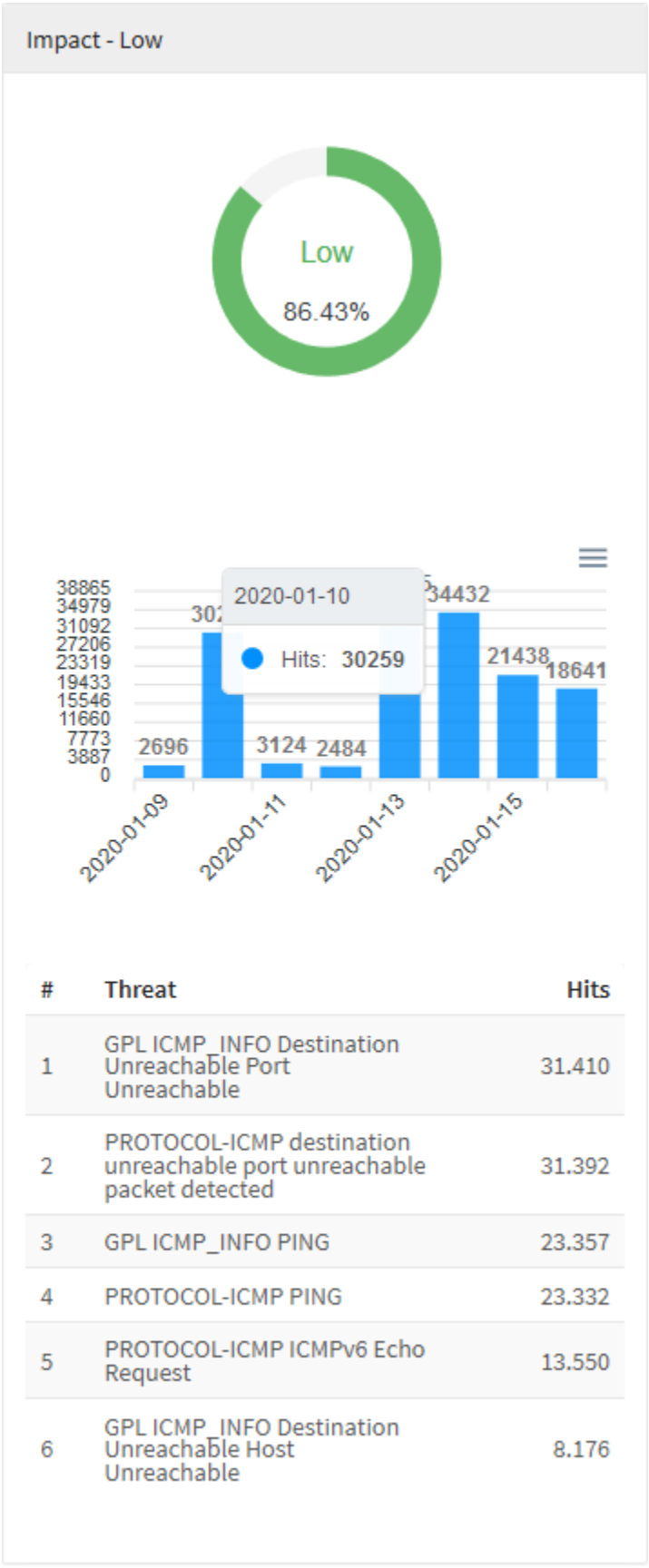




#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	31.410
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	31.392
3	GPL ICMP_INFO PING	23.357
4	PROTOCOL-ICMP PING	23.332
5	PROTOCOL-ICMP ICMPv6 Echo Request	13.550
6	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.176

Impact - Low

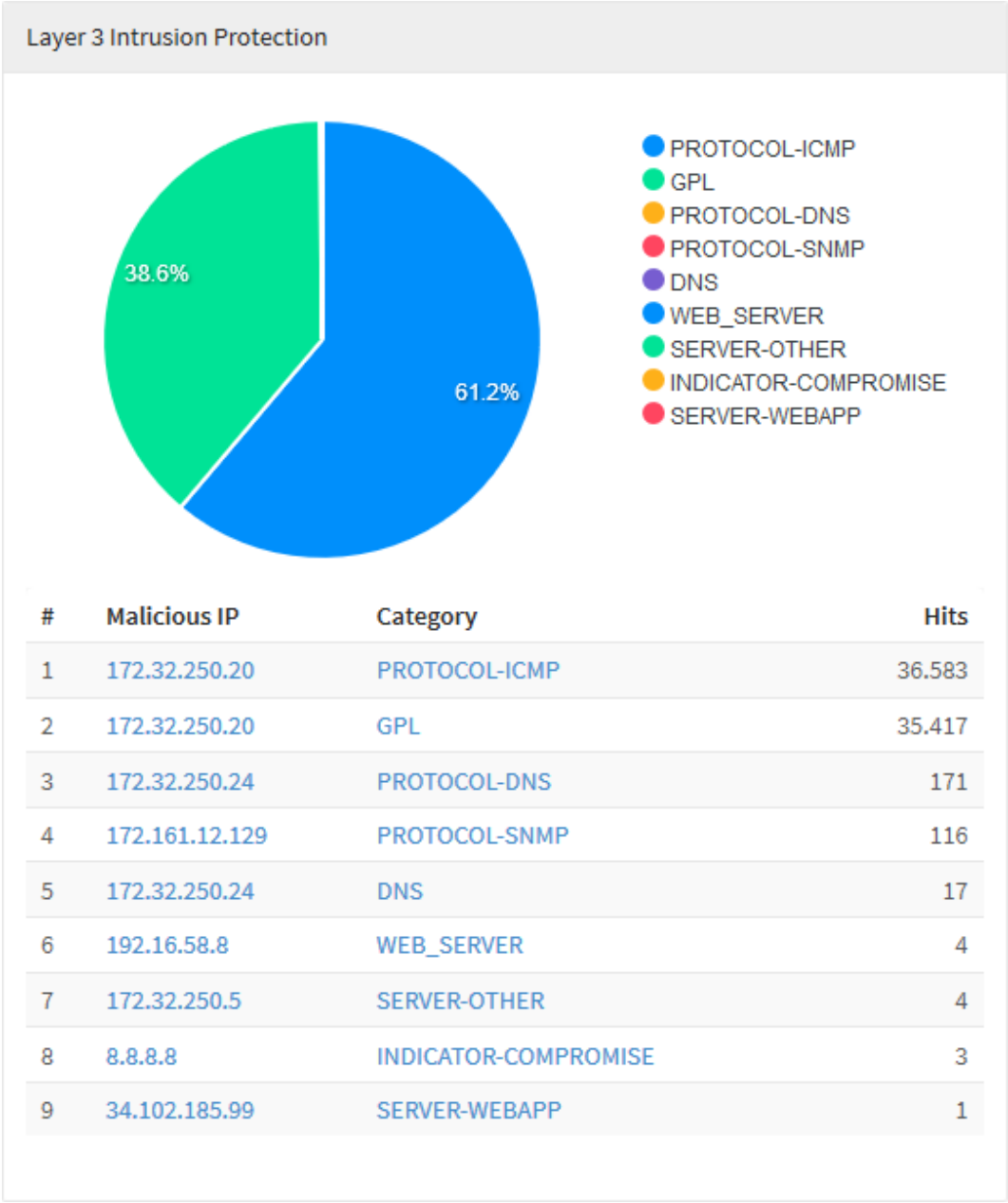
Ao passar o mouse por cima do gráfico, um resumo do período é exibido, conforme demonstrado na imagem abaixo:



#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	31.410
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	31.392
3	GPL ICMP_INFO PING	23.357
4	PROTOCOL-ICMP PING	23.332
5	PROTOCOL-ICMP ICMPv6 Echo Request	13.550
6	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.176

UTM - Intrusion Prevention - Layer 3 Intrusion Protection

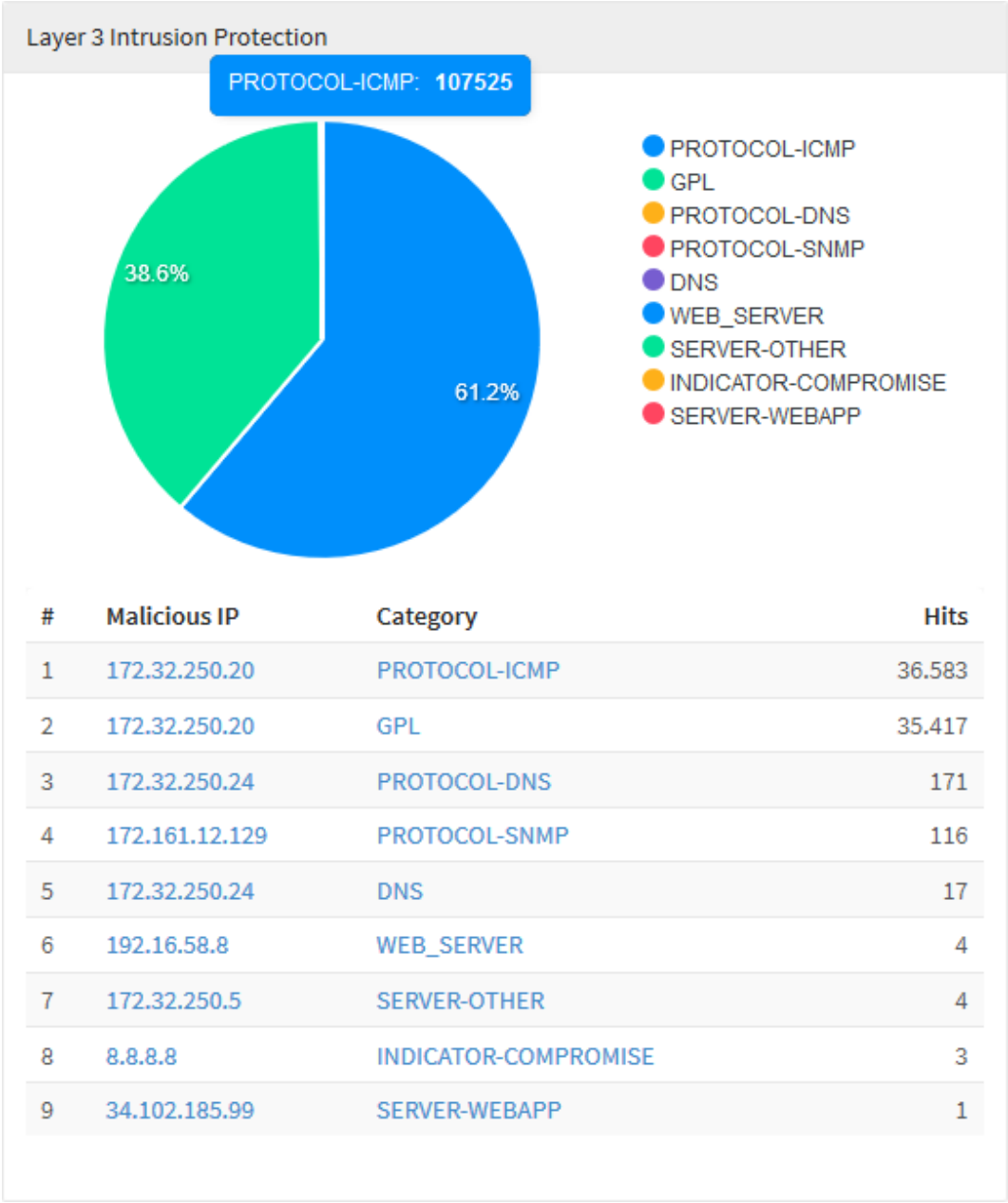
Em “*Layer 3 Intrusion Protection*” temos um gráfico exibindo as dez categorias de alertas de intrusão mais detectadas na camada 3 do *IPS* (*Intrusion Prevention System*). Ao clicar em um dos IPs ou uma das categorias, você será redirecionado para Events usando o item que foi clicado como filtro, criando 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.



#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

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:

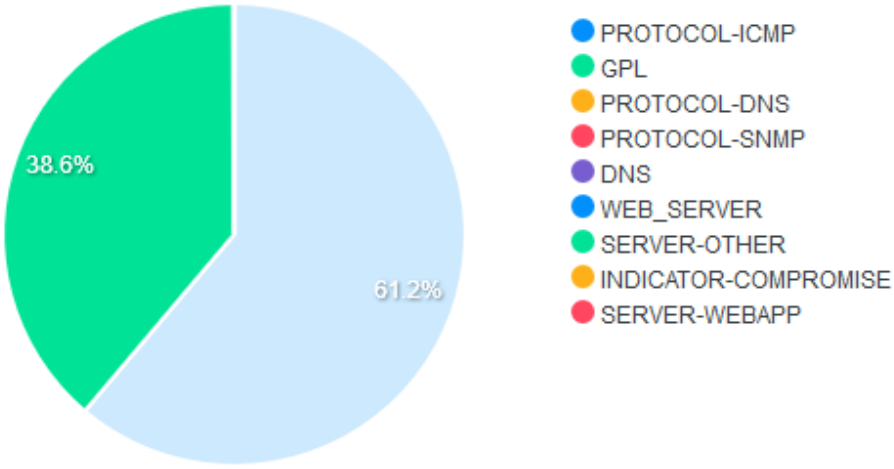


#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

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 Protection



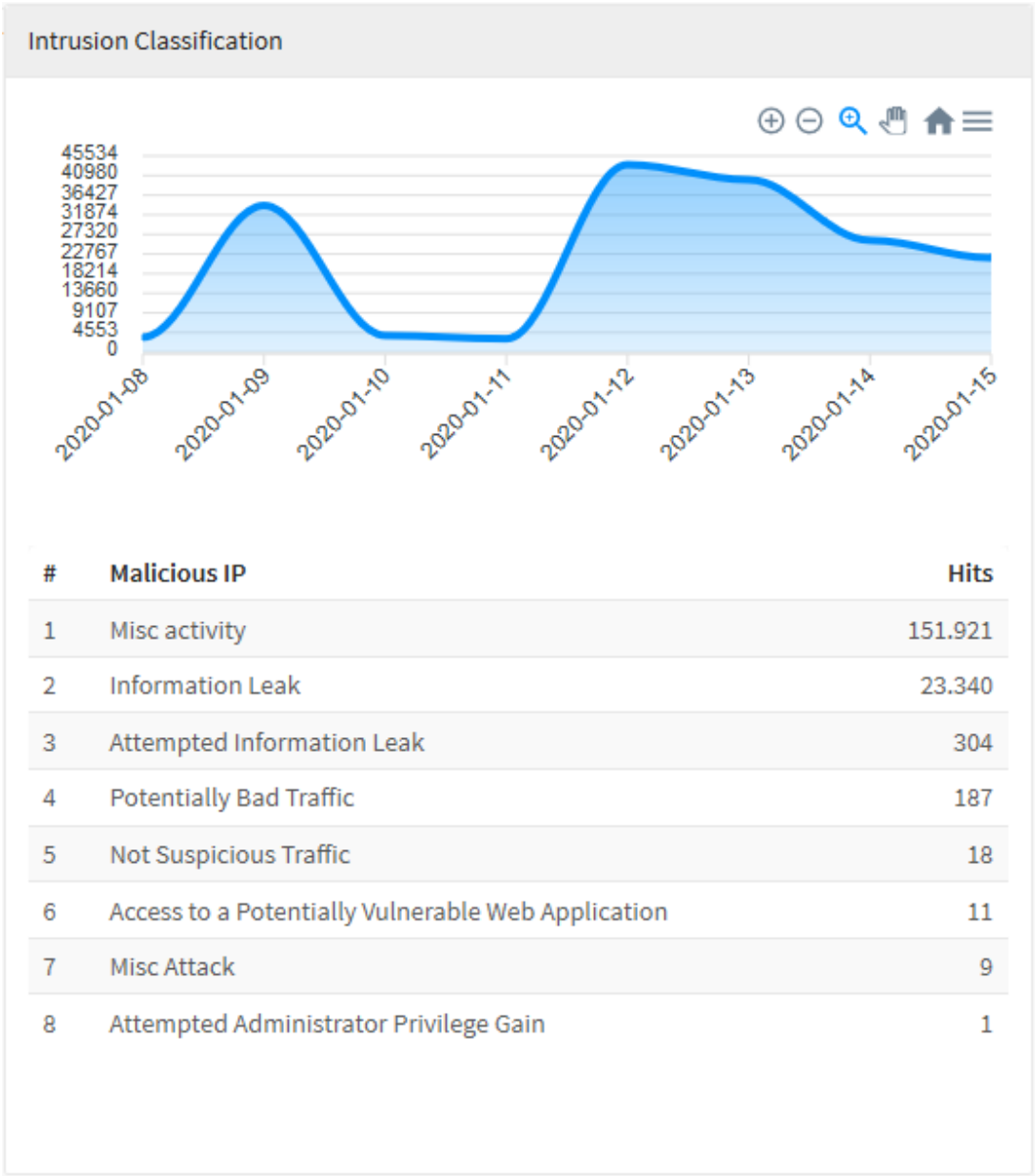
#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

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.

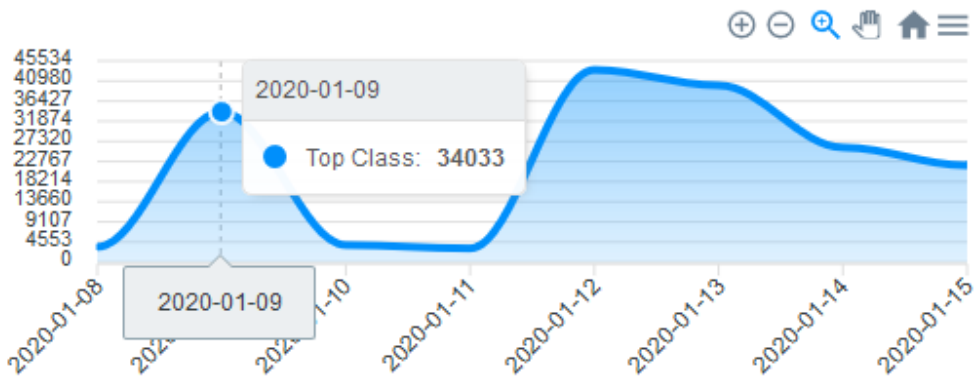


#	Malicious IP	Hits
1	Misc activity	151.921
2	Information Leak	23.340
3	Attempted Information Leak	304
4	Potentially Bad Traffic	187
5	Not Suspicious Traffic	18
6	Access to a Potentially Vulnerable Web Application	11
7	Misc Attack	9
8	Attempted Administrator Privilege Gain	1

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



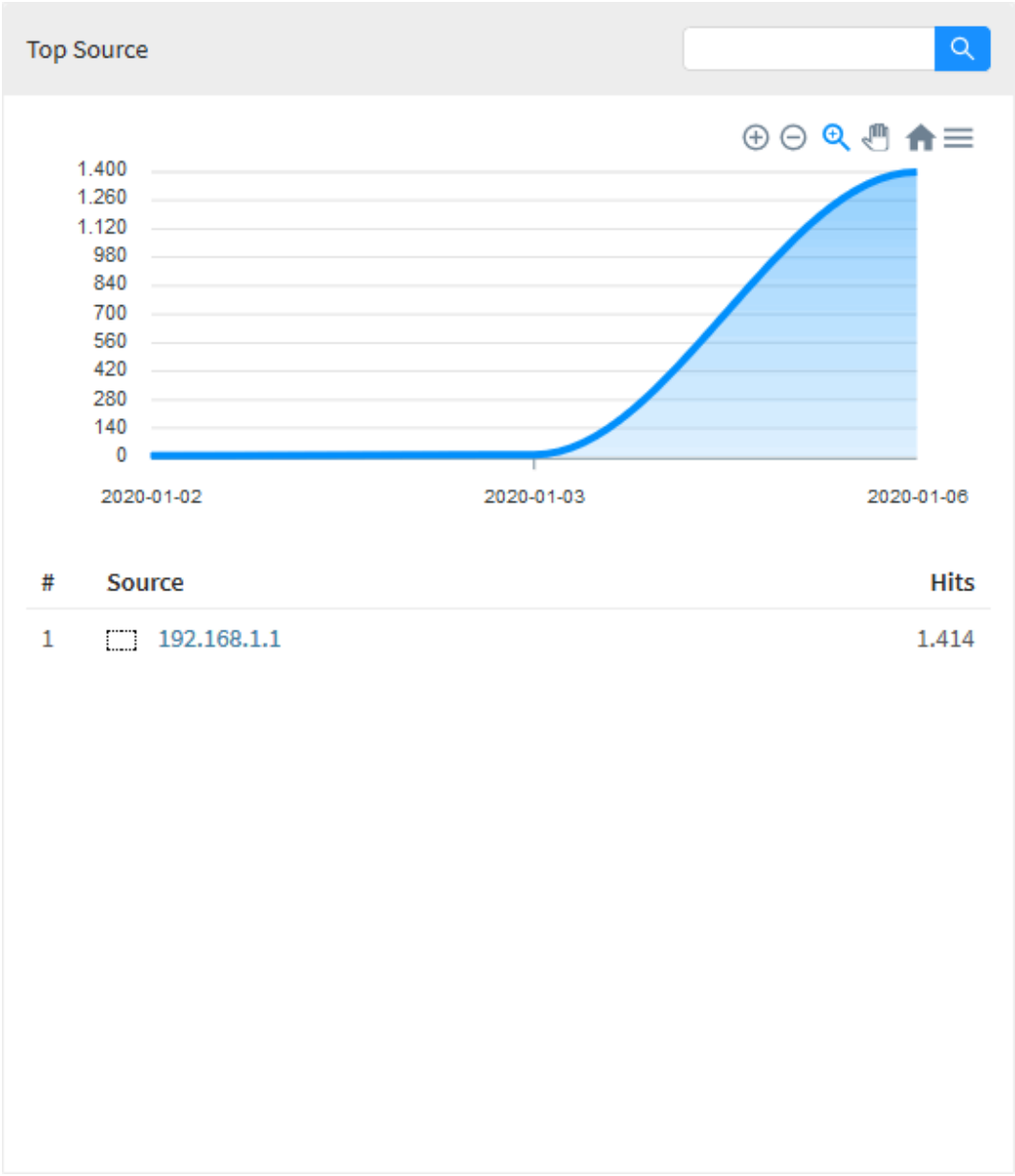
#	Malicious IP	Hits
1	Misc activity	151.921
2	Information Leak	23.340
3	Attempted Information Leak	304
4	Potentially Bad Traffic	187
5	Not Suspicious Traffic	18
6	Access to a Potentially Vulnerable Web Application	11
7	Misc Attack	9
8	Attempted Administrator Privilege Gain	1

Intrusion Classification - Resumo das classes

UTM - Intrusion Prevention - Top Source

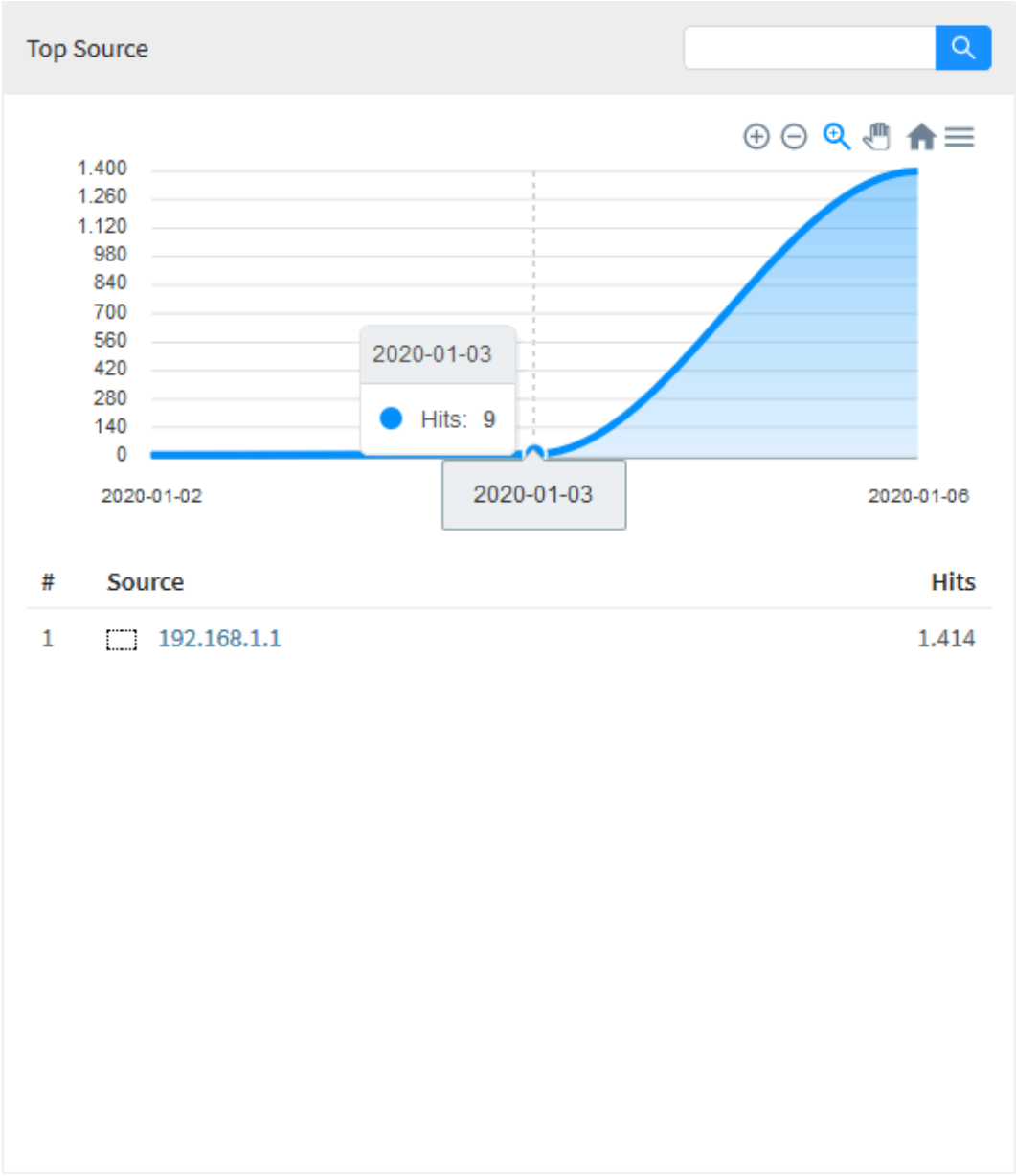
Em “*Top Source*” é exibido um gráfico de linha representando as dez fontes de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista 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:

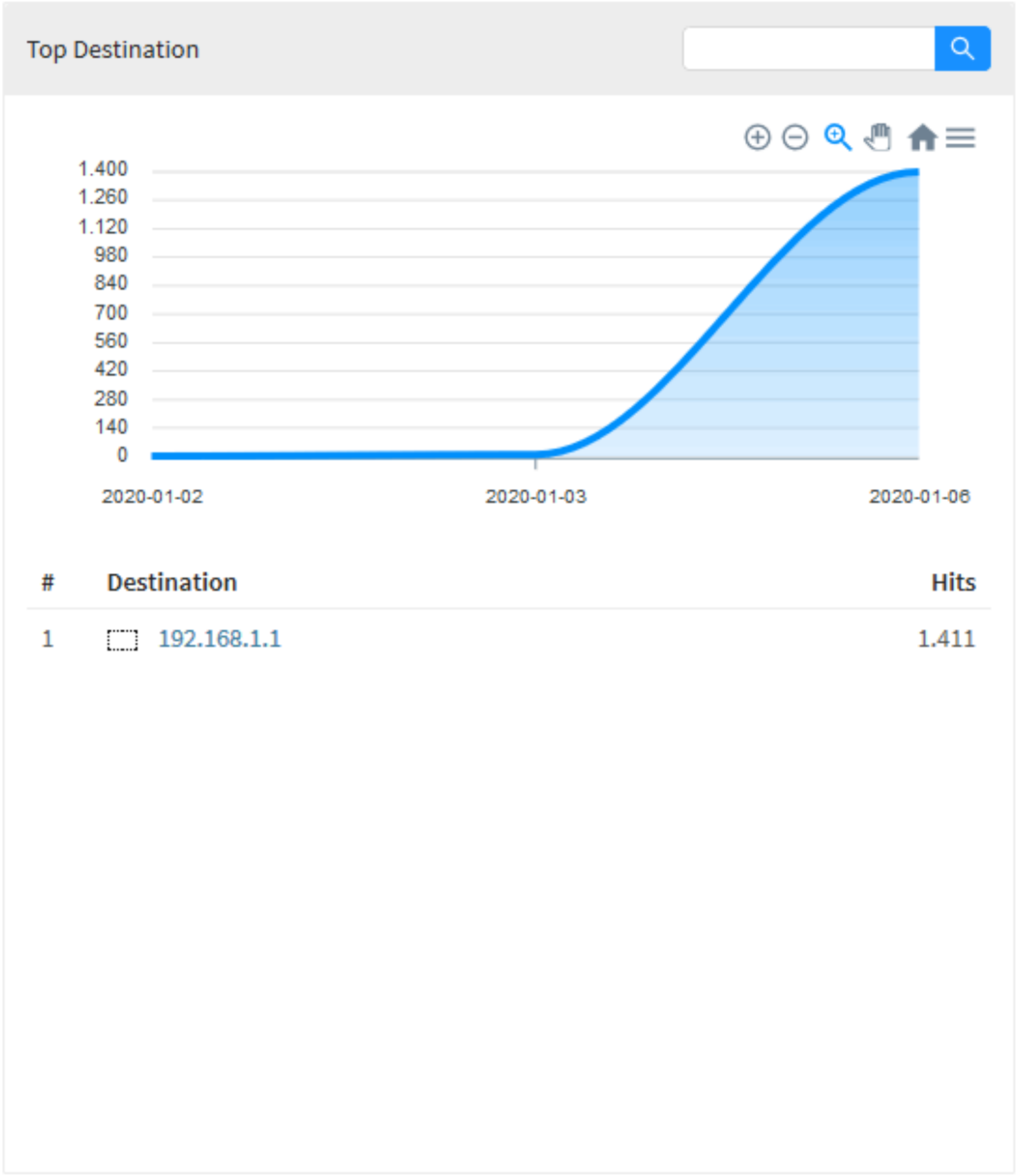


Top Source - Resumo

UTM - Intrusion Prevention - Top Destination

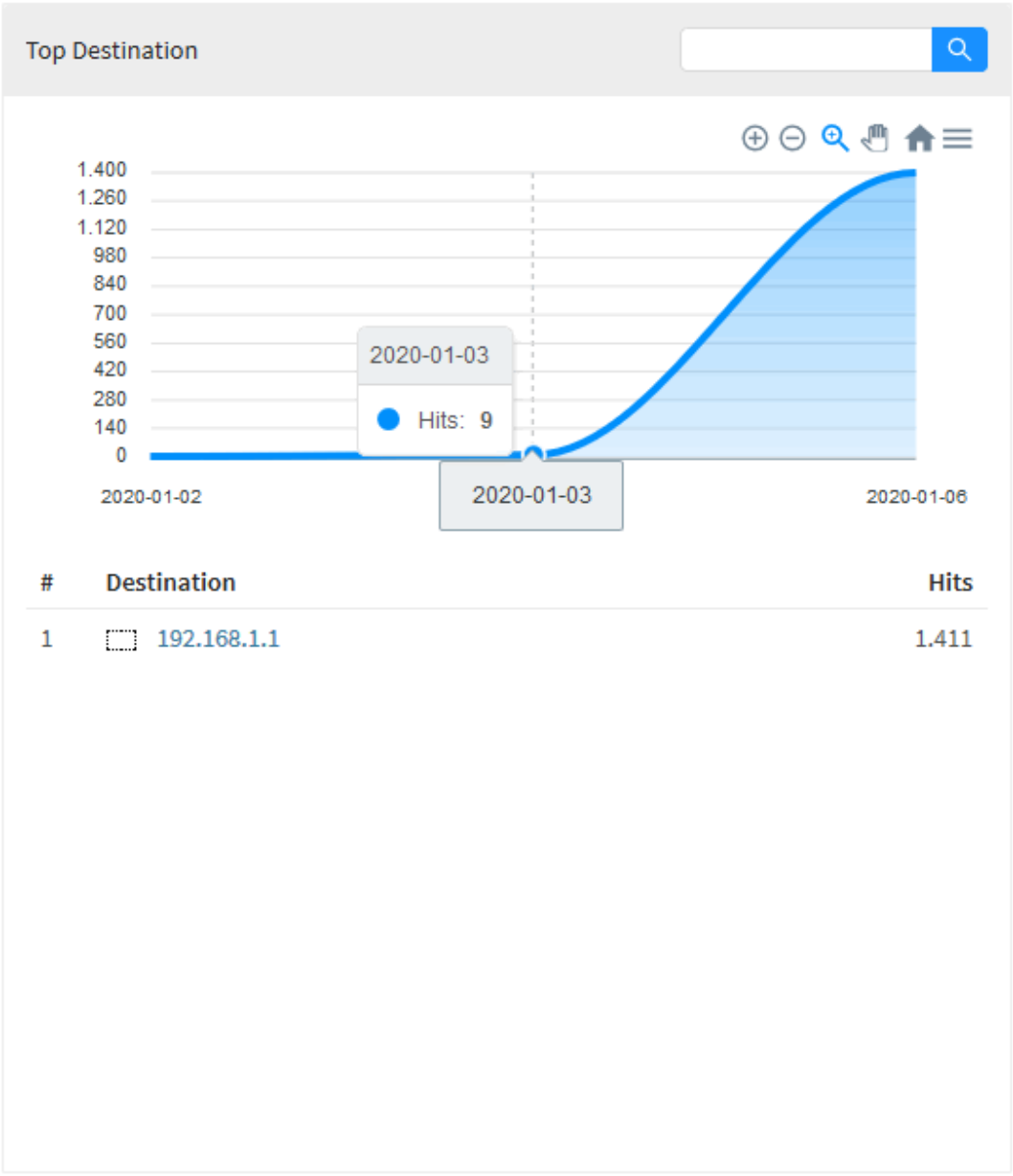
Em “*Top Destination*” tem-se um gráfico de linha exibindo os dez destinos de alerta de intrusão mais recorrentes em relação ao período de tempo previamente especificado, ao passar o mouse sobre o gráfico ele mostrará a data e a quantia de acessos a essas fontes em geral. Logo abaixo tem-se uma lista 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 *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.

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



Top Destination

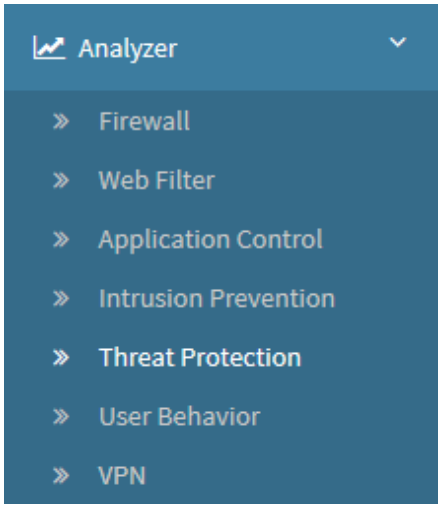
Ao passar o mouse sobre o gráfico, ele evidenciará a data e o número de acessos da classe mais alta deste dia em específico:



Top Destination - Resumo de Acessos

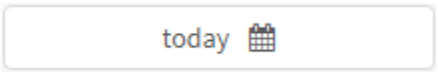
UTM - Threat Protection

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:

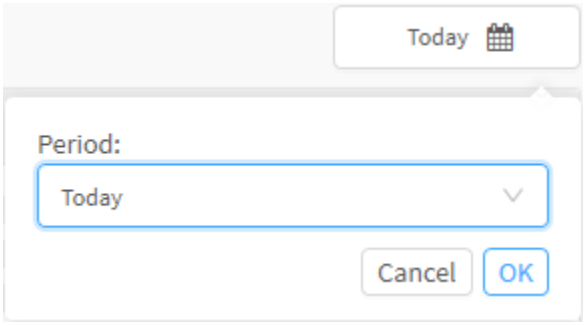


Threat Protection - Caixa de Seleção

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.

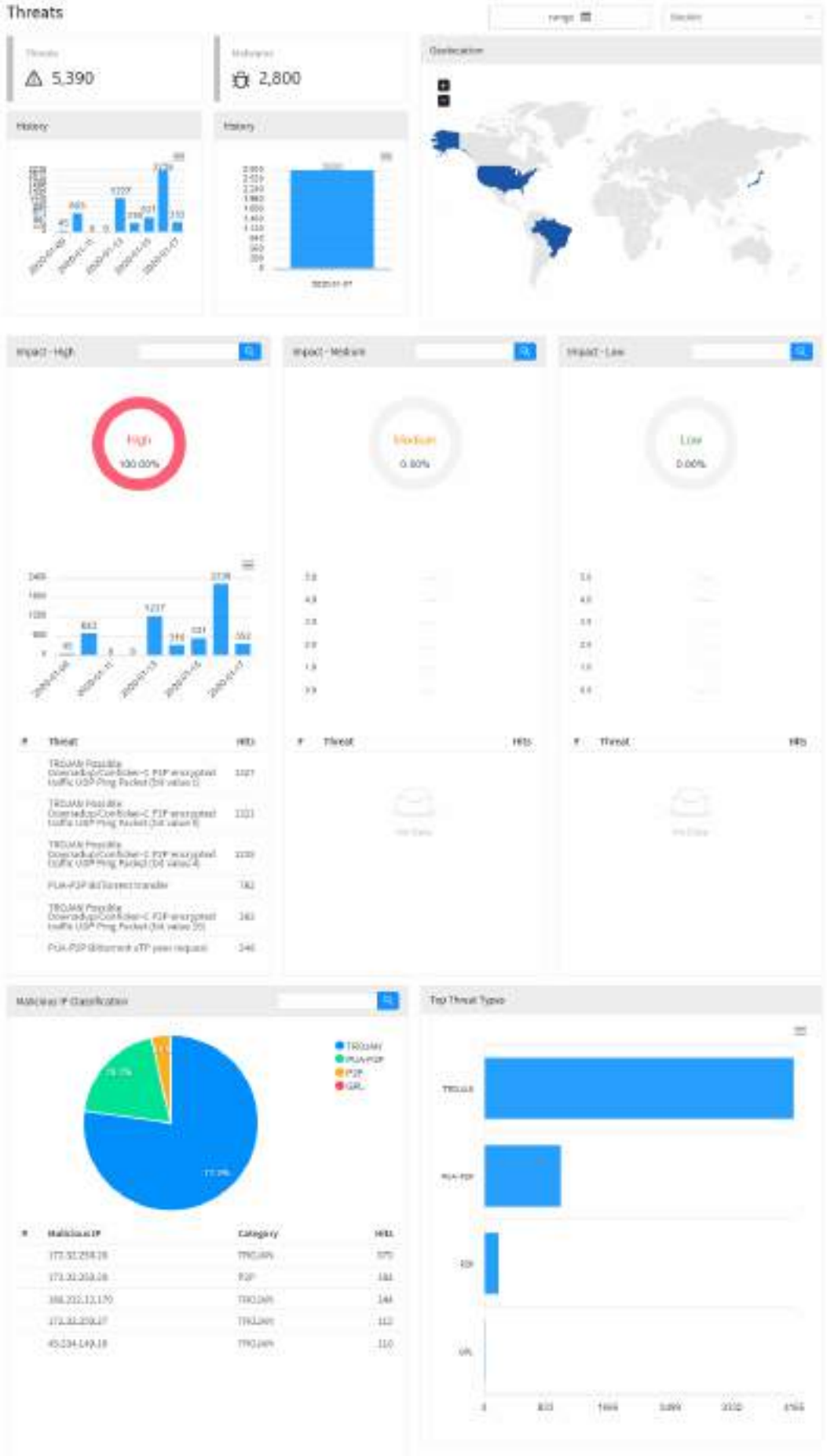
Selecione o período desejado:

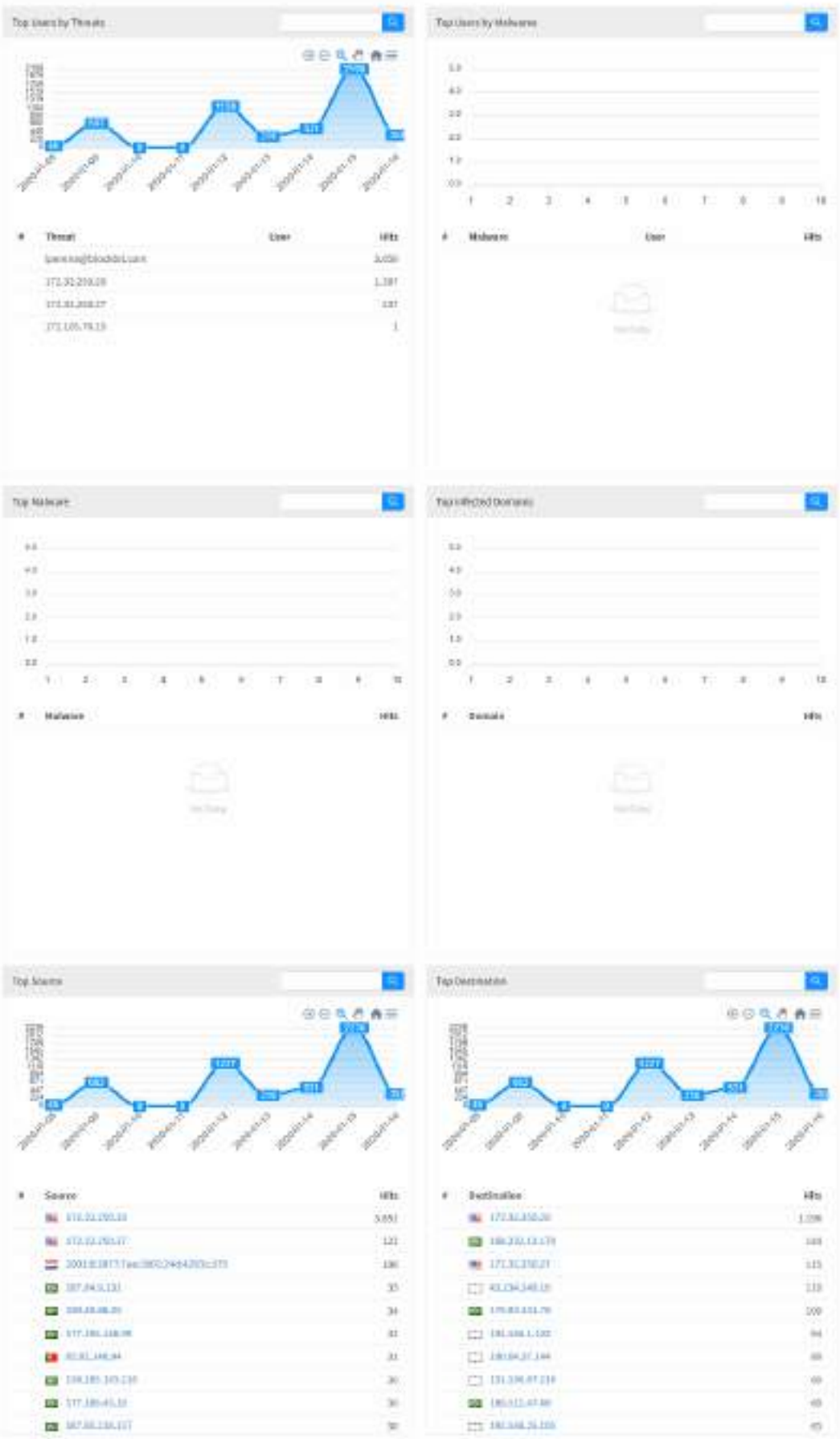


Threat Protection - Seleção de Data

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

A tela abaixo será exibida:


Threats
5,390
2,800
High
100.00%
Medium
0.00%
Low
0.00%



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;
- []: Serve para mover o gráfico;
- []: 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 [**  **]**.

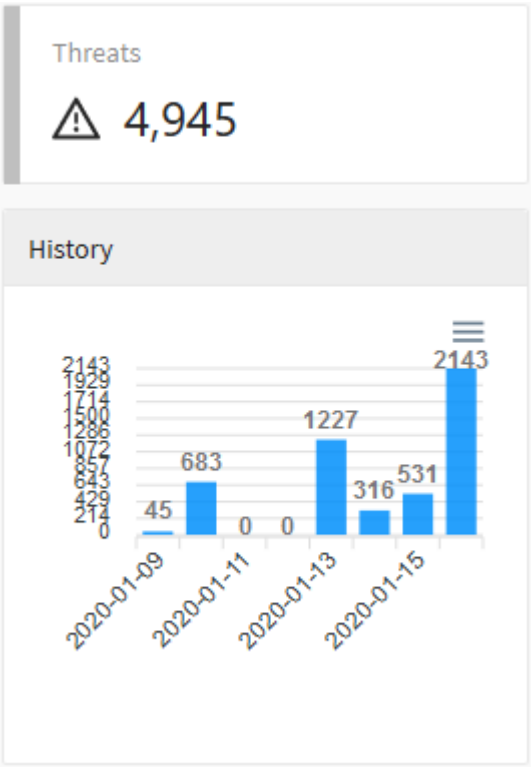
A seguir, analisaremos em detalhes os componentes de "*Threat Protection*":

- *Threats e History*;
- *Malwares e History*;
- *Geolocation*;
- *Impact - High*;
- *Impact - Medium*;
- *Impact - Low*;
- *Malicious IP Classification*;
- *Top Threat Types*;
- *Top Users by Threats*;
- *Top Users by Malware*;
- *Top Malware*;
- *Top Infected Domains*;
- *Top Source*;
- *Top Destination*.

UTM - Threat Protection - Threats e History

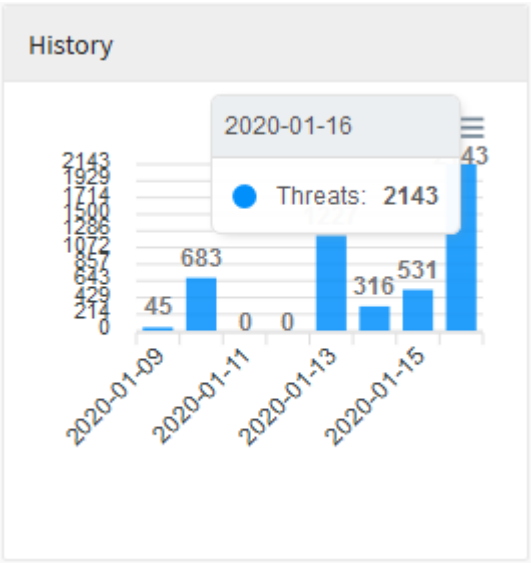
O painel “*Threats*” exibe um total de ameaças detectadas. Logo abaixo, é exibido o histórico em um gráfico de linhas demonstrando a quantia de ameaças detectadas por dia.

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:

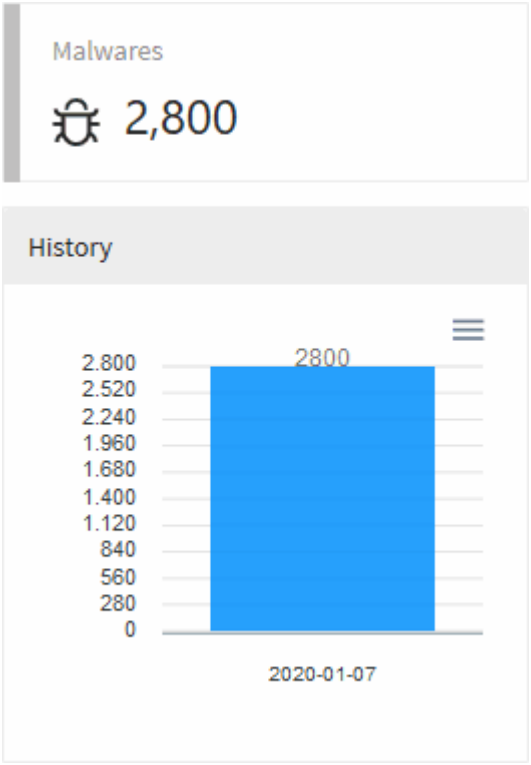


Threat Protection - *History* - Resumo das ameaças

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.

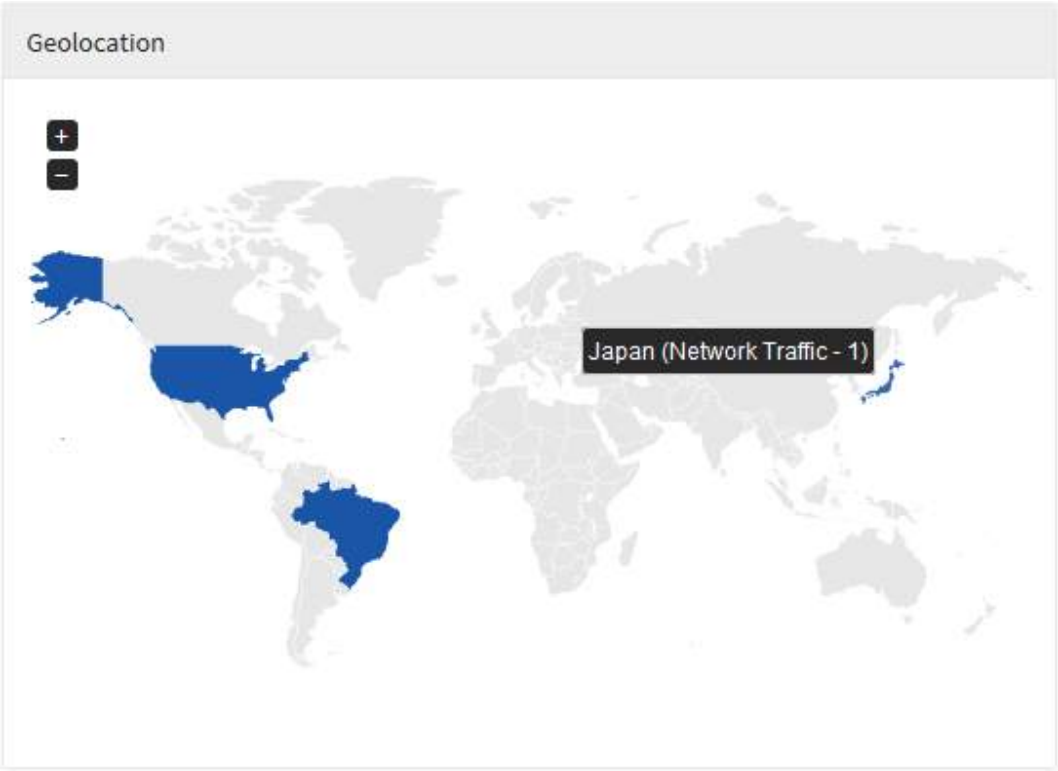
Para mais informações a respeito do menu de navegação presente no topo deste gráfico cheque esta página.



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.

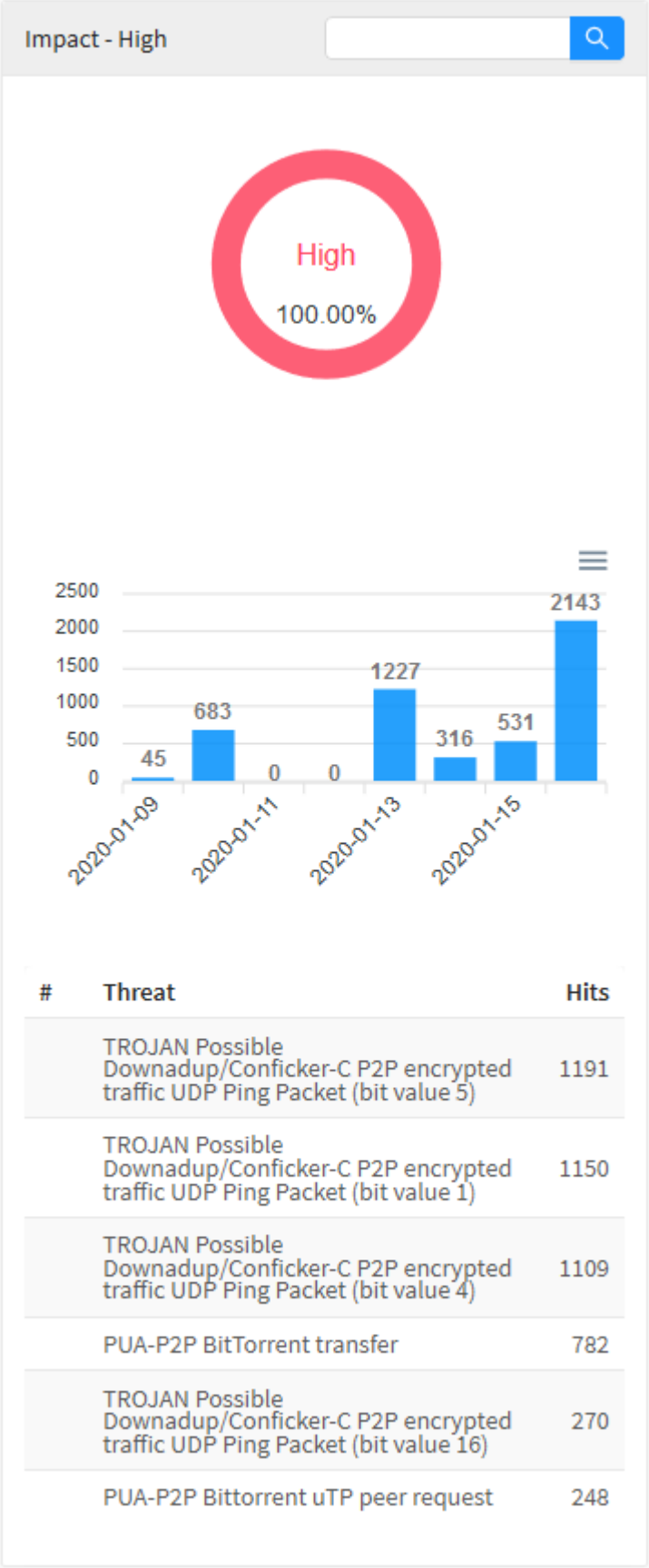


Threat Protection – Geolocation

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.



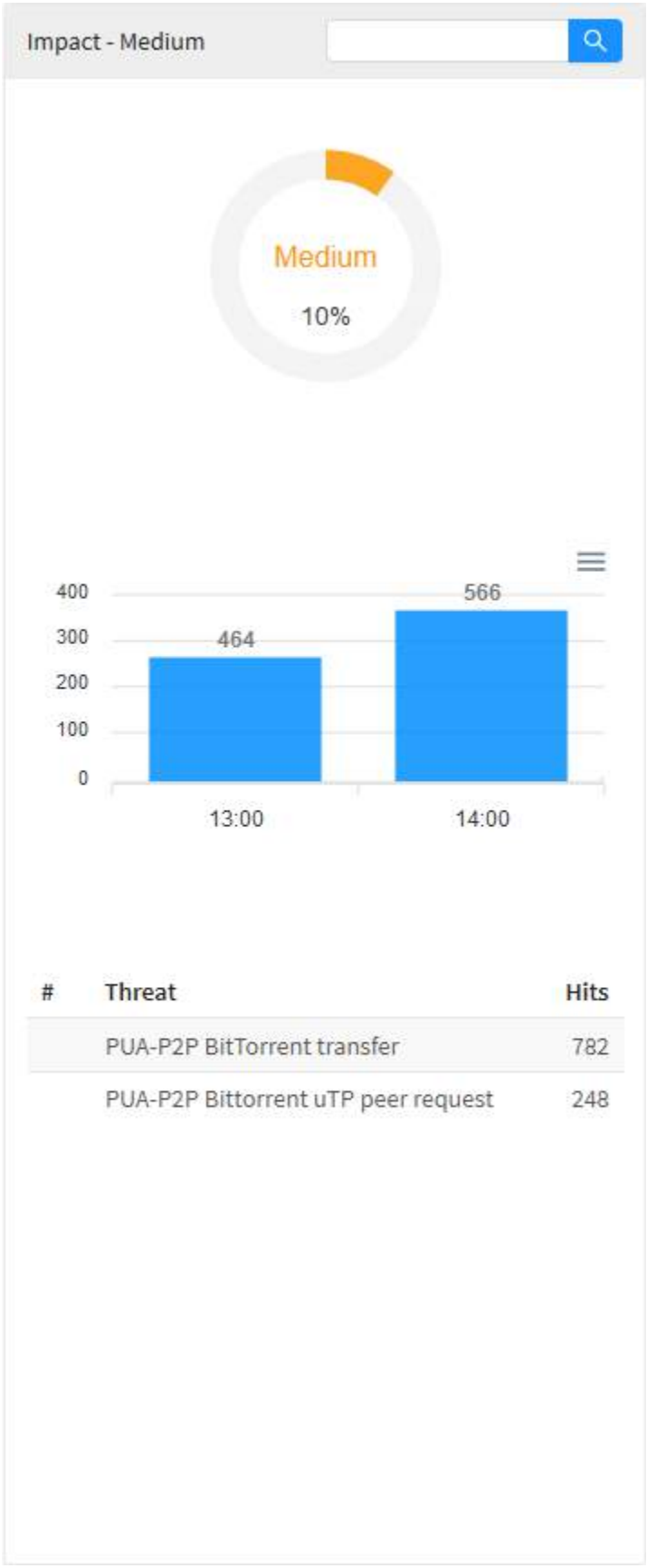
#	Threat	Hits
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	1191
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	1150
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	1109
	PUA-P2P BitTorrent transfer	782
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 16)	270
	PUA-P2P Bittorrent uTP peer request	248

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.

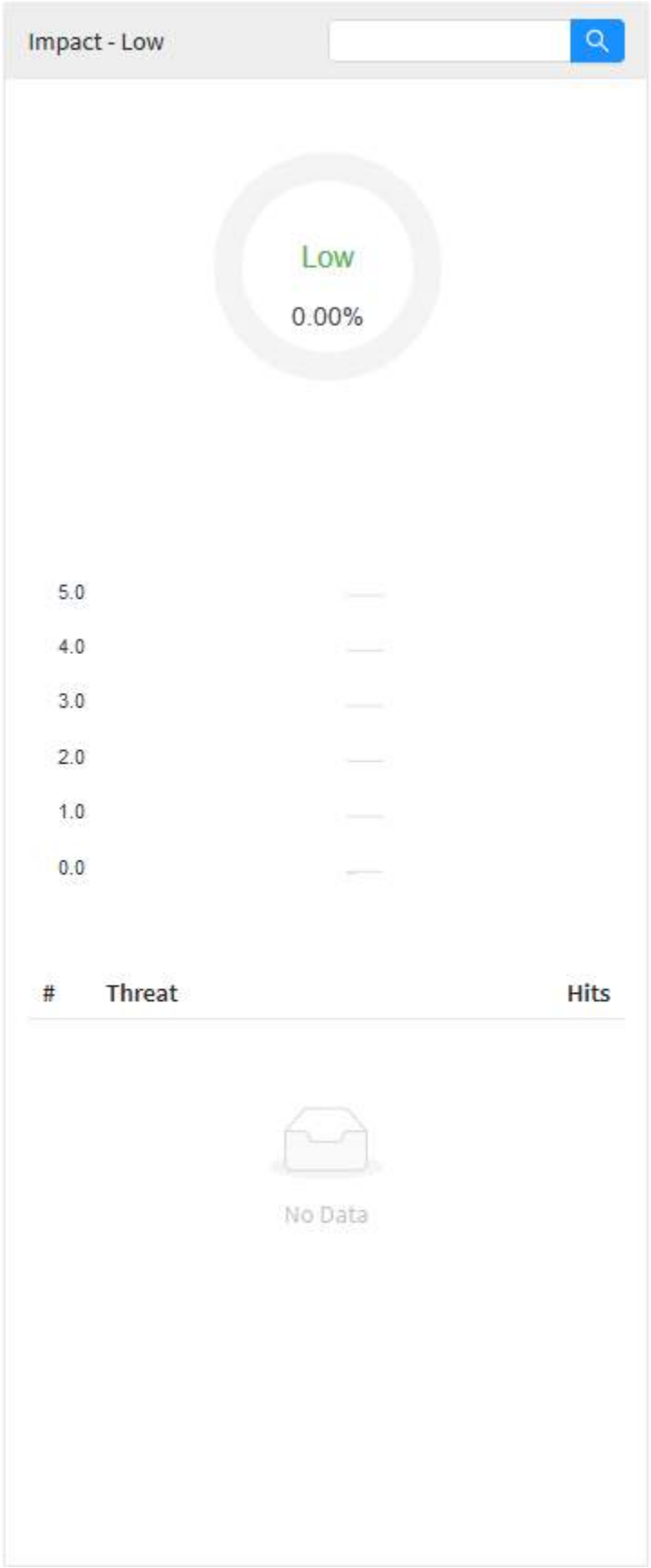


Threat Protection – Impact Medium

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.

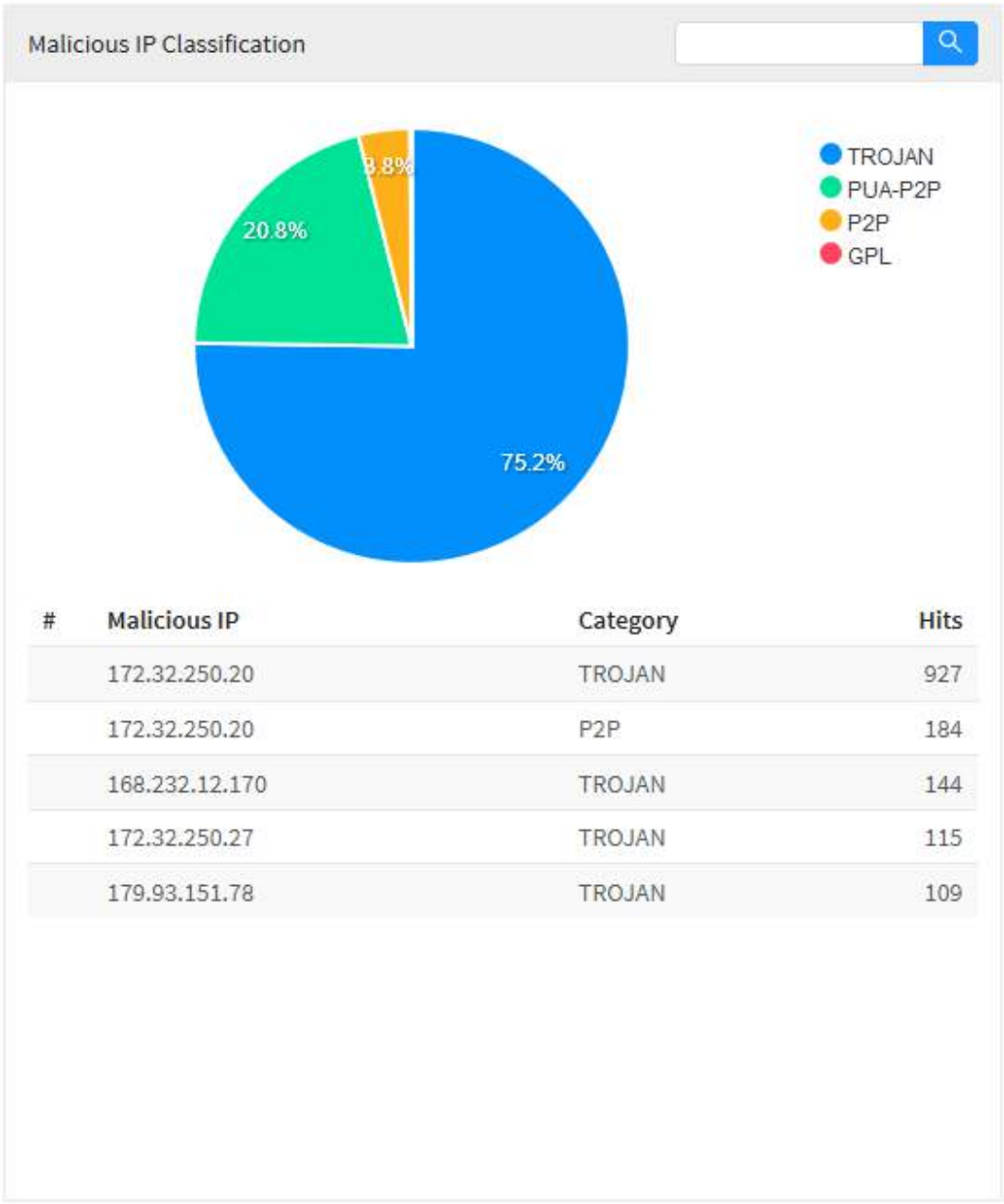


Threat Protection – Impact Low

UTM - Threat Protection - Malicious IP Classification

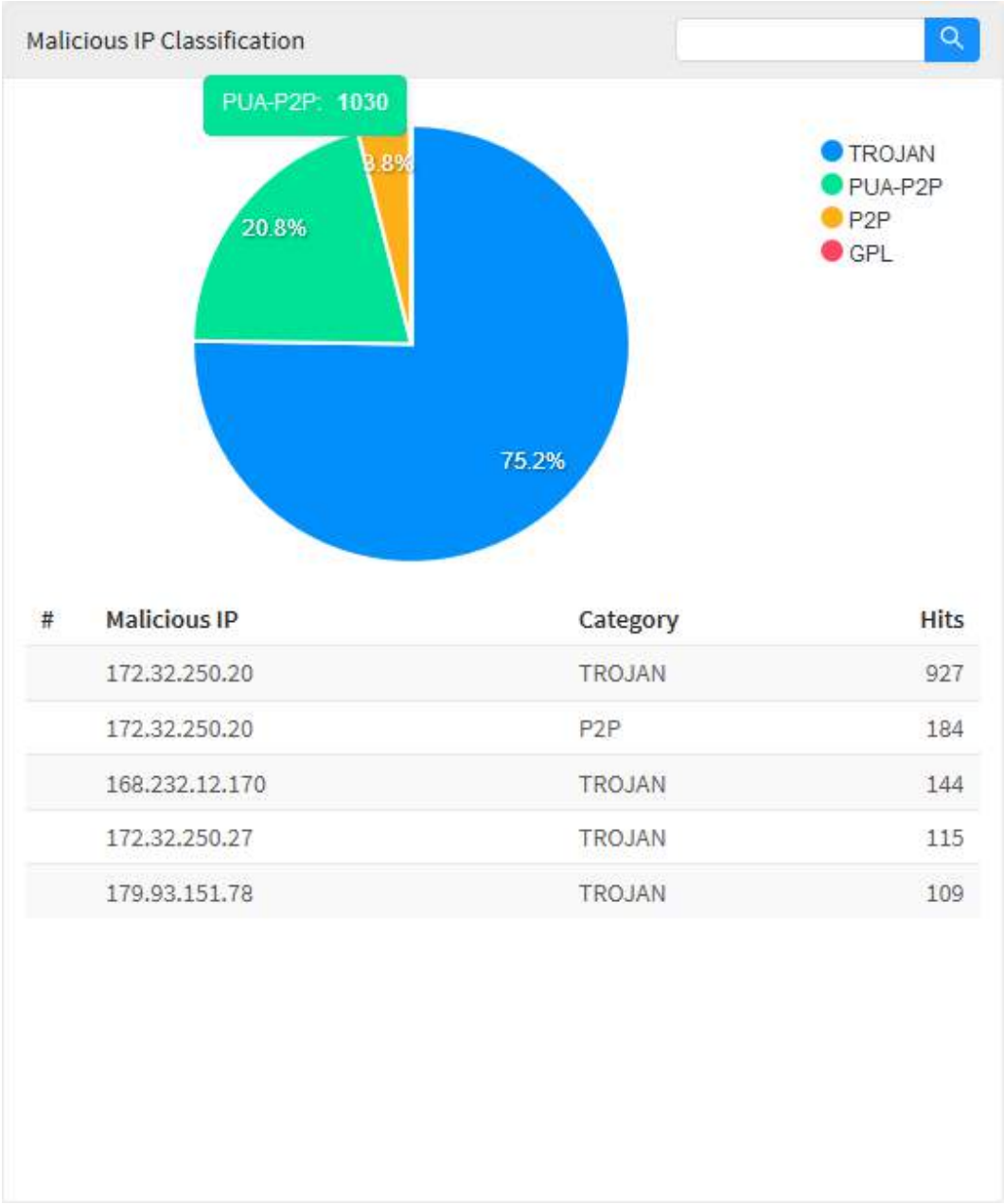
Em “*Malicious IP Classification*” temos um gráfico de rosca exibindo as dez categorias de alertas de *IP* Malicioso mais detectadas na rede, ao passar o mouse sobre cada parte do gráfico ou seu texto correspondente, ele o destacará e exibirá um número com a quantia de acessos a essa categoria de *IP* 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

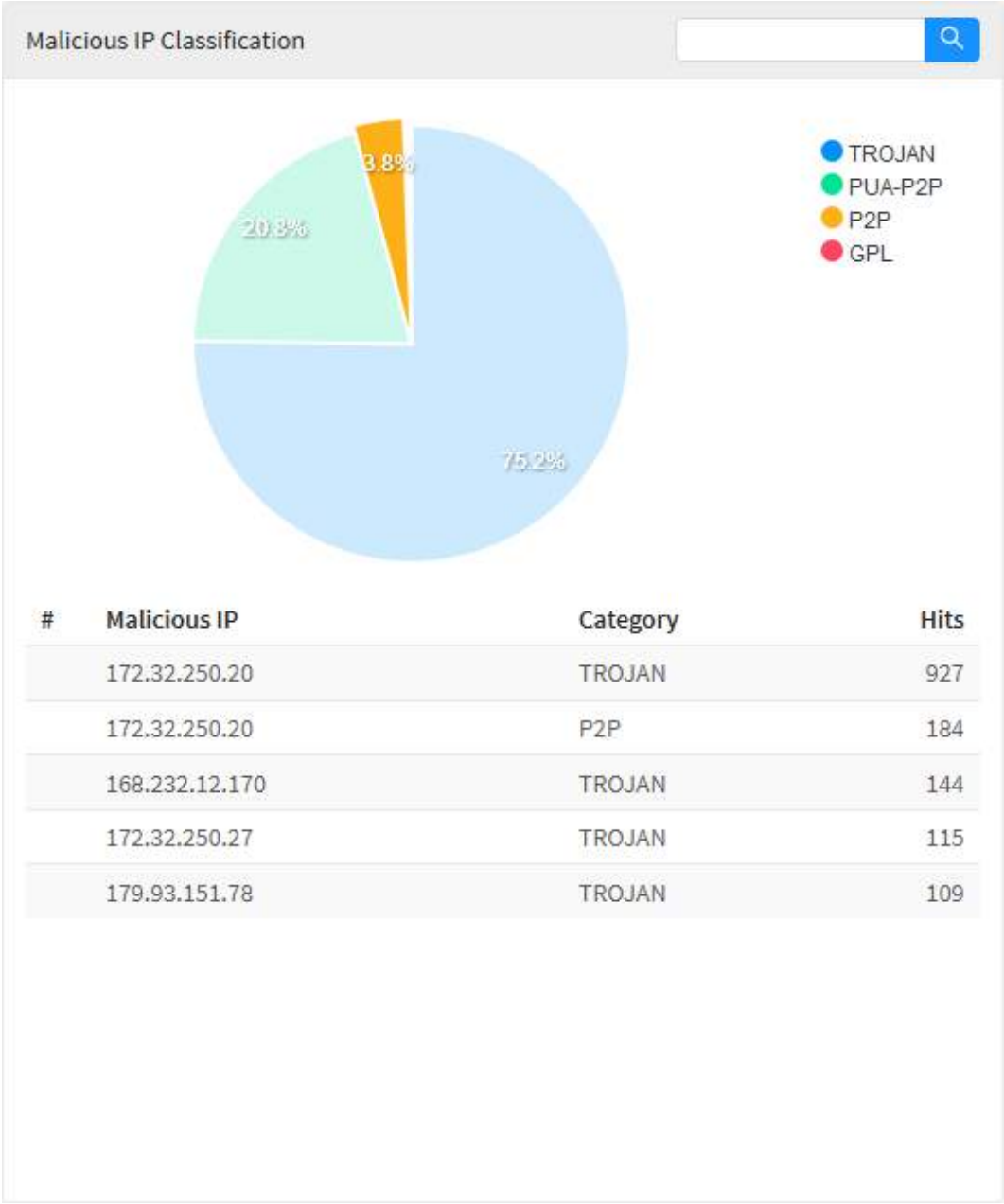
Ao passar o mouse por cima do gráfico, *ele exibirá um número com a quantia de IPs* maliciosos, conforme demonstrado na imagem abaixo:



#	Malicious IP	Category	Hits
	172.32.250.20	TROJAN	927
	172.32.250.20	P2P	184
	168.232.12.170	TROJAN	144
	172.32.250.27	TROJAN	115
	179.93.151.78	TROJAN	109

Threat Protection – Malicious IP Classification - Resumo

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



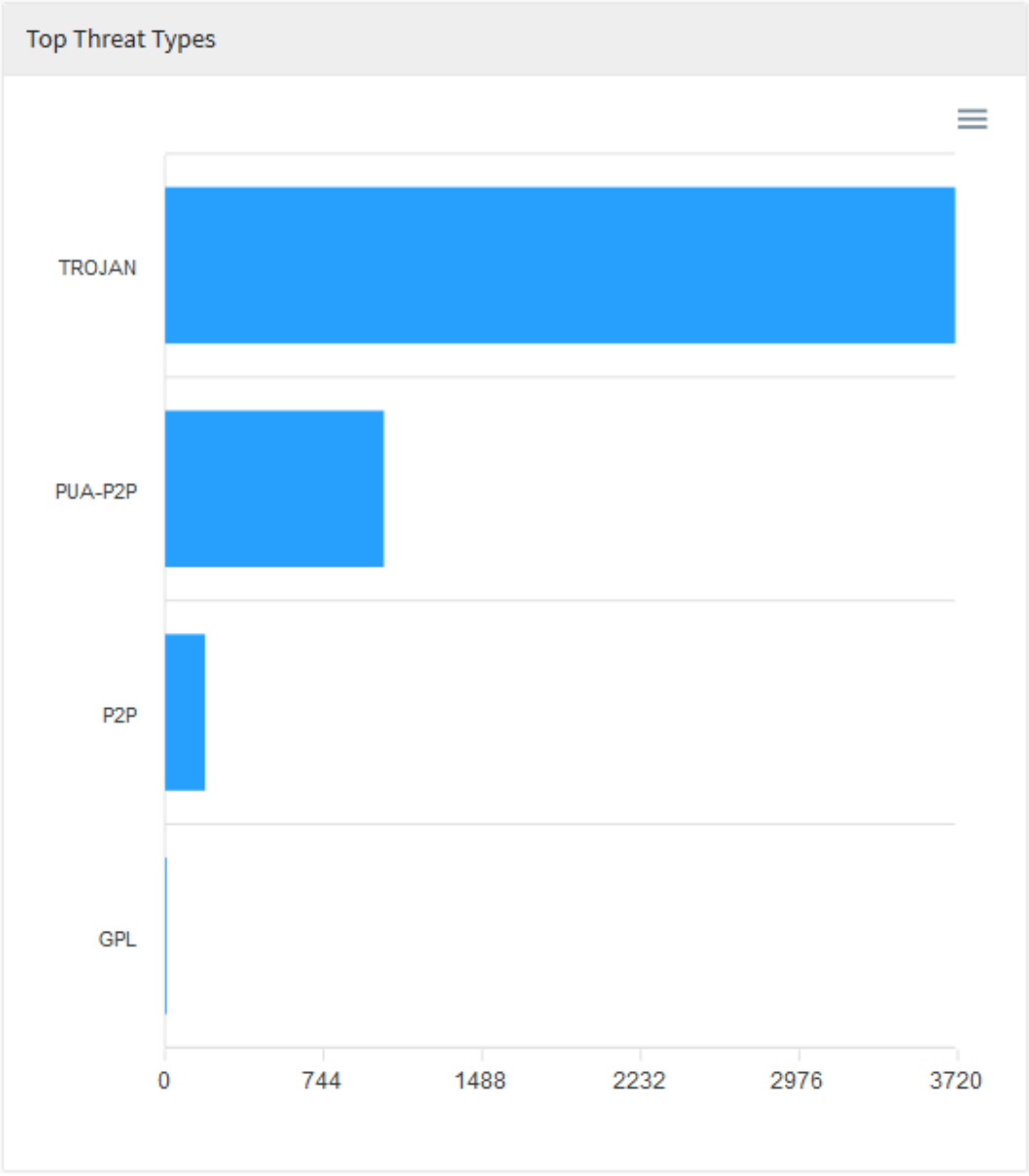
#	Malicious IP	Category	Hits
	172.32.250.20	TROJAN	927
	172.32.250.20	P2P	184
	168.232.12.170	TROJAN	144
	172.32.250.27	TROJAN	115
	179.93.151.78	TROJAN	109

Threat Protection – Malicious IP Classification - Resumo

UTM - Threat Protection - Top Threat Types

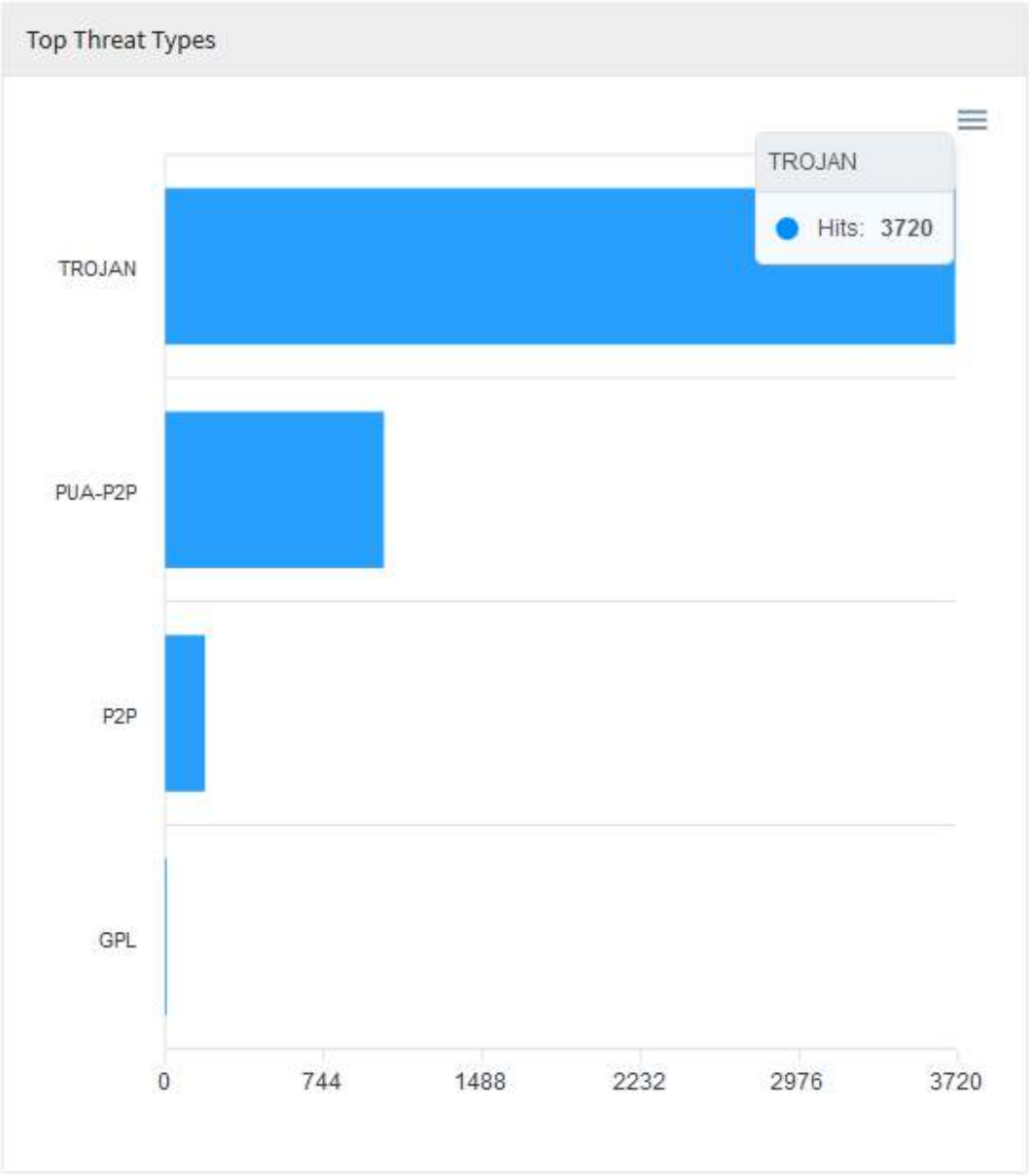
Em “*Top Threat Types*” é exibido um gráfico de barras representando os tipos de ameaça mais recorrentes em relação a quantia de vezes que elas foram detectadas

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:

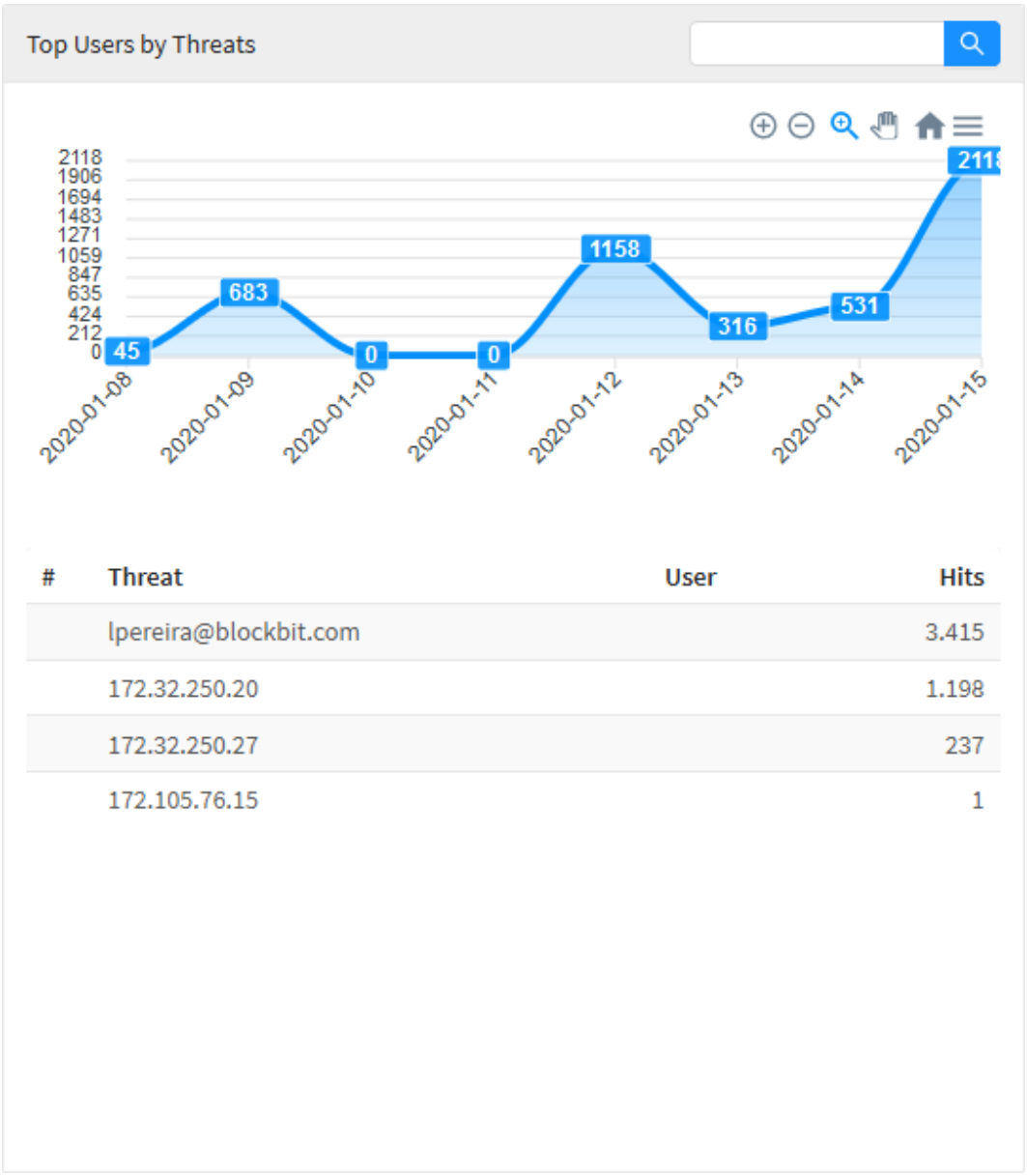


Threat Protection – Top Threat Types - Resumo

UTM - Threat Protection - Top Users by Threats

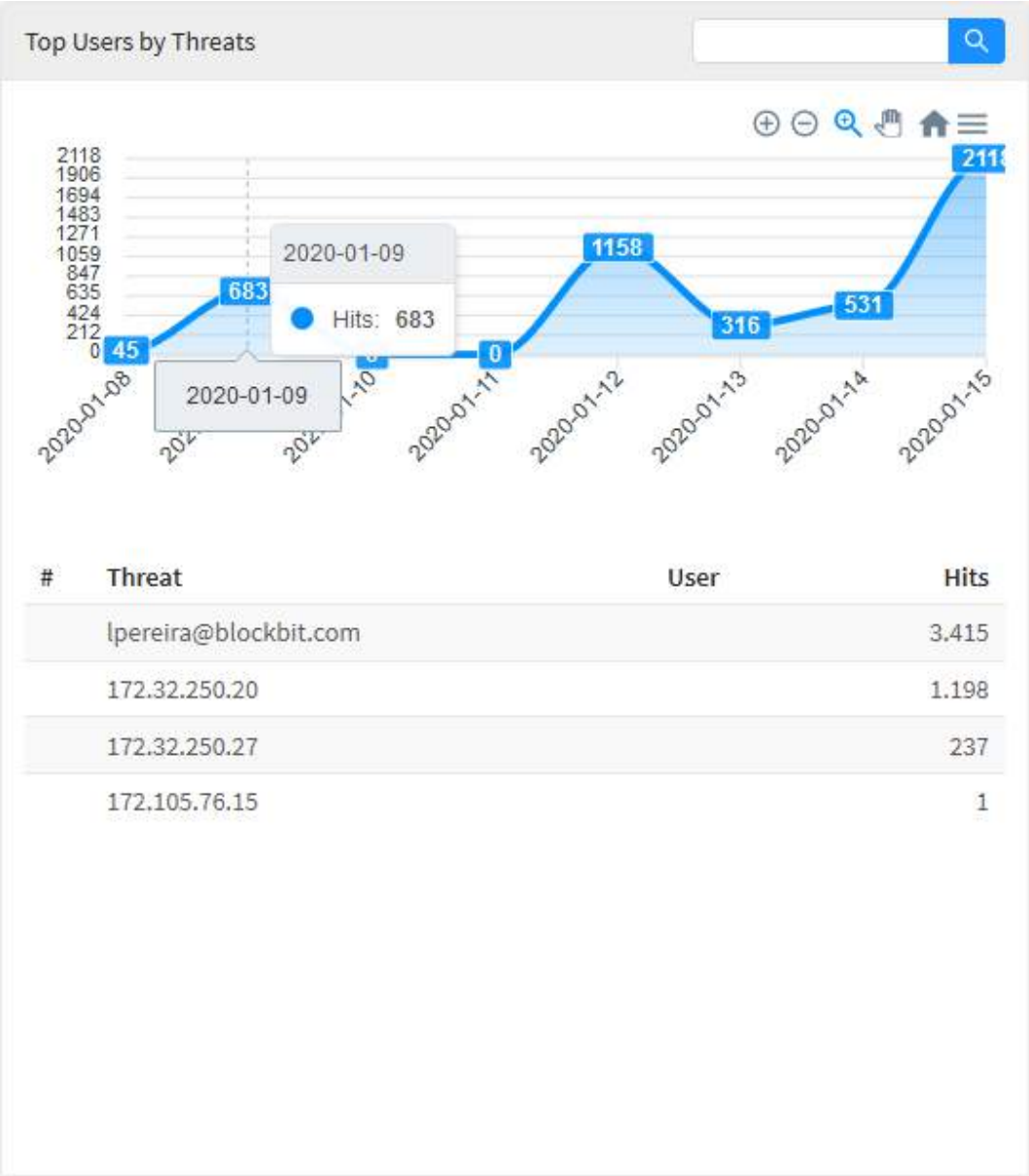
Em “*Top Users by Threats*” temos um gráfico de linha exibindo a quantia de ameaças por dia, ao passar o mouse sobre cada parte do gráfico, ele o destacará e exibirá um número com a quantia de ameaças do dia selecionado. Logo abaixo do gráfico, temos uma listagem dos dez usuários que mais foram afetados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



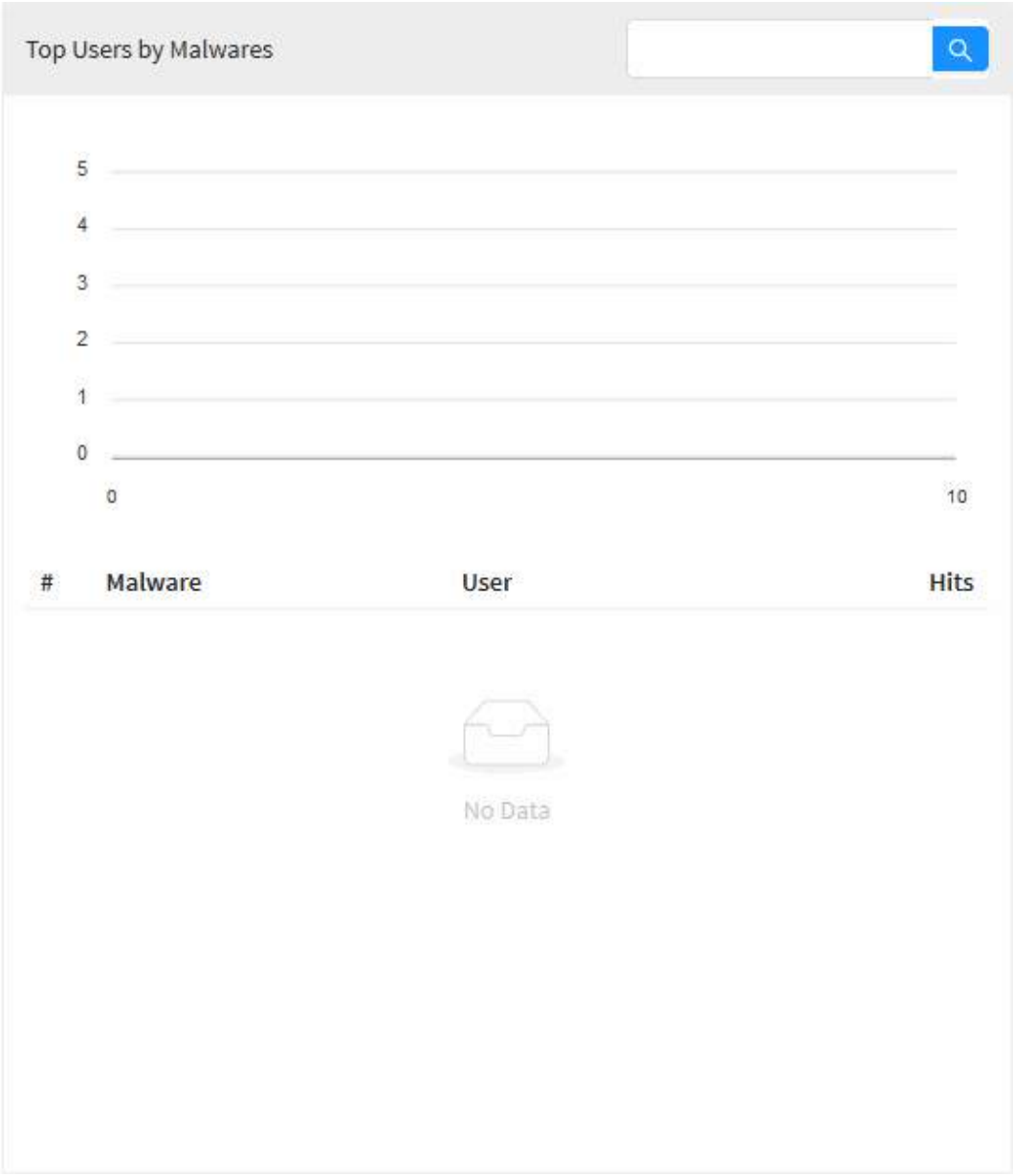
#	Threat	User	Hits
	lpereira@blockbit.com		3.415
	172.32.250.20		1.198
	172.32.250.27		237
	172.105.76.15		1

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 *IP*s, 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.

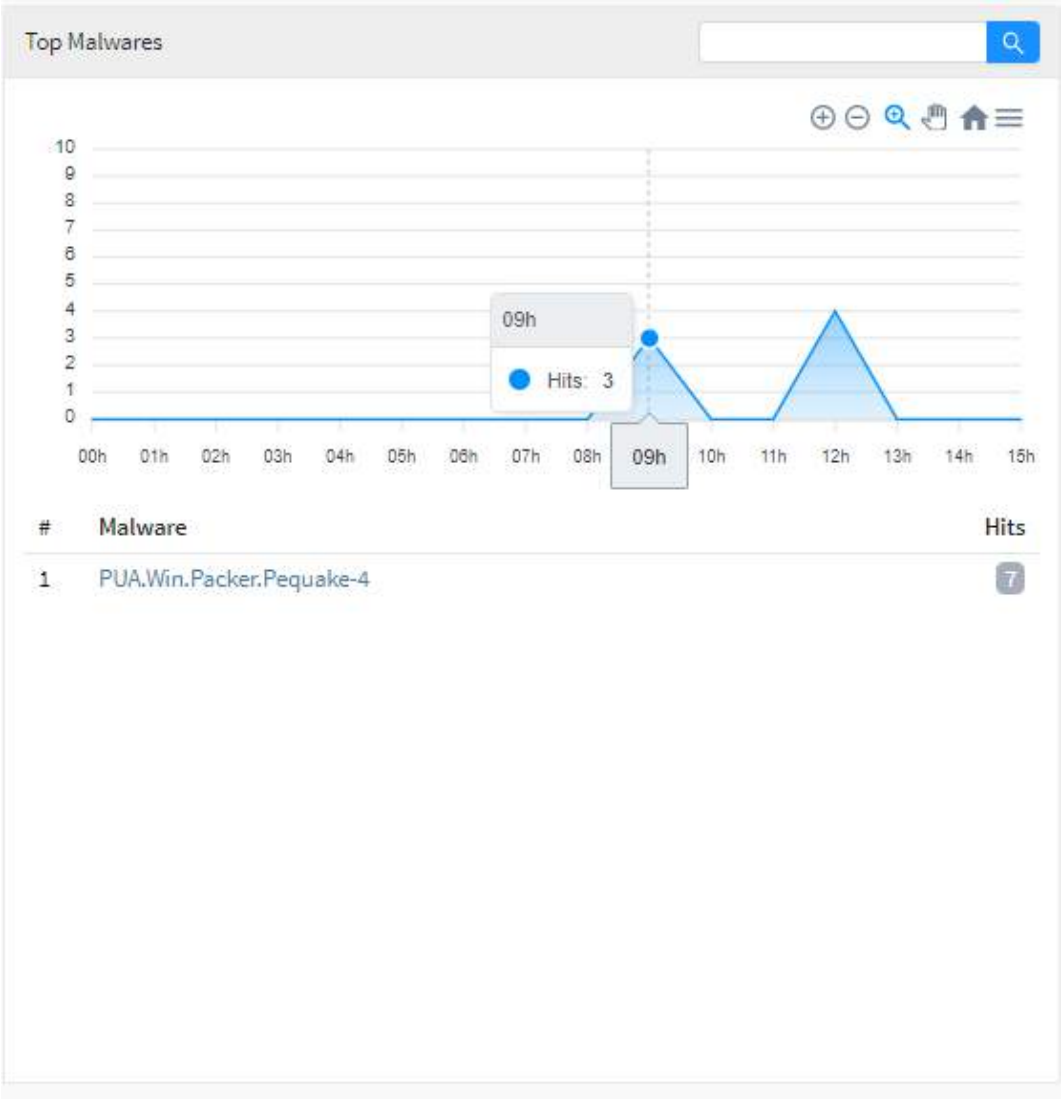


Threat Protection – Top Users by Malware

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.

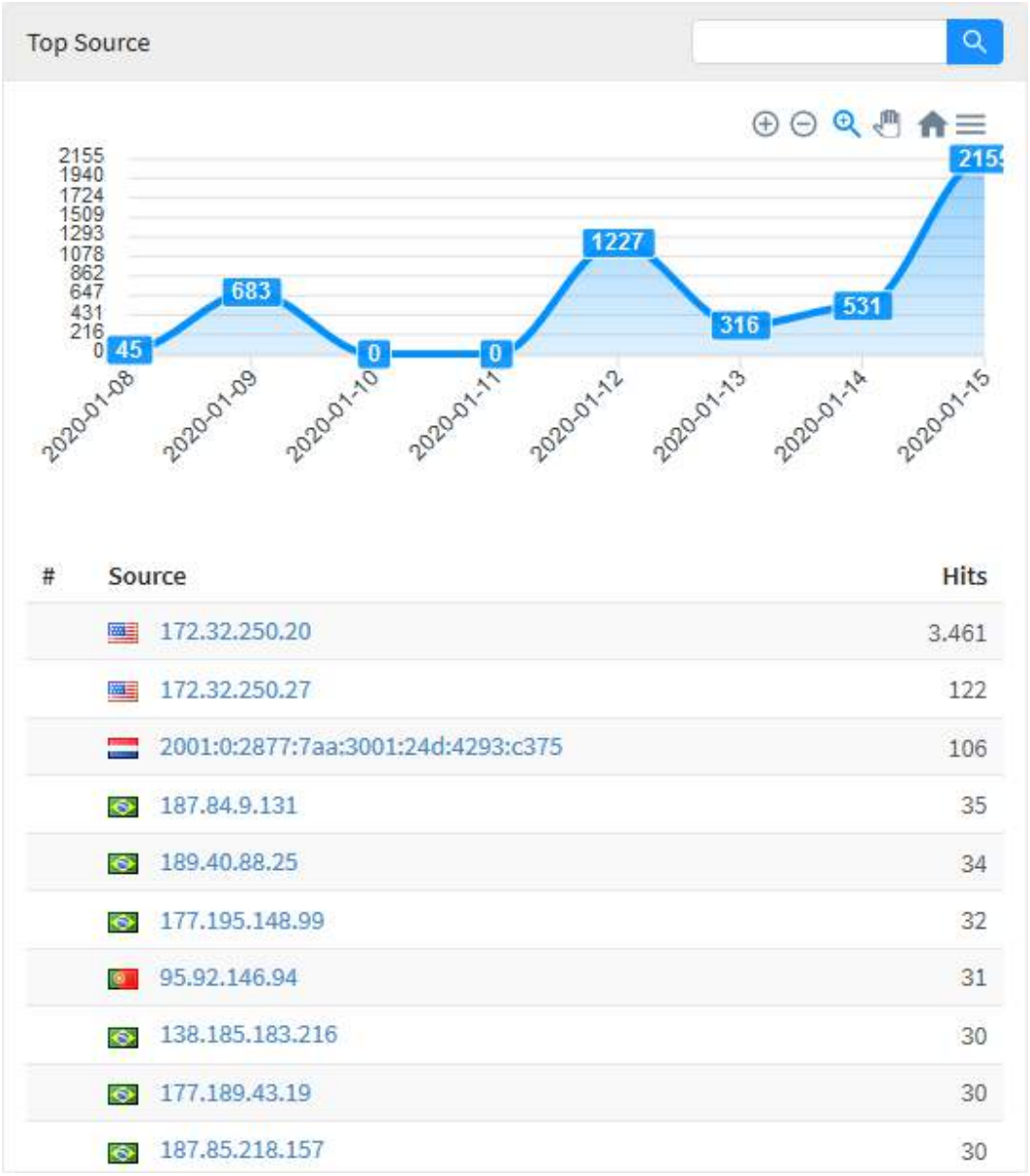
Para mais informações a respeito da barra de busca presente no topo deste gráfico cheque esta página.

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

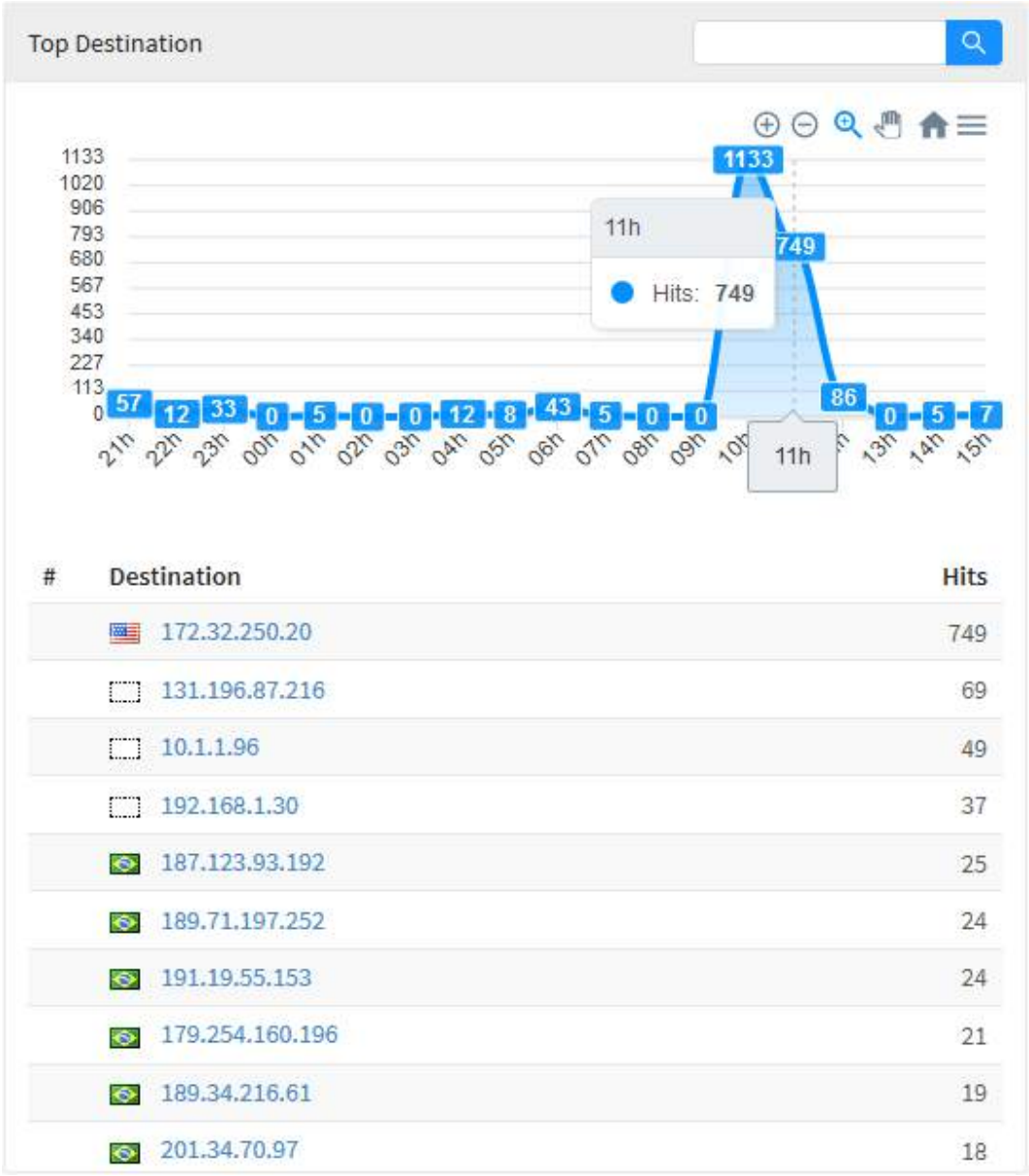
UTM - Threat Protection - Top Destination

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:

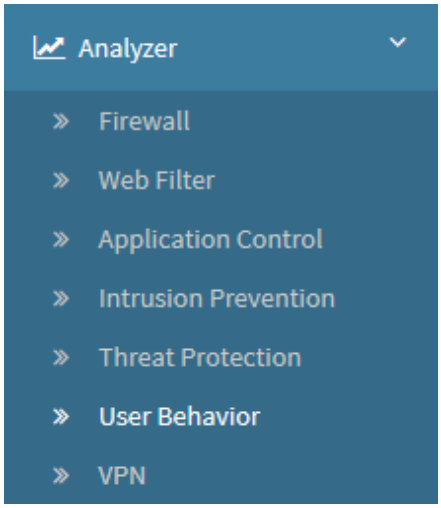


#	Destination	Hits
	172.32.250.20	749
	131.196.87.216	69
	10.1.1.96	49
	192.168.1.30	37
	187.123.93.192	25
	189.71.197.252	24
	191.19.55.153	24
	179.254.160.196	21
	189.34.216.61	19
	201.34.70.97	18

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

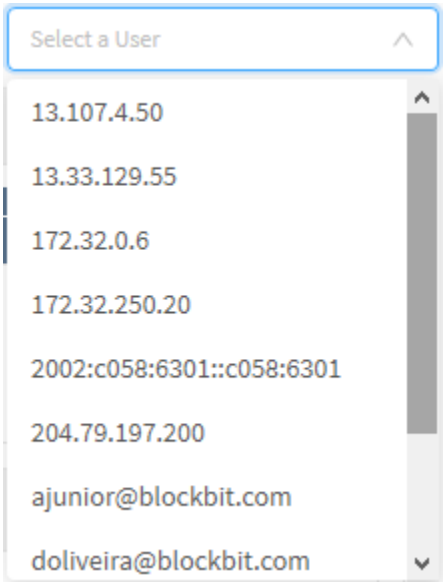
O relatório “User Behavior” é um resumo do comportamento de determinado usuário de um dispositivo, informando o IP do usuário, hostname da máquina, o Sistema Operacional que o usuário utiliza e uma classificação geral das ameaças (dispostas em "top 10"), sendo possível extrair um relatório dentro de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

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.

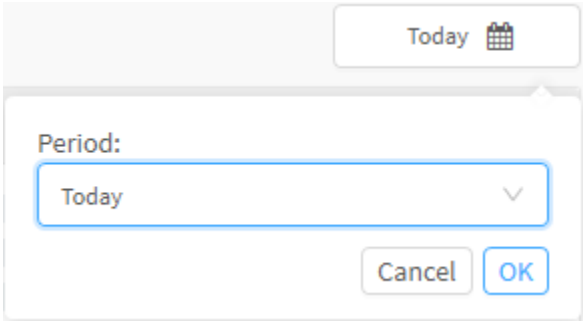


Selecionando *o usuário.*

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:



Seleção de Data

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

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;
- **[]:** 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 []**.

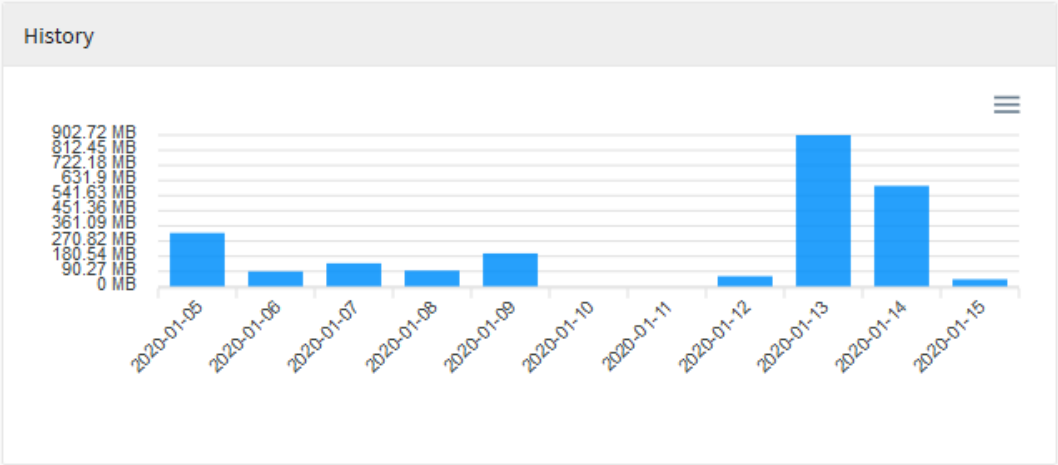
A seguir, analisaremos cada um desses relatórios em detalhe:

- *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.



User Behavior - History

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.

Analysis Panel

Network Traffic

Total Traffic

2.37 GB

Top Services

#	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 Source

#	Source	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

Top Destination

#	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

Policy Usage

Policy Tags

w SSL

Top Profiles

#	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

Application Usage

Total Application

1.74 KB

Top Applications

#	Applications	Hits
1	CDN - Content Delivery Network	1.043
2	Microsoft Update	547
3	HTTP	50
4	Google API SSL	48
5	MSN	18

Web Usage

Total Traffic

0

Allowed Sites

0

Denied Sites

0

Top Categories

#	Categories	Hits
1	Information Technology	1.628
2	Search Engines and Portals	763
3	Freeware and Software Download	527
4	Business and Economy	145
5	Web Hosting	91

Top Destination

#	Ip	Hits
1	2.23.98.145	476
2	201.0.217.42	449
3	13.107.4.50	273
4	52.114.142.2	117
5	191.252.51.215	111

THREAT PROTECTION

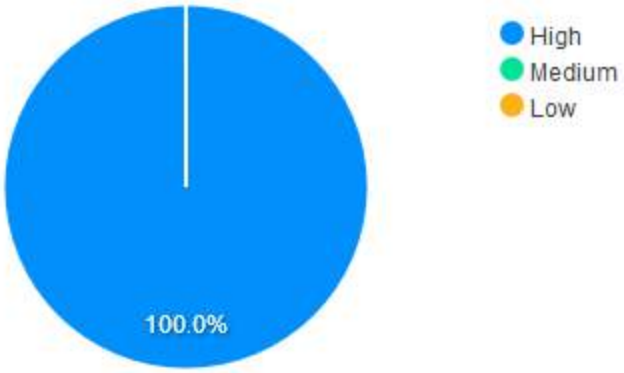
Total Threats

1,198

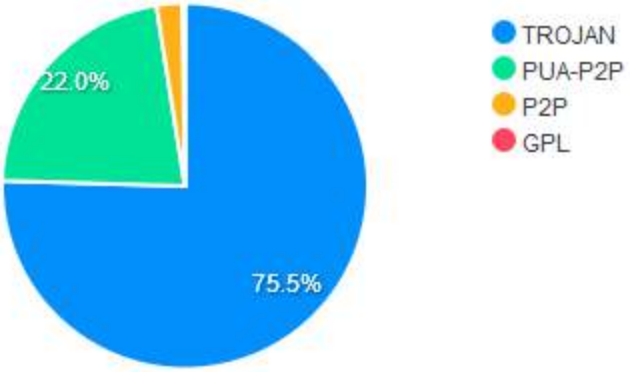
Total Malwares

0

Impacts



Malicious IP Classification



Top Threats

#	Threats	Hits
1	TROJAN Possible 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

Top Malwares

#	Malwares	Hits

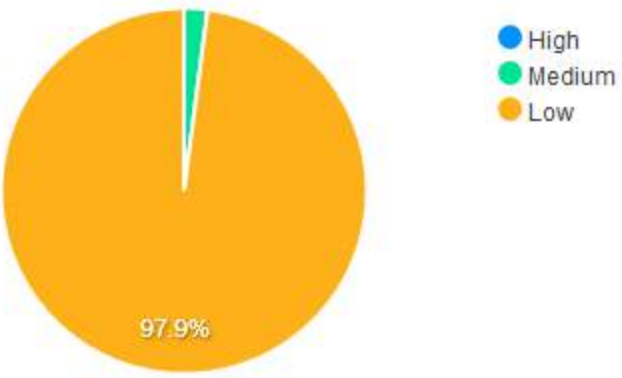
No Data

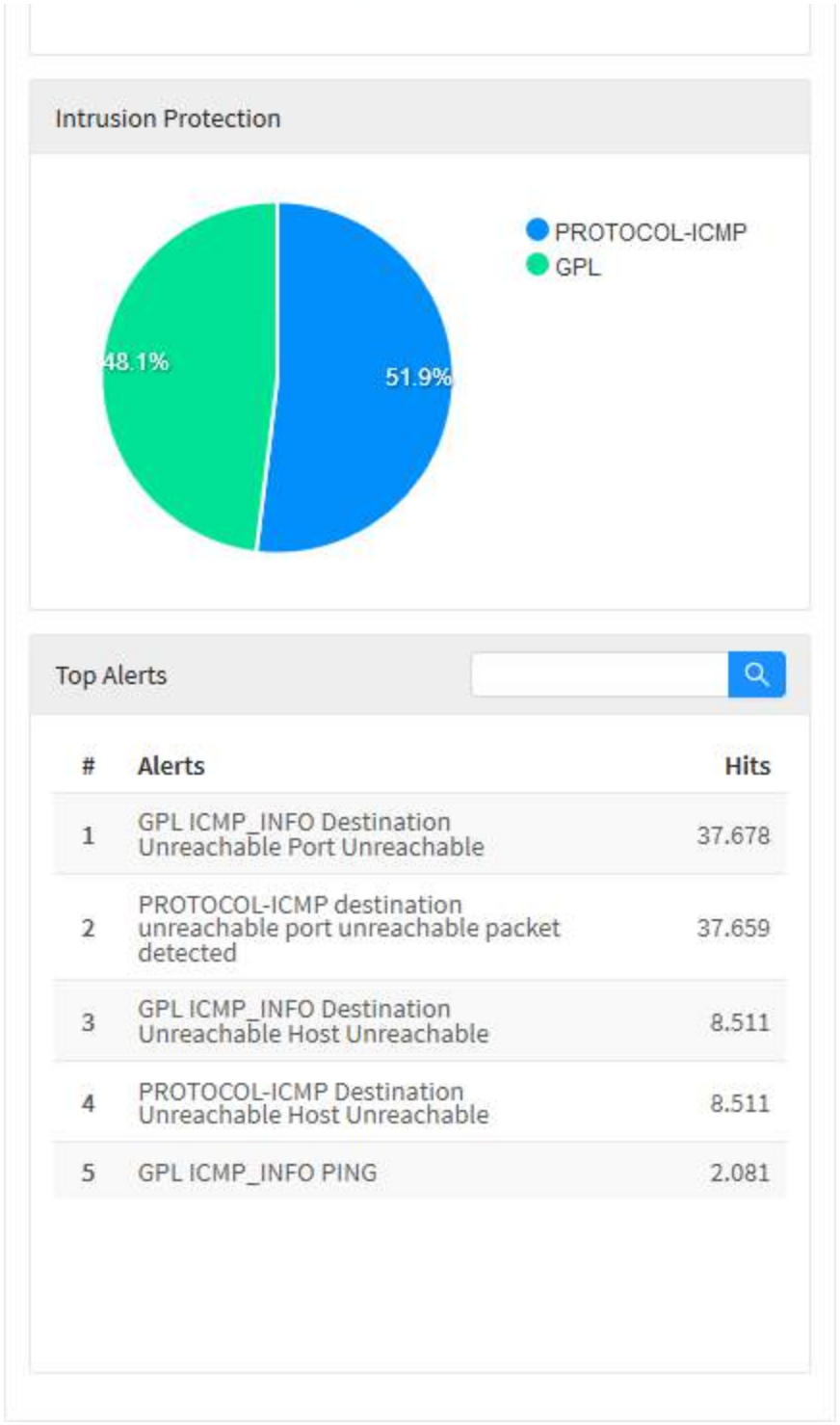
INTRUSION PREVENTION

Total Alerts

100,666

Impacts





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

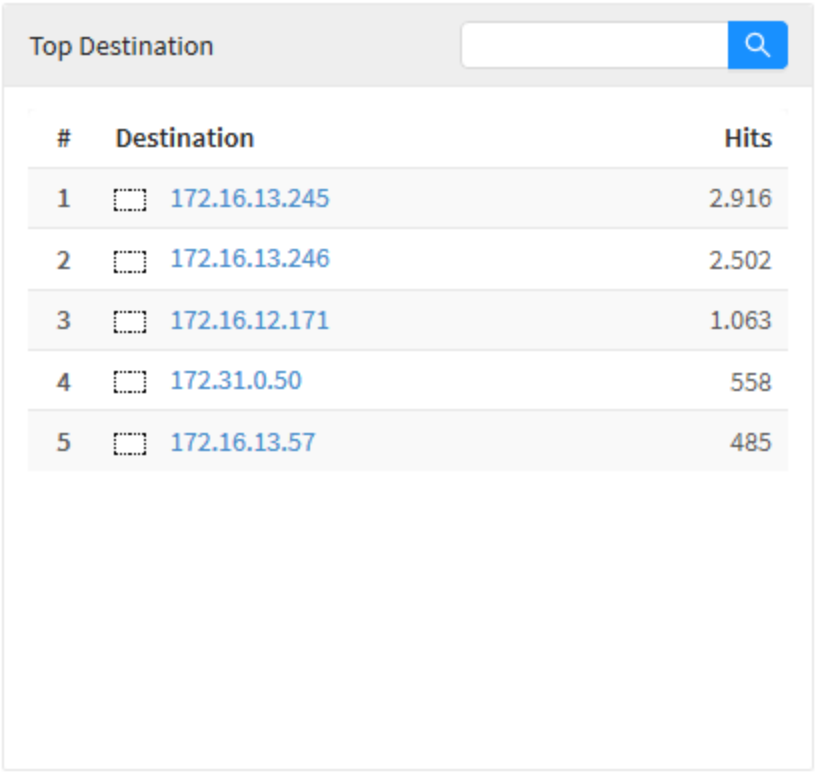
2.37 GB

Top Services

#	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 Source

#	Source	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

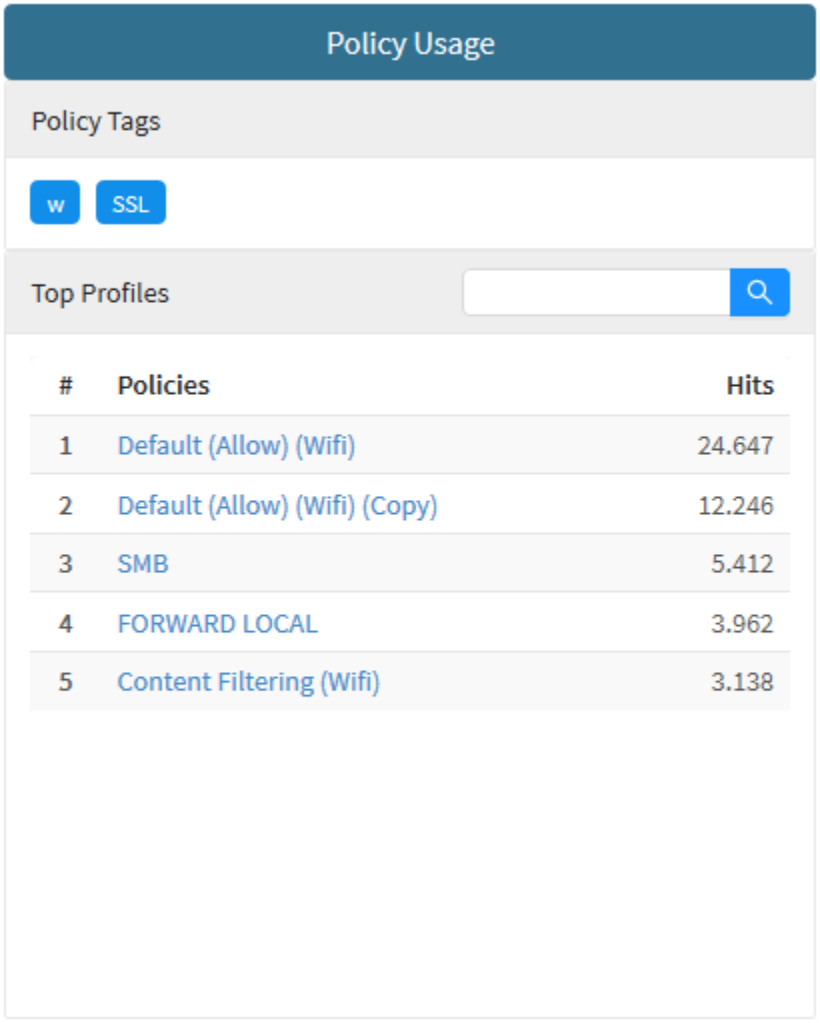


User Behavior - Analysis Panel - Network Traffic

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.

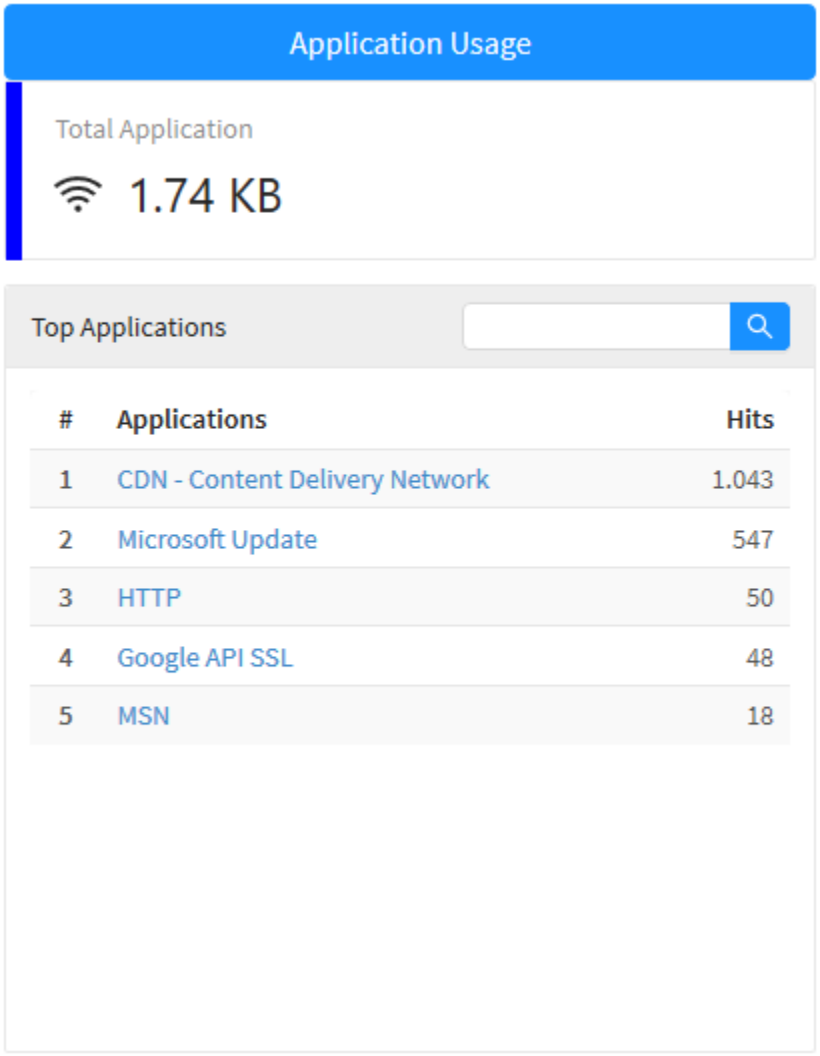


Analysis Panel - Policy Usage

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.



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

0

Allowed Sites

0

Denied Sites

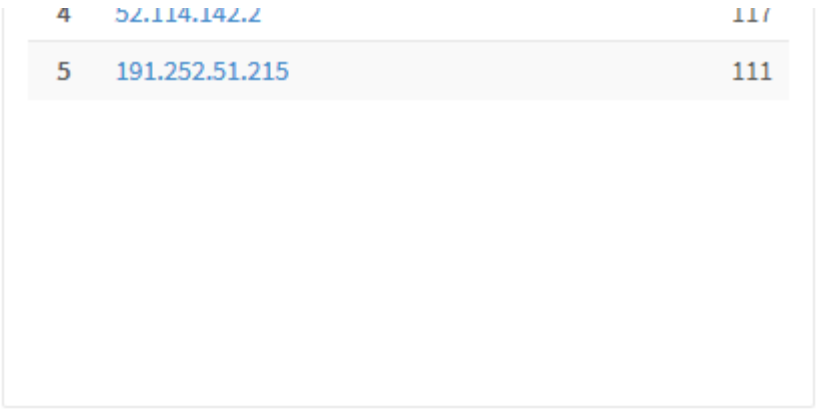
0

Top Categories

#	Categories	Hits
1	Information Technology	1.628
2	Search Engines and Portals	763
3	Freeware and Software Download	527
4	Business and Economy	145
5	Web Hosting	91

Top Destination

#	Ip	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.

THREAT PROTECTION

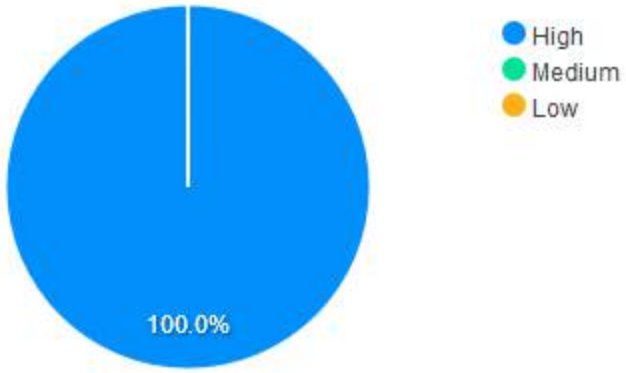
Total Threats

1,198

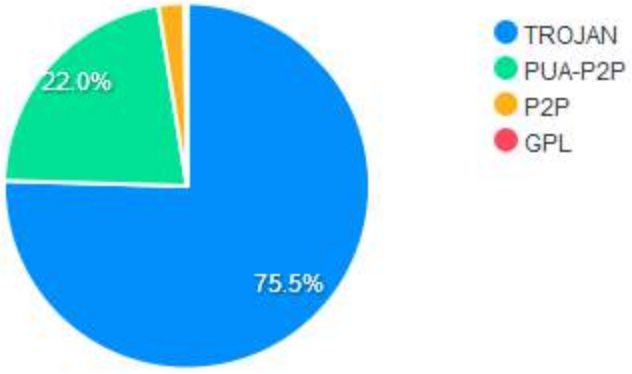
Total Malwares

0

Impacts



Malicious IP Classification



Top Threats

#	Threats	Hits
	TROJAN Possible	

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

Top Malwares

#	Malwares	Hits

No Data

Analysis Panel - Threat Protection

UTM - User Behavior - Analysis Panel - Intrusion Prevention

Em “*Intrusion Prevention*” temos:

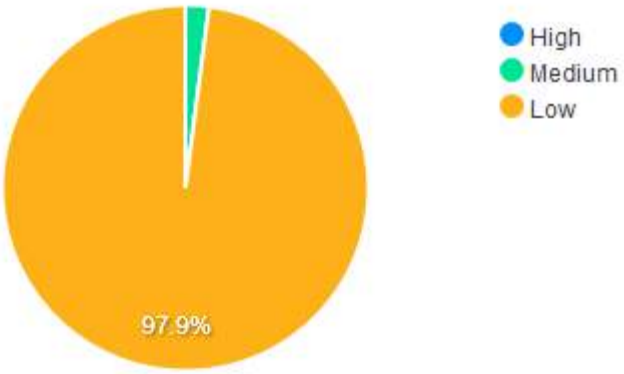
“*Total Alerts*” exibindo o total de alertas referentes a esse usuário, em “*Impacts*” temos os níveis de impacto dos alertas previamente citados, “*Intrusion Protection*” exibe um gráfico de rosca onde é possível de se ver os tipos de invasão detectados pelo sistema e por fim, em “*Top Alerts*” temos uma listagem dos 5 alertas referentes a esse usuário e quantas vezes eles ocorreram.

INTRUSION PREVENTION

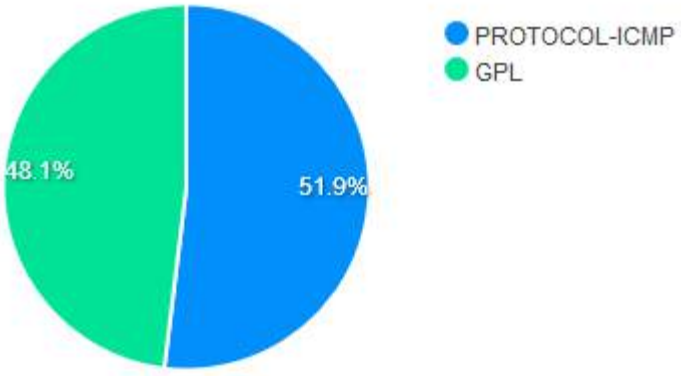
Total Alerts

100,666

Impacts



Intrusion Protection



Top Alerts

#	Alerts	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	37.678
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	37.659
3	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.511

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.

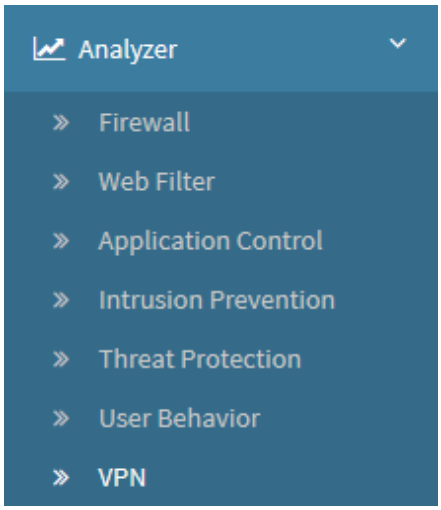
User Behavior - Geolocation

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*”.



VPN

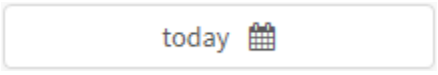
A função principal deste recurso é fornecer informações sólidas sobre as *VPNs* da rede, possibilitando ter uma visão holística da estrutura, facilitando um gerenciamento integrado e resposta rápida em caso de alguma eventualidade. Neste painel temos os seguintes relatórios estatísticos das *VPN*:

- 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:



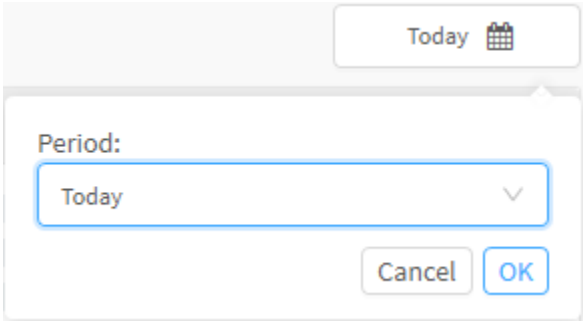
VPN - Caixa de seleção de data

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;

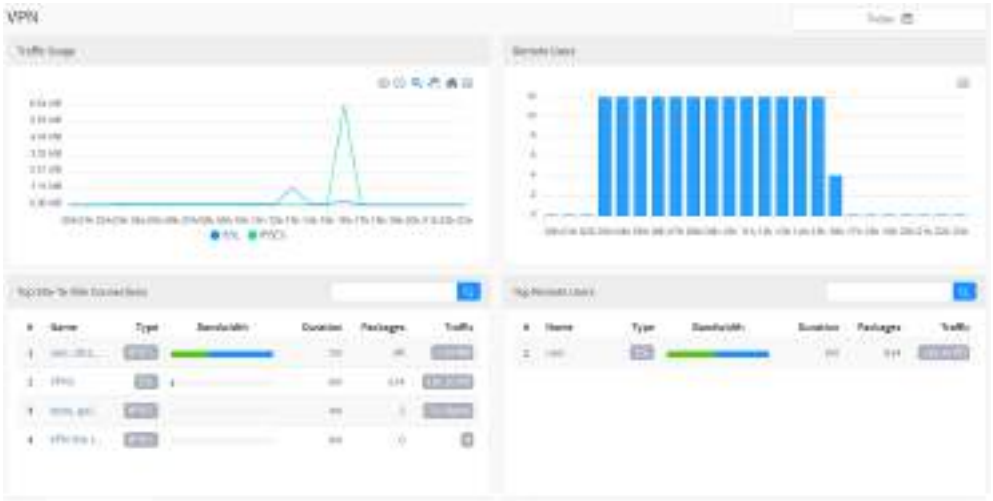
- **Last month:** Exibe os resultados do último mês.

Selecione o período desejado:



VPN - Seleção de Data

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



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;
- **[ ]:** 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.

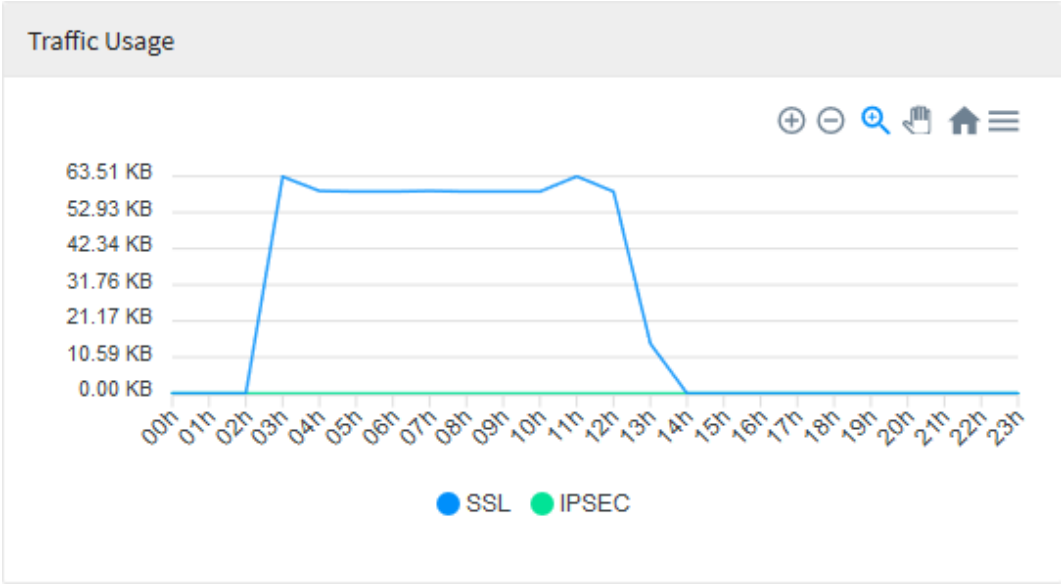
Para efetuar uma pesquisa, digite um termo na barra de busca e clique no **botão de busca [ ]**.

A seguir, iremos analisar cada painel desta página.

- *Traffic Usage;*
- *Remote User;*
- *Top Site-to-Site;*
- *Top Remote User.*

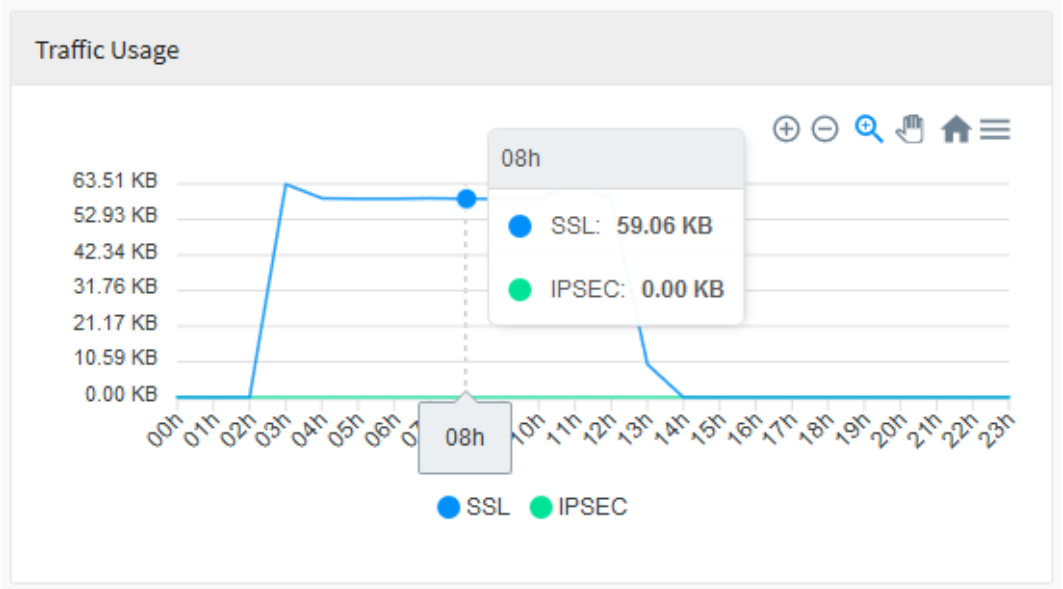
UTM - VPN - Traffic Usage

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

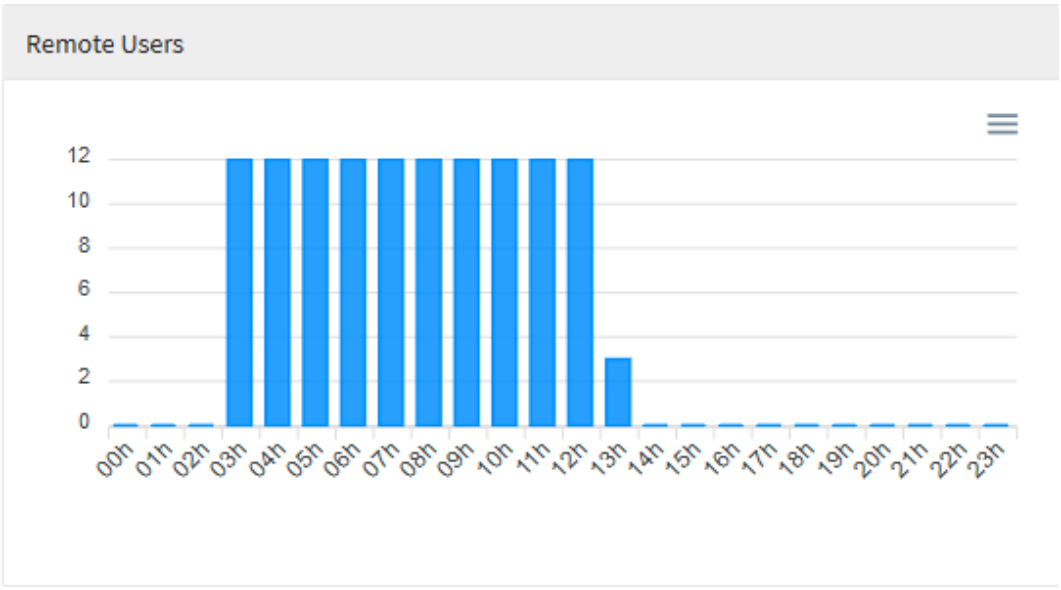
Ao passar o mouse por cima do gráfico, um resumo de todo o tráfego do período é exibido, conforme demonstrado na imagem abaixo:



Analyzer – VPN - Traffic usage - Detalhes

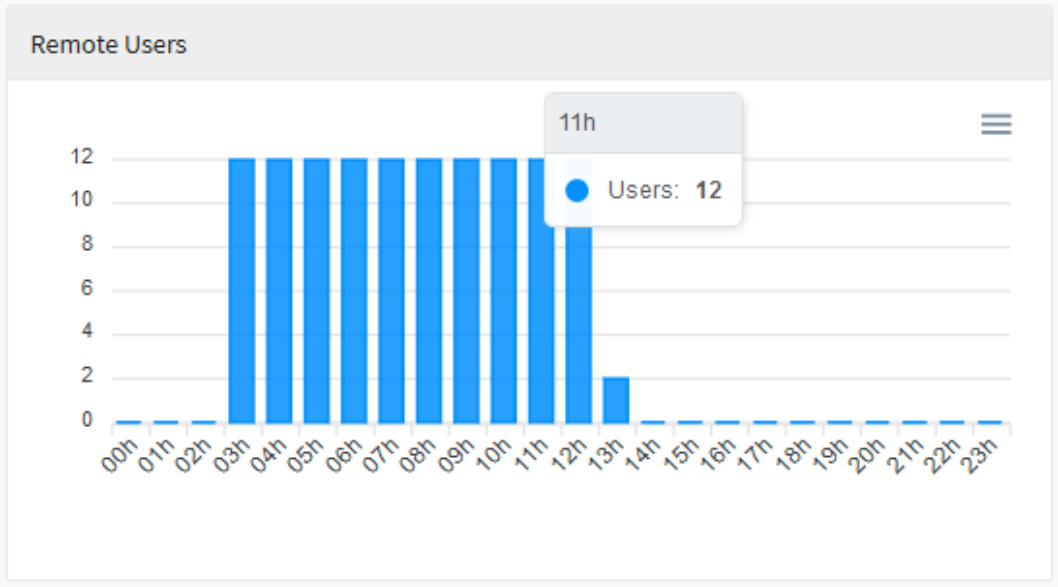
UTM - VPN - Remote User

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.

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.

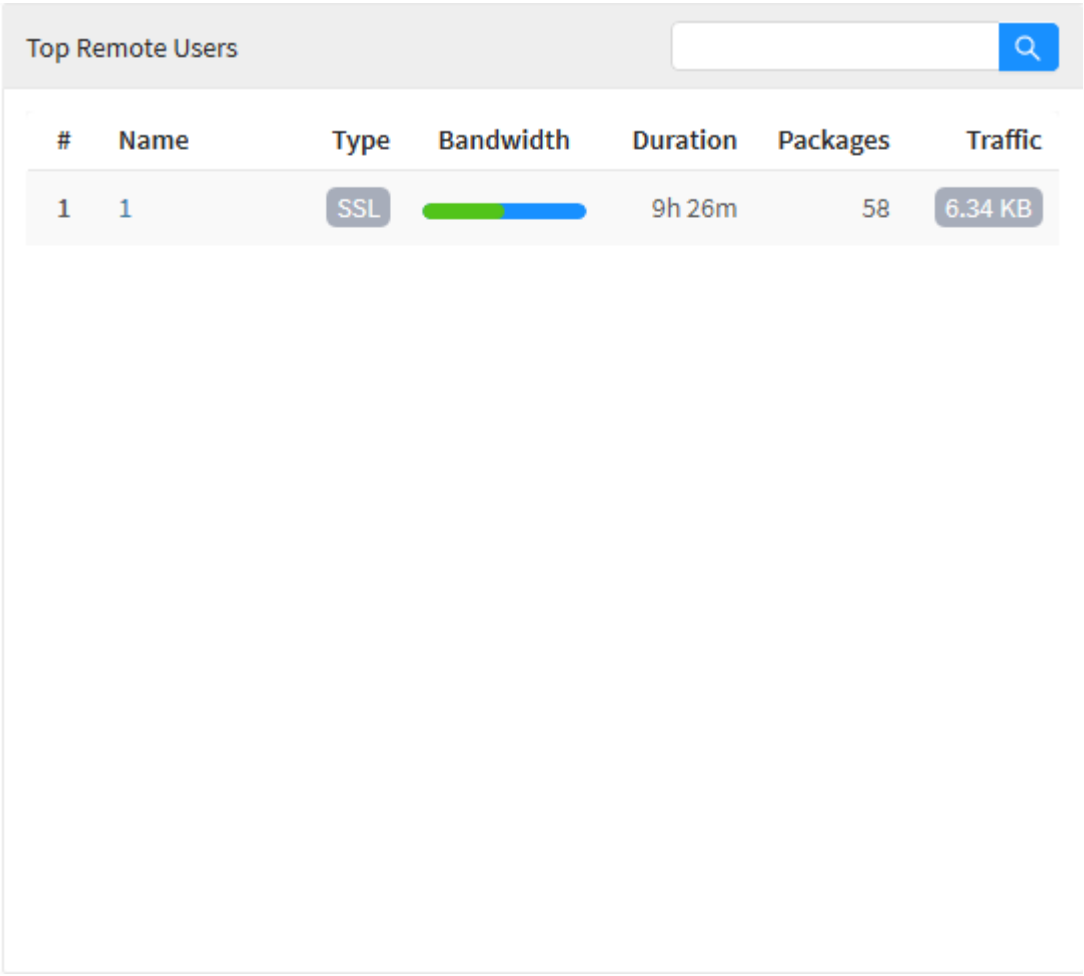
Analyzer – VPN - Top Site-to-Site Connections Search

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.*

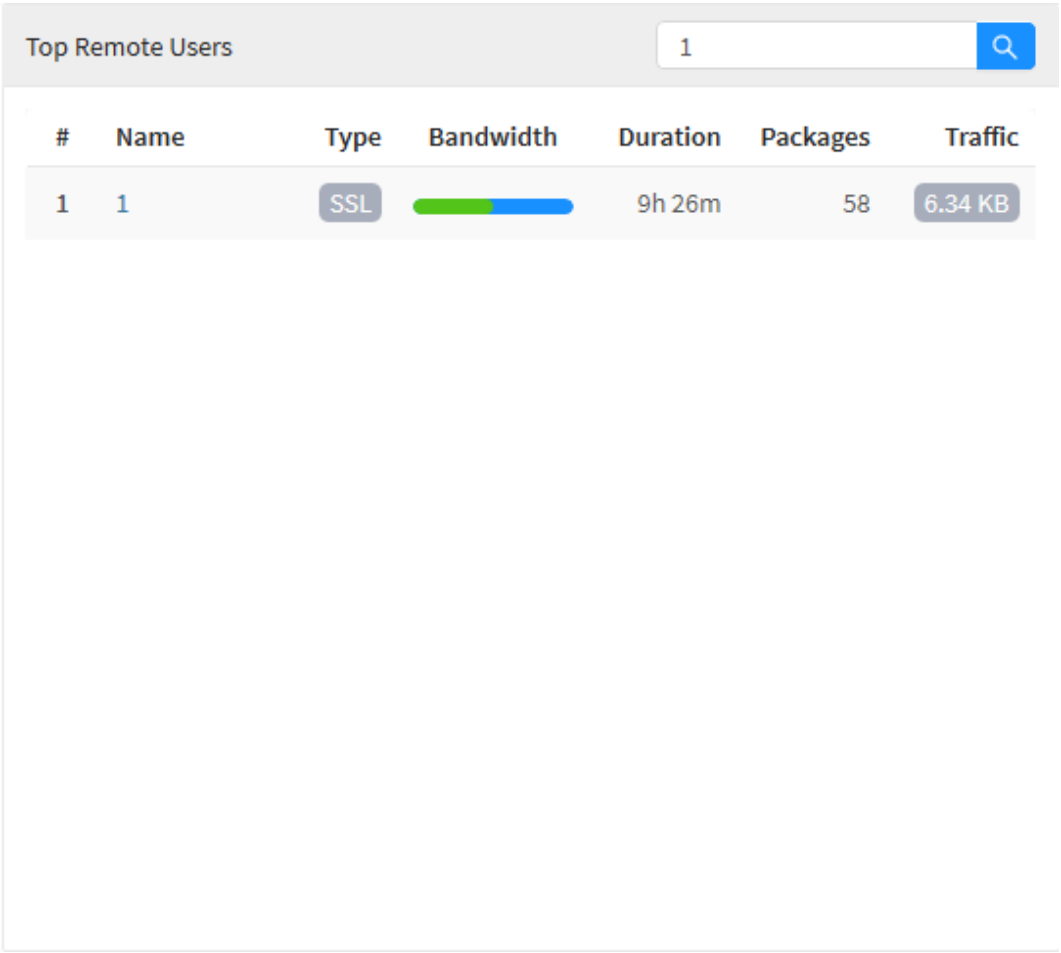
UTM - VPN - Top Remote User

O painel "*Top Remote User*" tem como função exibir as informações estatísticas referentes aos usuários remotos.



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.



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"*:

Tabela 1 - Ações de uma Política

Ações	
Allow	Permitir
Deny	Negar
Reject	Rejeitar

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

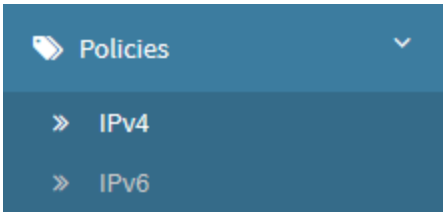
Contém as opções:

- 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*";



Opção *IPv4*

Surgirá a Tela de "*Policies IPv4*", conforme demonstrado pela imagem a seguir:

IPv4

Esta seção irá se aprofundar em:

- Criação de grupos de políticas;
- Cadastro e Remoção de políticas.

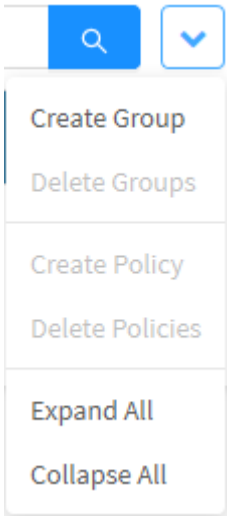
A seguir, vamos analisar cada componente deste painel.

IPv4 - Menu de ações

No topo direito da tela temos o menu de ações:

IPv4 – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



IPv4 – Menu de ações

O menu é composto das seguintes opções:

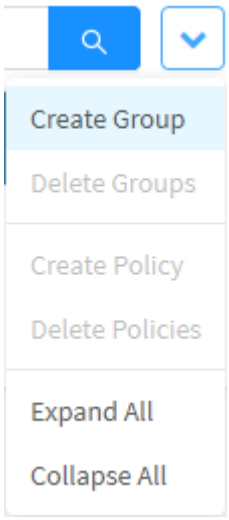
- *Create Group*;
- *Delete Groups*;
- *Create Policy*;
- *Delete Policies*;
- *Expand All* e *Collapse All*.

A seguir cada opção do menu de ações será detalhada.

IPv4 - Menu de ações - Create Group

Através da opção “*Create Group*” é possível criar um novo grupo. Para acessar, clique no **menu de ações [ ]**.

1. Clique na opção “*Create Group*”;

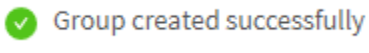


IPv4 - Menu de ações - *Create Group*

2. A tela “*Create Group*” será exibida. Adicione o nome do grupo desejado:

IPv4 – Create Group

Após nomear o grupo, caso deseje cancelar clique no botão ***Cancel*[** Cancel **]**. Para concluir a criação do grupo clique no botão ***Save*[** Save **]**.



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.

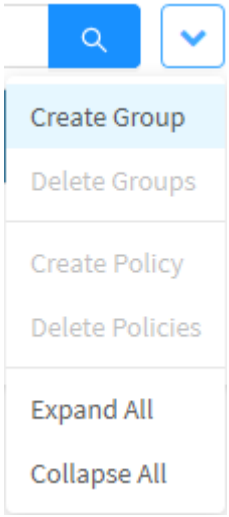
Efetuaremos a demonstração criando os seguintes grupos:

- *Block;*
- *Forward;*
- *Masking (NAT);*
- *Web Filter.*

Grupo: *Block*

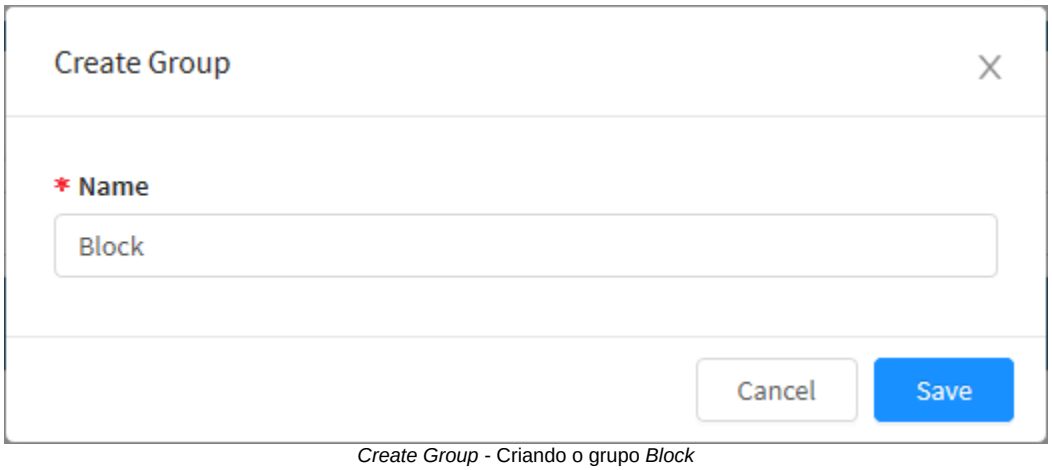
Finalidade: Definir as políticas para aplicar o *"bloqueio"* imediato e definitivo de tráfegos específicos já conhecidos como INAPROPRIADOS. Sem a intervenção de "*proxies*".

Para adicionar os grupos de políticas, acesse o **menu de ações[**  **]** e selecione a opção ***[Create Group]***.



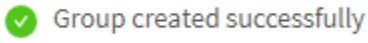
IPv4 - Menu de ações - *Create Group*

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:



Create Group - Criando o grupo *Block*

Após ter digitado o nome indicado, clique no botão **[** Save **]**;



Group created successfully

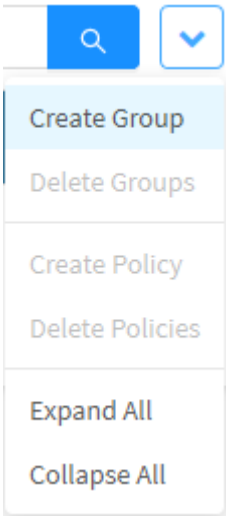
O grupo foi criado com sucesso.

Grupo: *Forward* (*FW*)

Finalidade: Definir as políticas de gerenciamento do tráfego entre as redes/ subredes internas.

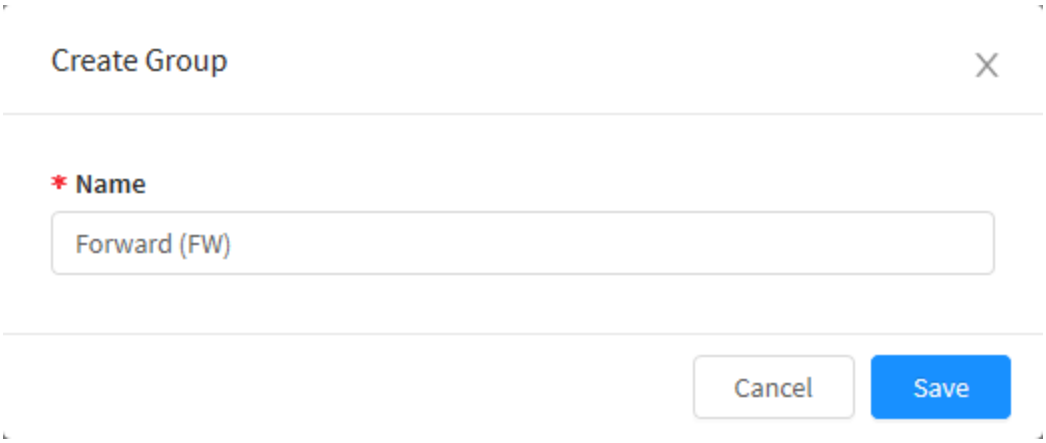
Neste grupo vamos definir políticas de *"bloqueio"* do tráfego não autorizado, para detecção e geração de *"log"* e políticas de *"Greylist"*, ou seja, permitir o tráfego inicialmente classificado como "confiável", no entanto com a condição de "Inspecionar" o tráfego e validar a sua legitimidade e aplicar 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]***.



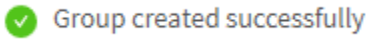
IPv4 - Menu de ações - *Create Group*

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:



Create Group - Criando o grupo *Forward*

Após ter digitado o nome indicado, clique no botão **[**  **]**;



Group created successfully

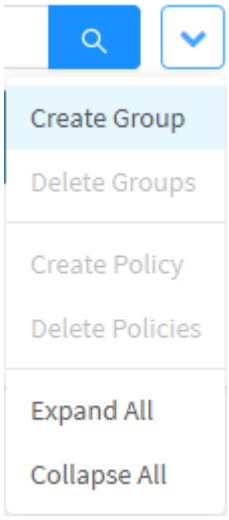
O grupo foi criado com sucesso.

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]***.

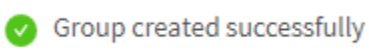


IPv4 - Menu de ações - *Create Group*

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:

Create Group - Criando o grupo *Masking (NAT)*

Após ter digitado o nome indicado, clique no botão **[Save]**;



Group created successfully

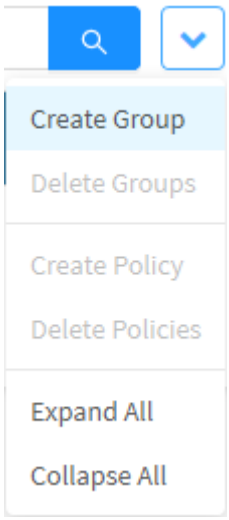
O grupo foi criado com sucesso.

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*".*

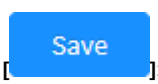
Para adicionar os grupos de políticas, acesse o **menu de ações[**  **]** e selecione a opção ***[Create Group]***.

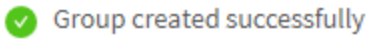


IPv4 - Menu de ações - *Create Group*

Para efetuar este exemplo, crie o grupo, como exemplificado na imagem a seguir:

Create Group - Criando o grupo *Web Filter*

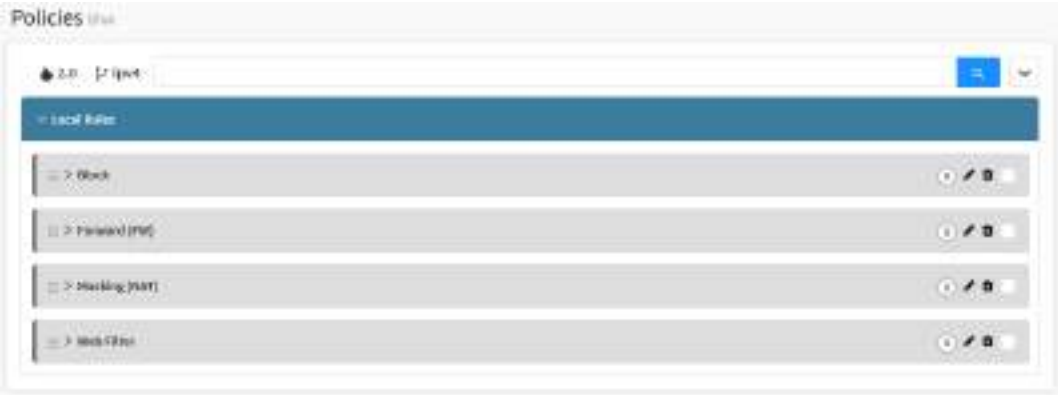
Após ter digitado o nome indicado, clique no botão **[**  **]**;



Group created successfully

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.



IPv4 – Policy Groups

Para ver o cadastro de algumas políticas básicas, acesse *Policies IPv4* - Exemplos - Criação de Políticas.

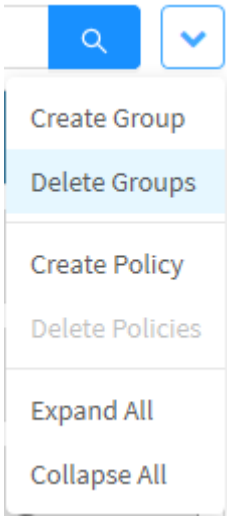
IPv4 - Menu de ações - Delete Groups

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:

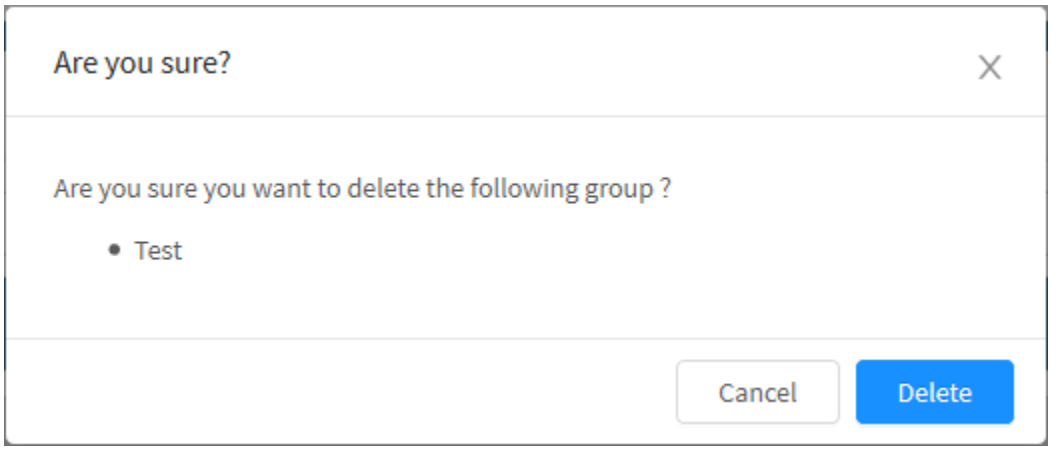
IPv4 – Delete Groups

2. Entre no **menu de ações [ ]** e clique no botão “*Delete Groups*”.



IPv4 – Menu de ações - *Delete Groups*

3. Surgirá a mensagem se deseja realmente deletar os pacotes selecionados:



IPv4 – Delete Groups

Caso deseje cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].

Group deleted succesfully

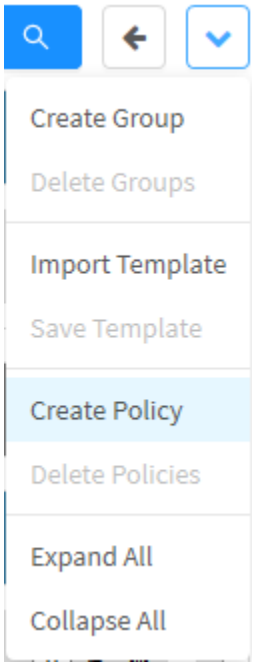
Após realizar esses procedimentos os grupos terão sido excluídos com sucesso.

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).

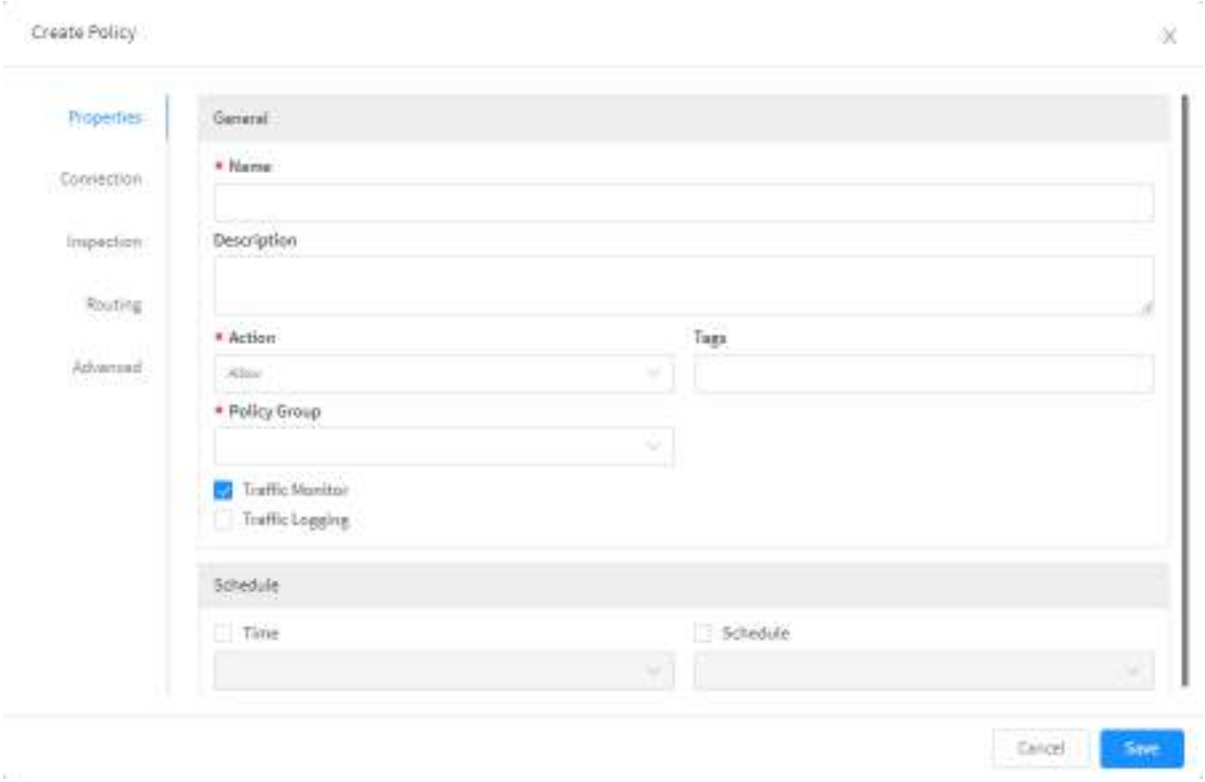
Para criar uma política, siga os passos:

1. No **menu de ações [ ]**, clique na opção “*Create Policy*”;



IPv4 - Menu de Ações - *Create Policy*

2. Surgirá a tela *Policy Form*;



IPv4 – Policy Form

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*

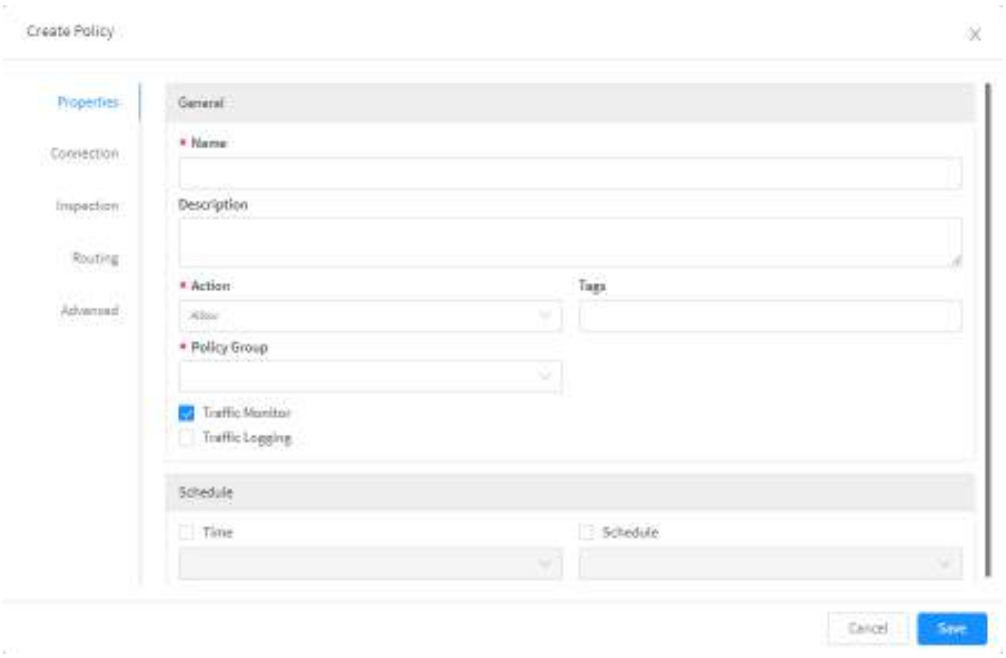
Nesta aba estão contidos os painéis:

- *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]**:*



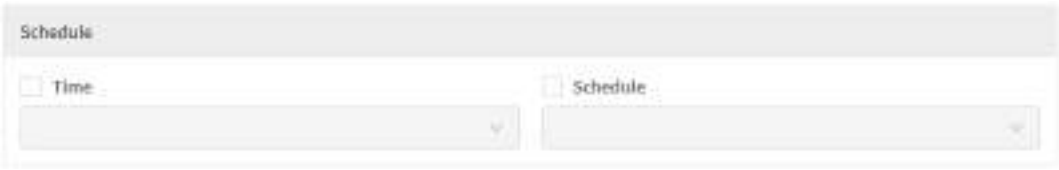
IPv4 – Properties - General

- ***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 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 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.

Schedule

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel **[Schedule]**:



IPv4 – Properties - Schedule

- ***Time[ ]*:** Caso a caixa de seleção estiver selecionada, determina se a regra se aplicará em dias úteis (“*Business*”), finais de semana (“*Weekend*”) 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.

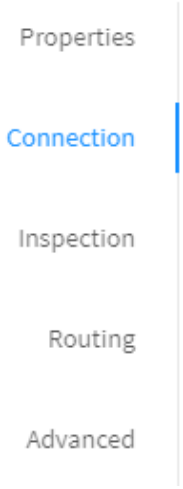
A seguir analisaremos o conteúdo da aba *Connection*.

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.

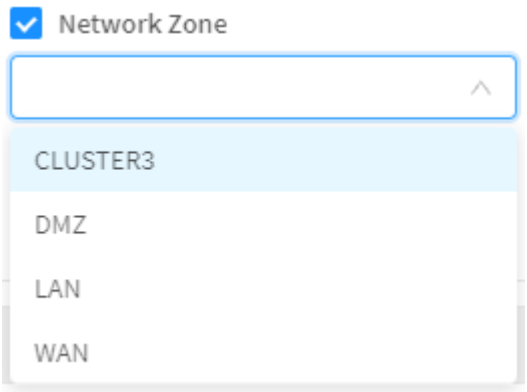
A seguir analisaremos a função de cada campo dos painéis.

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*]**:

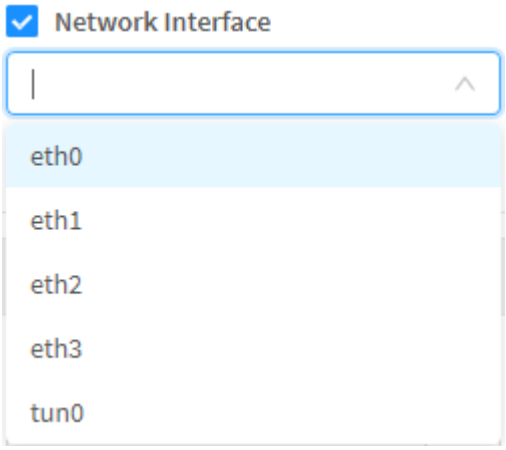
IPv4 – Connection - Source

- ***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 Cluster3, DMZ, *LAN e WAN* 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*;



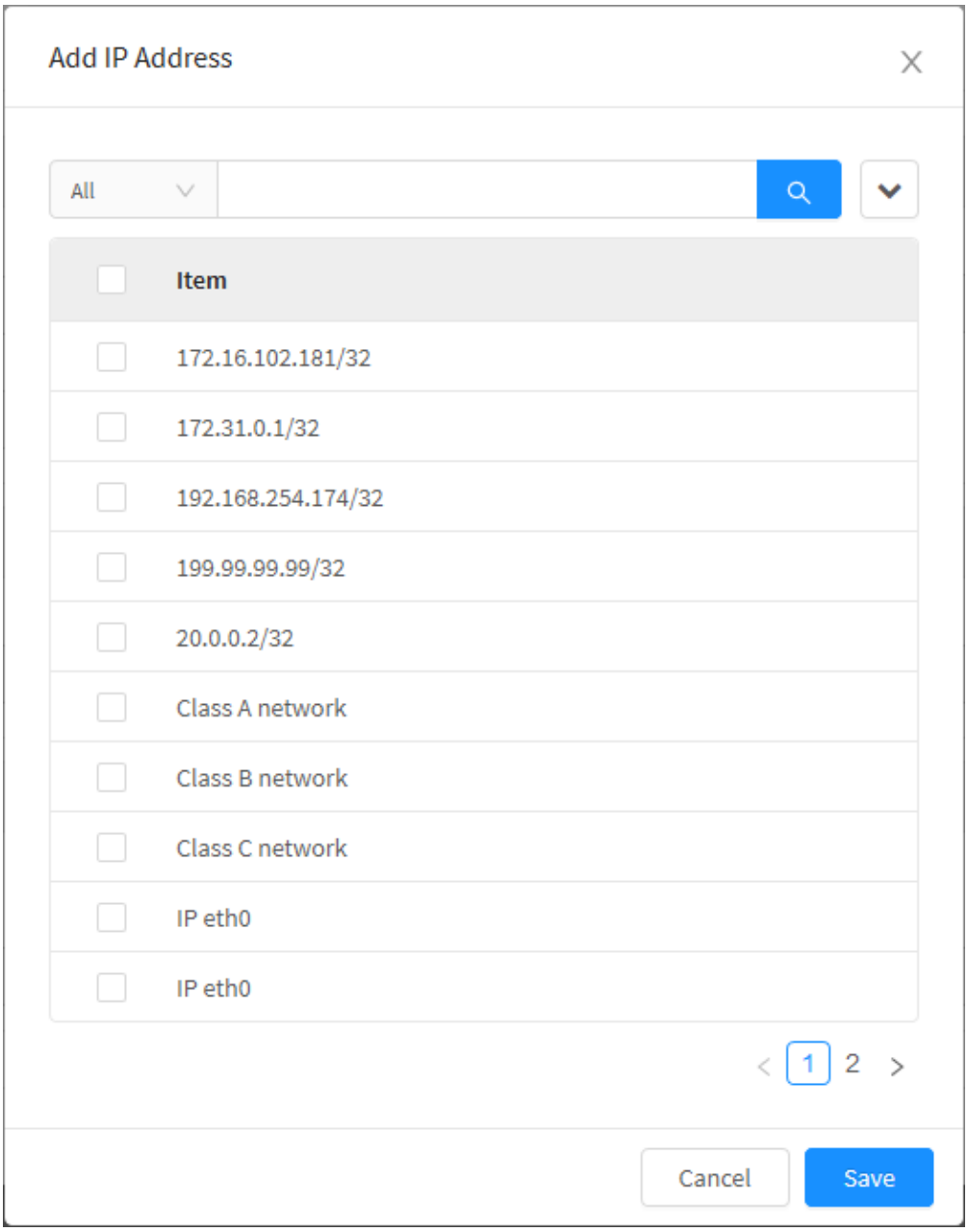
IPv4 – Connection - Source - Network Zone

- ***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;*



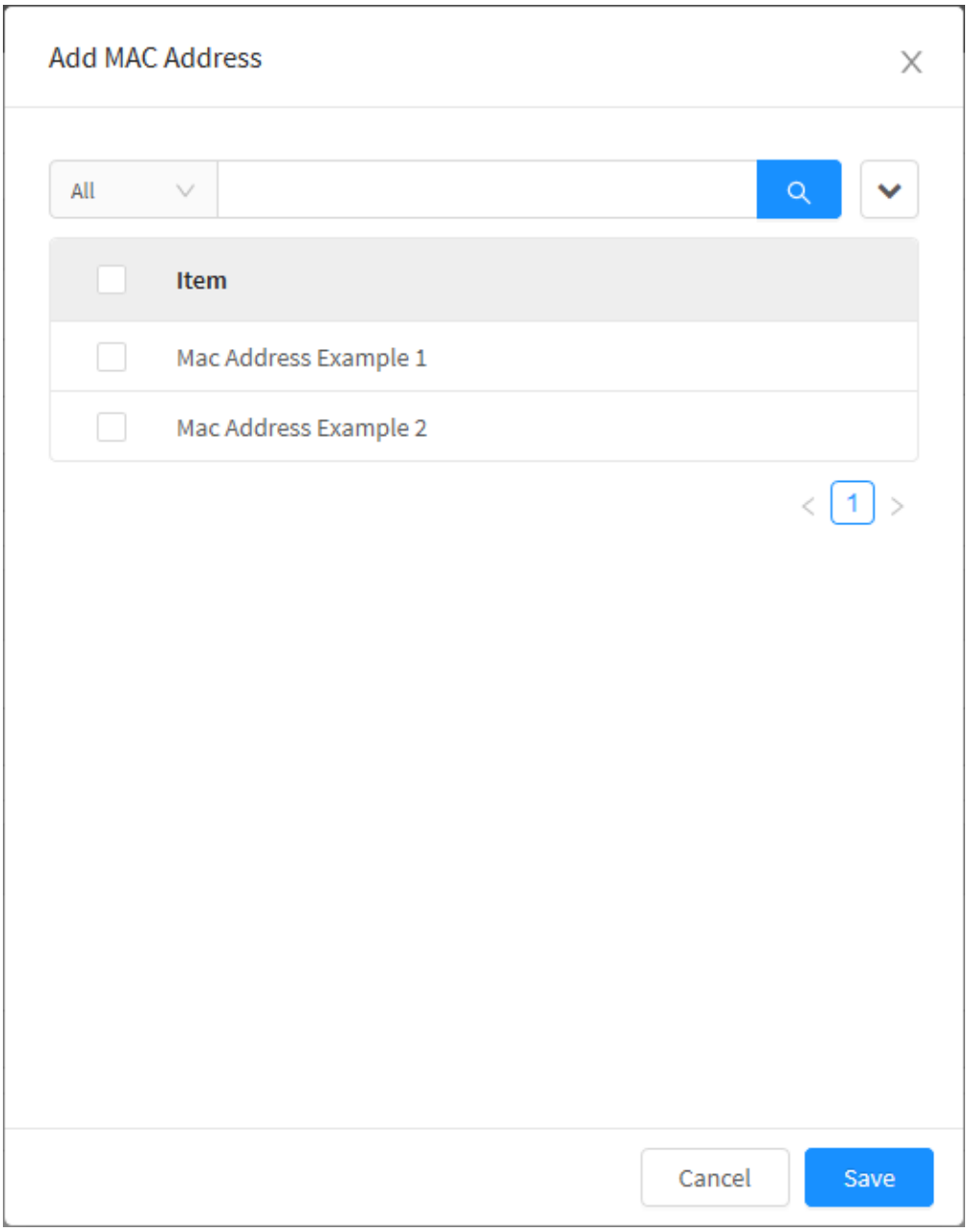
IPv4 – Connection - Source - Network Interface

- ***IP Address[ ]*:** 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*;



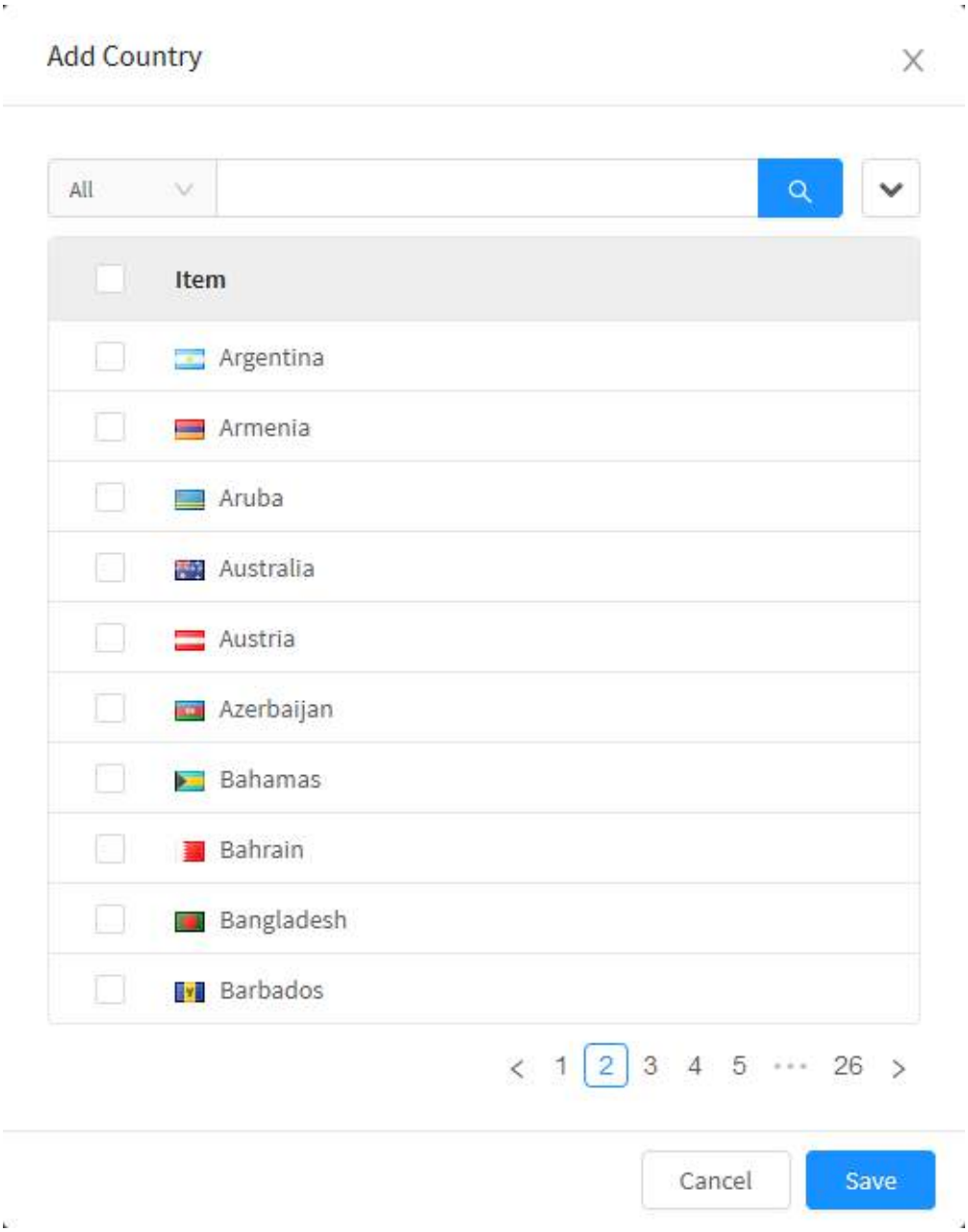
IPv4 – Connection - Source - IP Address

- ***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*;



IPv4 – Connection - Source - Mac Address

- ***Country[ ]*:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Países para serem usado como filtro de origem. Ao clicar sobre o botão **[ ]**, a tela abaixo será exibida para selecionar um ou mais país que irá compor a regra.



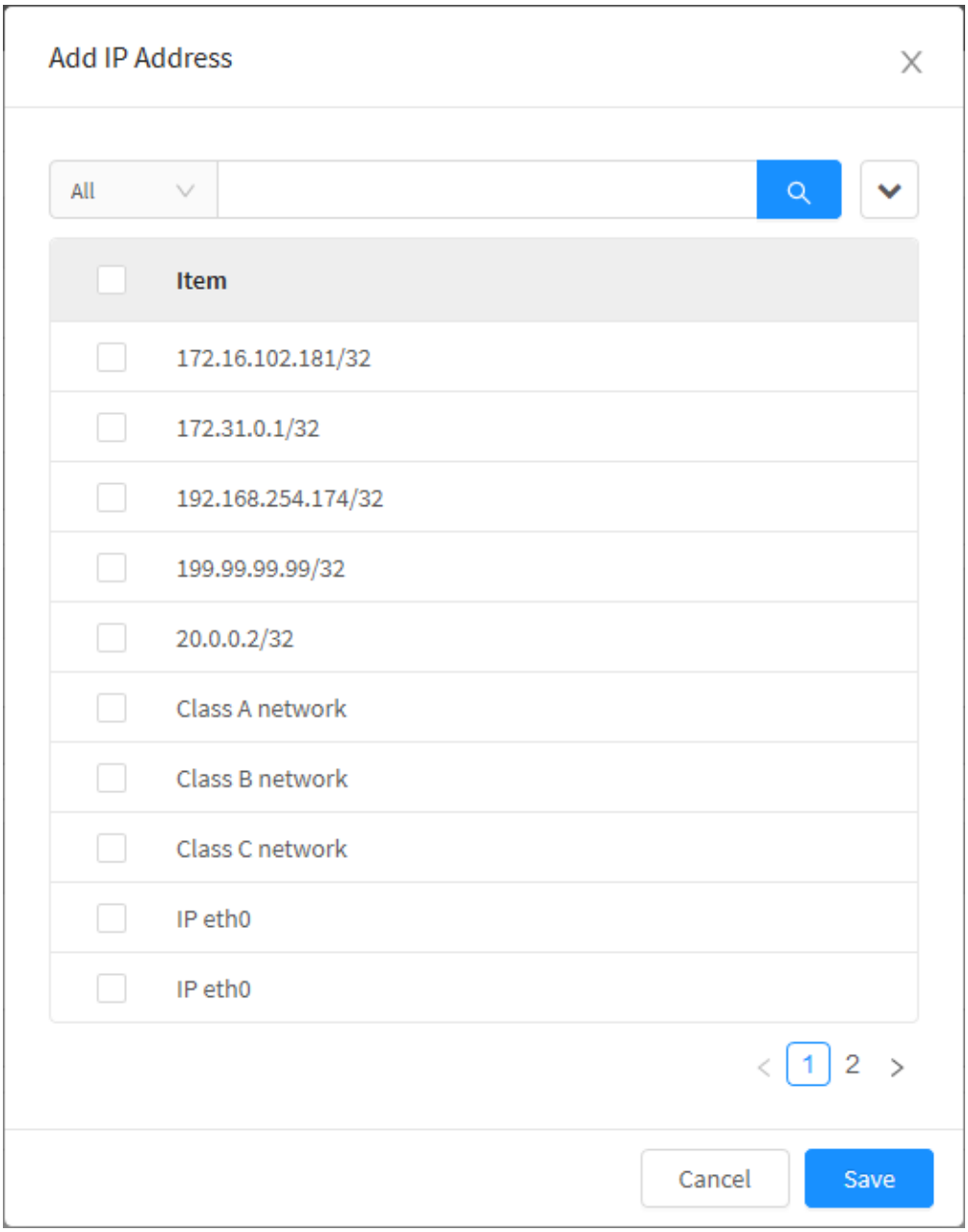
IPv4 – Connection - Source - Country

Destination

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*]**:

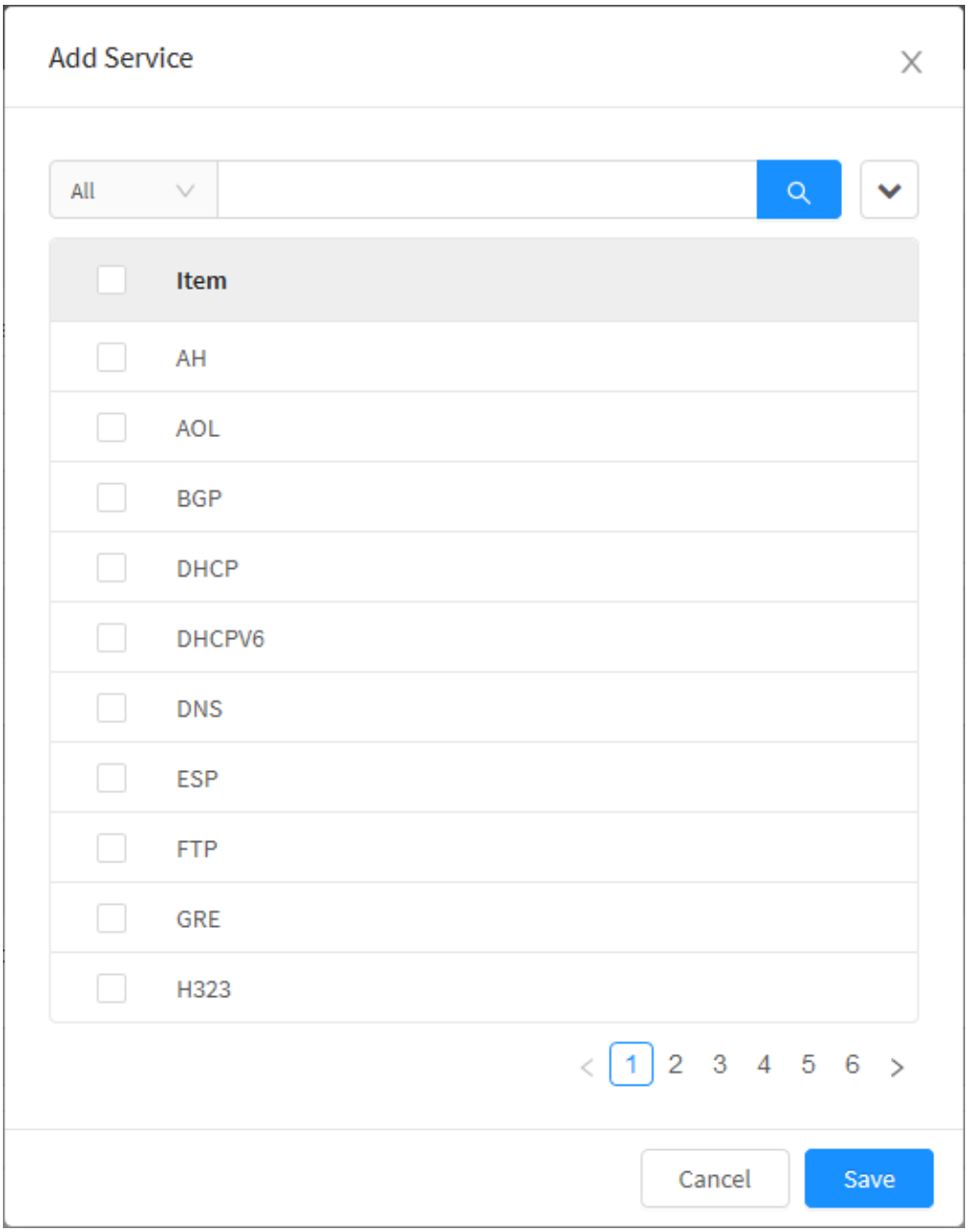
IPv4 – Connection - Destination

- ***IP Address[ ]*:** 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 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*;



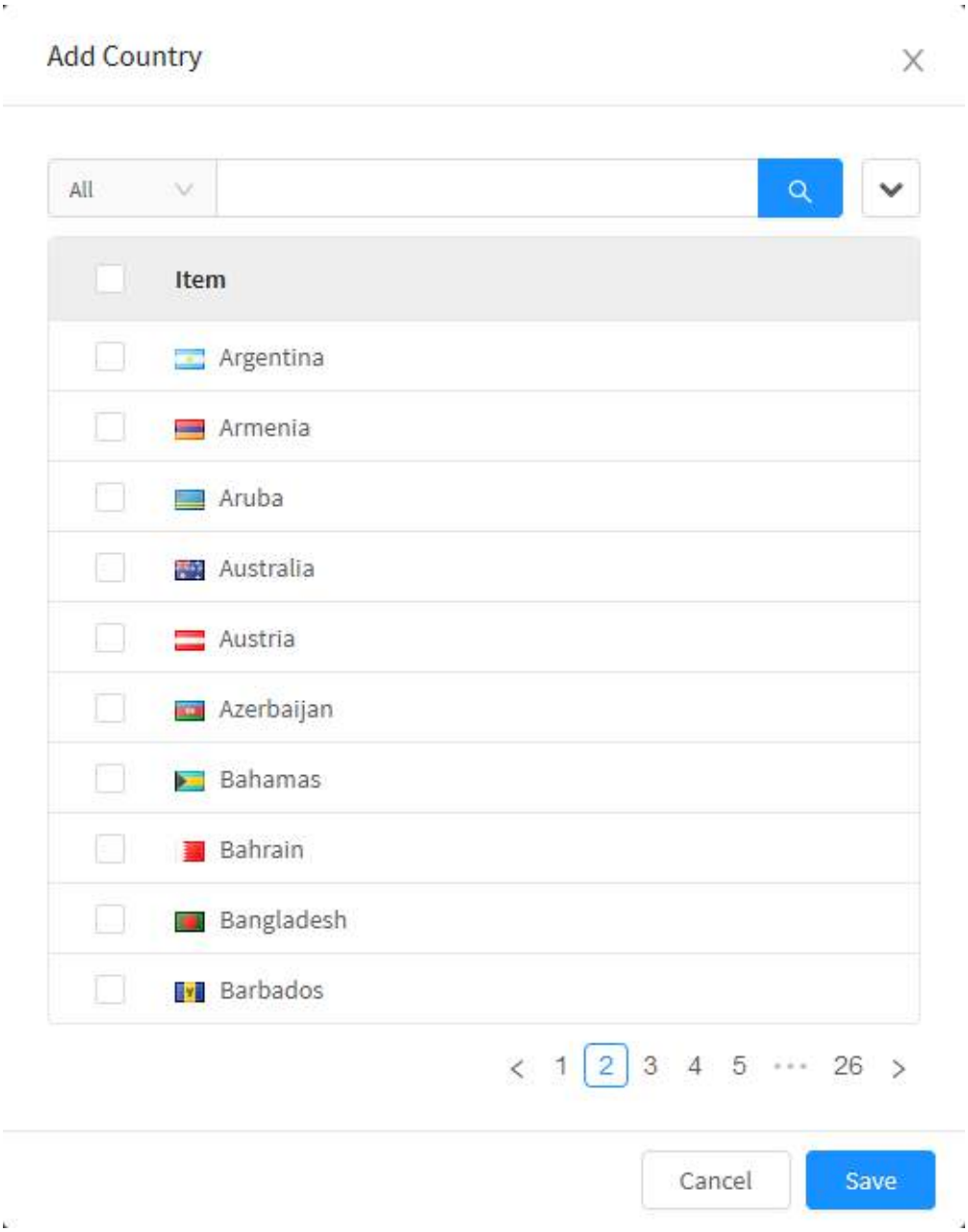
IPv4 – Connection - Destination - IP Address

- ***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*;



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.



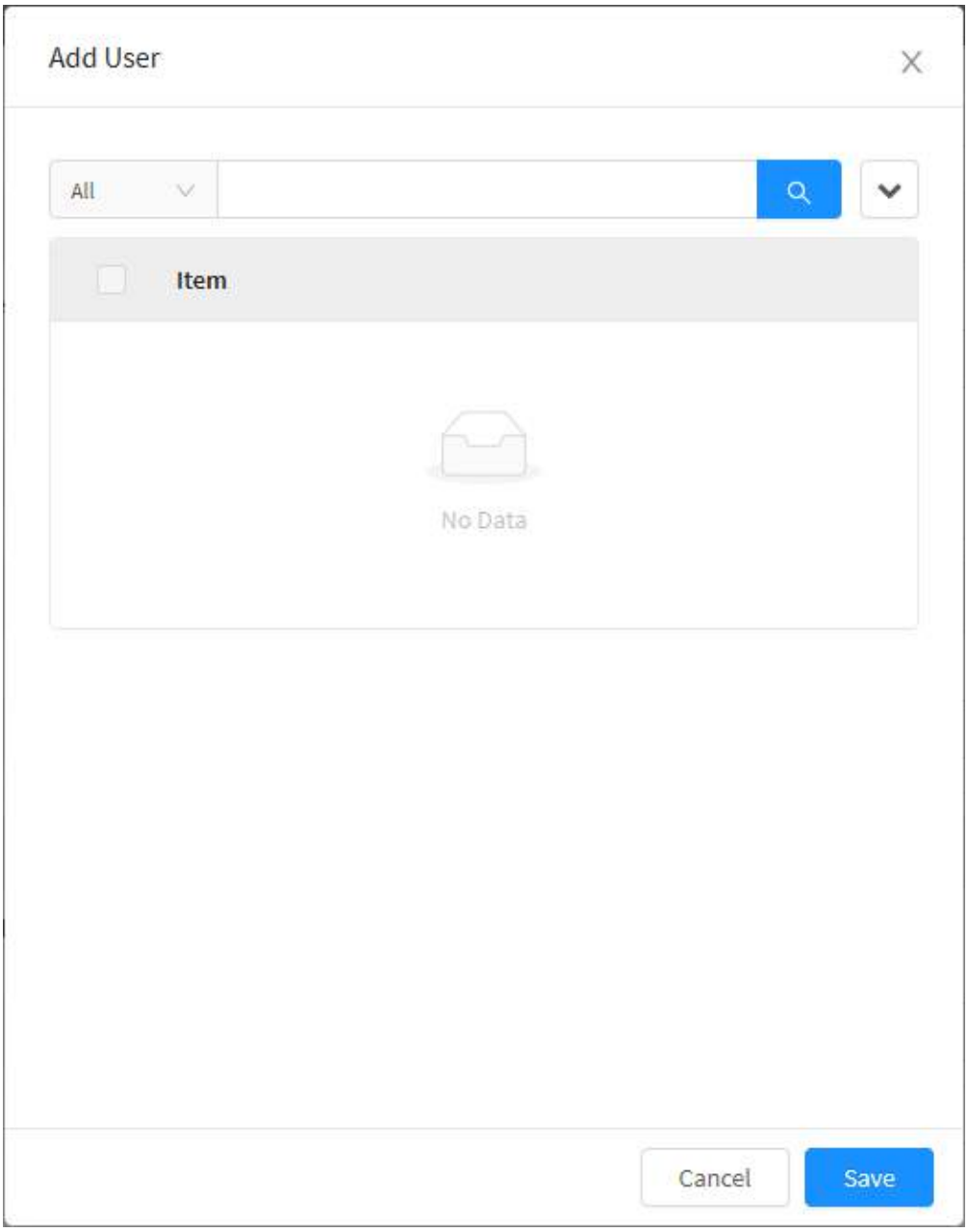
IPv4 – Connection - Destination - Country

Identification

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*]**:

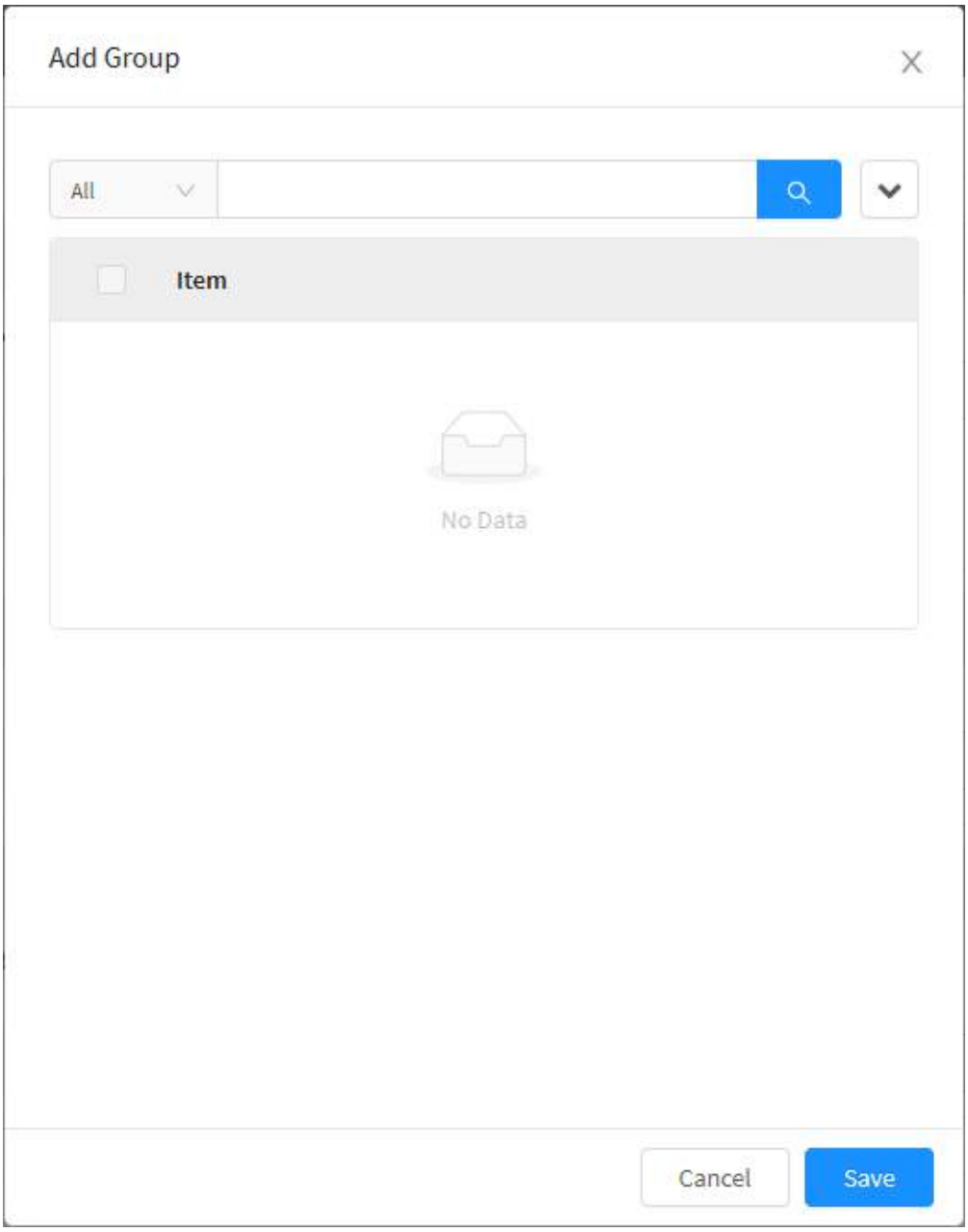
Policies IPv4 – Connection - Identification

- ***Authenticated[ ]*:** Caso habilitada, esta caixa de seleção determina se a política exige autenticação;
- ***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 **[ ]**, a tela abaixo será exibida para selecionar um ou mais usuário que irão compor a regra;



IPv4 – Connection - Destination - Users

- ***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.



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*[ ]:** 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* [ ]:** 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*

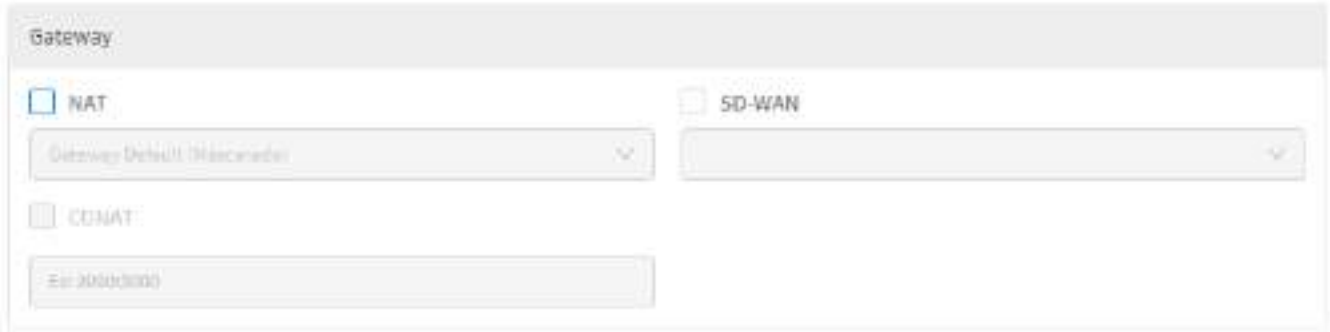
Nesta aba estão contidos os painéis:

- Gateway
- Roteamento de Aplicativos.
- *QoS*

A seguir analisaremos a função de cada campo dos painéis.

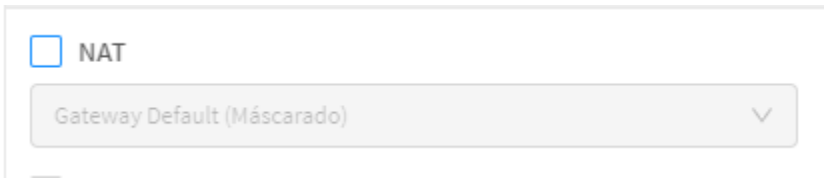
Gateway

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel **[*Gateway*]**:



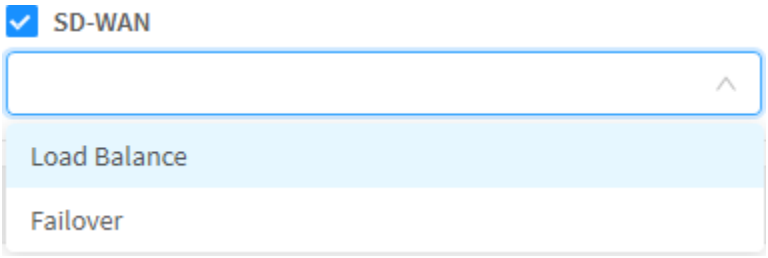
IPv4 – Roteamento - Gateway

- ***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;



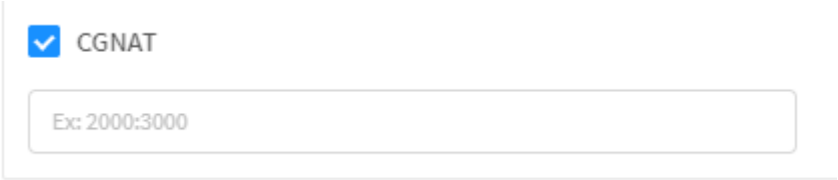
IPv4 – Roteamento - Gateway - NAT

- ***SD-WAN[ ]*:** Permite configurar o uso do *SD-WAN* na política, podendo escolher o perfil que se aplica a política;



IPv4 – Roteamento - Gateway - SD-WAN

- ***CGNAT [ ]*:** 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*]**:

IPv4 – Roteamento - QoS

- ***Controle de Banda [ ]*:** Permite ativar e selecionar a prioridade do tráfego, os valores podem ser ajustados em ***Configurações >> Rede >> Controle 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

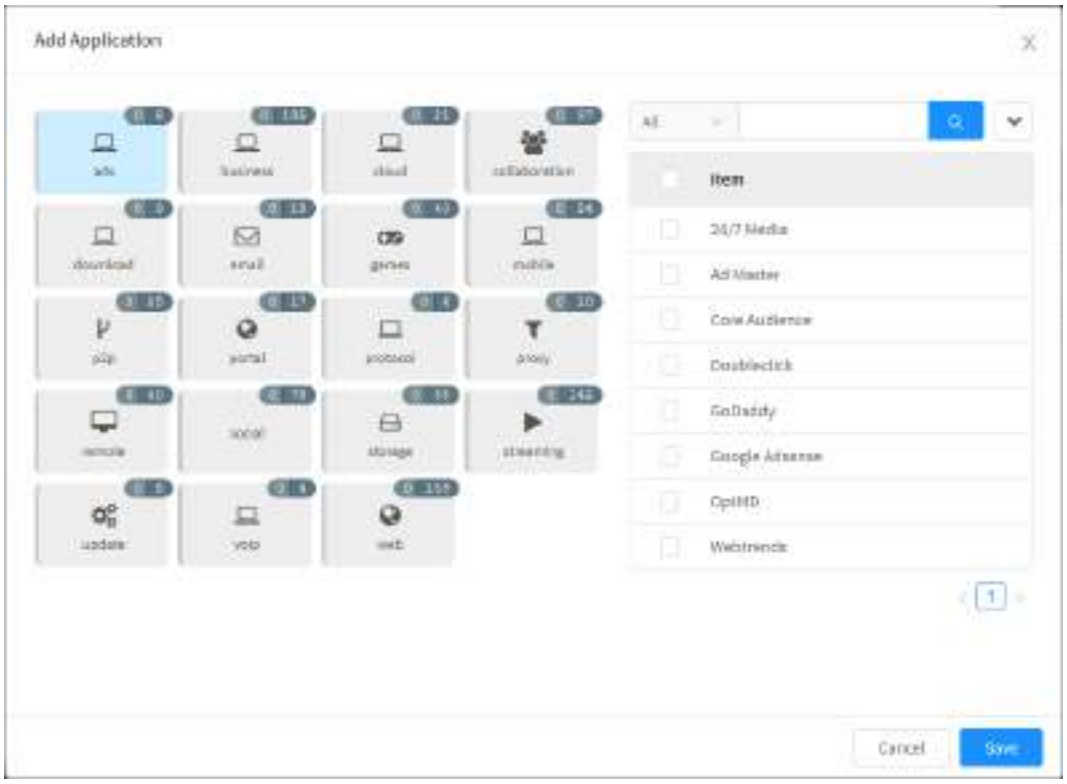
O painel **[*Roteamento de Aplicativos*]** serve para aplicar balanceamento de rotas em determinadas aplicações, é necessário selecionar ao menos um perfil de *SD-WAN* e ativar a *Inspeção SSL*. Abaixo segue uma descrição da função de cada campo do formulário exibido no painel **[*Roteamento de Aplicativos*]**:

IPv4 – Roteamento - QoS - Roteamento de Aplicativos

Para que as opções deste painel fiquem disponíveis para edição, é necessário ativar a Inspeção *SSL* na aba *Inspeção*.

Ao aplicar o roteamento por aplicação, o tráfego desta mesma seguirá um outro caminho independente do que foi definido no *Gateway* da conexão original.

- ***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;



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.

IPv4 - Abas Laterais - *Advanced*

Advanced

Abaixo segue uma descrição da função dos campos do formulário *Advanced*:

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 [☑]:** 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*.

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:

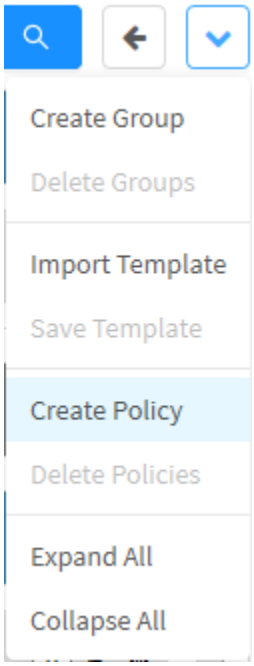
- Exemplo 1 - Política de Navegação via *Proxy* com *Deep Inspection* habilitado para *ATP*;
- Exemplo 2 - Política de Filtro de conteúdo *WEB* - Bloqueando categorias de improdutividade;
- Exemplo 3 - Política de Filtro de aplicativos - Bloqueando aplicativos *WEB 2*;
- Exemplo 4 - Política de *NAT* - 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*";



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*";

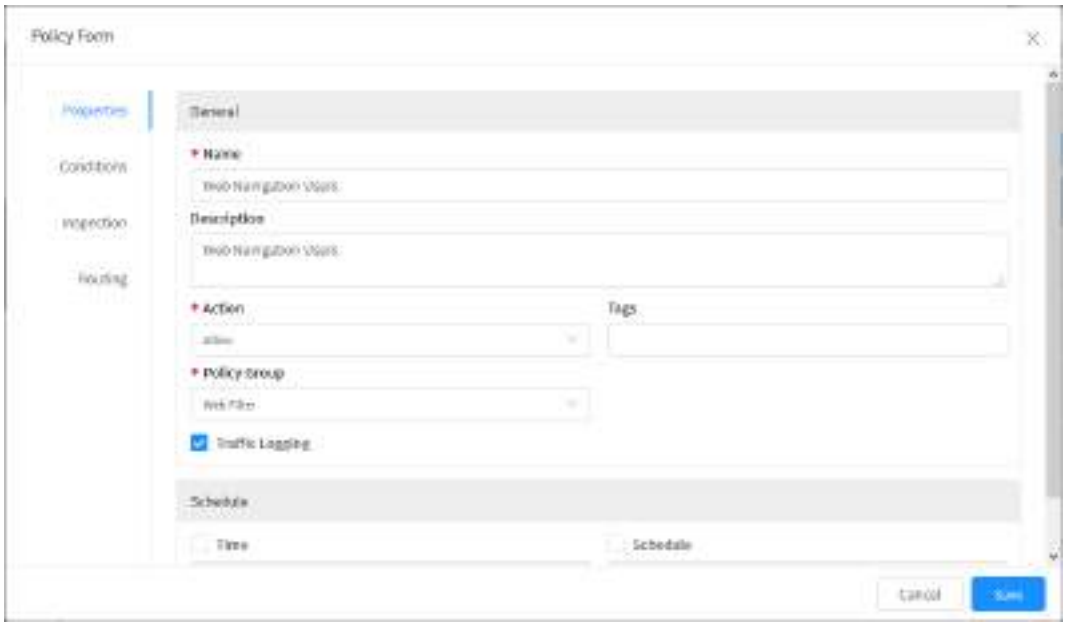
Em ***Description*** digite "*Web Navigation Users*";

Em ***Action*** selecione a opção "*Allow*";

Em ***Policy Group*** selecione "*Web Filter*";

Marque a caixa de seleção ***Traffic Logging[ ]***.

Você terá chego no resultado ilustrado pela imagem abaixo:



Create Policy – Ex. 1 – *Properties*

Selecione a próxima aba, **[*Conditions*]**.

Conditions

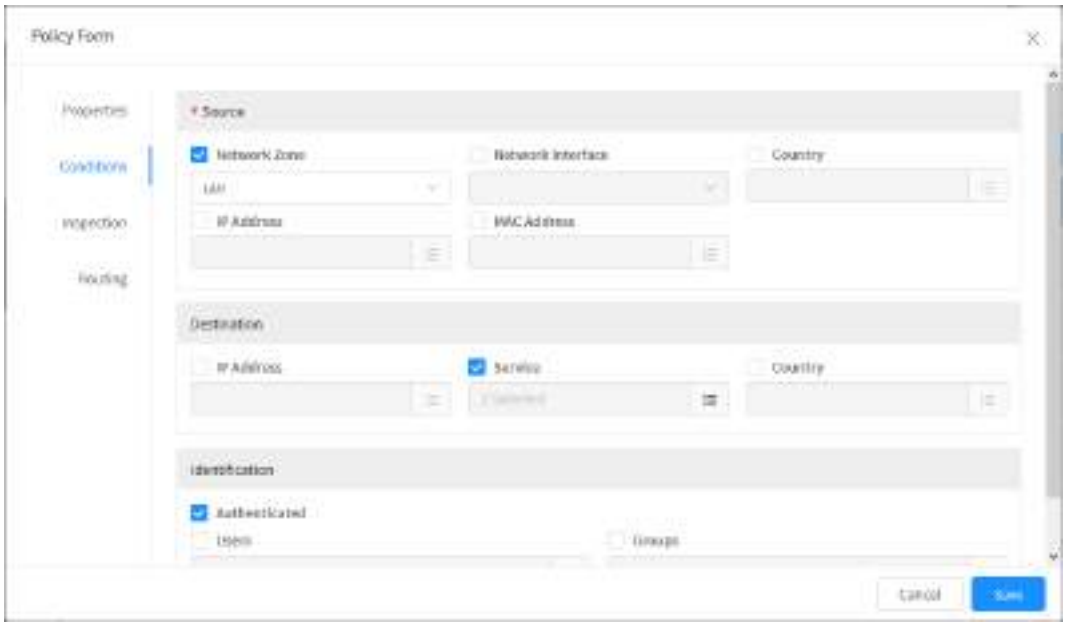
Na aba **[*Conditions*]**, em ***Network Zone*** selecione: “*LAN*”;

Em ***Service*** selecione *HTTP* e *HTTPS*;

Marque a caixa de seleção ***Authenticated [ ]***.

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.



Create Policy – Ex. 1 – *Conditions*

Selecione a próxima aba, **[*Inspection*]**.

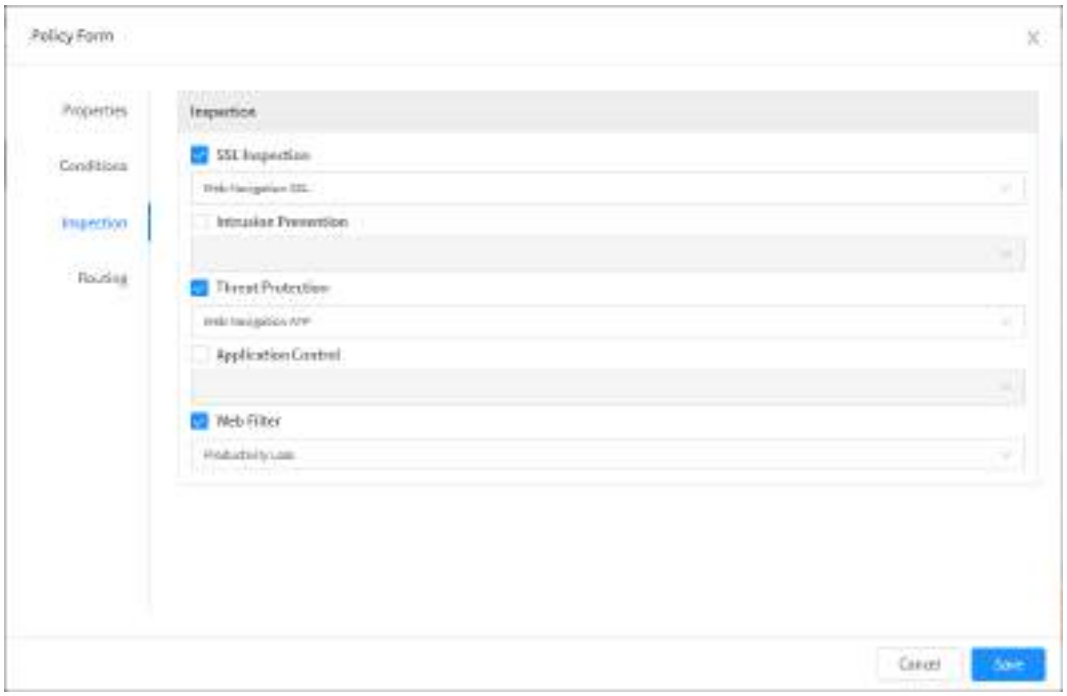
Inspection

Na aba **[*Inspection*]**, marque a caixa de seleção ***SSL Inspection [✓]*** e adicione um perfil que inspecione ***HTTPS*** *(Para mais informações, consulte esta página);*

Marque a caixa de seleção **Threat Protection *[✓]*** 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);*

Você terá chego no resultado ilustrado pela imagem abaixo:



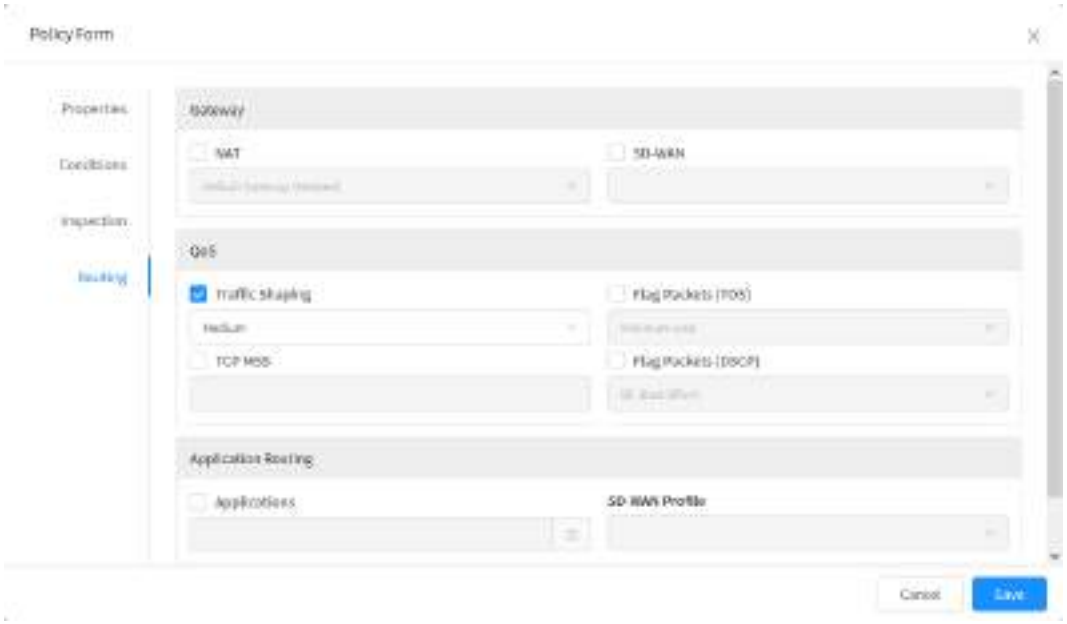
Create Policy – Ex. 1 – *Inspection*

Selecione a próxima aba, **[*Routing*]**.

Routing

Na aba **[*Routing*]**, marque a caixa de seleção ***Traffic Shaping [ ]*** e selecione a opção ***Medium***.

Você terá chego no resultado ilustrado pela imagem abaixo:



Add Policy – Ex. 1 – *Routing*

Após ter configurado cada aba de acordo com a definição da política aplicada, clique em **[** Save **]**.

Policy Saved Successfully

A tela ilustrada na imagem a seguir será exibida:

Add Policy – Web Navigation Users

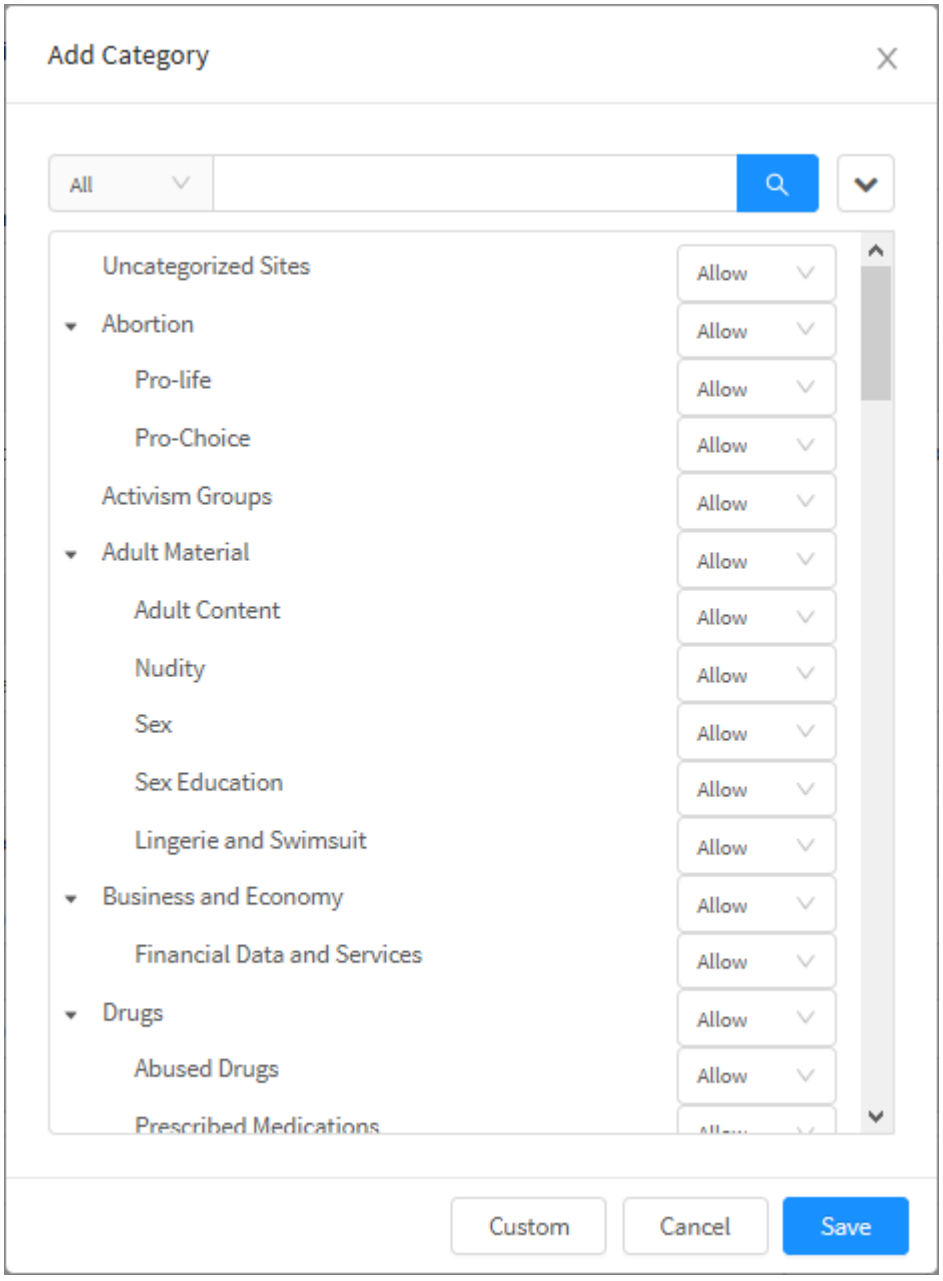
Após salvar, para que a política entre em ação será necessário acessar a **fila de comandos [**  **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Após realizar esses procedimentos a política terá sido configurada com sucesso.

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 **[ ]** com o fim de identificar as categorias que se enquadram neste tipo de classificação.



Services - Web Filter – Web Categories

Lista das categorias identificadas como improdutivas.

- Entretenimento;
- *MP3*;
- Jogos de azar e apostas;
- Jogos /Games;

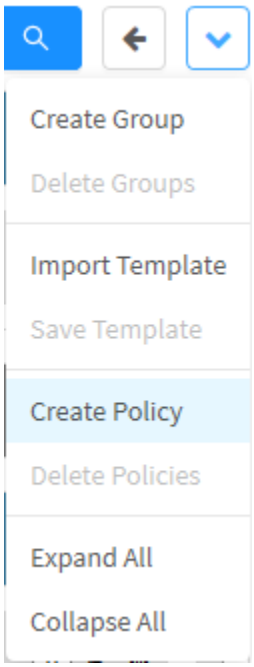
- Gestão de largura de banda;
- Rádio e TV na *Internet*;
- *Streaming* mídia;
- Sociedade e estilos de vida;
- Anúncios pessoais e namoros;
- Sites pessoais na *Web*;
- Esportes;
- Turismo.

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;*
- **[*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*";



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*";

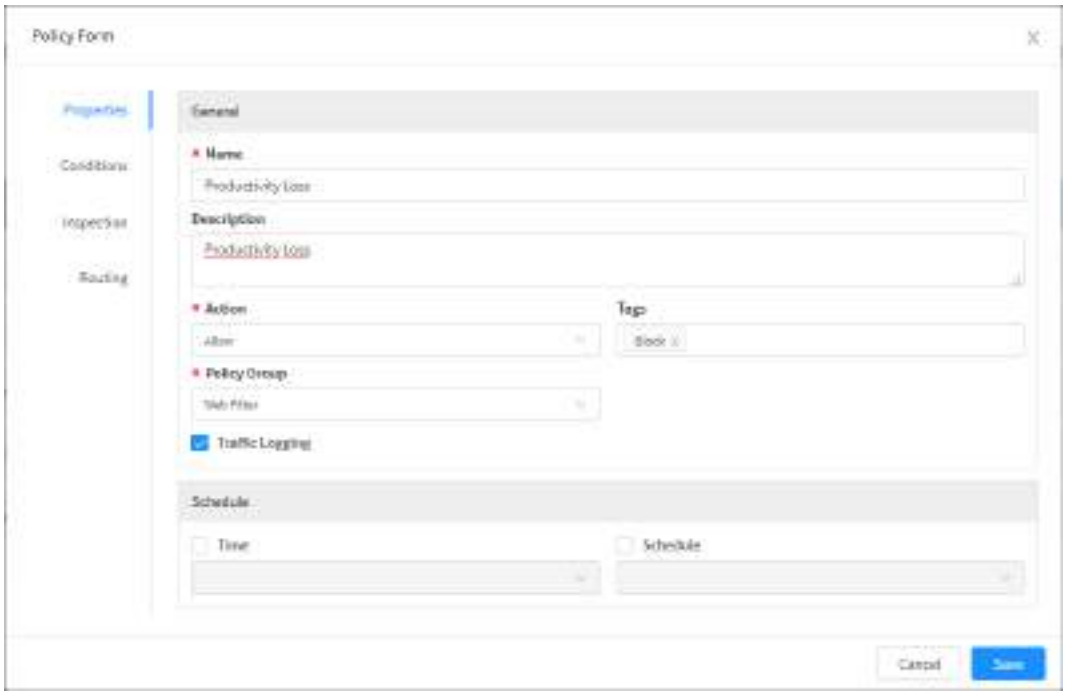
Em ***Action*** deixe a opção *"Allow"*, você efetuará o bloqueio através do perfil de *Web Filter*;

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:



Create Policy – Ex. 2 – *Properties*

Selecione a próxima aba, **[*Conditions*]**.

Conditions

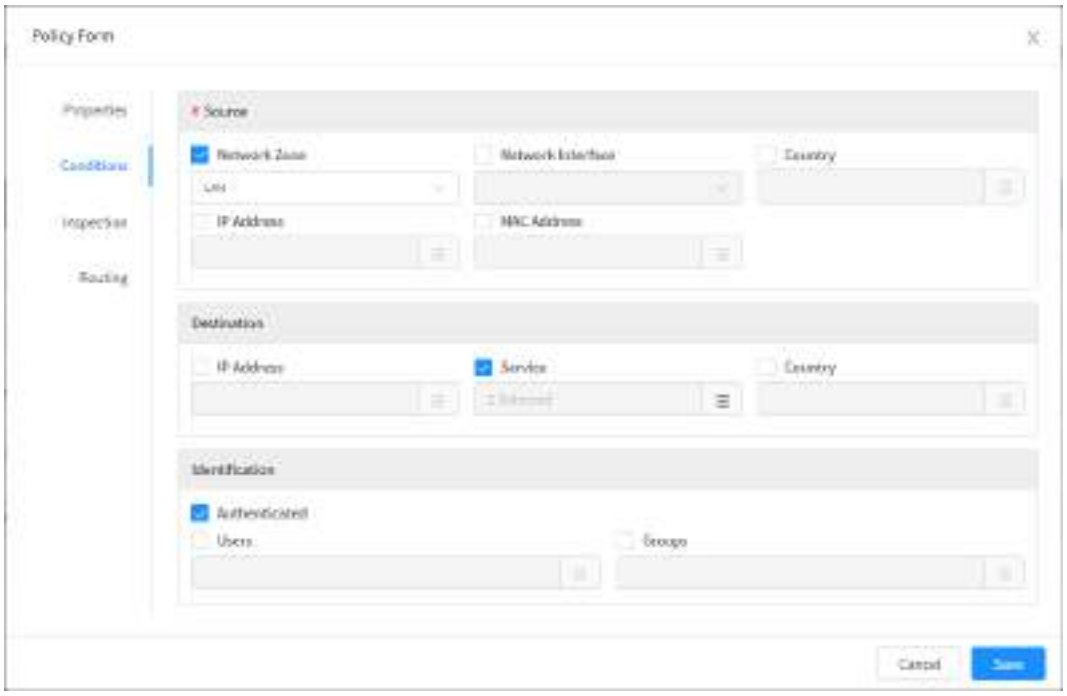
Na aba **[*Conditions*]**, em ***Network Zone*** selecione: “*LAN*”;

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.



Create Policy – Ex. 2 – *Conditions*

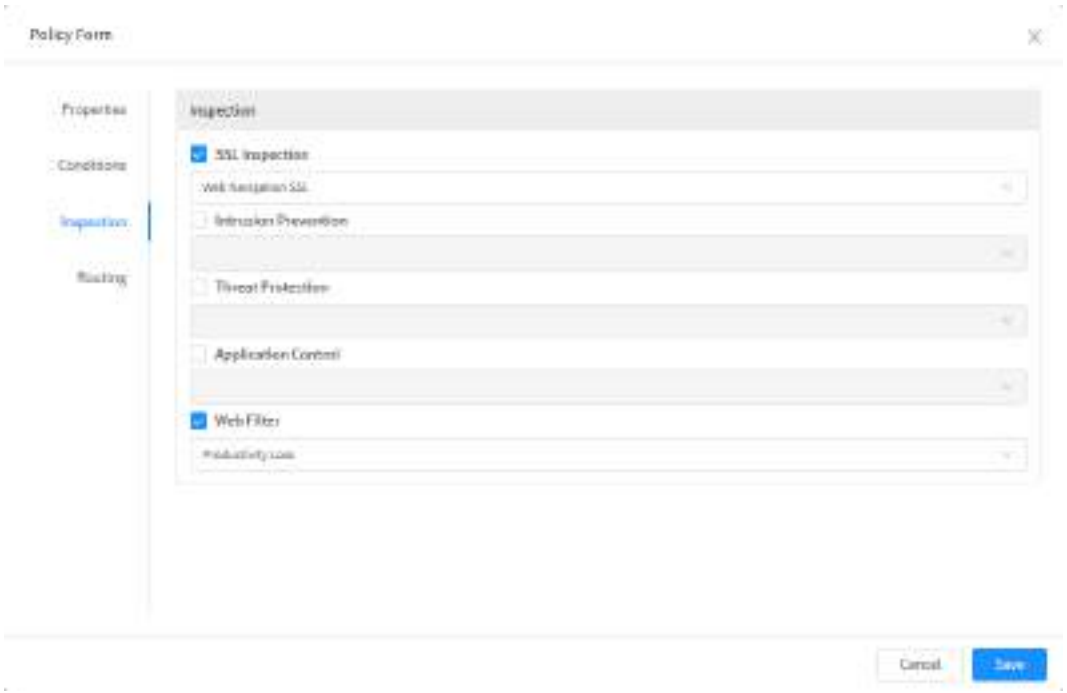
Selecione a próxima aba, **[*Inspection*]**.

Inspection

Na aba **[*Inspection*]**, marque a caixa de seleção ***SSL Inspection [✓]*** e adicione um perfil que inspecione ***HTTPS*** *(Para mais informações, cheque esta página);*

*Marque a caixa de seleção **Web Filter [✓]** e selecione o perfil relacionado as categorias de improdutividade (Para mais informações, cheque a esta página);*

Você terá chego no resultado ilustrado pela imagem abaixo:

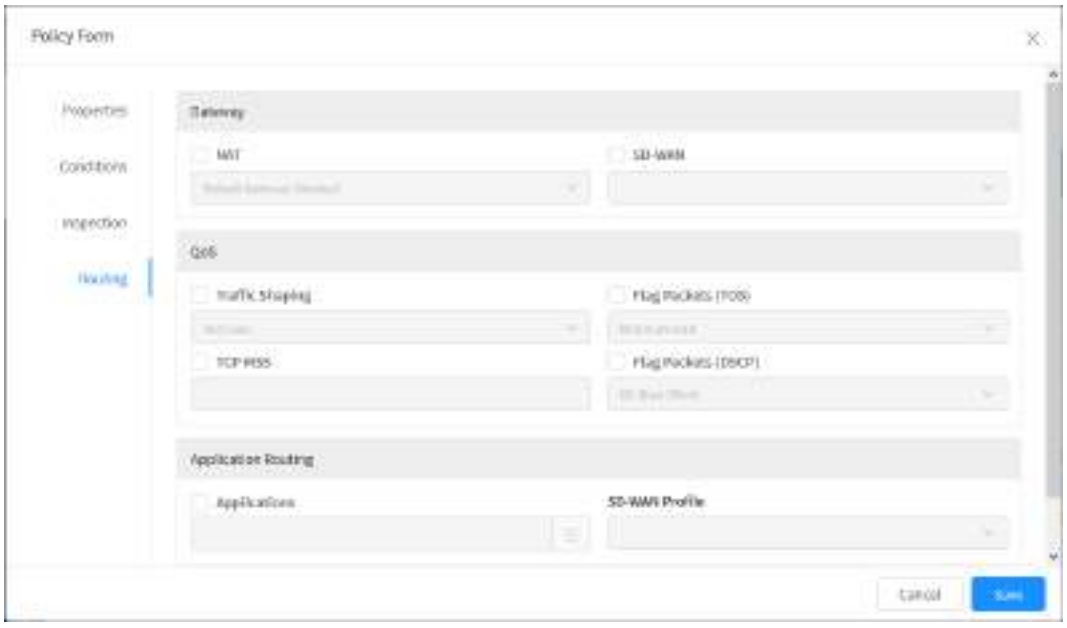


Create Policy – Ex. 2 – *Inspection*

Selecione a próxima aba, **[*Routing*]**.

Routing

Na aba **[*Routing*]**, nenhum controle será ativado, conforme exemplificado pela imagem a seguir:



Create Policy – Ex. 2 – *Routing*

Após ter configurado cada aba de acordo com a definição da política aplicada, clique em **[** Save **]**.

Policy Saved Successfully

A tela ilustrada na imagem a seguir será exibida:

Create Policy – Productivity Loss

Após salvar, para que a política entre em ação será necessário acessar a **fila de comandos [** 1 **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

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

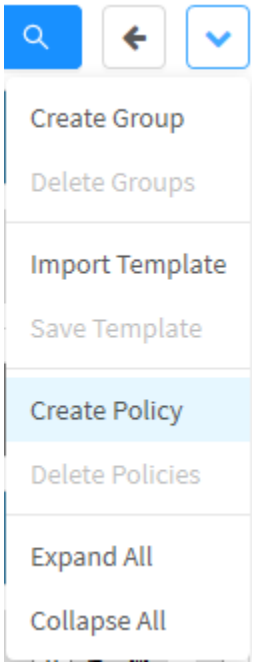
Lista dos aplicativos identificados como improdutivos ou de risco de segurança.

- *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*.*

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*";

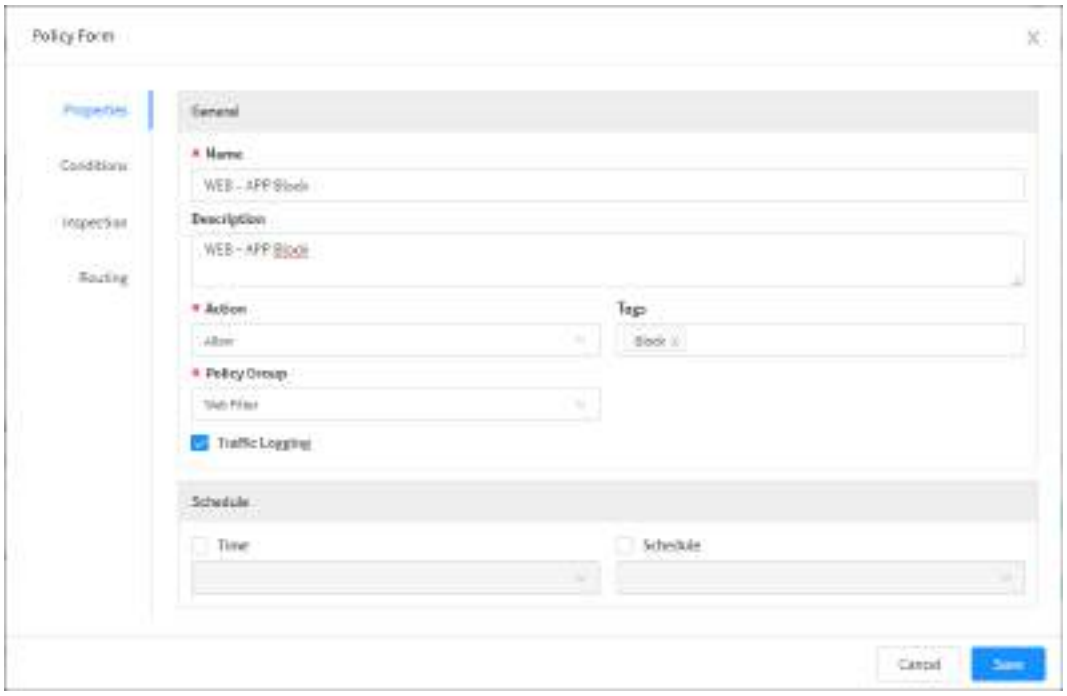
Em ***Action*** deixe a opção *"Allow"*, você efetuará o bloqueio através dos perfis de *Web Filter* e *Application Control*;

Em ***Policy Group*** selecione "*Web Filter*";

Em ***Tags*** digite "*Block*";

Marque a caixa de seleção ***Traffic Logging[☑]***.

Você terá chego no resultado ilustrado pela imagem abaixo:



Create Policy – Ex. 3 – *Properties*

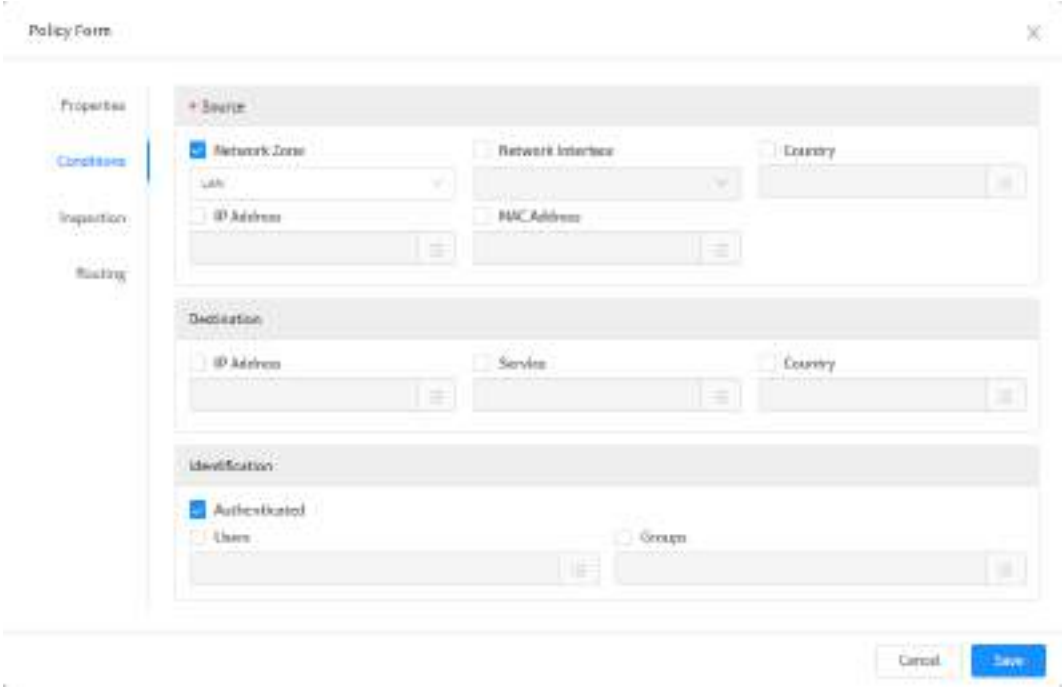
Selecione a próxima aba, **[Conditions]**.

Conditions

Na aba **[Conditions]**, em ***Network Zone*** selecione a opção: "*LAN*";

Em ***Identification*** marque a caixa de seleção ***Authenticated[ ]***;

Você terá chego no resultado ilustrado pela imagem abaixo:



Create Policy – Ex. 3 – *Conditions*

Selecione a próxima aba, **[*Inspection*]**.

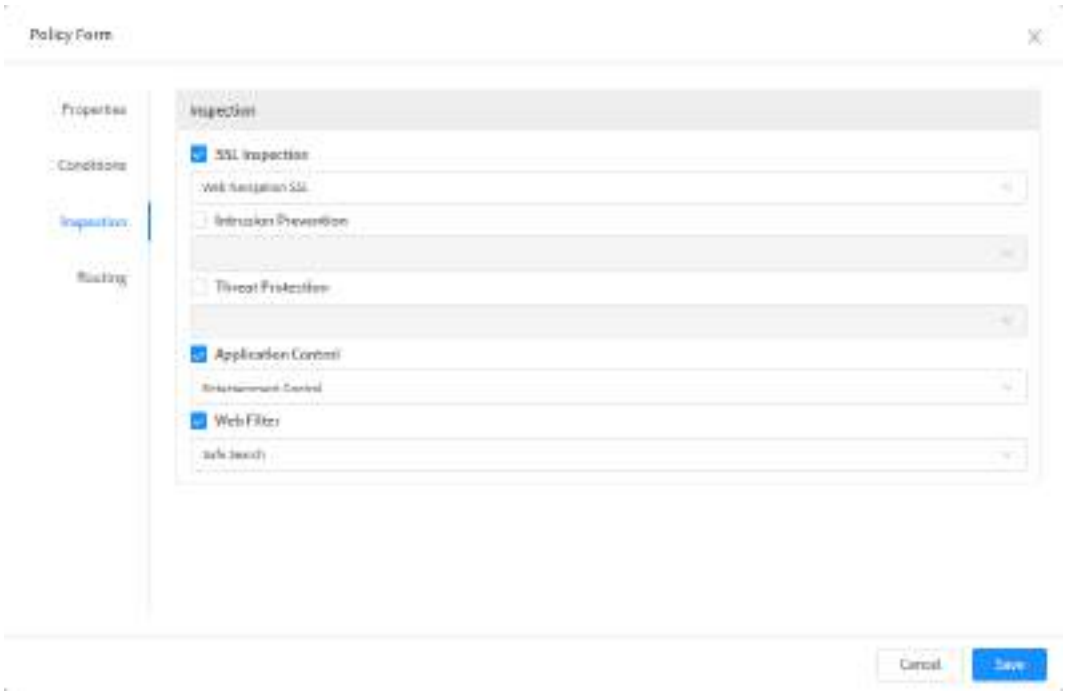
Inspection

Na aba **[*Inspection*]**, marque a caixa de seleção ***SSL Inspection[✓]*** e adicione um perfil que inspecione ***HTTPS*** *(Para mais informações, consulte a página);*

Marque a caixa de seleção ***Application Control[✓]*** *e* selecione o perfil relacionado a todas as categorias aplicação improdutivas ou de risco (Para mais informações, consulte a *página);*

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);*

Você terá chego no resultado ilustrado pela imagem abaixo:

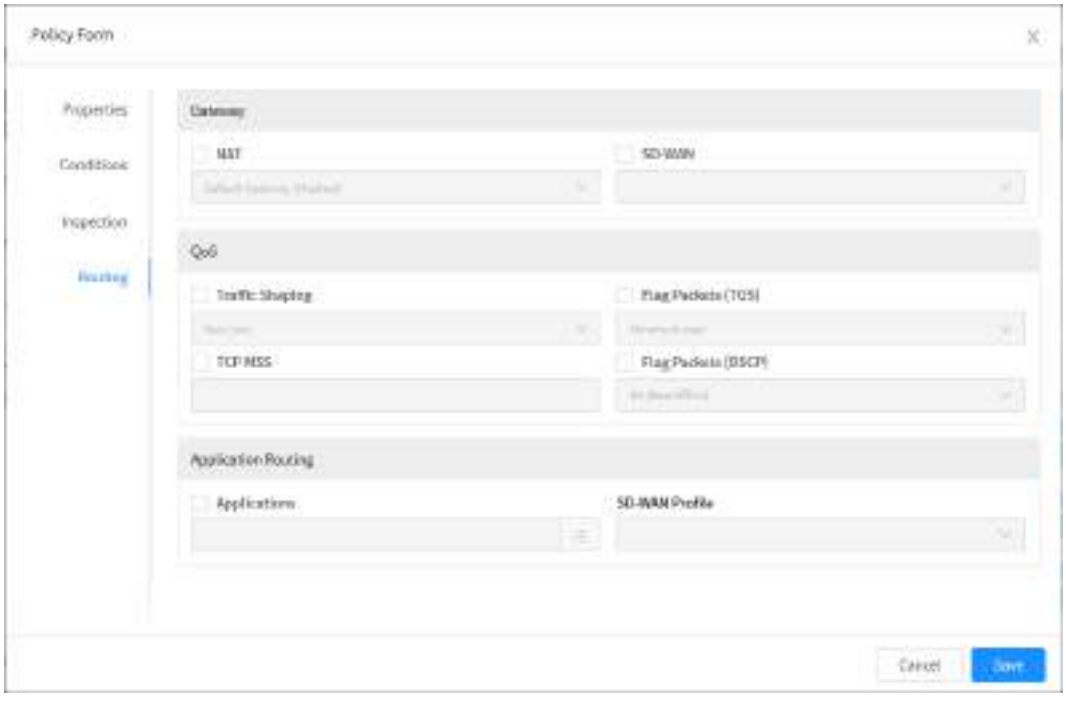


Create Policy – Ex. 3 – *Inspection*

Selecione a próxima aba, **[*Routing*]**.

Routing

Na aba **[*Routing*]**, nenhum controle será ativado, conforme exemplificado pela imagem a seguir:



Create Policy – Ex. 3 – *Routing*

Após ter configurado cada aba de acordo com a definição da política aplicada, clique em **[** Save **]**.

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 mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

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

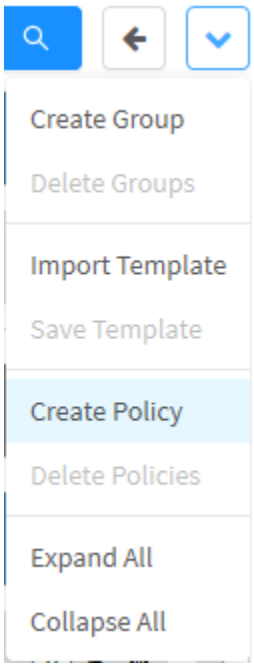
https://technet.microsoft.com/en-us/library/cc708602(v=ws.10).aspx

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 [ ]**, clique na opção "*Create Policy*";



IPv4 - Menu de Ações - *Create Policy*

Configure cada aba de acordo com as definições demonstradas à seguir.

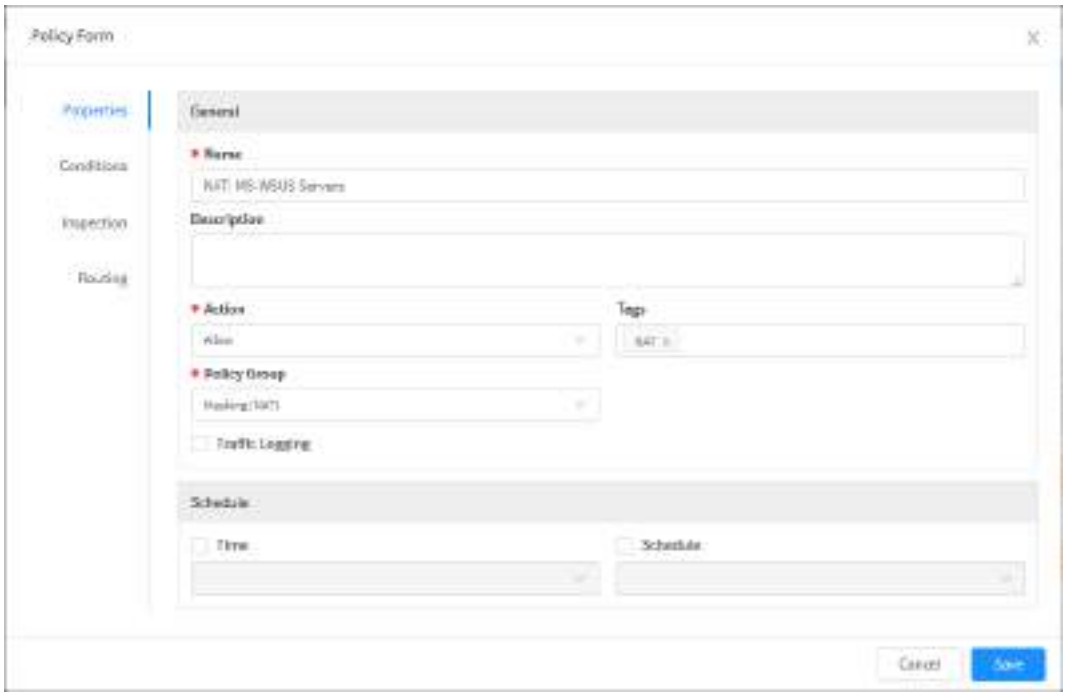
Properties

Na aba **[*Properties*]**, em ***Name*** nomeie como: “NAT: MS-WSUS Servers”;

Em ***Tags*** inclua “NAT”;

Em ***Policy Group*** selecione “*Masking (NAT)*”;

Você terá chego no resultado ilustrado pela imagem abaixo:



Add Policy – Ex. 4 – *Properties*

Selecione a próxima aba, **[*Conditions*]**.

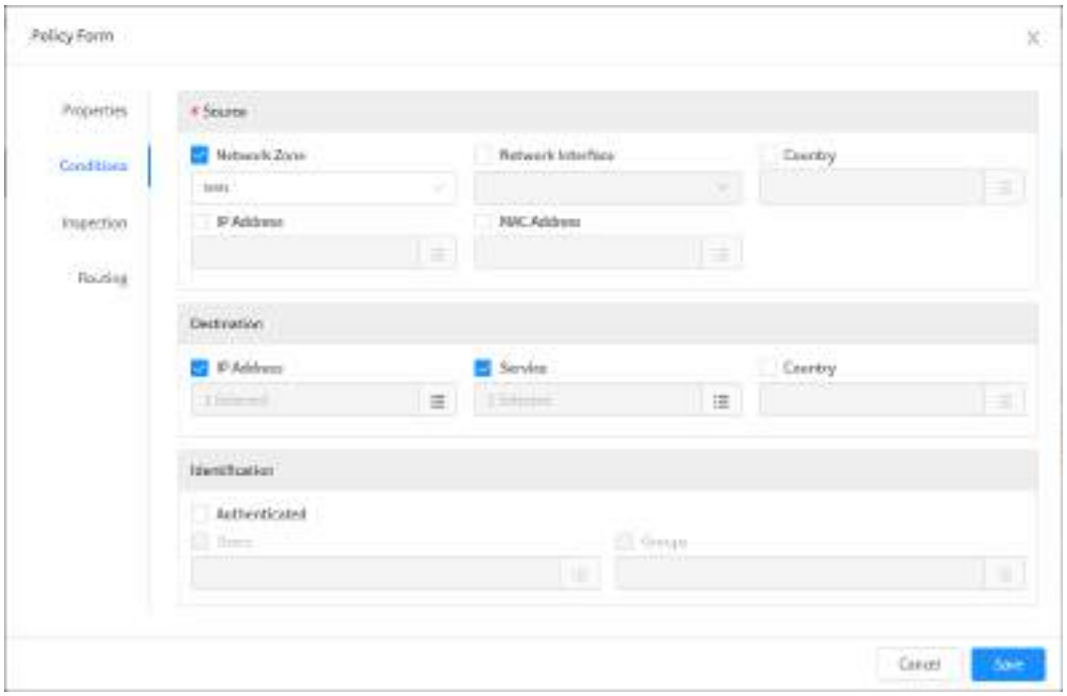
Conditions

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);

Você terá chego no resultado ilustrado pela imagem abaixo:



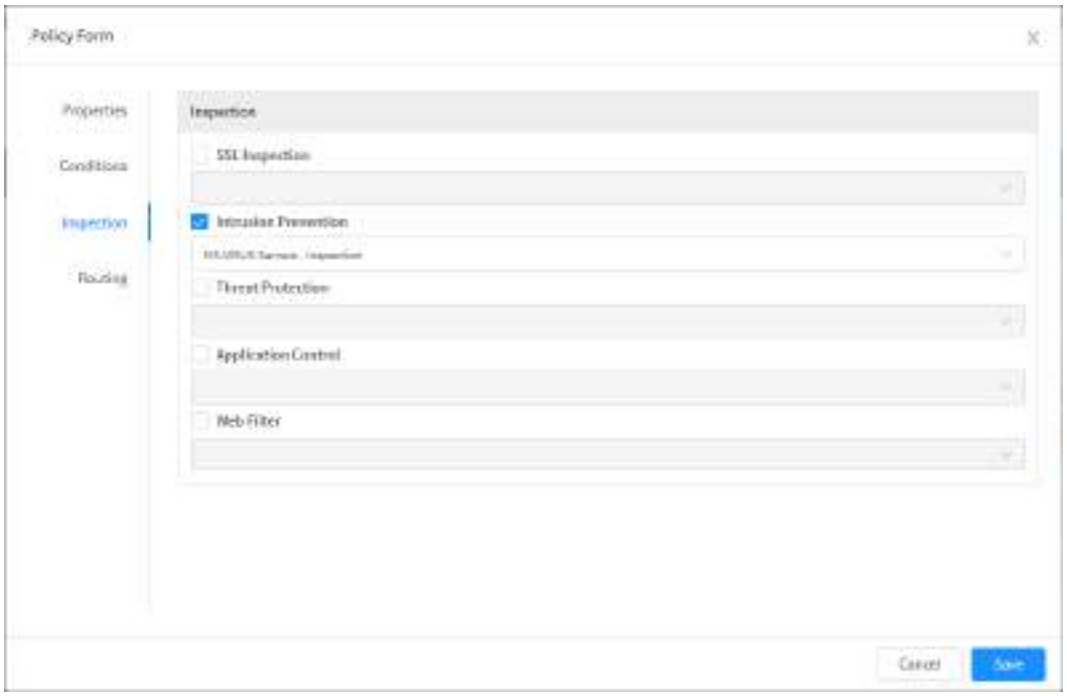
Create Policy – Ex. 4 – *Conditions*

Selecione a próxima aba, **[*Inspection*]**.

Inspection

Na aba **[*Inspection*]**, habilite a caixa de seleção de ***Intrusion Prevention [✓]*** e selecione um perfil para efetuar *Deep Inspection* (*Para mais informações, cheque a página*);

Você terá chego no resultado ilustrado pela imagem abaixo:



Create Policy – Ex. 4 – *Inspection*

Selecione a próxima aba, **[*Routing*]**.

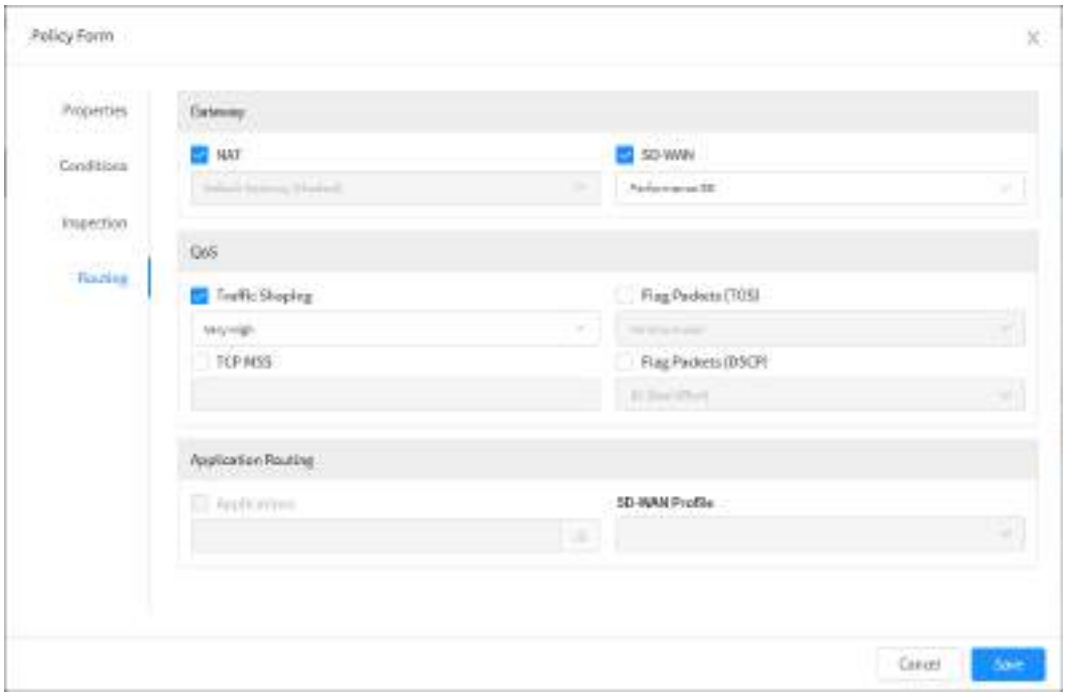
Routing

Na aba **[*Routing*]**, marcar a caixa de seleção ***NAT[ ]***;

Marcar a caixa de seleção de ***SD-WAN[ ]*** e selecionar a opção "*Performance BB*";

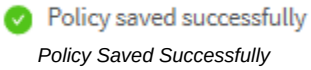
Em ***Traffic Shaping*** selecione a opção "*Very High*";

Você terá chego no resultado ilustrado pela imagem abaixo:



Create Policy – Ex. 4 – *Routing*

Após ter configurado cada aba de acordo com a definição da política aplicada, clique em **[** Save **]**.



Policy Saved Successfully

A tela ilustrada na imagem a seguir será exibida:

Create Policy – Ex. 4 – *NAT: MS-WSUS Servers*.

Após salvar, para que a política 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.

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.

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.

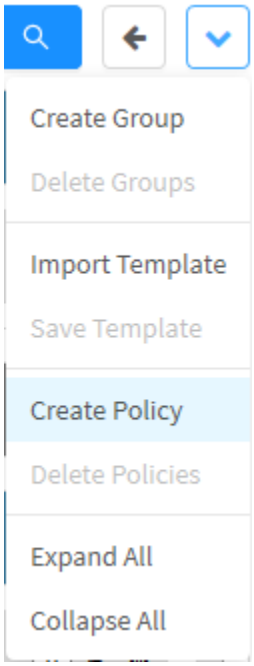
Exemplo 5 - Política de NAT para todos os protocolos com IPS e Proxy

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 [ ]**, clique na opção "*Create Policy*";



IPv4 - Menu de Ações - *Create Policy*

Configure cada aba de acordo com as definições demonstradas à seguir.

Properties

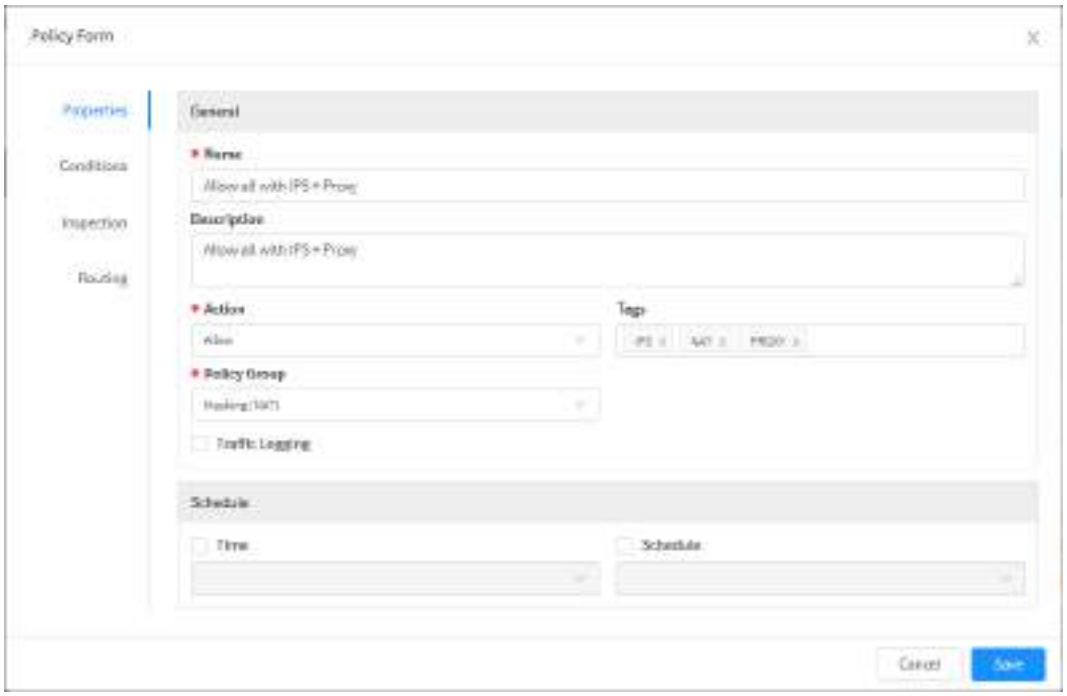
Na aba **[*Properties*]**, em ***Name*** nomeie como: "*Allow all with IPS + Proxy*";

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:



Create Policy – Ex. 5 – *Properties*

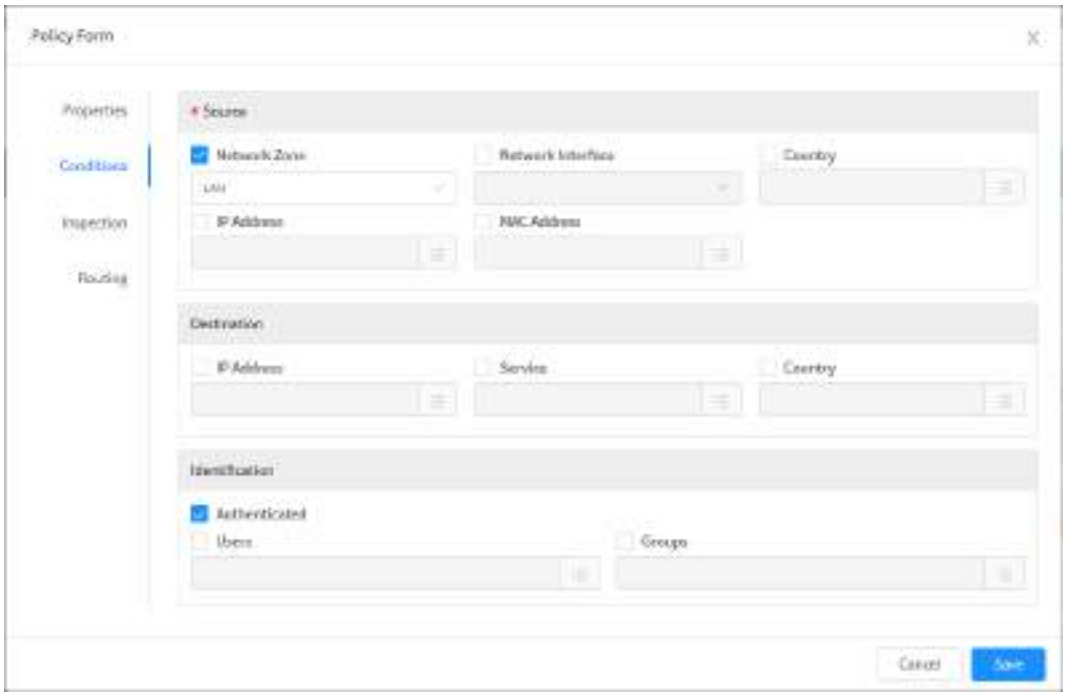
Selecione a próxima aba: **[*Conditions*]**.

Conditions

Na aba **[*Conditions*]**, em ***Network Zone*** selecione: “*LAN*”;

Marque a caixa de seleção ***Authenticated***.

Você terá chego no resultado ilustrado pela imagem abaixo:



Create Policy – Ex. 5 – *Conditions*

Selecione a próxima aba: **[*Inspection*]**.

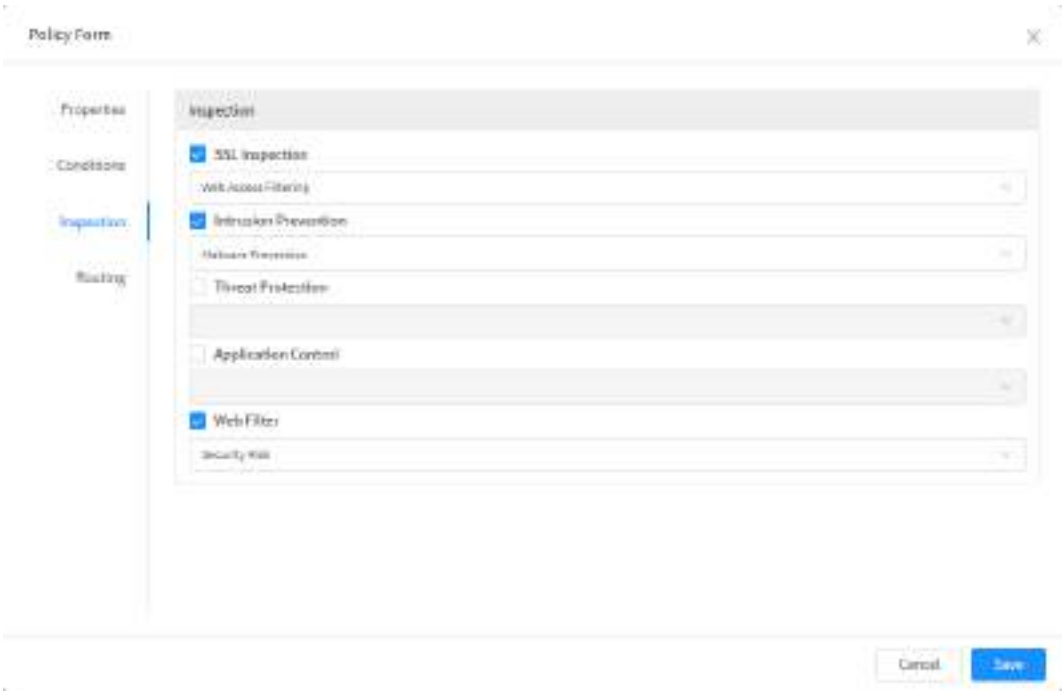
Inspection

Na aba **[*Inspection*]**, habilite a caixa de seleção de ***SSL Inspection [☑]*** e selecione um perfil para inspecionar ***SMTP, POP3, FTP*, *HTTP*, *HTTPS*** e ***SSL*** *(Para mais informações, consulte esta página);*

Habilite a caixa de seleção de ***Intrusion Prevention [☑]*** e selecione o perfil de inspeção desejado (*Para mais informações, consulte a página*);

Marque a caixa de seleção ***Web Filter [☑]*** e selecione o perfil desejado (Para mais informações, consulte esta página);

Você terá chego no resultado ilustrado pela imagem abaixo:



Create Policy – Ex. 5 – *Inspection*

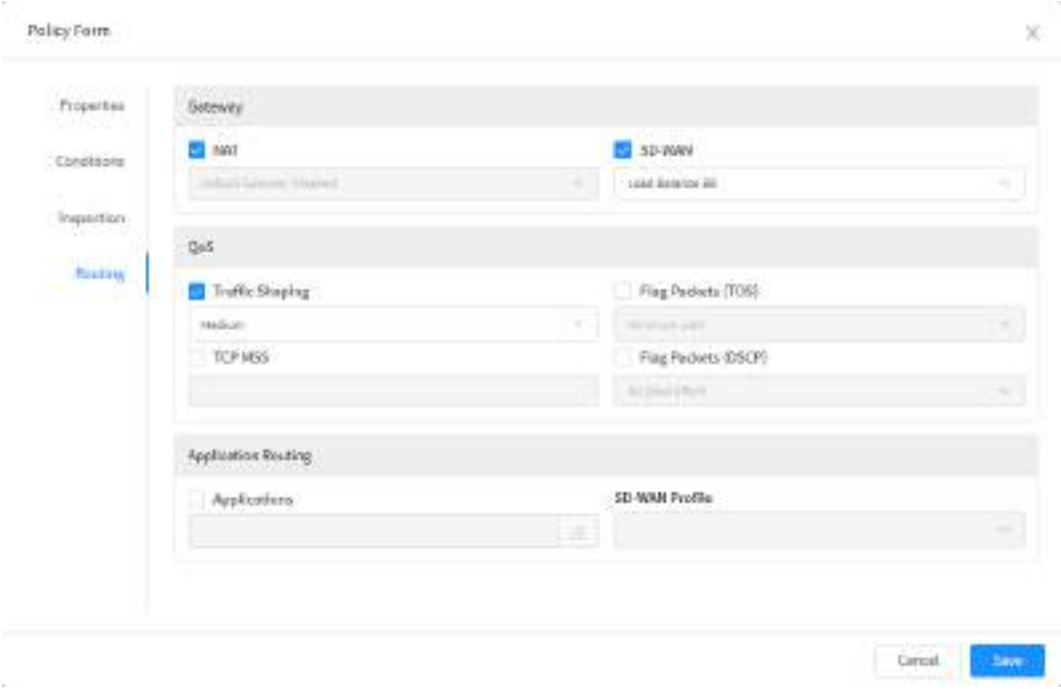
Selecione a próxima aba: **[*Routing*]**.

Routing

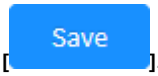
Na aba **[*Routing*]**, marcar a caixa de seleção ***Nat***;

Marcar a caixa de seleção de ***SD-WAN*** e selecionar a opção “*Load Balance BB*”;

Em ***Traffic Shaping*** selecione a opção “*Medium*”;



Create Policy – Ex. 5 – *Routing*

Após ter configurado cada aba de acordo com a definição da política aplicada, clique em **[**  **]**.

Policy Saved Successfully

A tela ilustrada na imagem a seguir será exibida:

Create Policy – Ex. 5 – *Allow all with IPS + PROXY*

Após salvar, para que a política 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.

Após realizar esses procedimentos a política terá sido configurada com sucesso.

Pronto! Agora é só aplicar alguns testes.

Para tanto, use uma estação de trabalho devidamente configurada e navegue na *WEB*.

Depois verifique os registros de Tráfego no *Dashboard*.

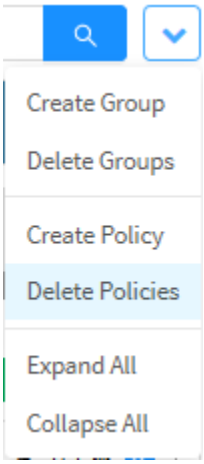
IPv4 - Menu de ações - Delete Policies

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*;

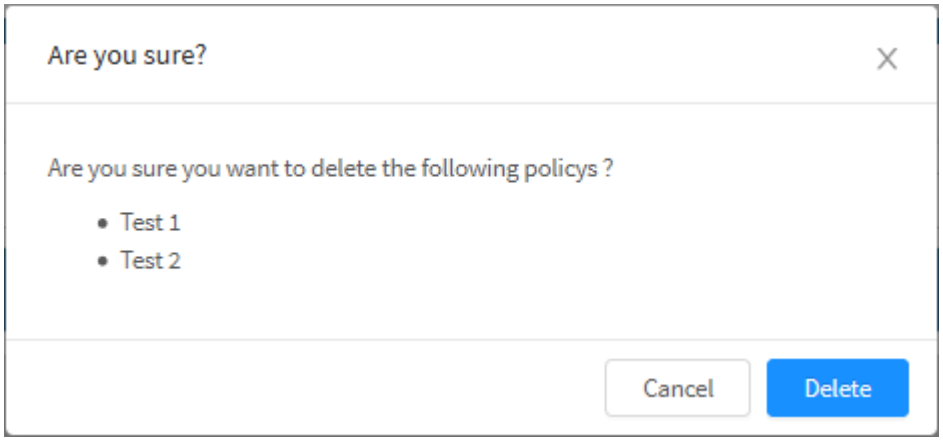
Políticas selecionadas para serem deletadas

2. No **menu de ações [ ]**, clique na opção “*Delete Policies*”;



Policies IPv4 - Menu de Ações - *Delete Policies*

3. Surgirá a tela perguntando se deseja deletar os itens:



Policies IPv4 - Are you sure you want to delete the following policies

Caso desejar cancelar, clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].

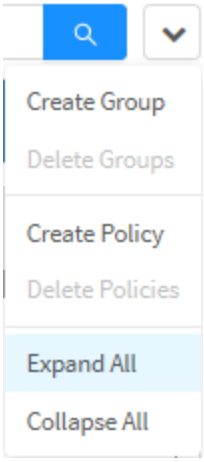
Policy Deleted successfully

As *Policies* foram removidas com sucesso.

IPv4 - Menu de ações - Expand All e Collapse All

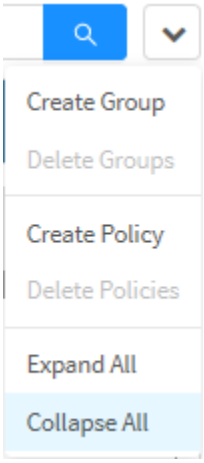
O botão “*Expand All*” tem como finalidade expandir o grupo de políticas. Para expandir o grupo de políticas, siga os seguintes passos:

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.

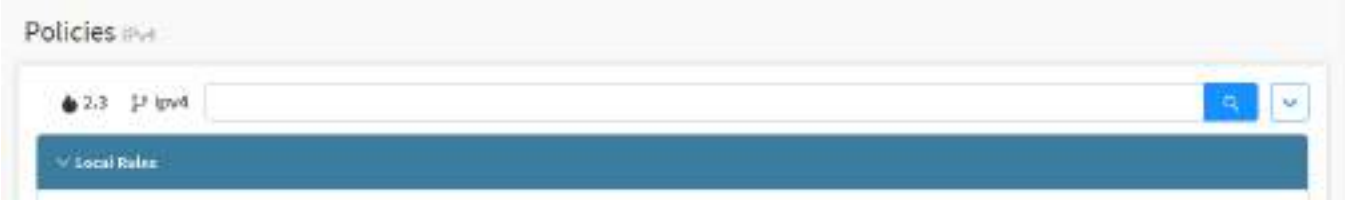


Policies IPv4 – Menu de ações – *Collapse All*

IPv4 - Menu de ações - Validate Policies

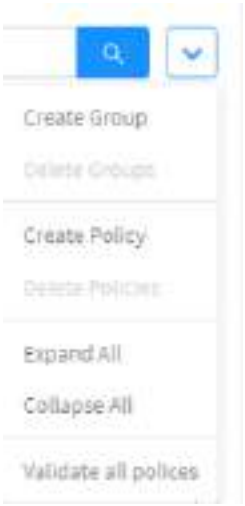
O botão “*Validate Policies*” serve para verificar a existência de Políticas redundantes, em duplicidade, ou em condição de ofuscamento (sobreposição).

No menu principal de Políticas IPv4, clique em opções [ ], e a opção de validar políticas estará disponível:



Policies IPv4 – Menu Principal

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.

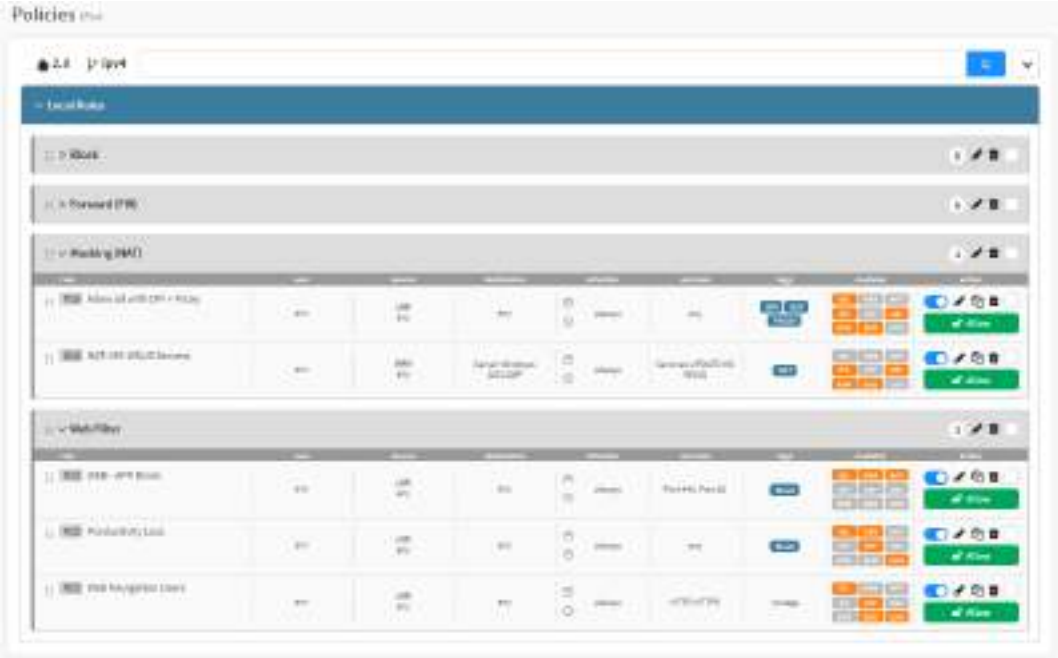
Ofuscamento: Ocorre quando uma Política sobrepõe a outra em termos de ação, ou seja a ação descrita já é feita por uma anterior.

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.



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.

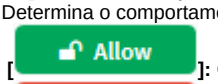
É importante, lembrar que as políticas são ordenadas por “Prioridade”, sendo que elas são aplicadas considerando o método “*First Match Wins*” (Que literalmente quer dizer “O 1º entre os concorrentes VENCE”). Logo, as políticas localizadas acima tem prioridade enquanto as abaixo possuem menor prioridade.

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*);
- **[ ]** Expande para exibir as políticas criadas no grupo;

- [] 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*** []**:** 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***[]**:** 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***[]**:** 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:
    - [

]**:** Como o próprio nome diz, esta opção serve para conceder acesso;
    - [

]**:** O acesso é negado;
    - [

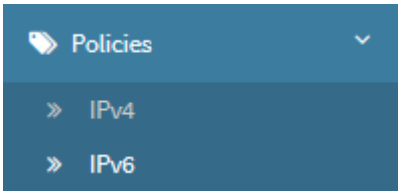
]**:** O acesso é negado, porém uma mensagem de rejeição é exibida ao usuário.

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*";



Opção *IPv6*

Surgirá a Tela de "*Policies IPv6*", conforme demonstrado pela imagem a seguir:

IPv6

Esta seção irá se aprofundar em:

- Criação de grupos de políticas;
- Cadastro e Remoção de políticas.

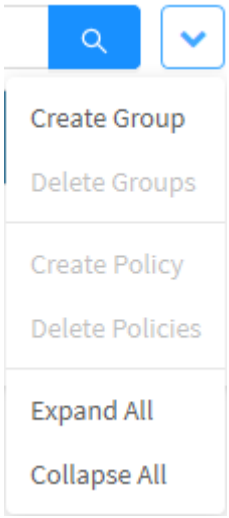
A seguir, vamos analisar cada componente deste painel.

IPv6 - Menu de ações

No topo direito da tela temos o menu de ações:

IPv6 – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



IPv6 – Menu de ações

O menu é composto das seguintes opções:

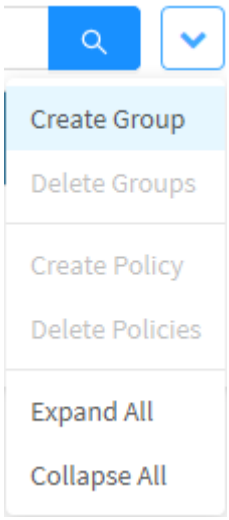
- *Create Group*;
- *Delete Groups*;
- *Create Policy*;
- *Delete Policies*;
- *Expand All* e *Collapse All*.

A seguir cada opção do menu de ações será detalhada.

IPv6 - Menu de ações - Create Group

Através da opção “*Create Group*” é possível criar um novo grupo. Para acessar, clique no **menu de ações [**  **]**.

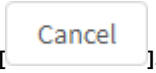
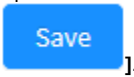
1. Clique na opção “*Create Group*”;

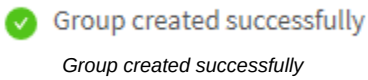


IPv6 - Menu de ações - *Create Group*

2. A tela “*Create Group*” será exibida. Adicione o nome do grupo desejado:

IPv6 – Create Group

Após nomear o grupo, caso deseje cancelar clique no botão ***Cancel*[**  **]**. Para concluir a criação do grupo clique no botão ***Save*[**  **]**.



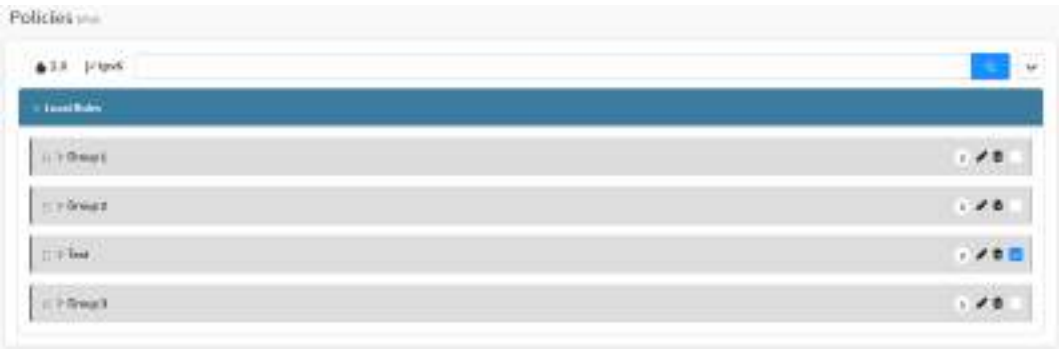
Group created successfully

O grupo foi criado com sucesso.

IPv6 - Menu de ações - Delete Groups

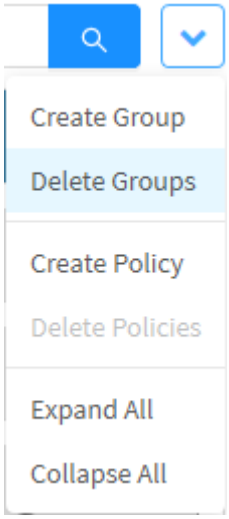
Através do botão “*Delete Groups*” é possível deletar vários grupos instalados ao mesmo tempo. Para deletar pelo menu de ações, siga os seguintes passos:

1. Selecione qual(is) grupo(s) deseja deletar clicando no ***checkbox*[ ]**, como demonstrado pela imagem abaixo:



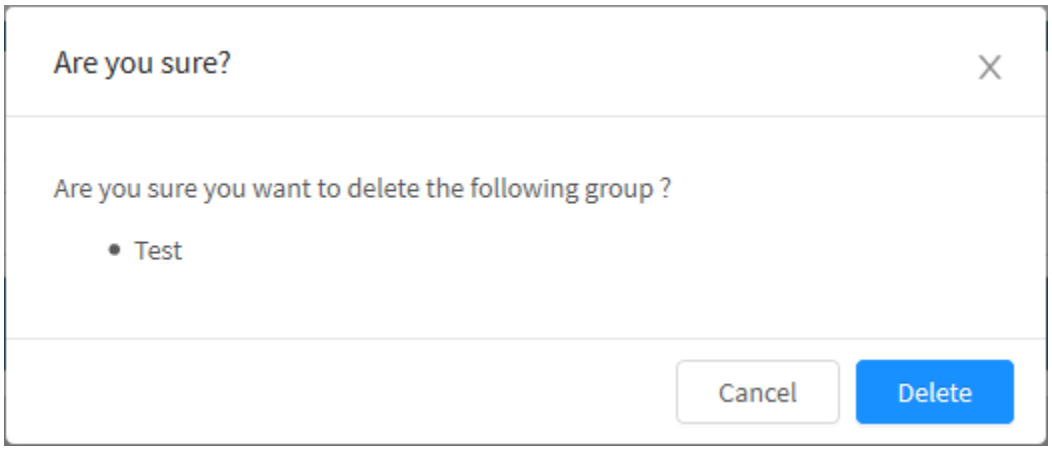
IPv6 – Delete Groups

2. Entre no **menu de ações [ ]** e clique no botão “*Delete Groups*”.



IPv6 – Menu de ações - *Delete Groups*

3. Surgirá a mensagem se deseja realmente deletar os pacotes selecionados:



IPv6 – Delete Groups

Caso deseje cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].

Group deleted succesfully

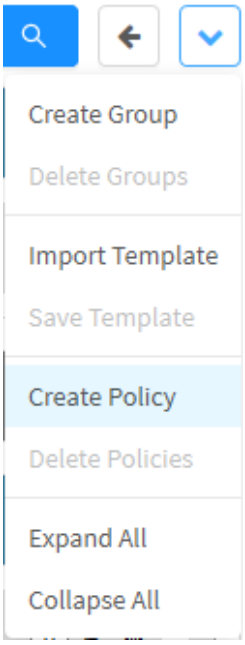
Após realizar esses procedimentos os grupos terão sido excluídos com sucesso.

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).

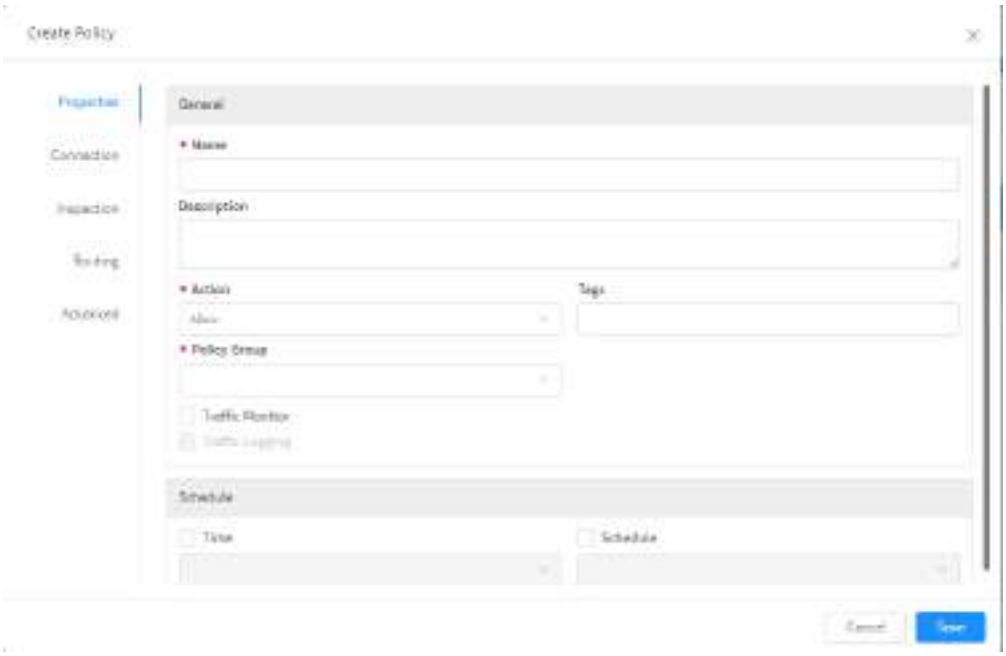
Para criar uma política, siga os passos:

1. No **menu de ações [ ]**, clique na opção “*Create Policy*”;



IPv6 - Menu de Ações - *Create Policy*

2. Surgirá a tela *Policy Form*;



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*

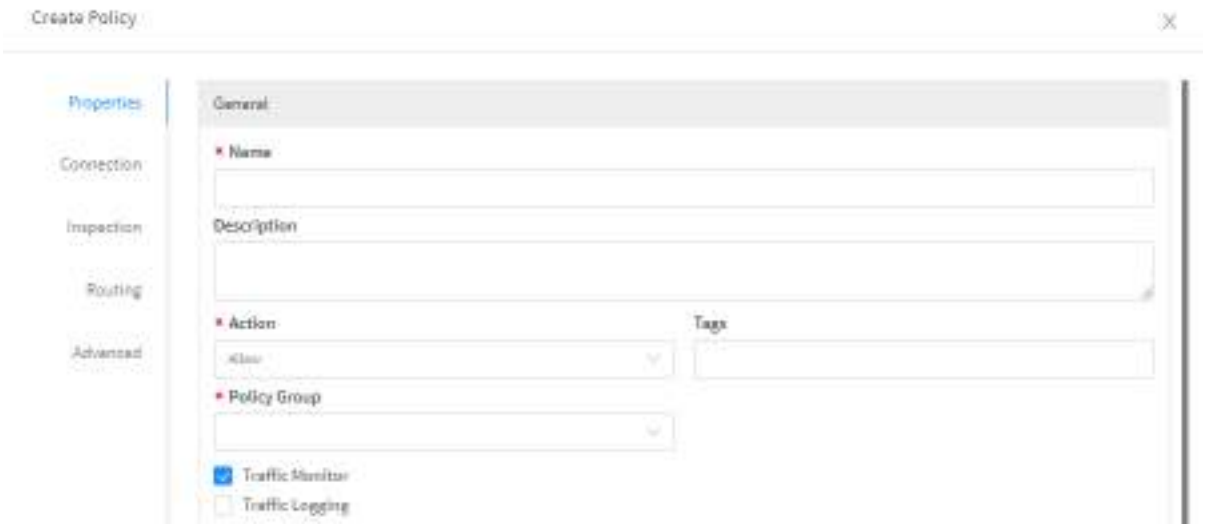
Nesta aba estão contidos os painéis:

- *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]**:*



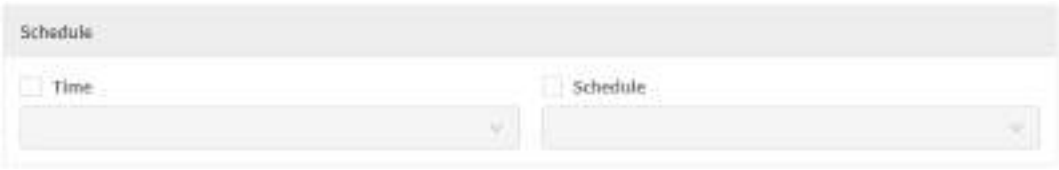
IPv6 – Properties - General

- ***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 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]**:



IPv6 – Properties - Schedule

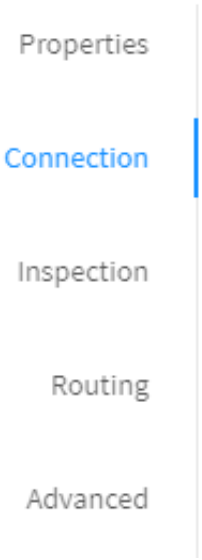
- ***Time*[ ]:** Caso a caixa de seleção estiver selecionada, determina se a regra se aplicará em dias úteis ("*Business*"), finais de semana ("*Weekend*") ou em algum outro objeto do tipo "*Time*" que tenha sido criado previamente;
- ***Schedule*[ ]:** Caso a caixa de seleção estiver selecionada, permite 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*.

- *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.



IPv6 - Abas Laterais - *Connection*

Nesta aba estão contidos os painéis:

- Source;
- Destination;
- Identification.

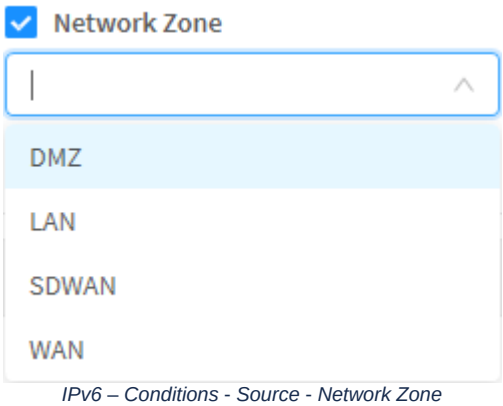
A seguir analisaremos a função de cada campo dos painéis.

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*]**:

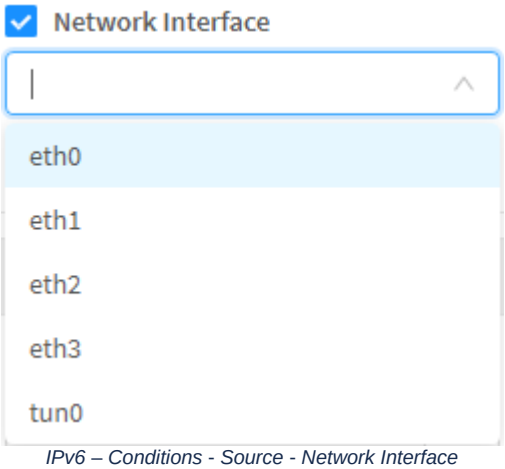
IPv6 – Conditions - Source

- ***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*;



IPv6 – Conditions - Source - Network Zone

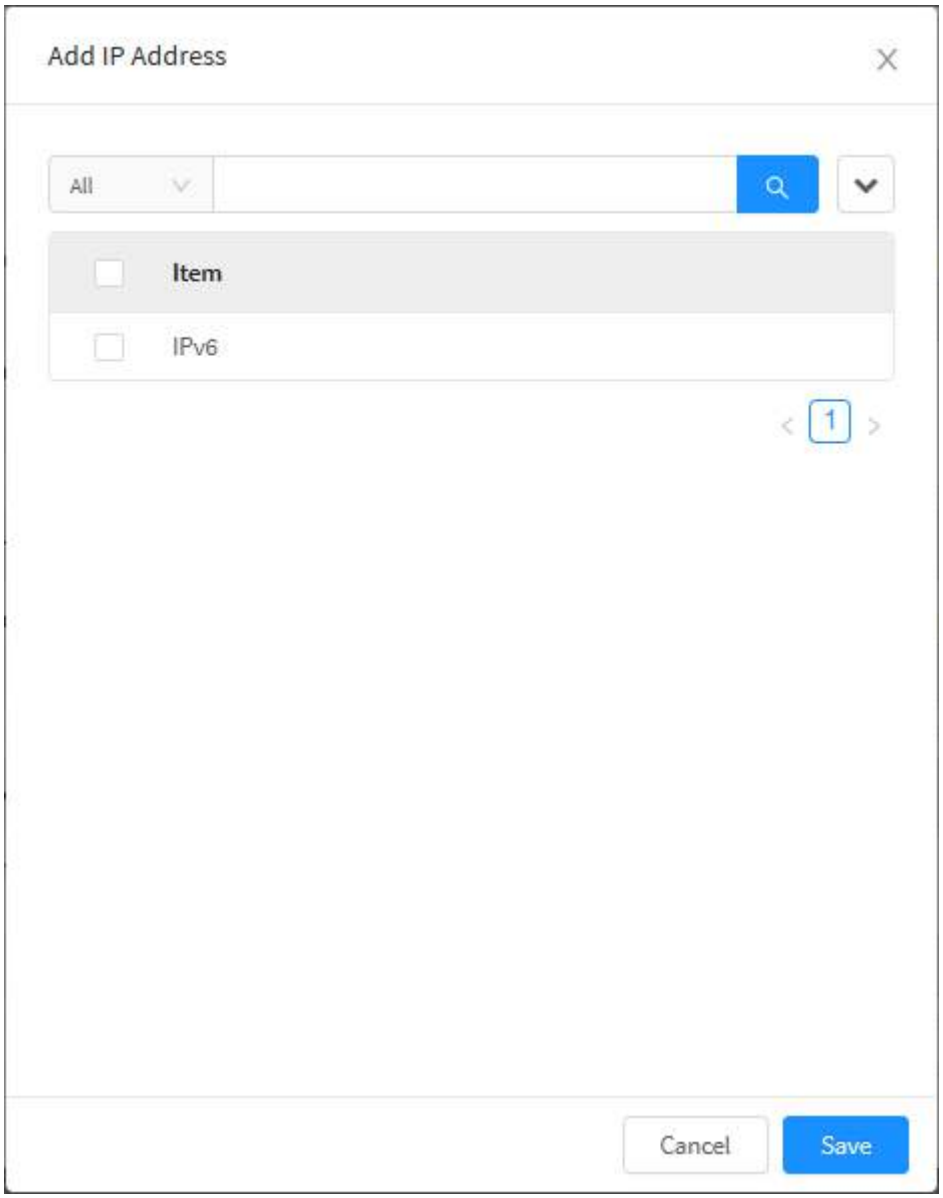
- ***Network Interface[ ]*:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar interface de rede para serem utilizadas como filtro de origem. As interfaces que aparecem nesse menu são criadas em *Network - Interfaces;*



IPv6 – Conditions - Source - Network Interface

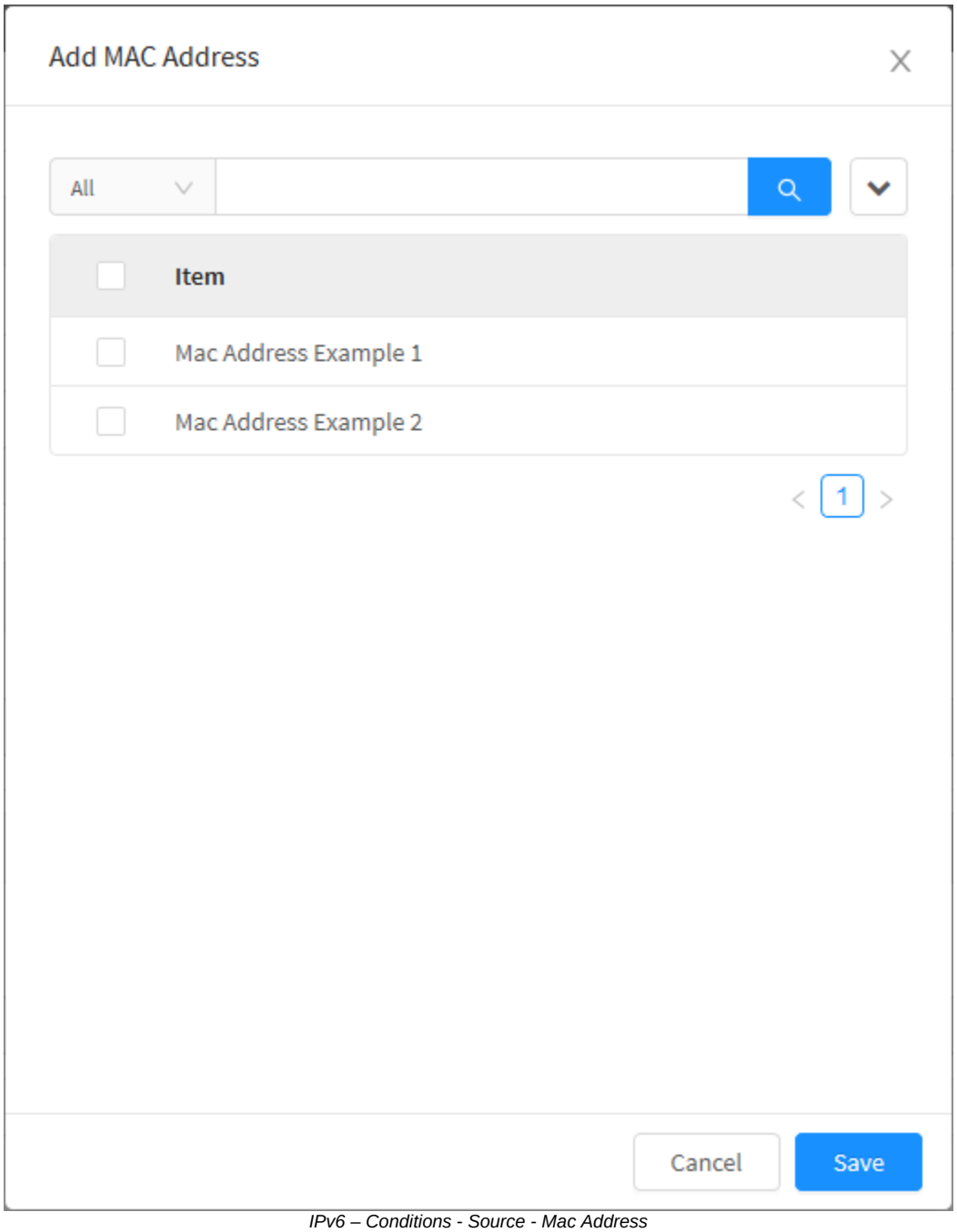
- ***IP Address[ ]*:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de Endereço *IPv6* (*IPs*, redes ou conjuntos) para serem utilizados como filtro de origem. Ao clicar sobre o botão **[ ]**, a tela abaixo será exibida para selecionar um ou mais 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.



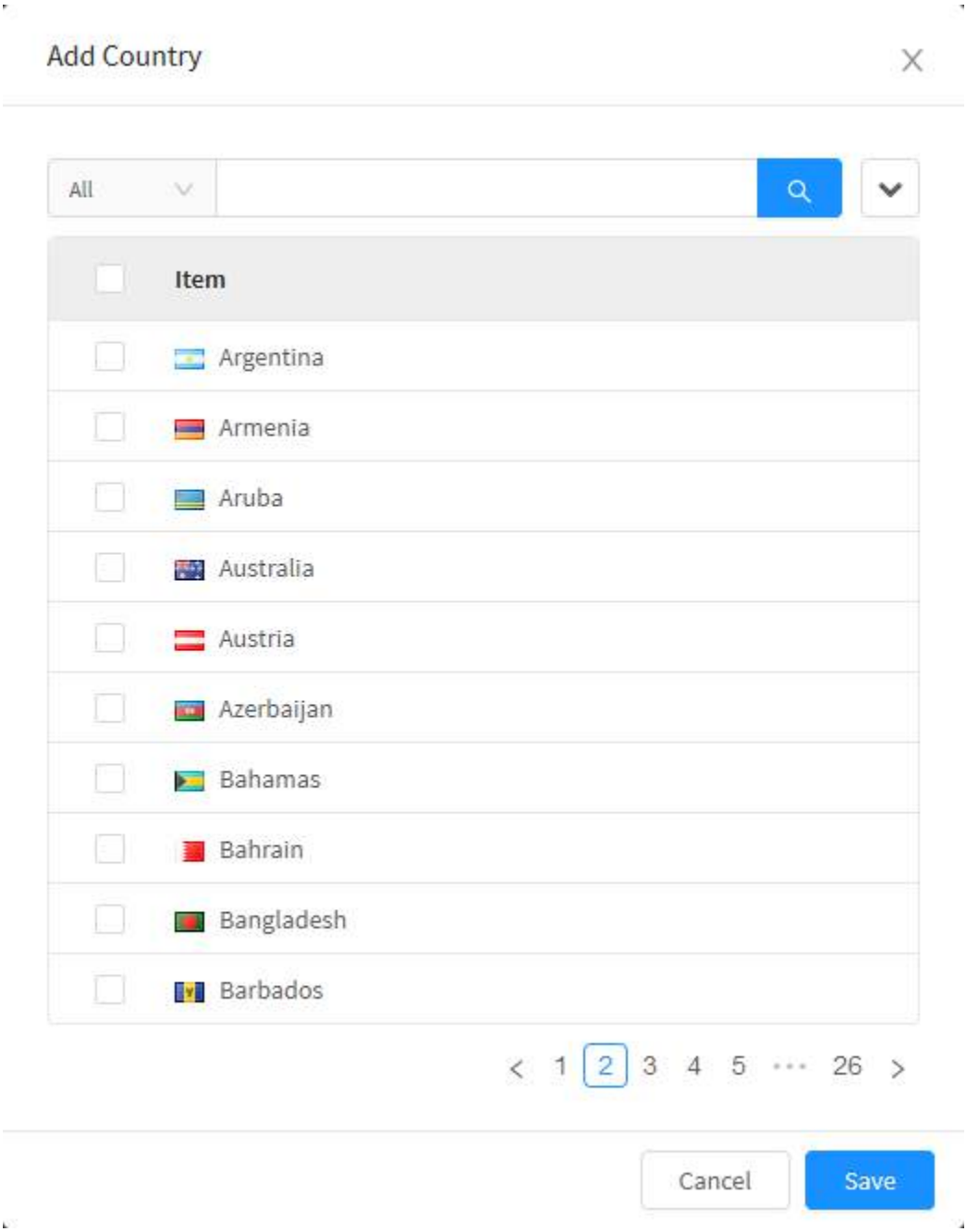
IPv6 – Conditions - Source - IP Address

- ***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*;



IPv6 – Conditions - Source - Mac Address

- ***Country[ ]*:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Países para serem usado como filtro de origem. Ao clicar sobre o botão **[ ]**, a tela abaixo será exibida para selecionar um ou mais país que irá compor a regra.



IPv6 – Conditions - Source - Country

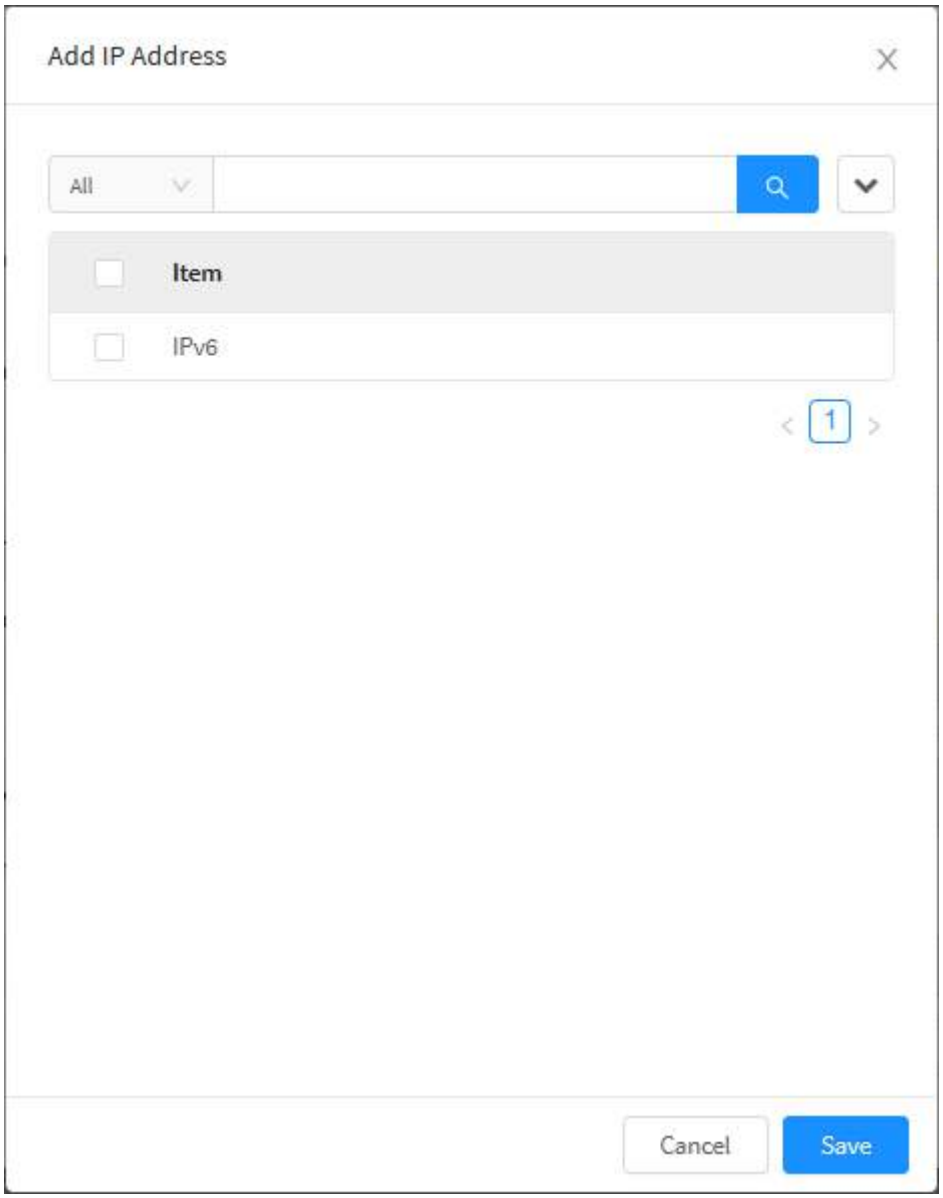
Destination

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*]**:

IPv6 – Conditions - Destination

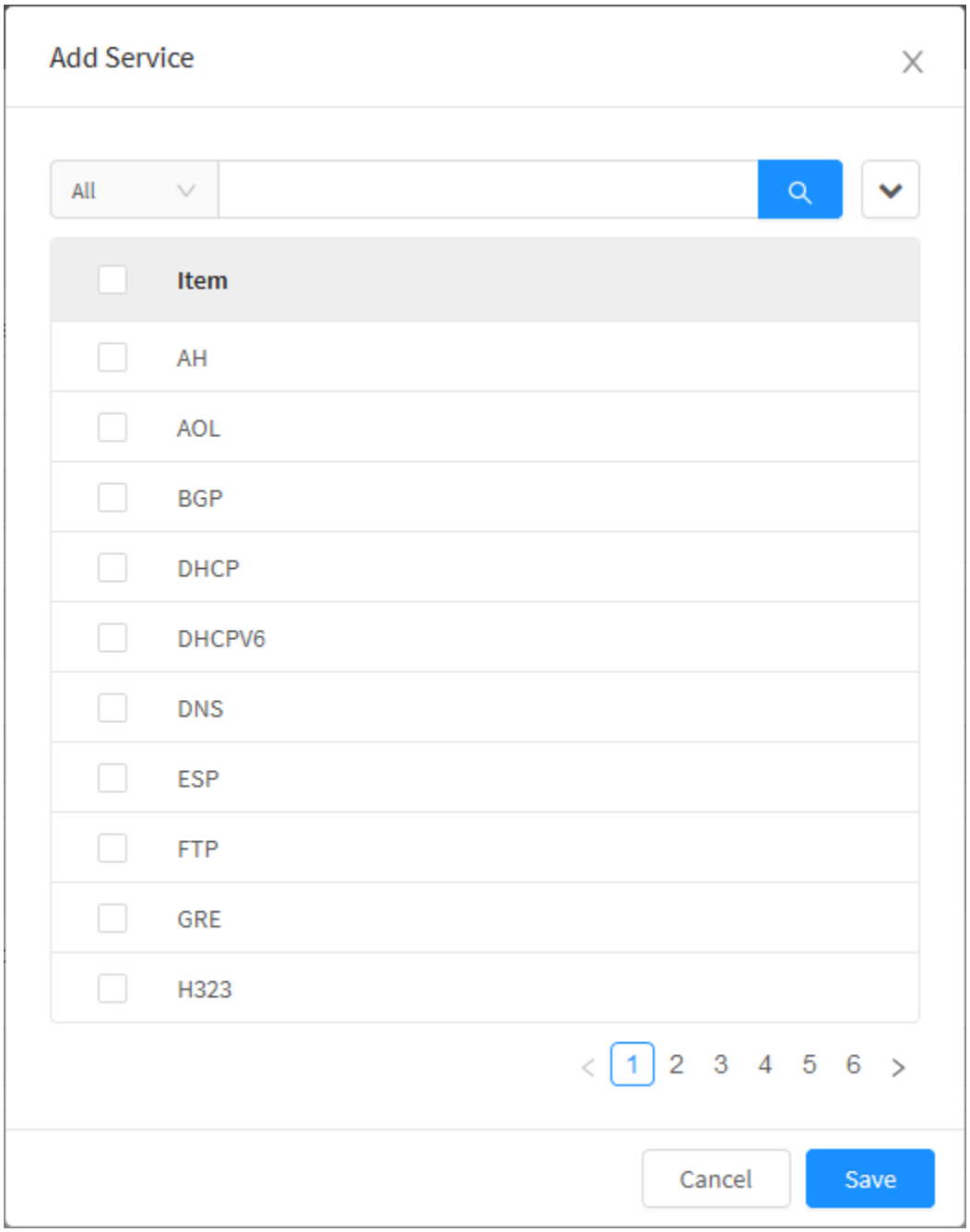
- ***IP Address[ ]*:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite selecionar Objeto(s) de Endereço *IPv6* (*IPs* , redes ou conjuntos) para serem utilizados como filtro de destino. Ao clicar sobre o botão **[ ]**, a tela abaixo será exibida para selecionar um ou mais 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.



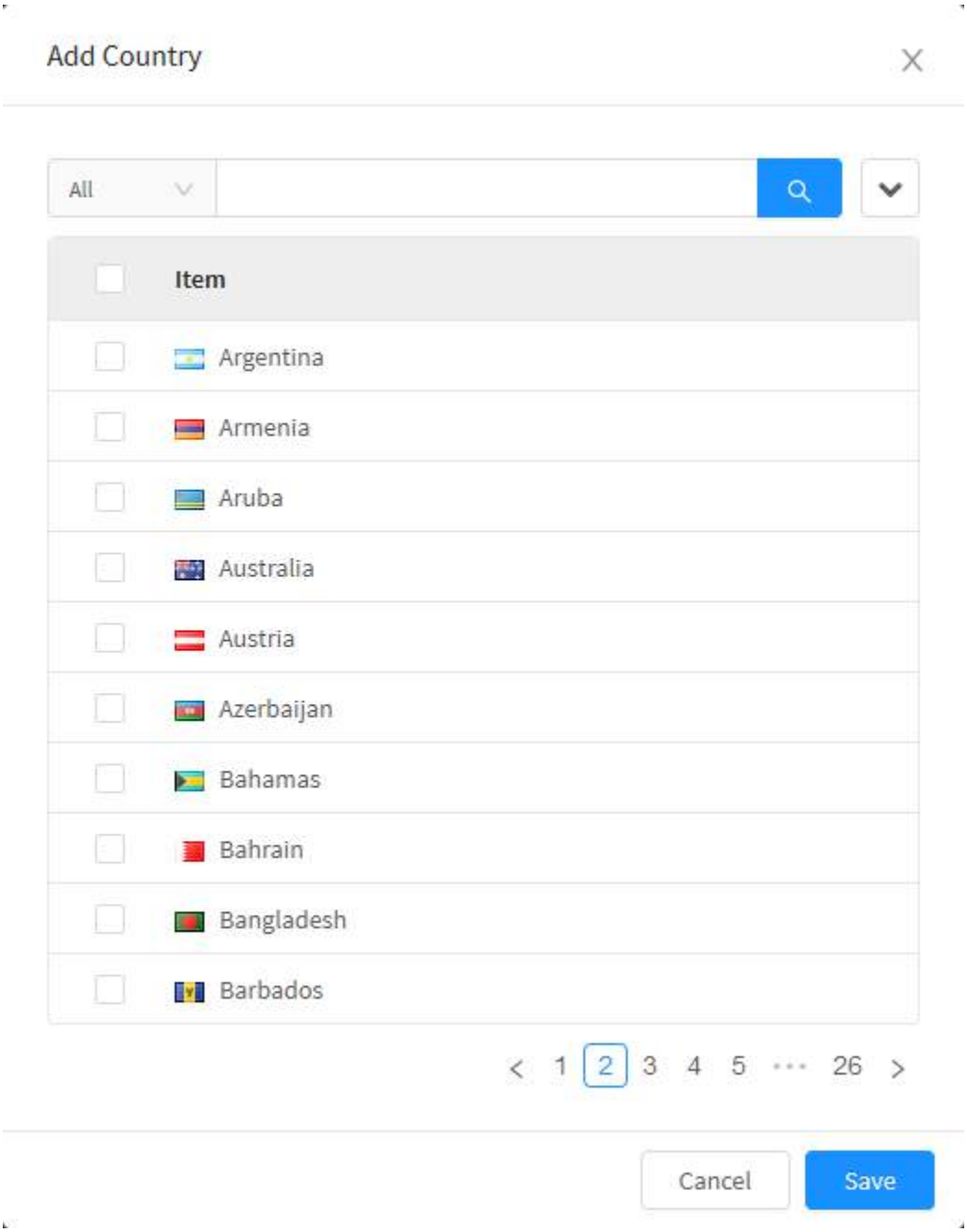
IPv6 – Conditions - Destination - IP Address

- ***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*;



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.



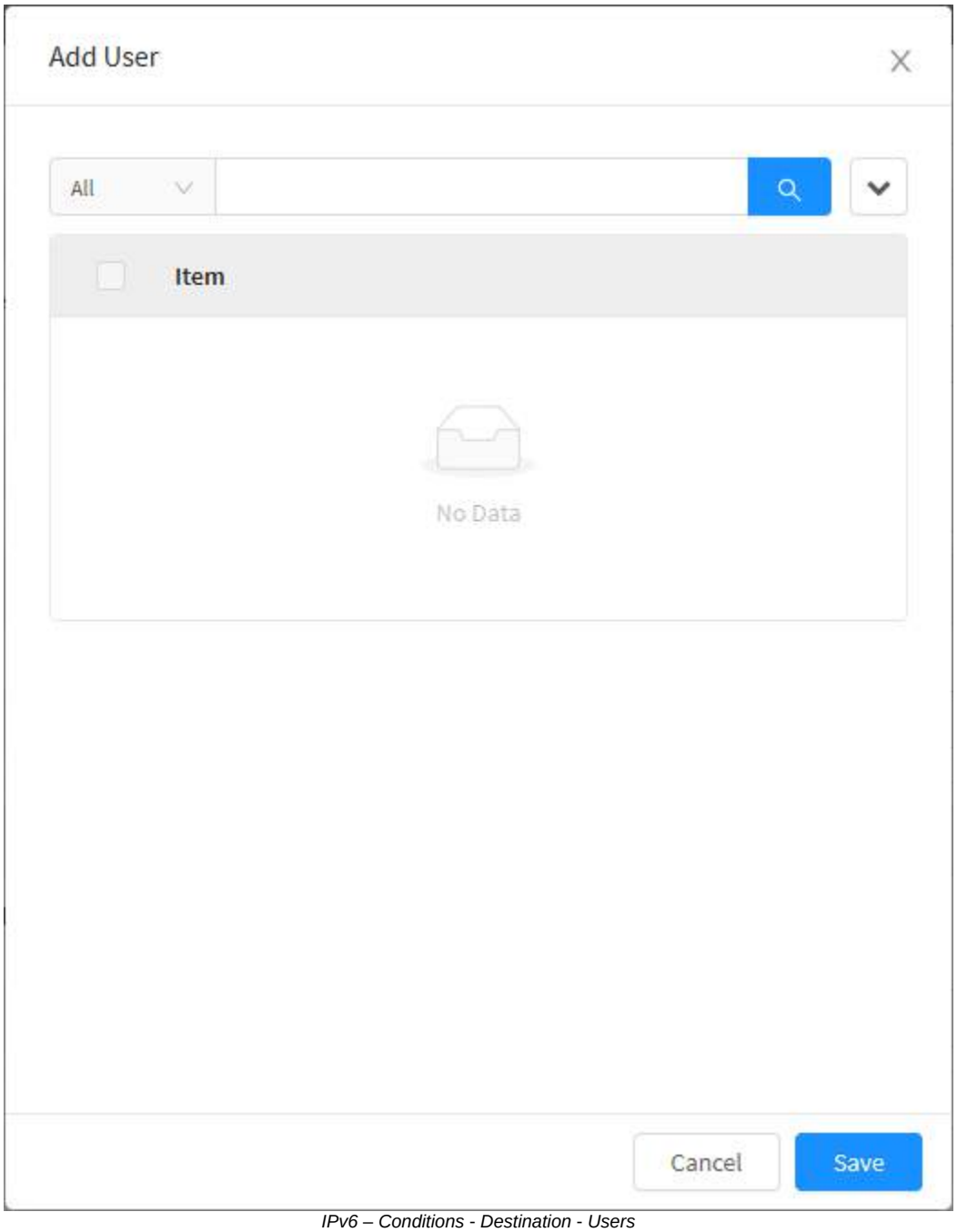
IPv6 – Conditions - Destination - Country

Identification

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*]**:

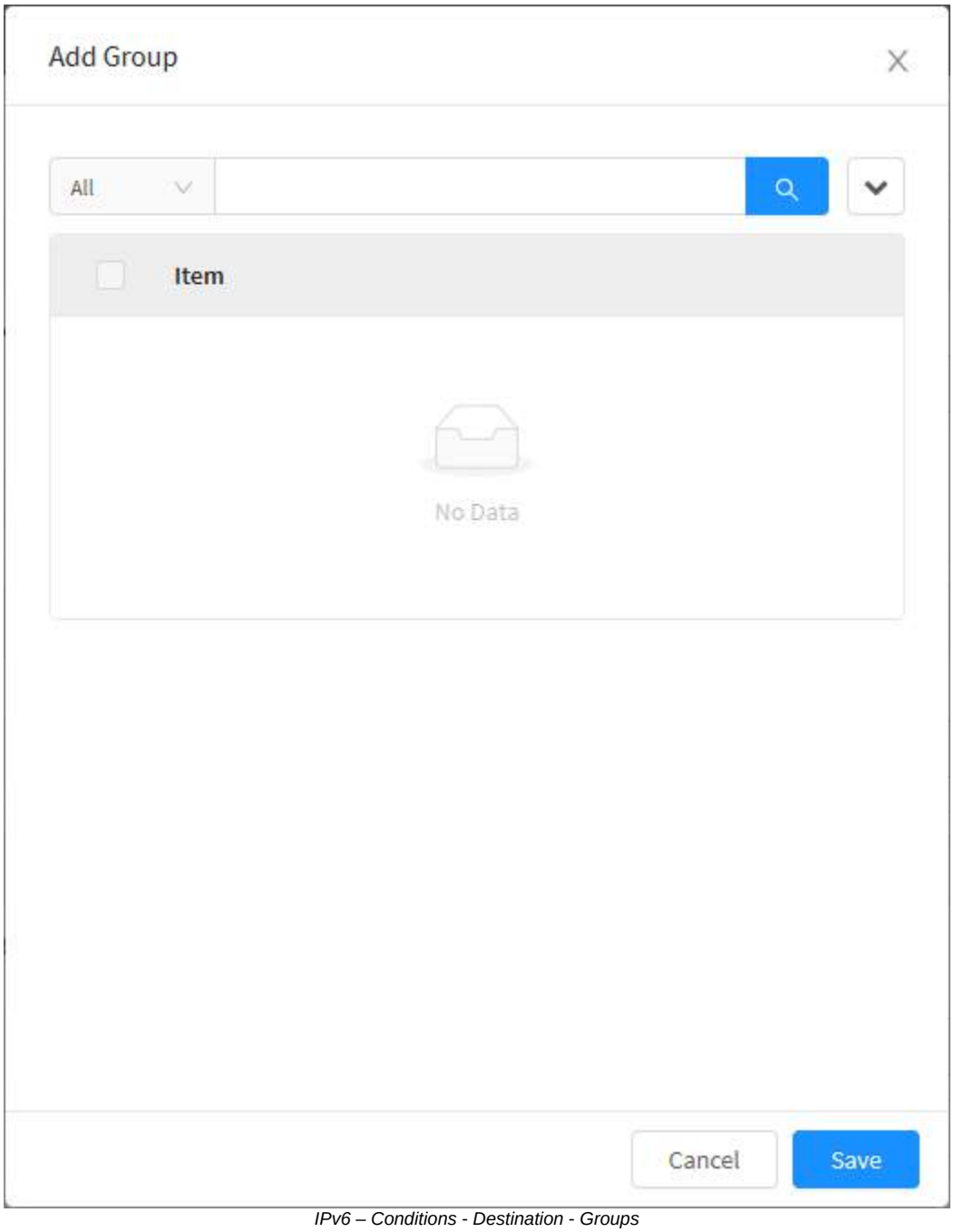
Policies IPv6 – Conditions - Identification

- ***Authenticated[ ]*:** Caso habilitada, esta caixa de seleção determina se a política exige autenticação;
- ***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 **[ ]**, a tela abaixo será exibida para selecionar um ou mais usuário que irão compor a regra;



IPv6 – Conditions - Destination - Users

- ***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.



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.

IPv6 - Abas Laterais - *Inspection*

Esta aba contém o painel

- Inspection.

Inspection

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel **[*Inspection*]**:

IPv6 – Inspection - 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*;

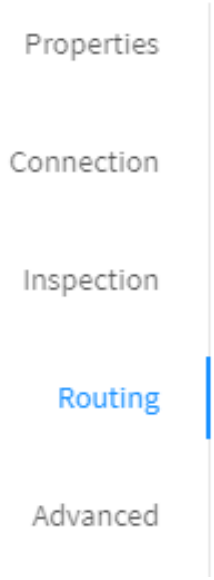
- ***Threat Protection*** **[ ]:** Este campo só fica disponível ao marcar a caixa de checagem. Este campo permite aplicar *IPS* nas políticas. Os perfis exibidos nesse menu são criados em *Services - Threat Protection*;
- ***Application Control*** **[ ]:** Este campo só fica disponível ao marcar a caixa 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*** **[ ]:** 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.



IPv6 - Abas Laterais - *Routing*

Nesta aba estão contidos os painéis:

- Gateway
- QoS
- *Application Routing*.

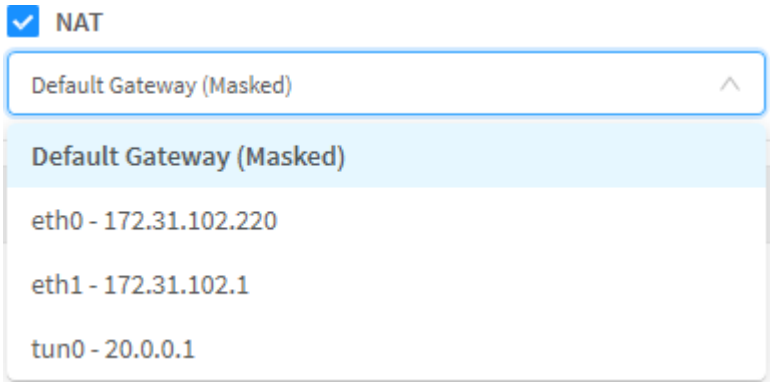
A seguir analisaremos a função de cada campo dos painéis.

Gateway

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel **[*Gateway*]**:

IPv6 – Routing - Gateway

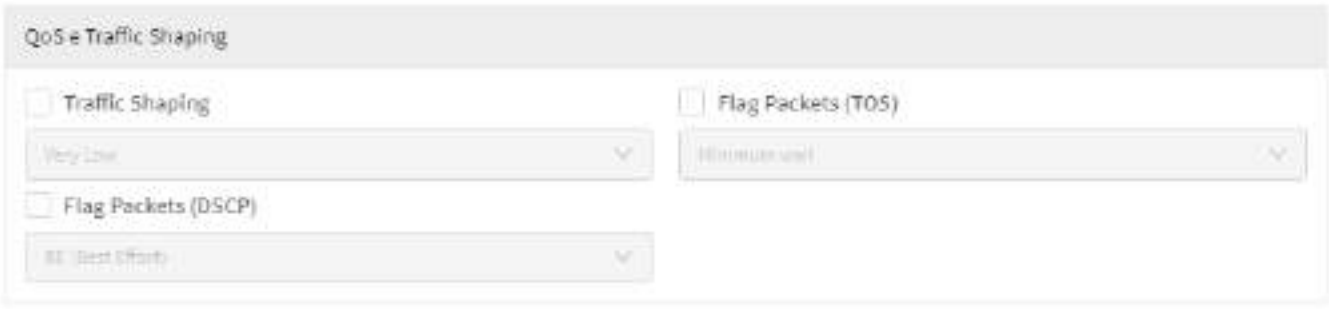
- ***NAT[ ]*:** Permite ativar o *NAT* e a escolha do endereço para tradução de origem, por padrão é configurado o *IP* do *link* do *Gateway* Padrão;



IPv6 – Routing - Gateway - NAT

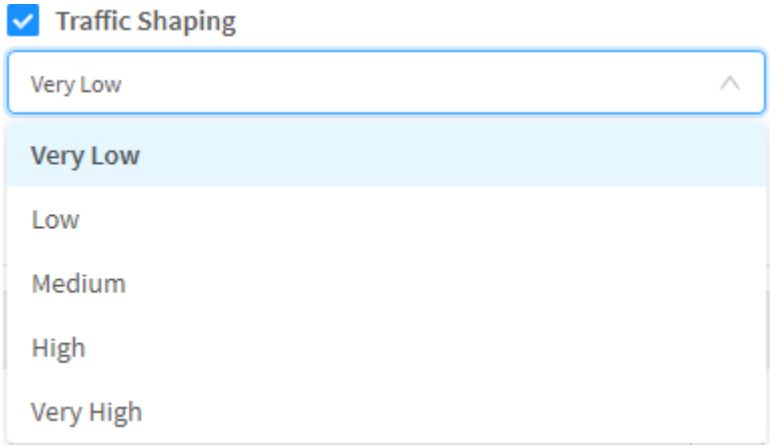
QoS

Abaixo segue uma descrição da função de cada campo do formulário exibido no painel **[*QoS*]**:



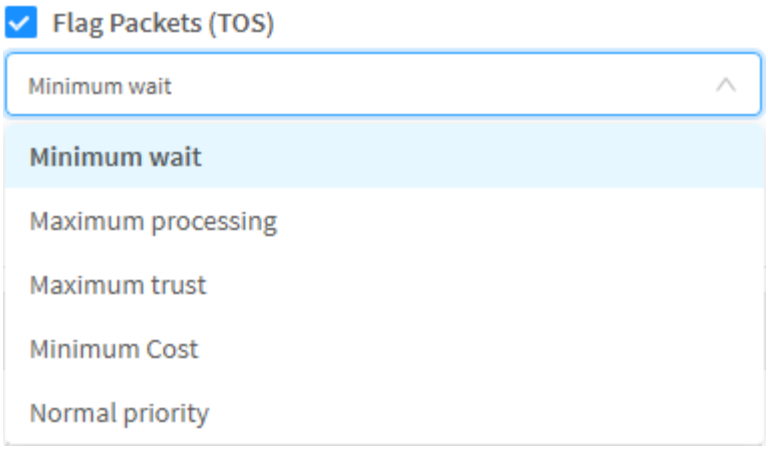
IPv6 – Routing - QoS

- ***Traffic Shaping[ ]*:** Permite ativar e selecionar a prioridade do tráfego, os valores podem ser ajustados em ***System >> Network >> Traffic Shaping;***



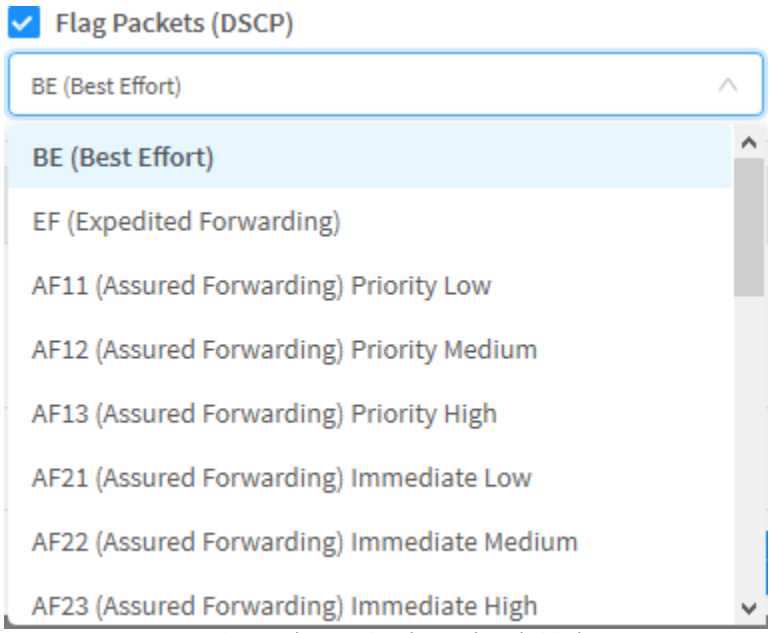
IPv6 – Routing - QoS - Traffic Shaping

- **Flag packets (*TOS*)[ ]:** Ao ativar permite a marcação do pacote conforme as opções: Espera mínima, Processamento máximo, Confiança máximo, Custo mínimo e prioridade normal;



IPv6 – Routing - QoS - Flag packets (TOS)

- ***Flag packets (DSCP)[ ]*:** Ao ativar permite a marcação do pacote conforme as opções.



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.

IPv6 - Abas Laterais - *Inspection*

Advanced

Abaixo segue uma descrição da função dos campos do formulário *Advanced*:

IPv6 – 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 *[☑]*:** 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.

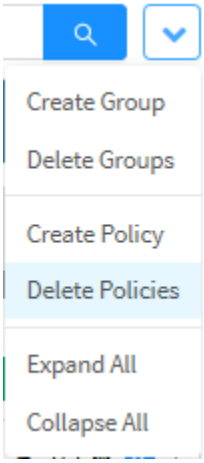
IPv6 - Menu de ações - Delete Policies

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*;

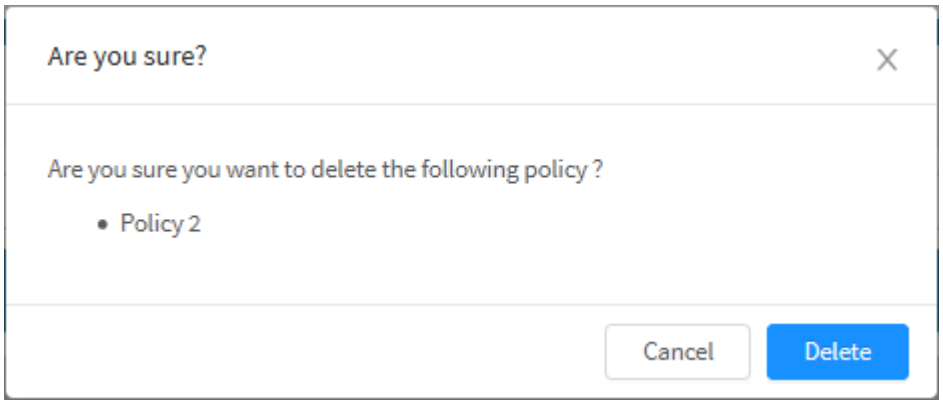
Políticas selecionadas para serem deletadas

2. No **menu de ações [ ]**, clique na opção “*Delete Policies*”;



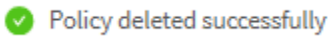
Policies IPv6 - Menu de Ações - *Delete Policies*

3. Surgirá a tela perguntando se deseja deletar os itens:



Policies IPv6 - Are you sure you want to delete the following policies

Caso desejar cancelar, clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].



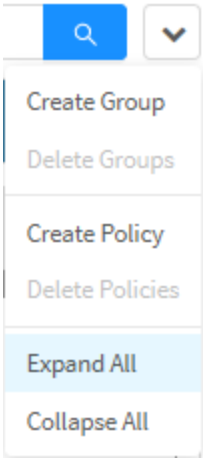
Policy Deleted successfully

As *Policies* foram removidas com sucesso.

IPv6 - Menu de ações - Expand All e Collapse All

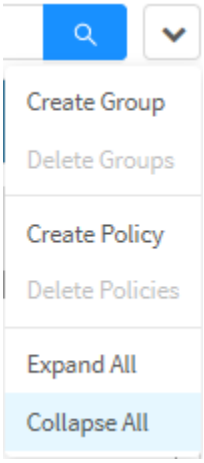
O botão “*Expand All*” tem como finalidade expandir o grupo de políticas. Para expandir o grupo de políticas, siga os seguintes passos:

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.

IPv6 – Policies

O topo do painel Policy contém:

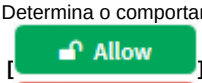
- **Nome do Pacote:** Apresenta o nome do Pacote de Políticas cadastrado;
- **Versão do Sistema[ ]:** Apresenta a versão na qual o Pacote de Políticas foi criado. É de extrema importância criar Pacotes de Políticas da mesma versão que o UTM, caso contrário, o pacote não será compatível;
- **IP[ ]:** 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*);
- **[ ]** Expande para exibir as políticas criadas no grupo;
- **[ ]** Informa quantas políticas existe no grupo;
- **[ ]** Permite editar as configurações adicionadas na opção *Create Group* do menu de ações;
- **[ ]** 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:

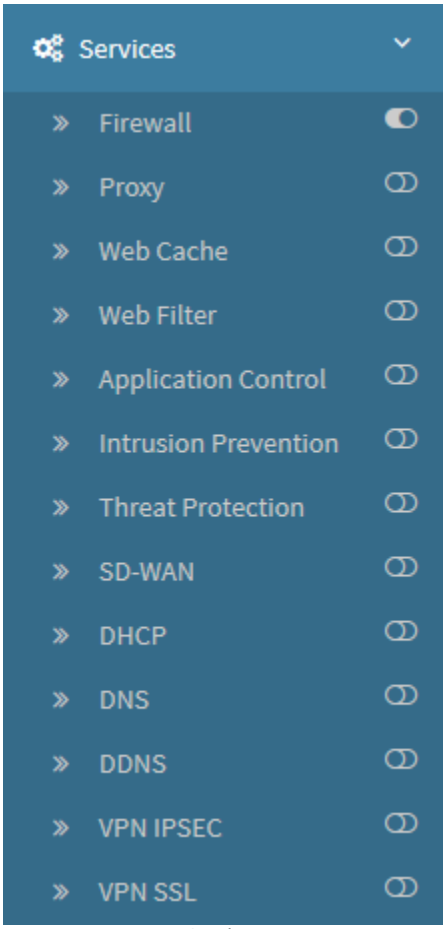
- ***Move*** **[**  **]:** Ao clicar e arrastar, move a ordem da política e permite reorganizar a prioridade de acordo com qual política está acima (*First Match Wins*);
- ***Id*** **[**  **]:** Exibe o número de identificação da política, é possível clicar nele para servir como filtro no campo de busca;
- ***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*****[**  **]:** 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*****[**  **]:** 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:
        - **[**  **]:** Como o próprio nome diz, esta opção serve para conceder acesso;
        - **[**  **]:** O acesso é negado;
        - **[**  **]:** O acesso é negado, porém uma mensagem de rejeição é exibida ao usuário.

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 [ ], para desativar um serviço utilize o botão [ ].



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.

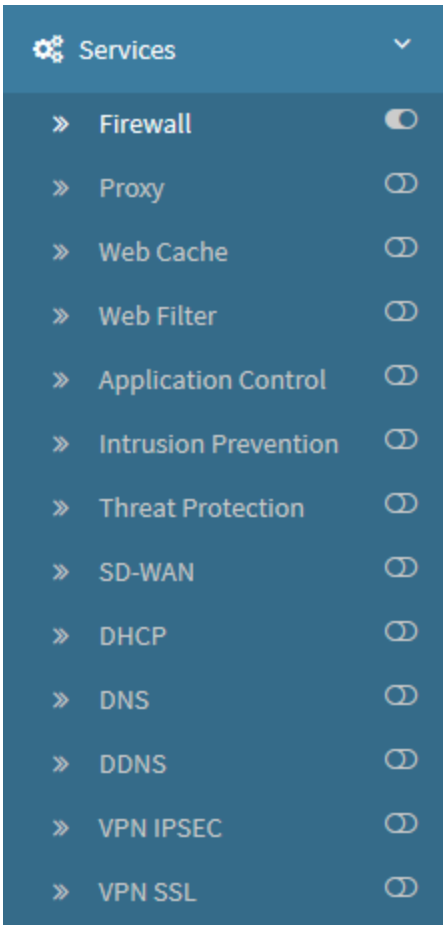
O Blockbit UTM foi projetado para proteger as informações confidenciais da sua organização através de controles de segurança utilizados para impedir a invasão de programas maliciosos na rede.

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 políticas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem como análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados e Controle de Tráfego.

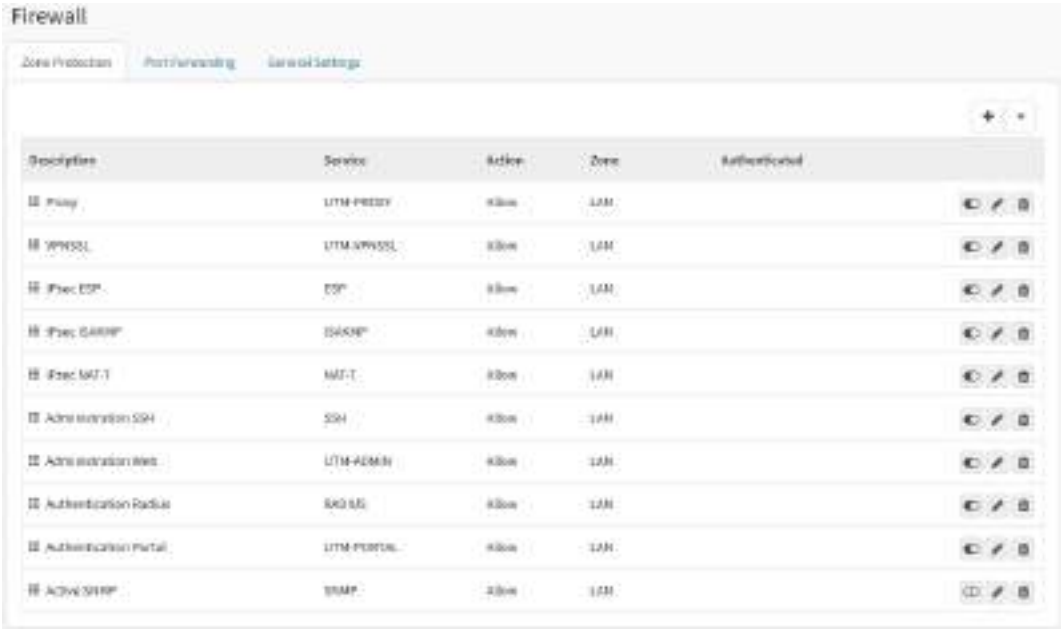
O serviço é pré-configurado para permitir acesso aos serviços locais do Blockbit UTM.

Para acessar esta tela, basta selecionar a opção "*Firewall*".



Services - Firewall

A tela abaixo será exibida:



Firewall

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.

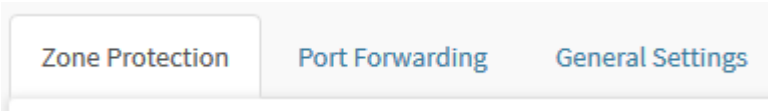
As políticas de *Zone Protection* por definição são caracterizadas por perfil de acesso, por *"*Zona de rede*"* e pelas *"*Ações*"* de tratamento do pacote que permite inclusive *"*Inspecionar*"* o tráfego de **[Entrada].**

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.

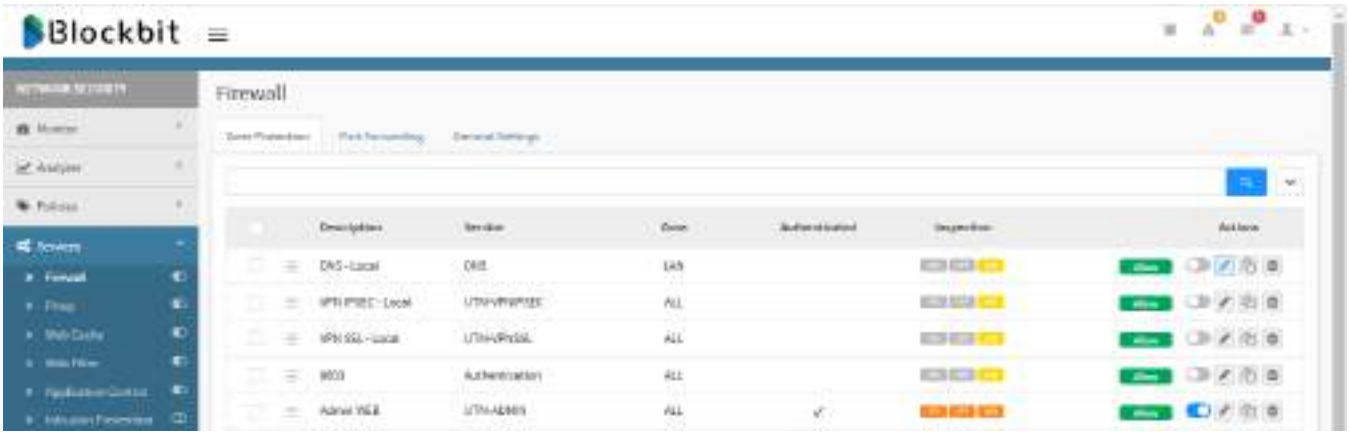
Para abrir a tela "*Zone Protection*", basta selecionar a opção "*Firewall*" no menu vertical à esquerda.

Caso a aba não esteja selecionada, clique em *"Zone Protection".*



Aba *Zone Protection*

Surgirá a tela "*Zone Protection*", conforme demonstrado pela imagem abaixo:



Zone Protection

A área de Zone Protection conta com uma barra de pesquisa que permite localizar objetos e conteúdos nestes objetos.

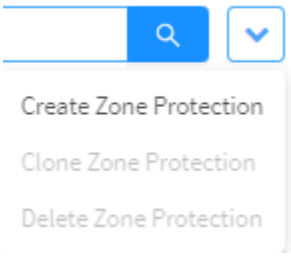
Esta sessão irá abordar:

- 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.

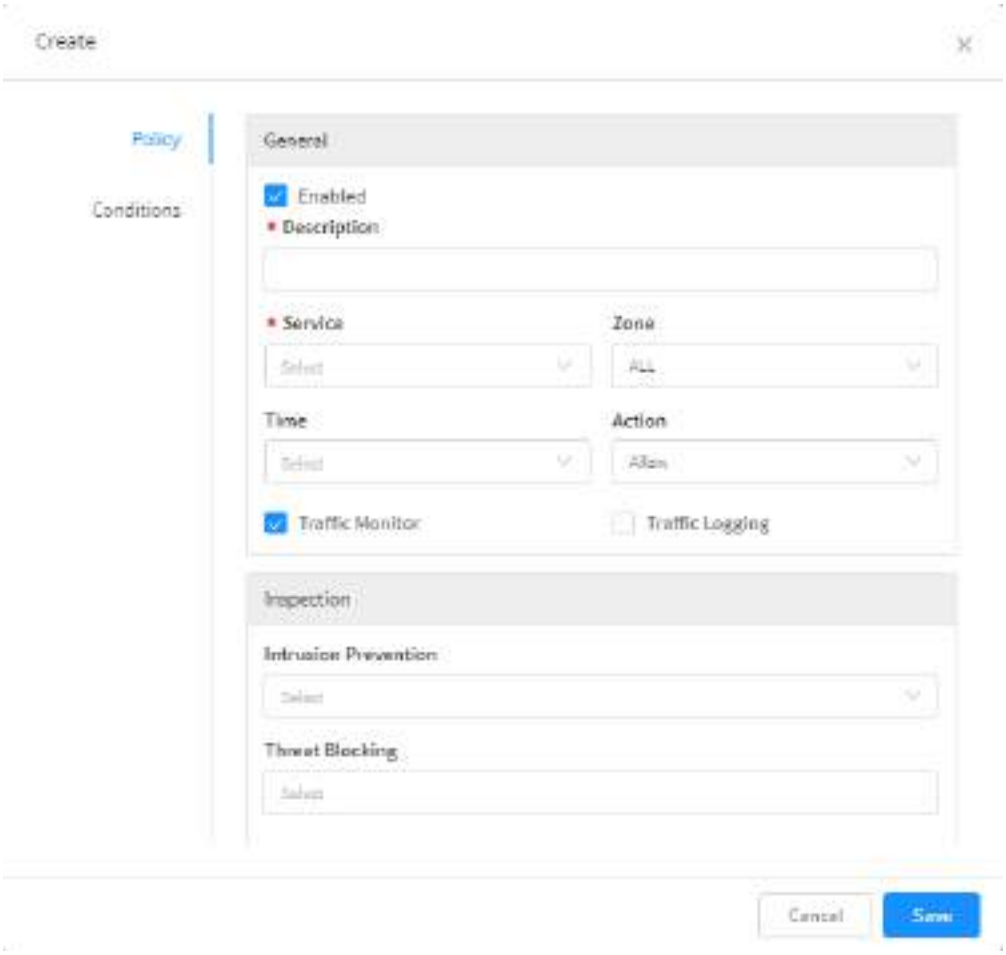
Zone Protection - Botão de Criação

Para criar uma política de *firewall* do tipo *Zone Protection* específica, clique no botão localizado no canto superior direito:



Zone Protection – Botão de Criação

Ao clicar neste botão a janela abaixo é exibida:



Zone Protection – Botão de Criação - Janela

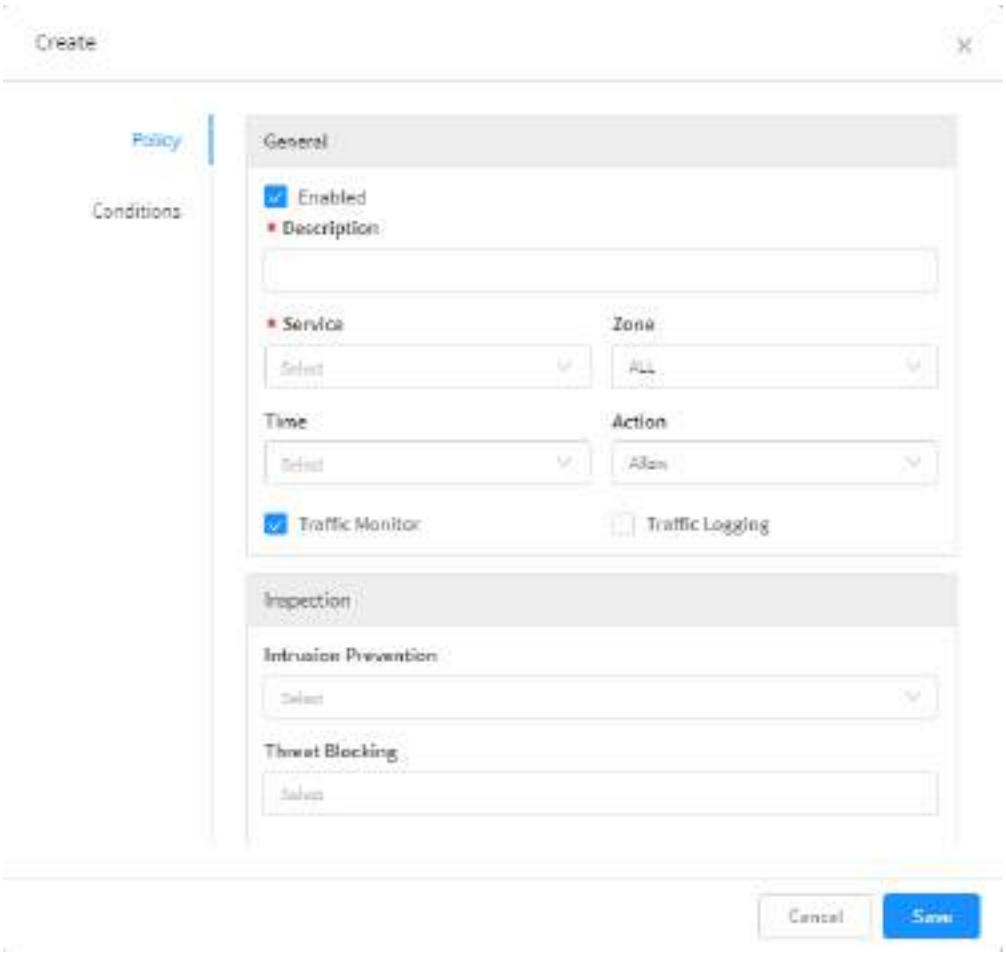
O menu é composto pelas sessões:

- *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:



Zone Protection – Policy

- ***Enabled*[ ]:** Determina se estará com o *status* **ativado**[ ] ou **desativado**[ ];
- ***Description*:** Define uma descrição para identificação;
- ***Service*:** Determina o serviço que será utilizado na criação da política, os serviços que aparecerem neste campo são criados em *Objects - Services*;
- ***Zone*:** Determina o tipo de agrupamento de *interfaces* que será utilizado. Estes agrupamentos são criados em *Network - Interfaces*;
- **Time:** Determina o tempo no qual a política será aplicada, os itens que aparecerem neste campo são criados em *Objects* - Times;
- ***Action*:** Define a ação que será tomada, podendo ser:
  - ***Allow*;**
  - ***Deny*;**
  - ***Reject*.**
- **Traffic Monitor:** Ao checar a caixa *Traffic Monitor*[ ], 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.

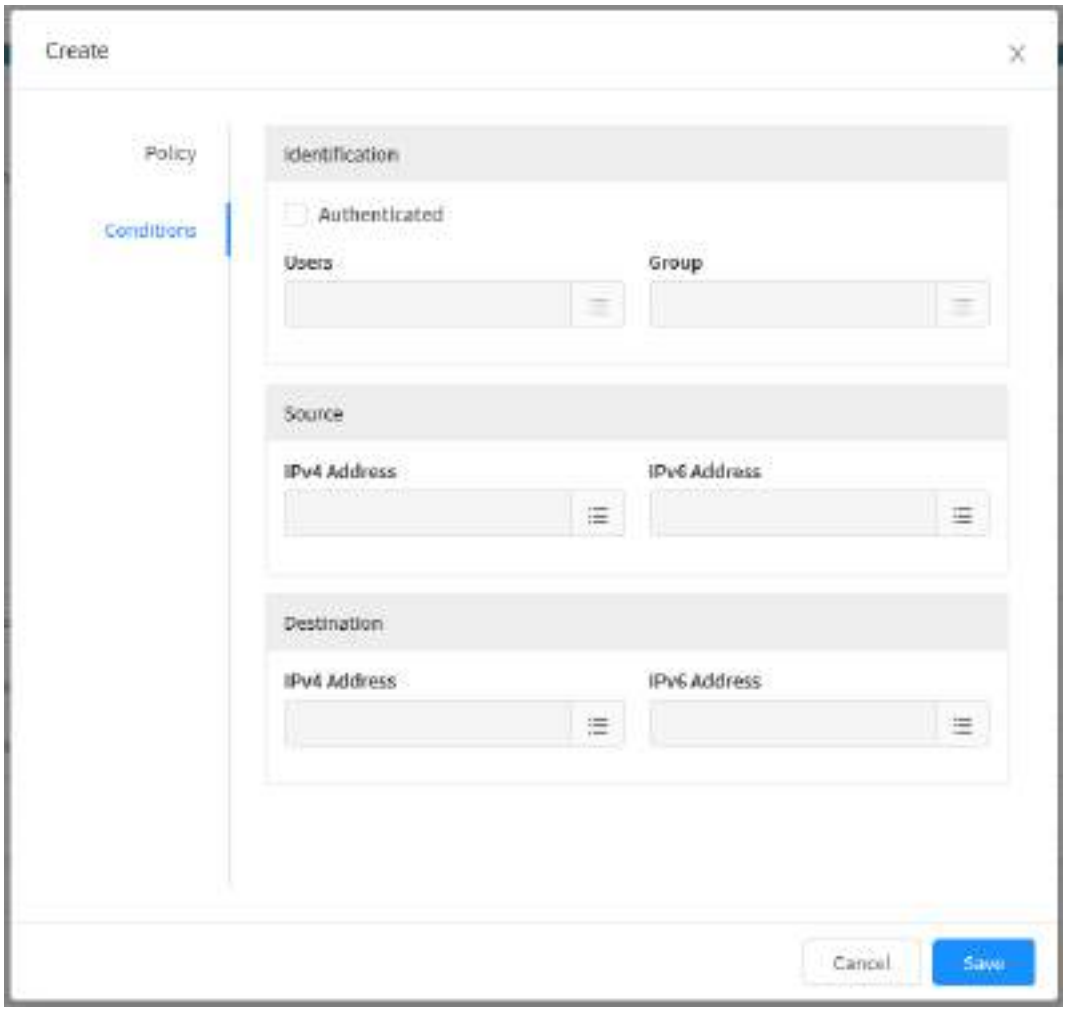
Isso conclui a configuração, caso não seja necessária nenhuma "*condition*", salve as alterações clicando em ***Save*[Save]**, caso deseje fechar essa janela, clique em **[ ]** para cancelar todas as configurações e voltar a tela anterior.

Após salvar, será necessário acessar a **fila de comandos [1]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

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:



Zone Protection – Conditions

- ***Authenticated[ ]:*** 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 salvar as alterações clique em ***Save*[Save]**, caso contrário, clique em **[ ]** para cancelar todas as configurações e voltar 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 comandos acesse a página: UTM - Fila de comandos.

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).

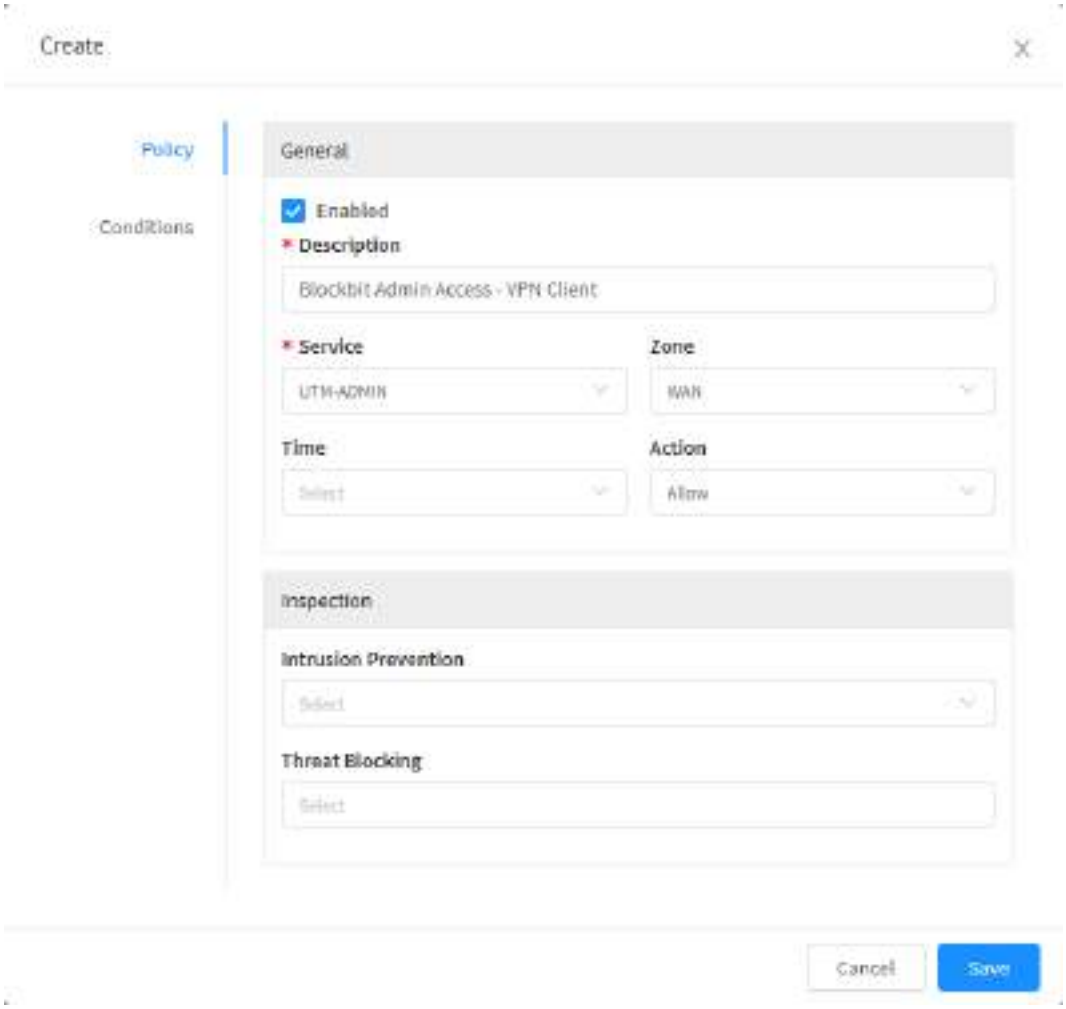
Para mais informações sobre como efetuar a remoção, clique nesta página.

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.

Policy



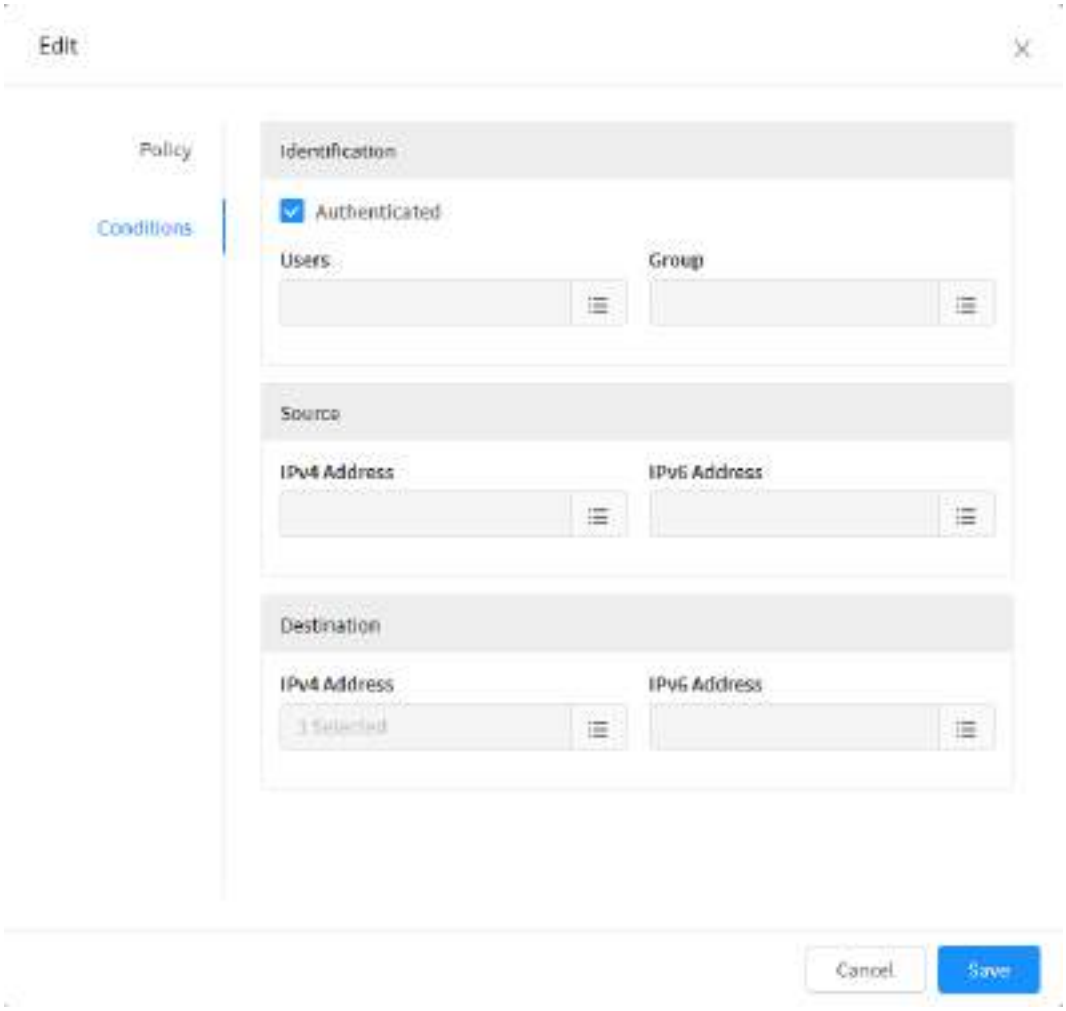
Zone Protection - Access interface admin for VPN client - Policy

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



Zone Protection - Access interface admin for VPN client - Conditions

Complete especificamente os campos à seguir:

- **Authenticated [ ]:** 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.

Por fim, clique em ***Save***[Save], caso contrário, clique em [ ] para cancelar todas as configurações e voltar 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 comandos acesse a página: UTM - Fila de comandos.

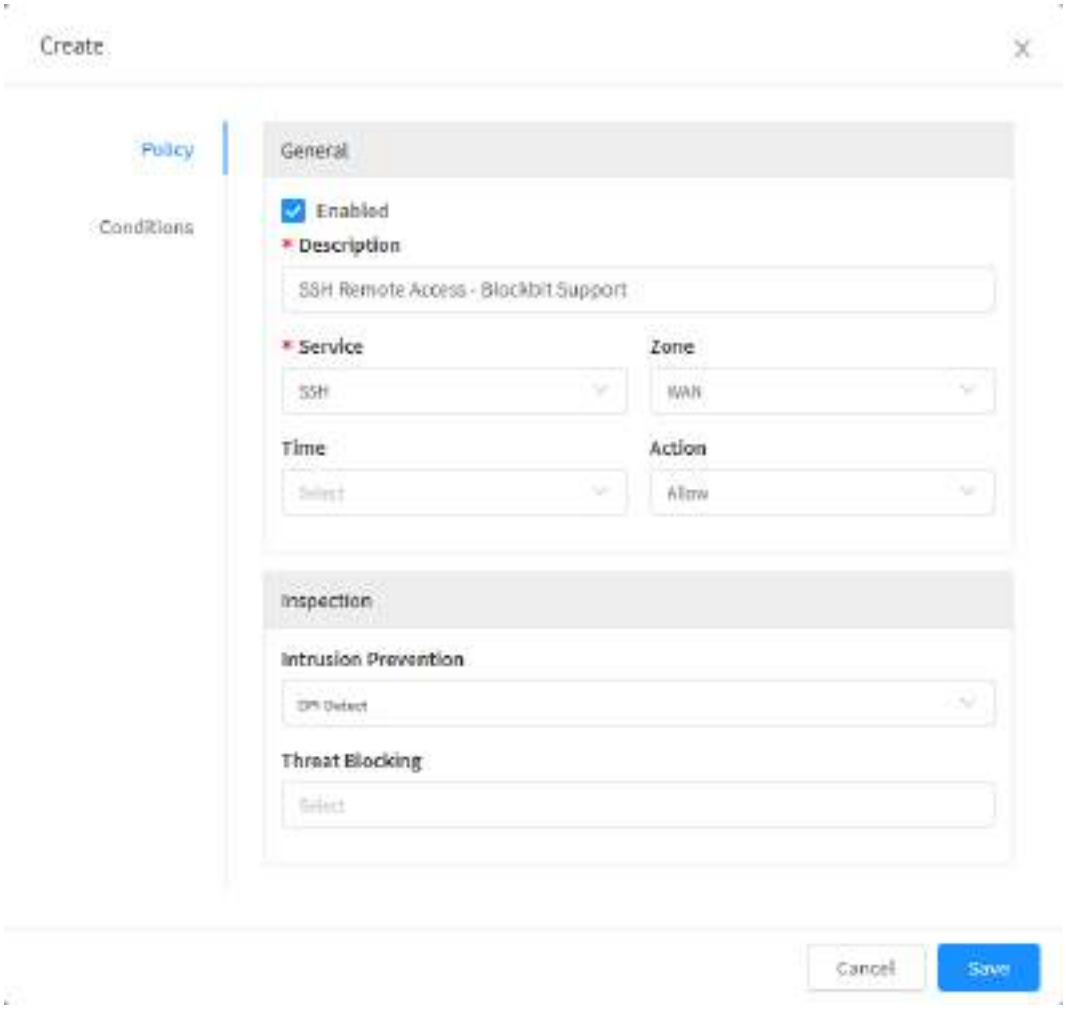
Isso conclui o exemplo 1.

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.

Policy



Zone Protection - SSH Remote Access – Policy

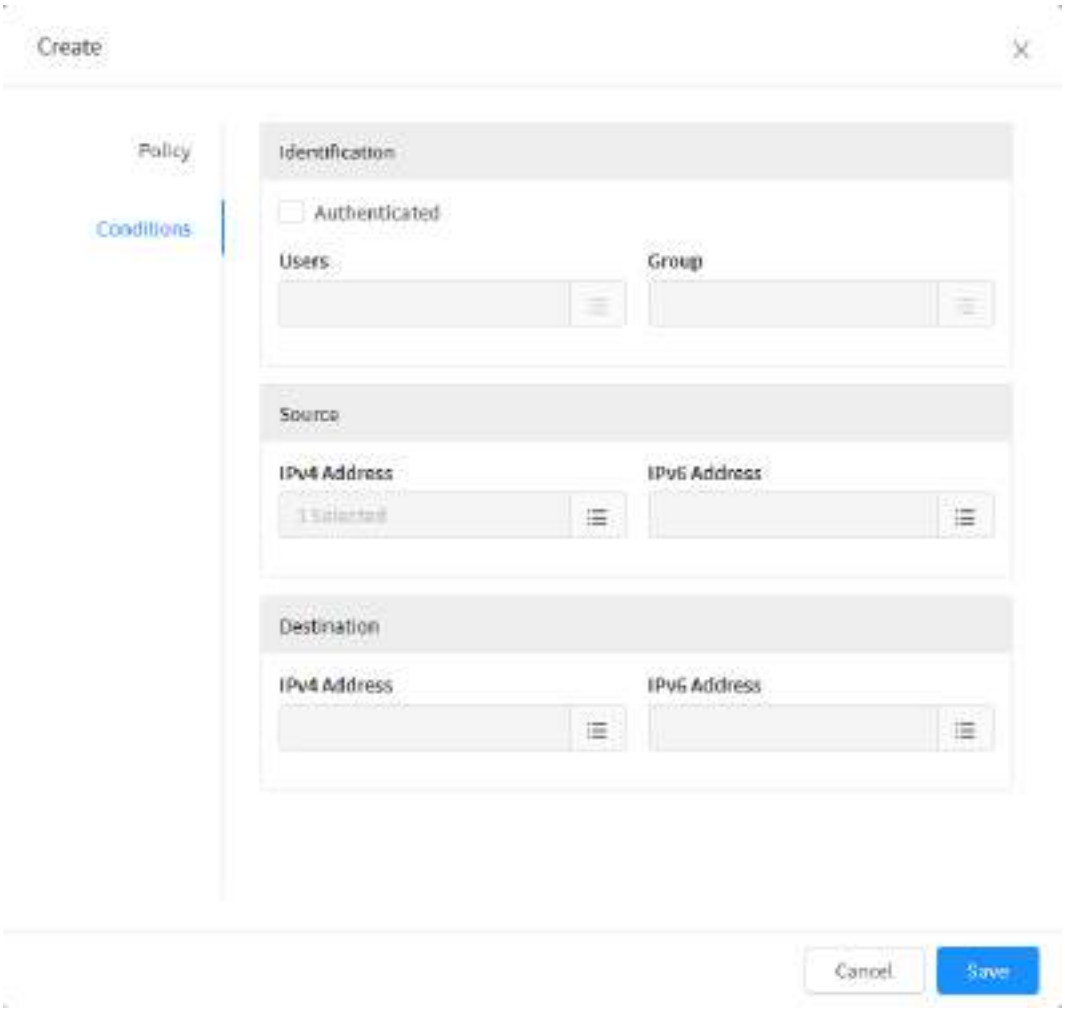
Complete especificamente os campos à seguir:

- ***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

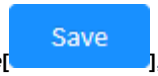


Zone Protection - SSH Remote Access - Conditions

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.

Por fim, clique em ***Save***[

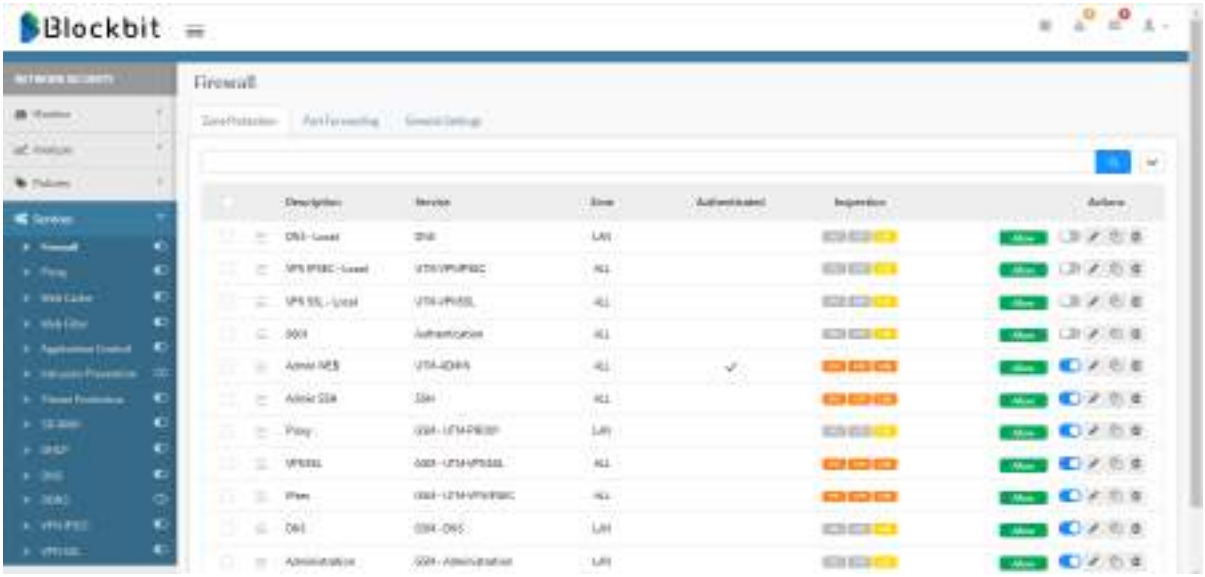
], caso contrário, clique em **[**  **]** para cancelar todas as configurações e voltar a tela anterior.

Após salvar, será necessário acessar a **fila de comandos [**  **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Isso conclui o exemplo 2.

Zone Protection - Colunas

A seguir, explicaremos cada coluna da aba *Zone Protection*:



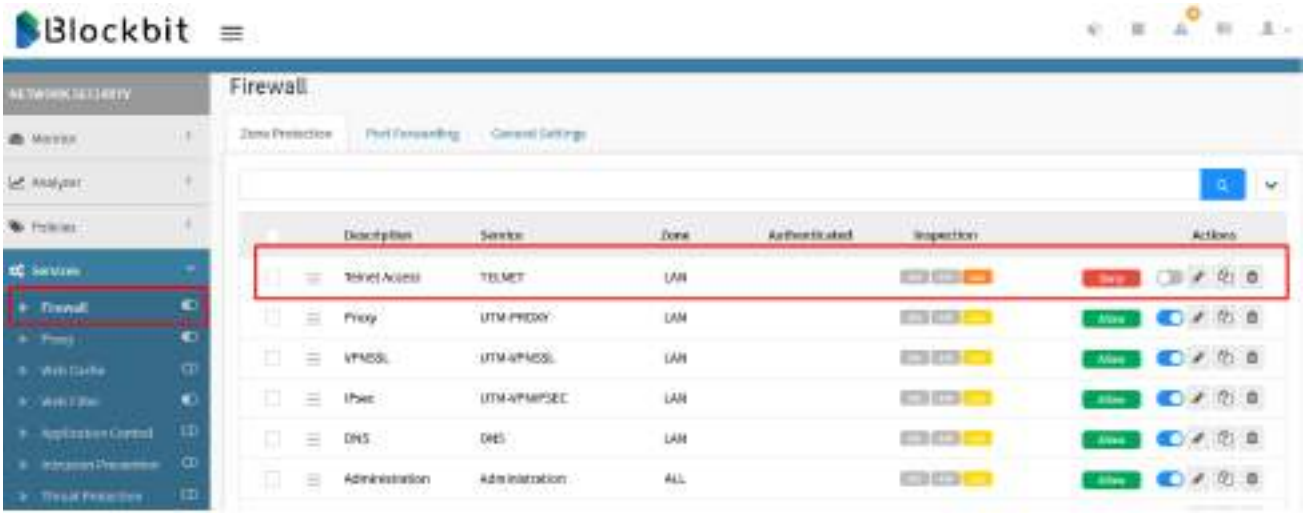
Zone Protection

- ***Select* [ ]:** Permite selecionar uma política do *Firewall;*
- ***Move*[ ]:** 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;
- ***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;
- ***Inspection*:** Exibe caso a política tenha ativado *Intrusion Prevention* [IPS], *Threat Blocking* [ATP] *ou Log*[LOG];
- ***Actions Menu*:** Disponibiliza as seguintes ações essenciais:
  - **Botão *Enable*[ ]/*Disable*[ ]:** Permite ativar ou desativar uma política do *Firewall*;
  - **Botão *Edit*[ ]:** Permite editar as configurações da *interface* cadastrada no Botão de Adição;
  - **Botão *Delete*[ ]:** Permite remover um dos itens.
  - **Botão *Clone*[ ]:** Permite clonar uma das políticas.

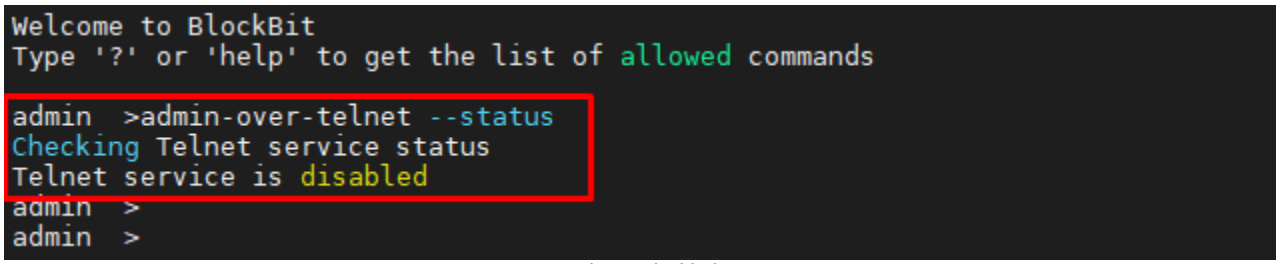
Zone Protection - Coluna Services

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.

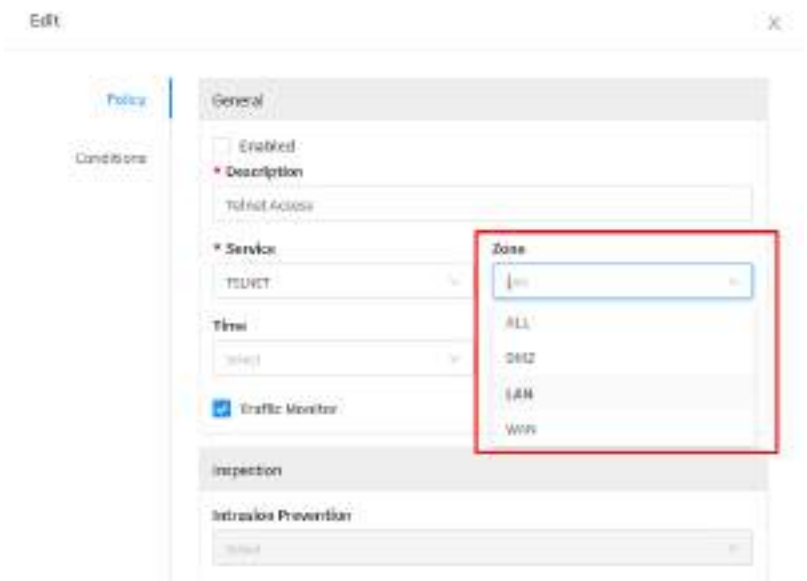


Firewall - Zone Protection

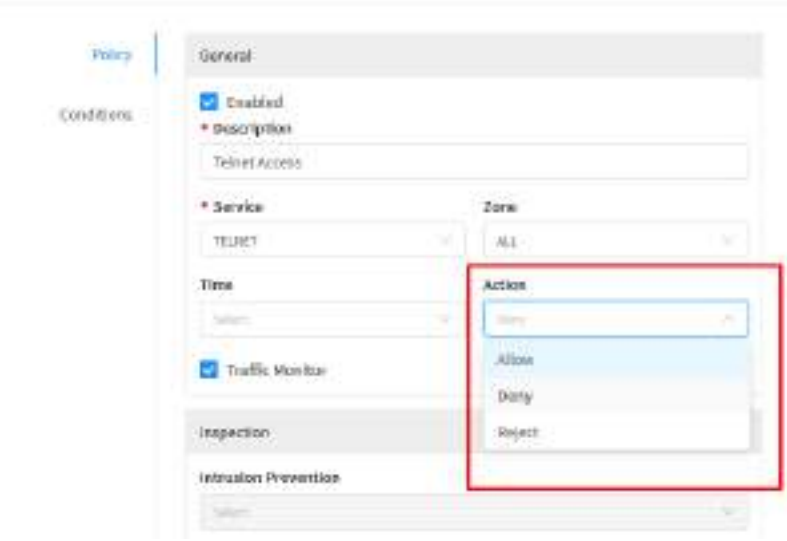


Telnet - Disabled

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*:



Zone Protection - Create - Zone



Zone Protection - Create - Action

Após criar, a regra será exibida na tela principal da seguinte maneira:

Zone Protection - Telnet Rule

Abaixo vemos os comandos que podem ser utilizados para gerenciar a função:

```
admin  >
admin  >
admin  >admin-over-telnet
Usage: admin-over-telnet <enable|disable|status>

--enable: Enables service
--disable: Disables service
--status: Check service status

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>

admin  >
```

CLI Interface - Telnet Management Commands

Utilizando o comando *"admin-over-telnet --enable"* habilitamos o serviço Telnet pela porta 23:

```
admin  >
admin  >admin-over-telnet --enable
Success Telnet service, enabled and started
admin  >
```

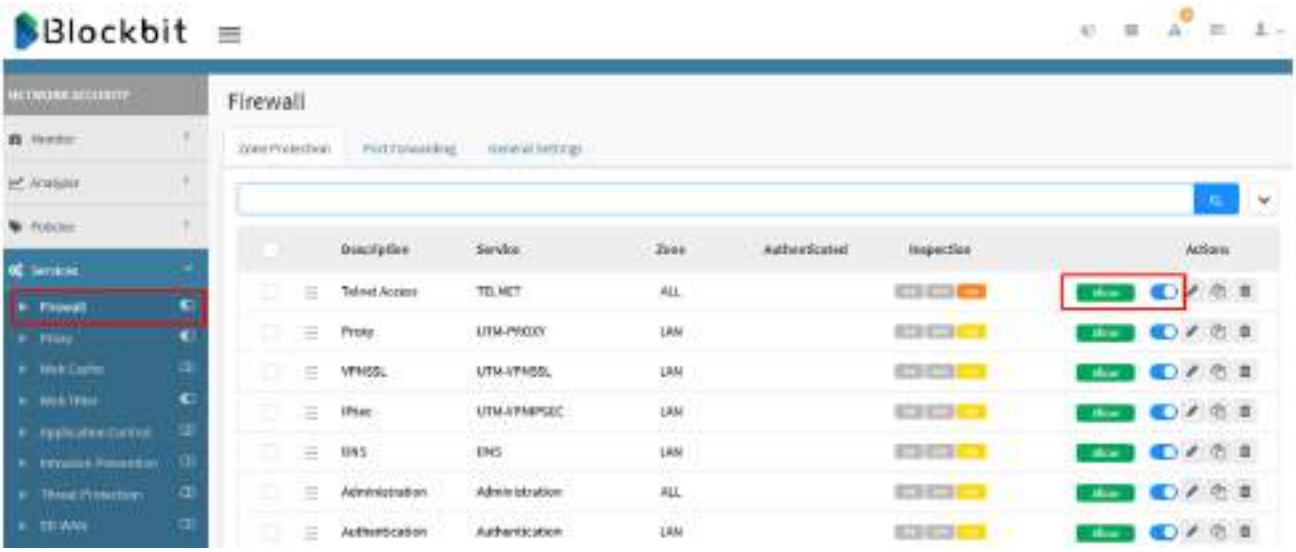
Enabling Telnet

Para desabilitar, devemos utilizar o comando "*admin-over-telnet --disable*":

```
admin  >
admin  >admin-over-telnet --disable
Telnet disabled with success
admin  >
```

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:

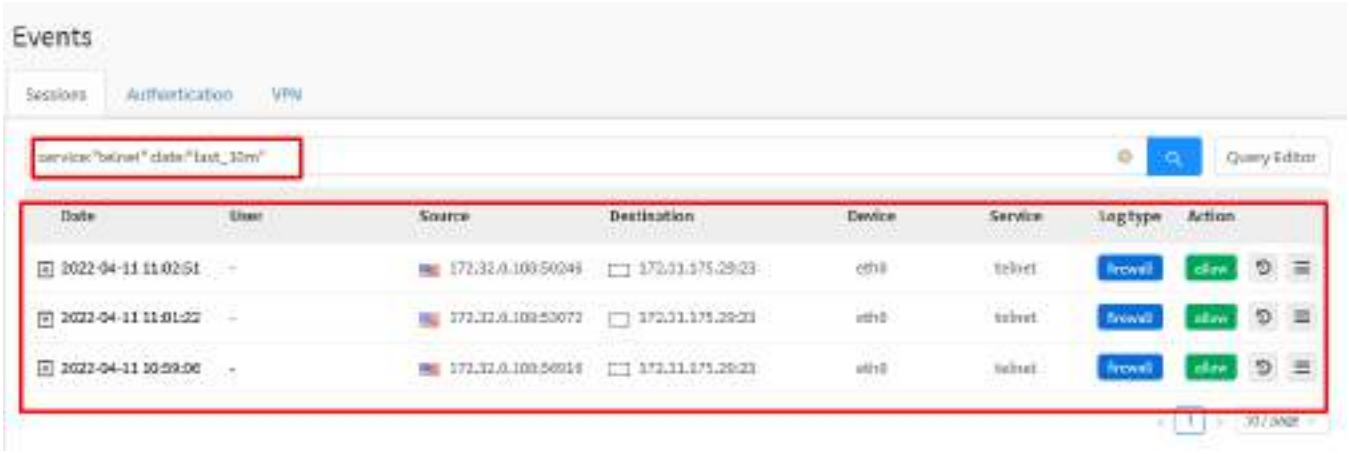


Zone Protection com Telnet Habilitada

As regras com o serviço Telnet habilitado podem ser visualizadas em Security Events:

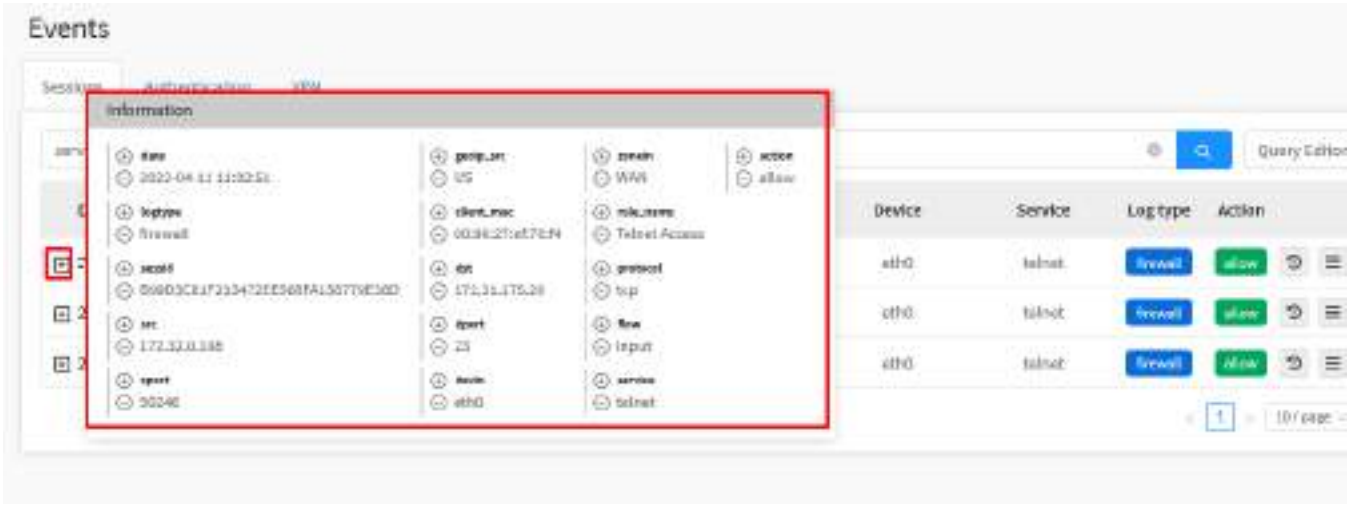
Enabled Telnet

Utilizando o Query editor, podemos pesquisar também as regras com Telnet ativo:



Security Events - Query Editor

Ao clicar sobre o botão de mais [⊞] é possível obter mais informações sobre da regra:



Query Editor - More information

Em Live Sessions também podemos conferir a regra em funcionamento:

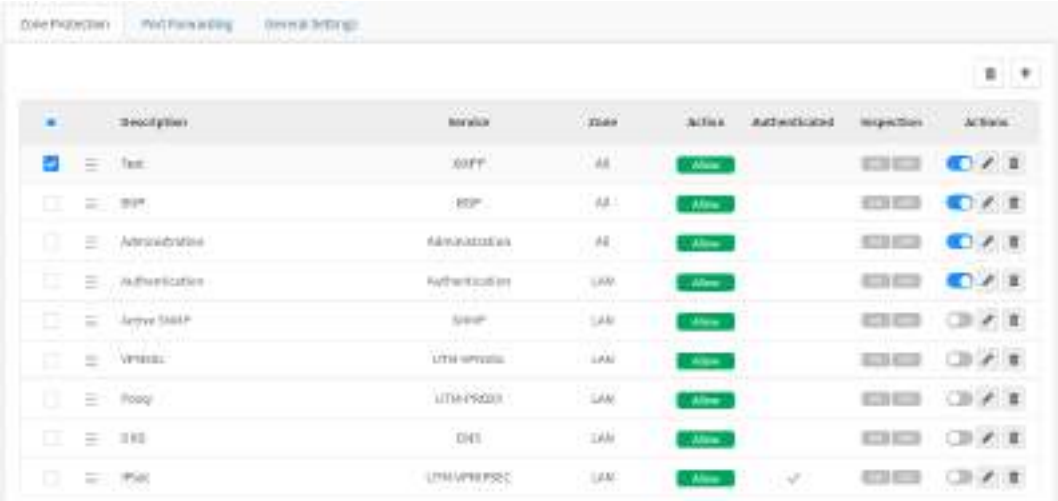
Live Sessions

Deste modo conseguimos habilitar e verificar o funcionamento do serviço Telnet.

Zone Protection - Remove

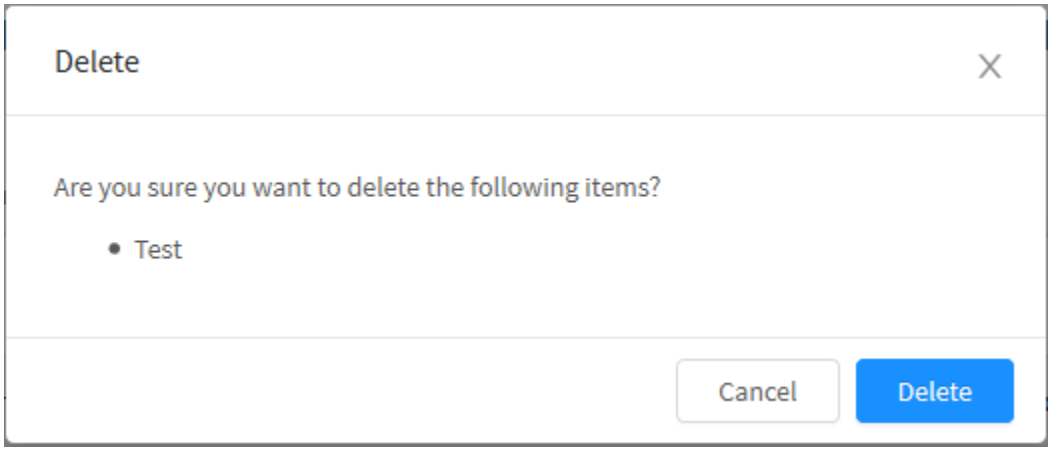
Através deste botão é possível deletar vários itens ao mesmo tempo. Siga o exemplo abaixo:

1. Selecione os itens que deseja deletar clicando no ícone de **seleção[ ]**;



Zone Protection - Seleção para deleção

2. Clique no botão **[ ]**, surgirá uma tela perguntado se deseja deletar o item selecionado:



Zone Protection - Remove itens

Caso deseje cancelar clique no botão **[ ]**. Para concluir a deleção clique no botão **[ ]**.

O item foi deletado com sucesso.

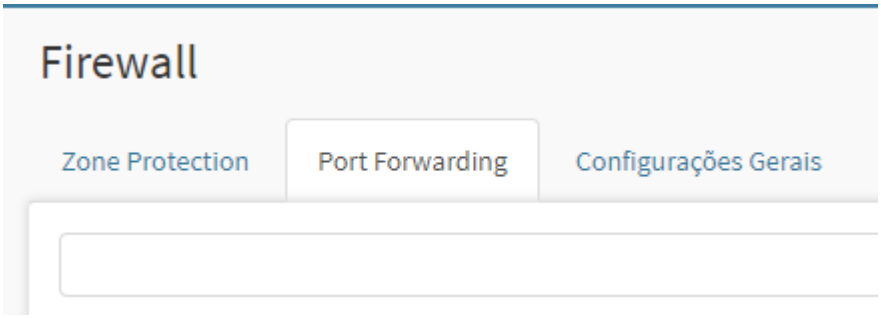
Firewall - Port Forwarding

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.

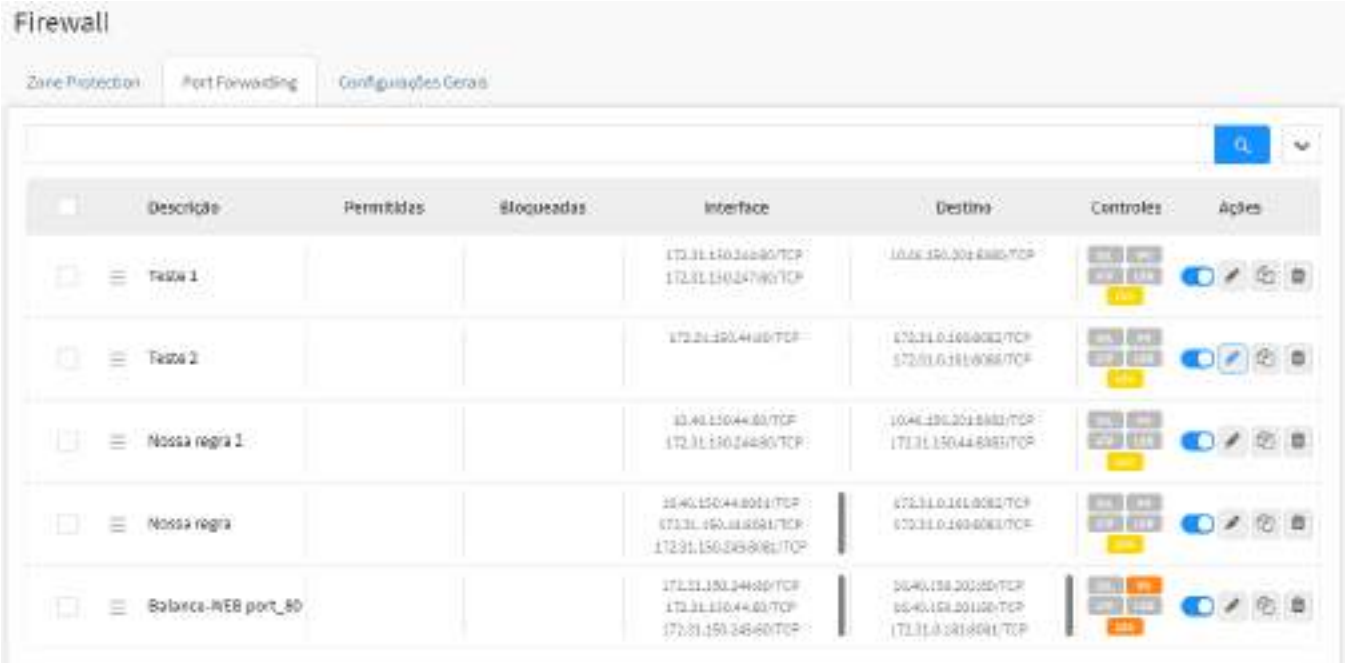
As regras de *Port Forwarding* são carregadas de cima para baixo, assim sendo, as regras que estiverem no topo da tabela possuem prioridade sobre as abaixo (sendo possível até que elas sobreponham as configurações das regras de baixo).

Para abrir a tela, clique na aba “Port Forwarding”.



Aba *Port Forwarding*

Surgirá a tela abaixo:



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 [] permite replicar as políticas individualmente.

Esta sessão irá abordar:

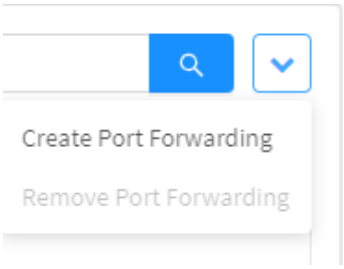
- Cadastro, Edição e Remoção de políticas de redirecionamento;
- Ativação e Desativação destas mesmas;
- Exemplos de políticas de redirecionamento
- Detalhes das colunas desta tela.

A seguir, analisaremos as funções localizadas no topo desta tela.

Port Forwarding - Botão de Adição

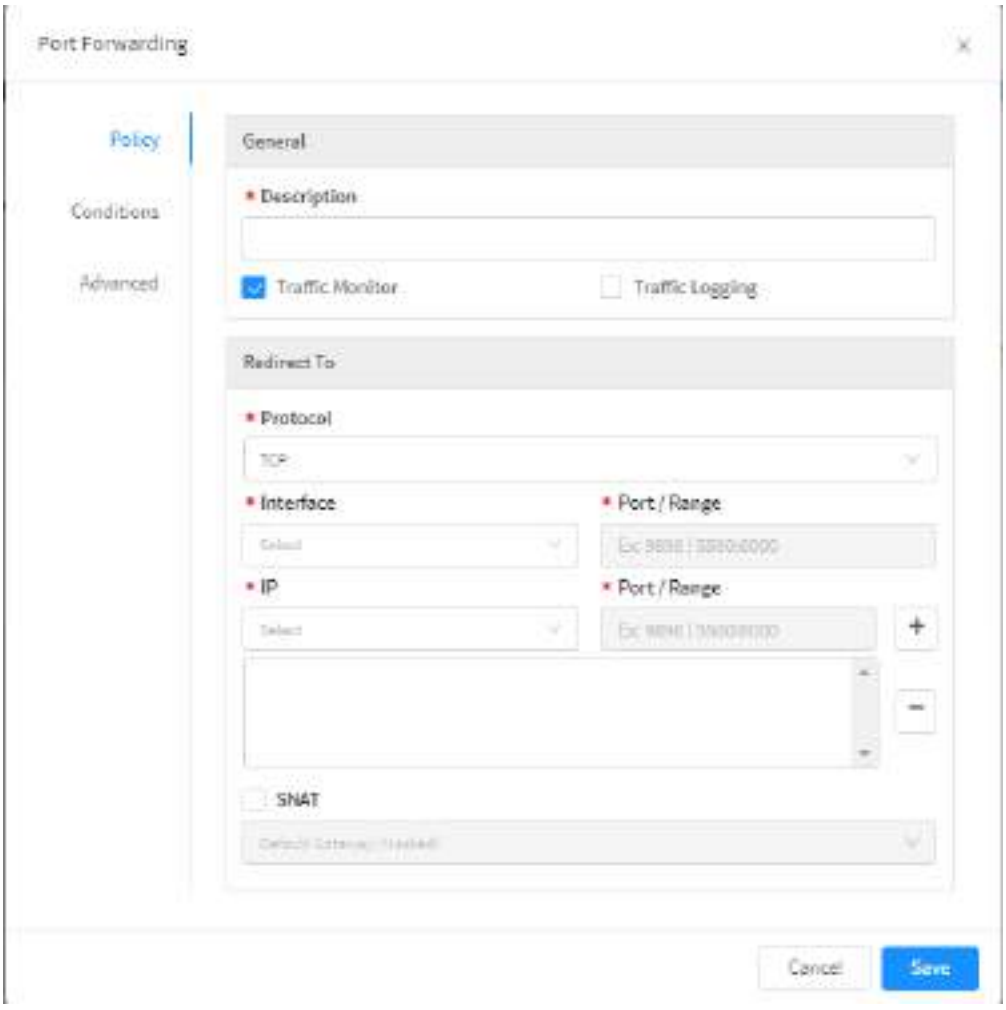
Através desta janela é possível criar um *Port Forwarding* e configurar as permissões de mascaramento e redirecionamento de tráfego entre os barramentos.

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:



Port Forwarding - Criando um novo *Port Forwarding*

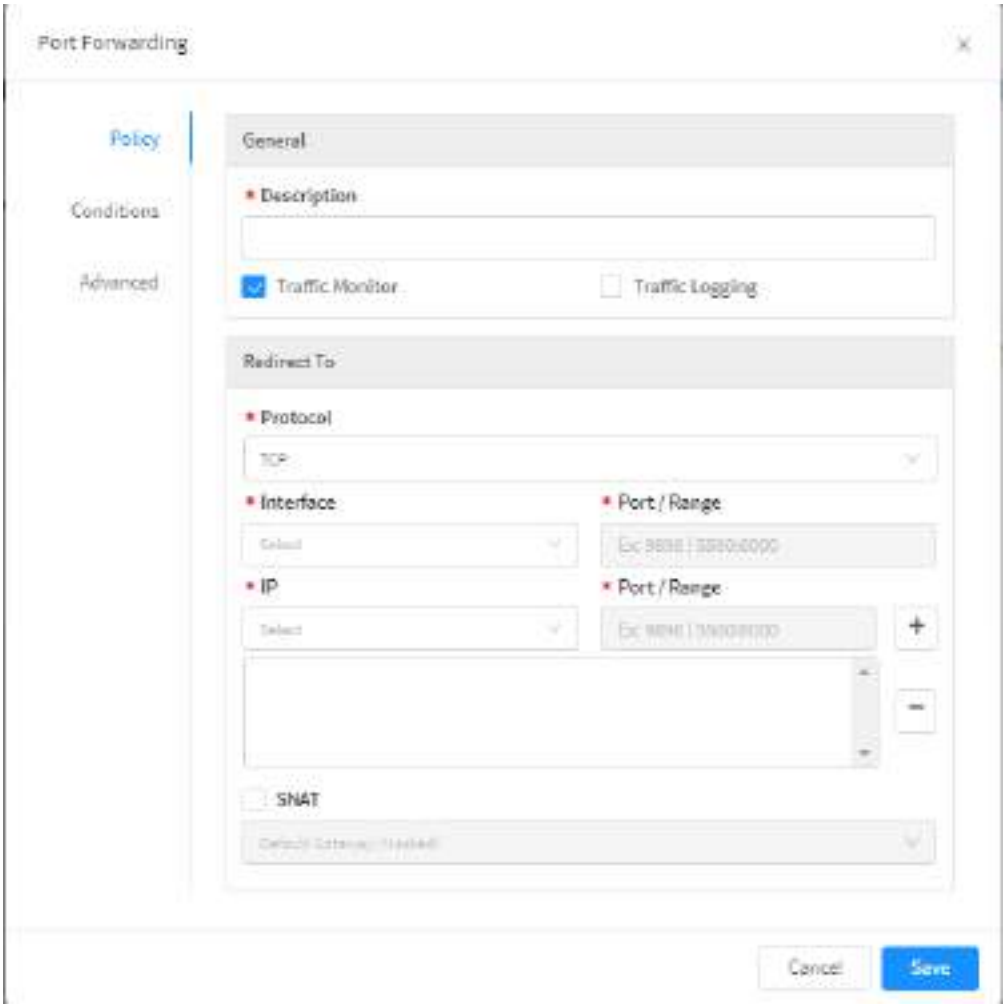
O menu é composto por várias sessões e painéis:

- *Policy*;
  - *General*;
  - *Redirect to*.
- *Conditions*;
  - *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:



Port Forwarding - Policy

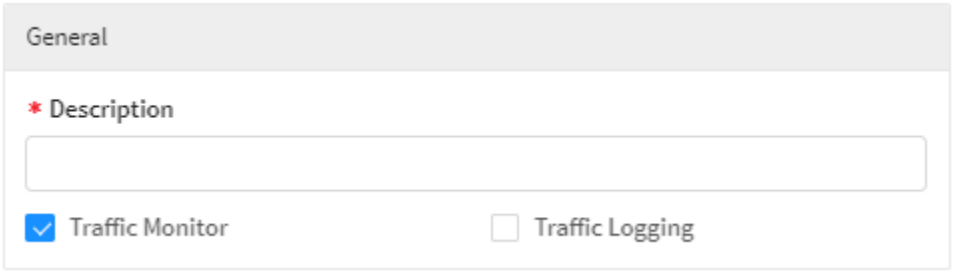
Esta aba é composta pelos painéis:

- *General;*
- *Redirect to.*

Iniciaremos detalhando o painel *General*.

General

Este painel contém apenas o campo para adicionar a descrição da política.



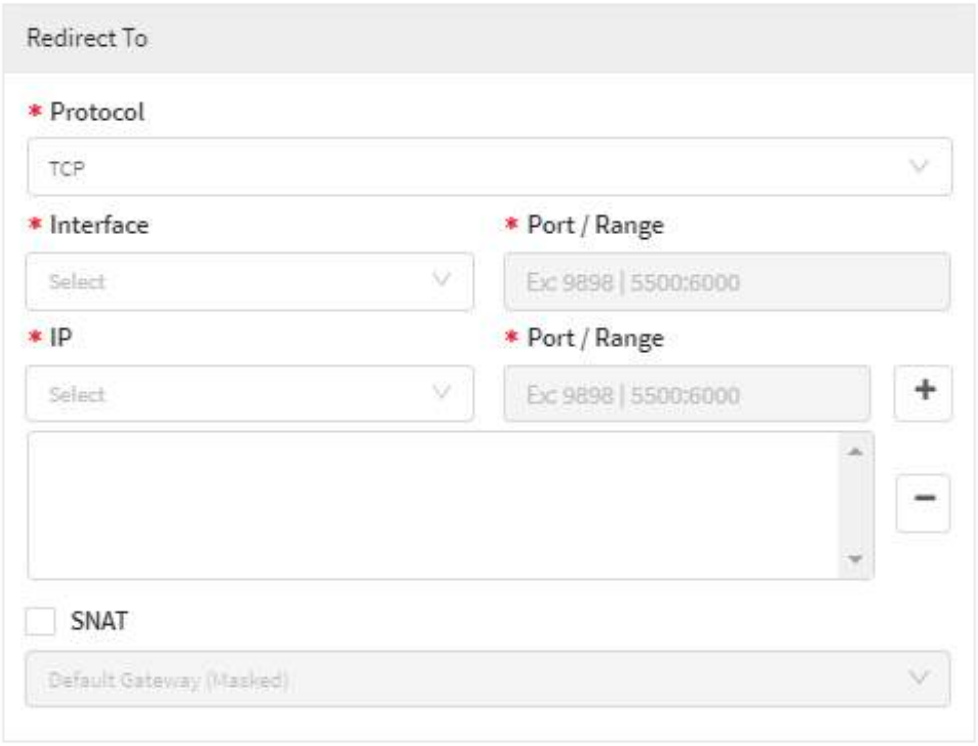
Policy - General

- **Description:** Define uma descrição para identificação;
- **Traffic Monitor:** Com a caixa de *Traffic Monitor* checada [ ], serão coletados dados sobre o tráfego de informações das sessões associadas ao *Port Forwarding;*
- **Traffic Logging:** Com a caixa de *Traffic Logging* checada [ ], serão gerados logs referentes ao tráfego de informações das sessões associadas ao *Port Forwarding*.

À seguir detalharemos o painel *Redirect to*.

Redirect To

Este painel contém os recursos para configuração do redirecionamento da política de *Port Forwarding*



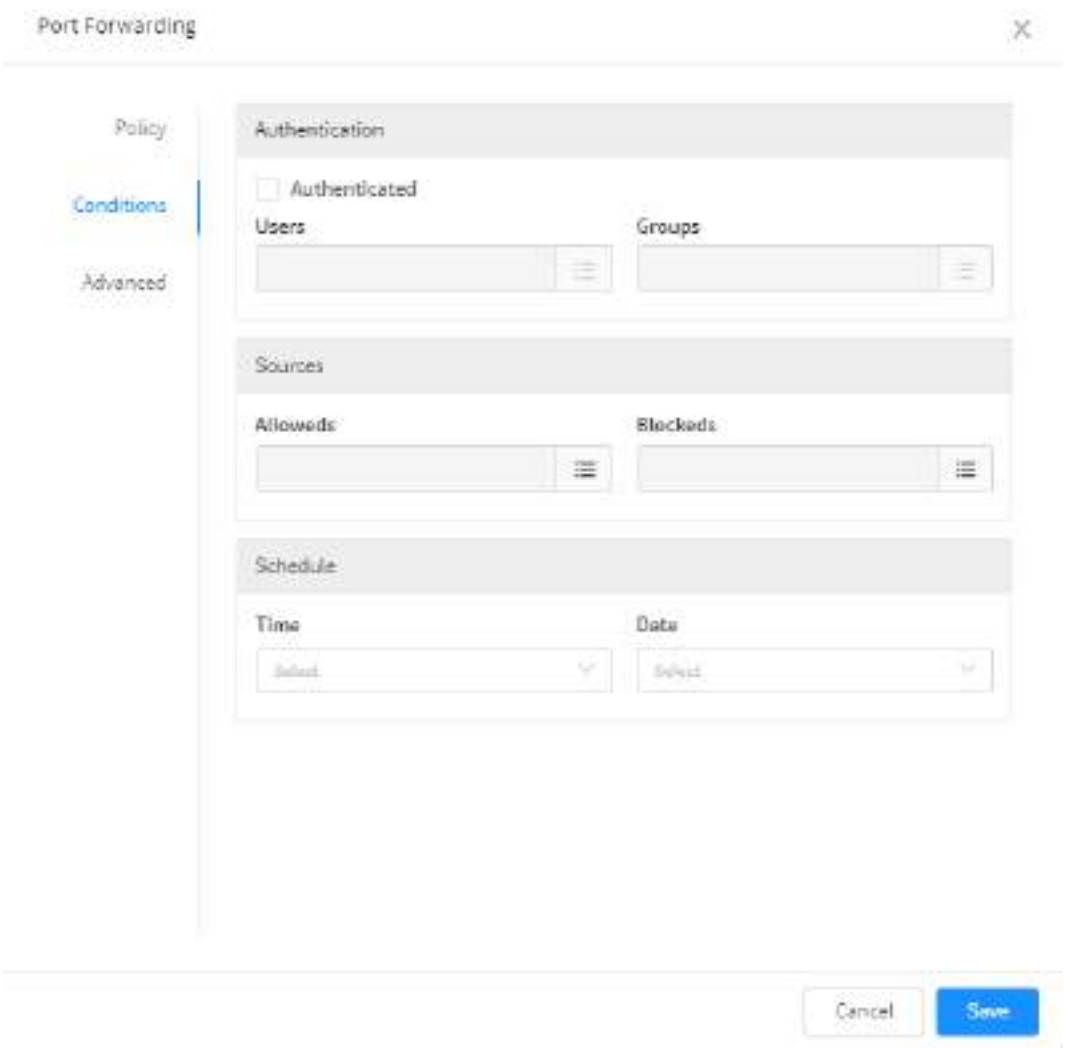
Policy - Redirect to

- **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 página.
- **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

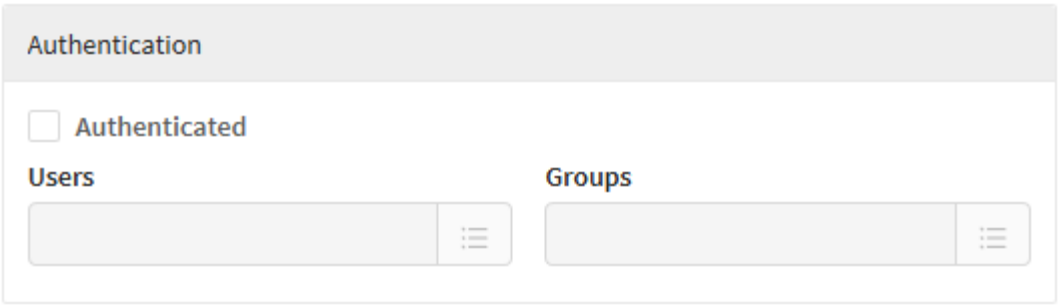
Esta aba é composta pelos painéis:

- *Authentication;*
- *Sources;*
- *Schedule*.

Iniciaremos detalhando o painel *Authentication*.

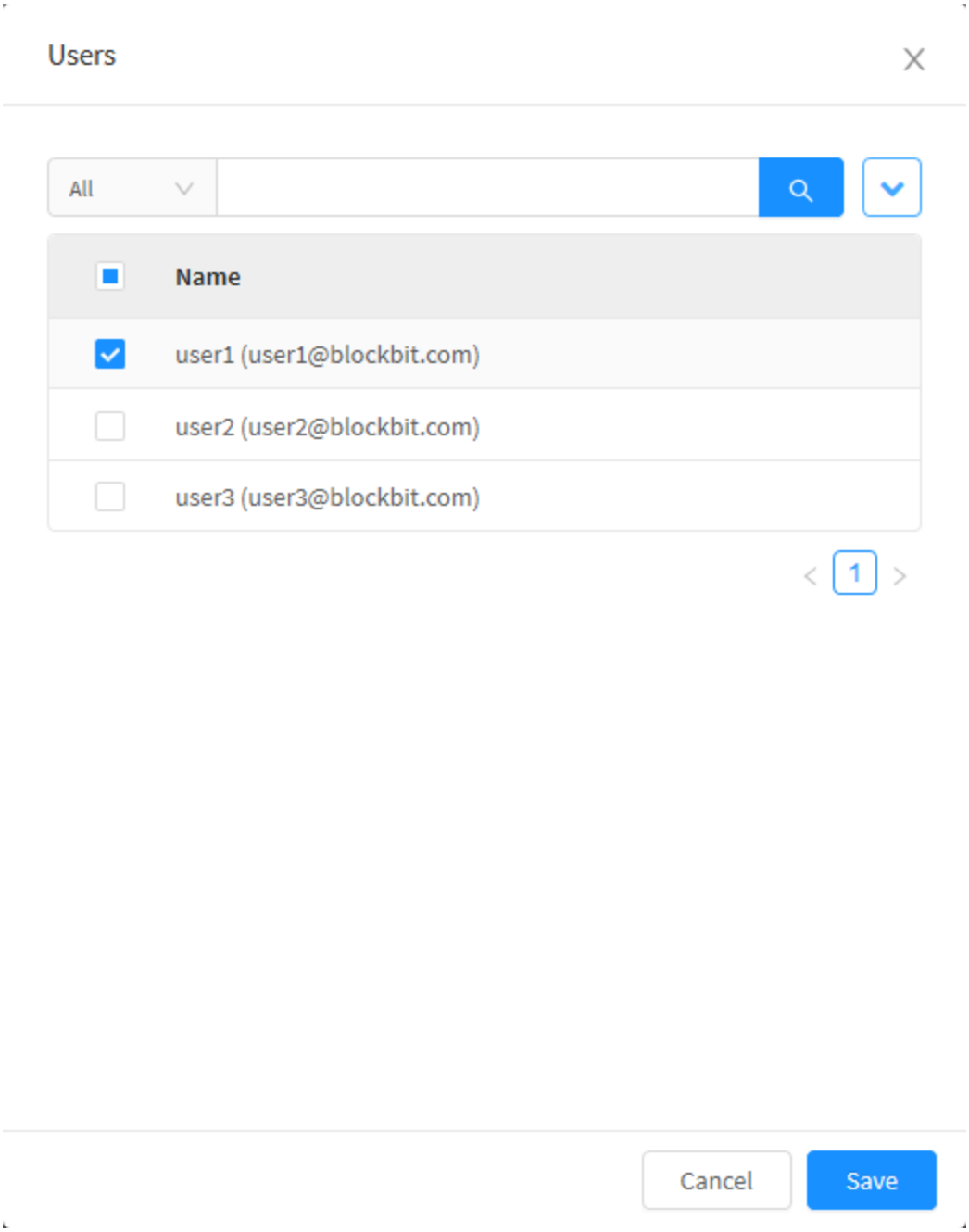
Authentication

Neste painel estão localizadas os recursos que permitem condicionar a ativação do *Port Forward* por autenticação.



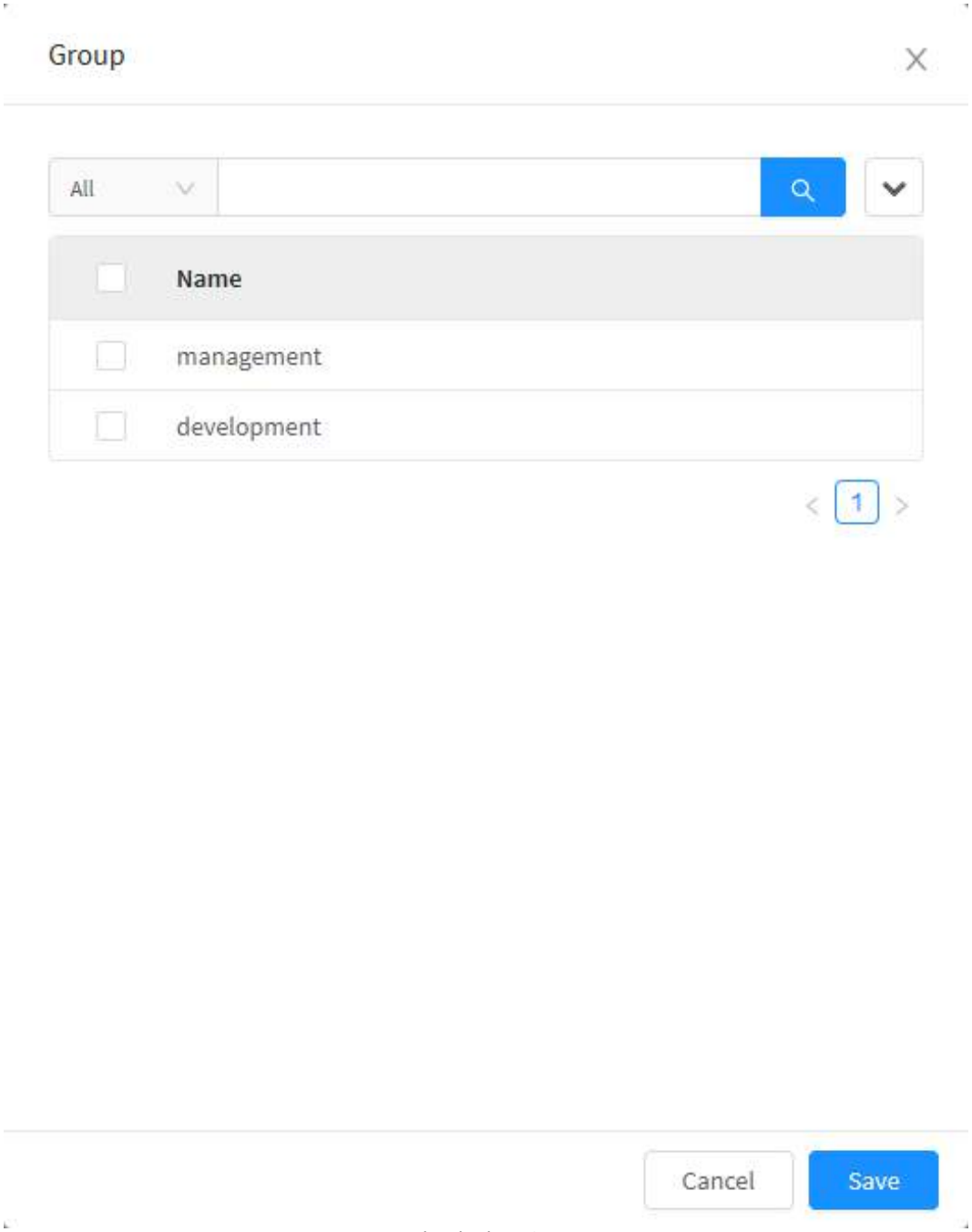
Conditions - Authentication

- ***Authenticated[ ]:*** 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 caixa de checagem **authenticated** marcada, clique em **[ ]** para determinar à quais usuários o *port forwarding* será aplicado, conforme demonstrado pela imagem abaixo. Ao finalizar a seleção, clique em **[Save]** caso contrário, clique em **[Cancel]** para cancelar;



Authentication - Users

- ***Groups*:** Com a caixa de checagem **authenticated** marcada, clique em **[** **]** para determinar à quais grupos de usuários o *port forwarding* será aplicado, conforme demonstrado pela imagem abaixo. Ao finalizar a seleção, clique em **[** Save **]** caso contrário, clique em **[** Cancel **]** para cancelar;

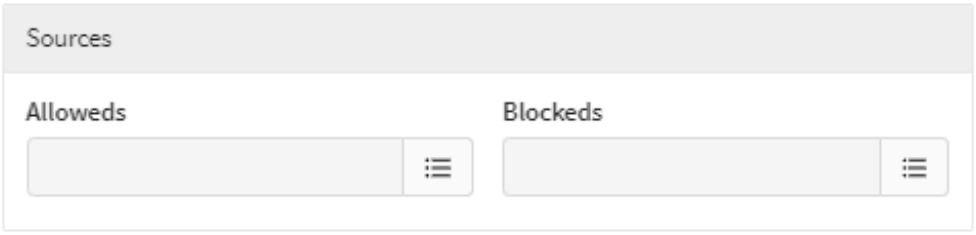


Authentication - Group

À seguir, detalharemos o painel *Sources*.

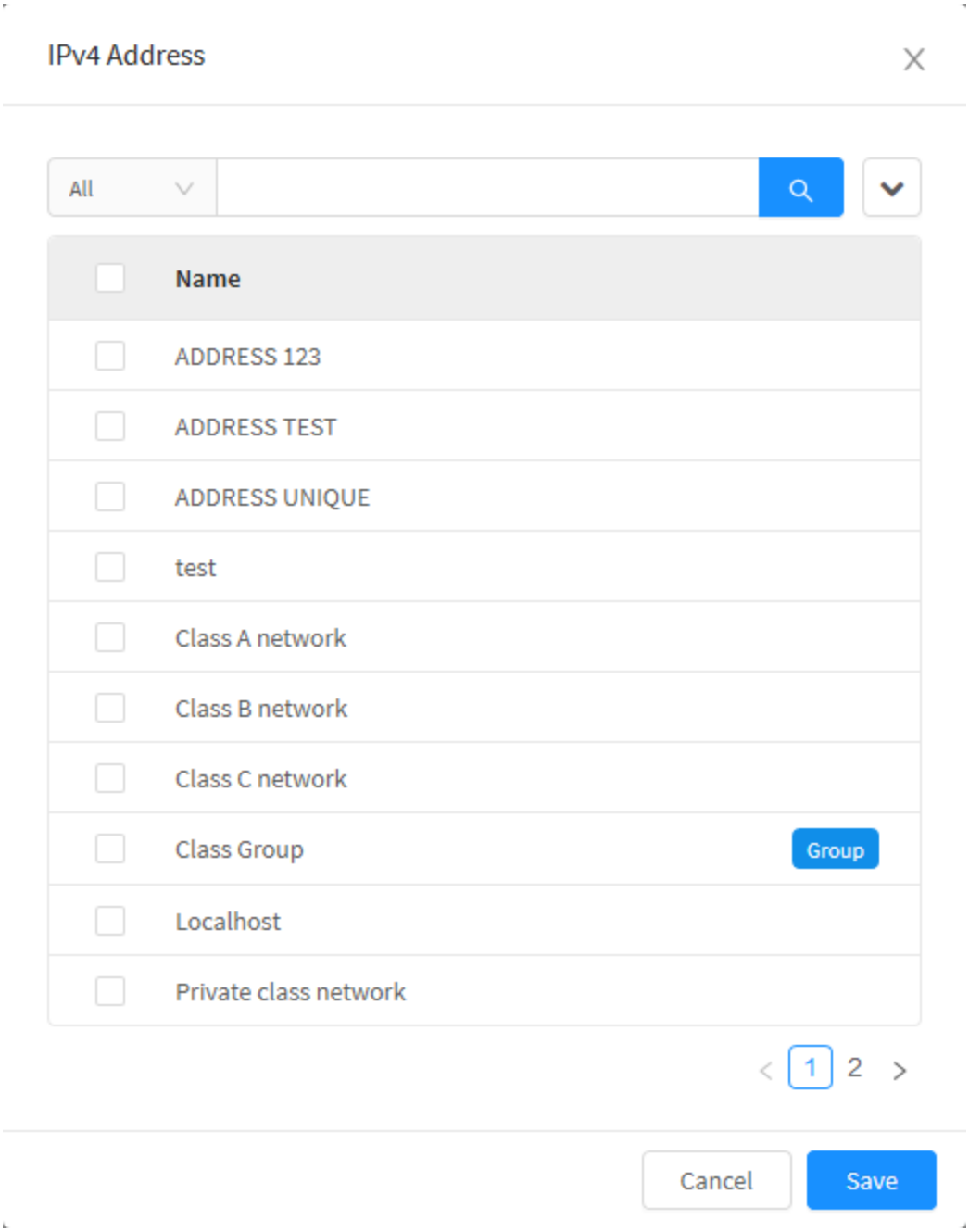
Sources

Neste painel estão localizadas os recursos que permitem condicionar a ativação do *Port Forward* de acordo com a origem do tráfego.



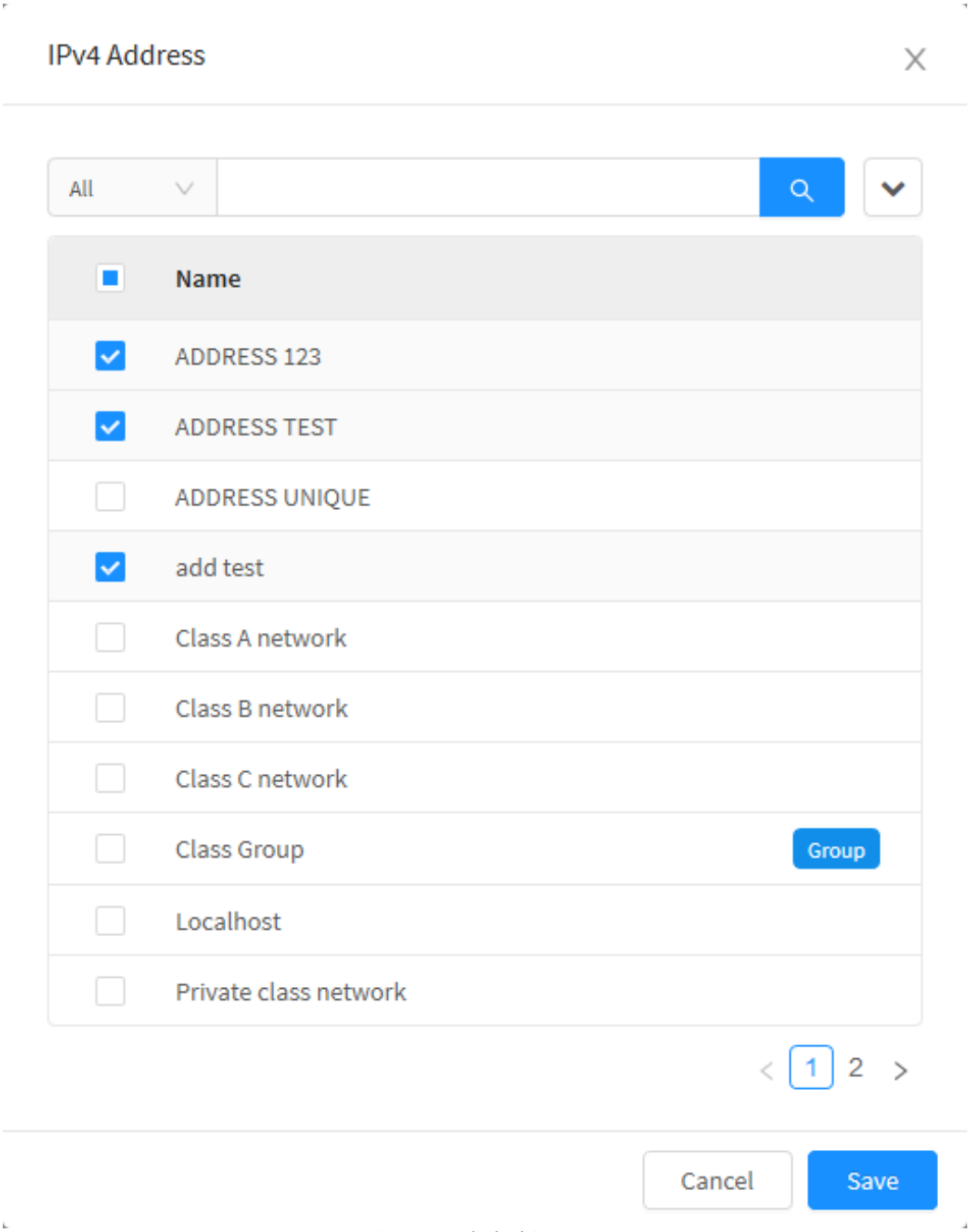
Conditions - Sources

- ***Alloweds:*** 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 **[Save]** caso contrário, clique em **[Cancel]** para cancelar;



Sources - Allowed Sources

- ***Blockeds:*** 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 **[** **]** caso contrário, clique em **[** **]** para cancelar;

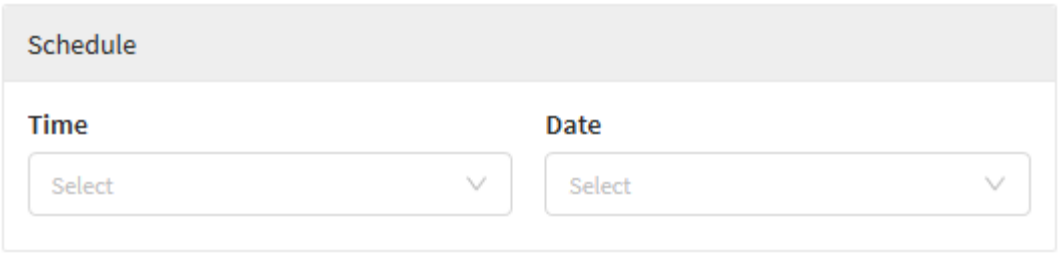


Sources - Blocked Sources

À seguir, detalharemos o painel *Schedule*.

Schedule

Neste painel estão localizadas os recursos que permitem controlar a ativação do *Port Forward* em um período específico.



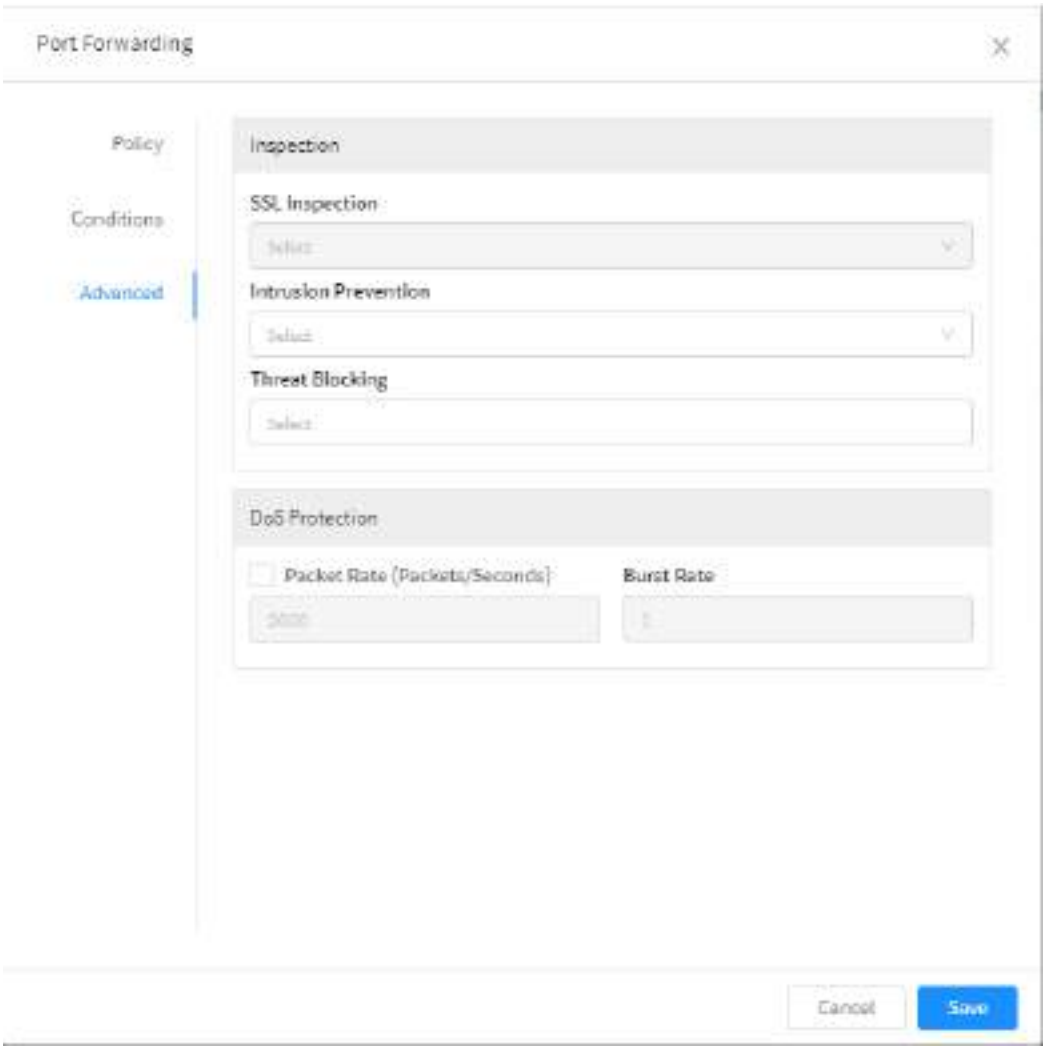
Condition - Schedule

- ***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

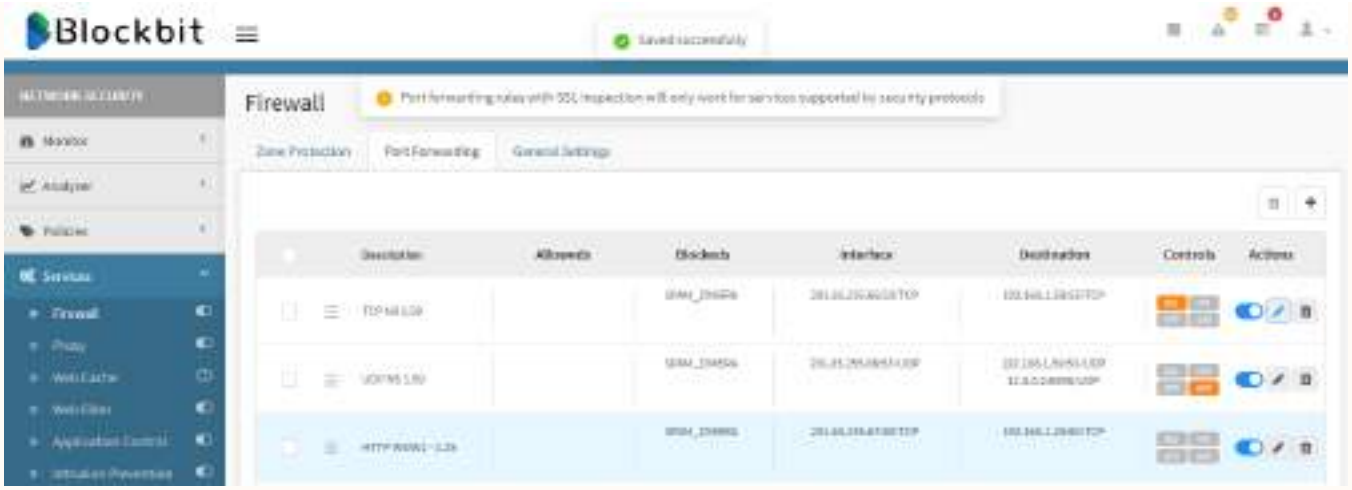
Em "*Advanced*" configuramos quais inspeções serão aplicadas no *port forwarding*:



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:

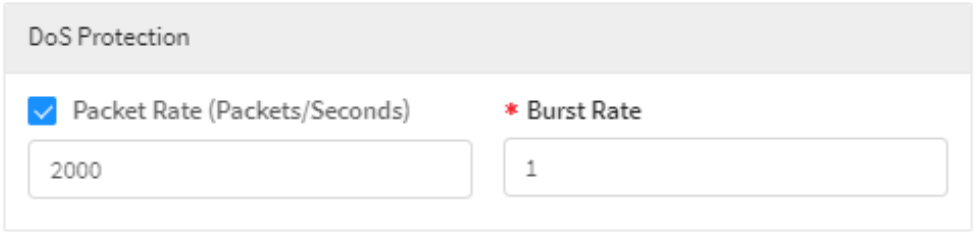


Alerta - Regras de redirecionamento com Inspeção *SSL* só funcionarão para serviços em que o protocolo de segurança é suportado

- ***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 **[** **]** ou selecione ela novamente no menu. Para limpar esse campo, basta clicar em **[** **]**. Possui as opções abaixo:
  - *Abuse*;
  - *Anonymizers*;
  - *Attacks*;
  - *Malware*;
  - *Reputation*;
  - *Spam*.

DoS Protection

Neste painel estão disponíveis os controles de DoS Protection:



Port Forwarding - Configurações de DoS Protection

- ***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 *Packet Rate*, permitindo assim flexibilizar o controle de tráfego para picos de tráfego ocasionais.

Para salvar as alterações clique em **[** **]**, caso contrário, clique em **[** **]** ou em **[** **]** para cancelar todas as configurações e voltar 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 comandos acesse a página: UTM - Fila de comandos.

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.

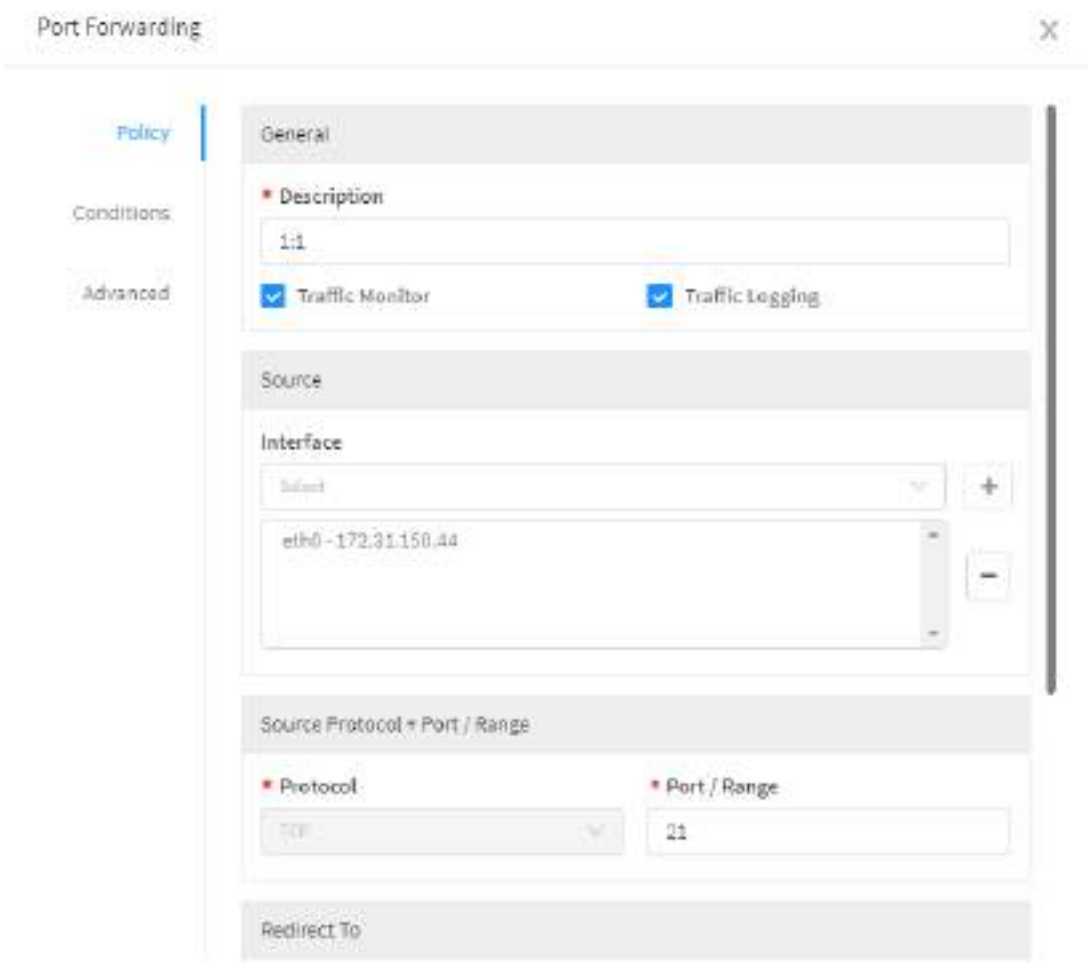
Este recurso configura as políticas de "Encaminhamento" com tráfego permitido, baseadas nos endereços de IP Origem/Destino e Portas definidas na respectiva política de DNAT.

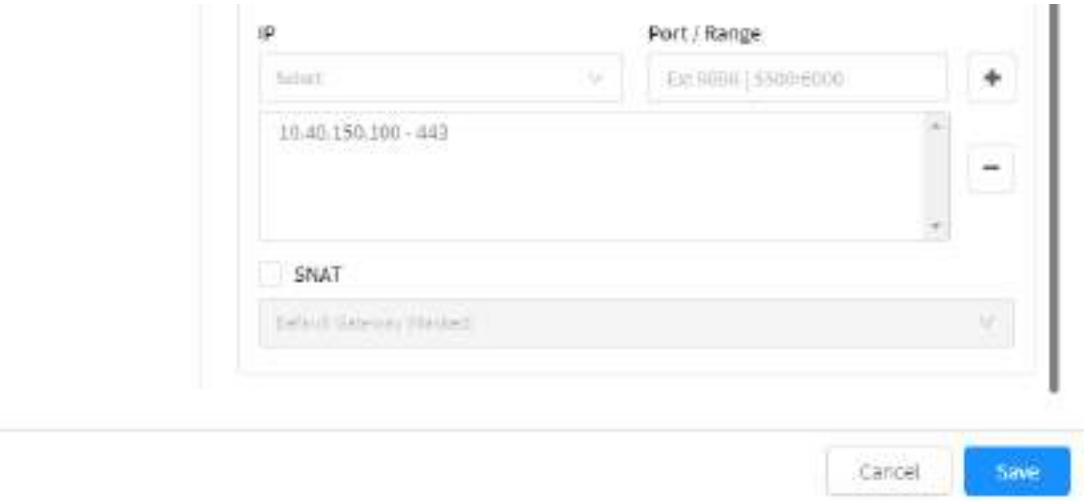
Alguns detalhes não serão considerados neste exemplo, caso deseje mais informações, consulte esta página.

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;





Port Forwarding - Policy 1

Depois clique em [Save].

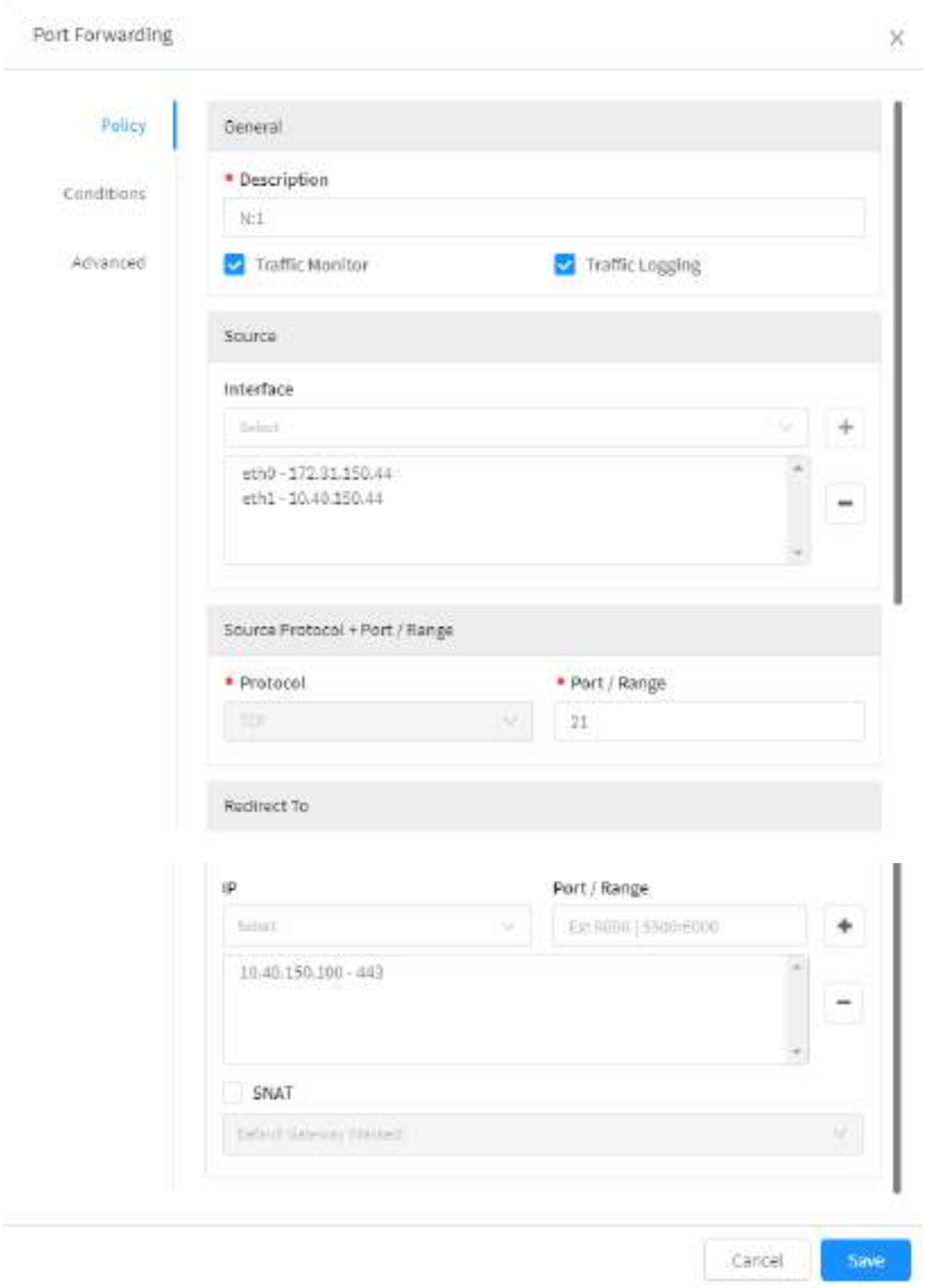
Após salvar, para que o encaminhamento entre em ação será necessário acessar a **fila de comandos [** **1** **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Após realizar esses procedimentos a política terá sido configurada com sucesso.

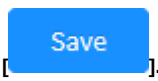
Exemplo II - Port Forwarding N:1

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;



Port Forwarding - Policy 2

Depois clique em **[**  **].**

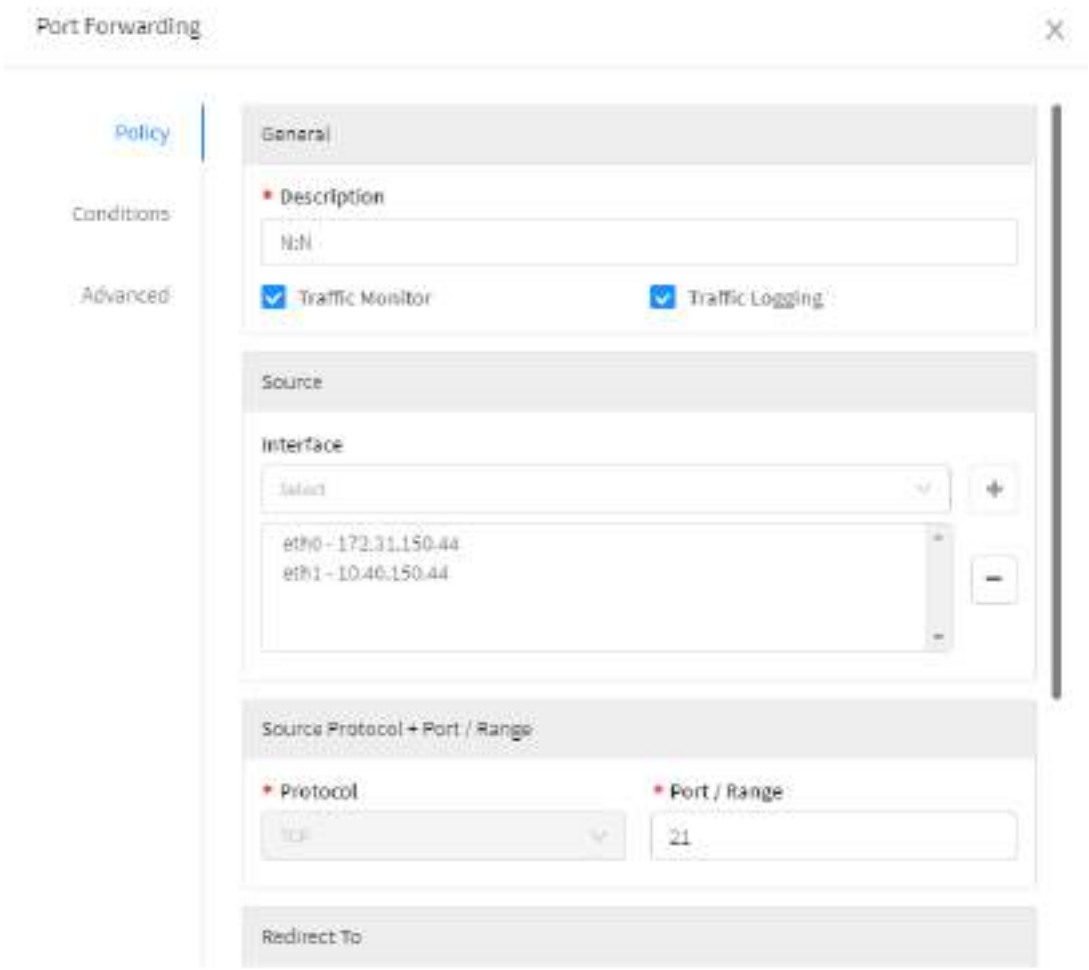
Após salvar, para que o encaminhamento entre em ação será necessário acessar a **fila de comandos [**  **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

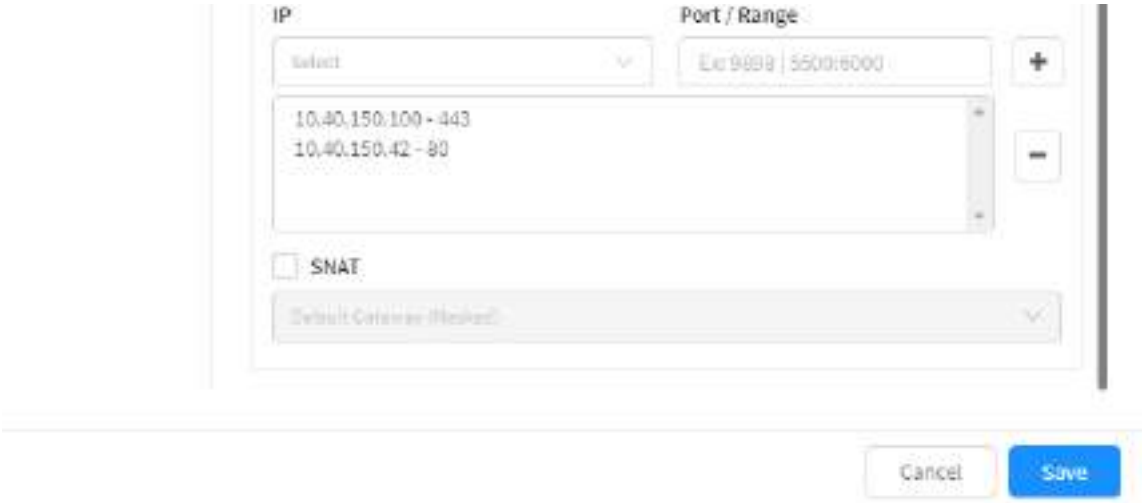
Após realizar esses procedimentos a política terá sido configurada com sucesso e, assim, será possível redirecionar o tráfego da porta X, em diferentes entradas/interfaces do Blockbit, para UM host da rede interna.

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;





Port Forwarding - Policy 3

Depois clique em **[** Save **].**

> Quando configurado 2 ou mais destinos a regra criada obedecerá o padrão "first match wins", ou seja, o primeiro IP configurado como destino será o principal, e caso esteja indisponível o redirecionamento será feito pelos outros IPs configurados.

Após salvar, para que o encaminhamento entre em ação será necessário acessar a **fila de comandos [** 1 **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

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 N hosts da rede interna.

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.

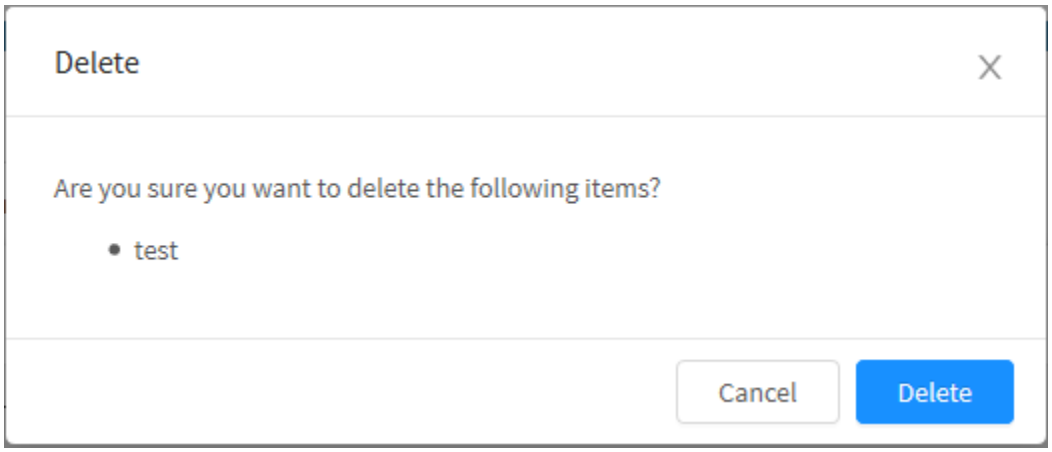
Port Forwarding - Botão de Remoção

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[ ]**;

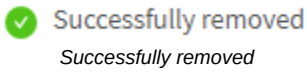
Port Forwarding - Seleção para deleção

2. Clique no botão de **remoção[ ]** e uma tela perguntado se deseja deletar o item selecionado:



Port Forwarding - Remove itens

Caso deseje cancelar clique no botão **[** Cancel **]**. Para concluir a deleção clique no botão **[** Delete **]**.



Successfully removed

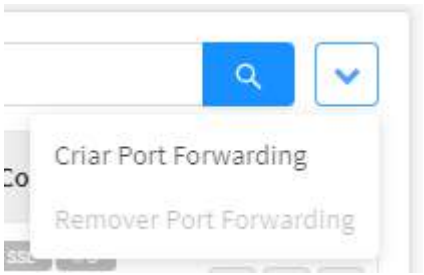
O item foi deletado com sucesso.

À seguir detalharemos o conteúdo das colunas.

Port Forwarding - Criar Port Forwarding

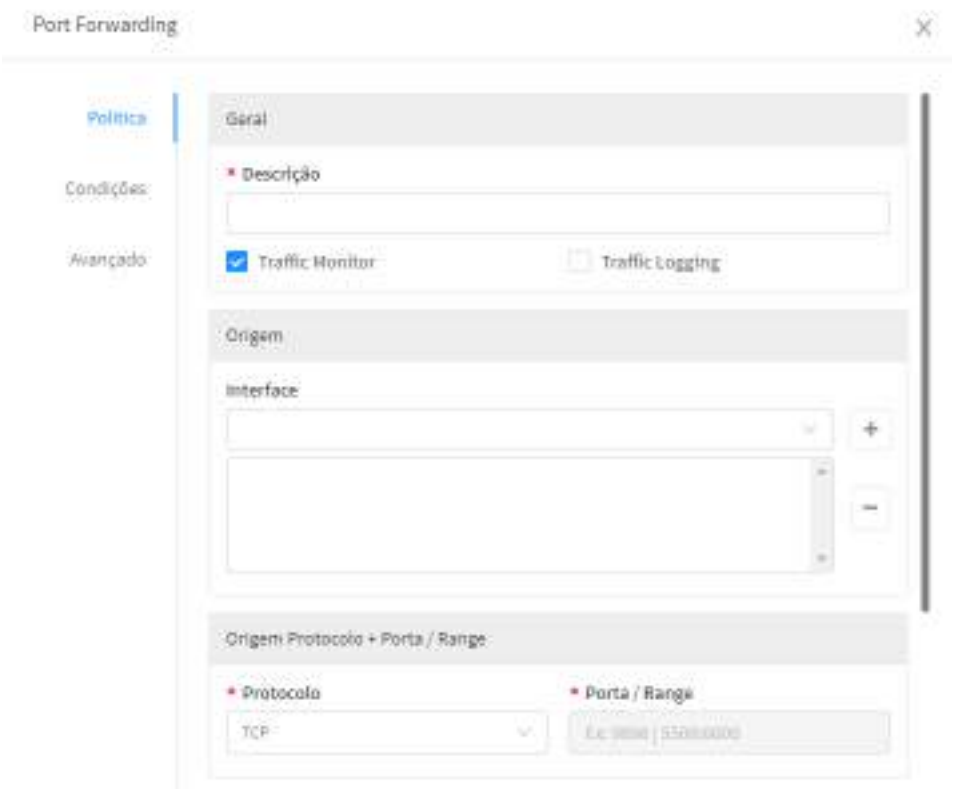
Através desta janela é possível criar um *Port Forwarding* e configurar as permissões de mascaramento e redirecionamento de tráfego entre os barramentos.

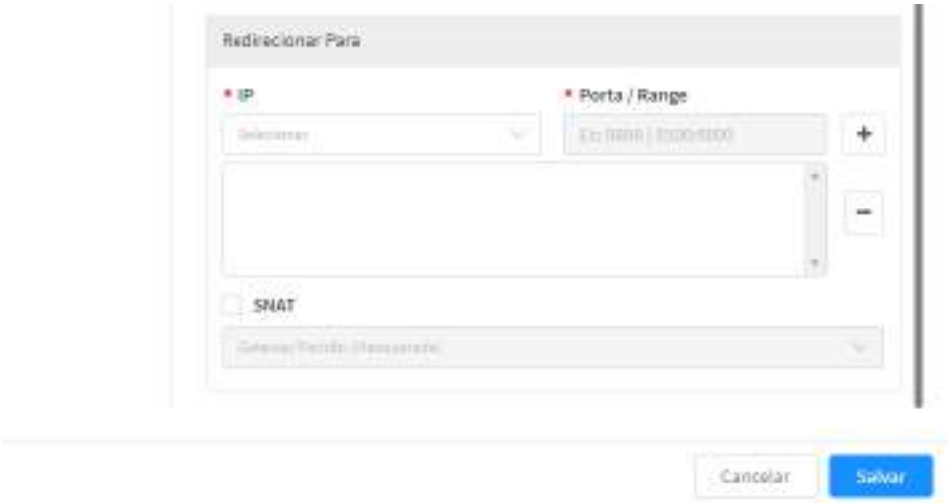
Para criar um Port Forwarding, clique no botão localizado no topo superior direito:



Port Forwarding – Botão de Criação

Ao clicar neste botão a janela abaixo é exibida:





Port Forwarding - Criando um novo *Port Forwarding*

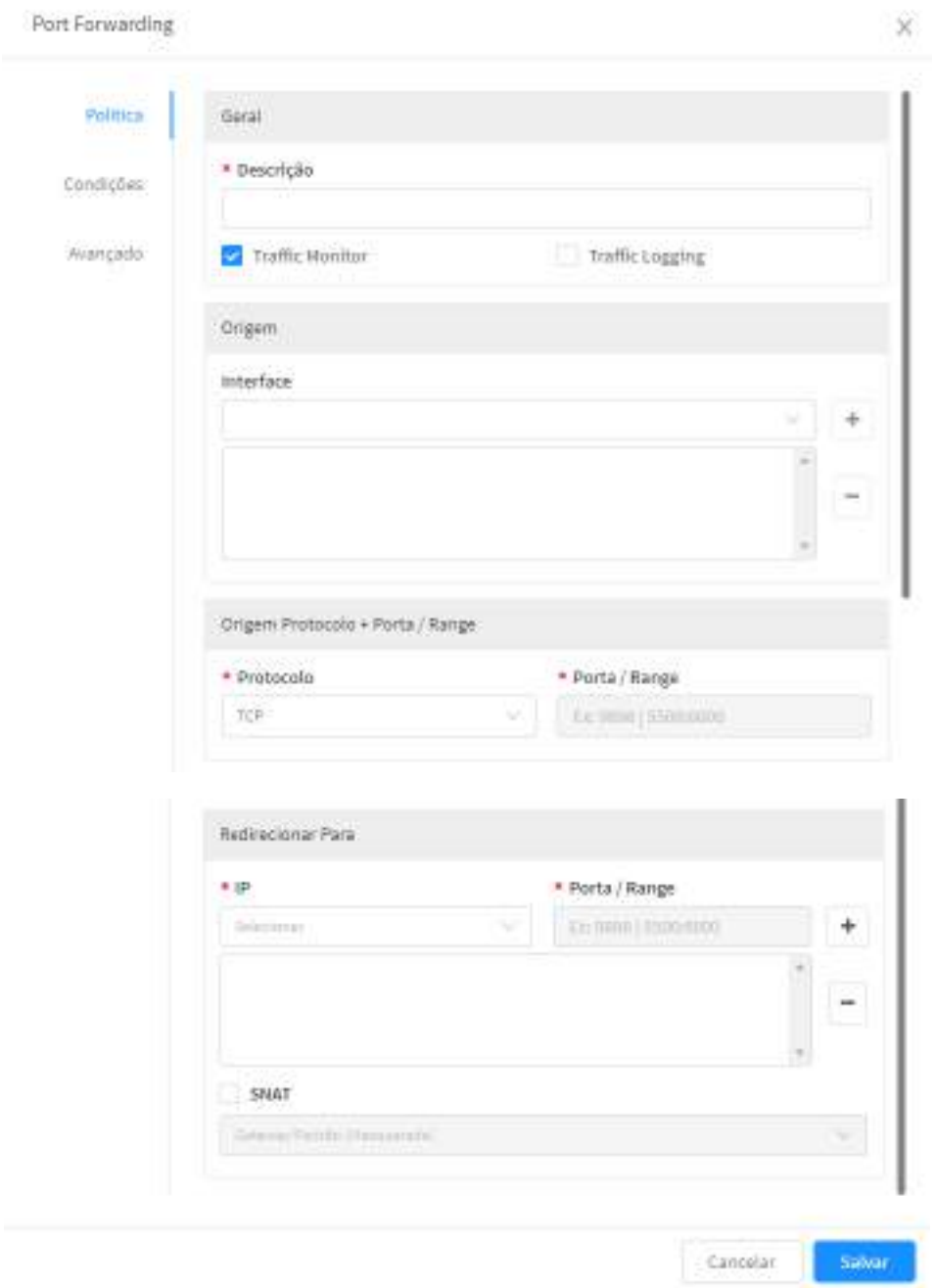
O menu é composto por várias sessões e painéis:

- *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:



Port Forwarding - Política

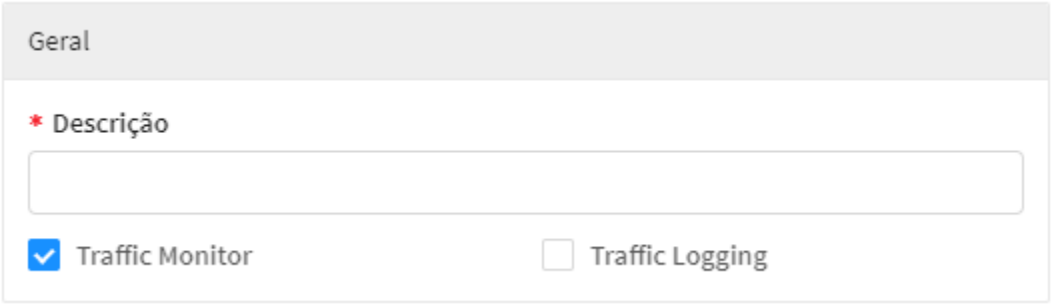
Esta aba é composta pelos painéis:

- *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.



Política - Geral

- **Descrição:** Define uma descrição para identificação;
- **Traffic Monitor:** Com a caixa de *Traffic Monitor* checada [ ], serão coletados dados sobre o tráfego de informações das sessões associadas ao *Port Forwarding;*
- **Traffic Logging:** Com a caixa de *Traffic Logging* checada [ ], serão gerados logs referentes ao tráfego de informações das sessões associadas ao *Port Forwarding*.

À seguir detalharemos o painel "*Origem"*

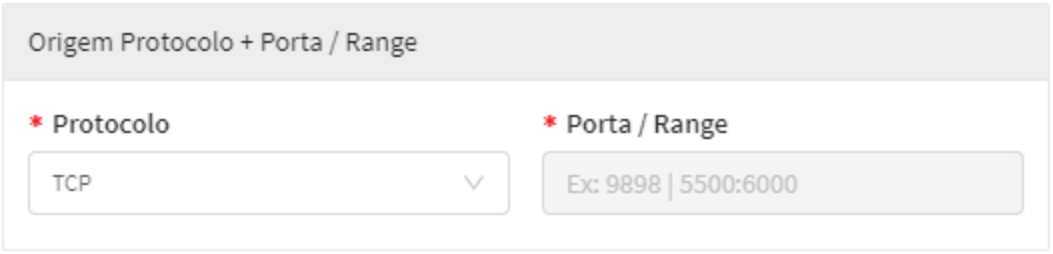
Origem

Política - Origem

- ***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



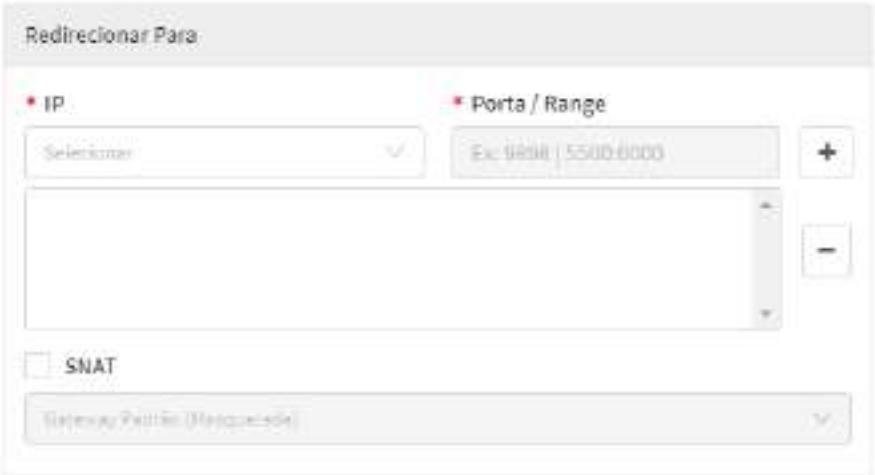
Política - Origem Protocolo + Porta/Range

- **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*



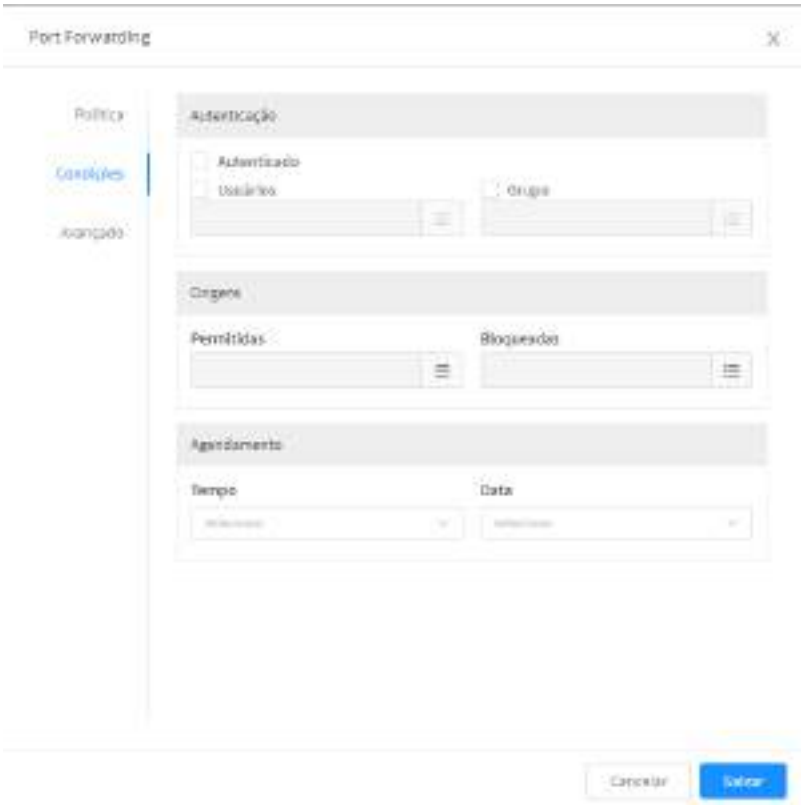
Política - Redirecionar Para

- ***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 página.
- **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:



Port Forwarding - Conditions

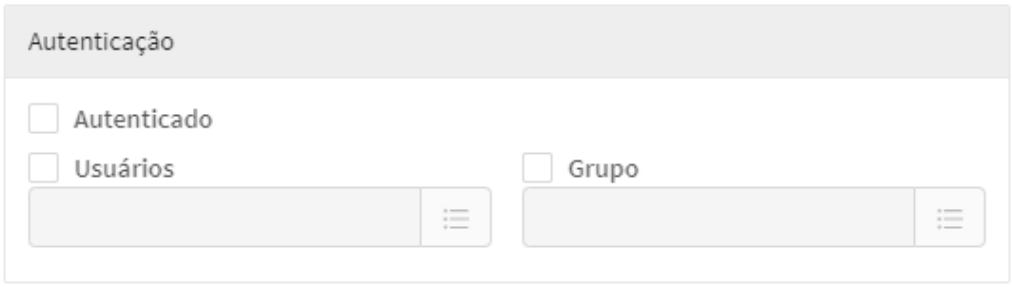
Esta aba é composta pelos painéis:

- *Autenticação*
- *Origens*
- *Agendamento*

Iniciaremos detalhando o painel *Authentication*.

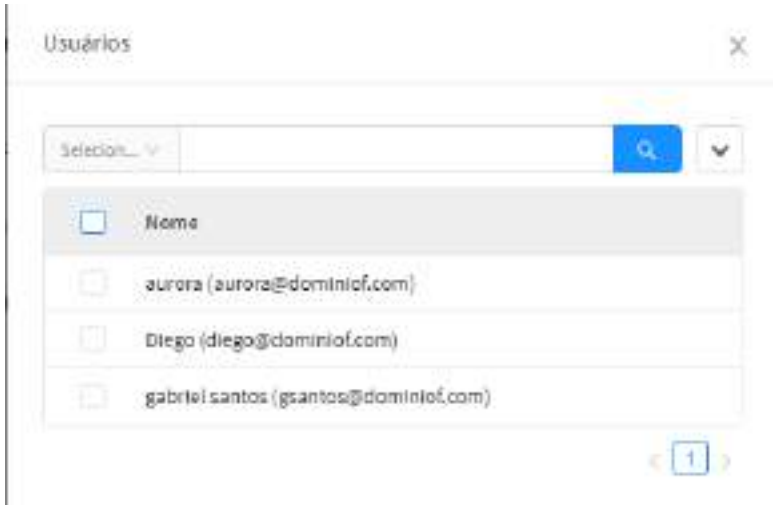
Autenticação

Neste painel estão localizadas os recursos que permitem condicionar a ativação do *Port Forward* por autenticação.

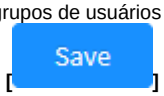
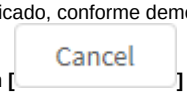


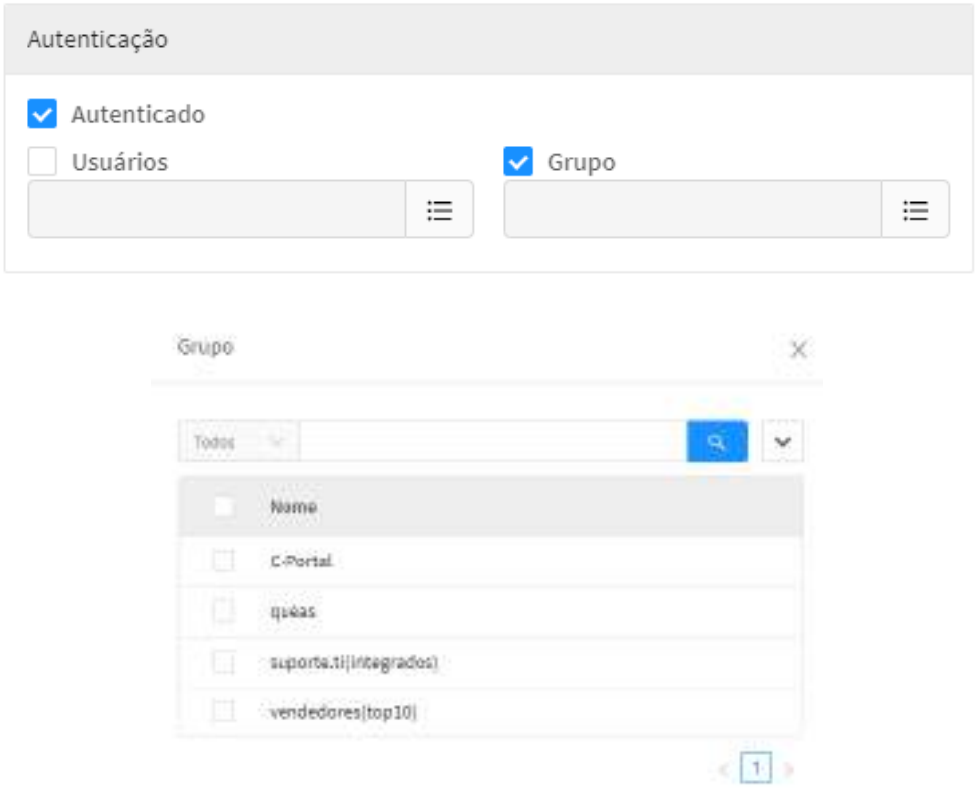
Condições - Autenticação

- ***Autenticado[ ]:*** 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:
    - ***Usuários*:** Com a caixa de checagem **autenticado**marcada, clique em **[ ]** para determinar à quais usuários o *port forwarding* será aplicado, conforme demonstrado pela imagem abaixo. Ao finalizar a seleção, clique em **[** Save **]** caso contrário, clique em **[** Cancel **]** para cancelar;



Autenticação - Usuários

- ***Grupo*:** Com a caixa de checagem **autenticado** marcada, clique em **[**  **]** para determinar à quais grupos de usuários o *port forwarding* será aplicado, conforme demonstrado pela imagem abaixo. Ao finalizar a seleção, clique em **[**  **]** caso contrário, clique em **[**  **]** para cancelar;



Autenticação - Grupo

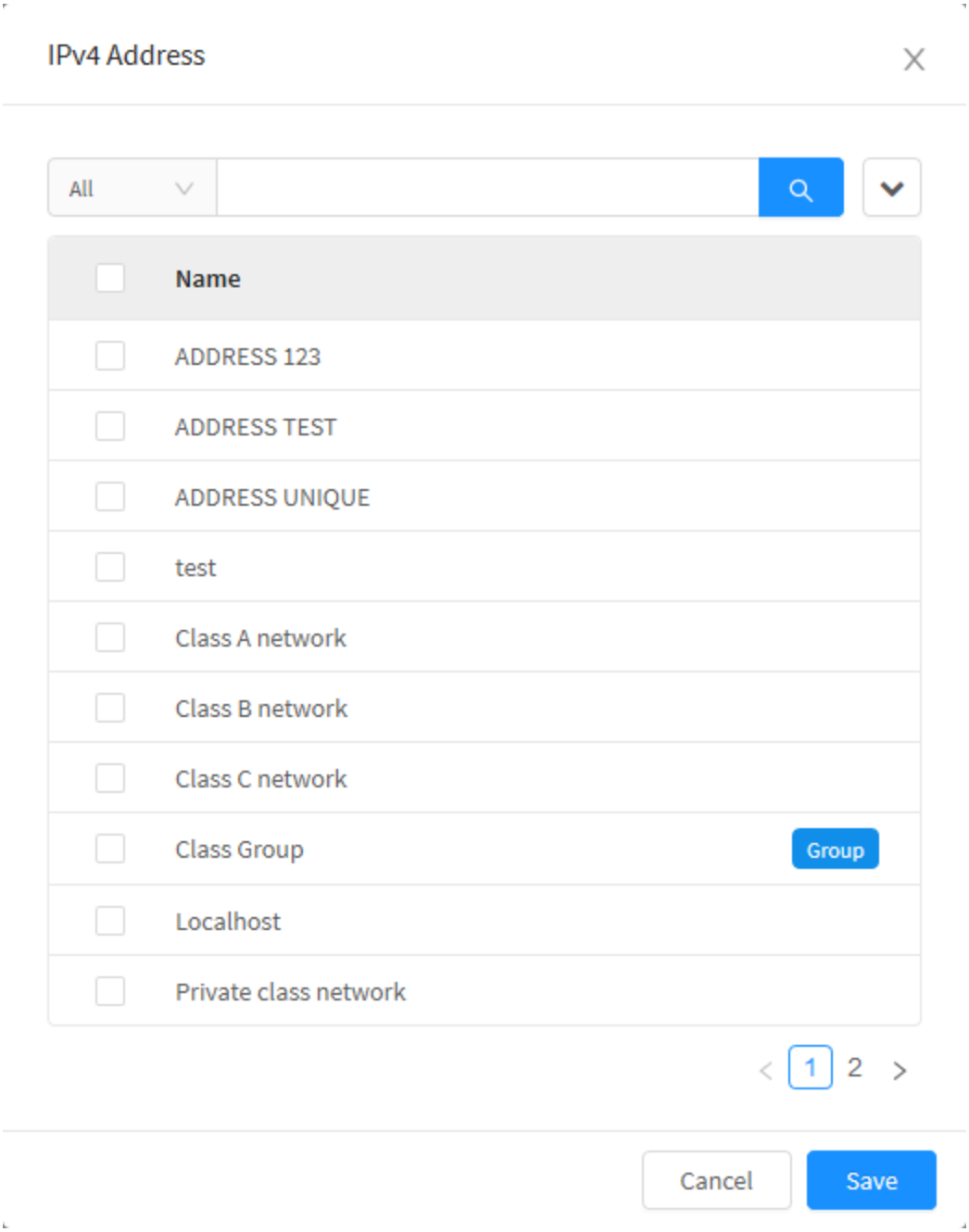
À seguir, detalharemos o painel *Origens*.

Origens

Neste painel estão localizadas os recursos que permitem condicionar a ativação do *Port Forward* de acordo com a origem do tráfego.

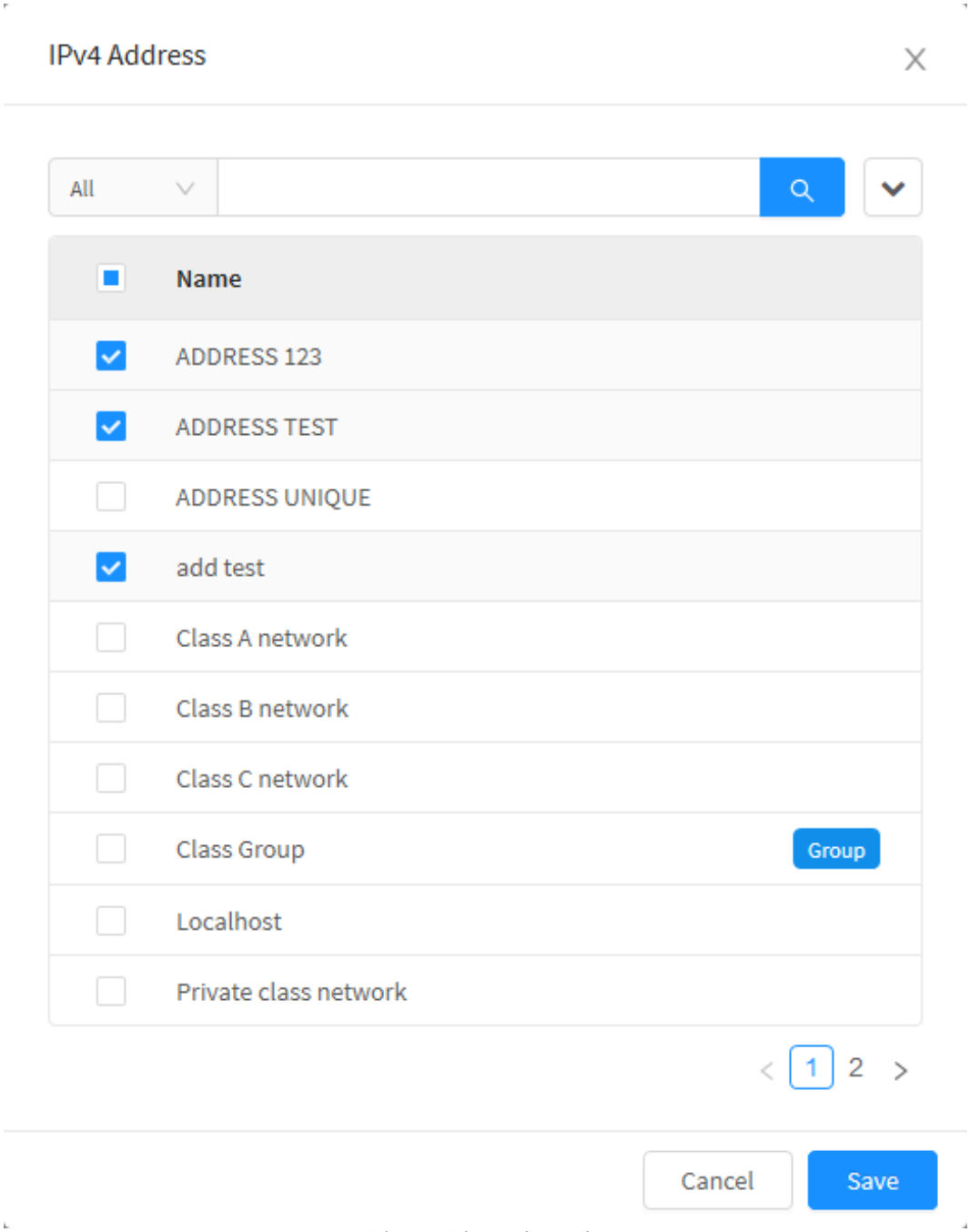
Condições - Origens

- ***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 **[ ]** caso contrário, clique em **[ ]** para cancelar;



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 **[ ]** caso contrário, clique em **[ ]** para cancelar;



Origens - Origens Bloqueadas

À seguir, detalharemos o painel *Schedule*.

Agendamento

Neste painel estão localizadas os recursos que permitem controlar a ativação do *Port Forward* em um período específico.

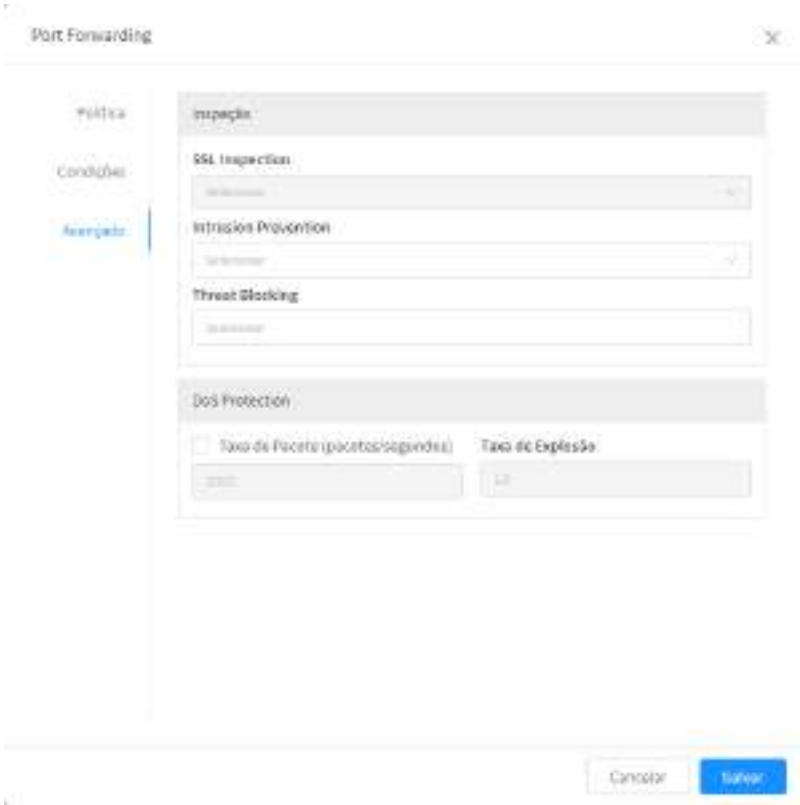
Condições - Agendamento

- ***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*:



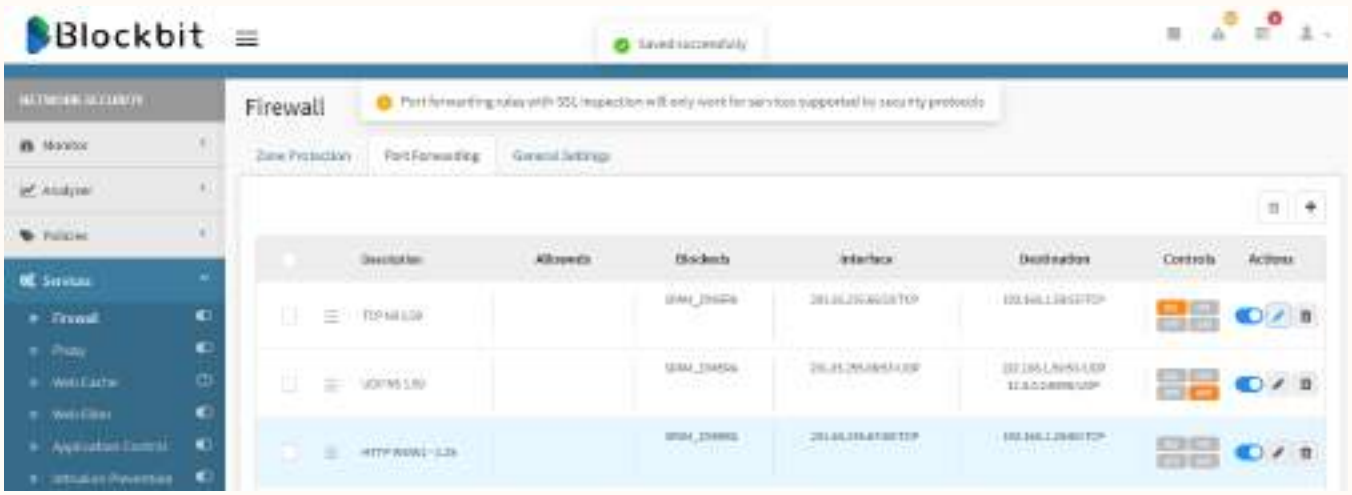
Port Forwarding - Avançado

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;

Avançado - Inspeção SSL

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:

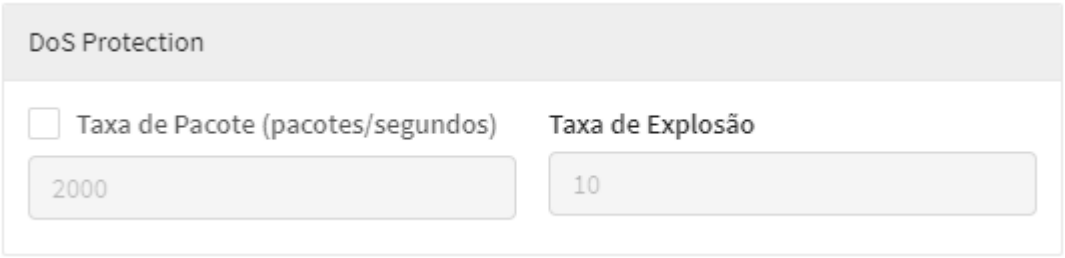


Alerta - Regras de redirecionamento com Inspeção *SSL* só funcionarão para serviços em que o protocolo de segurança é suportado

- ***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 **[ ]** ou selecione ela novamente no menu. Para limpar esse campo, basta clicar em **[ ]**. Possui as opções abaixo:
  - *Abuse*;
  - *Anonymizers*;
  - *Attacks*;
  - *Malware*;
  - *Reputation*;
  - *Spam*.

DoS Protection

Neste painel estão disponíveis os controles de DoS Protection:



Avançado - Configurações de DoS Protection

- ***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.
  - ***Taxa de Pacote :*** A opção *Taxa de Pacote* configura o *Firewall* para limitar as conexões a um valor máximo de pacotes por segundo.
  - ***Taxa de Explosão:*** A opção *Taxa de Explosão* 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 salvar as alterações clique em **[** Save **]**, caso contrário, clique em **[ ]** ou em **[** Cancel **]** para cancelar todas as configurações e voltar a tela anterior.

Após salvar, será necessário acessar a **fila de comandos [** 1 **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Para ilustrar melhor os procedimentos listados acima, à seguir, analisaremos alguns exemplos.

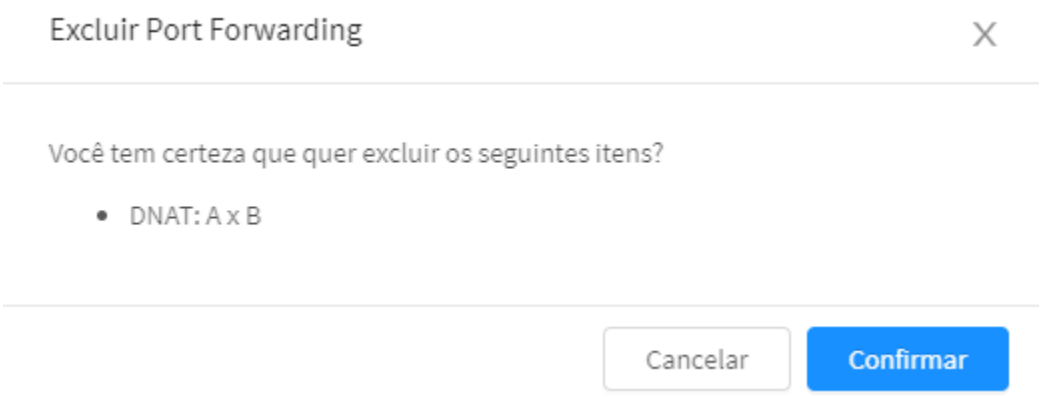
Port Forwarding - Excluir Port Forwarding

Através do botão de remoção é possível deletar vários itens ao mesmo tempo. Siga os seguintes passos:

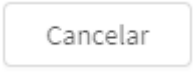
1. Selecione os itens que deseja deletar clicando no ícone de **seleção[ ]**;

Port Forwarding - Seleção para deleção

2. Clique no botão de **remoção[ ]** e uma tela perguntado se deseja deletar o item selecionado:



Port Forwarding - Remover Item

Caso deseje cancelar clique no botão **[**  **]**. Para concluir a deleção clique no botão **[**  **]**.

Removido com Sucesso

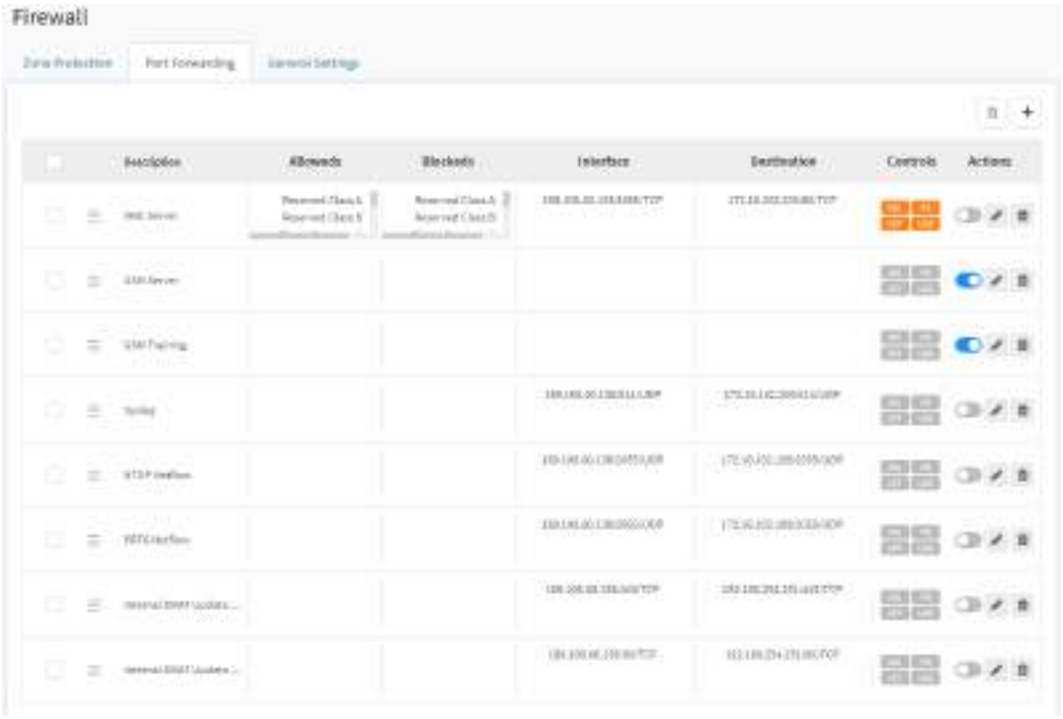
O item foi deletado com sucesso.

À seguir detalharemos o conteúdo das colunas.

Port Forwarding - Colunas

A seguir explicaremos cada coluna da aba *Port Forwarding*:

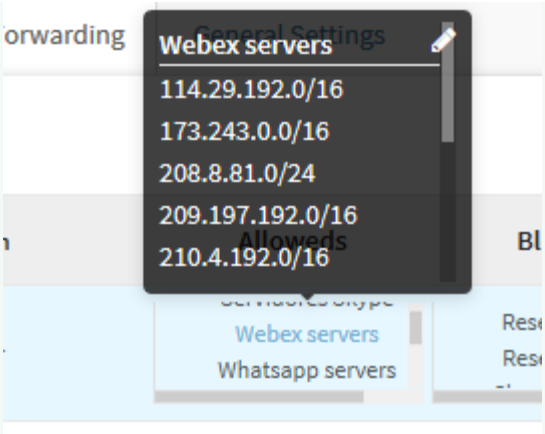
As regras de *Port Forwarding* são carregadas de cima para baixo, assim sendo, as regras mais no topo da tabela possuem prioridade sobre as abaixo (sendo possível até que elas sobreponham as configurações das regras de baixo).



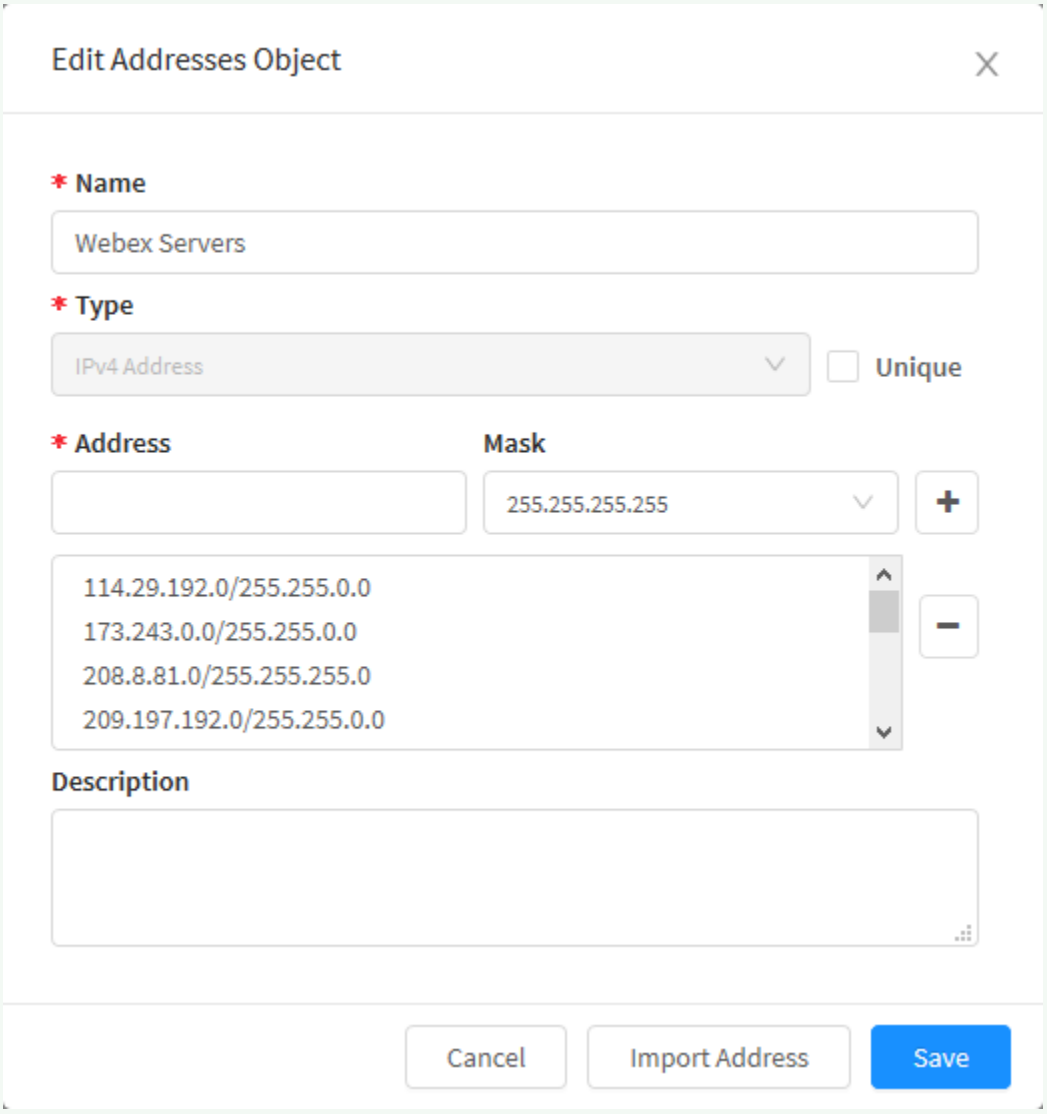
Port Forwarding

- ***Select* [ ]:** Permite selecionar uma política de *Port Forwarding;*
- ***Move[ ]:*** 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 [ ] exibido nesta janela é possível editar o objeto de endereço, conforme demonstrado abaixo:



- ***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*[IPS], *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

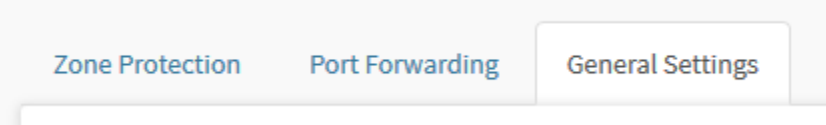
Através desta aba é possível habilitar e configurar as políticas de entrada para as portas e serviços locais do Blockbit UTM.

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*.

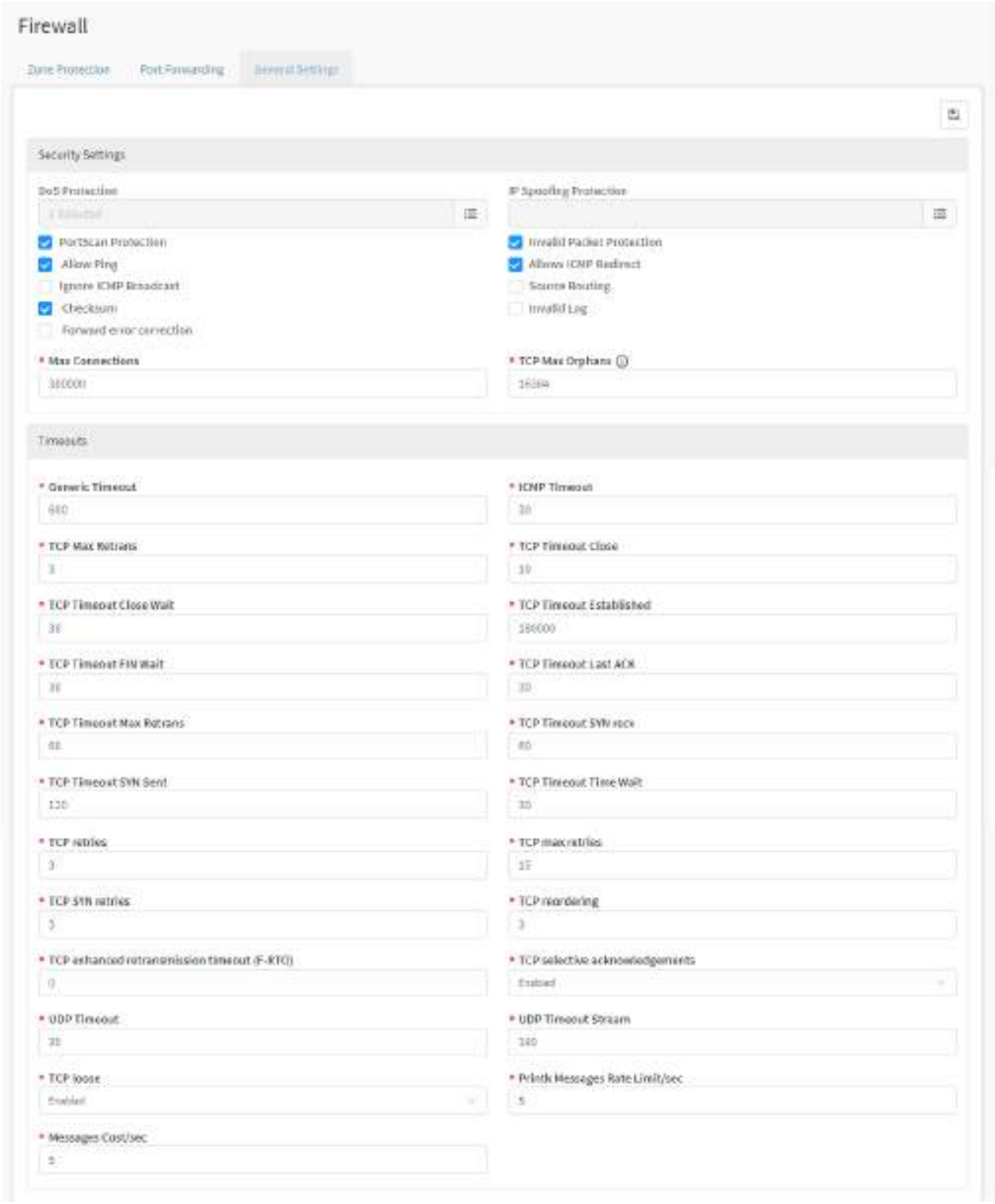
Os recursos pré-configurados referente aos itens das "Configurações de conexões" desta interface referem-se aos parâmetros de controle das conexões, a alteração destes valores implica diretamente no resultado de desempenho do servidor.

Para acessar, clique em *"General Settings".*



Aba *General Settings*

Surgirá a tela "*General Settings*", conforme demonstrado pela imagem abaixo:



General Settings

A tela "*General Settings*" é composta pelos seguintes painéis e recursos:

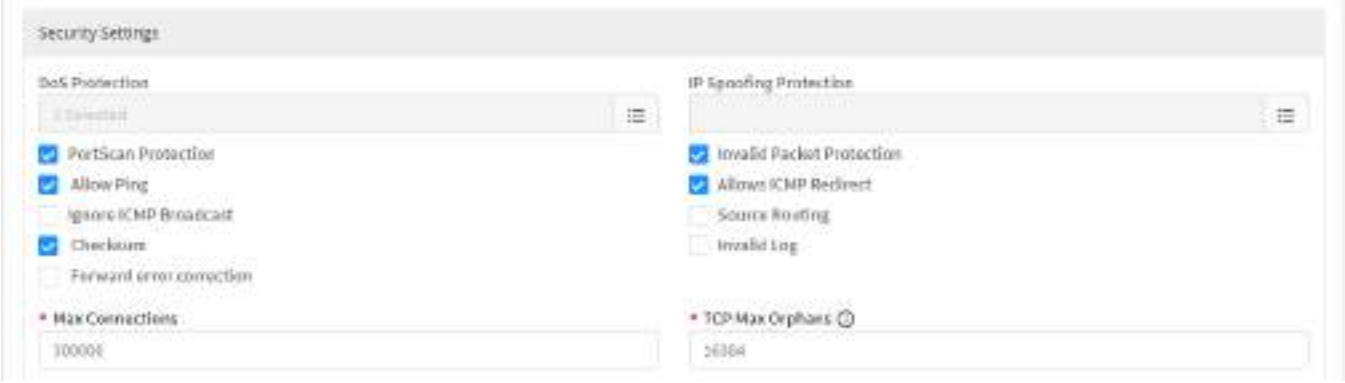
- *Security Settings*;

    - *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

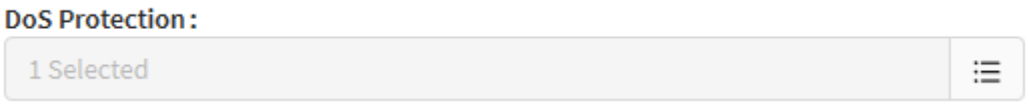
Serve para detalhar alguns dos itens de configurações dos parâmetros de segurança.



General Settings - Security Settings

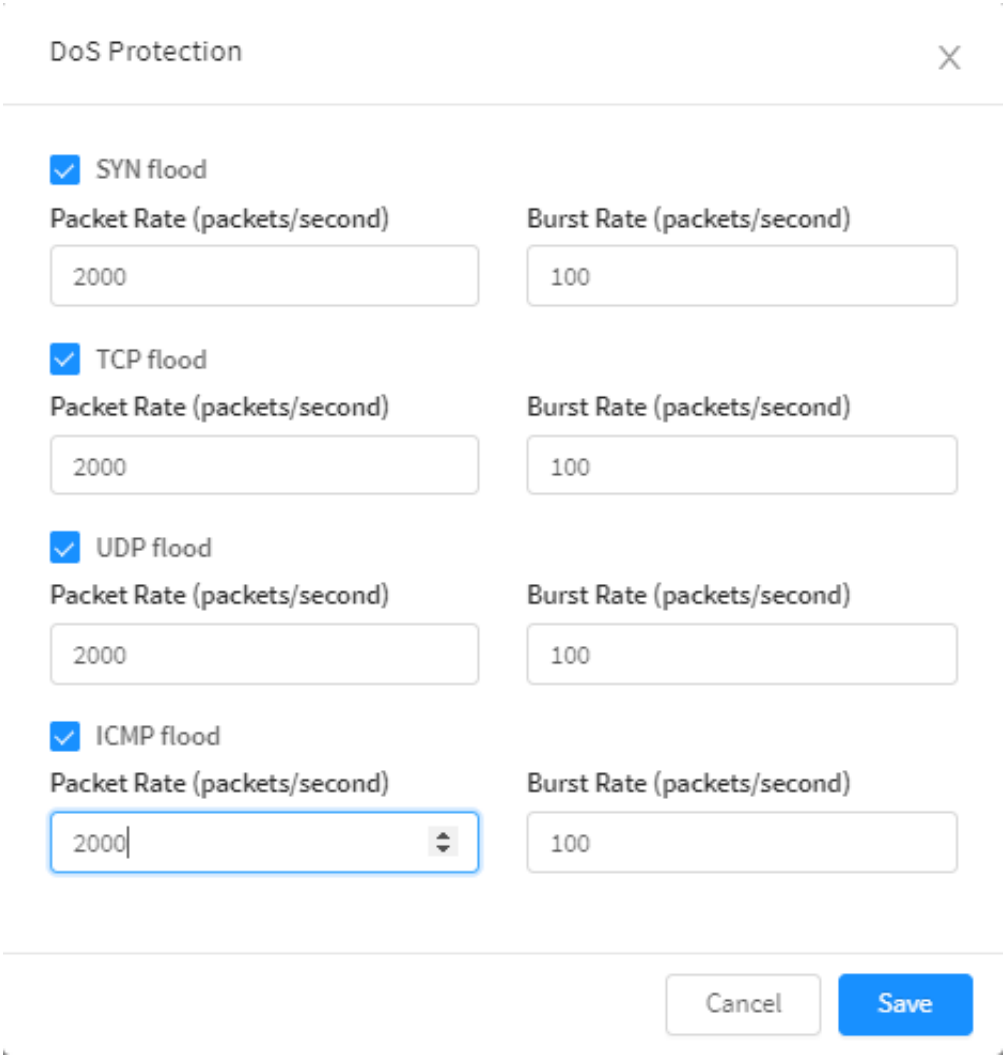
DoS Protection

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*.



Dos Protection

Ao clicar no botão **[** **]** a tela abaixo será exibida:



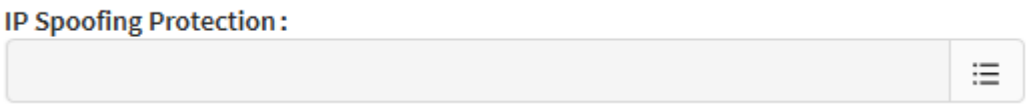
Dos Protection - Janela

- ***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

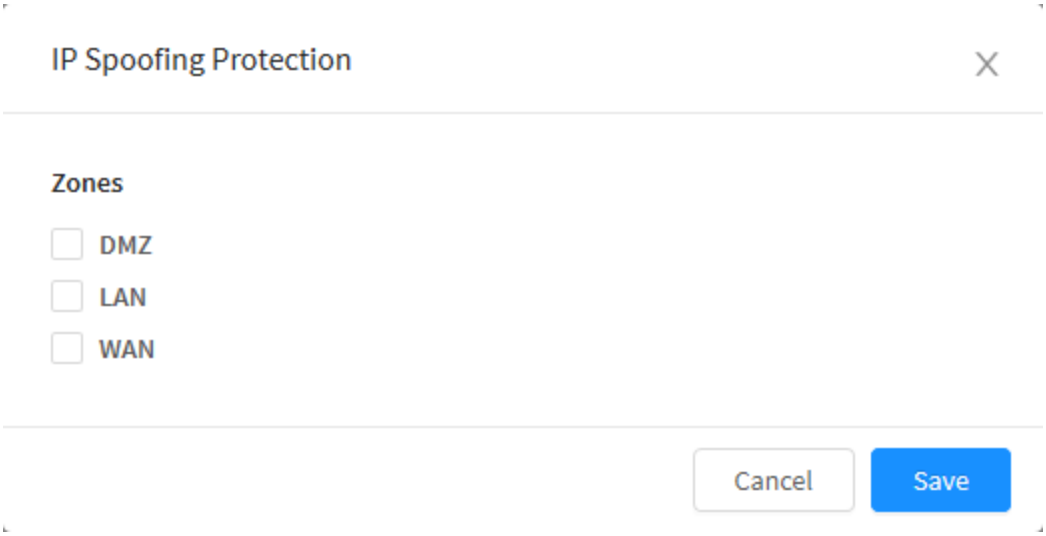
Este recurso habilita a proteção de *IP Spoofing* na zona de rede desejada.



IP Spoofing protection.

Zonas com [Proteção IP Spoofing] não permitem o uso do SD-WAN.

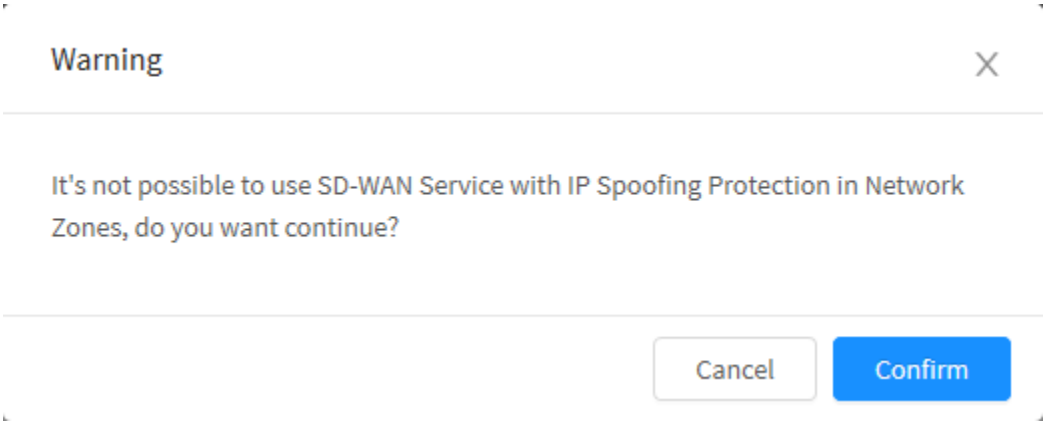
Ao clicar no botão **[ ]** a tela abaixo será exibida:



IP Spoofing protection Zones

Este recurso habilita a proteção de *IP Spoofing* na zona de rede desejada.

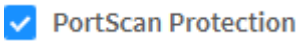
Esta opção pode causar problemas com o serviço de SD-WAN



Alert: SD-WAN and IP Spoofing Protection problems.

PortScan Protection

Este recurso permite identificação e o bloqueio de aplicativos com o objetivo de mapear as portas *TCP* e *UDP*. Aplicativos *PortScan* tentam identificar o *st atus* das portas, se estão fechadas, escutando ou abertas. Geralmente, os *port scanners* são usados por pessoas mal-intencionadas para identificar portas abertas, explorar vulnerabilidades e planejar invasões. **Recomendação**: Ex: *"[Habilitar]".*



PortScan Protection

Invalid Packet Protection

São considerados pacotes inválidos os que não respeitam o padrão do diagrama de estado *TCP* (*handshake*). Recomendação: Ex: "*[Habilitar]". O* serviço de firewall descarta os pacotes considerados inválidos.

Invalid Packet Protection

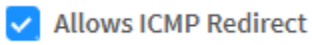
Allow Ping

Este recurso permite que todas as solicitações de *PING* (*Echo Request* e *Echo Reply*) sejam respondidas através de qualquer interface de rede do sistema. Recomendação: Ex: *"[Desabilitar]".*

Allow Ping

Allows ICMP Redirect

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]".*



Allows ICMP Redirect

Este item vem com padrão [Habilitado] por identificação de inúmeras estruturas de rede mal definidas.

Ignore ICMP Broadcast

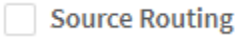
Esse recurso ignora o tráfego *ICMP Broadcast*, usado para fazer com que servidores participem involuntariamente de ataques *DOS*, enviando grande quantidade de pings aumentando exponencialmente o tráfego *NETBIOS* da rede e tornando os serviços reais indisponíveis.

Recomendação: Ex: *"[Habilitar]" Ignore ICMP Broadcast.*

Ignore ICMP 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]".*



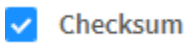
Source Routing

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

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.

FEC - Forward error correction

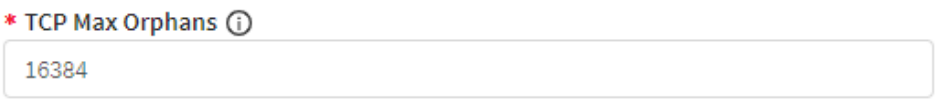
Max Connections

Número máximo de conexões.

Max connections

TCP Max Orphans

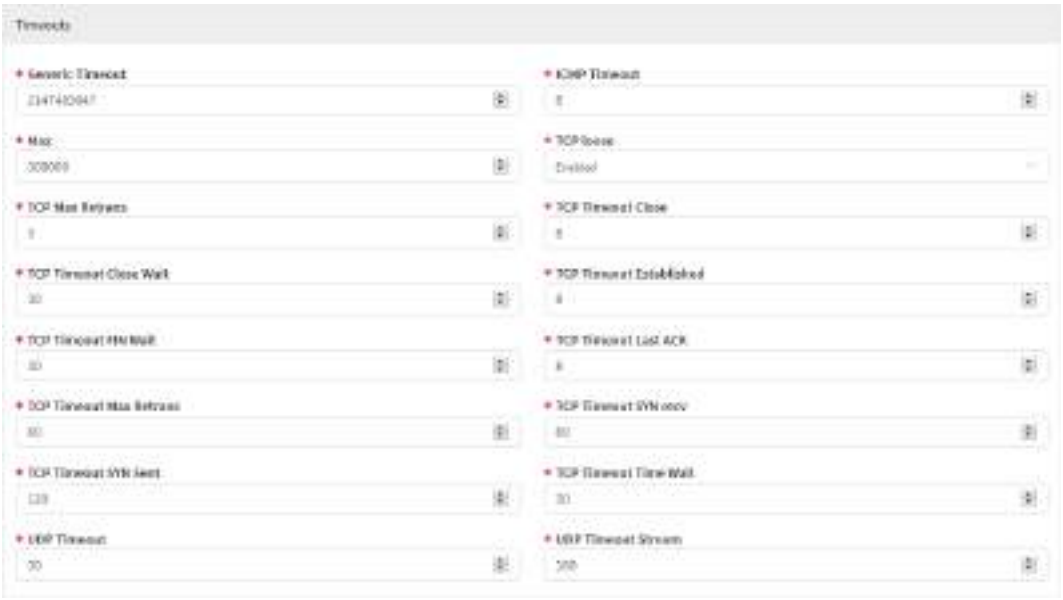
Número máximo de TCP sockets não associados a processos ou serviços, que são executados pelo OS no user space. Caso este número seja excedido, as conexões são imediatamente resetadas.



TCP Max 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.



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

ICMP Timeout

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

Max Connections

Tamanho máximo da tabela de *session tracking*, ou seja, de conexões estabelecidas simultaneamente. O valor padrão é 300.000 segundos.

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 Loose

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

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.

TCP timeout close

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.

TCP timeour close wait

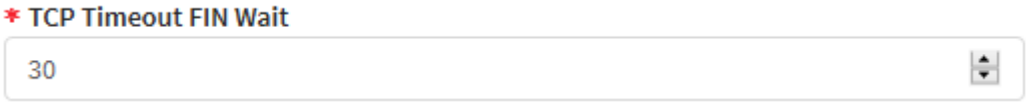
TCP Timeout Established

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 timeout established

TCP Timeout FIN Wait

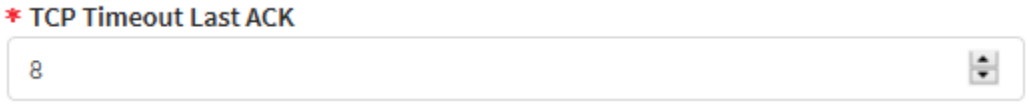
Define o *timeout* em segundos para conexões *TCP* com estado *FIN-WAIT-1* e *FIN-WAIT-2*, para serem removidas da tabela de *session tracking*. O valor mínimo é 0 e o valor padrão é 30 segundos.



Timeout 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.



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

TCP Timeout SYN Recv

Define o *timeout* em segundos para conexões *TCP* com o estado *SYN RECV*, para serem removidas da tabela de *session tracking*. O valor mínimo é 0 e o valor padrão é 60 segundos.

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

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

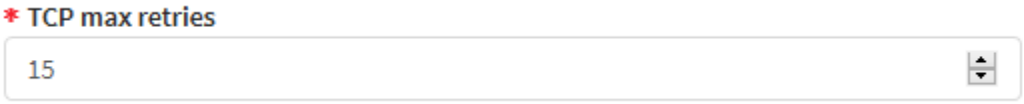
TCP Retries

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 retries

TCP Max Retries

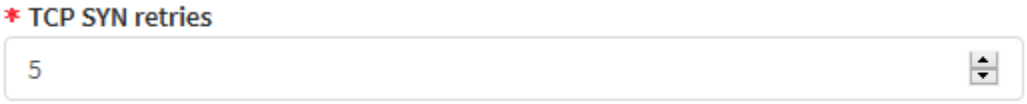
Define o máximo de vezes que a retransmissão de pacotes TCP será efetuada antes de interromper esse processo. O valor padrão é 15 (equivale a cerca de 13 a 30 minutos).



TCP max retries

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.

ATENÇÃO: 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.

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).

Para mais detalhes a respeito deste recurso, consulte o RFC 4138.

TCP enhanced retransmission timeout (F-RTO)

TCP Selective Acknowledgements

Este campo permite ativar ou desativar o recurso *TCP Selective Acknowledgements* (*SACK*). Esta funcionalidade atua enviando ao remetente um informe de tudo que foi recebido com sucesso de modo que todos os pacotes de dados e segmentos que foram perdidos, possam ser enviados novamente pelo remetente, garantindo a integridade dos pacotes de dados e limitando a quantia de retransmissões. Por padrão, este campo fica habilitado.

Para mais detalhes a respeito deste recurso, consulte o RFC 2018.

TCP selective acknowledgements

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

UDP Timeout Stream

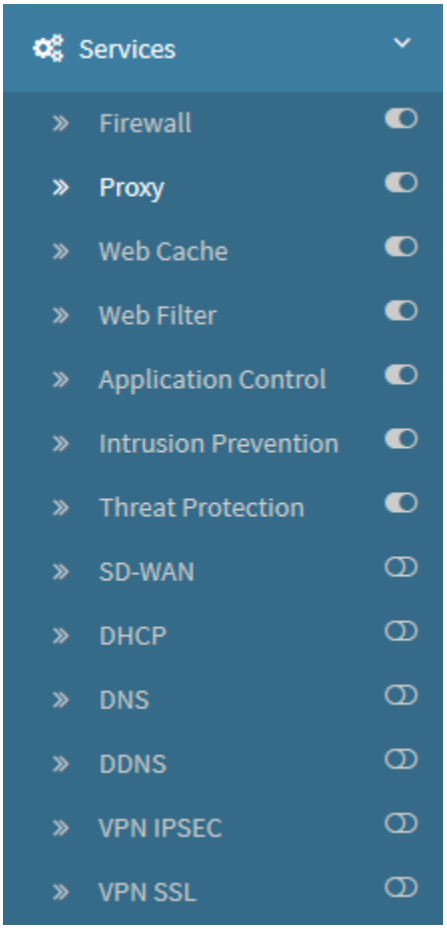
Define o *timeout* em segundos para conexões *UDP STREAM* (*ASSURED*). O valor mínimo é 0 e o valor padrão é 180 segundos.

UDP timeout stream

NGFW - Services - Proxy

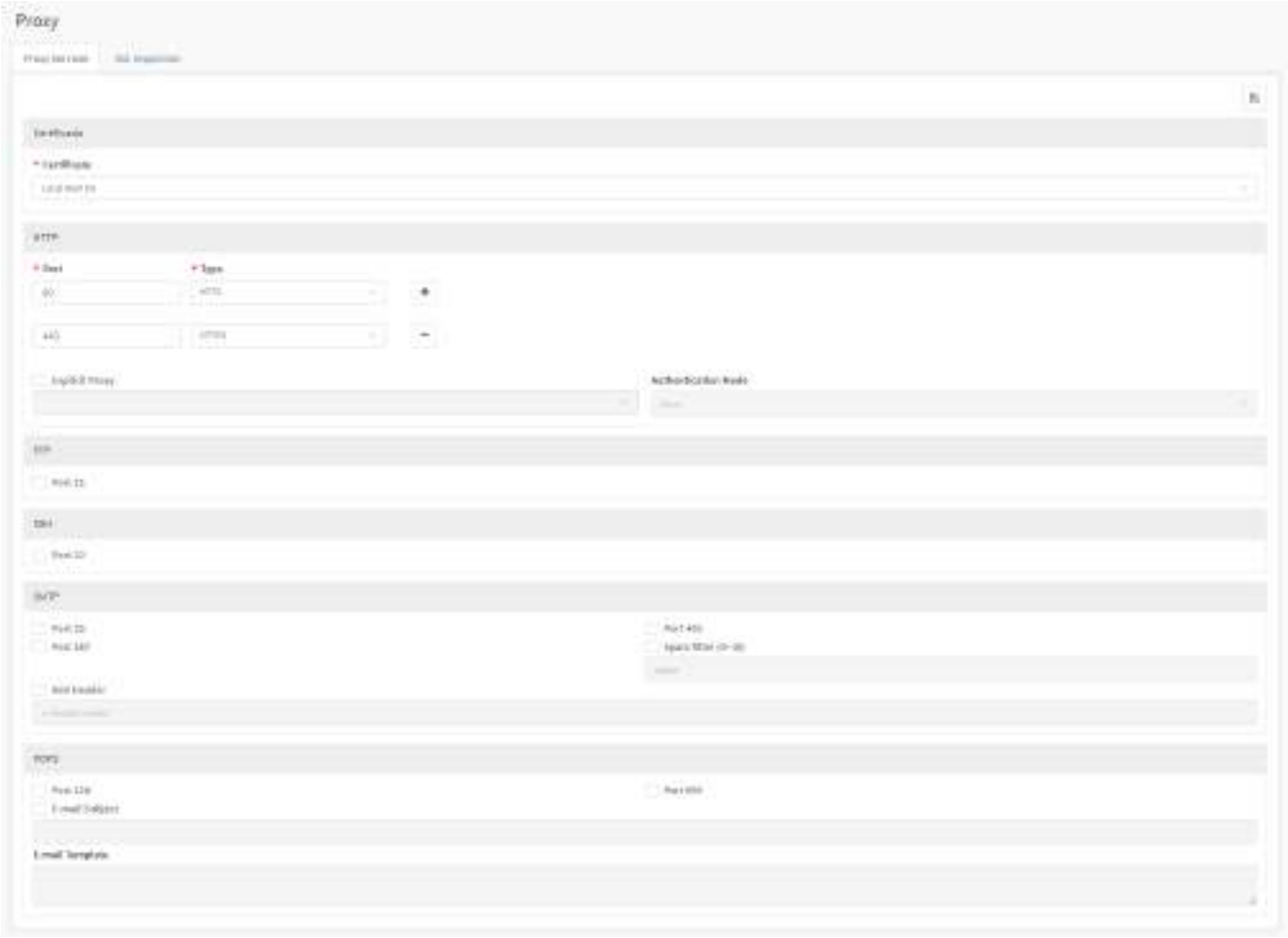
A tela *Proxy* tem como função configurar o funcionamento dos *proxies* do sistema e também como a inspeção *SSL* atuará. A seguir analisaremos mais detalhadamente.

Para acessar esta tela, basta navegar até o menu/opção “Serviços > *Proxy*”:



Services - Proxy

A tela abaixo será exibida:



Proxy

Essa tela possui as seguintes opções:

- *Proxy Services;*
- *Proxy SSH;*
- *SSL Inspection.*

A seguir analisaremos os componentes da aba 'Proxy Services'

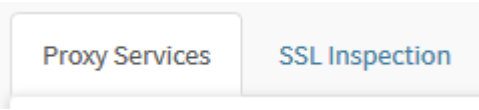
Proxy - Proxy Services

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 “P*roxies”* 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).

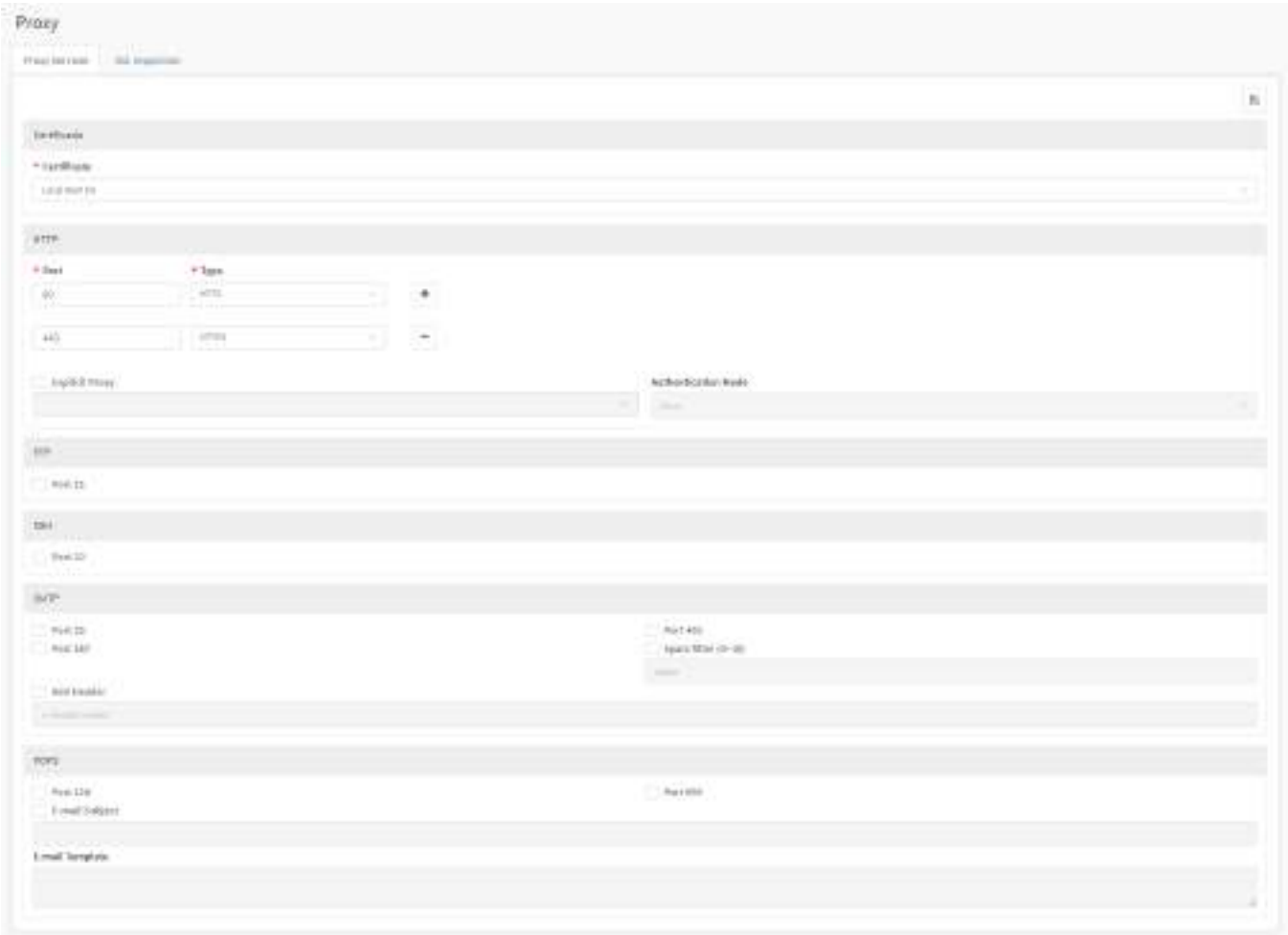
Na maioria das vezes os P*roxies* são utilizados por todos os clientes de uma sub-rede e devido a sua posição estratégica, normalmente eles implementam um sistema de cache para alguns serviços. Além disso, como os *proxies* trabalham com dados das aplicações, para cada serviço é necessário um P*roxy* 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:



Services – Proxy Services

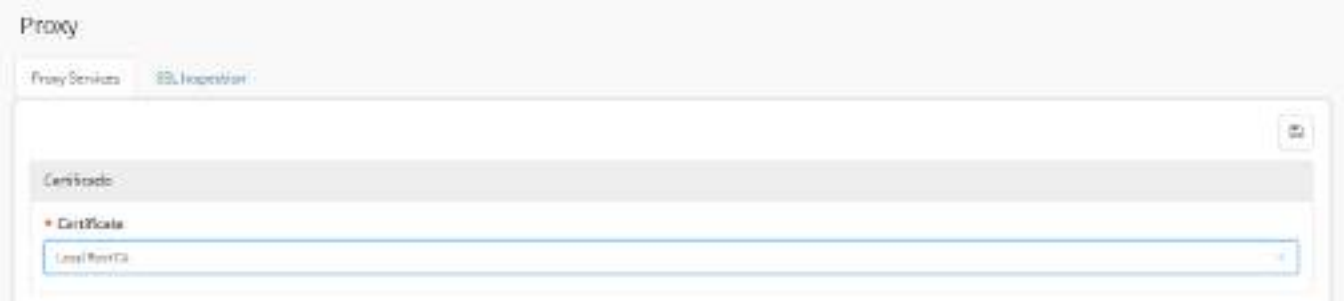
O Blockbit NGFW, inclui serviços de segurança por meio de P*roxies* ativos, os protocolos e serviços suportados são:

- *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 - 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:

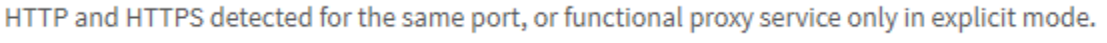
Proxy HTTP

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:



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 *TCP* 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 *proxy* 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

- **[ ] 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 *proxy* 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.

> 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.

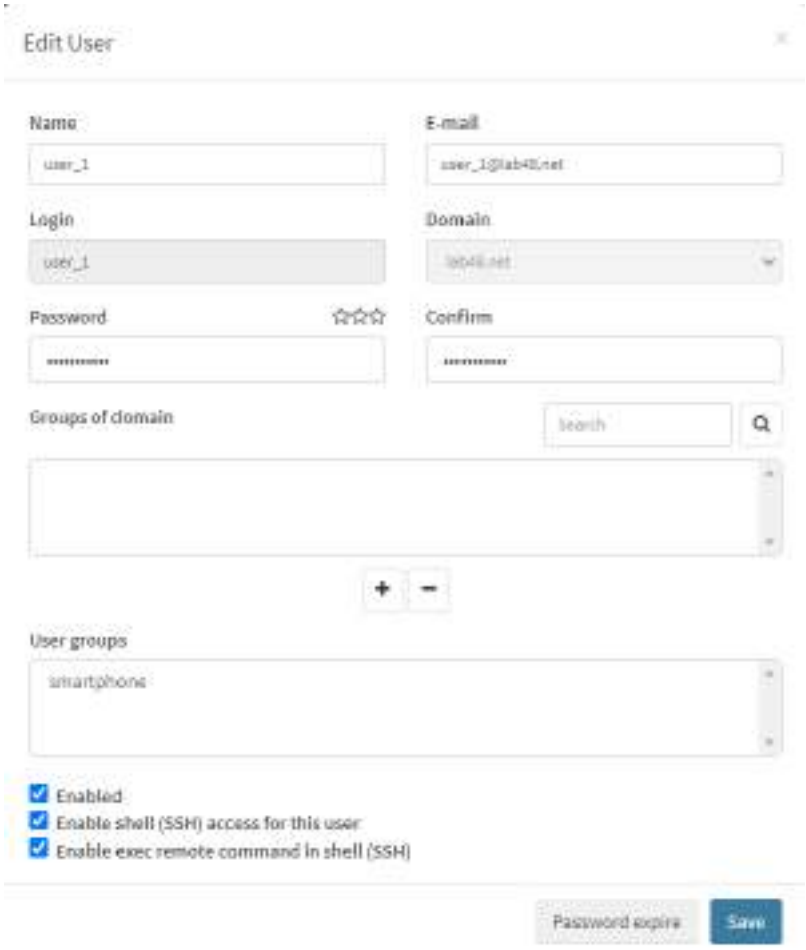
O uso do SSH deve ser limitado a administradores que necessitam acessar os serviços de rede, logar todo o tráfego, e também considere configurar o Multi-Factor Authentication para garantir que somente usuários legítimos possam utilizar SSH para acessar dispositivos, ação esta que pode reduzir a probabilidade 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:

Serviço de Proxy SSH

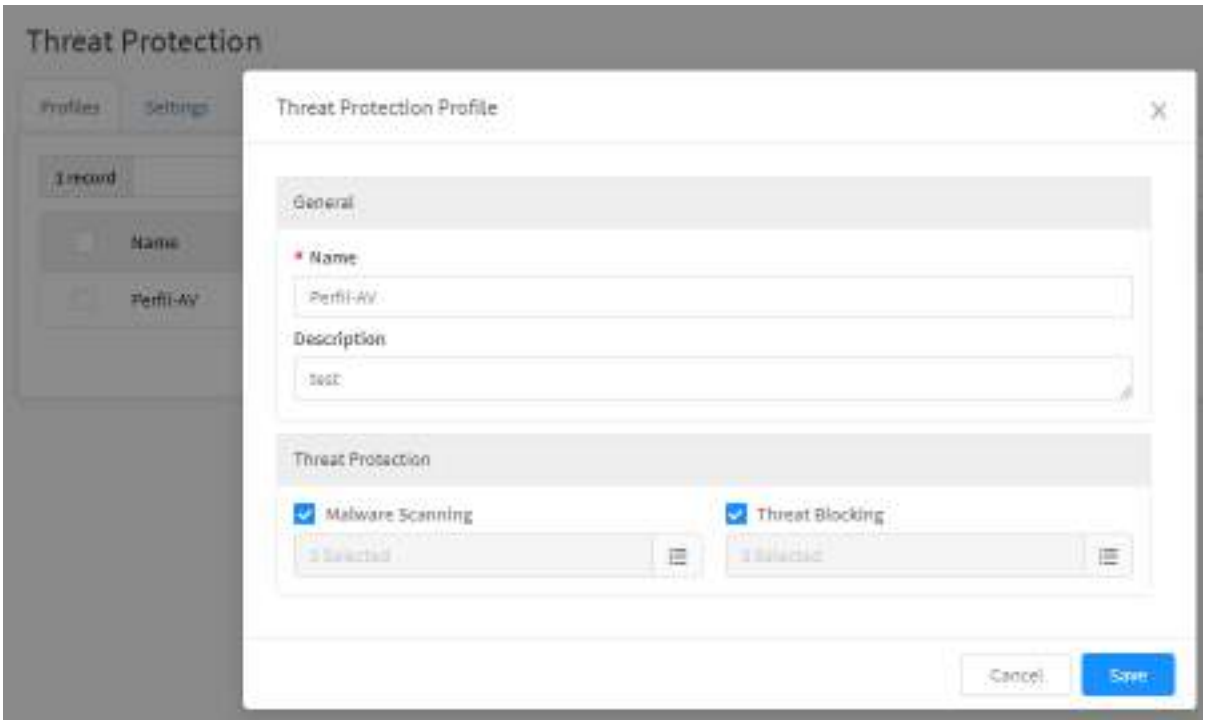
A seguir devemos ir para Configurações > Autenticação > Usuários, nesta outra seção podemos criar um usuário ou editar um pré-existente. A opção "Permitir acesso ao shell (SSH)" e "Permite executar comando remoto no shell (SSH)" devem ser marcadas:



Permissões de usuário

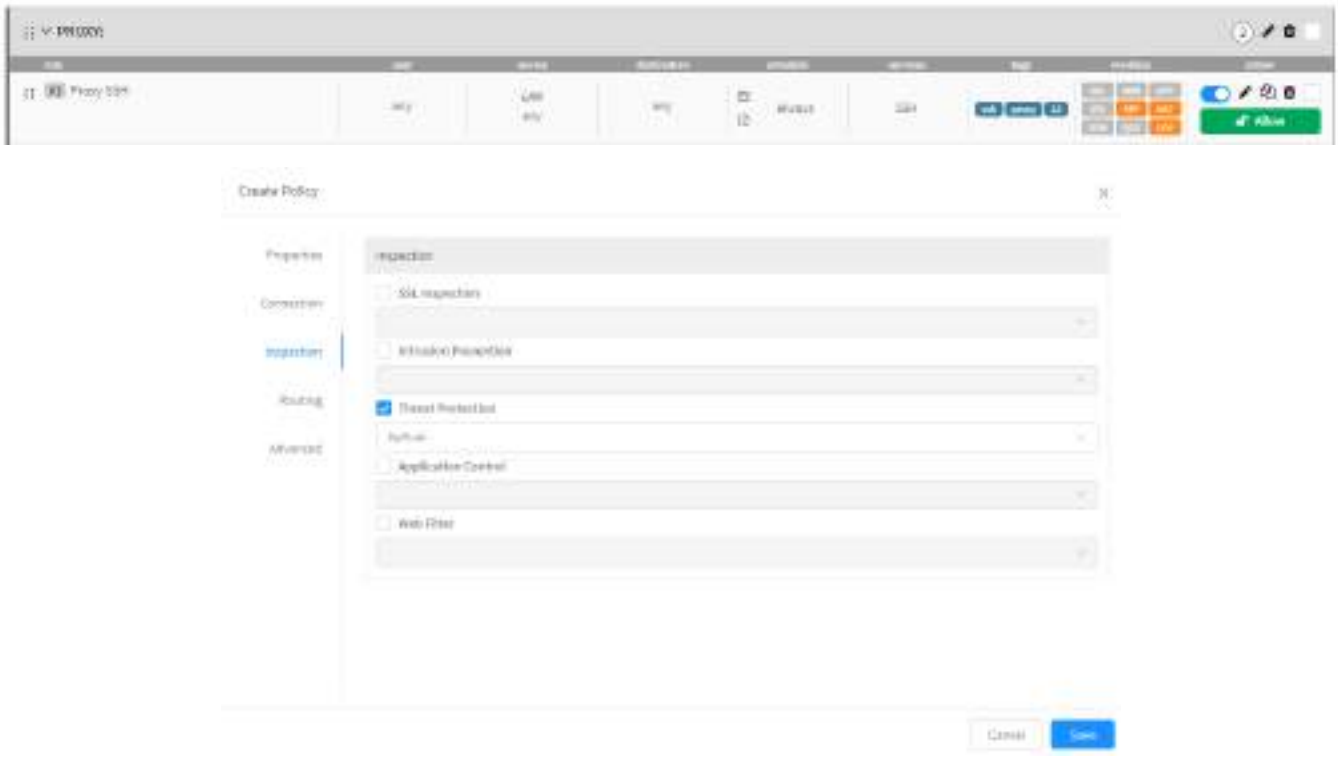
> É importante salientar que esta configuração é valida somente para usuário local, e logins remotos ***não*** terão a opção.

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":



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:



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:

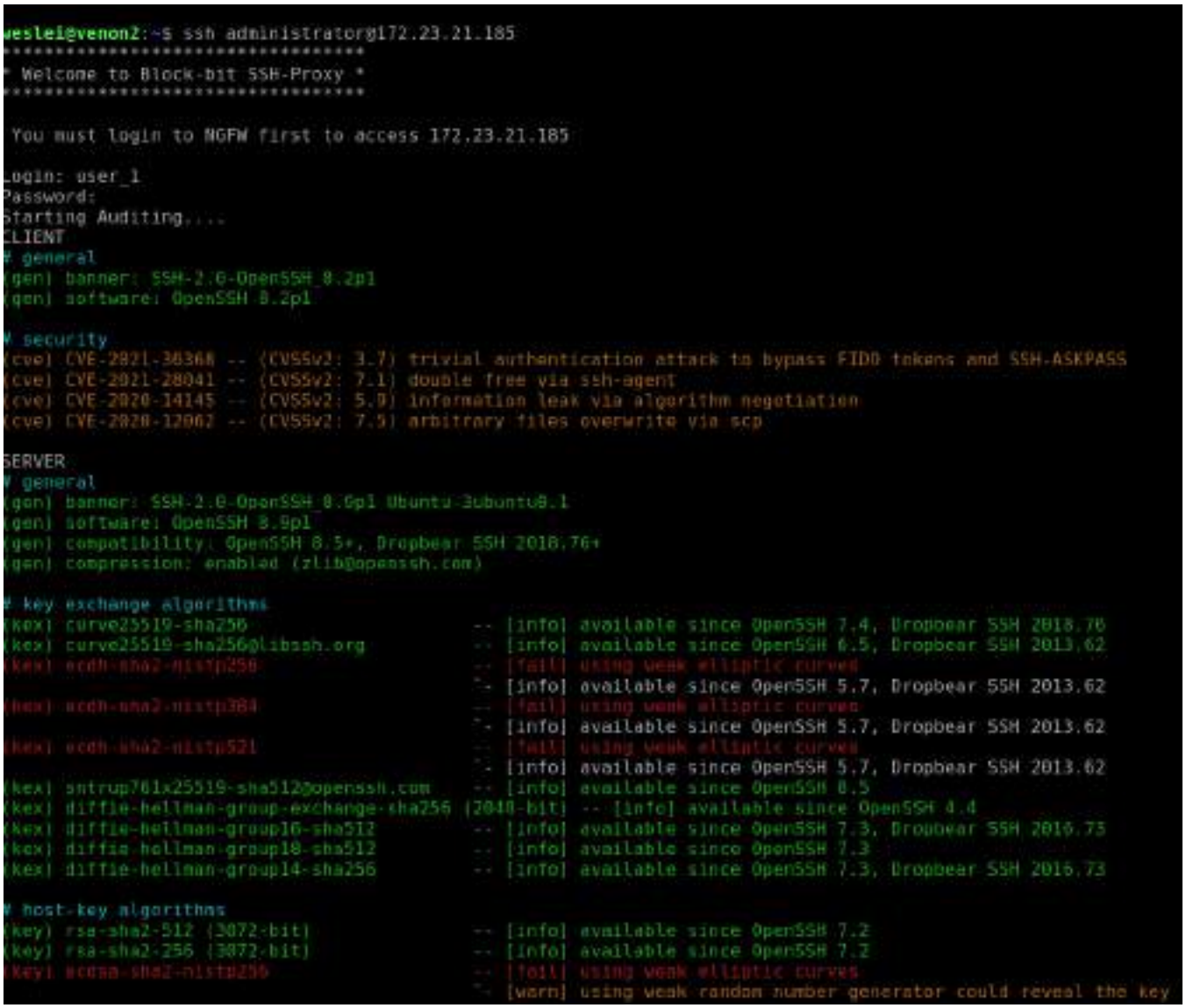
```
\*********************************
\* Welcome do Block-bit SSH-Proxy *
\*********************************

 You must login to NGFW first to access 172.16.12.100

 Username:
 Password:
```

SSH Proxy - validação de usuário

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:



Resultados da análise de vulnerabilidade

Deste modo finalizamos a configuração do Proxy SSH e acesso ao servidor.

Caso haja alguma notificação indicando a troca de "fingerprint" a mesma deve ser ignorada, uma vez que o SSH está sendo conectado no Blockbit.

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:

Proxy SMTP

- [ ] **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*.
- [ ] **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.
- [ ] **Porta 587:** Habilitação da porta *SMTP Submission* de conexão com os servidores *SMTP* Remotos. Porta [*SMTP Sub* 587/*TCP*].
- [ ] **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 *e-mail* 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”.

- [ ] **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.”.*

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 *proxy* 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: NGFW - Fila de comandos.

Caso seja necessário integrar filtro *Malware Scanning* por meio do tráfego *Proxy SMTP,* será necessário efetuar a habilitação e configuração do serviço *Threat Protection*.

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*]”.

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 POP*, analise as considerações abaixo:

Proxy POP3

- [ ] ***Port* 110:** Habilitação da porta padrão de conexão com os servidores *POP* Remotos. Porta [*POP3* - 110/*TCP*];
- [ ] ***Port* 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 esta porta nas conexões cliente-servidores por meios dos clientes de e-mail. Ex.: “Thunderbird e Outlook”.

- [ ] ***Email Subject:*** Este campo contempla um recurso de “Sinalização” que devolve ao usuário um *E-mail* de notificação do tipo *“Mailer Postmaster”* Informativo quanto ao tratamento aplicado sobre o *E-mail* recebido pelo proxy *POP* do servidor *POP* remoto;

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:
    %PROTOCOL% from %CLIENTIP%:%CLIENTPORT% to %SERVERIP%:%SERVERPORT%
```

Proxy POP3 - E-mail Template

O funcionamento do Proxy POP requer a configuração de uma “Política de Segurança” com o filtro de conteúdo Email Protection habilitado para o protocolo POP.

Para salvar todas as alterações, clique em **[ ]**.

Após salvar, para que o *proxy* 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.

Caso seja necessário integrar filtro *Malware Scanning* por meio do tráfego *Proxy POP,* será necessário efetuar a habilitação e configuração do serviço *Threat 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.

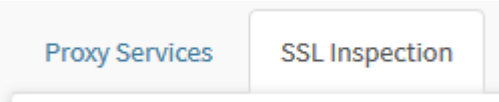
Este recurso atua basicamente conforme os seguintes passos:

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*".



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.

Proxy – SSL Inspection

A importação de certificados de servidor para inspeções de tráfego HTTP de entrada também é suportada. Após a importação dos mesmos, permite o seu uso na configuração de regra de IPS para Inspeção HTTP.

A solução permite a utilização de profile criado em diferentes regras de Firewall (origem, destino, tipo de serviço, ação e certificado).

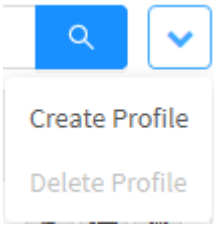
A seguir, o menu de ações será analisado e posteriormente nos aprofundaremos no conteúdo das colunas do painel *SSL Inspection*.

Proxy - SSL Inspection - Menu de ações

No topo direito da tela temos o menu de ações:

SSL Inspection – Botão do 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.

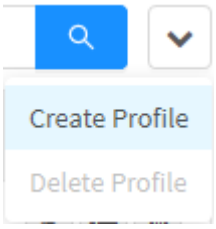
Proxy - SSL Inspection - Menu de Ação - Create Profile

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:

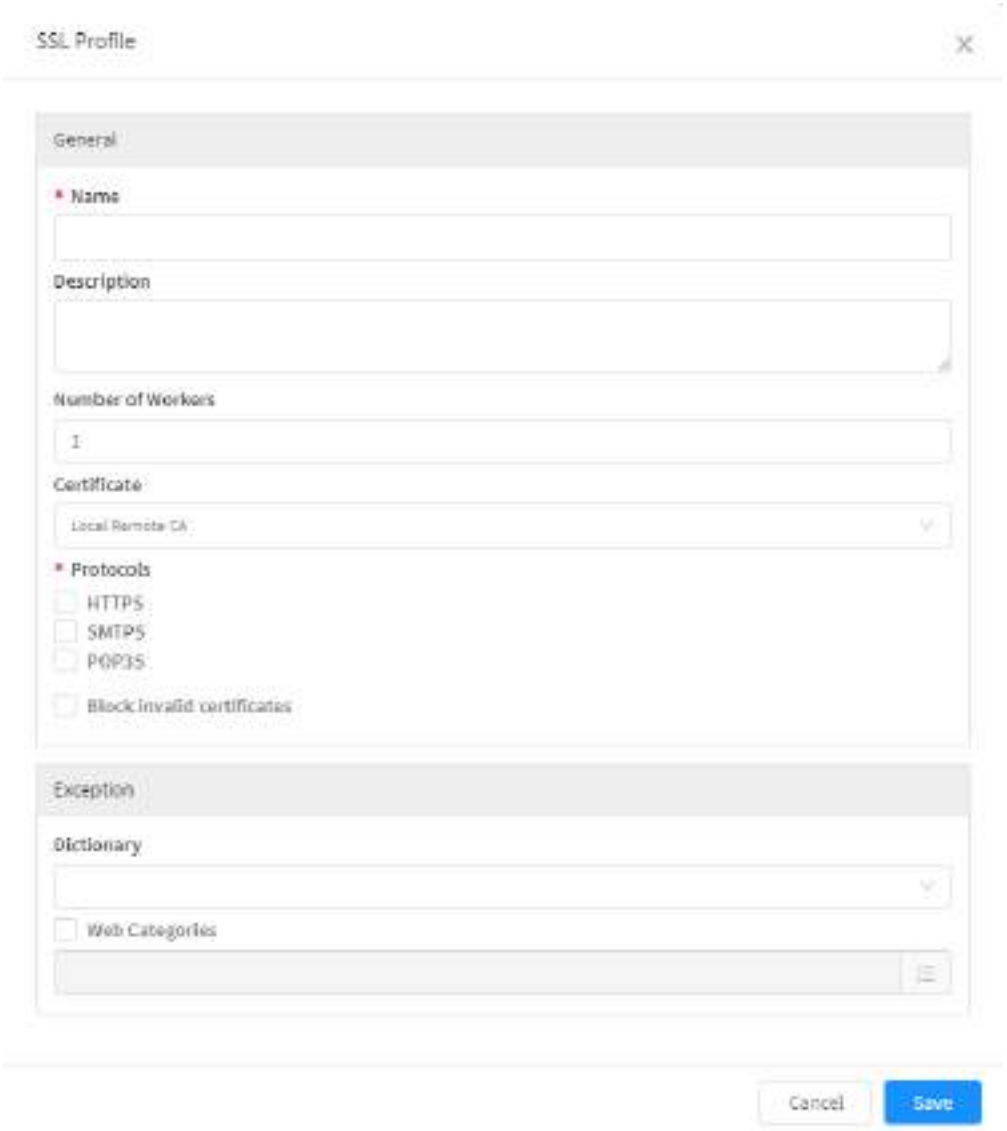
- General;
- Exception.

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 Inspection - SSL Profile

General

Neste painel são efetuadas as configurações gerais do perfil *SSL*.

SSL Inspection - SSL Profile - General

- ***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

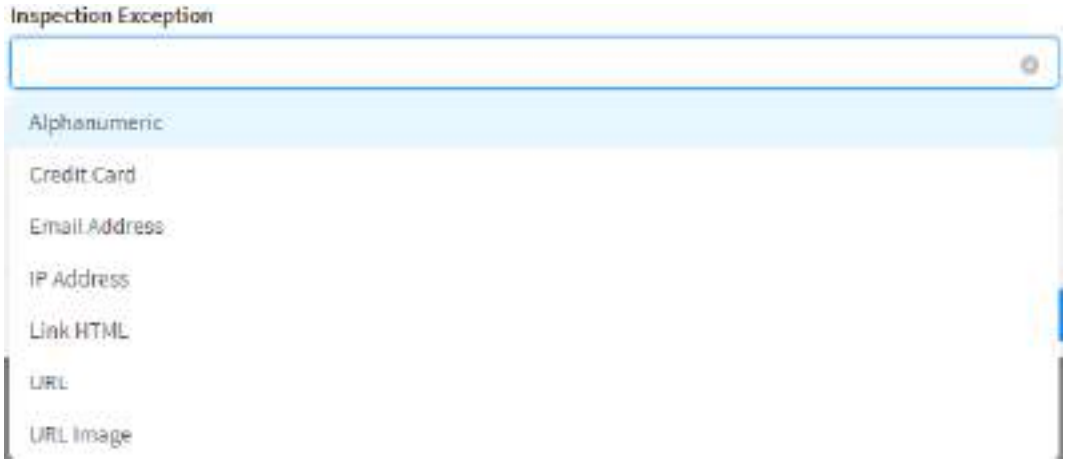
Neste painel são configuradas as exceções do perfil *SSL:*

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.

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).

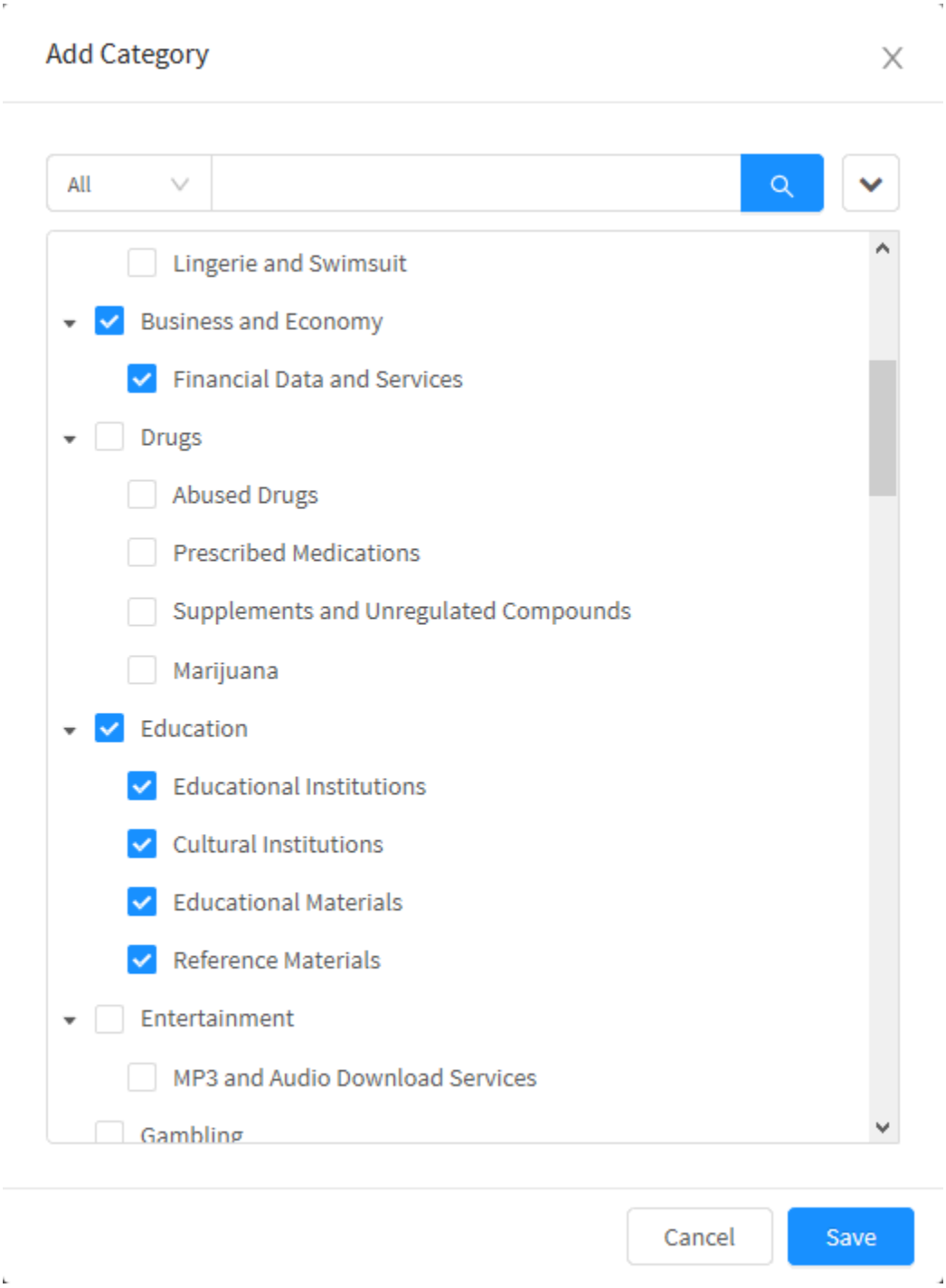
Para consultar o fluxo de inspeção de pacotes, consulte a arquitetura do UTM.



SSL Exception

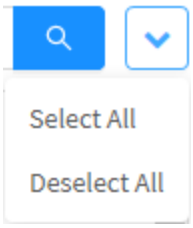
Este recurso atende os casos de condições específicas de Aplicações e Serviços que não leem os certificados do sistema, também não tem a opção de importar o certificado em sua aplicação, casos muito comuns para serviços e aplicativos de “Bancos, instituições financeiras e Governo”, e é muito útil para 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:



SSL Inspection - Add Category

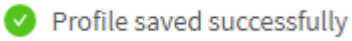
Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no **menu de ações [ ]**:



SSL Inspection - Add Category - Menu de Ações

Para sair deste painel, clique no botão ***Cancel*[** Cancel **]** ou clique no botão ***Save*[** Save **]** para concluir a adição das categorias.

Por fim, caso deseje cancelar a configuração clique no botão ***Cancel*[** Cancel **]**. Para concluir a criação do perfil clique no botão ***Save*[** Save **]**.



Profile saved successfully

O perfil foi criado com sucesso.

A seguir veremos como apagar um perfil em Delete Profile.

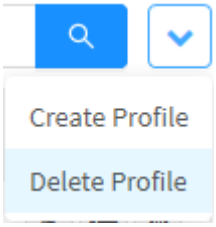
Proxy - SSL Inspection - Menu de Ação - Delete Profile

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*;

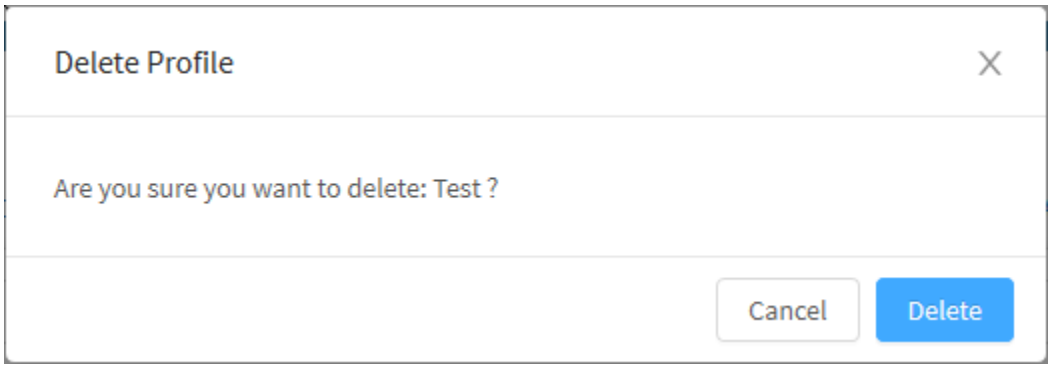
SSL Inspection – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete Profile*”.



SSL Inspection – Delete Profile.

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



SSL Inspection – Mensagem se deseja deletar os p*rofiles*

Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].

Profile deleted successfully

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

Proxy - SSL Inspection - Colunas

A seguir explicaremos cada coluna da aba *SSL Inspection*:

Profiles – SSL Inspection

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.

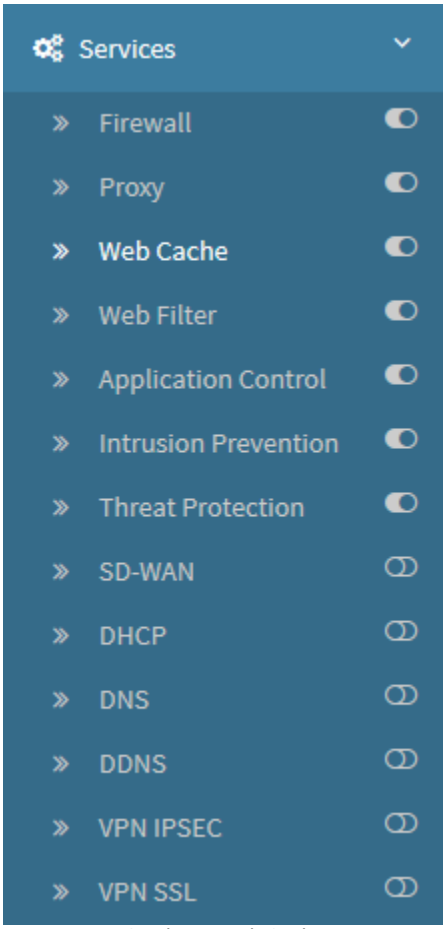
UTM - Services - Web Cache

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.

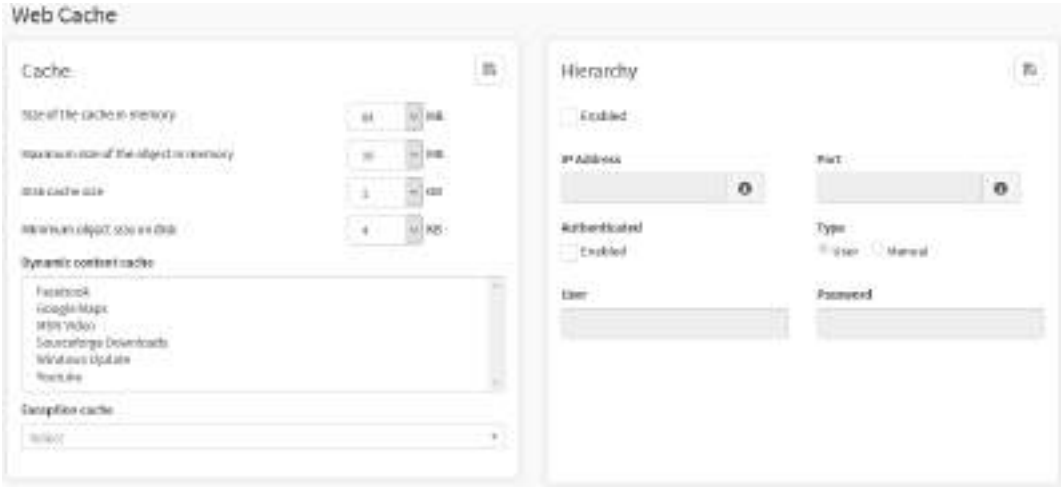
A configuração do serviço *Web Cache* é definida pela configuração dos controles de cache e ainda conta com o recurso de redirecionamento do tráfego para um *proxy* hierárquico.

Para acessar esta tela, basta selecionar a opção “*Web Cache*”.



Services - Web Cache

A tela abaixo será exibida:



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.

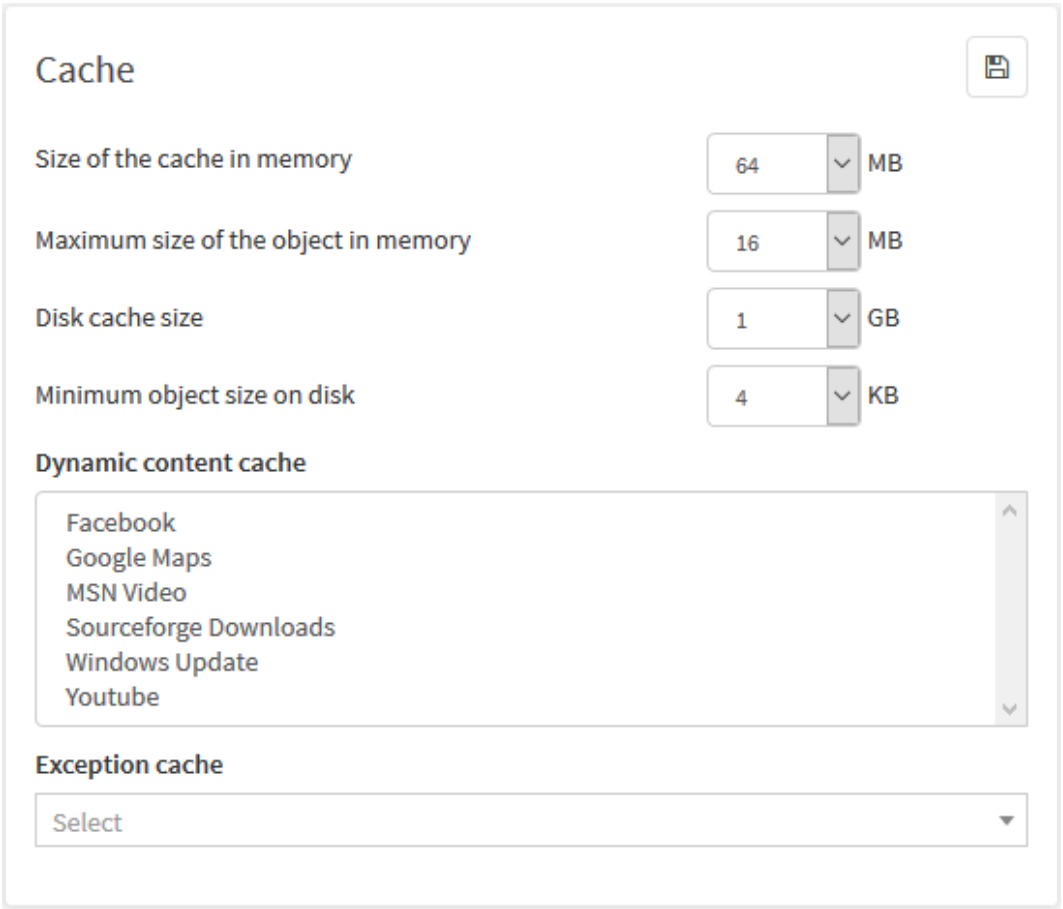
Normalmente a resposta a requisição é atendida de forma dinâmica onde cada servidor da pilha de servidores próximos a requisição responde fragmentos do conteúdo solicitado.

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.



Web Cache Settings

*Para salvar todas as alterações, clique em **[**  **]**.*

Após salvar, para que as alterações tenham efeito 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.

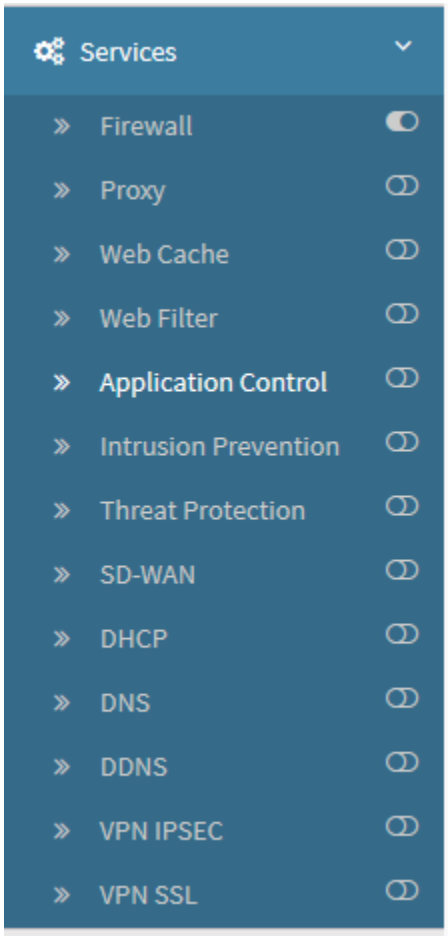
Após realizar esses procedimentos as configurações de *Cache* terão sido configuradas com sucesso.

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

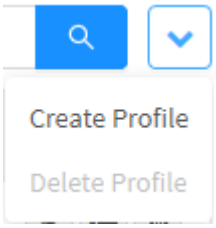
A seguir, o menu de ações será analisado e posteriormente nos aprofundaremos no conteúdo das colunas do painel *Application Control*.

Services - Application Control - Menu de ações

No topo direito da tela temos o menu de ações:

Application Control – Botão do 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.

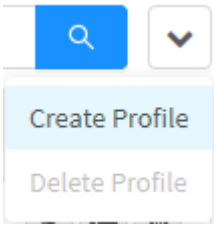
Services - Application Control - Menu de ações - Create Profile

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:

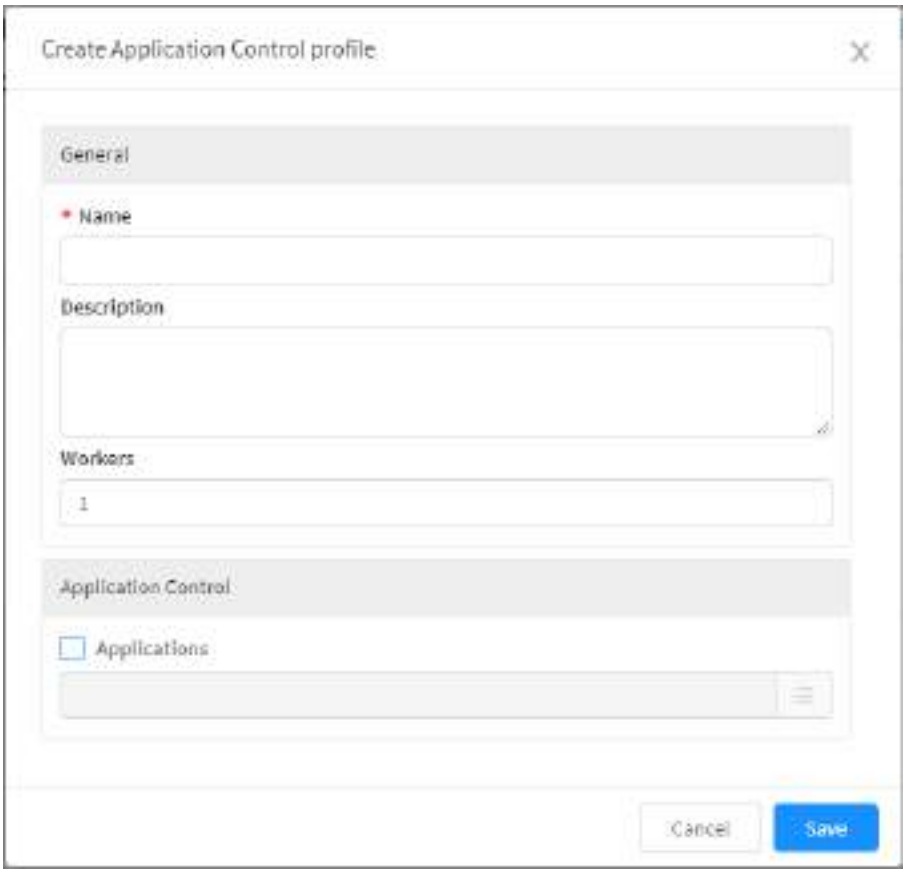
- General;
- Application Control.

Para acessar, clique no **menu de ações [ ]**, e selecione a opção “*Create Profile*”;



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.



Application Control - Create Profile

General

Em "*General*" temos as seguintes caixas de texto:

Application Control – General

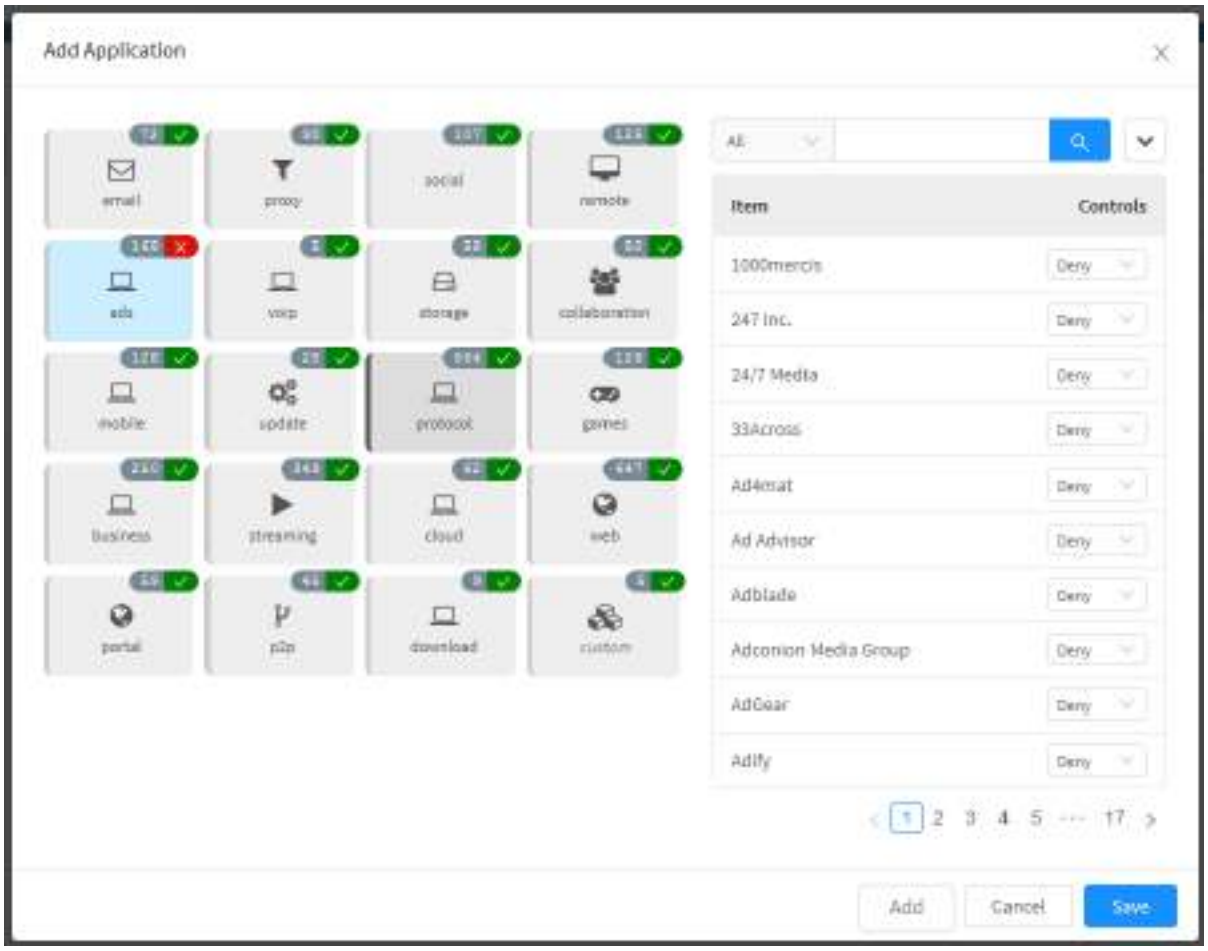
- ***Name:*** Definir um nome para o perfil. Ex.: *Deny All Ads*;
- ***Description*****:** Definir uma descrição para o perfil. Ex.: *Application Control to deny all ads.*
- ***Workers:*** Definir um número de workers, ou processos, por perfil de inspeção. Note que o campo vem pré-definido como 1.

Application Control

Em "*Application Control*" são determinadas as aplicações cujo acesso será permitido ou negado:

Application Control - Applications

Para editar as aplicações, certifique-se que o **checkbox [** **]** está habilitado, depois clique no botão **list applications [** **]** para administrar as permissões.



Application Control - Add *Application*

Ao selecionar um dos ícones à esquerda, as aplicações serão exibidos no painel à direita.

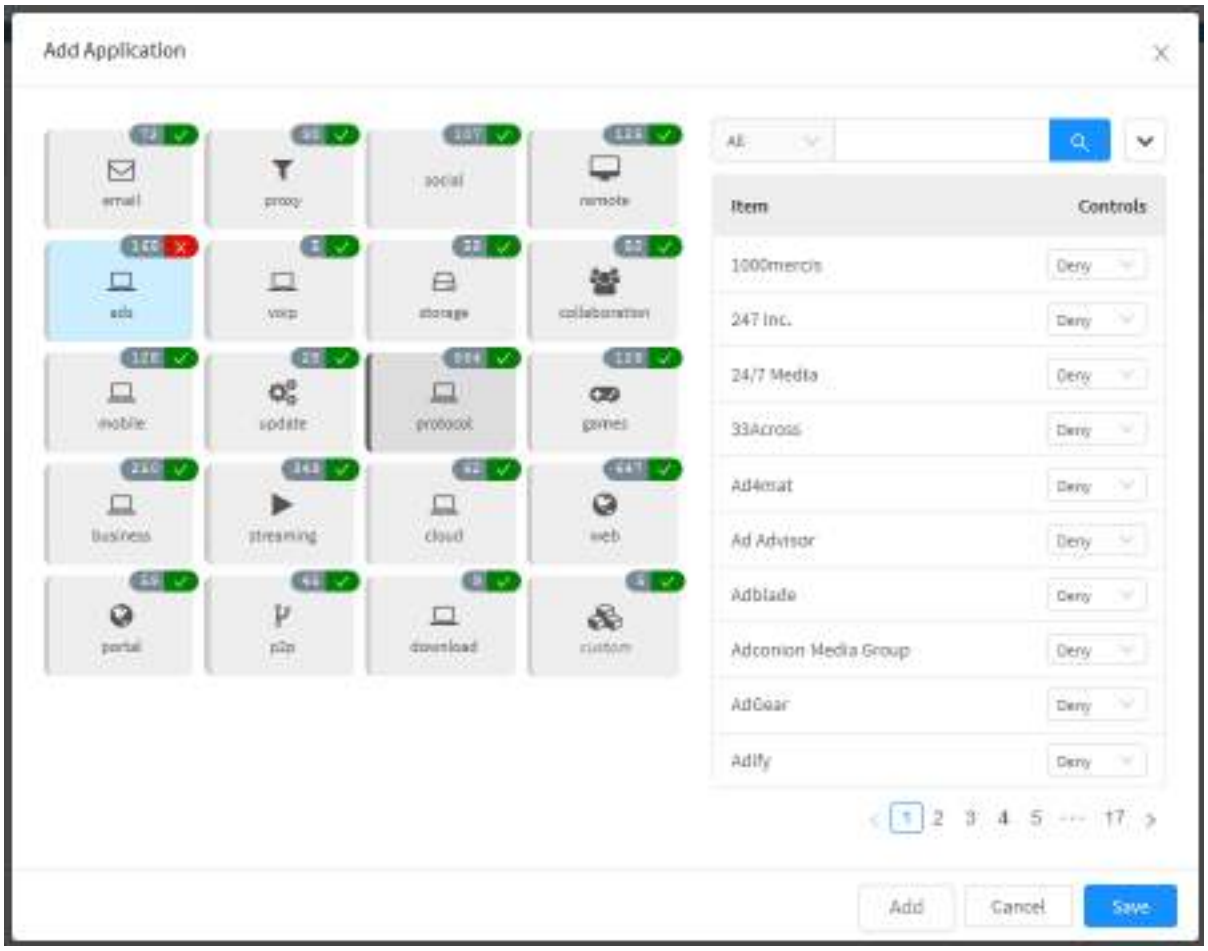
Para mais informações a respeito das categorias utilizadas pelo *Application Control*, consulte esta página.

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:

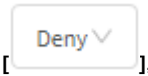
- **Allow:** O acesso às aplicações classificadas com esta categoria é permitido;
- **Block:** O acesso às aplicações classificadas com esta categoria é bloqueado;
- **Disable:** Esta categoria é desabilitada, isso significa que o *Application Control* irá ignorá-la e considerará apenas as aplicações em categorias permitidas ou bloqueadas.

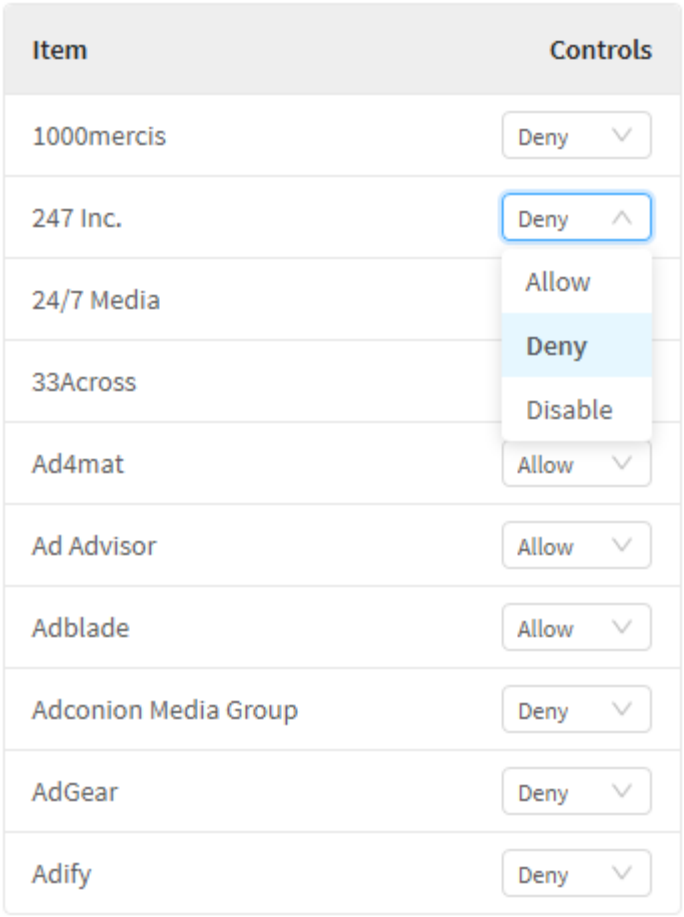
No exemplo abaixo, iremos desabilitar todas as propagandas.

Para tanto, selecione a categoria desejada, neste exemplo, selecionaremos a opção "*ads*":



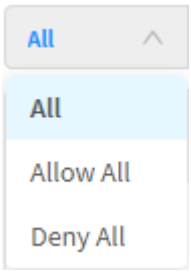
Application Control - Add Application - Opção "*ads*" selecionada

Determine a aplicação desejada e na caixa de seleção, escolha a opção **Deny [**  **]**, conforme exemplificado na imagem abaixo:



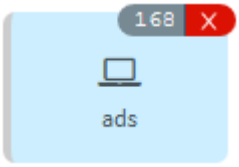
Application Control - Add Application - Itens negados

Caso seja necessário fazer uma configuração em todos os itens de uma categoria, basta selecionar a opção desejada no **menu de ações [ ]** ou na caixa de seleção demonstrada abaixo:



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:



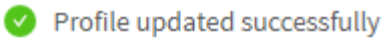
Application Control - Add Application - 7 itens negados e 99 permitidos

Por fim, caso deseje cancelar clique no botão ***Cancel***[Cancel]. Para concluir a edição das aplicações clique no botão ***Save***[Save].

Após, ter efetuado os processos anteriores, um resumo de todas as aplicações permitidas e negadas serão exibidas no campo Applications, conforme exemplificado abaixo:

Application Control - Applications - Applications allowed and denied

Para concluir este processo, basta clicar no botão ***Save***[Save] novamente.



Profile successfully updated

Após salvar, para que as alterações tenham efeito 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.*

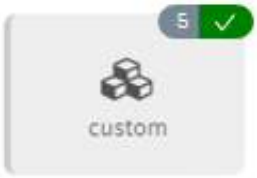
Criar grupo de aplicação customizado

Botão add[ ***]:*** Permite a adição de grupos customizados dinâmicos de aplicações baseados em características. Por exemplo, aplicações do tipo cliente/servidor, baseado em protocolos de rede e outras.

Ao clicar nesta opção, a seguinte tela será apresentada:

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.

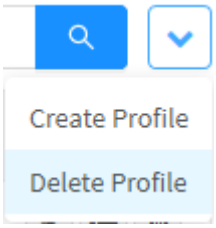
Services - Application Control - Menu de ações - Delete Profile

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;*

Application Control – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete Profile*”.

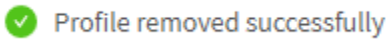


Application Control – Delete Profiles.

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

Application Control – Mensagem se deseja deletar os *Profiles*

Caso desejar cancelar clique no botão ***Cancel*[** Cancel **]**. Para concluir, clique no botão ***Delete*[** Delete **]**.



Profile removed successfully

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

Services - Application Control - Colunas

A seguir explicaremos cada coluna da aba *Application Control*:

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* [ ]:** Permite editar as configurações do *profile* adicionado na opção *Create Profile* do menu de ações;
    - **Botão *Delete* [ ]:** Deleta o *profile*, basicamente é o equivalente a *Delete Profile* do menu de ações.

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.

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
	MAPI
	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
	Issuu
	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

	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

	Aggregate Knowledge
	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

	Doubleclick
	DoubleVerify
	Dynamic Logic
	Effective Measure
	engage BDR
	Ensighten
	EQ Ads
	Evidon
	eXelate
	Exponential Interactive
	eyeReturn
	Federated Media
	Freewheel
	Genieo
	GoDaddy
	Google Adsense
	Greystripe
	iAd
	ICA
	Improve Digital
	Infonline
	InSkin Media
	Integral Ad Science
	Invitemedia
	iPerceptions
	Komli Media
	Krux
	LeadBolt
	Ligatus
	Lijit
	Lotame
	Marketo
	MaxPoint Interactive
	Maxymiser
	MdotM
	Media6Degrees
	Media Innovation Group
	MediaMath
	MediaV
	Microsoft Ads
	Millennial Media

	Mixpanel
	Moat
	Mobile Theory
	Monetate
	Motrixi
	MyBuys
	Neobux
	NetSeer
	Neustar Information Services
	Nexage
	Nielsen
	Nugg
	OpenX
	Optimizely
	OptMD
	OwnerIQ
	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
	HIKE
	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
	CAP

	CBT
	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
	DTK
	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
	FLEXlm
	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

	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
	HAP
	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
	HTTP
	HTTPMGT
	HTTP RPC Ep Map
	HTTPS
	Hybrid Point of Presence

	Hyper-G
	Hyperwave-ISP
	iafdbase
	IAFServer
	IASD
	IATP
	IAX
	IBM App
	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-lm
	Microsoft Global Catalog
	Microsoft Rome
	Microsoft Shuttle
	Microsoft System Center Operations Manager
	mit-ml-dev
	MIT ML Device
	MIT Spooler
	MobileIP
	MobilIP-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
	MTP
	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
	PTP
	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
	TPCP
	TPIP
	TPKT
	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
	Wii Shop Channel
	WLCCP
	World Fusion
	wpgs
	WSDD
	XWindows
	xact-backup
	Xbone
	XDMCP
	Xfer
	XNS
	XNS Authentication
	XNS Clearinghouse
	XNS Time
	XTP
	xvttp
	Xyplex
	Zebra

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

	FOX
	FreeStreams
	G4
	Game Front
	Game Informer
	GameSpot
	GameSpy
	GameStop
	GameTrailers
	Geewa
	GOMTV.net
	GTA Online
	Hangame
	Hattrick
	hi5
	Ifeng.com
	Isoball
	Joystiq
	King.com
	Kongregate
	Kotaku
	League of Legends
	Lineage
	LINE Games
	Magicland
	MapleStory
	Mesmo Games
	Minecraft
	Miniclip
	MyOnlineArcade
	Neopets
	Newgrounds
	Nexon
	NFL.com
	Nintendo
	OnLive
	PartyPoker
	Planetarium
	Playdom
	Playstation.com
	Playstation 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

Category	Application
Streaming	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
Cox
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
	HBO
	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
	Redbox Instant
	Rediff.com
	RedOrbit
	RedTube
	Reuters
	Rhapsody
	Roku
	RTMP
	RuTube
	SBS
	Shockwave
	SHOUTCast Radio
	Showbox
	SHOWTIME ANYTIME
	Silverlight
	Sina Video
	SIP
	sipXecs
	Slacker
	Slate Magazine
	Slingbox
	Slutload
	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

	SURF
	TeacherTube
	Telly
	Tencent Video
	The Atlantic
	The Blaze
	theCHIVE
	The Guardian
	The Internet Archive
	The Week Magazine
	Tianya
	Tidal
	Tightrope Interactive
	TMZ
	TNAFlix
	TopTenREVIEWS
	Toshiba Camera Stream
	Tube8
	Tudou
	TuneIn
	Turntable
	Tu TV
	Tvigle
	TVonline.cc
	TVU Networks
	TwitchTV
	Twitter Video
	UltraViolet
	UOL
	USA Today
	Ustream.tv
	Vdio
	VDOLive
	Veetle
	Veoh
	VEVO.com
	Viddler
	Video Sift
	Videosurf
	Viewsurf
	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
	Zoom

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
	MPM

	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
	BB
	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
	eBay
	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
	Hupu
	iBackup
	ICA Browser
	IFTTT
	iFunny
	IGN
	IloveIM
	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
	Tagoo
	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
	Poco
	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.

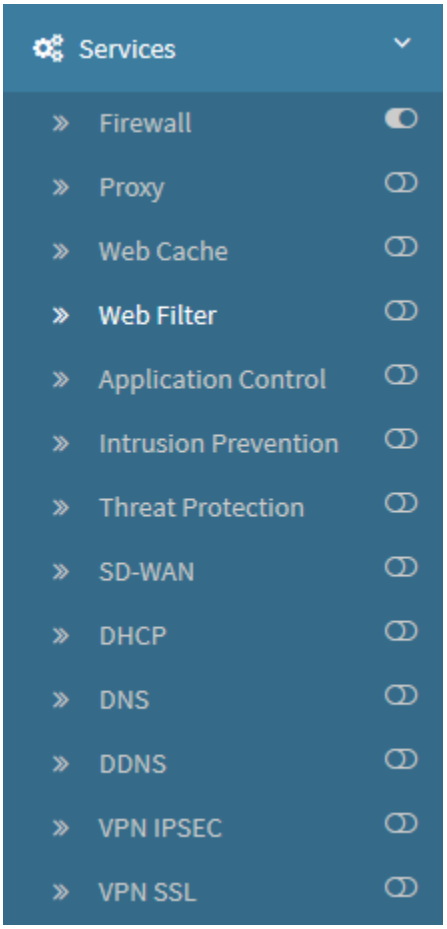
UTM - Services - Web Filter

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 *web*, *“Google, Yahoo e Bing”.*

Para acessar esta tela, basta selecionar a opção “*Web Filter*”.



Services - Web Filter

A tela abaixo será exibida:

Web Filter

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).

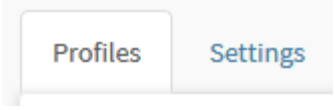
Nos perfis de Filtro de Conteúdo é possível Permitir, Bloquear e Desabilitar as categorias. Uma política que possua Web Filter habilitado leva em consideração apenas os URLs cujas categorias foram permitidas ou bloqueadas no Perfil, se o URL estiver desabilitado, o serviço irá passar para a próxima política 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 nenhuma política		Bloquear acesso

Para mais informações sobre *application control*, consulte esta página.

Caso a aba não esteja selecionada, clique em *"Profiles"*.



Aba *Profiles*

Surgirá a tela "*Profiles*" de *Web Filter*, conforme demonstrado pela imagem abaixo:

Web Filter - Profiles

Esta sessão irá abordar como cadastrar, editar e remover os perfis de *Web Filter*;

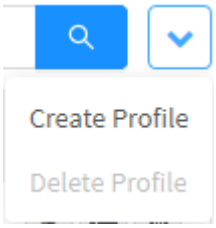
A seguir, analisaremos as funções localizadas no topo deste painel.

Web Filter - Profiles - Menu de Ações

No topo direito da tela temos o menu de ações:

Web Filter – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Web Filter – Menu de Ações

O menu é composto das seguintes opções:

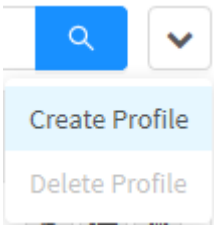
- *Create Profile*;
- *Delete Profile*.

A seguir cada opção do menu de ações será detalhada.

Web Filter - Profiles - Menu de Ações - Create Profile

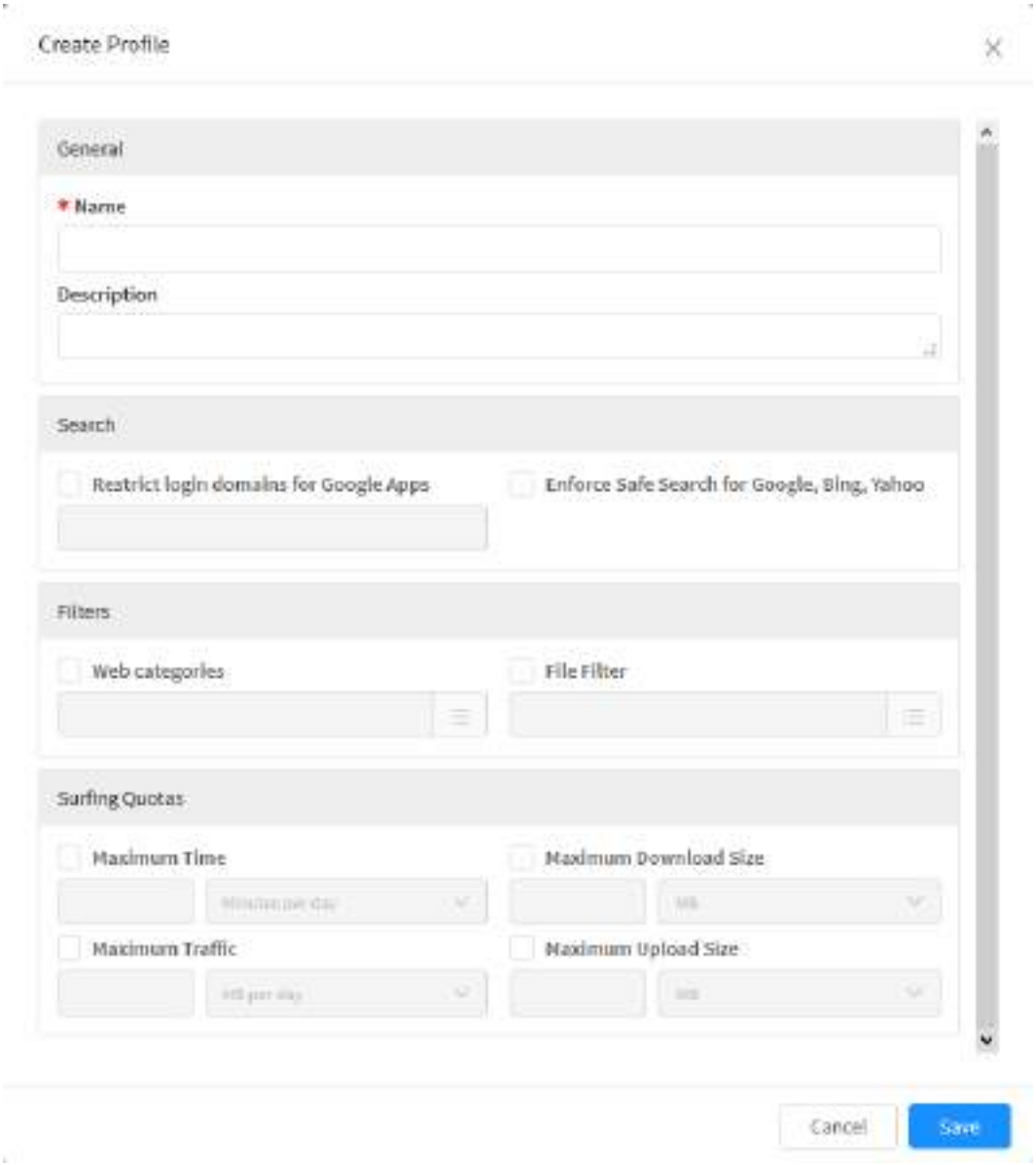
Através da opção “*Create Profile*” é possível criar um novo perfil de *Web Filter*. Para acessar, clique no **menu de ações [ ]**.

1. Clique na opção “*Create Profile*”;



Web Filter - Create Profile

2. A tela “*Create Profile*” será exibida. Conforme demonstrado pela imagem abaixo:



Create Profile

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

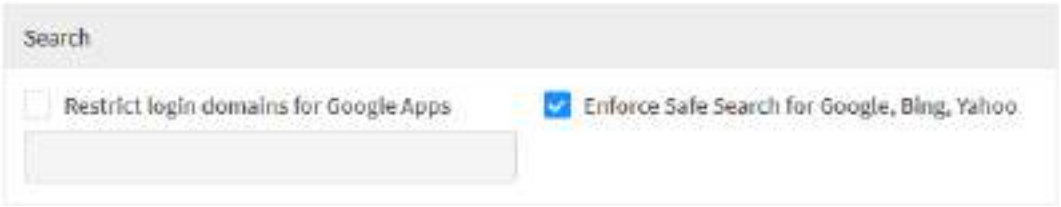
Em "*General*" temos as seguintes caixas de texto:

Web Filter – General

- ***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:

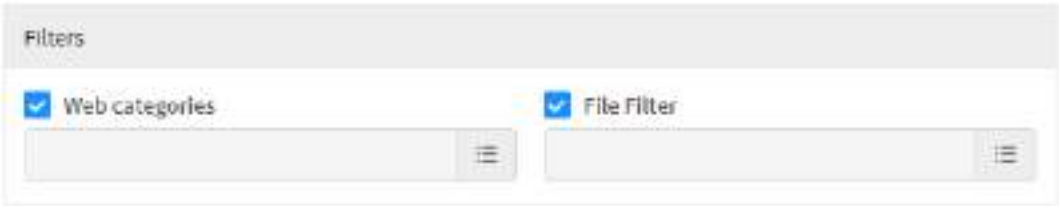


Web Filter - Search

- ***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[ ]*:** Esta caixa de checagem força a ativação do *Safe Search* nos mecanismos de busca. O UTM possui suporte aos filtros *Safe 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:

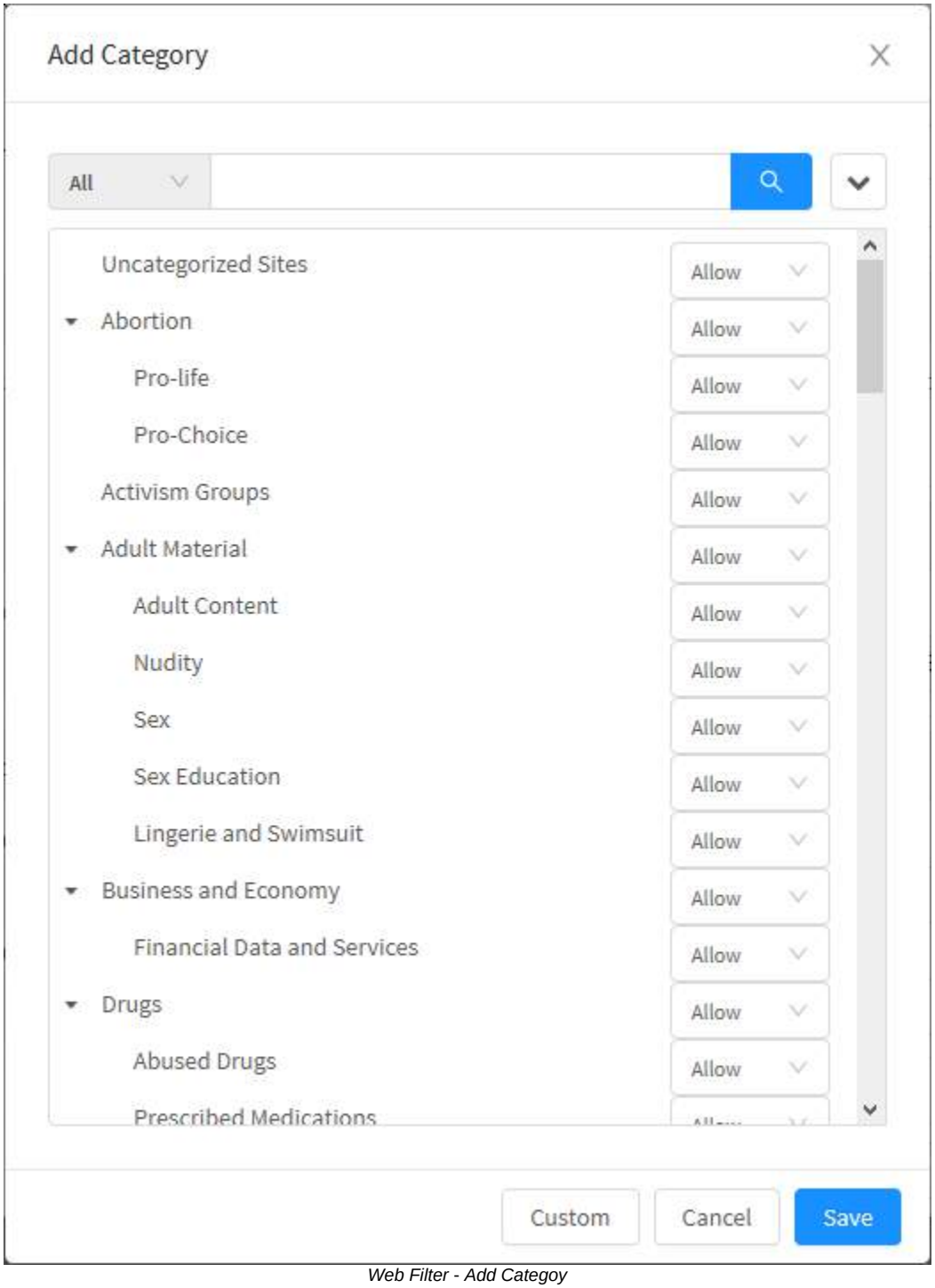


Web Filter - Filters

- ***Web categories [ ]:*** Permite selecionar as categorias *Web* para aplicar filtros de "Bloqueio" ou "Exceção" ao conjunto de políticas aplicadas. Para selecionar as categorias, clique no botão ***[ ]***, 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:

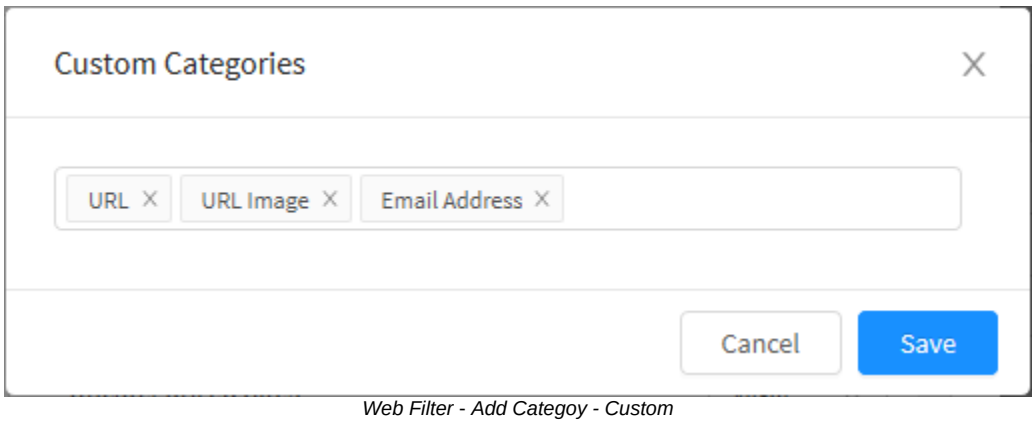
- **Allow:** O acesso a *URLs* classificadas com esta categoria é permitido;
- **Block:** O acesso a *URLs* classificadas com esta categoria é bloqueado;
- **Disable:** Esta categoria é desabilitada, isso significa que o *Web Filter* irá ignorá-la e considerará apenas as *URLs* em categorias permitidas ou bloqueadas.



Web Filter - Add Categoy

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 **]**;



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 adicionados como tags. Por fim, clique no botão ***Cancel*[** Cancel **]** para sair dessa janela ou clique no botão ***Save*[** Save **]** para salvar.

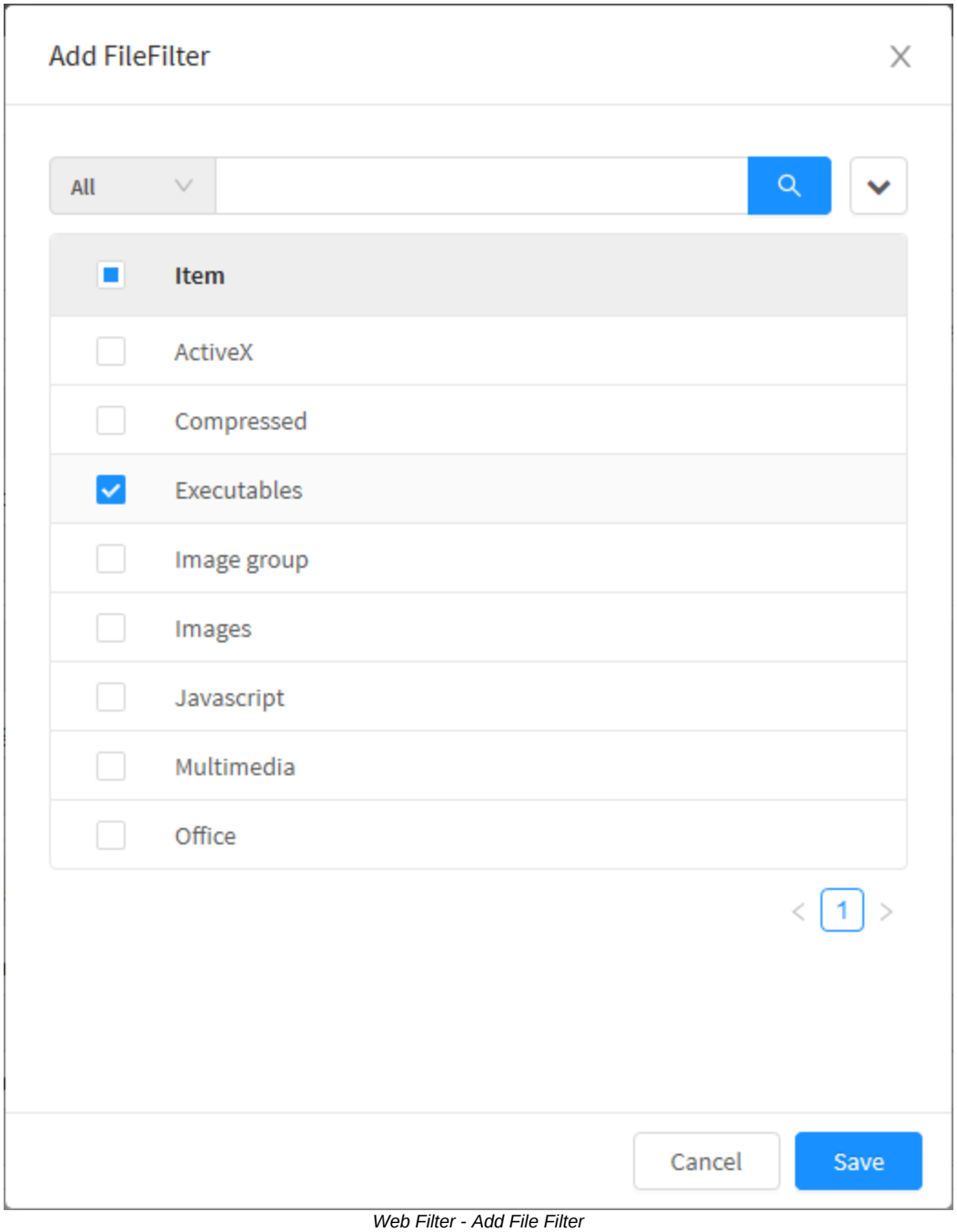
Para finalizar a adição das categorias, clique no botão ***Save*[** Save **]** para salvar ou clique no botão ***Cancel*[** Cancel **]** para sair desta janela.

- ***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.



Web Filter - Add File Filter

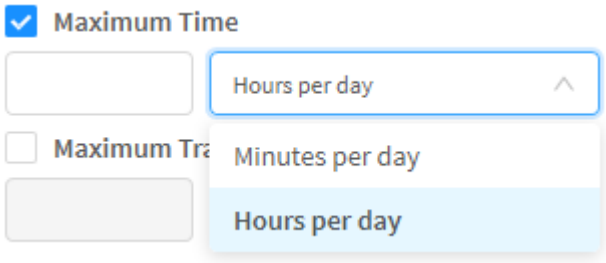
Clique no botão ***Cancel***[Cancel] para Cancelar. Clique no botão ***Save***[Save] para salvar.

Surfing Quotas

Em "*Surfing Quotas*" o seguinte painel é exibido:

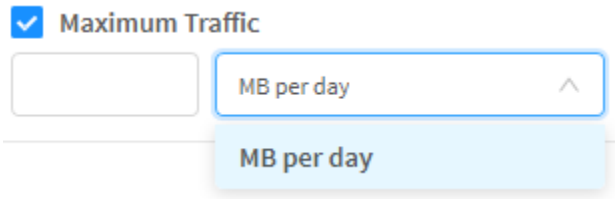
Web Filter - Surfing Quotas

- [☑] ***Maximum Time*:** Permite configurar uma quota de tempo em minutos ou horas por dia.



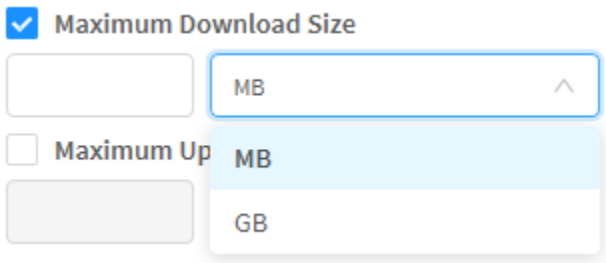
Web Filter – Maximum Time

- [☑] ***Maximum Traffic*:** Permite configurar uma quota de tráfego em MB por dia.



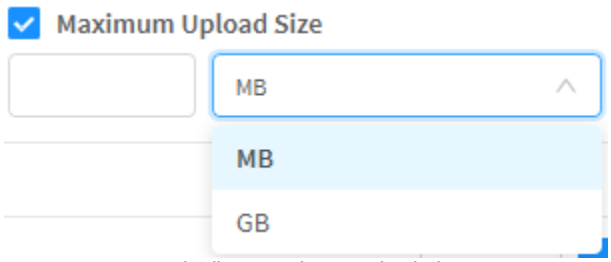
Web Filter – Maximum Traffic

- [☑] ***Max Download Size*:** Permite configurar o tamanho máximo para *download*, em MB ou GB.



Web Filter - Maximum Download Size

- [☑] ***Max Upload Size*:** Permite configurar o tamanho máximo para *upload*, em MB ou GB.



Web Filter - Maximum Upload Size

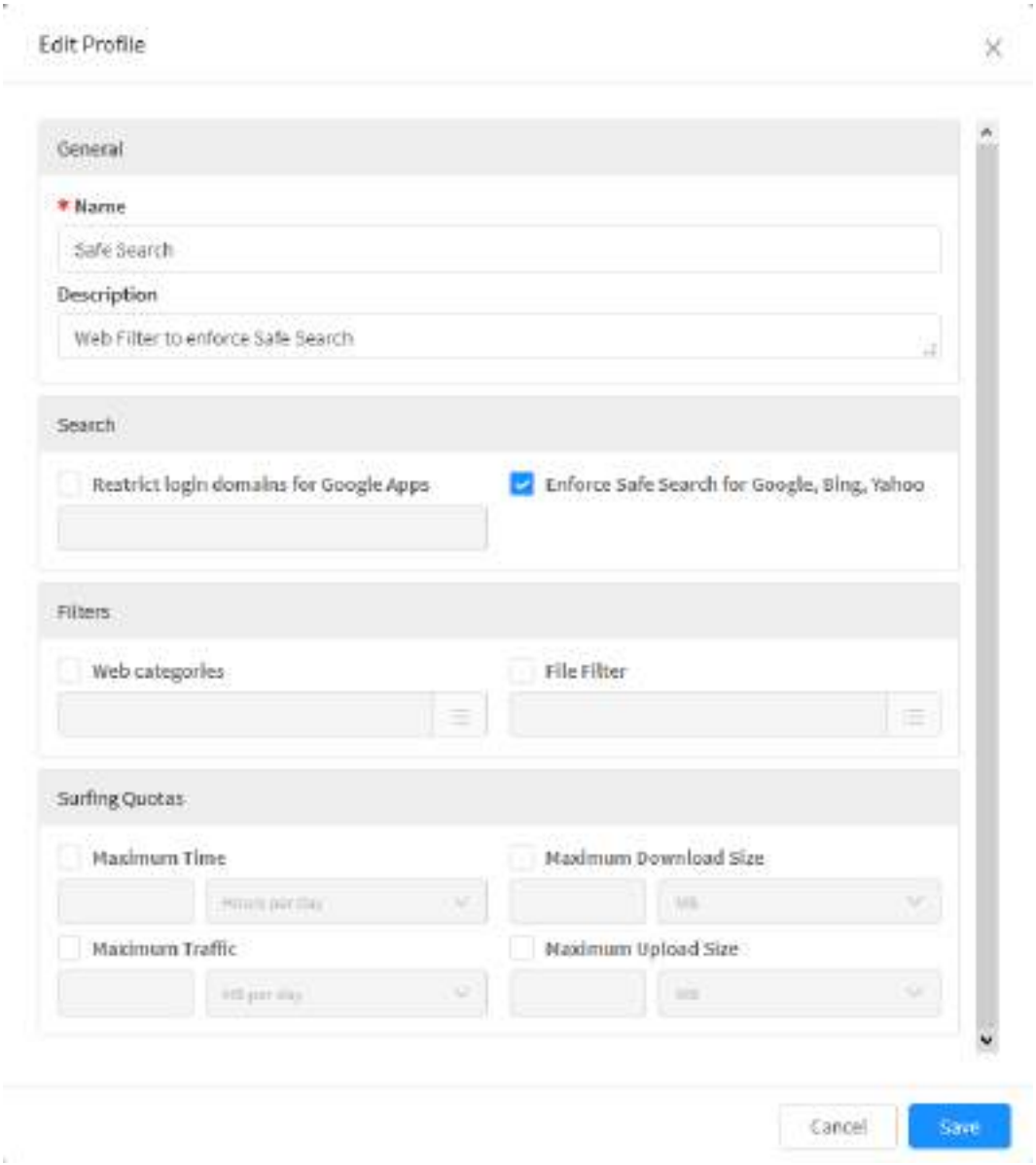
As configurações efetuadas no perfil podem ser adicionadas a uma política na aba *Inspection* na opção *Web Filter*.

Após finalizar todas as configurações, clique no botão ***Cancel***[Cancel] para voltar para o painel *Profiles* ou clique no botão ***Save***[Save] para salvar.

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*.

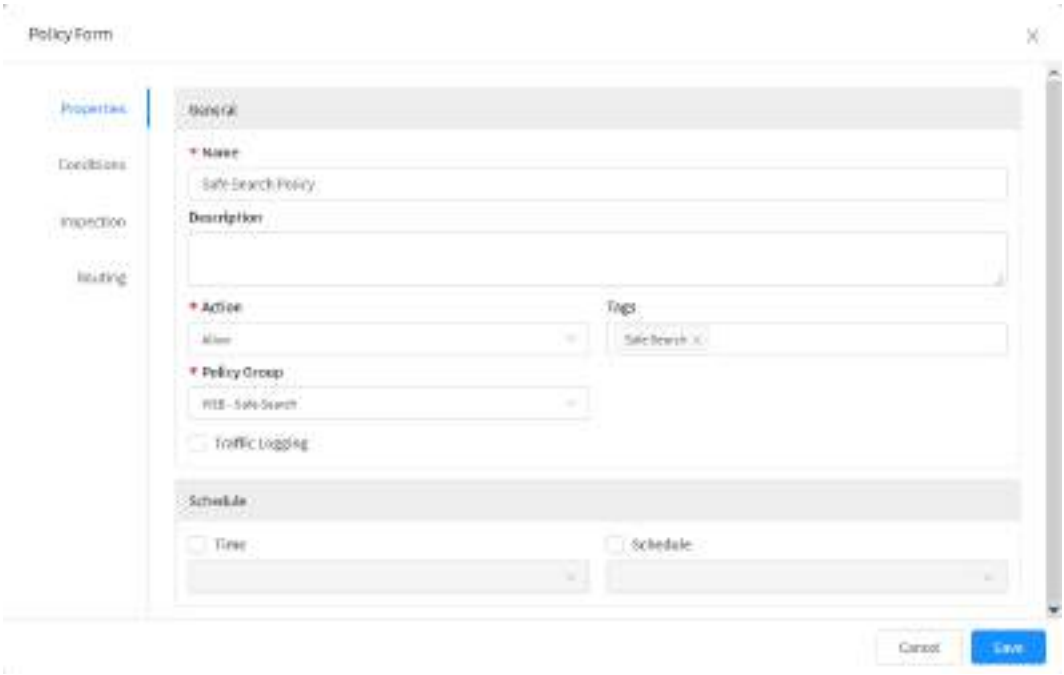


Web Filter - Safe Search

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.

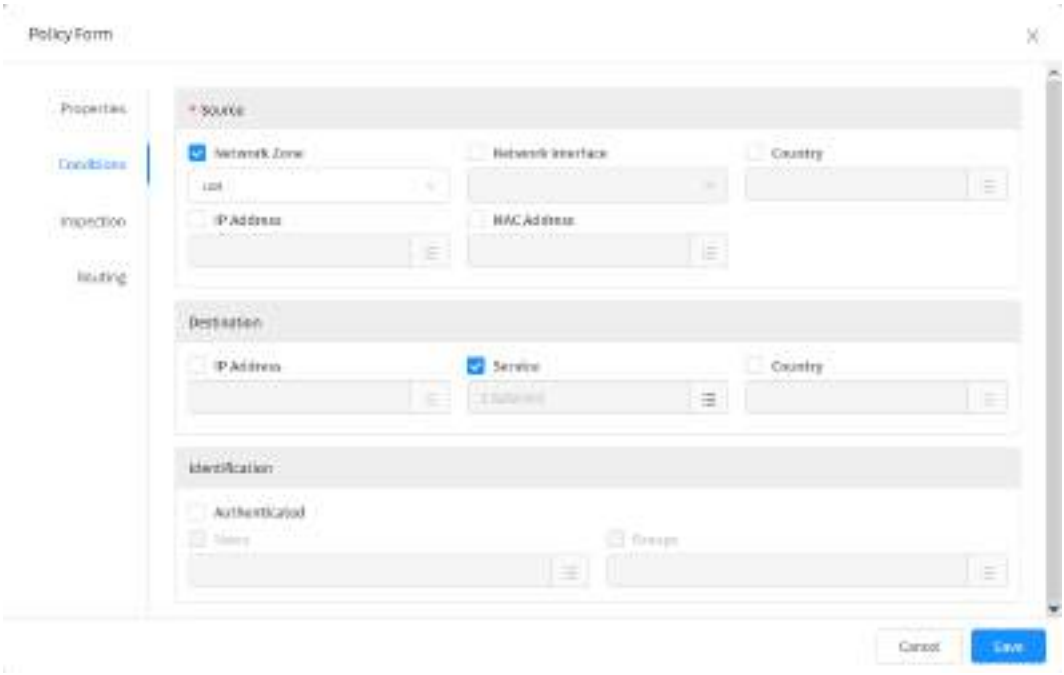


Web Filter - Policy - Properties

Na aba *Properties:*

- ***Name:*** *Safe Search Policy;*
- ***Action:*** *Allow;*
- ***Policy Group:*** *WEB - Safe Search;*
- ***Tags:*** *Safe Search.*

A seguir acesse a aba *Conditions:*

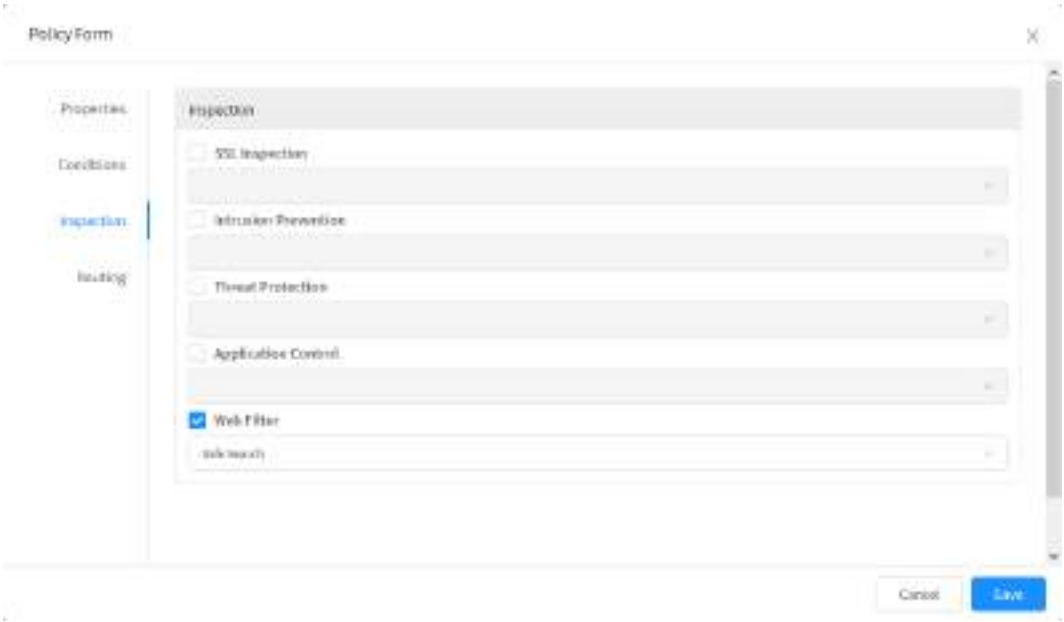


Web Filter - Policy - Conditions

Na aba *Conditions:*

- ***Network Zone[ ]:*** *LAN;*
- ***Service[ ]:*** *HTTP* e *HTTPS.*

A seguir acesse a aba *Inspection:*



Web Filter - Policy - Inspection

Na aba *Inspection:*

- ***Web Filter[ ]:*** *Safe Search* (ou o nome do *Web Filter* criado logo no início).

Você terá chego no resultado demonstrado abaixo:

Política *WEB - Safe Search*

Ao finalizar este passo o *Safe Search* entrará em vigor.

Para funcionamento correto no navegador Google Chrome e para efetuar uma pesquisa segura no Google, será necessário bloquear a porta 443 UDP, pois o Proxy só consegue fazer essa inspeção SSL no tráfego TCP.

Web UDP 443 Block

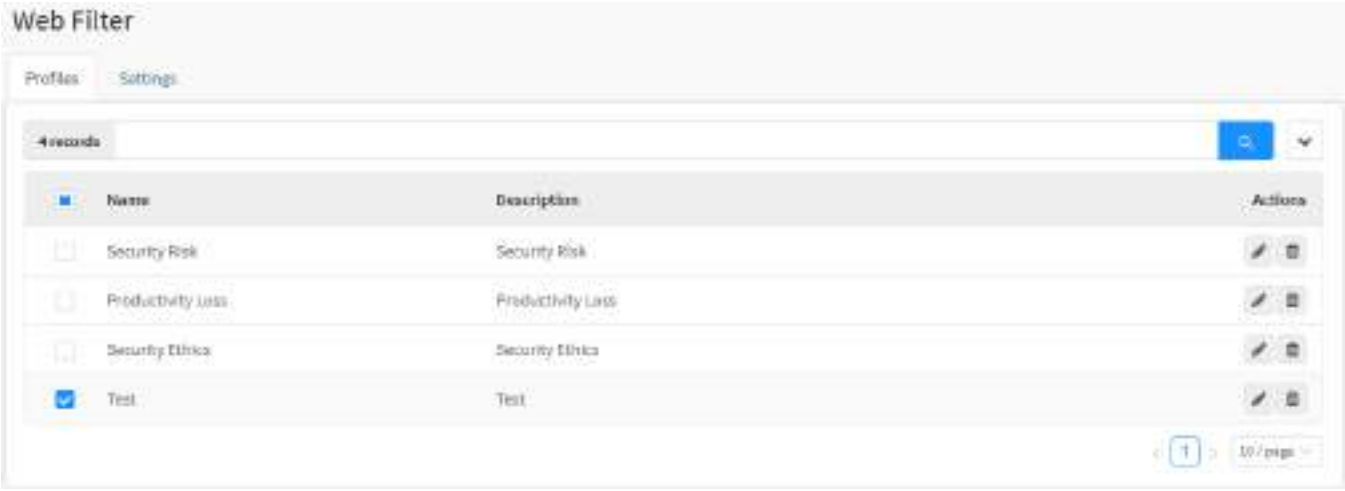
Para mais informações, a respeito de políticas, vide o capítulo Policy.

À seguir, detalharemos como remover um perfil de Web Filter.

Web Filter - Profiles - Menu de Ações - Delete Profile

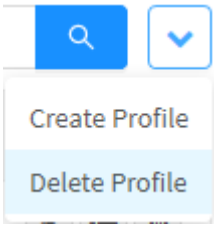
Através do botão “*Delete Profile*” é possível deletar os *Profiles* selecionados. Para deletar pelo Menu de ações, siga os seguintes passos:

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*;



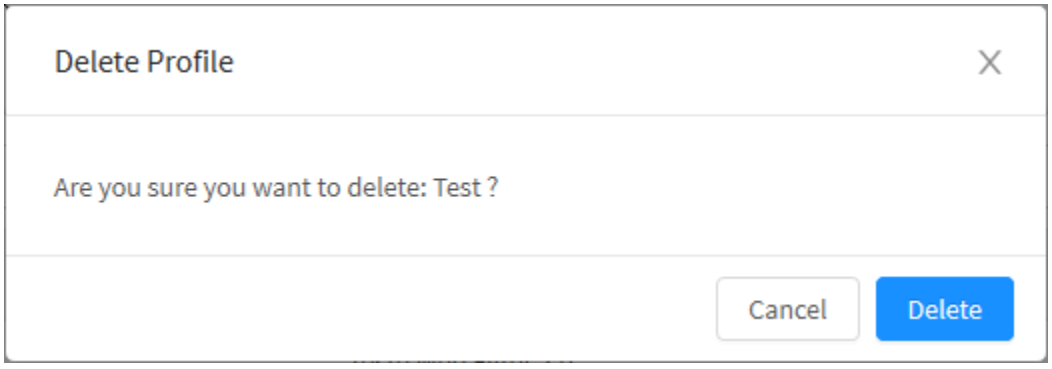
Web Filter – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete Profile*”.



Web Filter – Delete Profiles

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



Web Filter – Mensagem de deleção do *Profile*

Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].

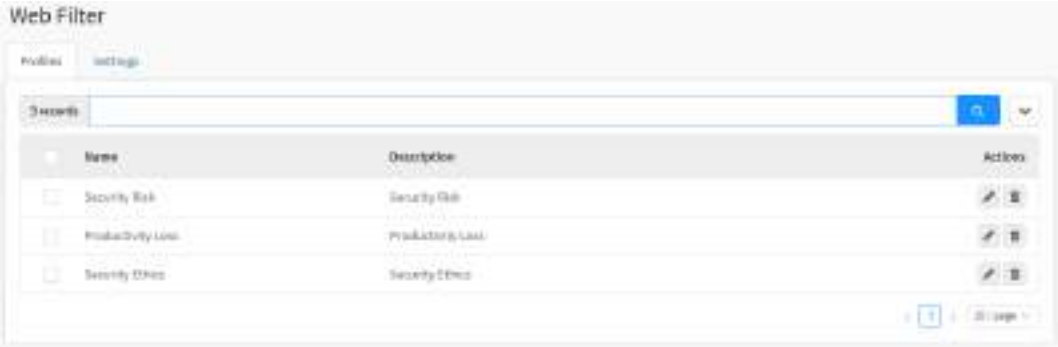
Profile deleted successfully

Após realizar esses procedimentos, os p*rofiles* 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*:



Profiles – *Web Filter*

A seguir explicaremos cada coluna:

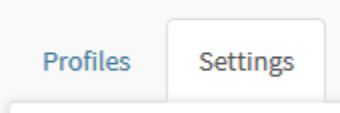
- **Caixa de Seleção[ ]:** Seleciona o *profile;*
- ***Name*:** Apresenta o nome do *profile* cadastrado;
- ***Description*:** Apresenta a descrição do *profile* cadastrado;
- ***Actions*:** A coluna “Actions” é composta pelos botões:
  - **Botão *Edit* [ ]:** Permite editar as configurações do *profile* adicionado na opção *Create Profile* do menu de ações;
  - **Botão *Delete* [ ]:** Deleta o *profile*, é equivalente a opção *Delete Profile* do menu de ações.

À seguir iremos analisar o conteúdo da aba *Settings*.

Web Filter - Settings

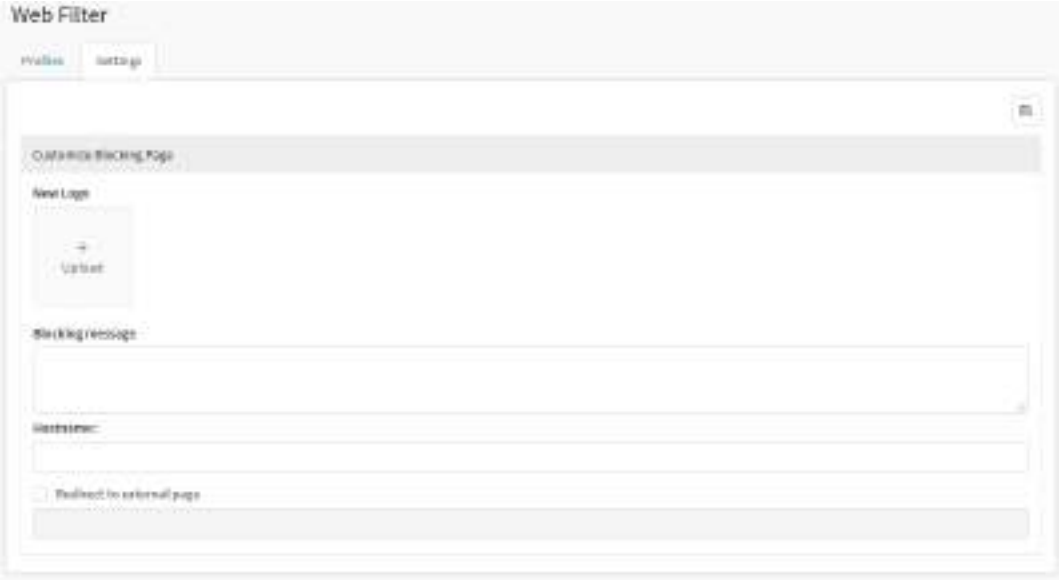
Este item permite customizar a página de bloqueio que é devolvida aos usuários da rede referente aos acessos *"Não Autorizados"* do tráfego *Web* (interceptados pelo *proxy*).

Para configurar a página de bloqueio, clique em *"Settings"*.



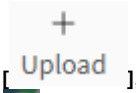
Aba *Settings*

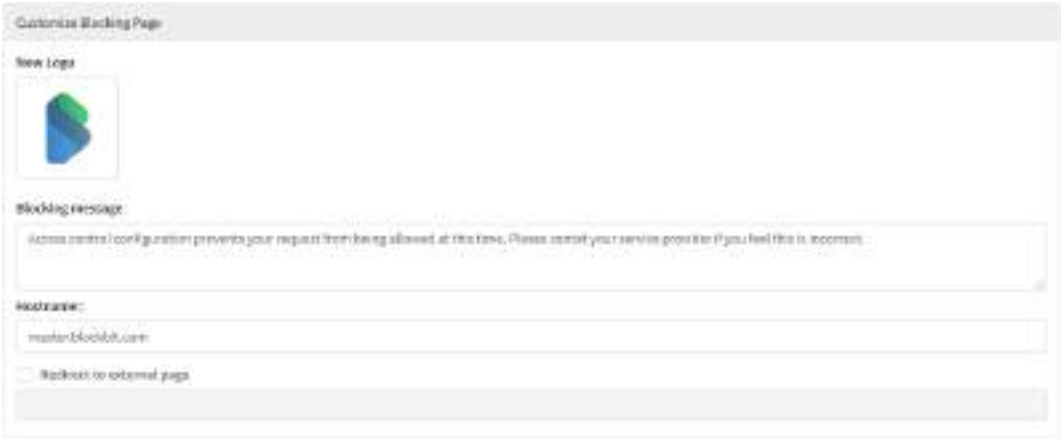
Surgirá o painel "*Customize Blocking Page*", conforme demonstrado pela imagem abaixo:



Web Filter - Settings

É possível alterar o "Logo" e redefinir a "Mensagem de bloqueio":

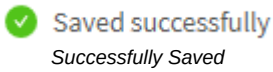
- ***New* logo:** É possível selecionar um novo logo para tela de bloqueio. Para fazer upload de uma imagem, basta clicar em ***Upload*** **[**  **]**, após carregar a imagem, para visualizá-la, clique em ***Preview File*** **[**  **]** por fim, caso deseje removê-la clique em ***Remove File*** **[**  **]**;
- ***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.



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 “Bloqueio” selecionada, o sistema retornará a tela de “Bloqueio”, com a mensagem especificada nas configurações acima.

Para salvar todas as alterações, clique em **[** **]**.



Successfully Saved

Após salvar, para que as configurações entrem em vigor 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.

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.

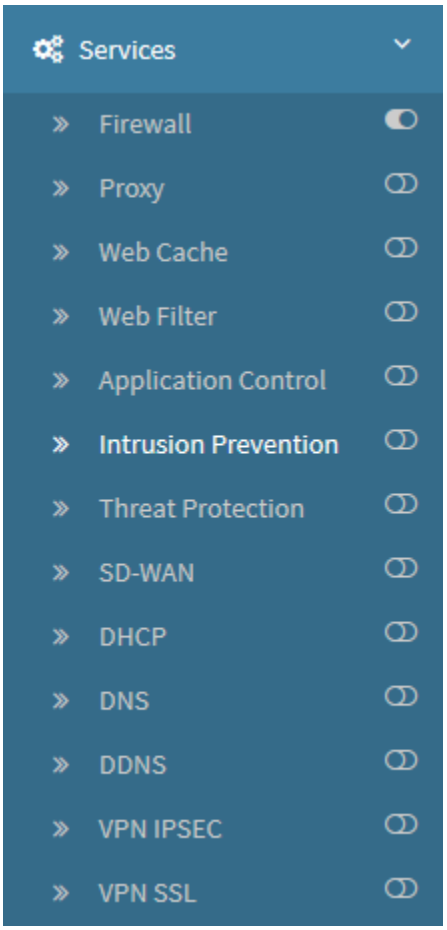
Baseado em assinaturas, regras e sensores ele compara e analisa o conteúdo de todo tráfego Inbound/Outbound “Redirecionado” através de mecanismos de detecção: assinaturas, anomalias de protocolos, controle de aplicações e gera os registros de todos os pacotes identificados na sua base de assinaturas, 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*”.



Services - Intrusion Prevetion

A tela abaixo será exibida:

Intrusion Prevention

A tela *Intrusion Prevention* comporta as seguintes abas:

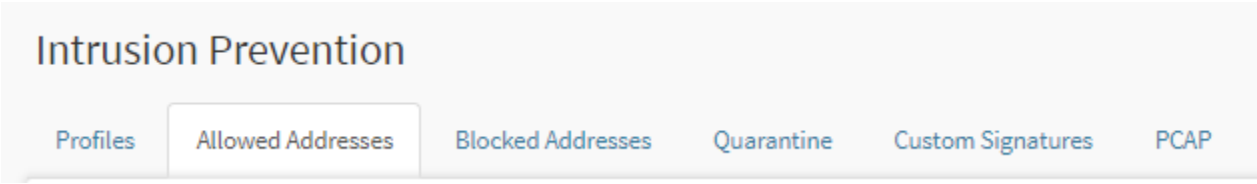
- *Profiles*;
- *Allowed Addresses List*;
- *Blocked Addresses List*;
- *Quarantine*;
- *Custom Signatures*;
- *PCAP*.

A seguir analisaremos os componentes da aba *Profiles*.

Intrusion Prevention - Aba Allowed Addresses

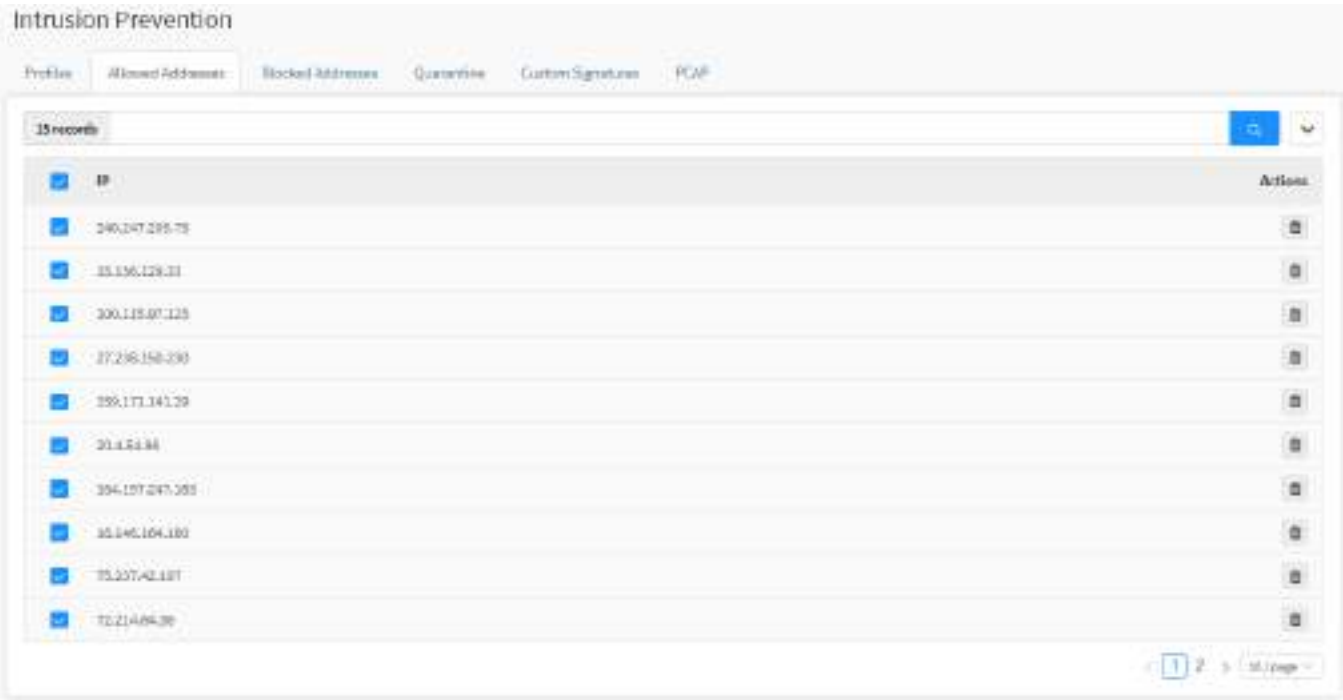
Na aba *Allowed Addresses* é possível cadastrar endereços *IP* tanto de origem como destino ou até mesmo importar uma lista de endereços *IP* para serem considerados confiáveis e darem um *bypass* nas assinaturas do *Intrusion Prevention.*

Caso a aba não esteja selecionada, clique em *"Allowed Addresses".*



Aba *Allowed Addresses*

Surgirá a tela "*Allowed Addresses*" do *Intrusion Prevention*, conforme demonstrado pela imagem abaixo:



Intrusion Prevention - Allowed Addresses

Esta sessão irá abordar como cadastrar, editar e remover os *IPs* de *Allowed Addresses* do *Intrusion Prevention*;

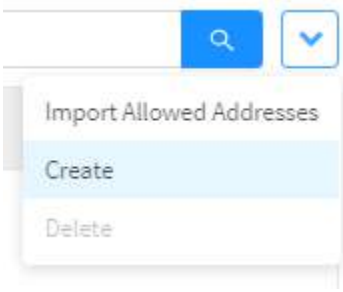
A seguir, analisaremos as funções localizadas no topo deste painel.

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:

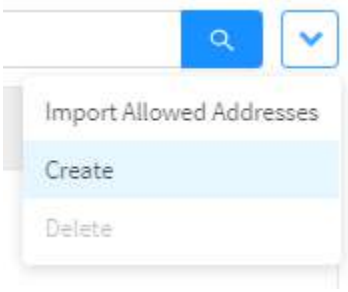
- *Import Allowed Addresses*;
- *Create*;
- *Delete*.

A seguir cada opção do menu de ações será detalhada.

Allowed Addresses - Menu de Ações - Create

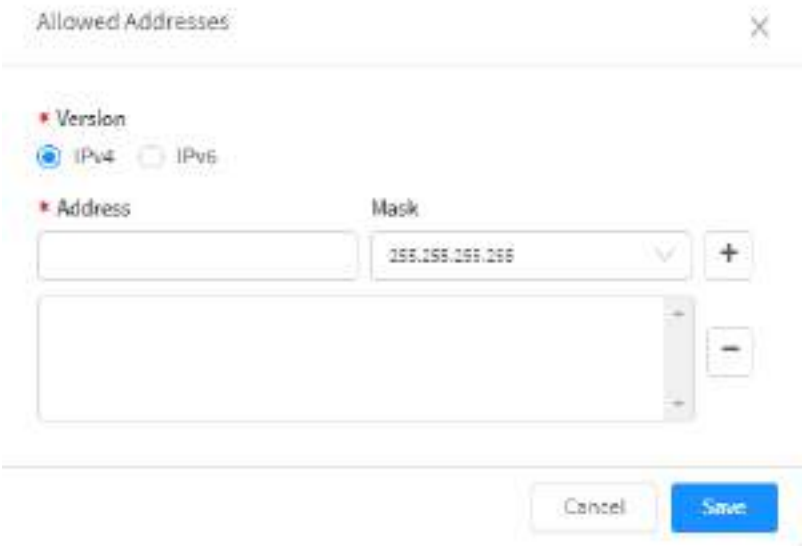
Através da opção “*Create*” é possível criar uma lista de *IPs*. Para acessar, clique no **menu de ações [ ]**.

1. Clique na opção “*Create Profile*”;



Allowed Addresses - Menu de Ações - *Create*

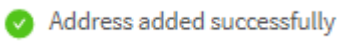
2. A tela “*Allowed Addresses*” será exibida. Conforme demonstrado na imagem abaixo:



Allowed Addresses - Import Allowed Addresses list

- ***Version*:** Determina entre *IPv4* e *IPv6*, qual será utilizado na *Allowed Addresses list*;
- ***Address*:** Neste campo, deve-se digitar o endereço *IP* que será adicionado na *Allowed Addresses list*;
- ***Mask*:** Neste campo, digite a máscara de rede*;*
- ***List*:** Clique no botão **[ ]**, caso pretenda remover um IP da lista clique em **[ ]**.

Caso deseje cancelar clique no botão ***Cancel*[ ]**. Para concluir a adição clique no botão ***Save*[ ]**.



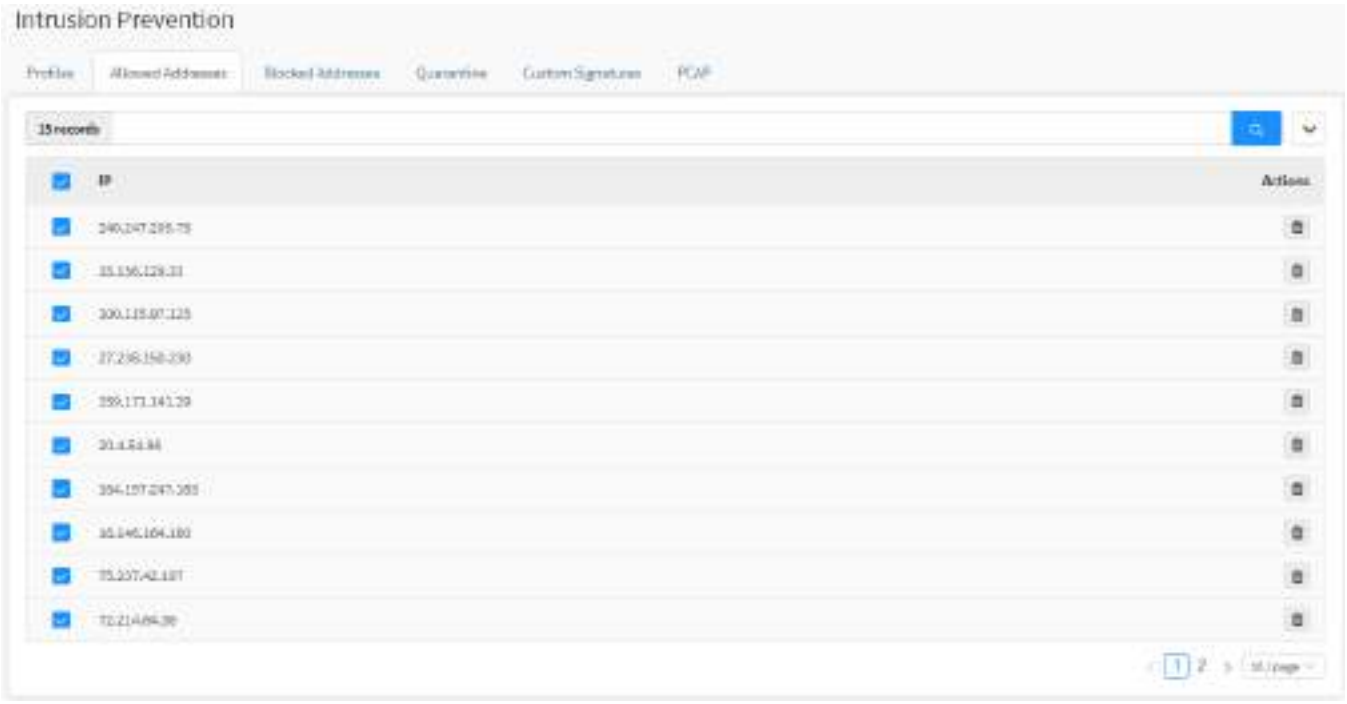
Address successfully added

As configurações foram feitas com sucesso.

Allowed Addresses - Menu de Ações - Delete

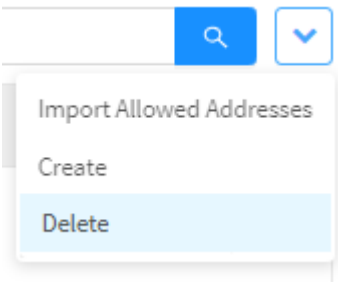
Através do botão “*Delete*” é possível deletar os *IPs* selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

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 **[ ]**:



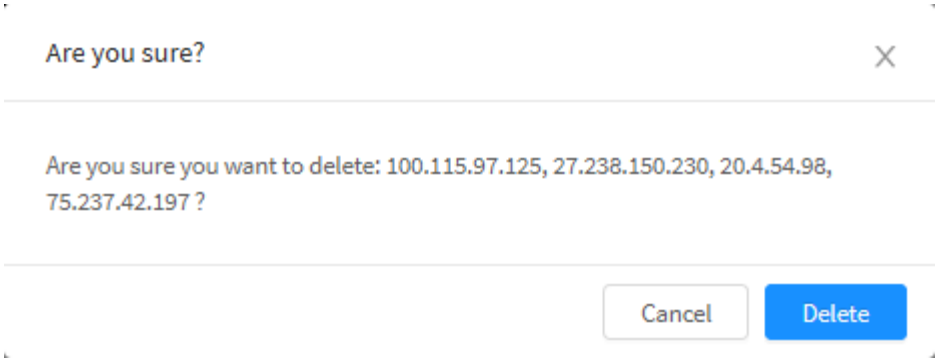
Allowed Addresses - Seleção dos *IPs* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete Profile*”.



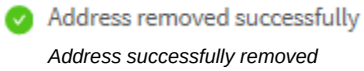
Allowed Addresses – Delete Profile

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



Allowed Addresses – Mensagem confirmando a exclusão de perfil

Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].



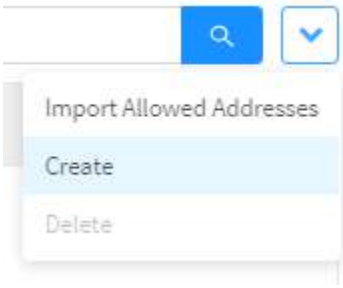
Address successfully removed

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

Allowed Addresses - Menu de Ações - Import Allowed Addresses list

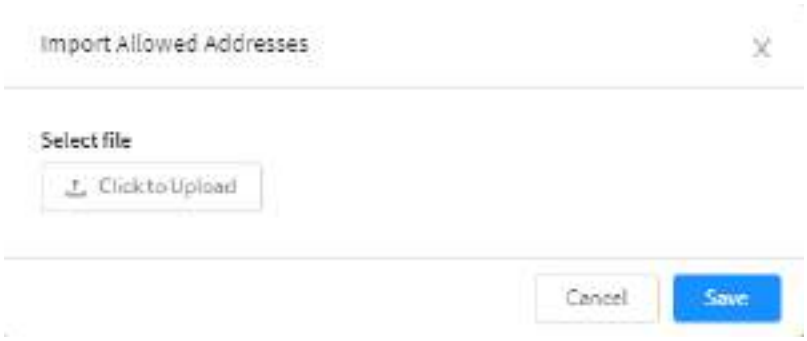
Através da opção "*Import Allowed Addresses*" é possível importar uma *Allowed Addresses list pré-criada para o UTM*. Para acessar, clique no **menu de ações [ ]**.

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:

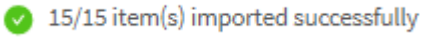


Allowed Addresses - Import Allowed Addresses list

3. Selecione o arquivo desejado clicando no botão **[** Click to Upload **]**.

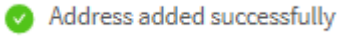
Este botão aceita arquivos de extensão .txt

4. Ao carregar o arquivo com sucesso, uma mensagem de confirmação será exibida:



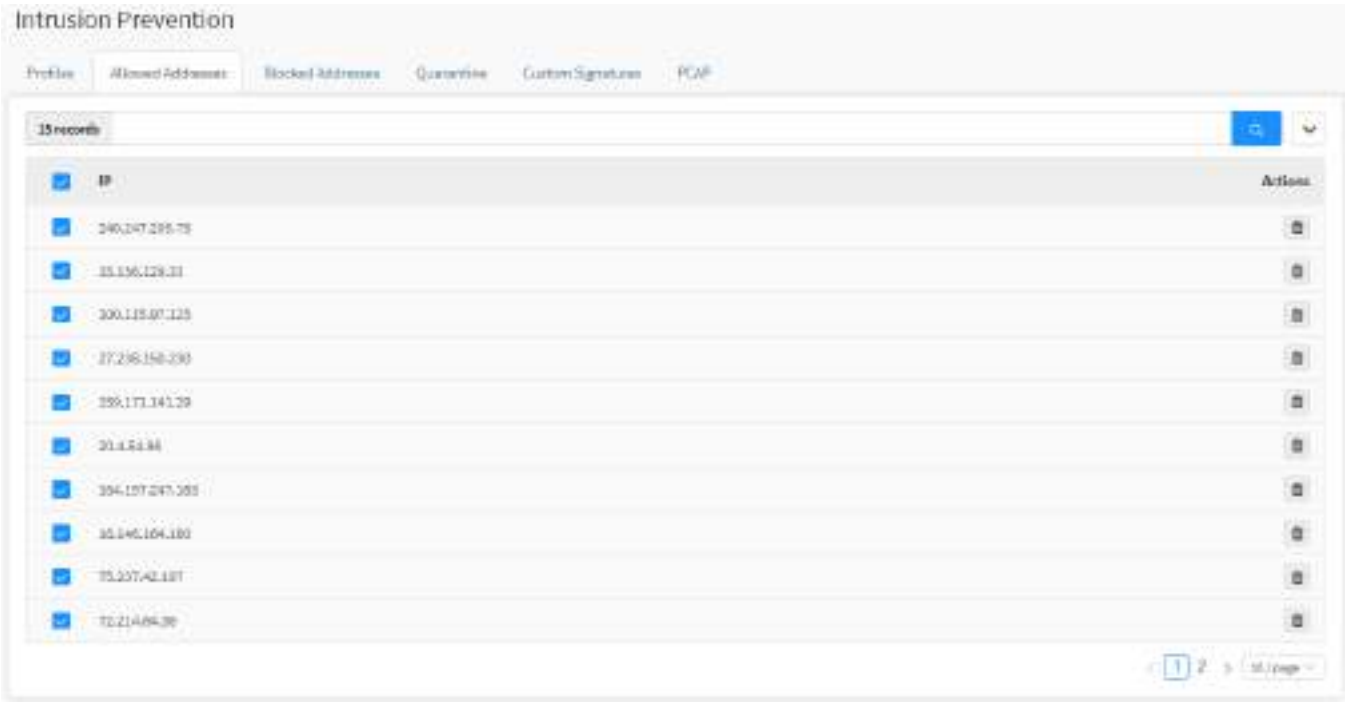
Item(s) successfully imported

5. Ao finalizar a adição dos itens, a seguinte mensagem de confirmação será exibida:



Address successfully added

6. Por fim, a tela exibirá todos os *IPs* adicionados:



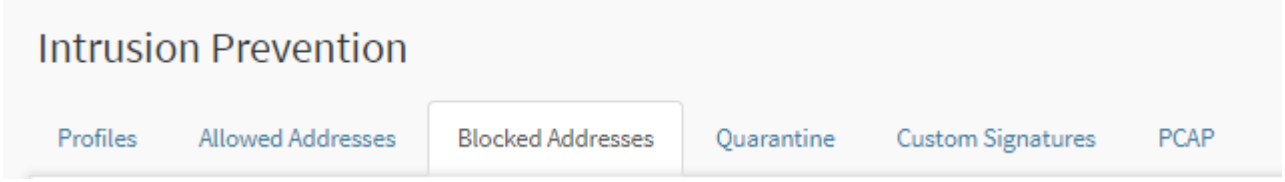
Allowed Addresses - IPs adicionados

Após realizar esses procedimentos, a importação terá sido efetuada com sucesso.

Intrusion Prevention - Aba Blocked Addresses list

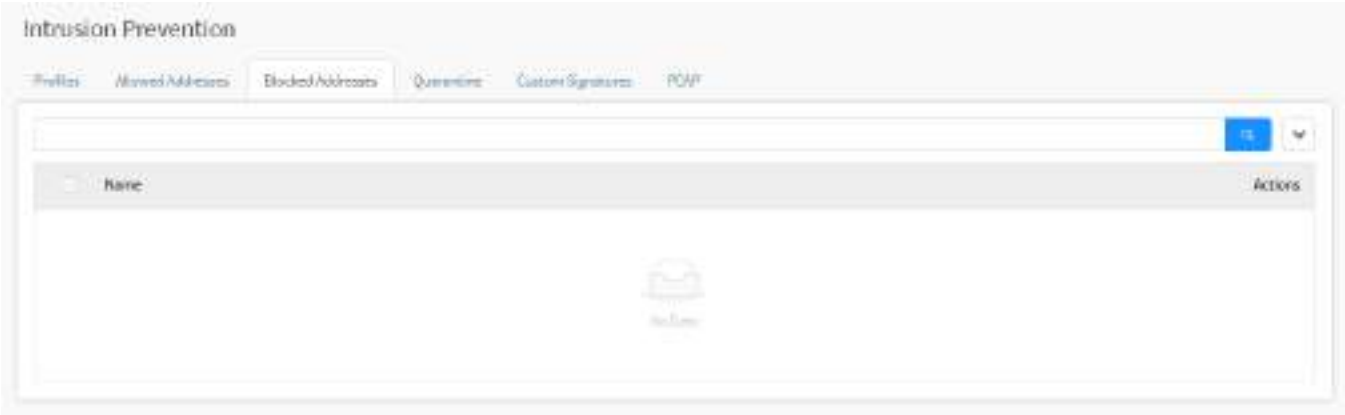
Nesta aba é possível administrar a lista de IPs suspeitos que o *Intrusion Prevention* utilizará.

Para efetuar as configurações, clique em *"Blocked Addresses"*.



Aba *Blocked Addresses*

Surgirá a tela "*Blocked Addresses*" do *Intrusion Prevention*, conforme demonstrado pela imagem abaixo:



Intrusion Prevention - Blocked Addresses list

Esta sessão irá abordar como cadastrar, editar e remover os *IPs* de *Blocked Addresses List* do *Intrusion Prevention*;

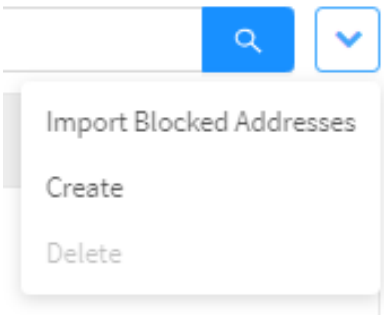
A seguir, analisaremos as funções localizadas no topo deste painel.

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:

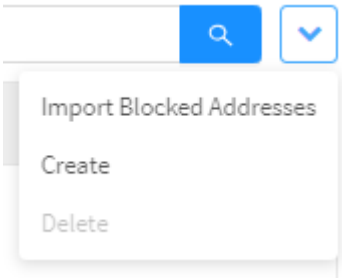
- *Import Blocked Addresses*;
- *Create*;
- *Delete*.

A seguir cada opção do menu de ações será detalhada.

Blocked Addresses - Menu de Ações - Create

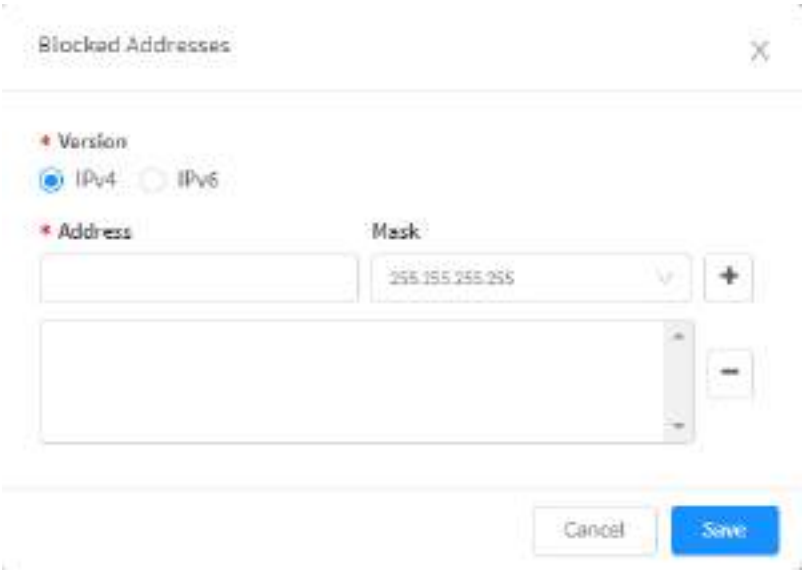
Através da opção “*Create*” é possível criar uma lista de *IPs*. Para acessar, clique no **menu de ações [ ]**.

1. Clique na opção “*Create*”;



Blocked Addresses - Menu de Ações - *Create*

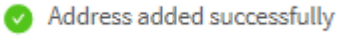
2. A tela “*Blocked Addresses*” será exibida. Conforme demonstrado na imagem abaixo:



Blocked Addresses - Create Blocked Addresses list

- ***Version*:** Determina entre *IPv4* e *IPv6*, qual será utilizado na *Blocked Addresses list*;
- ***Address*:** Neste campo, deve-se digitar o endereço *IP* que será adicionado na *Blocked Addresses list*;
- ***Mask*:** Neste campo, digite a máscara de rede*;*
- ***List*:** Clique no botão **[ ]**, para remover um *IP* da lista clique em **[ ]**.

Caso deseje cancelar clique no botão ***Cancel***[Cancel]. Para concluir a adição clique no botão ***Save***[Save].



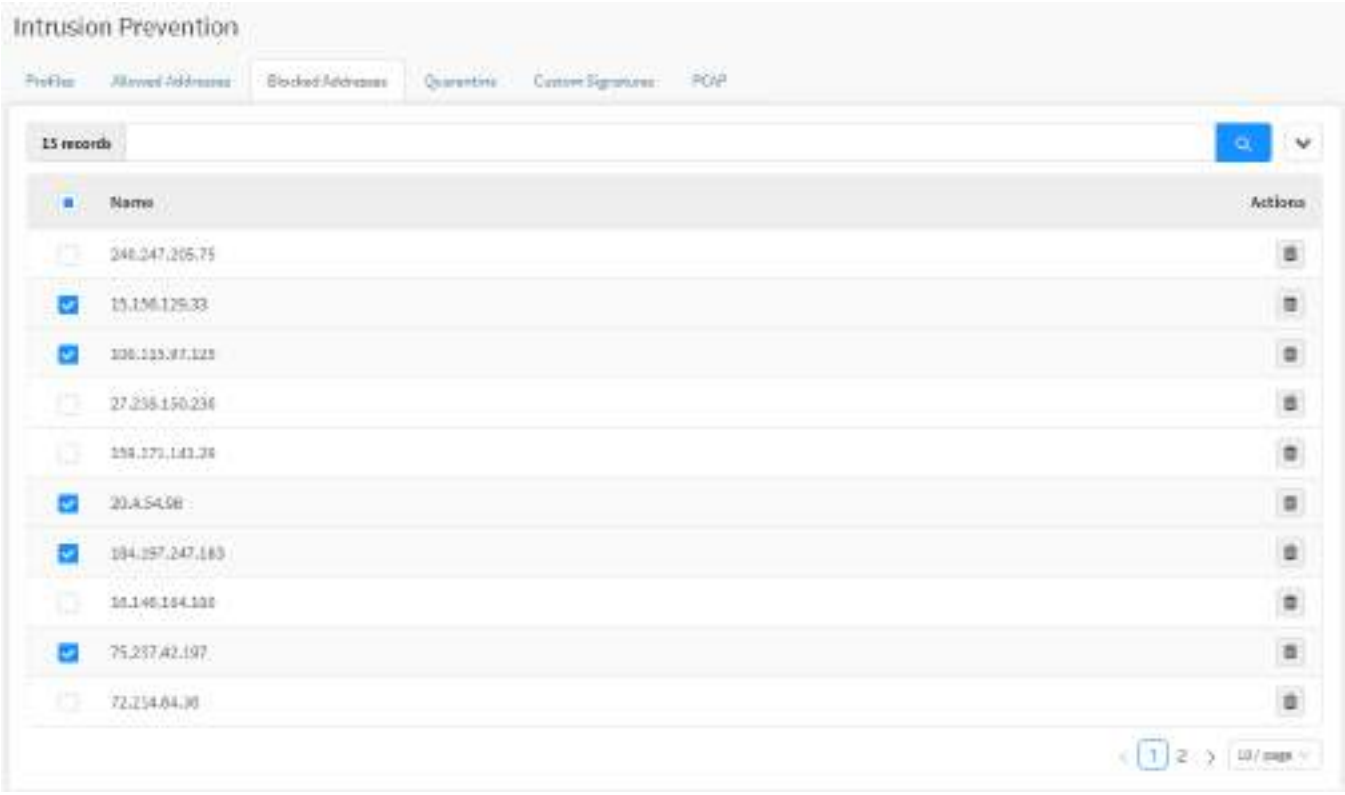
Address successfully added

As configurações foram feitas com sucesso.

Blocked Addresses - Menu de Ações - Delete

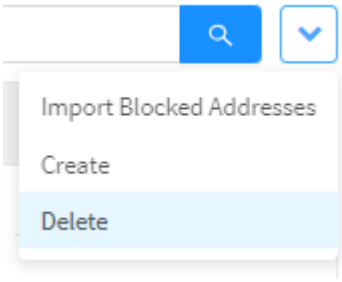
Através do botão “*Delete*” é possível deletar os *IPs* selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

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 **[ ]**.



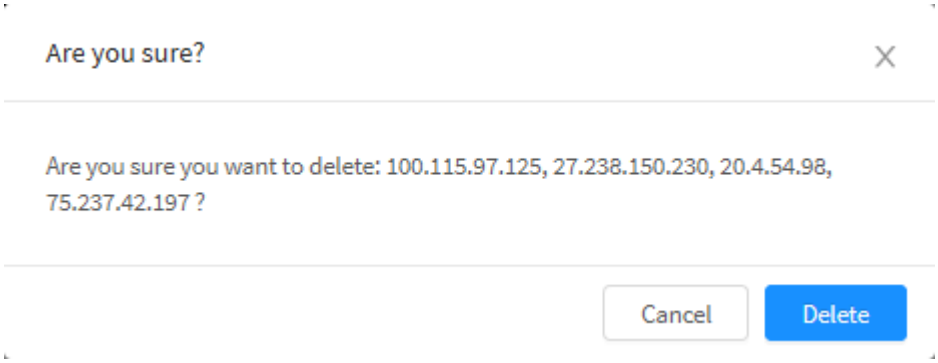
Blocked Addresses - Seleção dos *IPs* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete Profile*”.



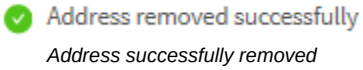
Blocked Addresses – Delete Profile

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



Blocked Addresses – Mensagem confirmando a exclusão de perfil

Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].



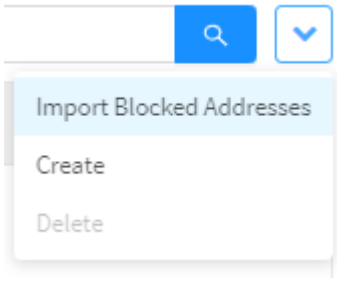
Address successfully removed

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

Blocked Addresses - Menu de Ações - Import Blocked Addresses

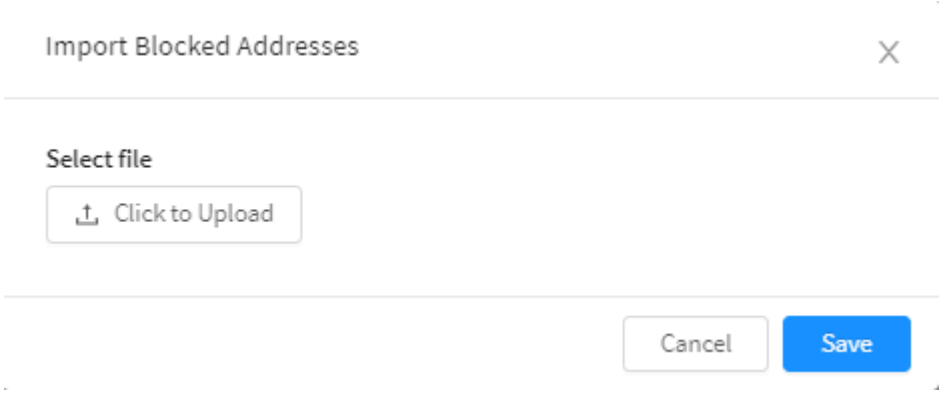
Através da opção “*Blocked Addresses*” é possível importar uma *Blocked Addresses list*. Para acessar, clique no **menu de ações [ ]**.

1. Clique no menu de ações:



Blocked Addresses - Menu de Ações - *Import Blocked Addresses*

2. A tela “*Import Blocked Addresses*” será exibida. Conforme demonstrado na imagem abaixo:

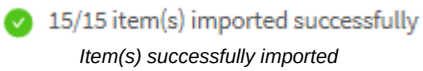


Blocked Addresses - Import Blocked Addresses

3. Selecione o arquivo desejado clicando no botão **[** Click to Upload **]**.

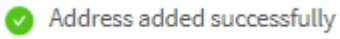
Este botão aceita arquivos de extensão .txt

4. Ao carregar o arquivo com sucesso, uma mensagem de confirmação será exibida:



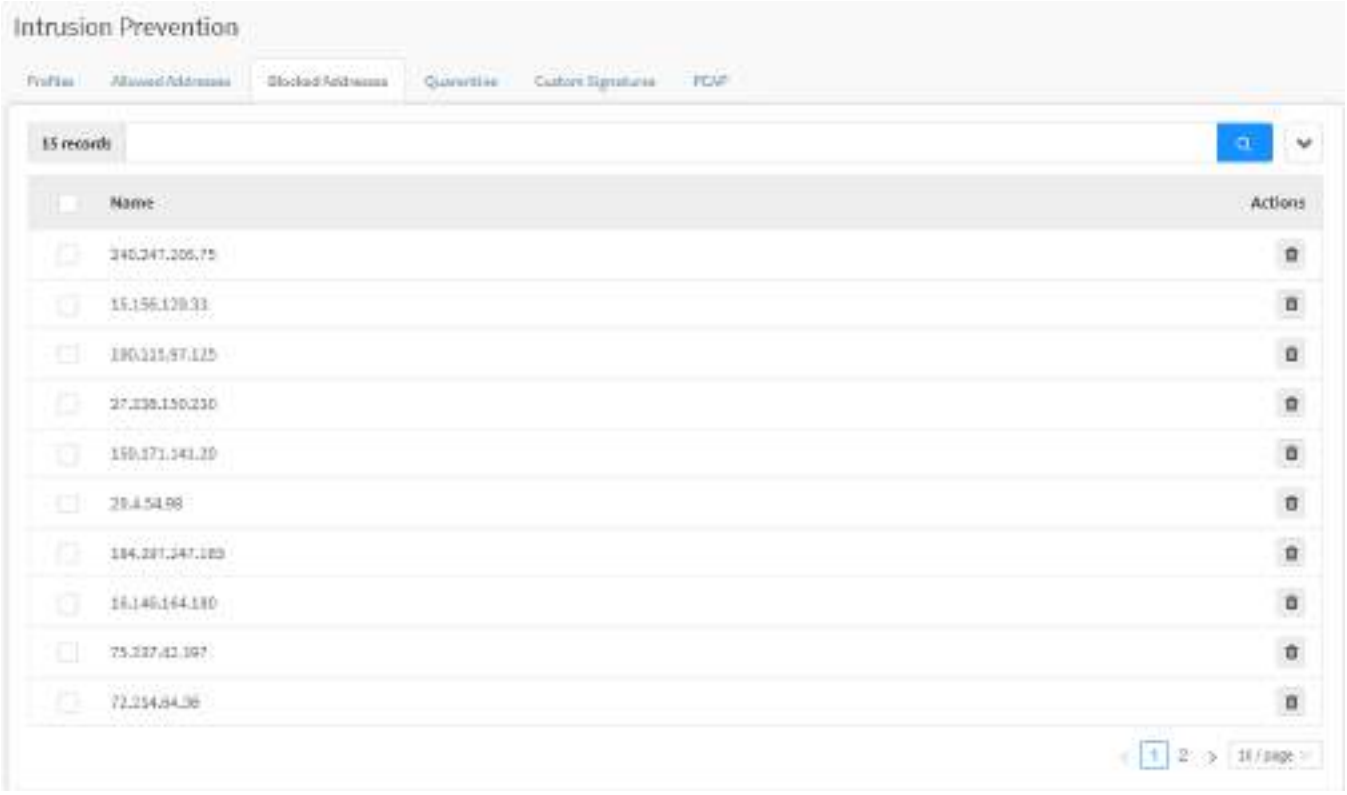
Item(s) successfully imported

5. Ao finalizar a adição dos itens, a seguinte mensagem de confirmação será exibida:



Address successfully added

6. Por fim, a tela exibirá todos os *IPs* adicionados:



Blocked Addresses List - IPs adicionados

Após realizar esses procedimentos, a importação terá sido efetuada com sucesso.

Intrusion Prevention - Aba Custom Signatures

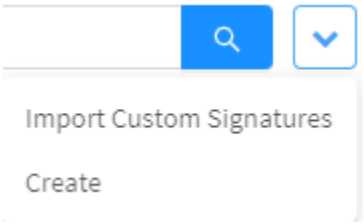
Em Custom Signatures, é possível inserir assinaturas, que eventualmente venham a ser relevantes.

Nesta seção, veremos como configurar uma nova assinatura:

Intrusion Prevention - Custom Signatures

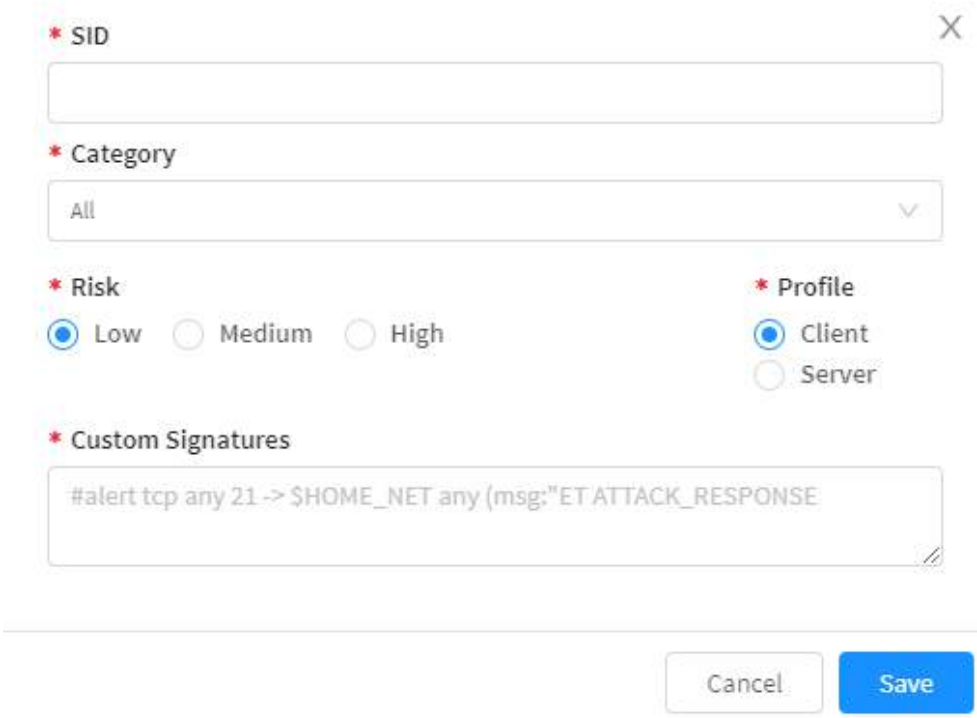
Create Signature

Em options [] encontra-se a opção "*Create*":



Custom Signatures - Create

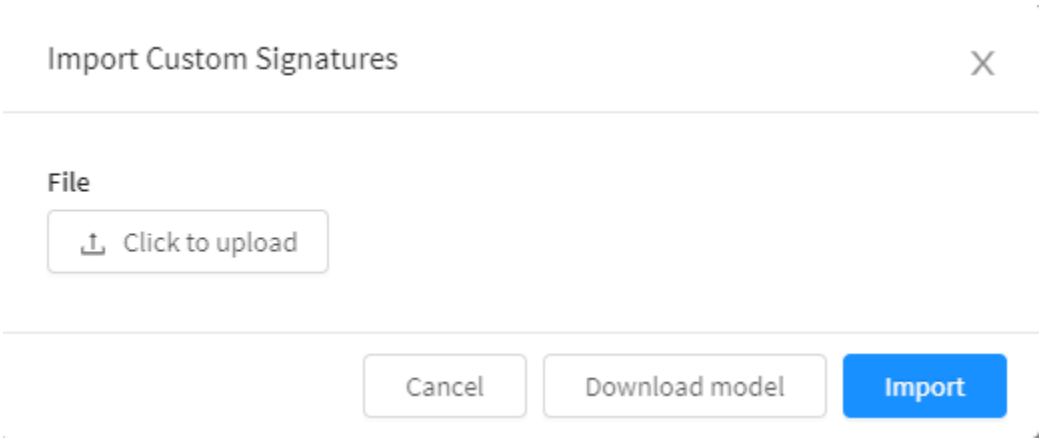
Após, a seguinte tela estará disponível:



Create menu

- ***SID:*** É o código de identificação da assinatura em questão;
- ***Category:*** Categorias disponíveis para este *SID*;
- ***Risk:*** Nível de risco de ameaça da assinatura;
- ***Profile:*** Permite selecionar o perfil da assinatura, se cliente (*Client*)ou servidor (*Server*);
- ***Custom Signatures:*** Permite nomear a assinatura.

Import custom signatures



Import menu

- ***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.

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:

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%.

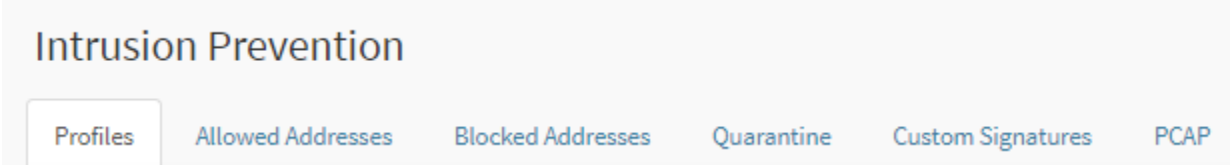
Actions: Ações tomadas quanto ao manuseio do arquivo por parte do sistema.

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".*



Aba *Profiles*

Surgirá a tela “*Profiles*” do *Intrusion Prevention*, conforme demonstrado pela imagem abaixo:

Intrusion Prevention - Profiles

Esta sessão irá abordar como cadastrar, editar e remover os perfis de *Intrusion Prevention*;

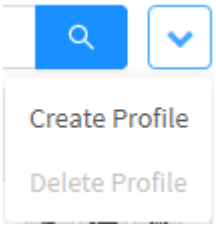
A seguir, analisaremos as funções localizadas no topo deste painel.

Intrusion Prevention - Aba Profiles - Menu de Ações

No topo direito da tela temos o menu de ações:

Intrusion Prevention – Botão do Menu de Ações

Ao clicar neste botão o menu abaixo é exibido:



Intrusion Prevention – Menu de Ações

O menu é composto das seguintes opções:

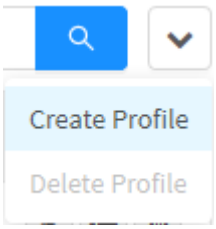
- Create Profile;
- Delete Profile.

A seguir cada opção do menu de ações será detalhada.

Intrusion Prevention - Aba Profiles - Create Profile

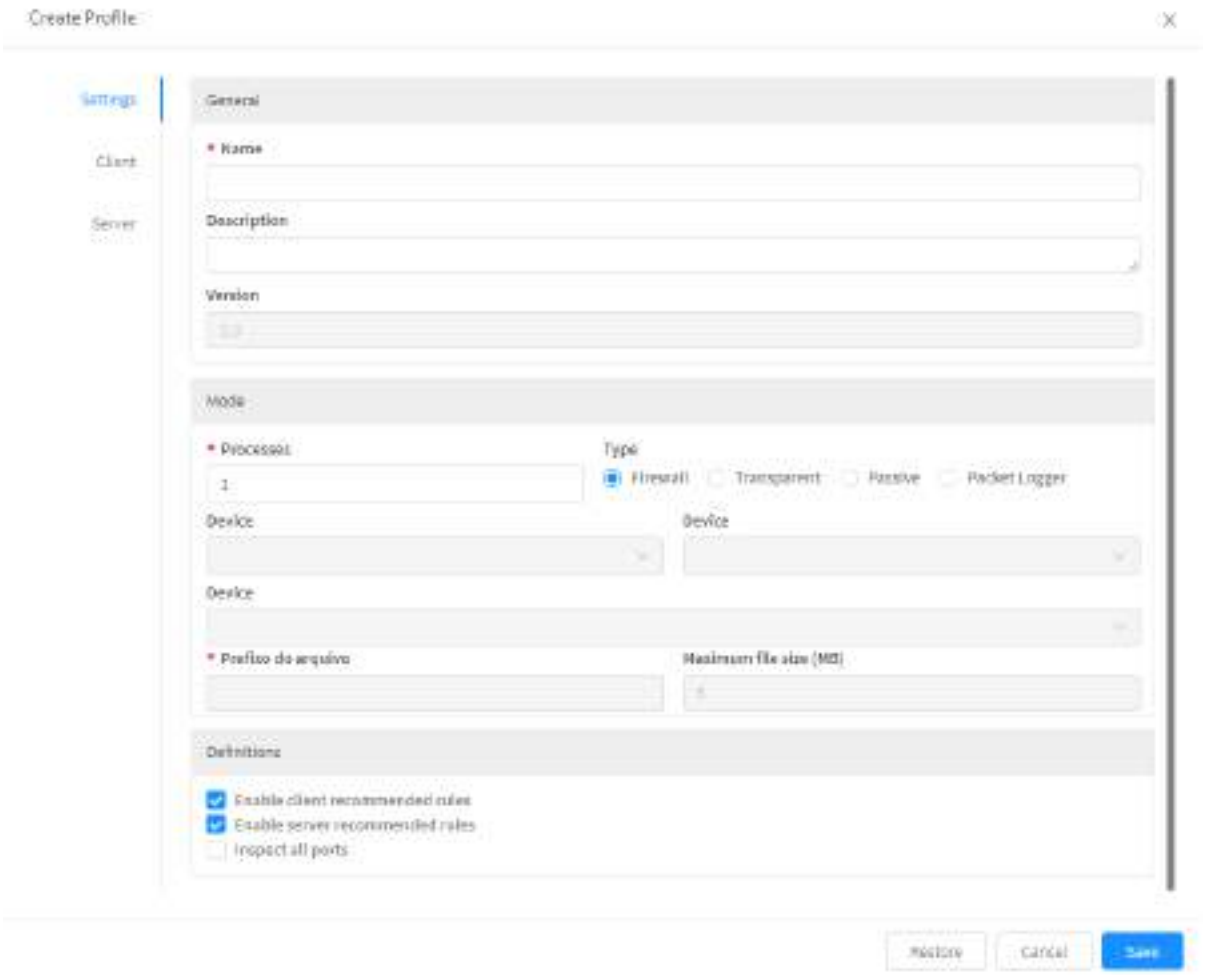
Através da opção “*Create Profile*” é possível criar um novo perfil de *Intrusion Prevention*. Para acessar, clique no **menu de ações [ ]**.

1. Clique na opção “*Create Profile*”;



Intrusion Prevention - Create Profile

2. A tela “*Add Profile*” será exibida. Preencha-a com os seguintes dados:



Intrusion Prevention - Create Profile

Aba Settings

Nesta aba é possível efetuar as configurações gerais, definições e o modo de atuação do *Intrusion Prevention*.

General

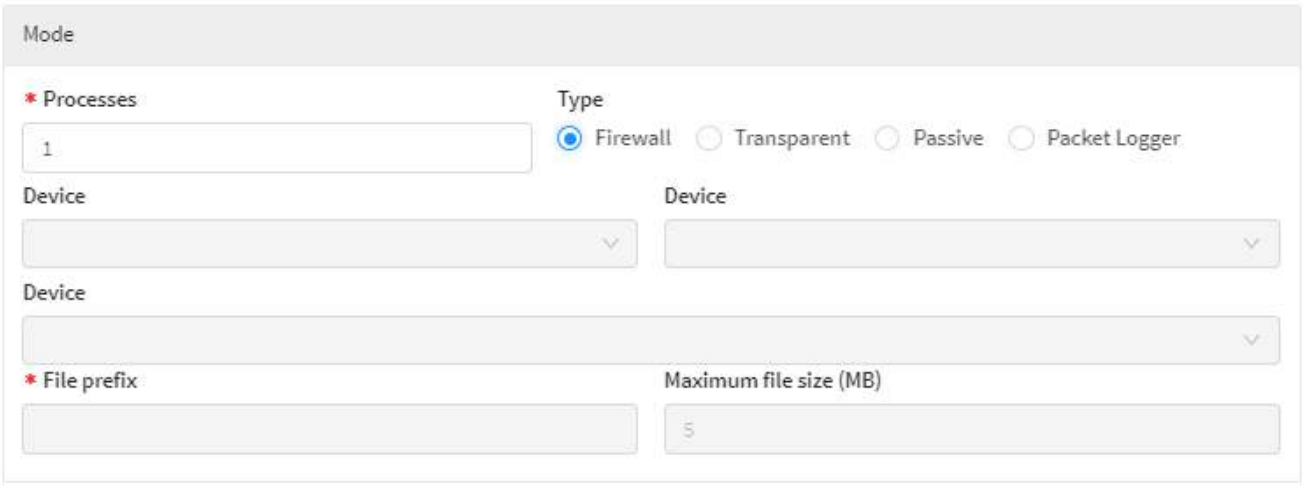
Em "*General*" temos as seguintes caixas de texto:

Intrusion Prevention – General

- ***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:



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 endereço IP. Conforme demonstrado abaixo:

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:

Intrusion Prevention - Definitions

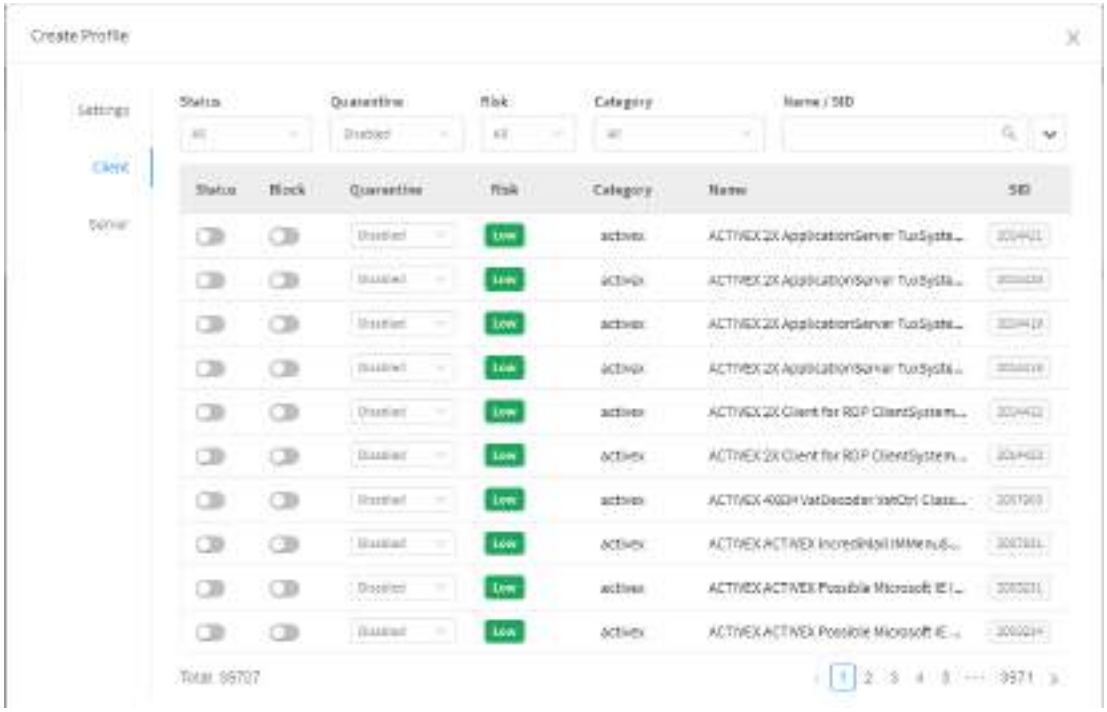
- ***Enable client recommended rules [ ]:*** A ativação desta opção habilita a exibição das regras *ATP padrão da Blockbit*. Estas regras serão exibidas aba *client*;

- ***Enable server recommended rules [ ]:*** A ativação desta opção habilita a exibição das regras *IPS padrão da Blockbit*. Estar regras serão exibidas na aba *server*;
- ***Inspect all ports[ ]*:** 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 [ ]*** na aba *Settings*, a aba *Client* irá exibir as assinaturas conforme demonstrado abaixo:

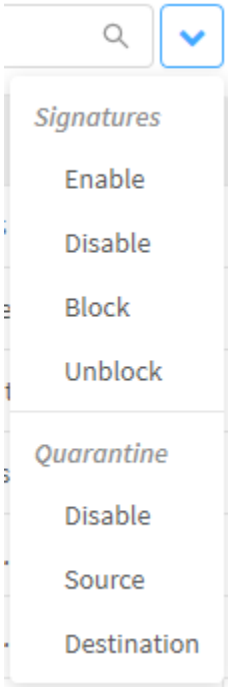


Intrusion Prevention - Client

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;
- **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*) 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:

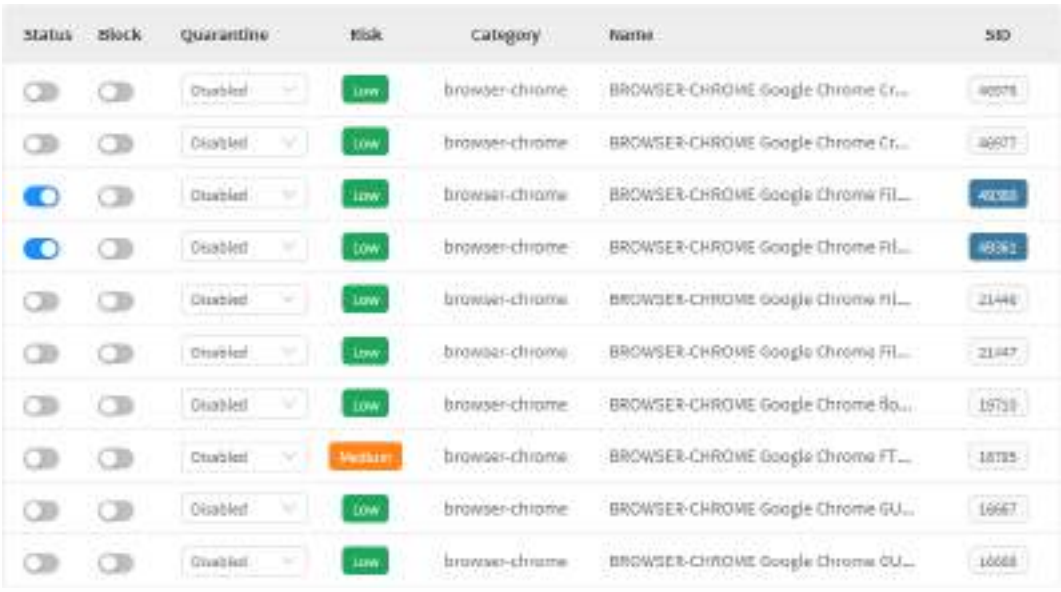


Intrusion Prevention - Ações

Para *alterar* a ação de determinada assinatura da base, clique no **[/]** de *"*Status*" e "*Bloqueio*"* da respectiva assinatura que deseja *"*Habilitar/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:

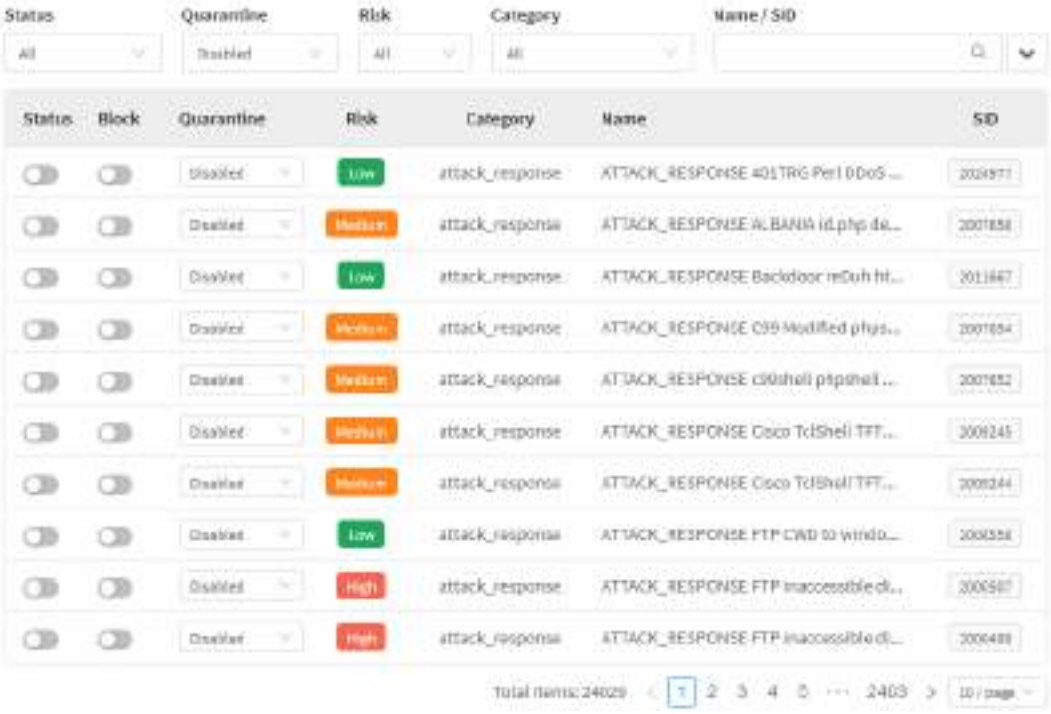


Intrusion Prevention - Highlighted SID example

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 **[ ]**.

Aba *Server*

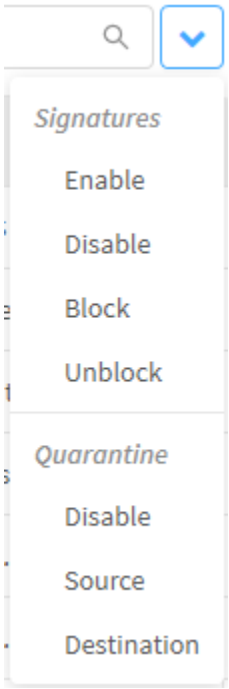
Ao habilitar a opção ***Enable server recommended rules [ ]*** na aba *Settings*, a aba *Server* irá exibir as assinaturas *IPS* conforme demonstrado abaixo:



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:
  - *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;
- **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:

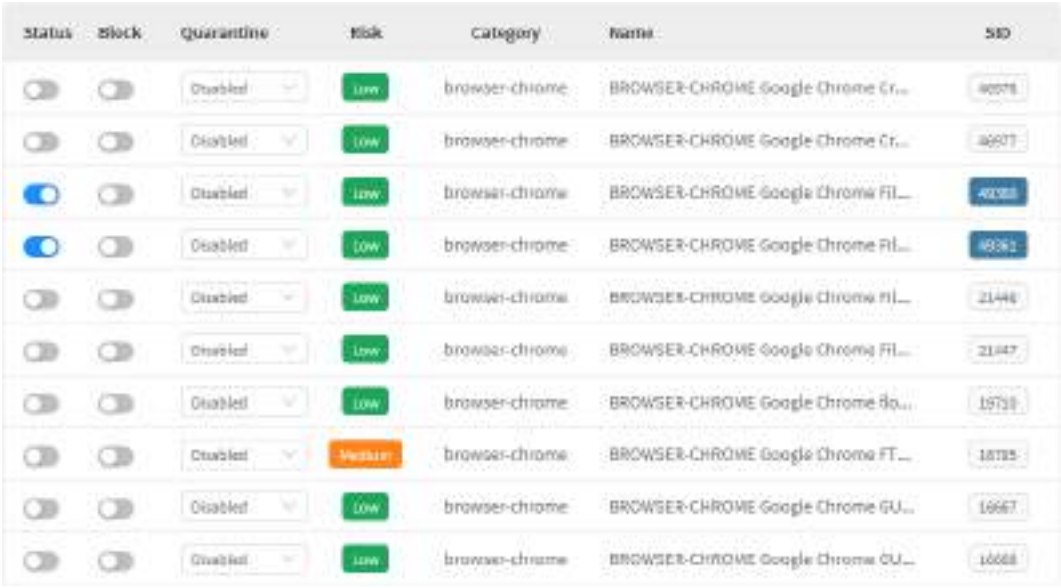


Intrusion Prevention - Ações

Para *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 *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:

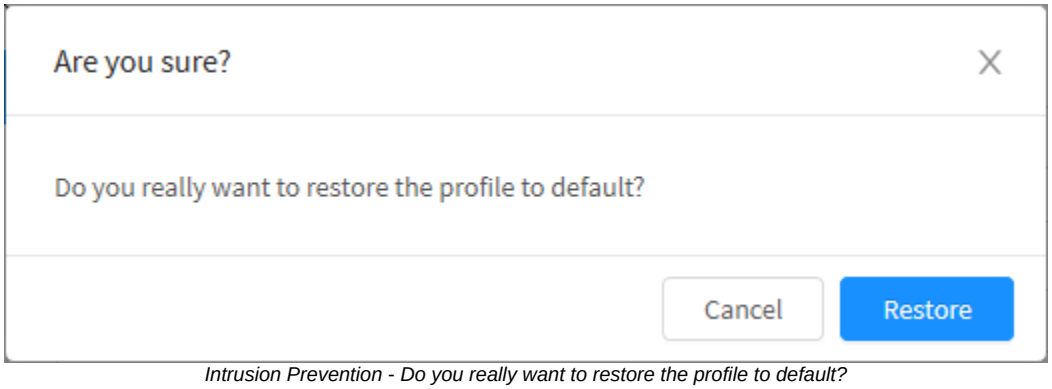


Intrusion Prevention - Highlighted SID example

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 [ ].

Botão *Restore*

Caso à qualquer momento queira restaurar o perfil e as configurações padrão da Blockbit, clique em ***Restore***[Restore], a seguinte janela será exibida.

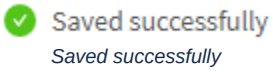


Intrusion Prevention - Do you really want to restore the profile to default?

Clique no botão ***Cancel***[Cancel] para sair dessa janela ou no botão ***Restore***[Restore] para restaurar.

Profile restored

Por fim, caso deseje cancelar clique no botão ***Cancel***[Cancel]. Para concluir a edição das aplicações clique no botão ***Save***[Save].



As configurações foram feitas com sucesso.

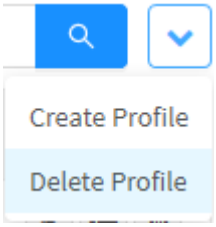
Intrusion Prevention - Aba Profiles - Delete Profile

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 **[ ]**. Ex.: *Test*;

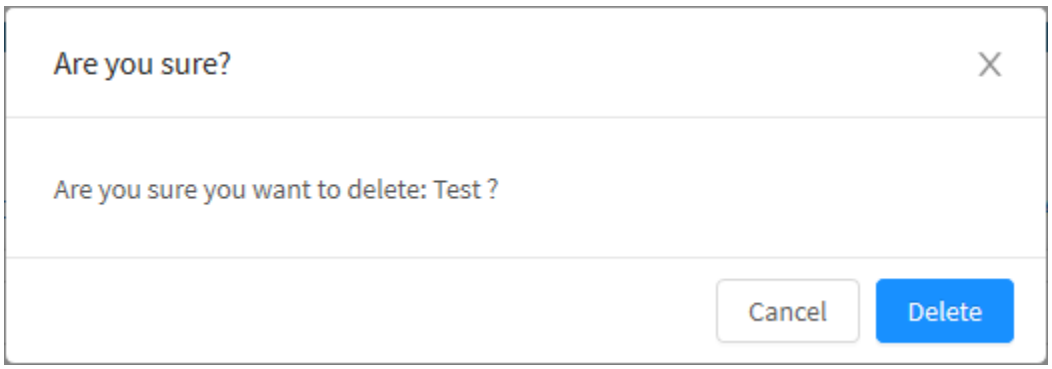
Intrusion Prevention – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete Profile*”.



Intrusion Prevention – Delete Profile

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



Intrusion Prevention – Mensagem se deseja deletar os *profiles*

Caso desejar cancelar clique no botão ***Cancel*[ ]**. Para concluir, clique no botão ***Delete*[ ]**.

Profile removed successfully

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*:

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 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*;
- ***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*, equivalente a opção *Delete Profile* do menu de ações.

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 *Intrusion 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".*

Aba *Quarantine*

Surgirá a tela "*Quarantine*" do *Intrusion Prevention*, conforme demonstrado pela imagem abaixo:

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.

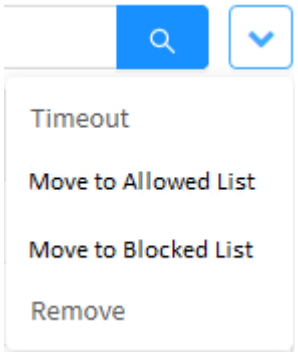
A seguir analisaremos as opções do menu de ações e a função das colunas da aba *Quarantine*.

Quarantine - Menu de Ações

No topo direito da tela temos o menu de ações:

Intrusion Prevention – Botão do 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:

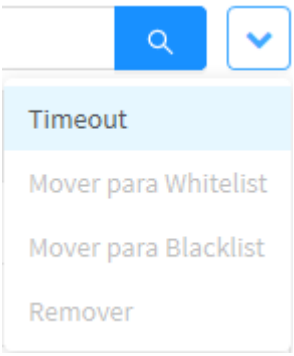
- *Timeout*;
- *Move to Allowed Addresses List*;
- *Move to Blocked Addresses List*;
- *Remove*.

A seguir cada opção do menu de ações será detalhada.

Quarantine - Menu de Ações - Timeout

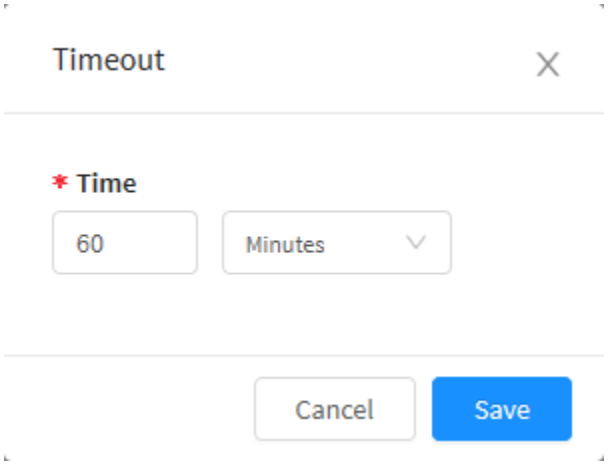
O tempo de permanência da quarentena de um determinado *IP* é configurável através desta opção. Para acessar, clique no **menu de ações [ ]**.

1. Clique na opção “*Timeout*”;



Intrusion Prevention - *Quarantine* - Menu de Ações - *Timeout*

2. A tela abaixo será exibida:



Quarantine - *Timeout*

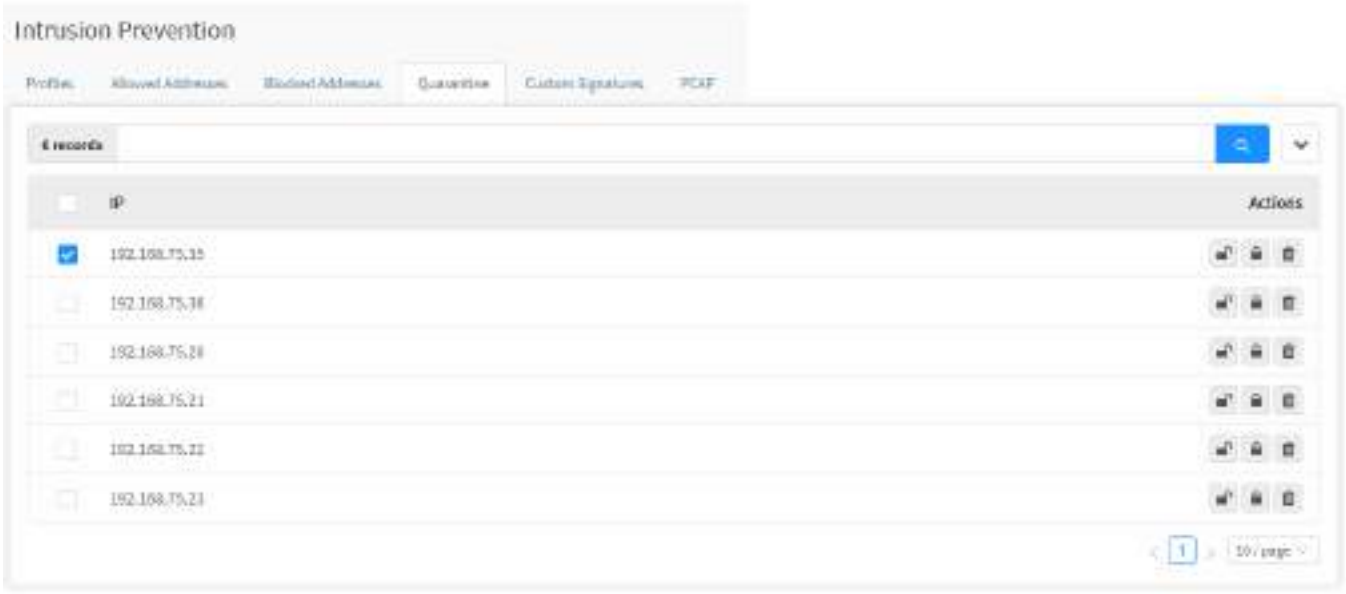
Neste painel poderá ser configurado o tempo de *timeout* para remover o endereço na quarentena, por *default* o sistema vai configurado com o tempo de 60 minutos. No primeiro campo, é possível determinar o tempo, já na caixa de seleção é possível definir se o tempo será em minutos ou horas.

Por fim, caso deseje cancelar clique no botão **[** Cancel **]**. Para concluir a edição das aplicações clique no botão **[** Save **]**.

Quarantine - Menu de Ações - Move to Allowed Addresses List

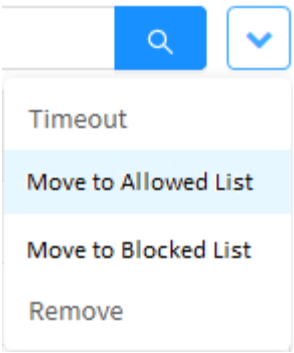
Através desta opção é possível mover um *IP* da quarentena para a *Allowed Addresses list*. Para tanto, siga os seguintes passos:

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 [☑];



Quarantine – Seleção dos *IPs* para mover para a *Allowed Addresses*

2. Clique na opção "*Move to Allowed Addresses list*";



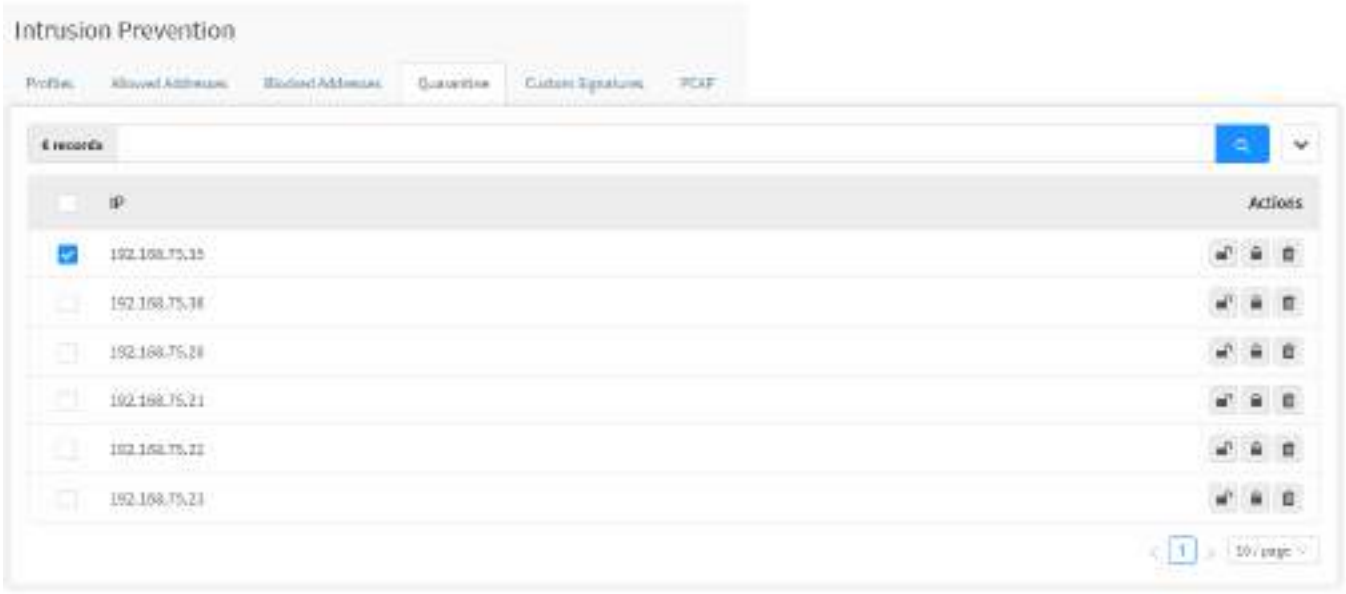
Intrusion Prevention - *Quarantine* - Menu de Ações - *Move to Allowed Addresses list*

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

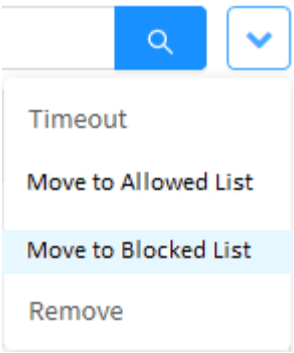
Através desta opção é possível mover um *IP* da quarentena para a *Blocked Addresses list*. Para tanto, siga os seguintes passos:

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 [ ];



Quarantine – Seleção dos *IPs* para mover para a *Blocked Addresses List*

2. Clique na opção "*Move to Blocked Addresses List*";



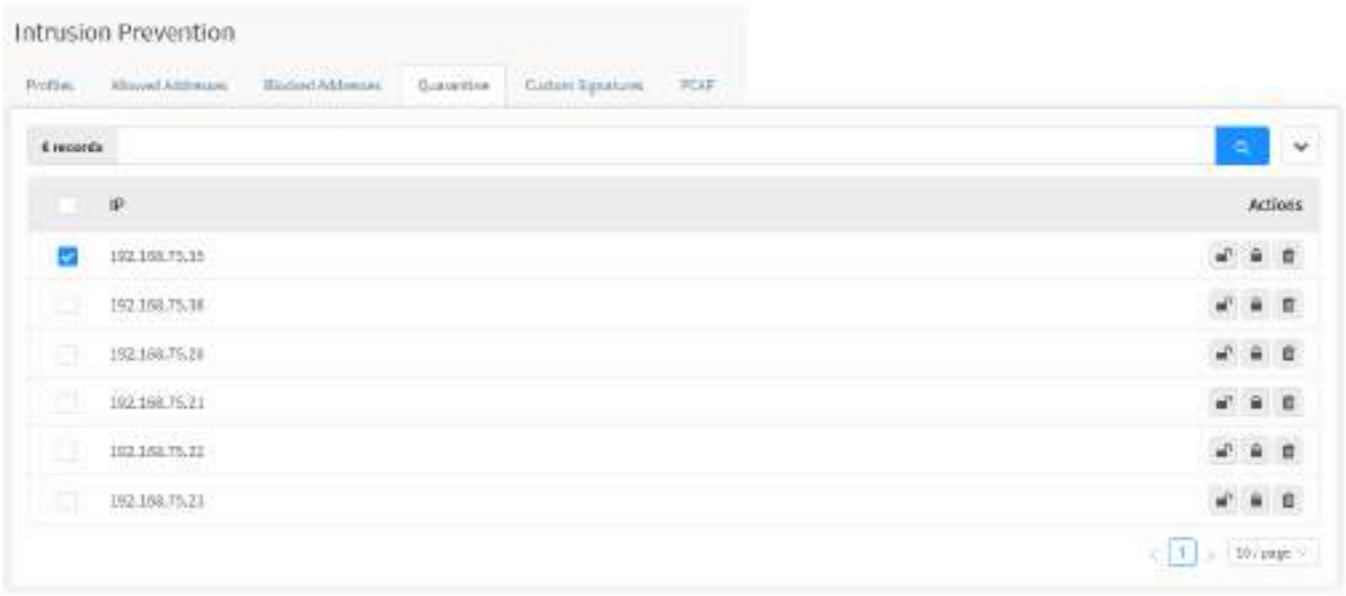
Intrusion Prevention - *Quarantine* - Menu de Ações - *Move to Blocked list*

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

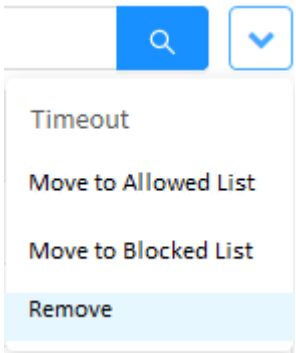
Através do botão “*Remove*” é possível remover os itens selecionados. Para remover pelo Menu de ações, siga os seguintes passos:

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 **[ ]**. Ex.: *Test;*



Quarantine - Seleção para deleção

2. Entre no **menu de ações [ ]** e clique na opção “*Remove*”.

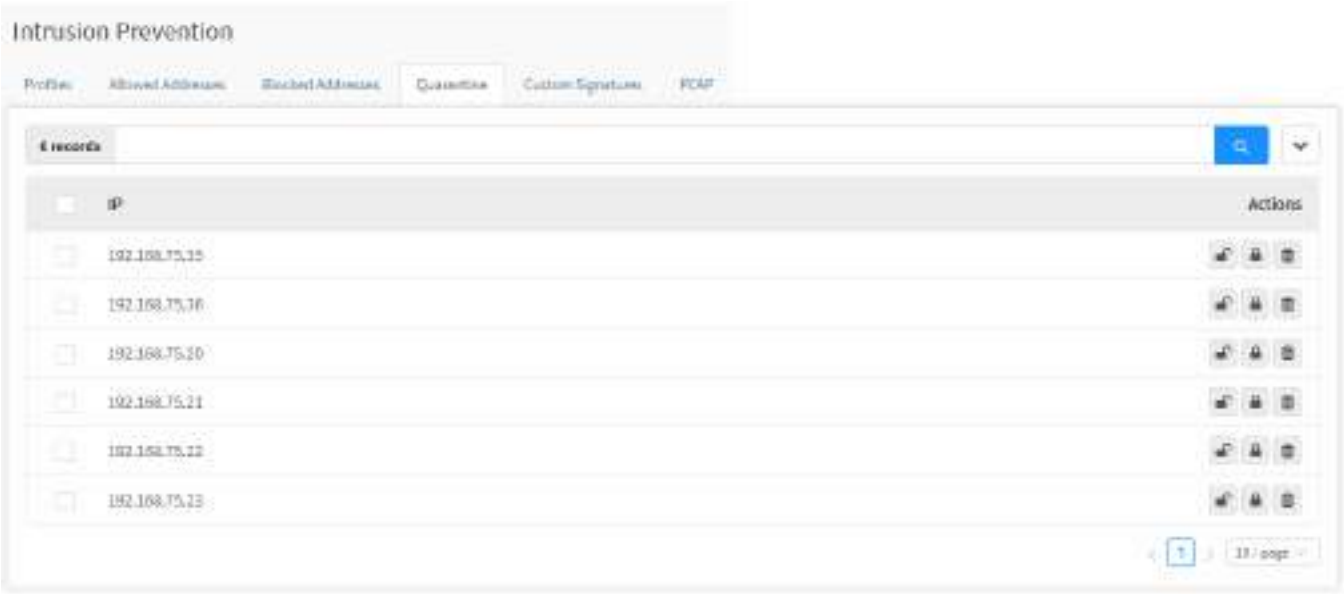


Quarantine - Menu de Ações - *Remove*

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*:



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;
    - **[ ]** 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 *Proxy.* O recurso conta com proteção de “D*ownloads/Upload*” de arquivos infectados, arquivos *“PUA - Potentially Unwanted Application* (Aplicações potencialmente indesejadas)*”,* detecção por “Análise heurística*”* e proteção contra “arquivos com senhas”.

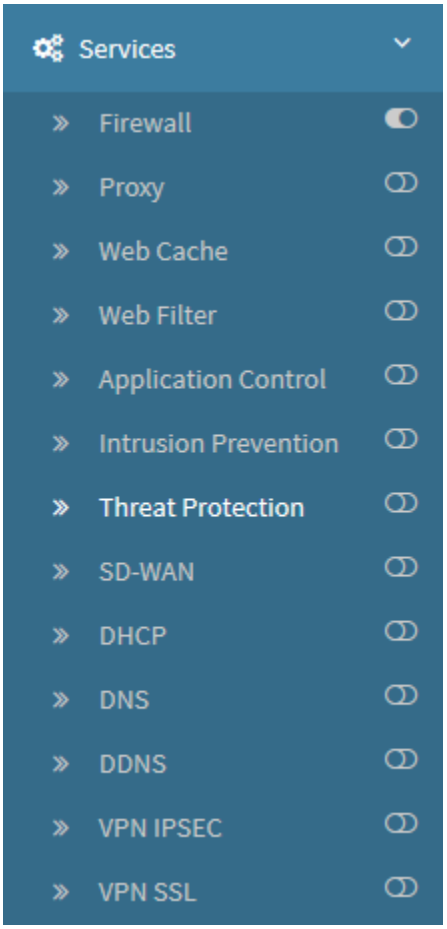
Diferente da maioria dos *Antimalware* e Antivírus concebidos para detectar e prevenir códigos maliciosos em dispositivos de *EPS “Endpoint Secure”*, o Blockbit UTM inclui um recurso interno de *Threat Protection* que é atualizado automaticamente na busca de novas ameaças que podem infectar sua rede. 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.



Services - Threat Protection

A tela abaixo será exibida:

Threat Protection

A tela comporta as seguintes abas:

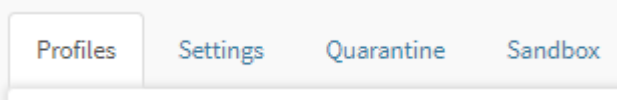
- *Profiles*;
- *Settings*;
- *Quarantine*;
- *Sandbox*.

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".*



Aba *Profiles*

Surgirá a tela “*Profiles*” do *Threat Protection*, conforme demonstrado pela imagem abaixo:

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.

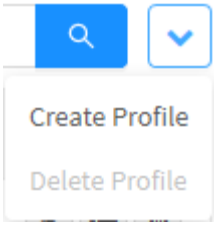
Threat Protection - Profiles - Menu de ações

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:

Threat Protection – Botão do menu de ações.

Ao clicar neste botão o menu abaixo é exibido:



Threat Protection – Menu de ações

O menu é composto das seguintes opções:

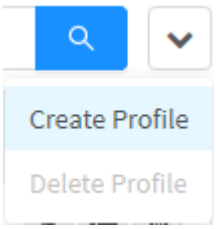
- *Create Profile*;
- *Delete Profile*.

A seguir cada opção do menu de ações será detalhada.

Threat Protection - Profiles - Menu de Ações - Create Profile

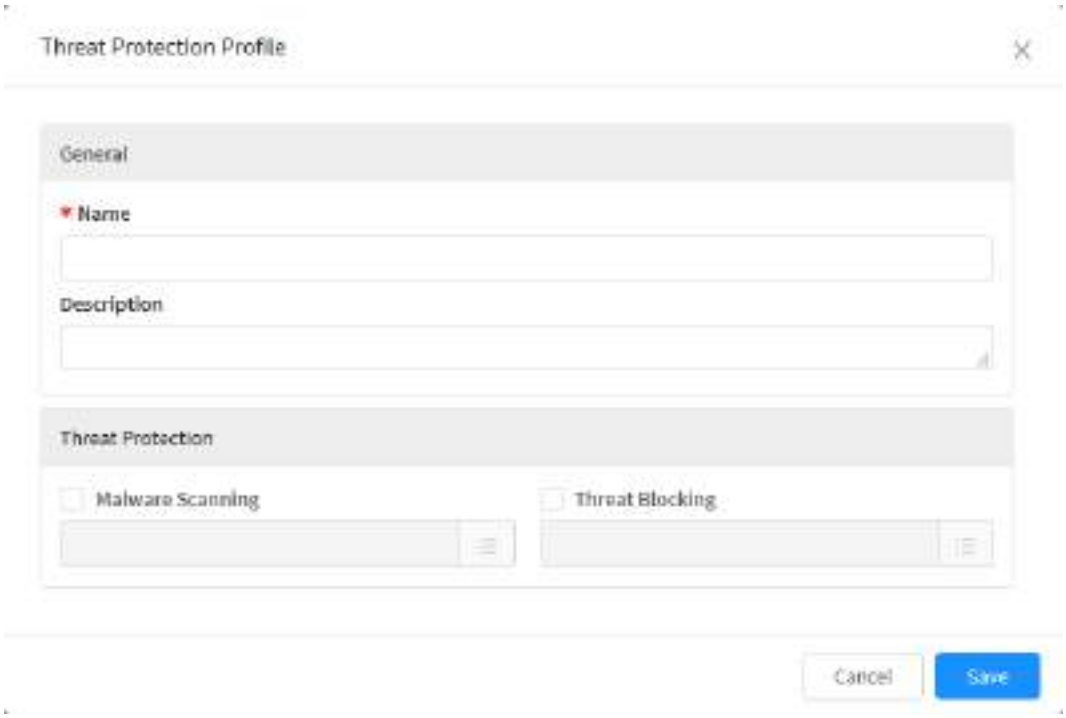
Através da opção “*Create Profile*” é possível criar um novo perfil de *Threat Protection*. Para acessar, clique no **menu de ações [ ]**.

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.



Threat Protection - Create Profile

General

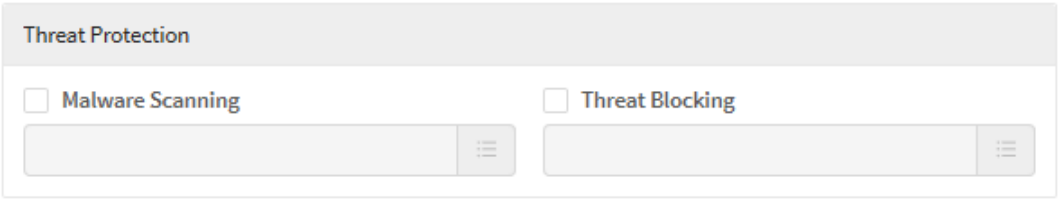
Em "*General*" temos as seguintes caixas de texto:

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.

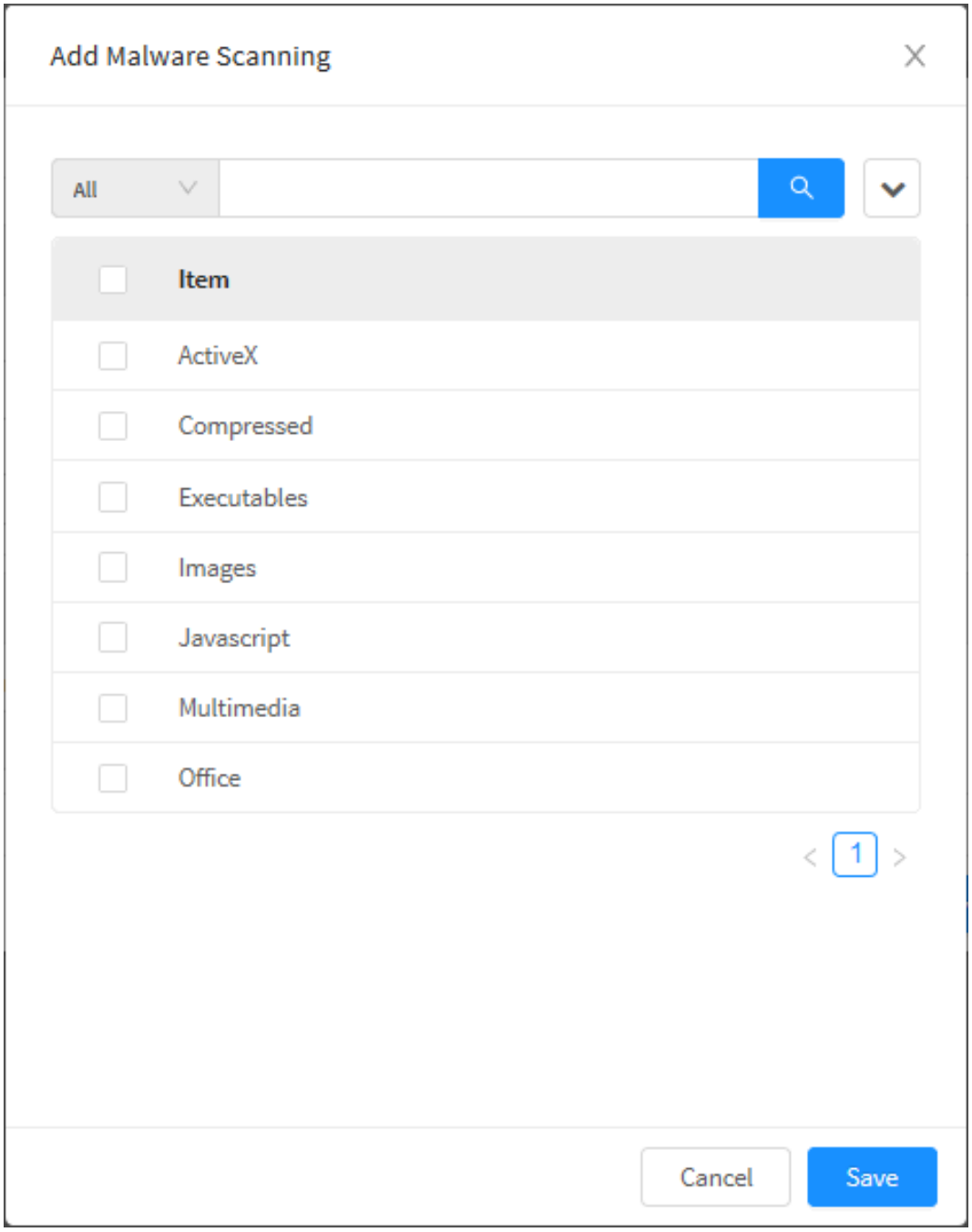


Threat Protection - Threat Protection

A seguir, analisaremos em detalhes estes dois campos.

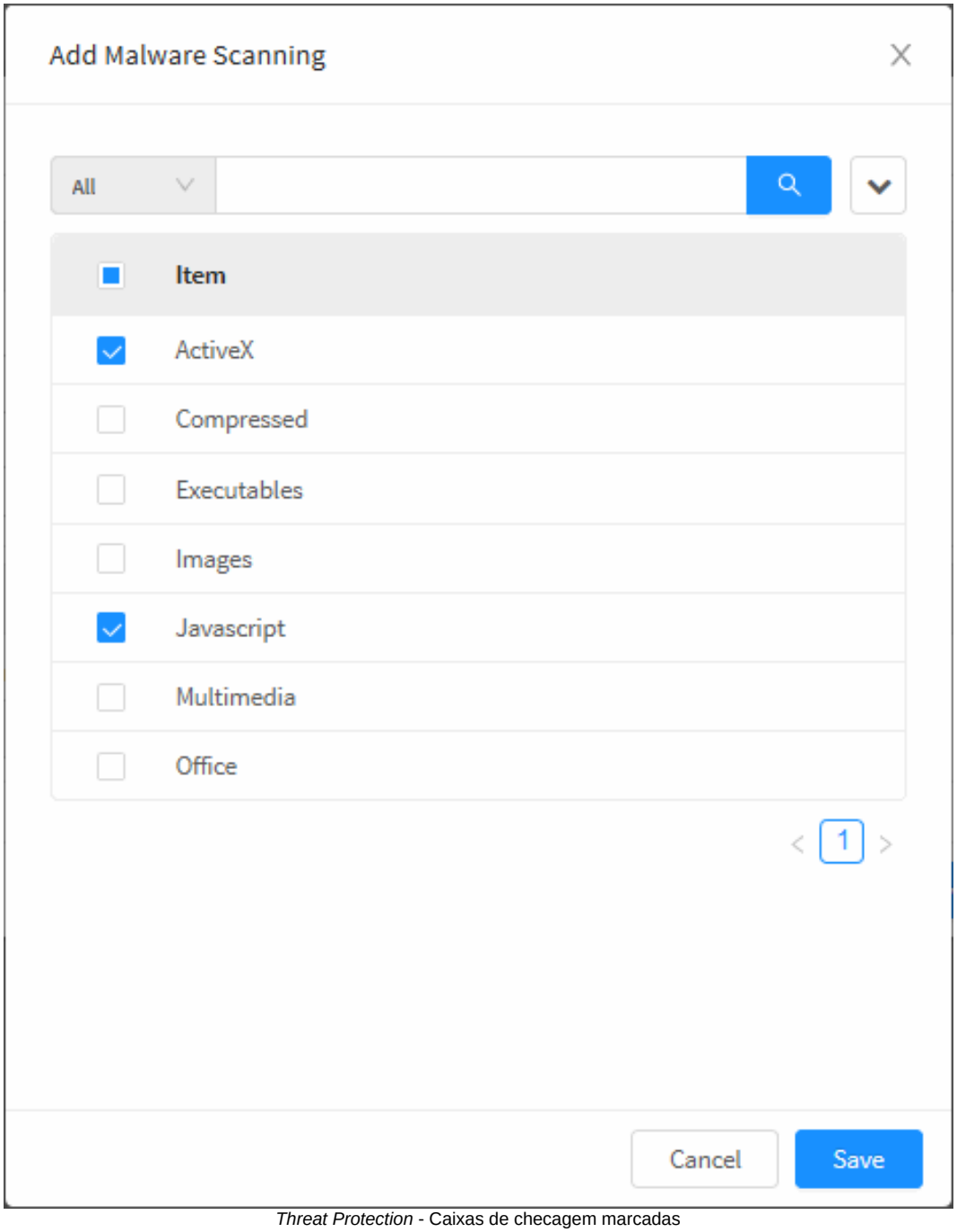
Malware Scanning

Para adicionar o *Malware Scanning*, certifique-se que o ***checkbox*** **[** **]** está habilitado, depois clique no botão ***list applications*** **[** **]** o seguinte painel, será exibido:



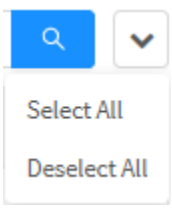
Threat Protection - Add Malware Scanning

Marque as caixas de checagem para adicionar *malware scanning*, conforme demonstrado abaixo:



Threat Protection - Caixas de checagem marcadas

Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no **menu de ações [ ]**:

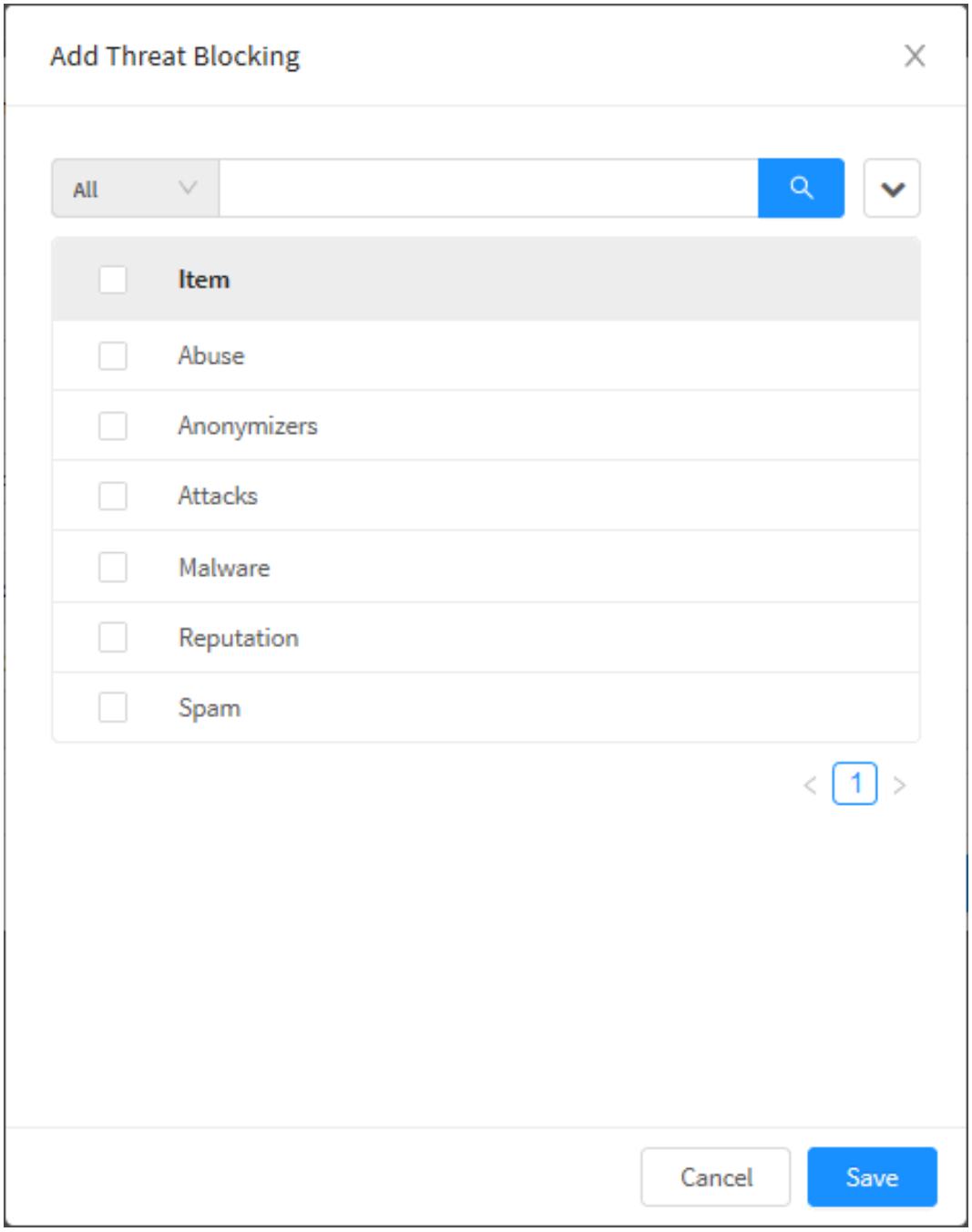


Threat Protection - Select all e *Deselect All*

Por fim, caso deseje cancelar clique no botão ***Cancel***[Cancel]. Para concluir adição do *Malware Scanning* das aplicações clique no botão ***Save***[Save].

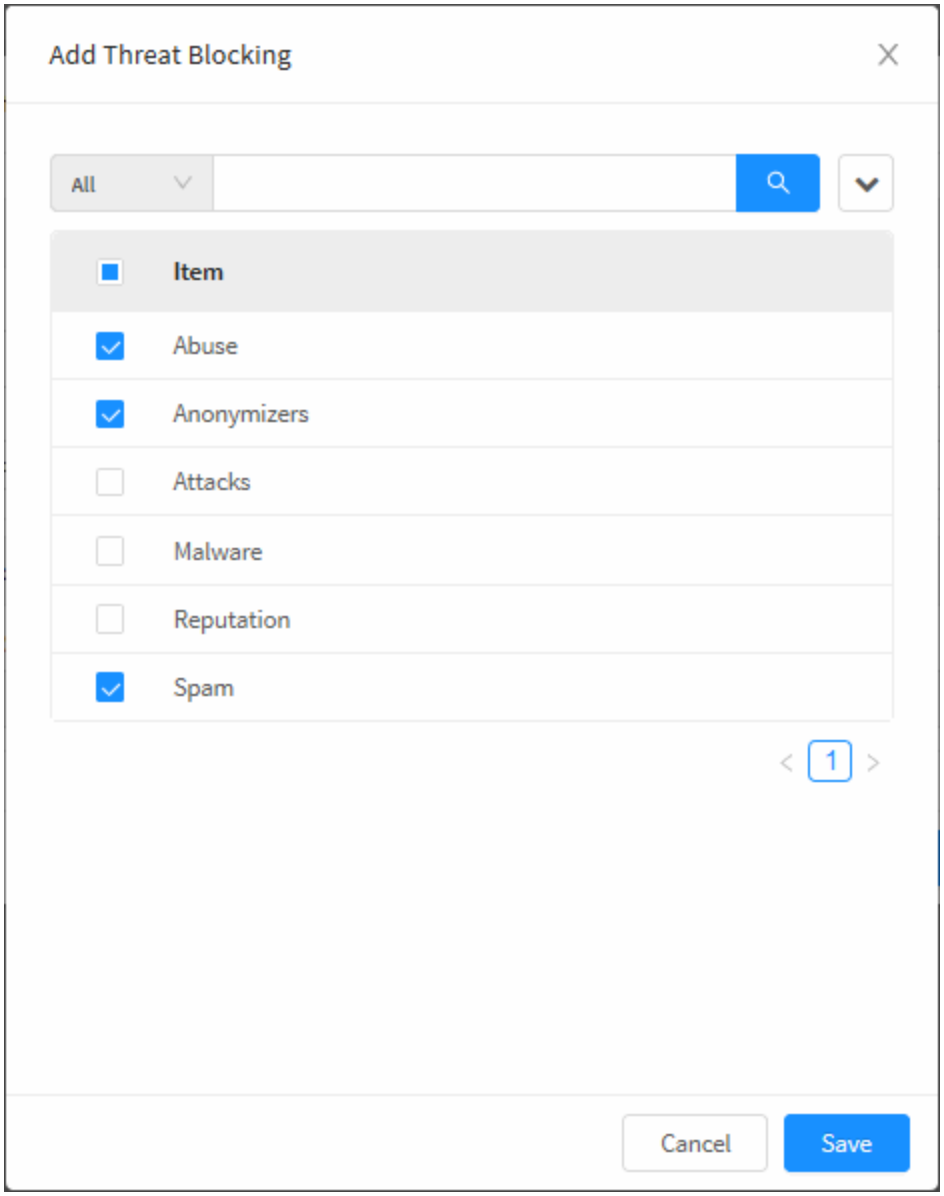
Threat Blocking

Para adicionar o *Threat Blocking*, certifique-se que o ***checkbox*** [☑] está habilitado, depois clique no botão ***list applications*** [☰] o seguinte painel, será exibido:



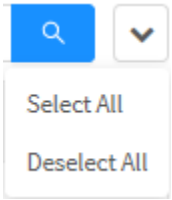
Threat Protection - Add Threat Blocking

Marque as caixas de checagem para adicionar o bloqueio de ameaças, conforme demonstrado abaixo:



Threat Protection - Add Threat Blocking

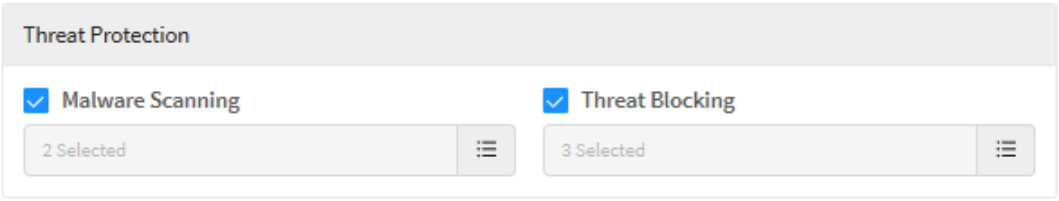
Caso seja necessário fazer uma configuração em todos os itens, basta selecionar a opção desejada no **menu de ações [ ]**:



Threat Protection - Select all e *Deselect All*

Por fim, caso deseje cancelar clique no botão ***Cancel***[Cancel]. 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 - Itens selecionados

Para concluir, basta clicar no botão ***Save***[Save] novamente.

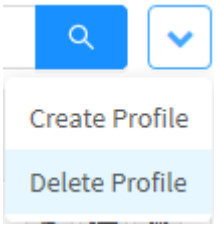
Threat Protection - Profiles - Menu de Ação - Delete Profile

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 **[ ]**. Ex.: *Test*;

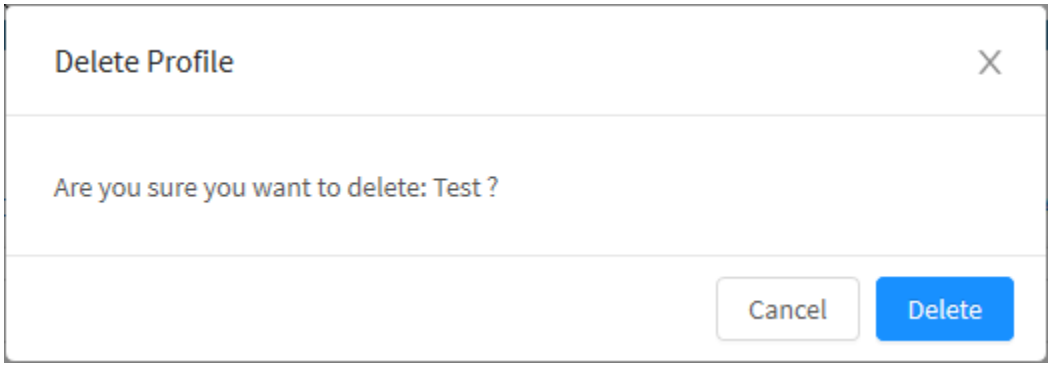
Threat Protection – Seleção dos *Profiles* para deletar

2. Entre no **menu de ações [ ]** e clique na opção “*Delete Profiles*”.



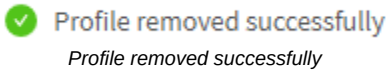
Threat Protection – Delete Profiles.

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



Threat Protection – Mensagem se deseja deletar os *Profiles*

Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].



Profile removed successfully

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

Threat Protection - Profiles - Colunas

A seguir explicaremos cada coluna da aba *Threat Protection*:

Profiles – *Threat Protection*

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.

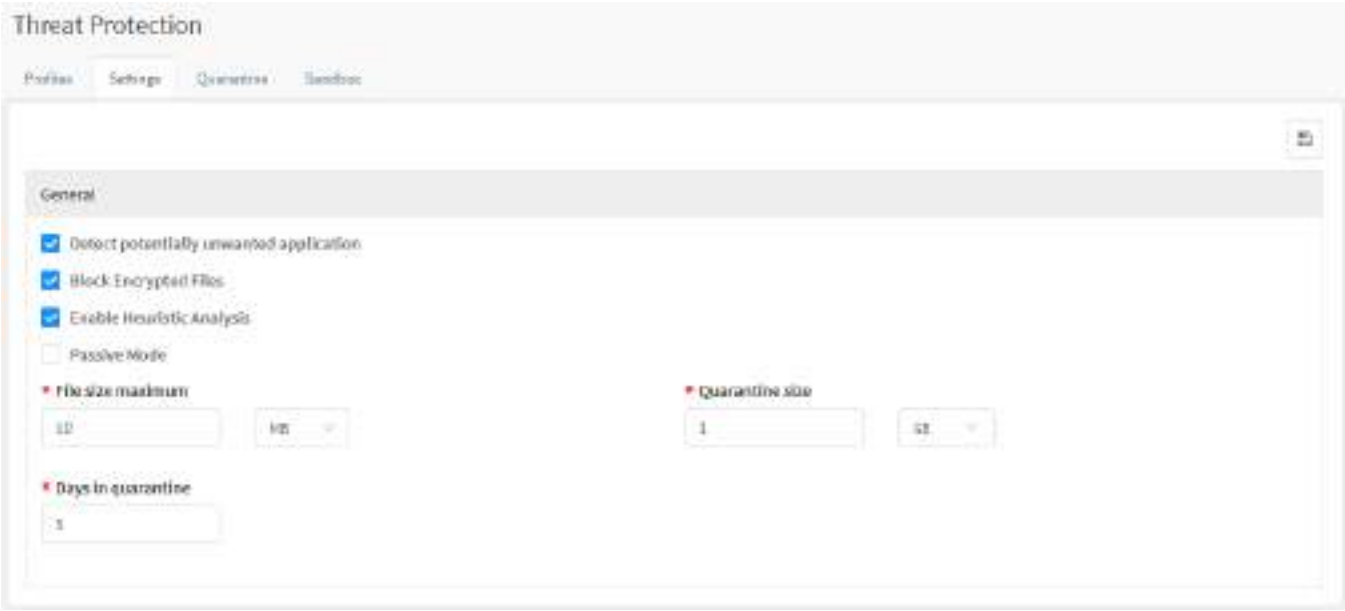
Threat Protection - Aba Settings

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"*.

Aba *Settings*

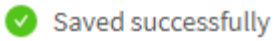
Surgirá a tela “*Settings*” do *Threat Protection*, conforme demonstrado pela imagem abaixo:



Threat Protection - Aba Settings - General

- ***Detect potentially unwanted application* [ ]:** Para habilitar a detecção de arquivos maliciosos;
- ***Block encrypted files [ ]:*** Para analisar arquivos bloqueados e realizar o bloqueio;
- ***Enable heuristic analysis [ ]:*** 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.



Saved successfully

Após salvar, para que as alterações tenham efeito 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.

Após realizar esses procedimentos as configurações terão sido efetuadas com sucesso.

Threat Protection - Aba Quarantine

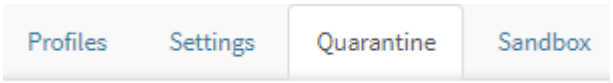
Na aba *Quarantine* é possível permite gerenciar todas as ameaças detectadas que estão na quarentena do Blockbit UTM.

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.

Para mais informações a respeito de Políticas, acesse esta página.

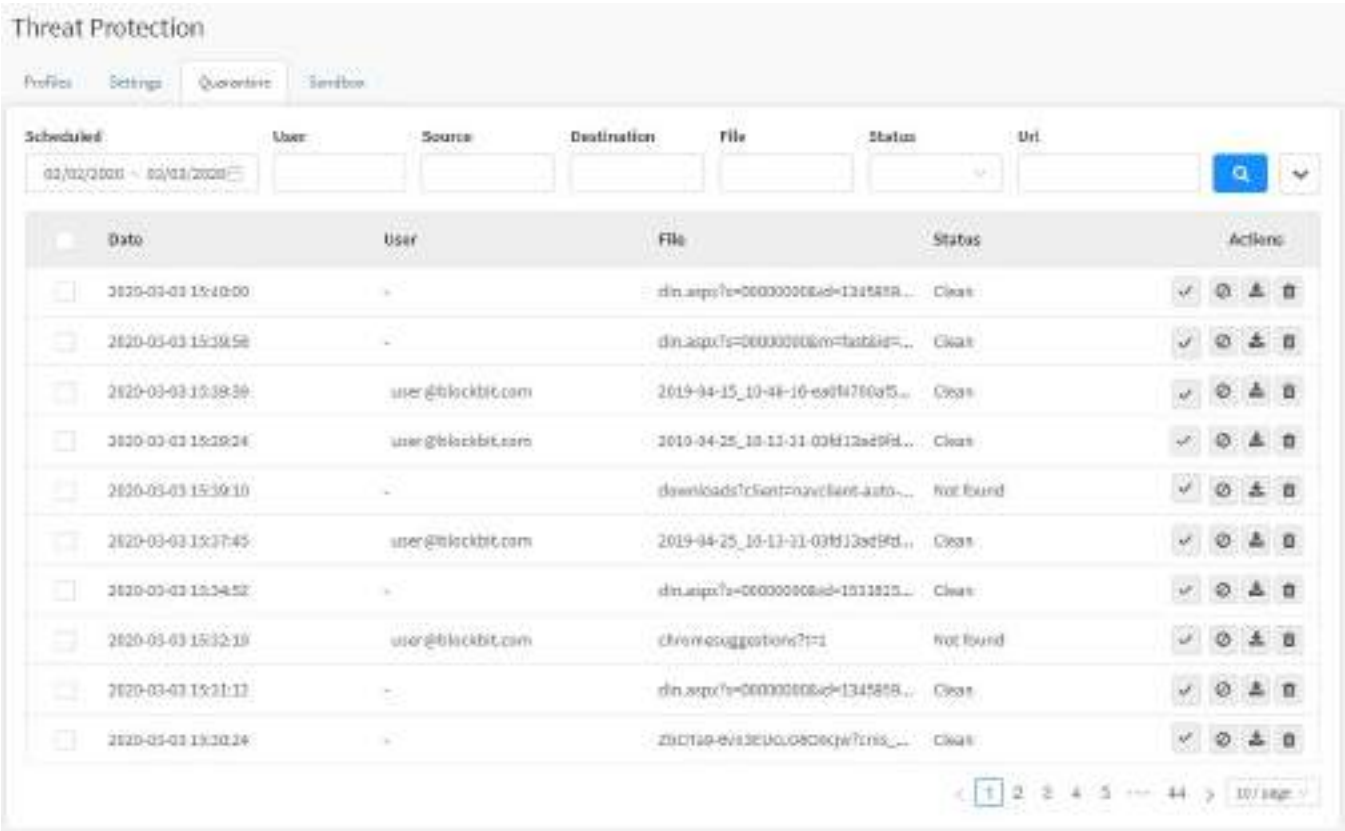
Para mais informações a respeito de perfis de *Threat Protection*, acesse esta página.

Para acessar este recurso, clique em *"Quarantine"*.



Aba *Quarantine*

Surgirá a tela "*Quarantine*" do *Threat Protection*, conforme demonstrado pela imagem abaixo:



Quarantine - Quarentena Populada

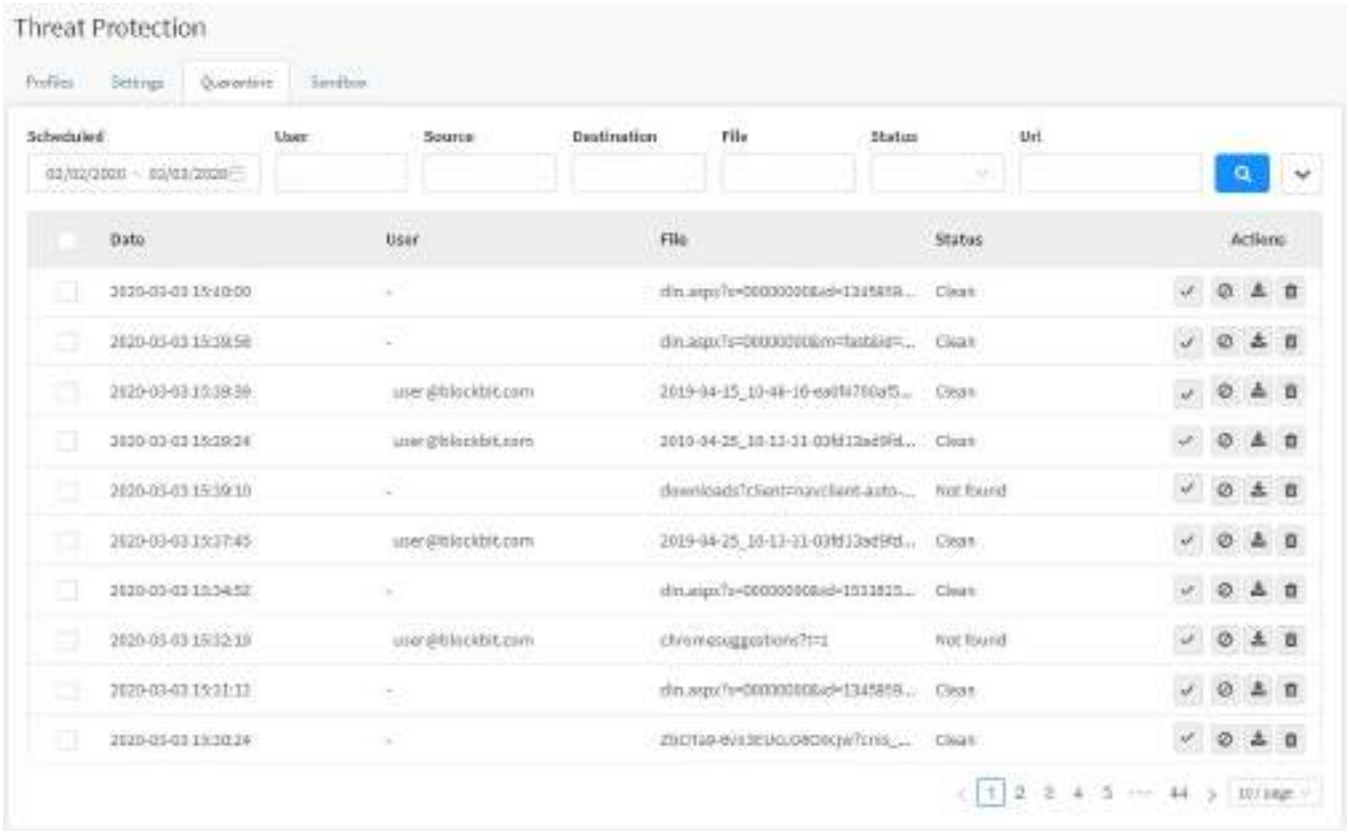
A quarentena possui uma barra de busca que permite o uso de filtros para efetuar uma pesquisa mais efetiva.

Quarantine - Barra de busca

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;
- **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.

Para efetuar uma busca, basta clicar em []. Os resultados são exibidos na tabela abaixo:



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*****[]:** Ao 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;

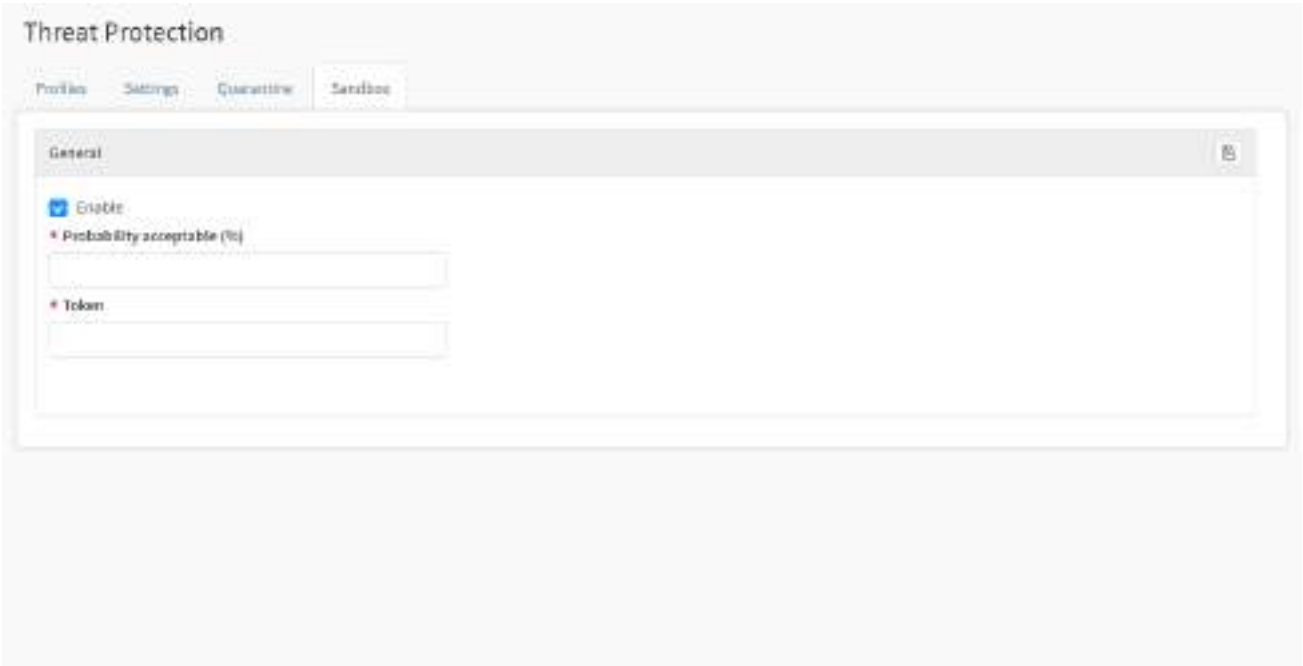
3 - Threat Protection do Blockbit verifica se o Hash gerado do arquivo foi verificado e classificado pelo Blockbit Labs, executando a ação de bloqueio ou liberação;

4 - Threat Protection do Blockbit analisa o arquivo em busca de ameaças utilizando o método tradicional (match com assinaturas de antimalware conhecidas);

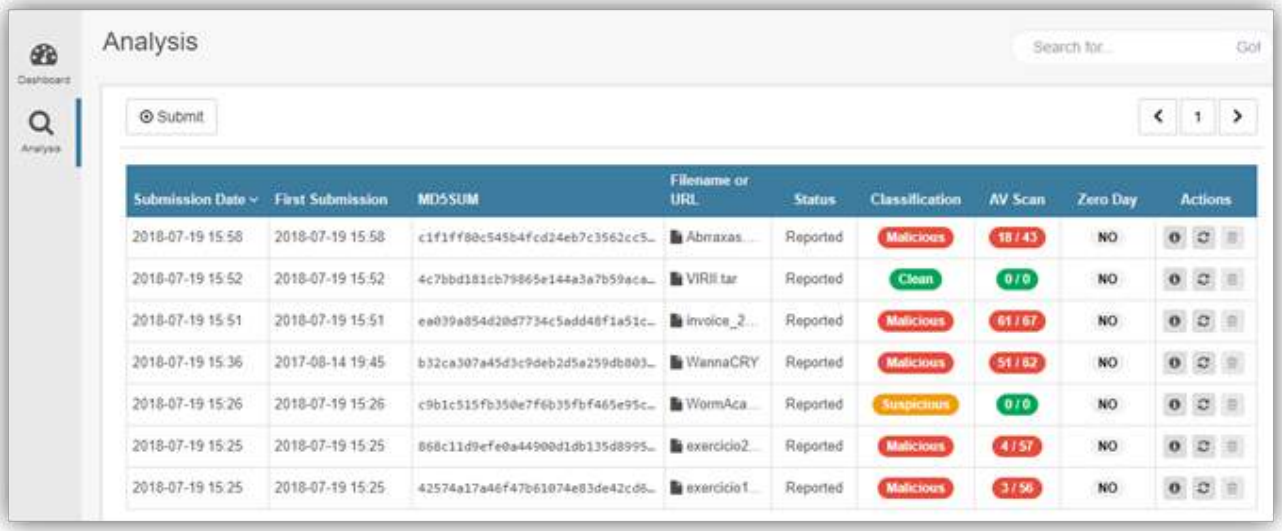
5 - Se o arquivo não der match em alguma assinatura conhecida ou na base de hash alimentada pelo Blockbit labs, mas apresentar um comportamento suspeito ele é enviado para análise em Sandbox.

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.

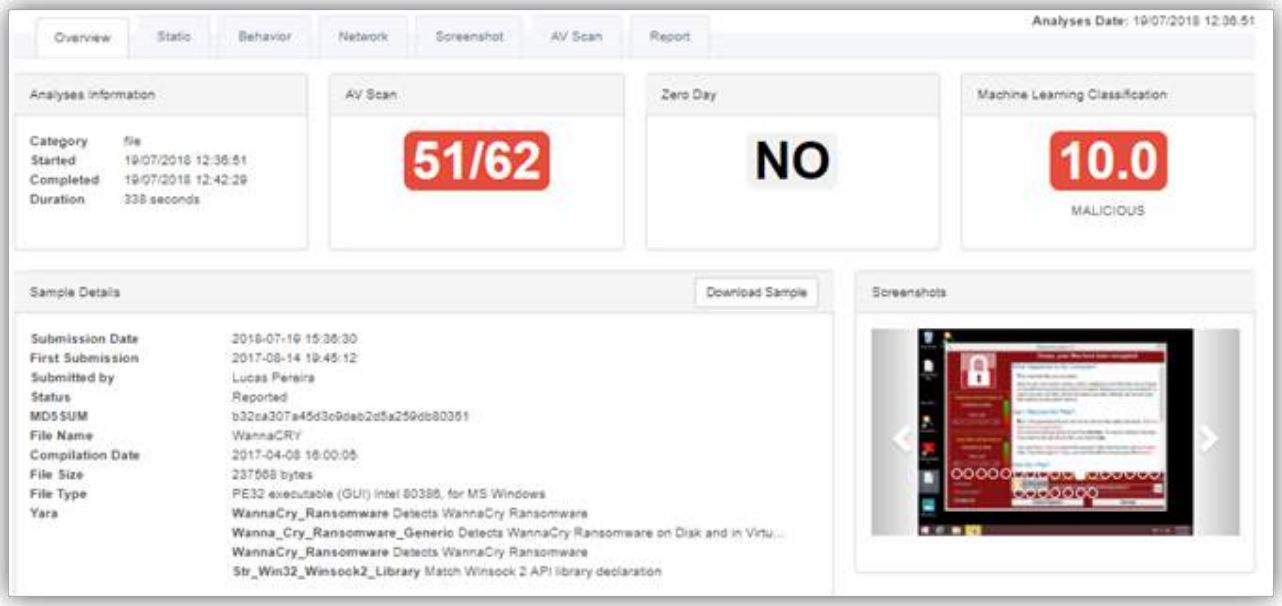
Sandboxes são usados para executar códigos maliciosos com segurança para evitar danos ao dispositivo host, à rede ou a outros dispositivos conectados. Usar uma *sandbox* para detectar malware oferece uma camada adicional de proteção contra ameaças de segurança, como ataques furtivos e explorações que usam vulnerabilidades de dia zero.



Threat Protection > Sandbox



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*.

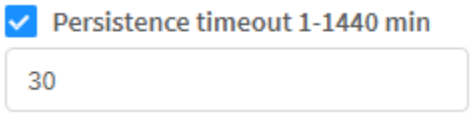
Persistência de *Link*

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 nos indicadores 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).



Persistência de conexão

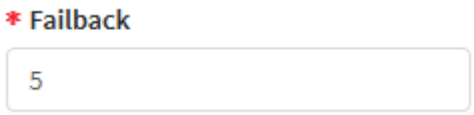
Ao habilitar a caixa de checagem no painel de perfil do *SD-WAN*, o administrador determina se a conexão por um único endereço de origem será persistente.

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.



Failback

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.

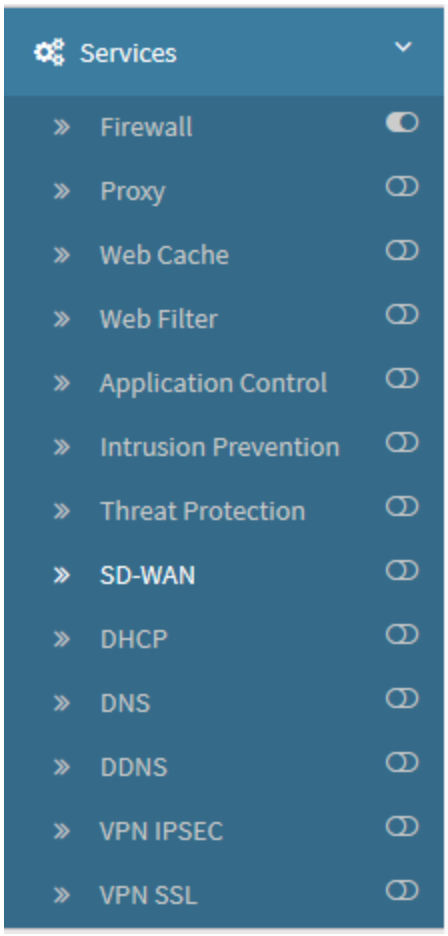
Recursos do *SD-WAN*

- ***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:



Services - SD-WAN

A tela abaixo será exibida:

SD-WAN – Profiles

A tela *SD-WAN* é comporta pelas seguintes abas:

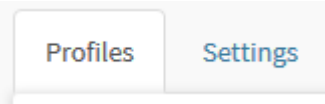
- *Profiles*;
- *Settings*;

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"*.



Aba *Profiles*

Surgirá a tela *a seguir*, conforme demonstrado pela imagem abaixo:

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*.

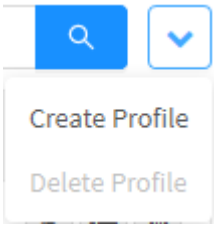
A seguir, analisaremos as funções localizadas no topo deste painel.

SD-WAN - Profiles - Menu de ações

No topo direito da tela temos o menu de ações:

SD-WAN – Botão do Menu de ações

Ao clicar neste botão o menu abaixo é exibido:



SD-WAN – Menu de ações

O menu é composto das seguintes opções:

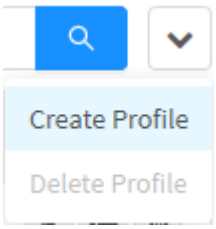
- *Create Profile*;
- *Delete Profile*.

A seguir cada opção do menu de ações será detalhada.

SD-WAN - Profiles - Menu de Ações - Create Profile

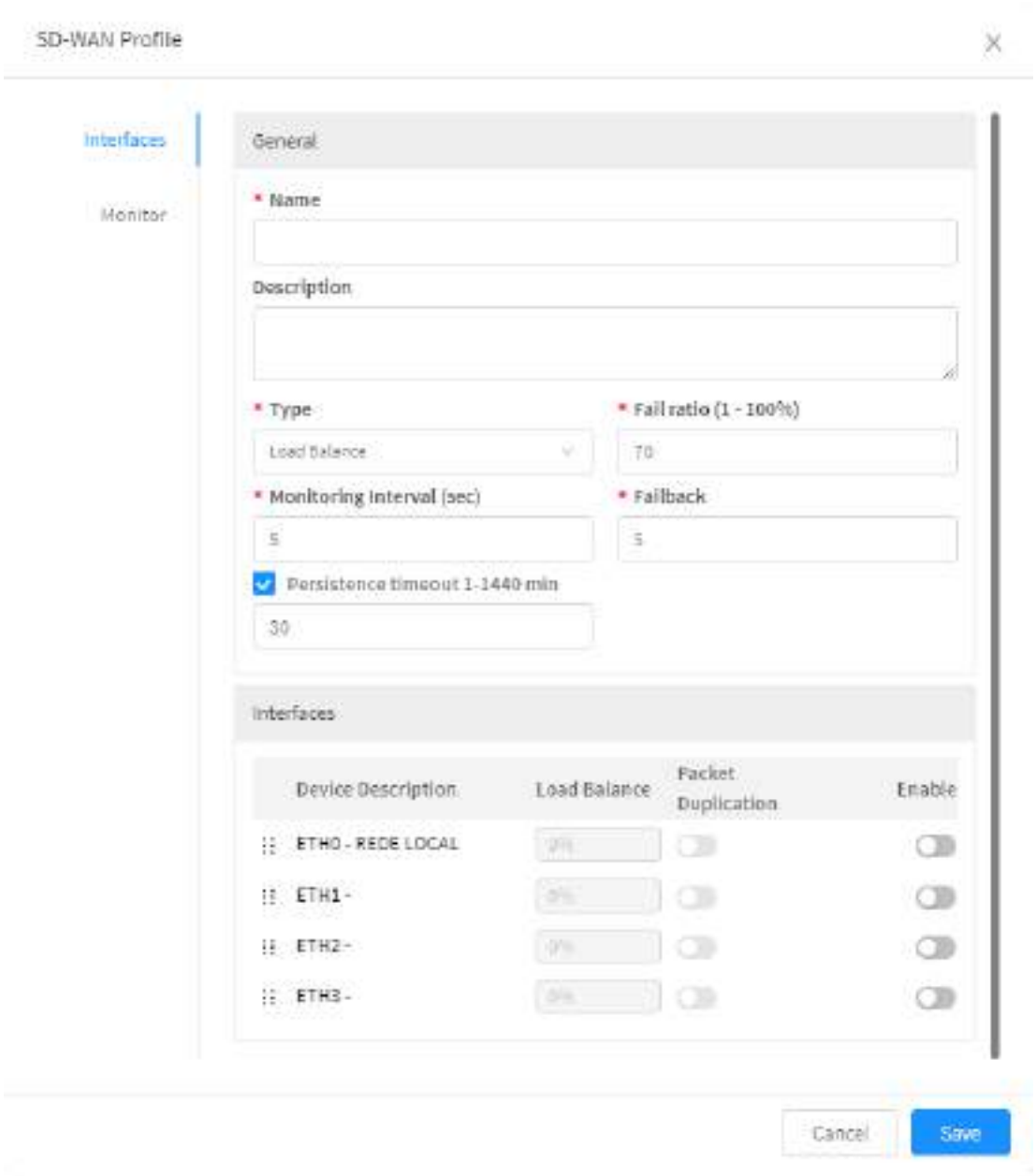
Através da opção “*Create Profile*” é possível criar um novo perfil de SD-WAN. Para acessar, clique no **Menu de ações [ ]**.

1. Clique na opção “*Create Profile*”;



SD-WAN - Create Profile

2. A tela demonstrada abaixo será exibida:

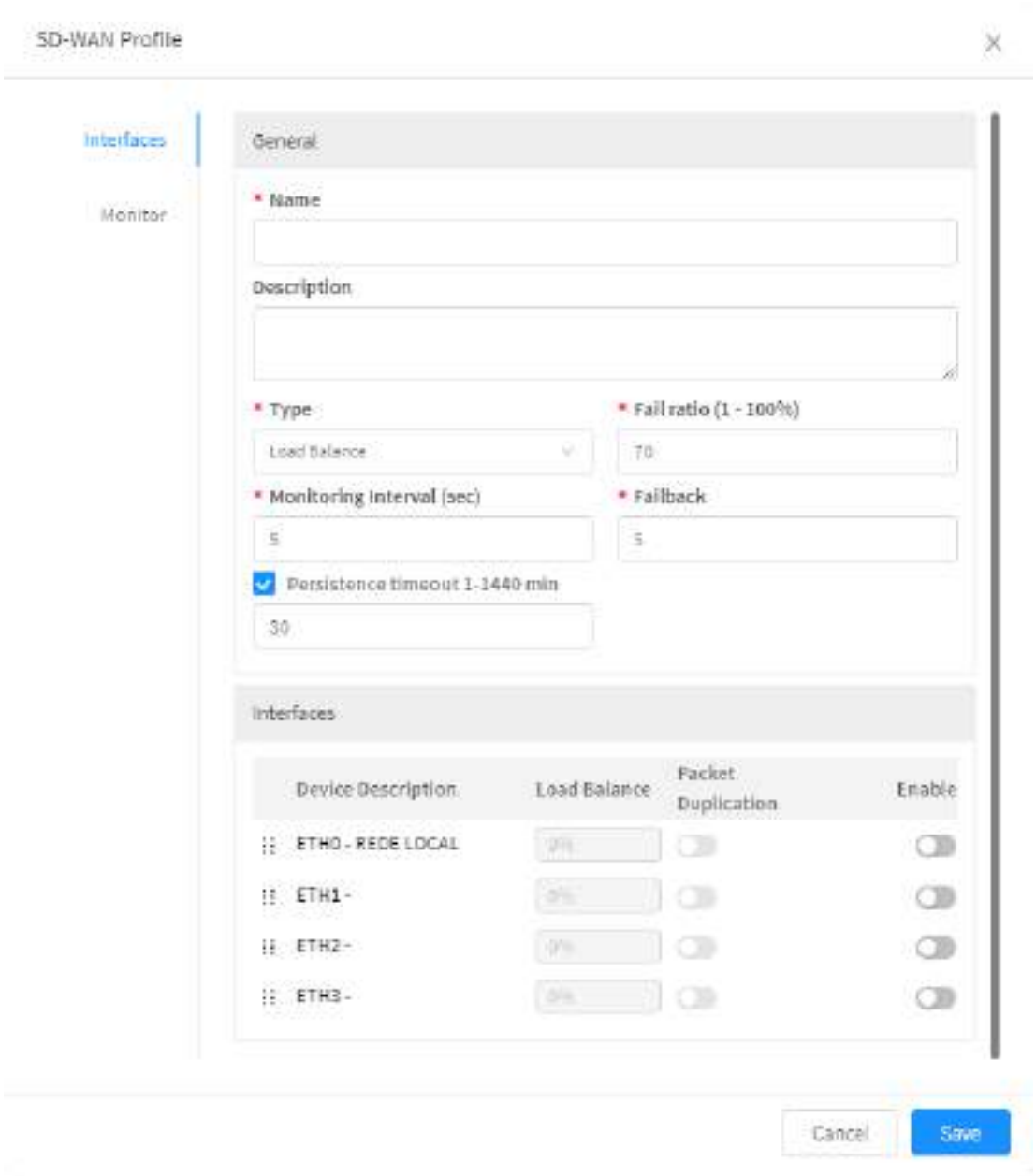


SD-WAN - Profile

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

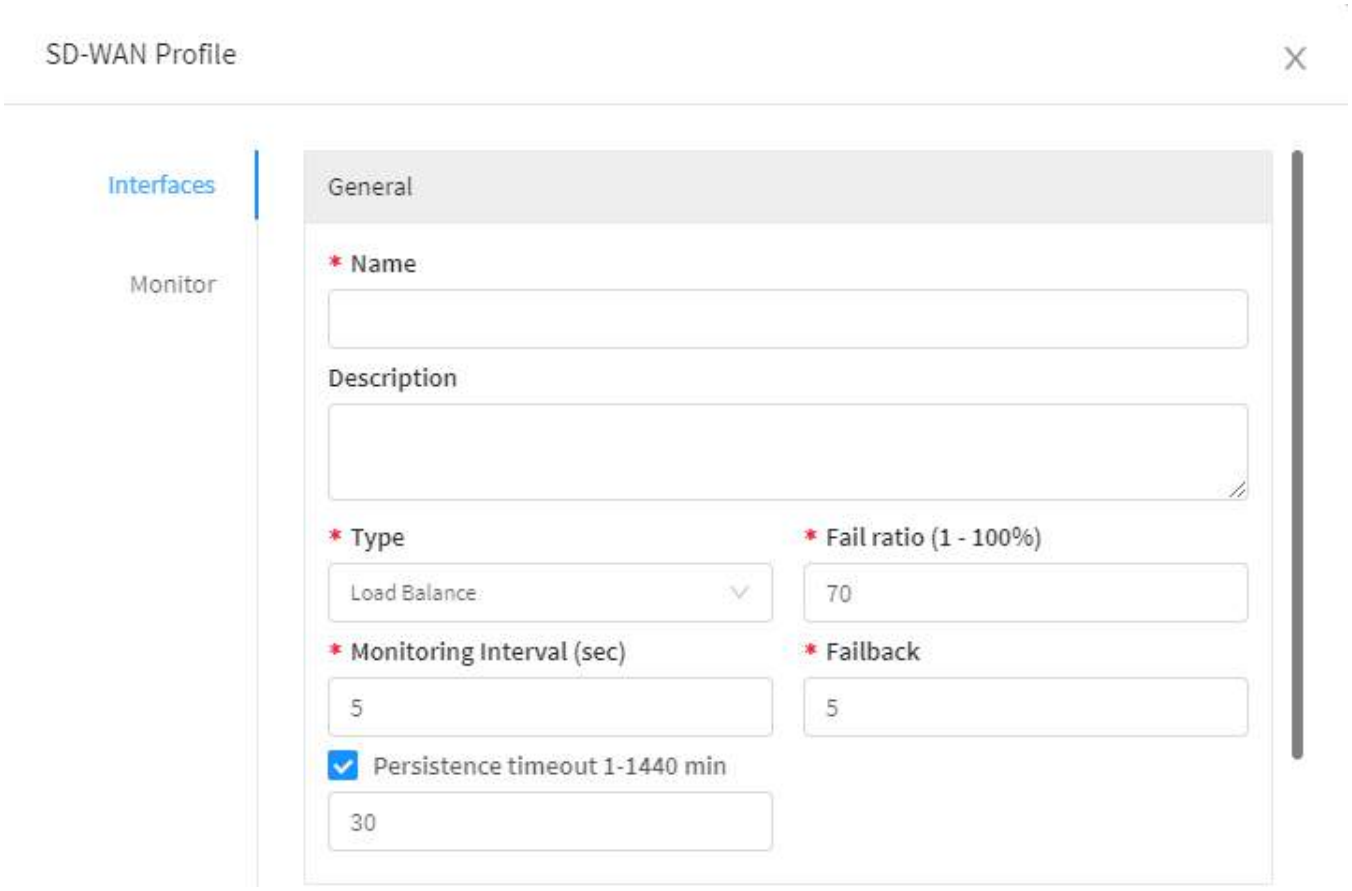
Nesta aba é possível configurar como o *SD-WAN* irá interagir com as interfaces *eth*.



SD-WAN – SD-WAN Profile - Aba *Interfaces*

Painel *General*

Em "*General*" temos as seguintes caixas de texto:

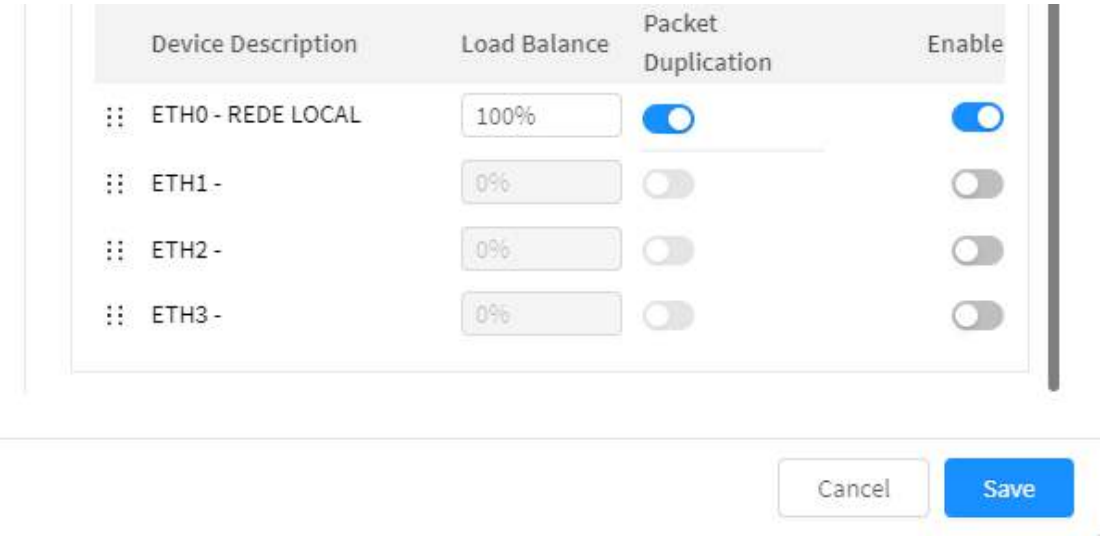


SD-WAN – General

- ***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:



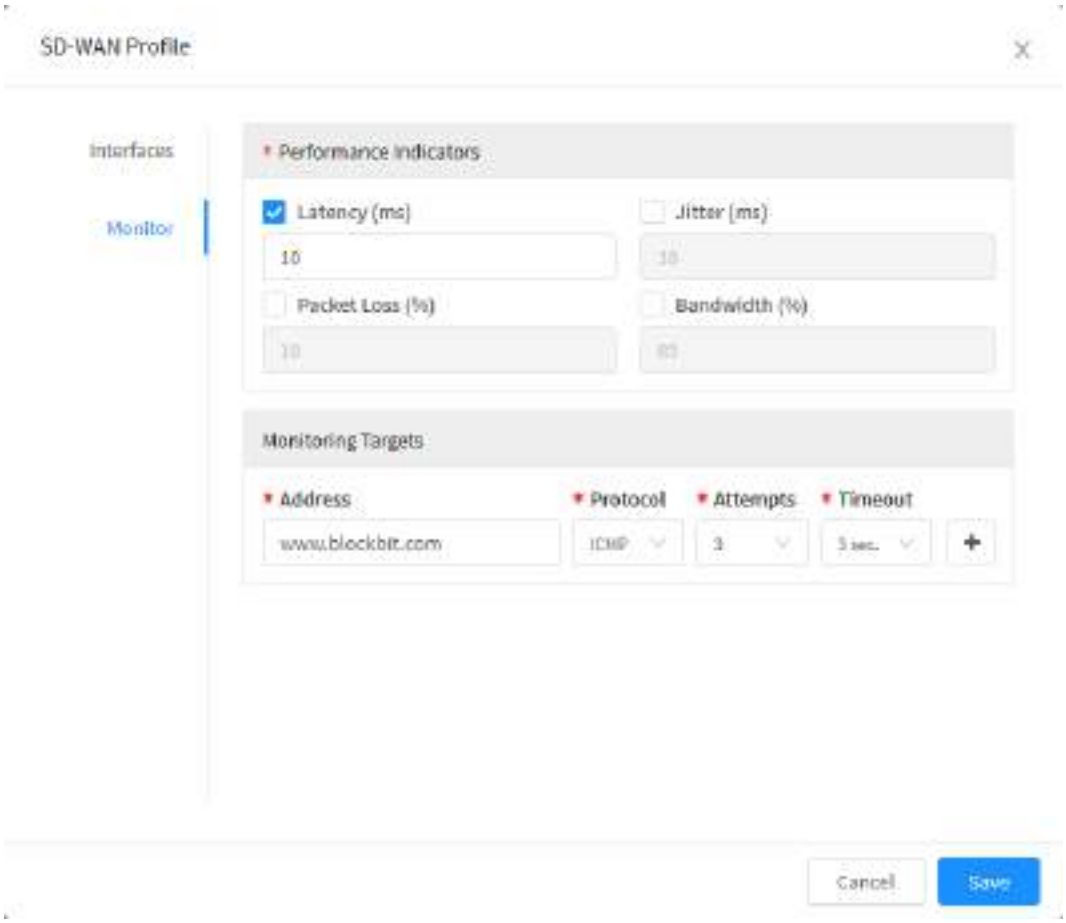
SD-WAN – Interfaces

Só é possível interagir com as interfaces que tiverem sido **habilitadas [ ]** caso uma interface estiver **desabilitada [ ]**, ela ficará esmaecida, não será possível editá-la e será desconsiderada.

- **Mover[ ]:** 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 automaticamente 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

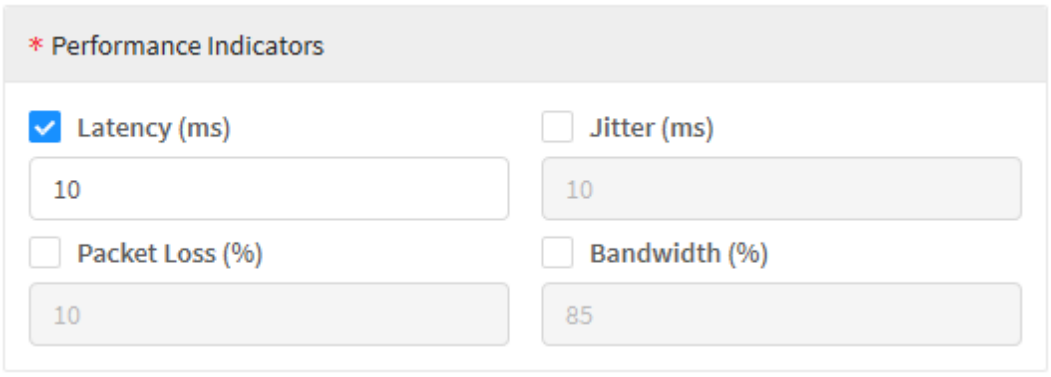
Nesta aba são configurados os indicadores de performance e alvos de monitoramento, utilizados pelo *SD-WAN*.



SD-WAN – SD-WAN Profile - Aba *Monitor*

Painel *Performance Indicators*

Em "*Performance Indicators*" temos as seguintes caixas de texto:

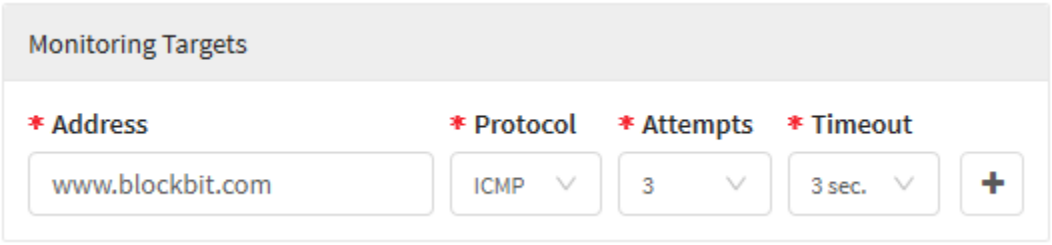


SD-WAN – SD-WAN Profile - Performance Indicators

- ***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%.

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 deseje cancelar clique no botão ***Cancel***[Cancel]. Para concluir a edição das aplicações clique no botão ***Save***[Save].

Para mais informações a respeito das particularidades e diferenças de cada tipo de perfil, cheque esta página.

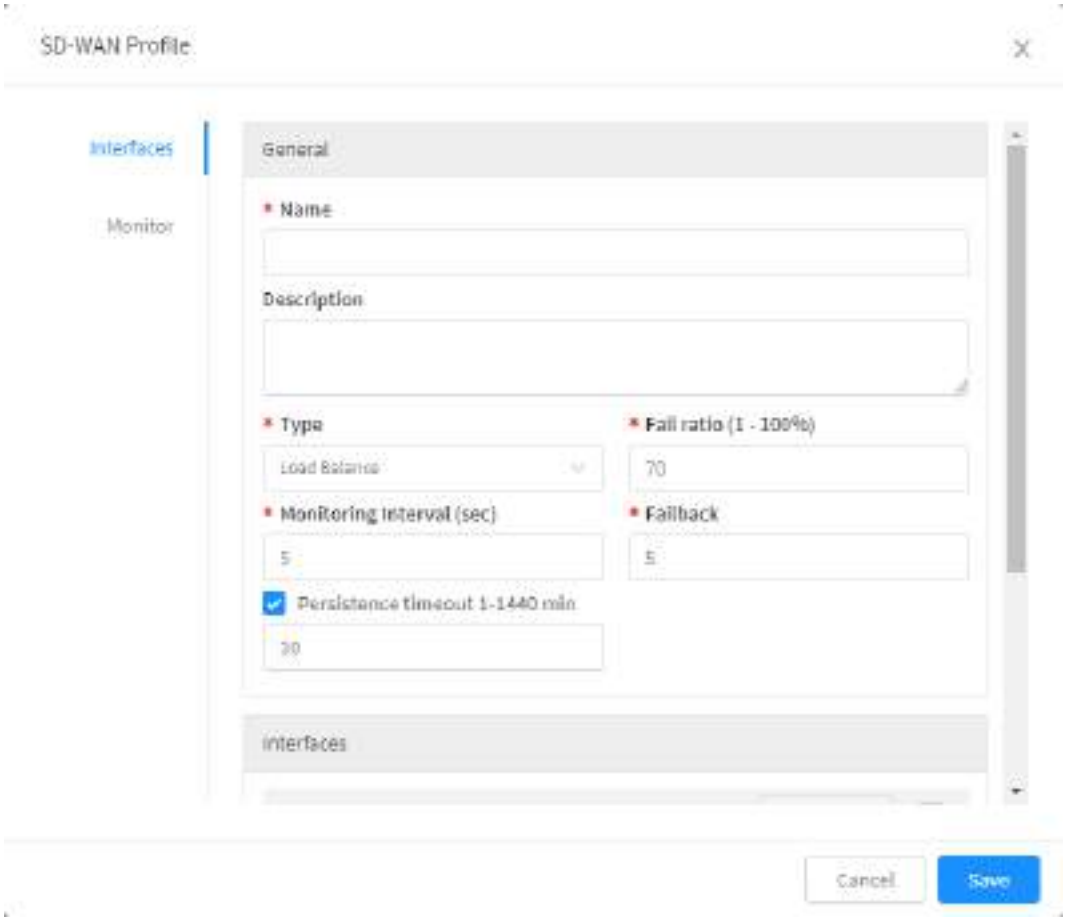
Para um exemplo de como configurar um perfil de *SD-WAN*, cheque esta página.

SD-WAN - Tipos de Perfil

Nas páginas a seguir iremos analisar a fundo cada particularidade dos modos de operação do SD-WAN.

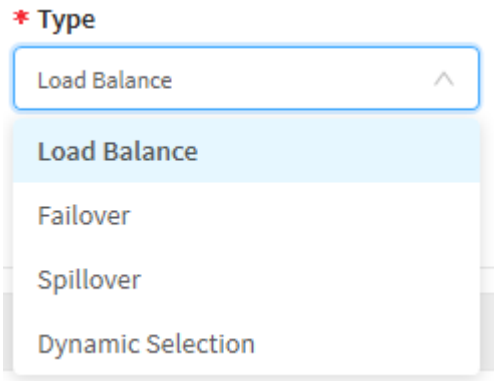
O *SD-WAN* contempla 4 modos de operação diferentes, para determinar qual deles será utilizado no perfil, siga as instruções abaixo:

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.



SD-WAN – Add profile.

2. Para determinar o modo de operação do *SD-WAN*, clique na caixa de seleção "*Type*" e determine a opção desejada



SD-WAN - Type

Conforme, demonstrado na imagem acima, o SD-WAN contempla os seguintes modos de operação:

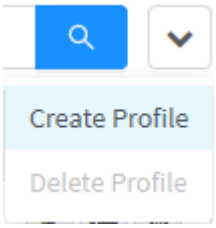
- *Load Balance*;
- *Failover*;
- *Spillover*;
- *Dynamic Selection*.

A analisaremos as distinções entre cada um destes tipos.

SD-WAN - Load balance

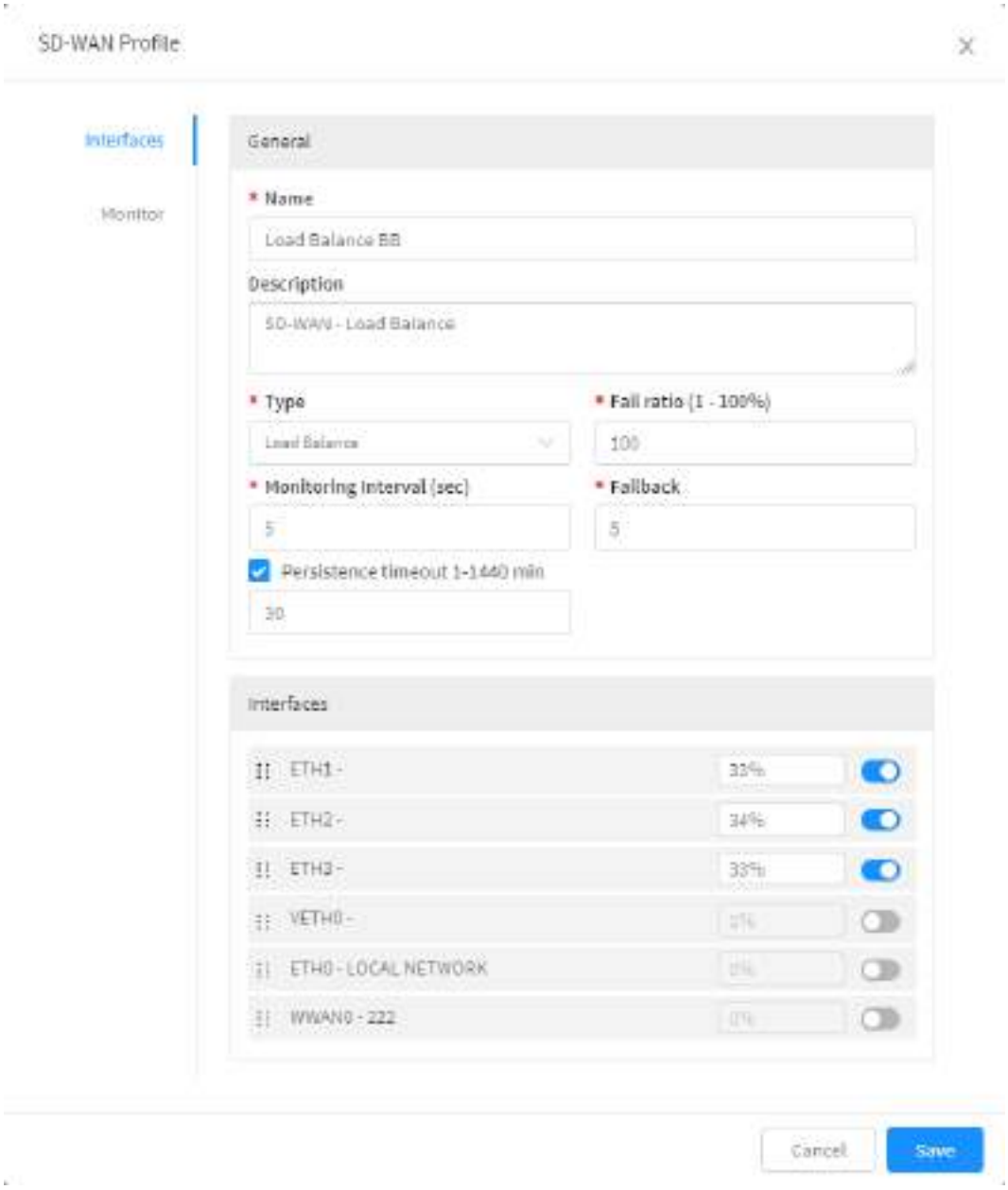
Utilizando-se do *Load balance*, é possível balancear através de % as novas conexões dessa forma redirecionado o tráfego de acordo com a % definida para cada *link* a fim de otimizar a utilização de recursos, maximizar o desempenho, minimizando o tempo de resposta evitando a sobrecarga de um determinado *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

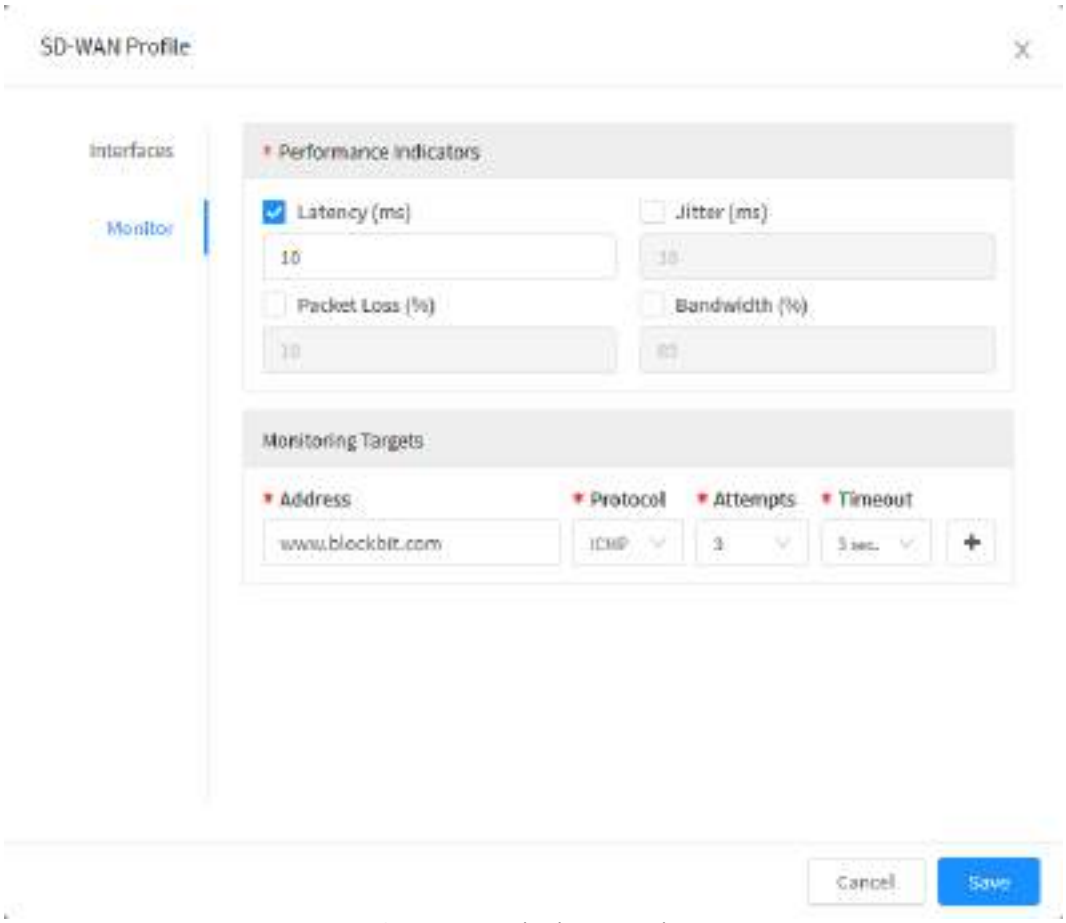
2. A tela demonstrada abaixo será exibida:



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* [☑]:** 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*":



SD-WAN – Load Balance - Monitor

4. Adicione os indicadores de performance e os alvos de monitoramento que desejar.

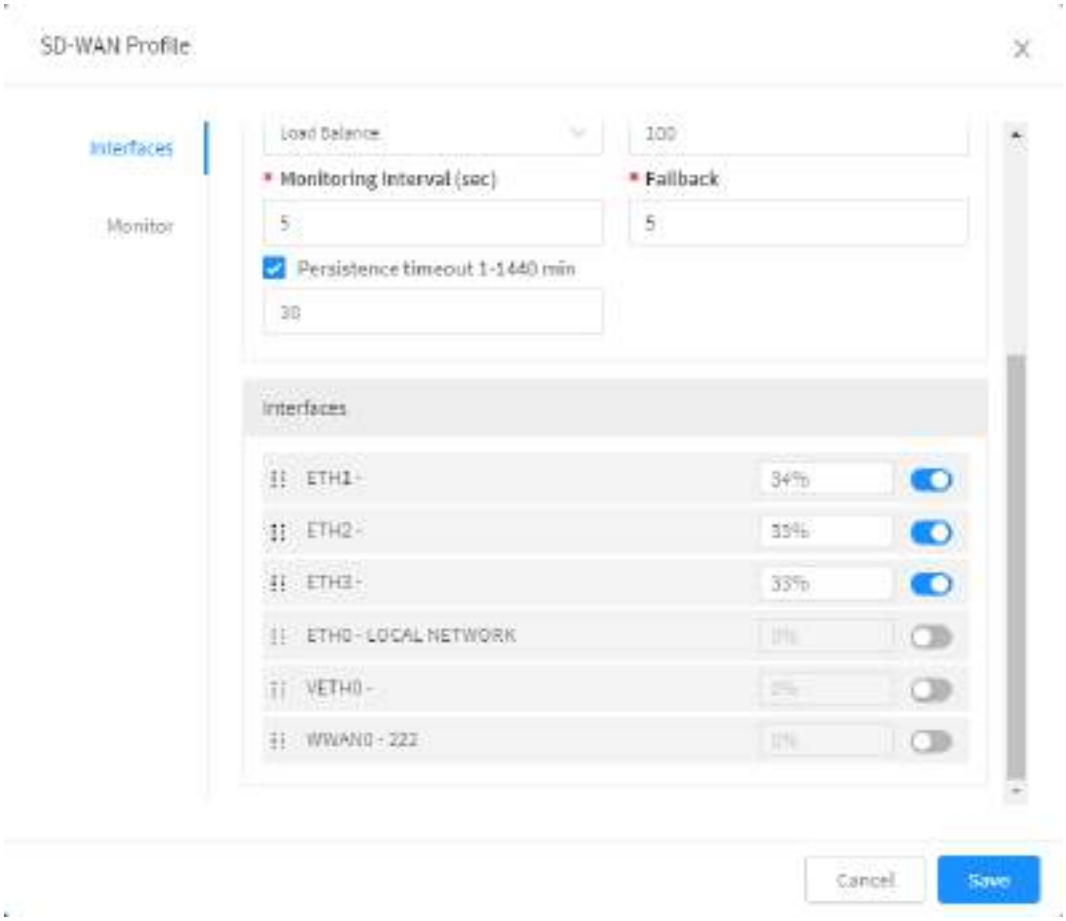
Após todos os campos devidamente preenchido clicar no botão **[** Save **]**;

SD-WAN – Profiles

Por fim, após salvar, para que o *SD-WAN* entre em ação será necessário acessar a **fila de comandos [** 1 **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

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.



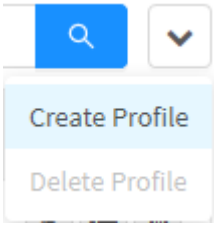
SD-WAN – Edit profile – Load Balance

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 online* 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

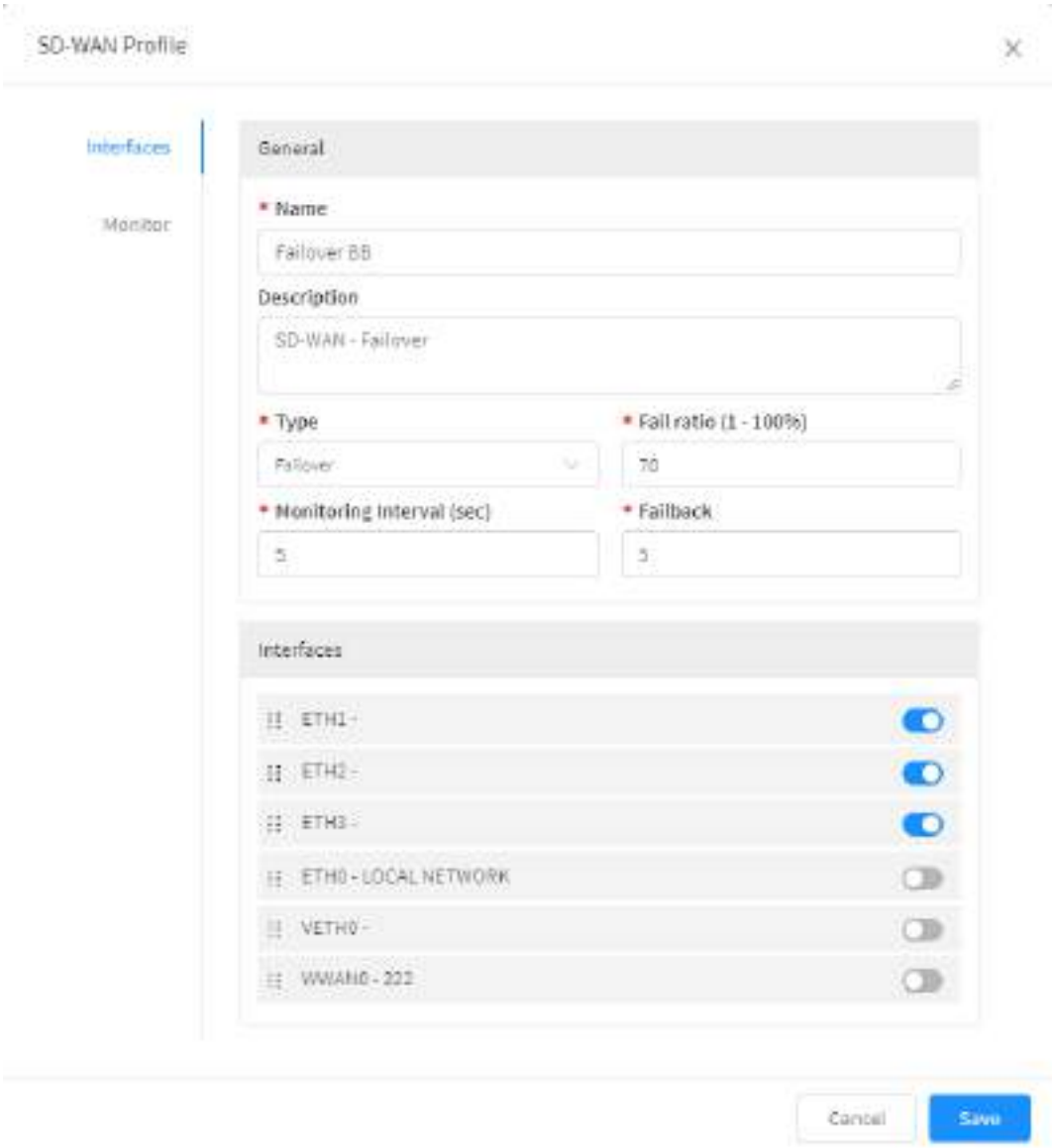
Failover monitora ativamente os *links* de *internet* e age conforme a falha, sendo capaz de aplicar testes de disponibilidade do *link* em tempo real, dessa forma definindo uma rota alternativa em caso de falha do *link* principal e restabelecimento automático do roteamento dos *links*.

1. Para acessar, clique no **Menu de ações [ ]** e selecione a opção “*Create Profile*”;



SD-WAN - Create Profile

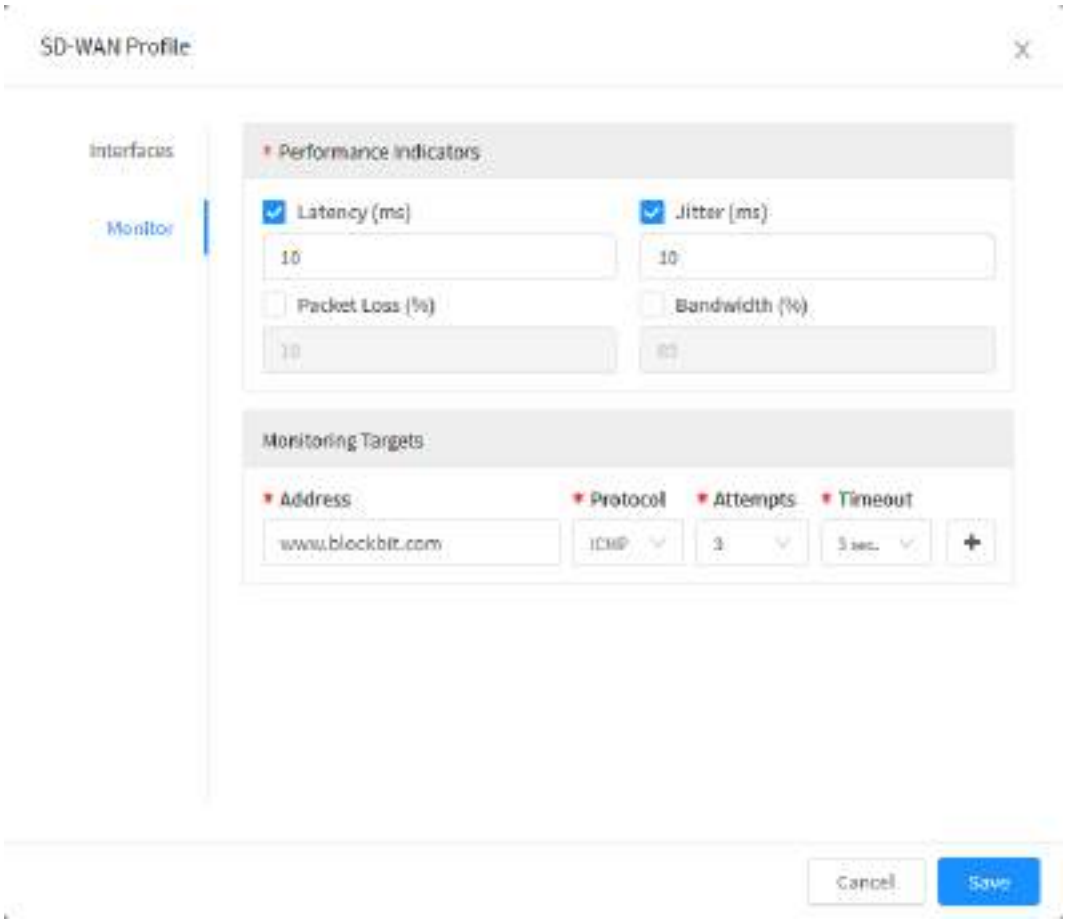
2. A tela demonstrada abaixo será exibida:



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 *internet* que serão usados na composição do perfil. Ex.: eth1, eth2, eth3;

3. Acesse a aba "*Monitor*":



SD-WAN – Failover - Monitor

4. Adicione os indicadores de performance e os alvos de monitoramento que desejar.

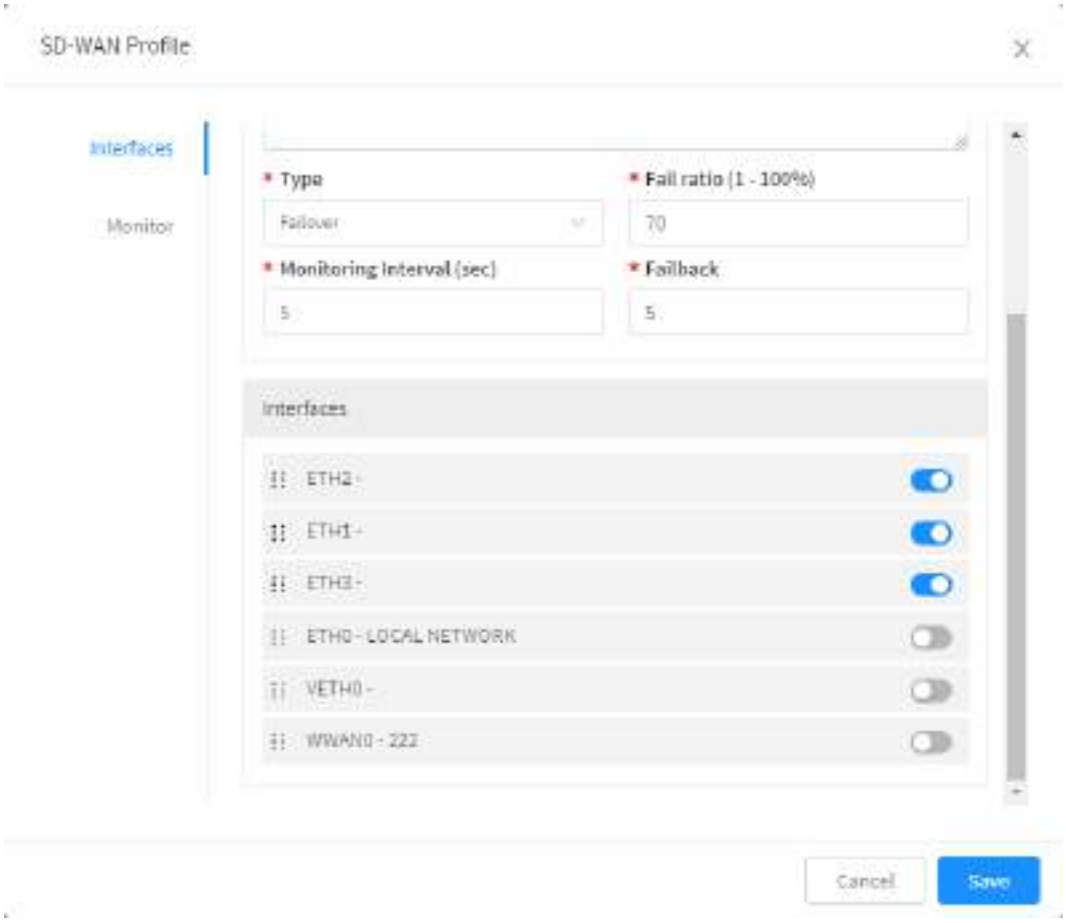
Após todos os campos devidamente preenchido clicar no botão **[** Save **]**;

SD-WAN – Profiles

Por fim, após salvar, para que o *SD-WAN* 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.

Após realizar esses procedimentos o *SD-WAN Failover* terá sido configurado com sucesso.

Ao editar o perfil cadastrado é possível visualizar o *status* do *link* conforme exibido na tela abaixo.



SD-WAN – Edit profile

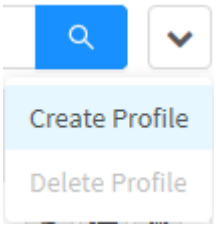
O sistema no módulo *failover* irá redirecionar os pacotes para o primeiro *link* online da lista, é possível ordenar os *links* clicando em **[⋮⋮]** e arrastando para posição desejada, dessa forma o *link* que estiver na primeira posição de cima para baixo será o *link* usado para saída do tráfego, 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 automaticamente irá retornar a saída para o primeiro *link* da lista.

As notificações de “falhas e restabelecimento dos *links*”, e do “restabelecimento automático do roteamento” são disparadas automaticamente em tempo real e podem ser visualizadas através da interface *WEB* clicando no ícone *[6]* ou por *e-mail.*

SD-WAN - Spillover

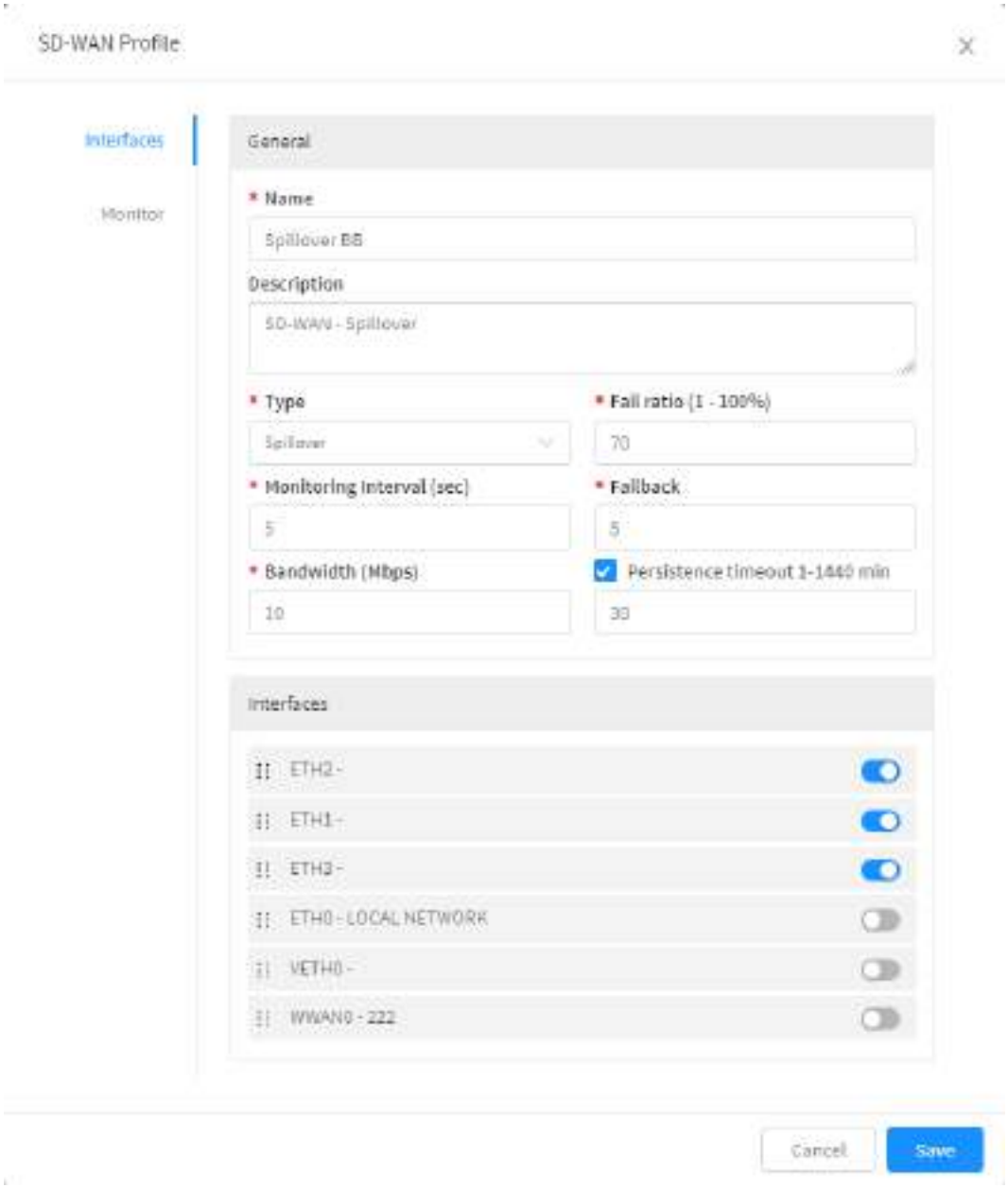
O *Spillover* consiste em um processo de transbordamento de tráfego baseado no limite da largura de banda configurado. Quando a banda excede o *band width* do *link* da primeira interface configurada com *status online* no perfil novos fluxos de tráfegos são realocados de forma *"Round Robin"* entre 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

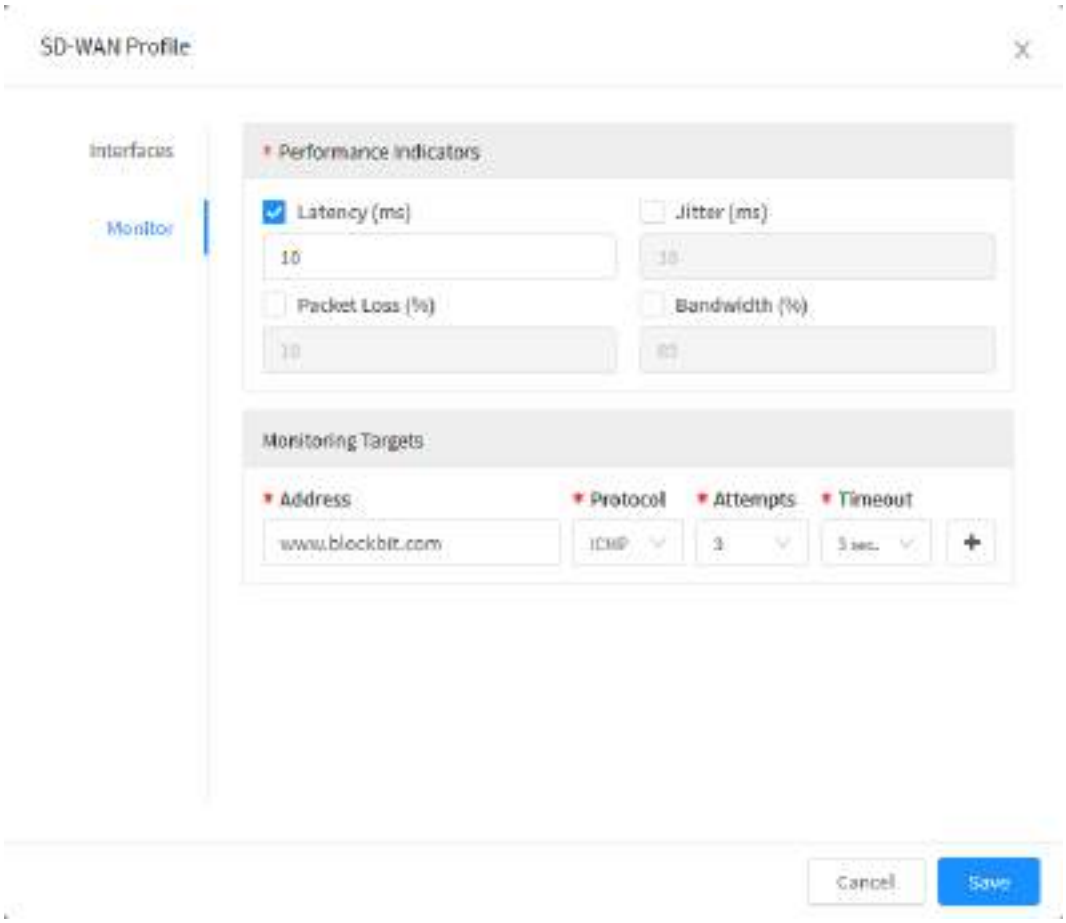
2. A tela demonstrada abaixo será exibida:



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*":



SD-WAN – Spillover - Monitor

4. Adicione os indicadores de performance e os alvos de monitoramento que desejar.

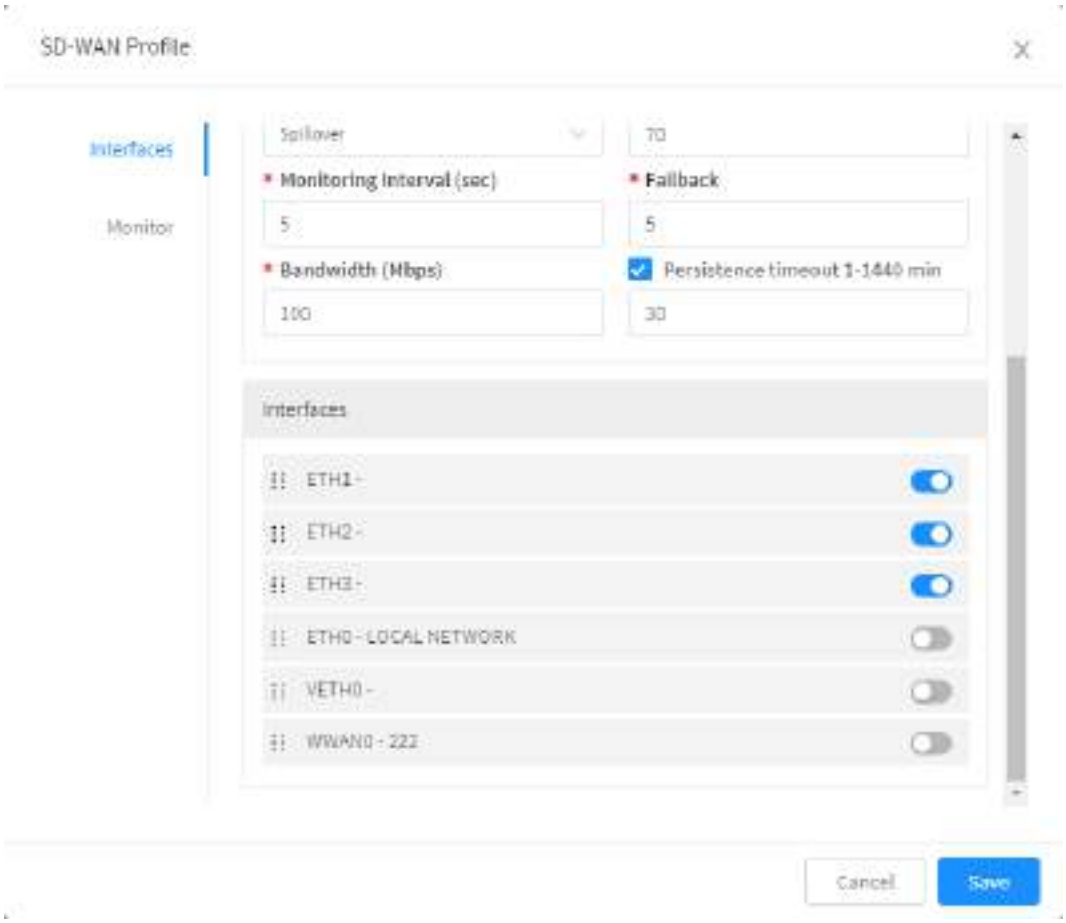
Após todos os campos devidamente preenchido clicar no botão **[** Save **]**;

SD-WAN – Profiles

Por fim, após salvar, para que o *SD-WAN* entre em ação será necessário acessar a **fila de comandos [** 1 **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

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.



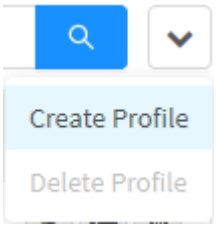
SD-WAN – Edit profile – Spillover Exemplo

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

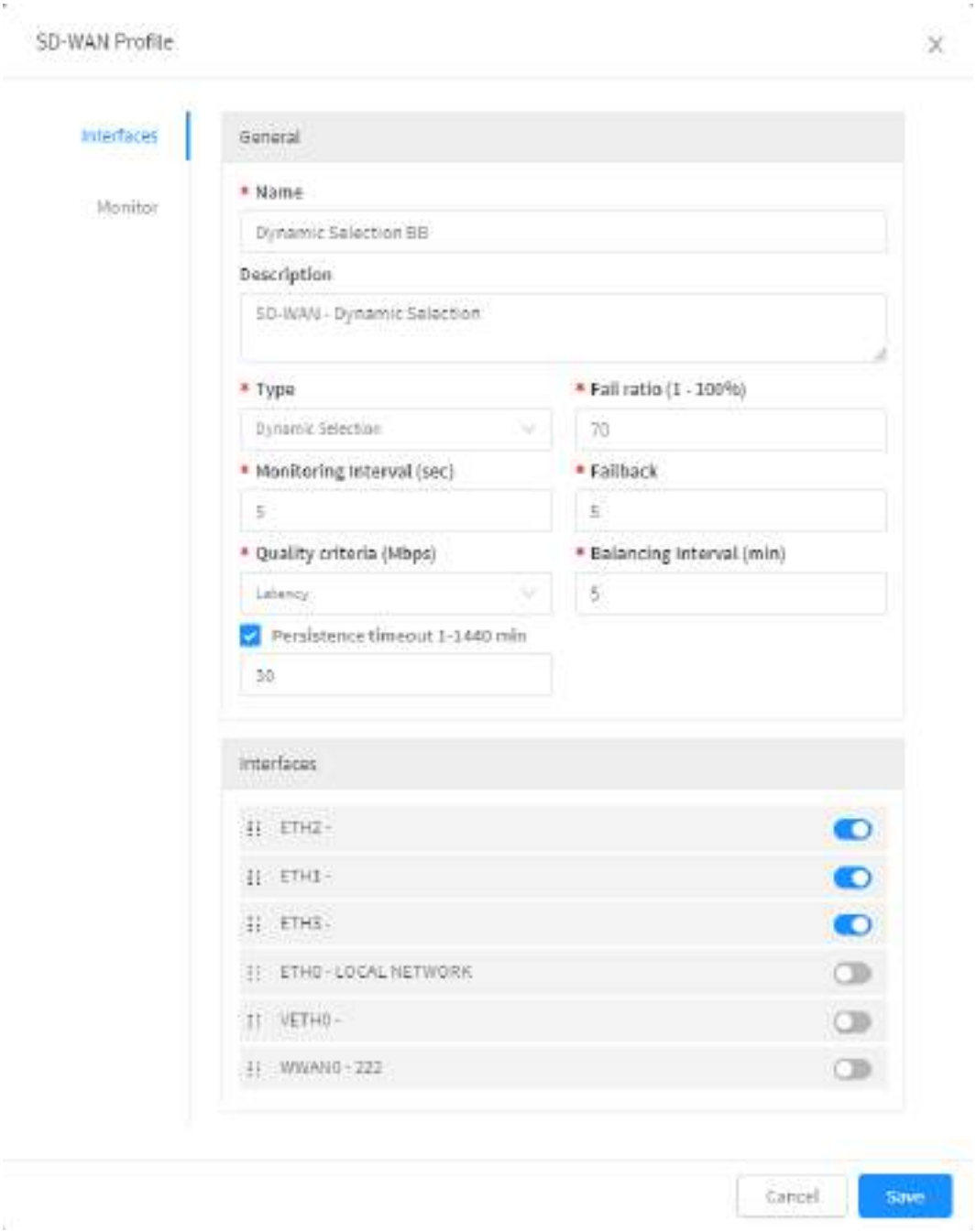
Em *Dynamic Selection* o tráfego é priorizado para o *link* que tiver um resultado melhor frente ao critério de qualidade, assim sendo, novos fluxos serão atribuídos a este mesmo. Assim sendo, o sistema dinamicamente distribui as % entre os *links* com melhor performance tendo como base o indicador de qualidade selecionado.

1. Para acessar, clique no **Menu de ações [ ]** e selecione a opção “*Create Profile*”;



SD-WAN - Create Profile

2. A tela demonstrada abaixo será exibida:



SD-WAN – Dynamic Selection – Interfaces

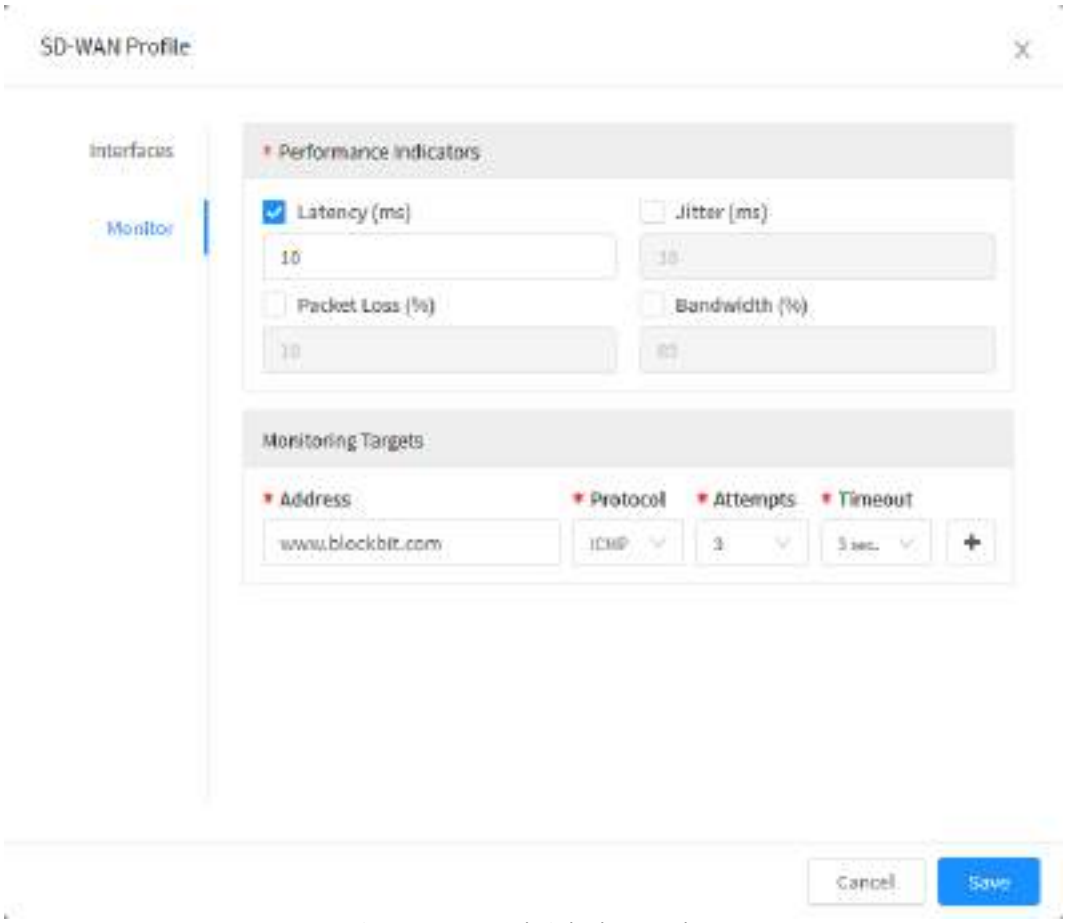
- ***Monitoring interval* (sec.) :** Definir o intervalo de monitoramento entre cada teste. Ex.: 5 segundos;

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 *links* 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%.

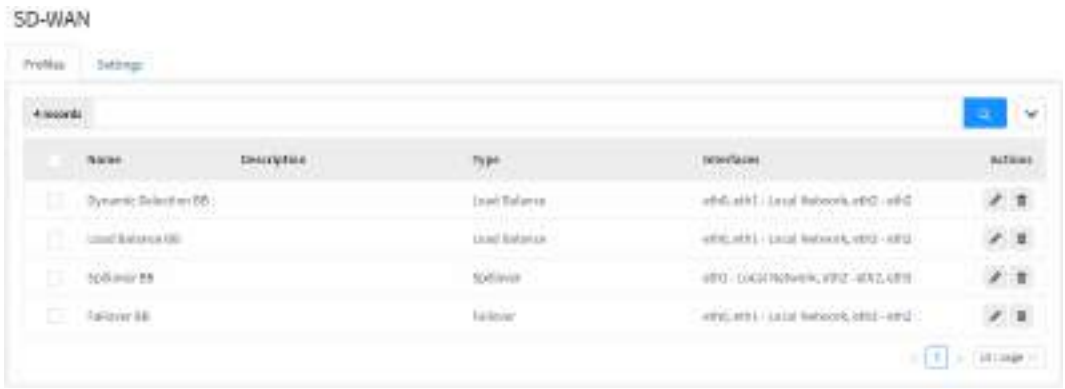
3. Acesse a aba "*Monitor*":



SD-WAN – Dynamic Selection - Monitor

4. Adicione os indicadores de performance e os alvos de monitoramento que desejar (FQDN, IPV4, IPV6).

Após todos os campos devidamente preenchido clicar no botão [Save].



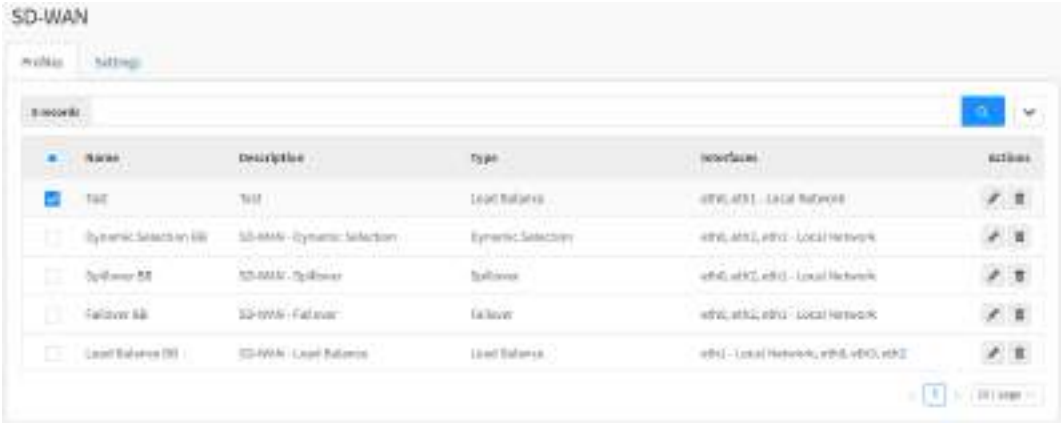
Por fim, após salvar, para que o *SD-WAN* entre em ação será necessário acessar a **fila de comandos [**  **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

Após realizar esses procedimentos o *SD-WAN Dynamic Selection* terá sido configurado com sucesso.

SD-WAN - Profiles - Menu de ações - Delete Profile

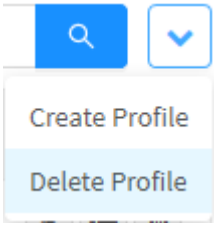
Através do botão “*Delete Profile*” é possível deletar os *Profiles* selecionados. Para deletar pelo menu de ações, siga os seguintes passos:

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 **[ ]**. Ex.: *Test*;



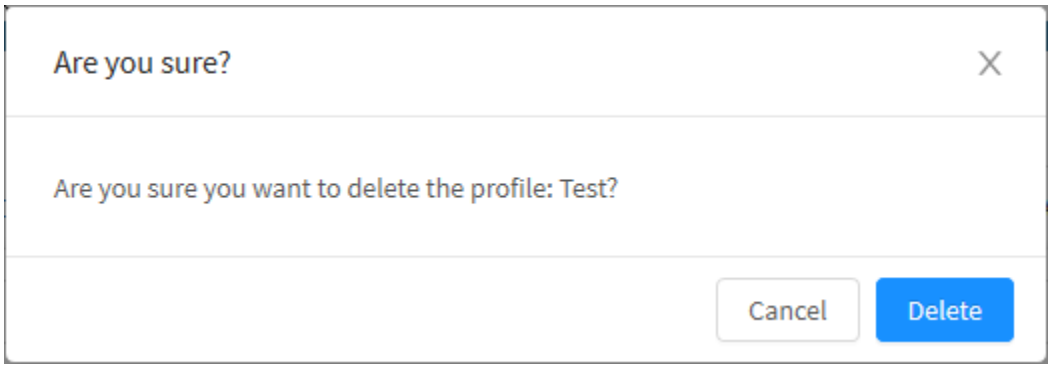
SD-WAN – Seleção dos *Profiles* para deletar

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 p*rofiles* selecionados:



SD-WAN – Mensagem se deseja deletar os *Profiles*

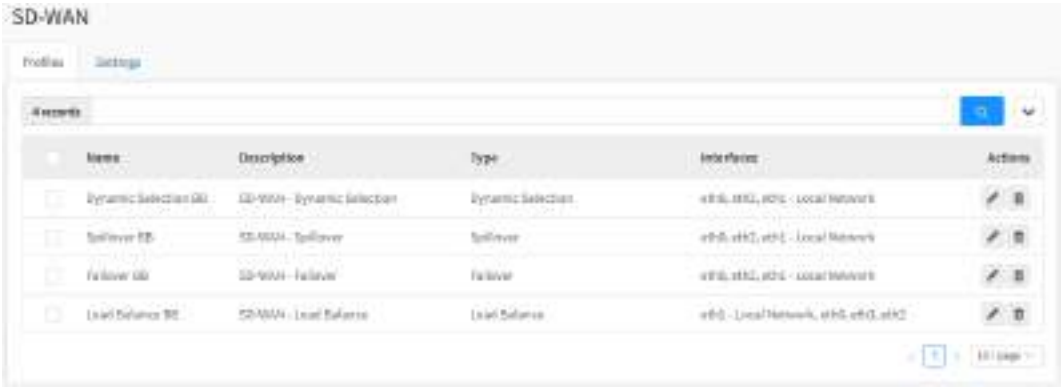
Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].

Profile deleted successfully

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

SD-WAN - Profiles - Colunas

A seguir explicaremos cada coluna da aba *SD-WAN*:



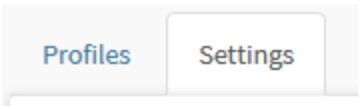
SD-WAN - Profiles

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:
  - **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.

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*".



Aba *Settings*

Surgirá a tela *a seguir*, conforme demonstrado pela imagem abaixo:

SD-WAN - Settings

Esta sessão irá abordar como cadastrar, editar e remover serviços de *SD-WAN*;

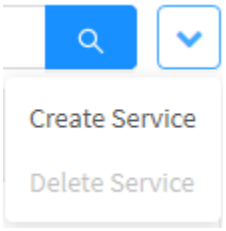
A seguir, analisaremos cada função deste painel.

SD-WAN - Settings - Menu de Ações

No topo direito da tela temos o menu de ações:

SD-WAN – Settings - Botão do 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:

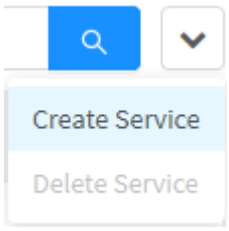
- *Create Service*;
- *Delete Service*.

A seguir cada opção do menu de ações será detalhada.

SD-WAN - Settings - Menu de Ações - Create Service

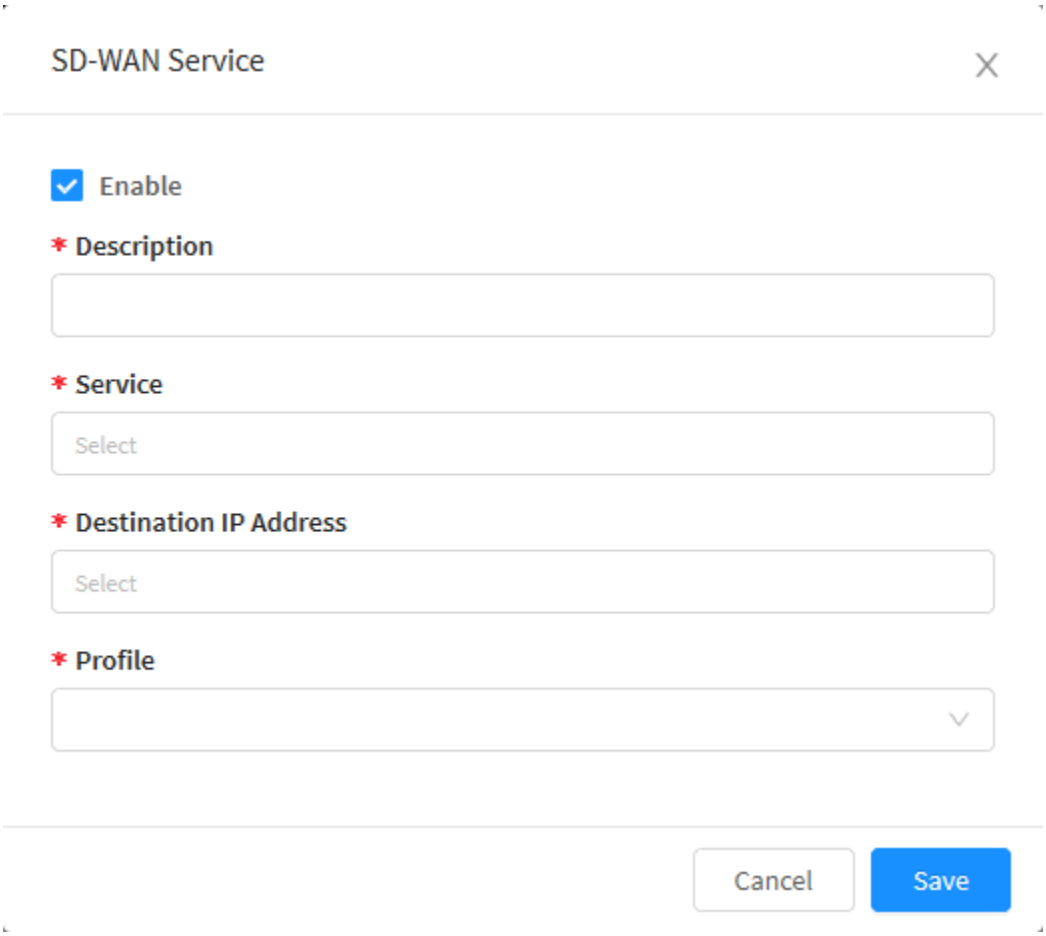
Através da opção “*Create Service*” é possível criar um novo serviço de SD-WAN. Para acessar, clique no **Menu de ações [ ]**.

1. Clique na opção “*Create Service*”;



SD-WAN - Create Service

2. A tela demonstrada abaixo será exibida:

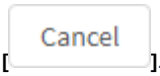


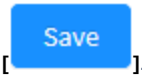
SD-WAN - Service

A seguir demonstraremos como configurar este painel.

- **[ ]*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.

Para cancelar clique no botão **[** 

]. Para concluir a edição das aplicações clique no botão **[** 

].

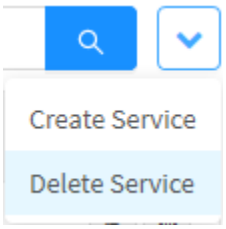
SD-WAN - Settings - Menu de Ações - Delete Service

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*;

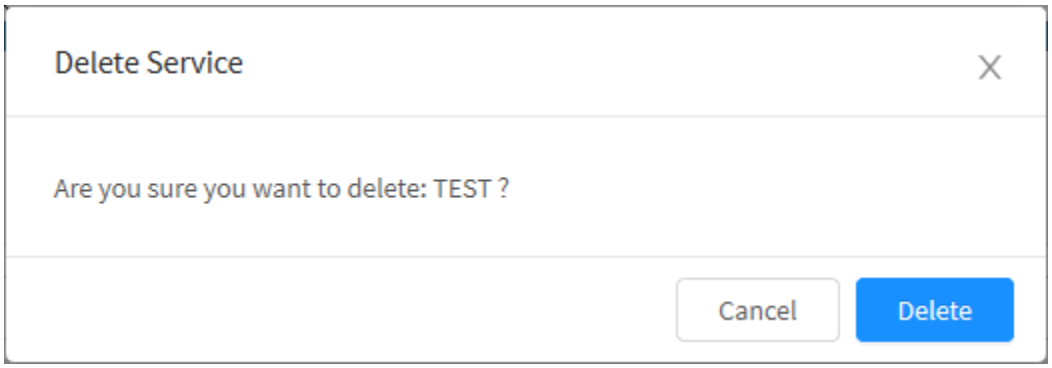
SD-WAN – Seleção dos *Services* para deletar

2. Entre no *Menu Actions* e clique na opção “*Delete Service*”.



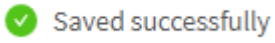
SD-WAN – Delete Service

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



SD-WAN – Mensagem se deseja deletar os *Services*

Caso desejar cancelar clique no botão ***Cancel***[Cancel]. Para concluir, clique no botão ***Delete***[Delete].



Saved successfully

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

SD-WAN - Settings - Colunas

A seguir explicaremos cada coluna da aba *Settings*:

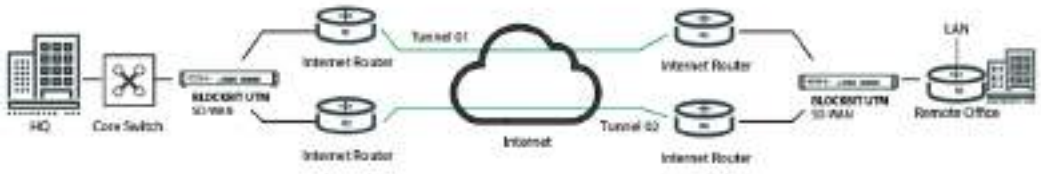
SD-WAN - Settings - Colunas

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;
- ***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:



SD-WAN

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

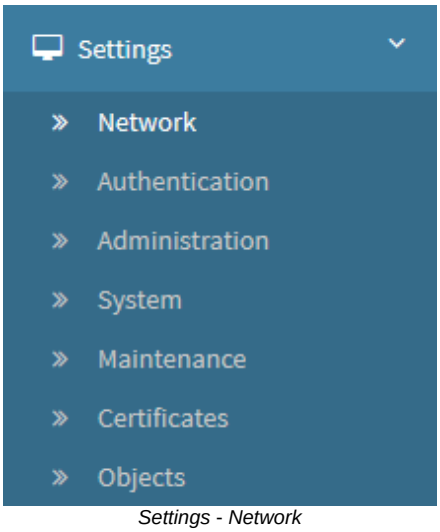
Nome	Endereço *IP LAN*	Endereço *IP* Administração	Endereço *IP Internet*	Endereço *IP* Virtual (TUN)
UTM - *HQ*	172.18.0.0/16	172.31.208.40	10.0.0.2	20.0.0.1
			11.0.0.2	21.0.0.1
UTM - *Remote Office*	172.17.0.0/16	172.31.208.41	100.0.0.2	20.0.0.2
			101.0.0.2	21.0.0.2

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;
2. **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*;
3. **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;
4. **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.

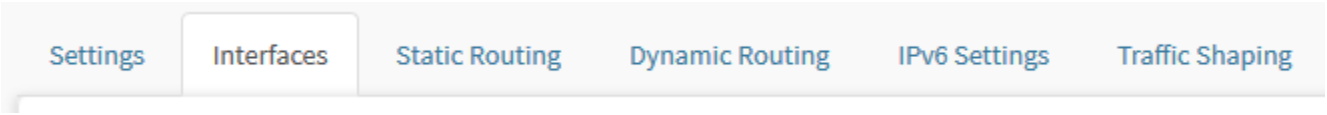
SD-WAN - Configurar Interface Tunnel

Inicialmente, acesse o menu *Settings* a aba *Network:*



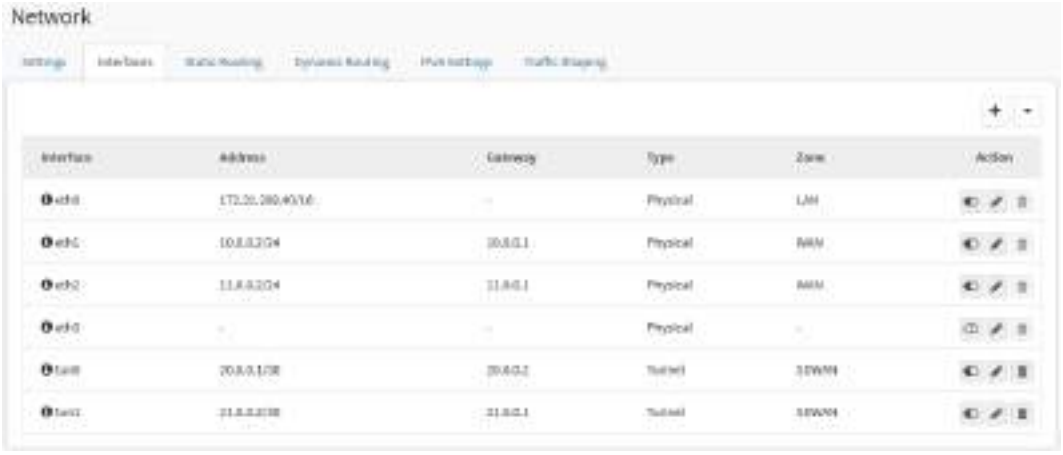
Settings - Network

Por fim, clique na aba *Interfaces*:



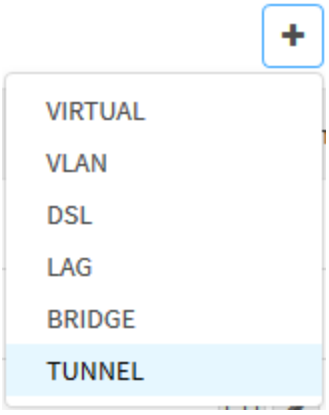
Aba *Interfaces*

Abaixo seguem as configurações do *UTM – HQ*:



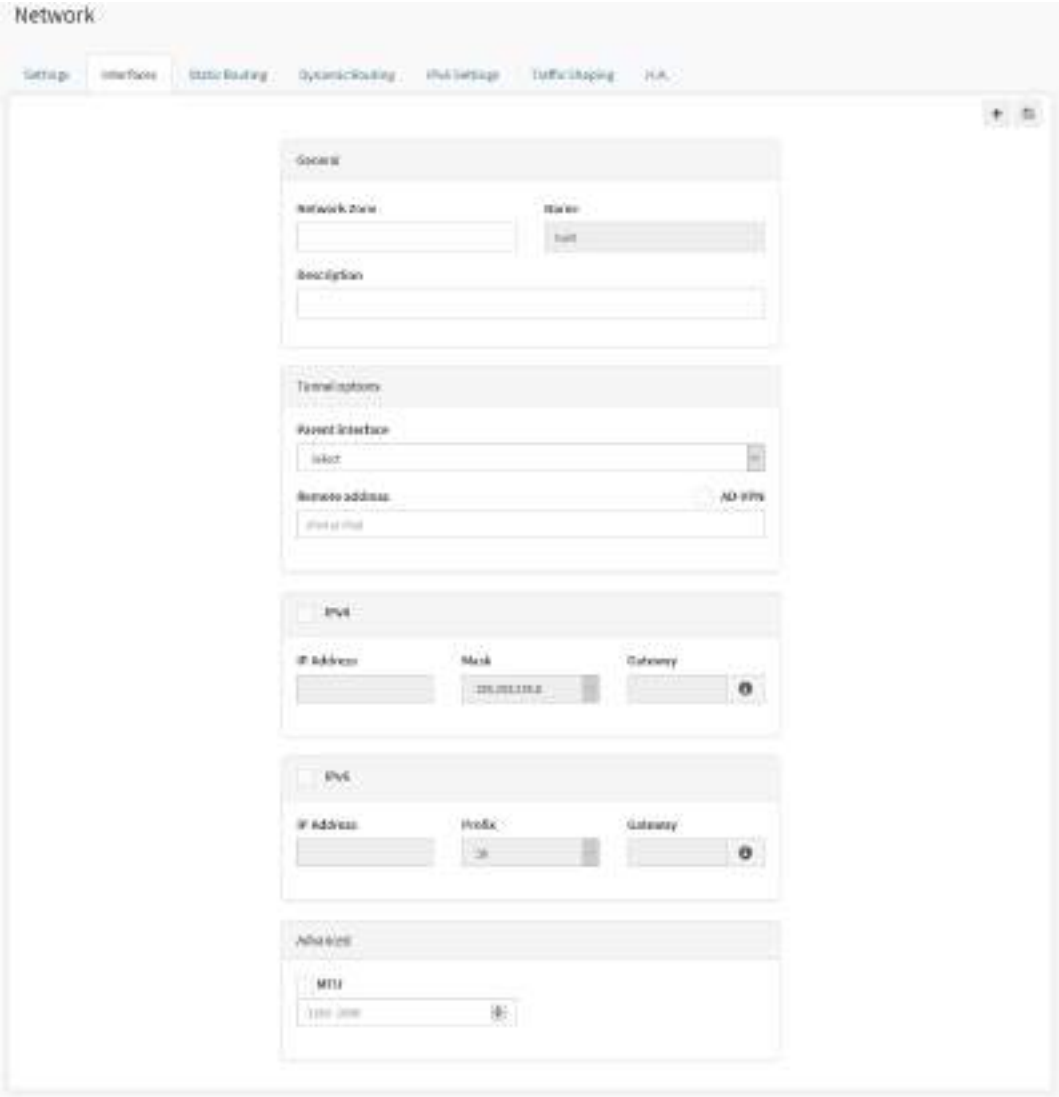
Network - Interfaces

Para criar interfaces *TUNNEL*, clique em ***Add*[ ]** e selecione a opção *TUNNEL*.



Interfaces - Add Tunnel

A seguinte tela será exibida:

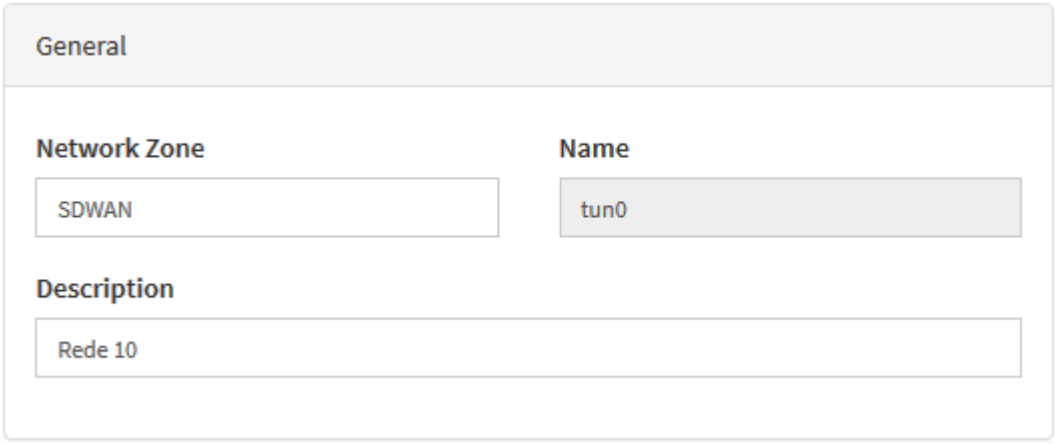


Interfaces – Network

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:



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

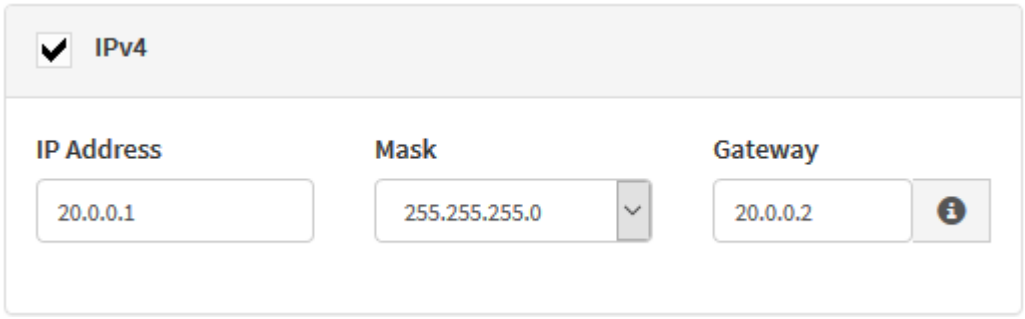
Complete o formulário conforme exemplificado a seguir:

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);

IPv4

Complete o formulário conforme exemplificado a seguir:



Interfaces – IPv4

- ***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*[ ]** para gravar as configurações feitas.

Após estes passos, devemos ter chego no resultado demonstrado pela imagem abaixo:

General

Network Zone

SDWAN

Name

tun0

Description

Network 10

Tunnel options

Parent interface

eth1

Remote address

100.0.0.2

AD-VPN

IPv4

IP Address

20.0.0.1

Mask

255.255.255.252

Gateway

20.0.0.2

IPv6

IP Address

Prefix

36

Gateway

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:

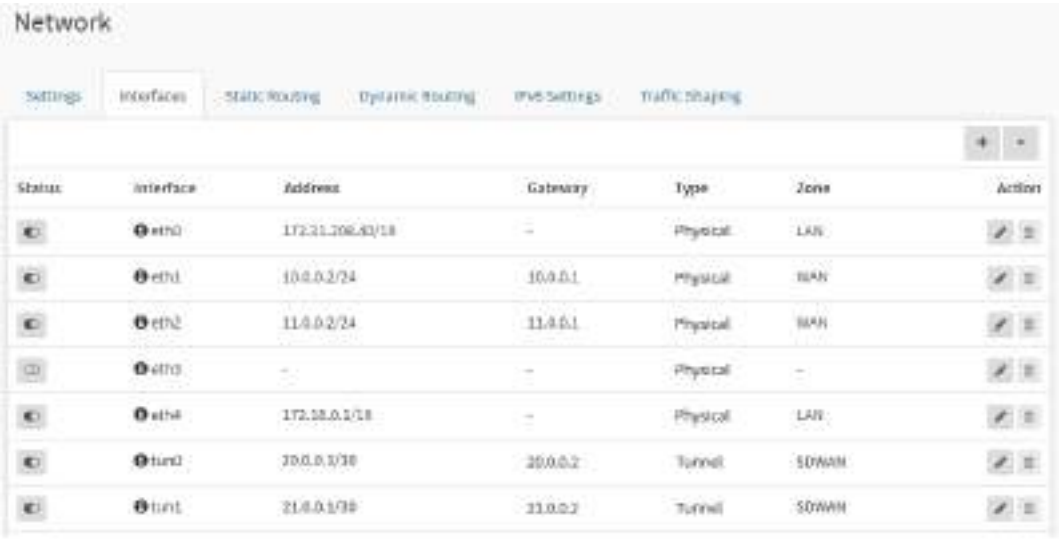
Opções do Túnel

- ***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:



Interfaces – Configurações da Rede

Abaixo seguem as configurações da interface tun0 do *UTM – Remote Office*:

General

Network Zone

SDWAN

Name

tun0

Description

Network 100

Opções do túnel

Parent interface

eth1

Remote address

AD-VPN

100.0.0.2

IPv4

IP Address

20.0.0.2

Mask

255.255.255.252

Gateway

20.0.0.1

IPv6

IP Address

Prefix

Gateway

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

SDWAN

Name

tun0

Description

Network 101

Opções do túnel

Parent interface

eth2

Remote address

AD-VPN

11.0.0.2

IPv4

IP Address

21.0.0.2

Mask

255.255.255.252

Gateway

21.0.0.1

IPv6

IP Address

Prefix

Gateway

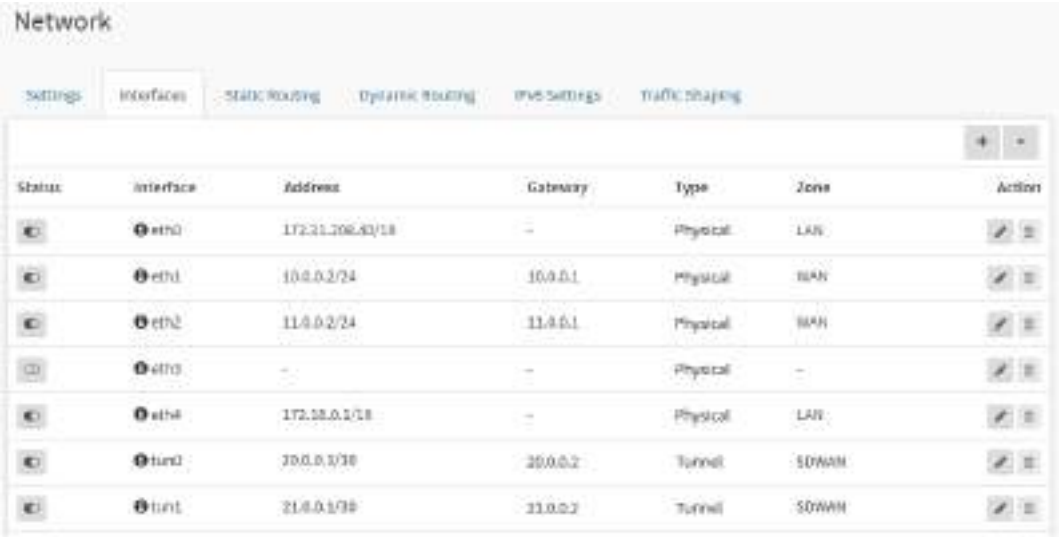
Advanced

MTU

1280 - 9000

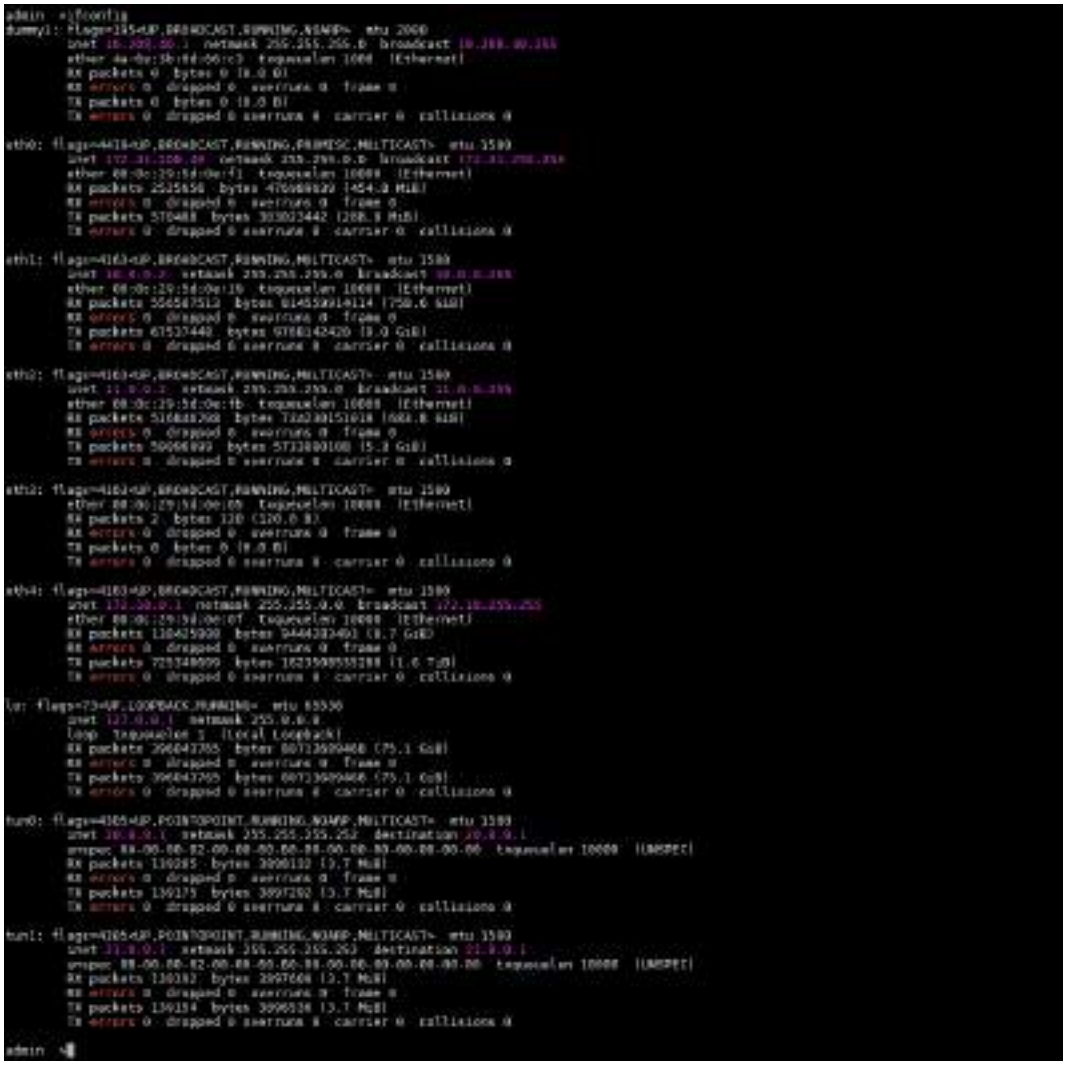
Interfaces – Remote Office - Configurações do tun1

Configurações finais:



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.



CLI - ifconfig

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

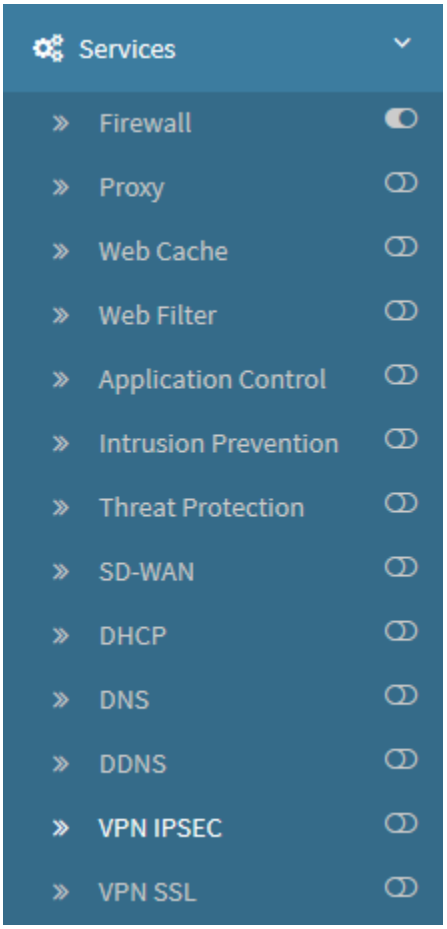
Para mais informações vide o capítulo a respeito de *CLI*.

A seguir, vamos configurar as VPNs.

SD-WAN: Configurar VPN

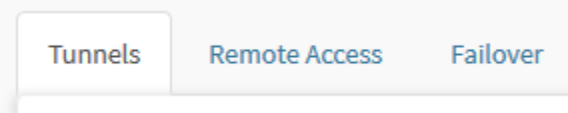
Após ter configurado as interfaces *tunnel*, siga os passos à seguir:

Inicialmente, acesse ***Services*** e clique na opção ***VPN IPSEC***:



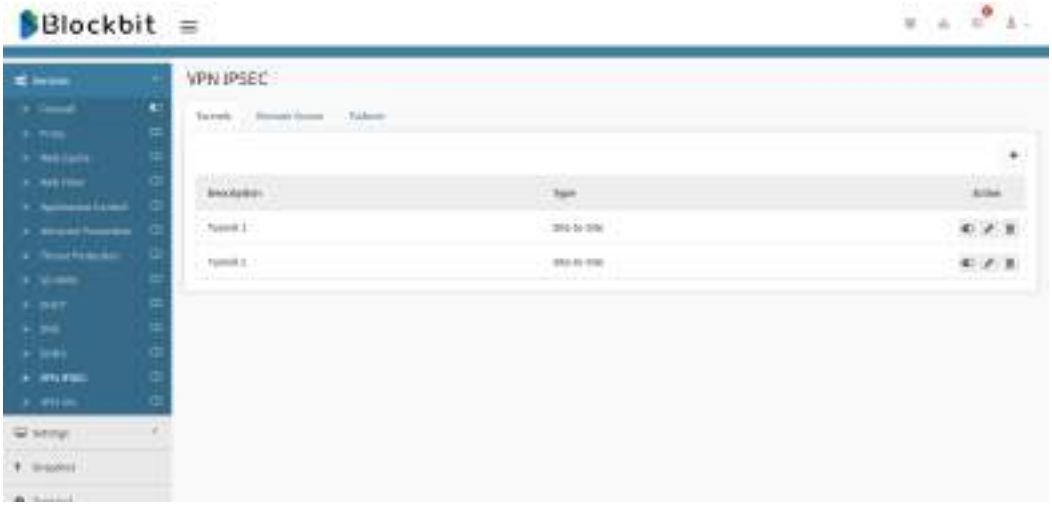
Services - VPN IPSEC

Feito isso, selecione a aba *Tunnels*:



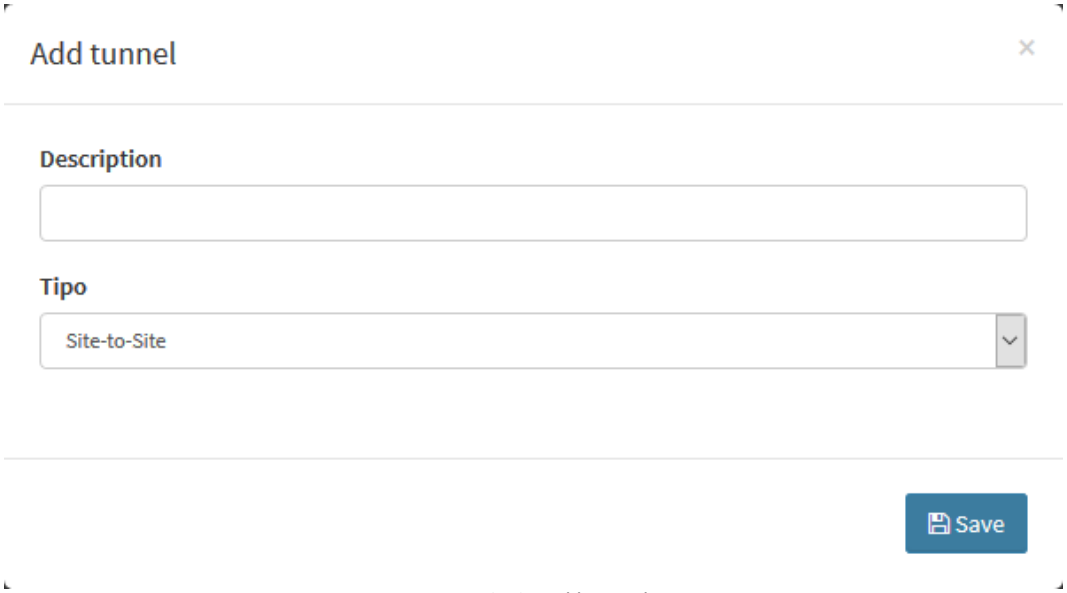
VPN IPSEC - Aba *Tunnels*

A seguinte tela será exibida:



VPN IPSEC - Tunnels

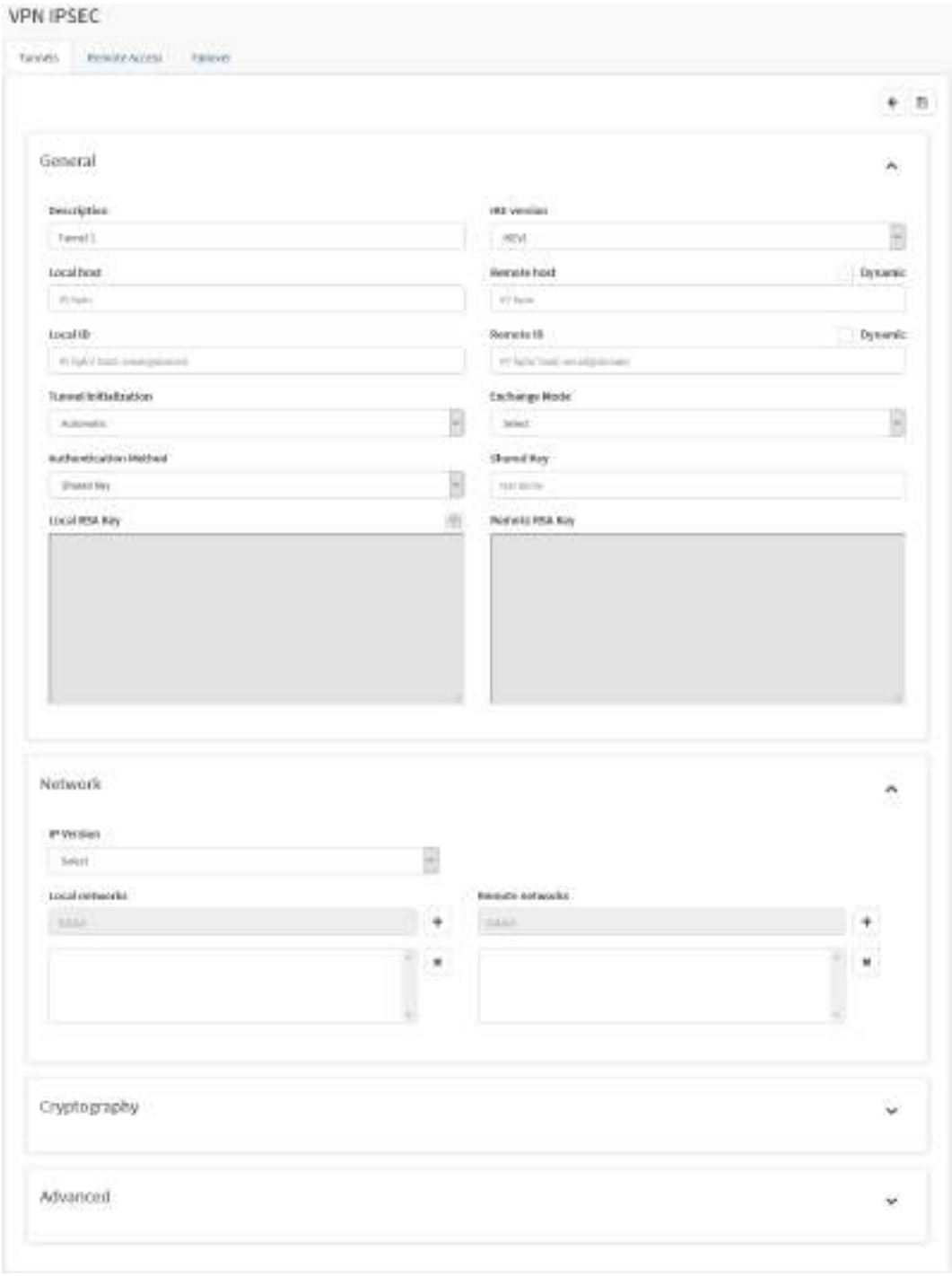
Clique no botão ***Add***[+] para adicionar uma nova *VPN*, a seguinte tela será exibida:



VPN IPSEC - Add Tunnel

- ***Description*****:** *Tunnel 1*;
- **Tipo:** *Site-to-Site.*

Clique em ***Save***[Save] para salvar as alterações e após esse passo, clique no botão ***Edit***[ ] para dar continuidade às configurações:

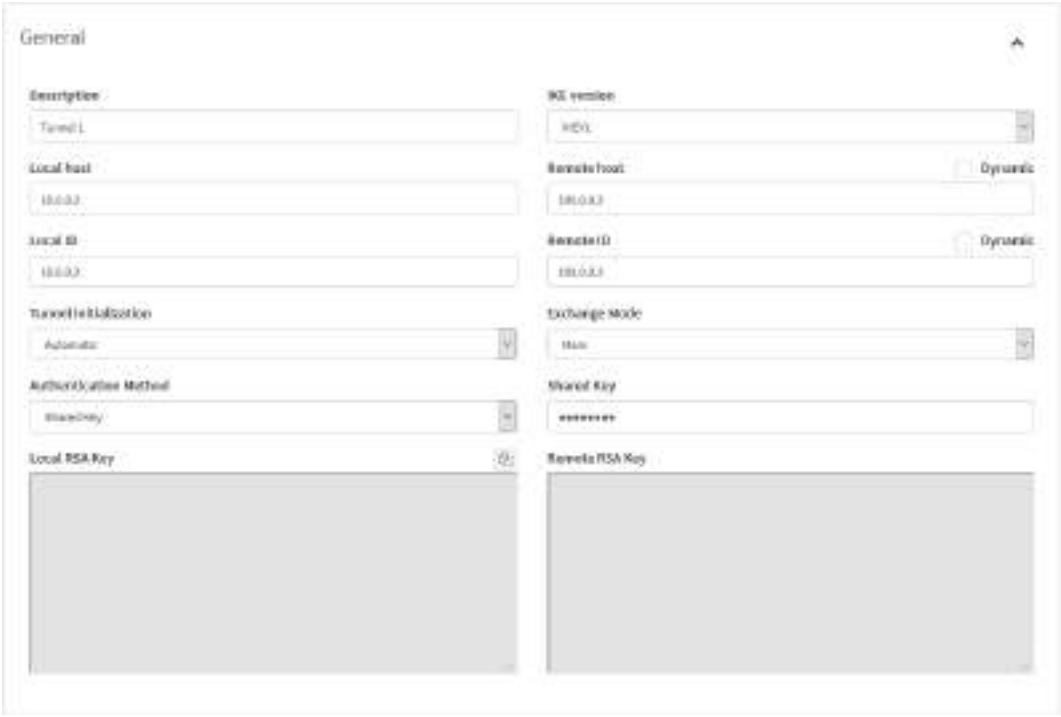


VPN IPSEC – Adicionando *VPN*

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:



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:

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

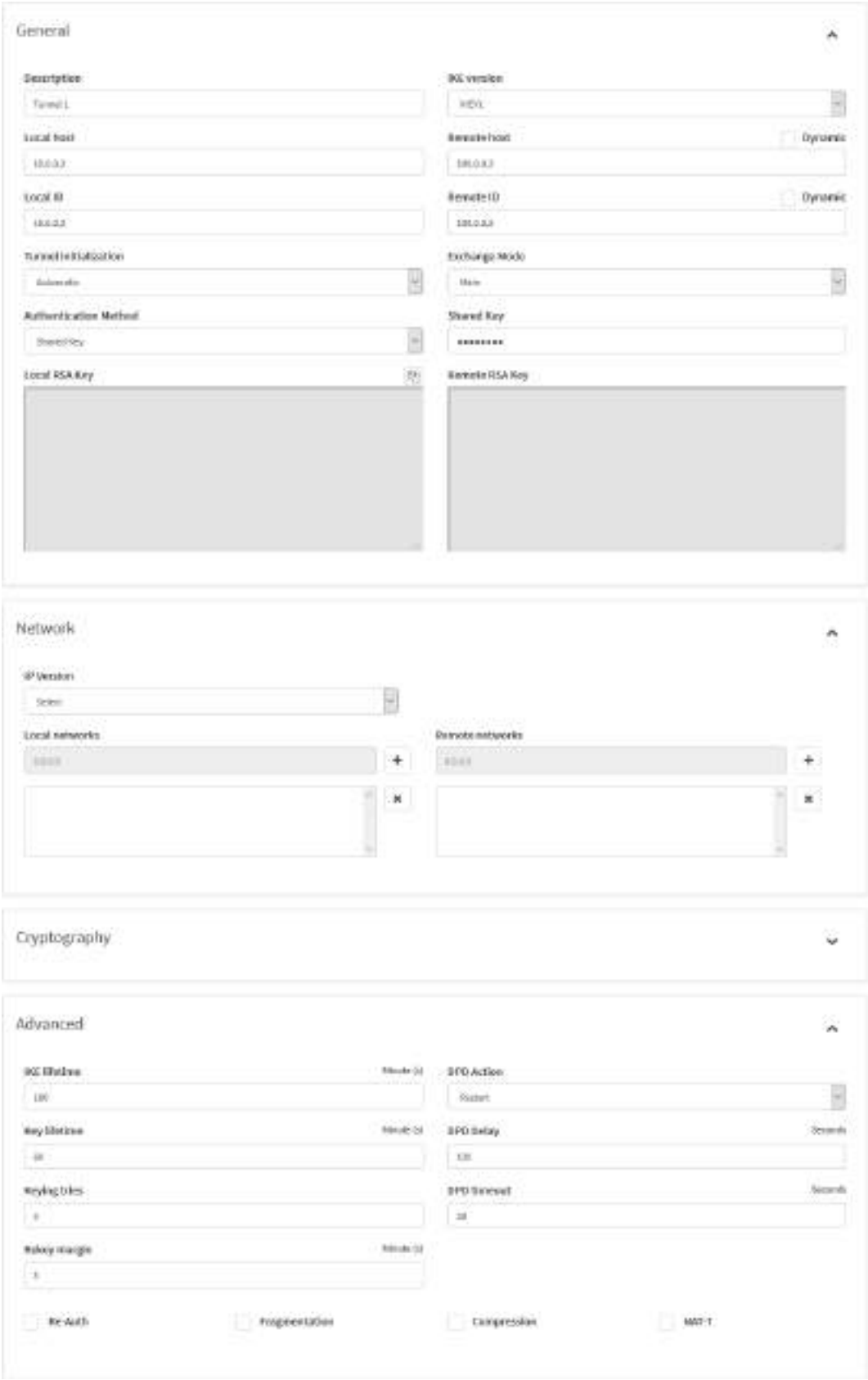
Complete o formulário conforme exemplificado a seguir:

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";

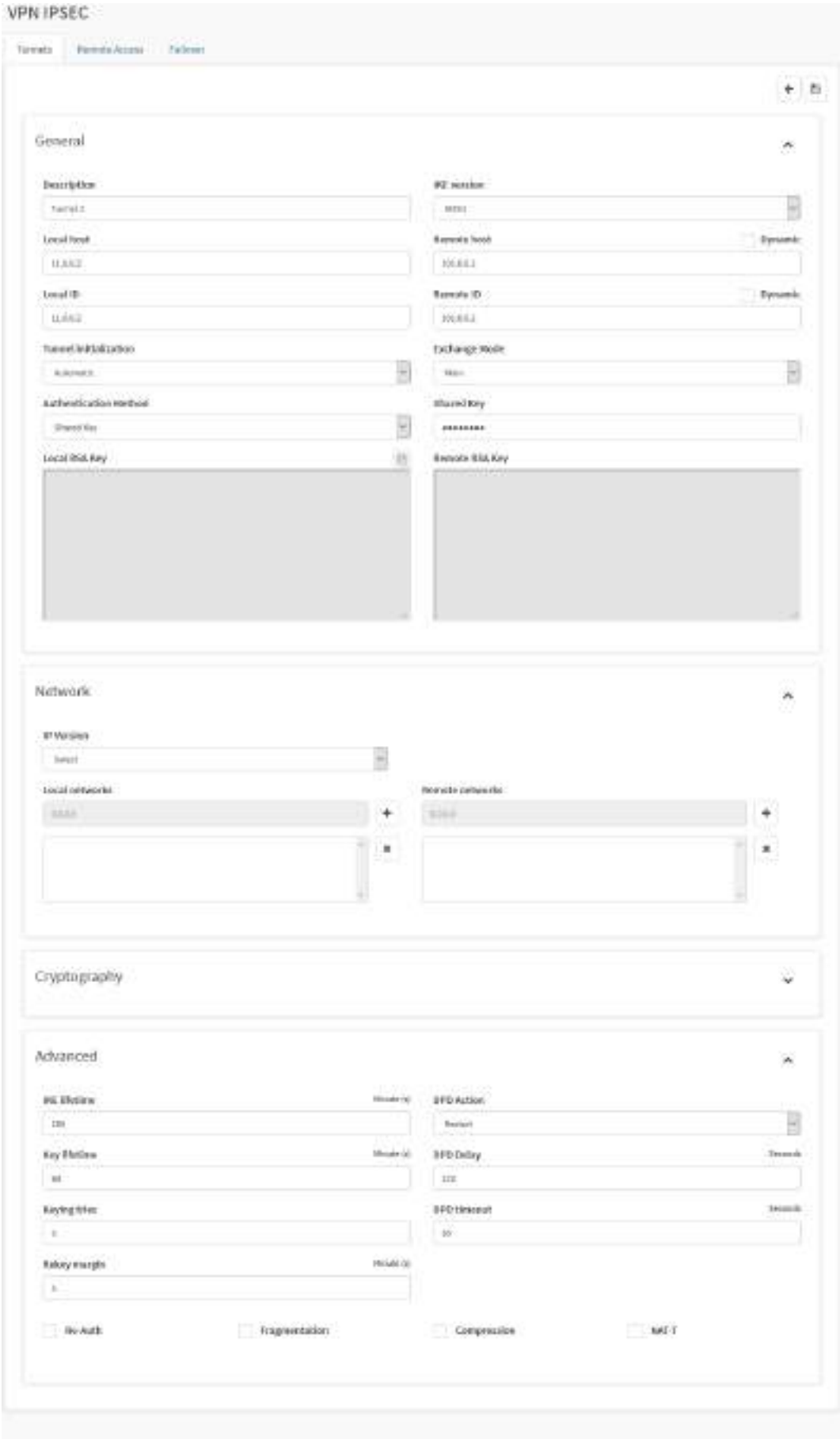
Todas as outras opções podem ficar no padrão, clique no botão ***Save*** **[**  **]** para salvar as configurações efetuadas.

Após estes passos, devemos ter chego no resultado demonstrado pela imagem abaixo:

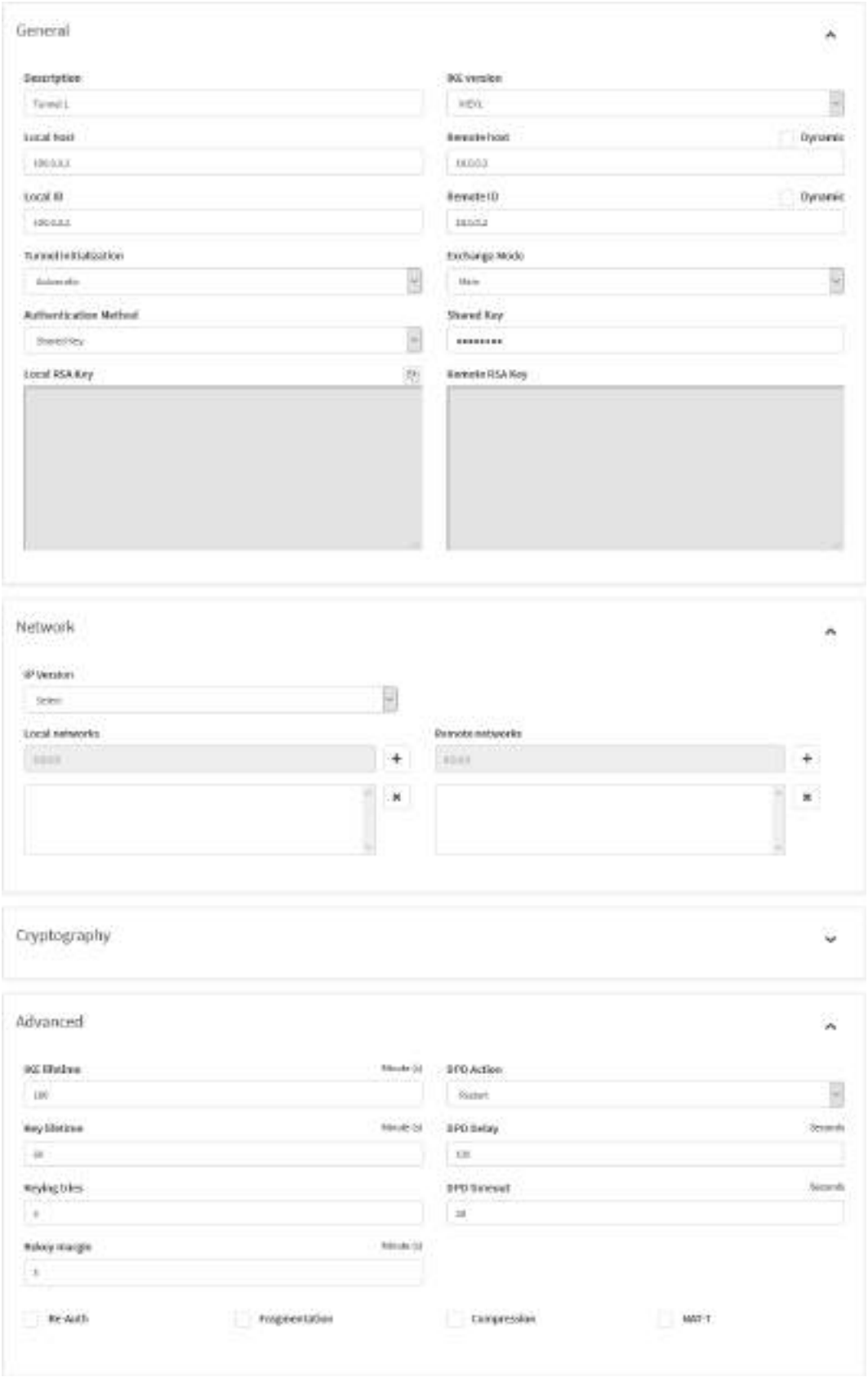


VPN IPSEC – Configurações do *Tunnel* 1

Repita esses passos nas duas pontas da rede. O *Tunnel* 2 deverá ter sido configurada conforme demonstrado pela imagem abaixo:

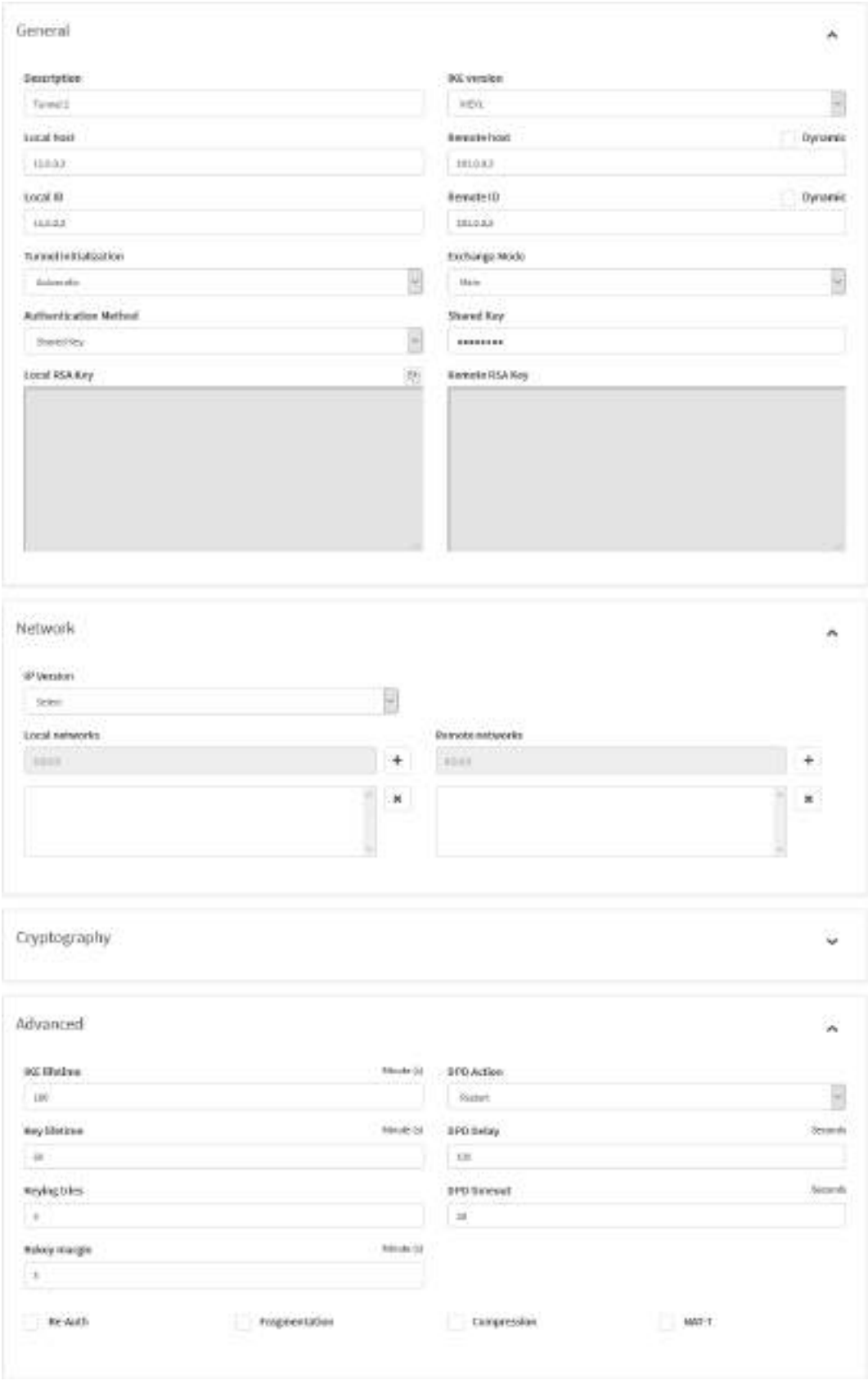

VPN IPSEC
General
Network
Cryptography
Advanced

Indo para o outro ponto, na UTM – *Remote Office* o *Tunnel* 1 deverá ter sido configurada conforme demonstrado pela imagem abaixo:



Remote Office - Configurações do *Tunnel* 1

As configurações do *Tunnel* 2 do UTM – *Remote Office* devem ficar conforme demonstrado na imagem abaixo:



Remote Office - Configurações do *tun2*

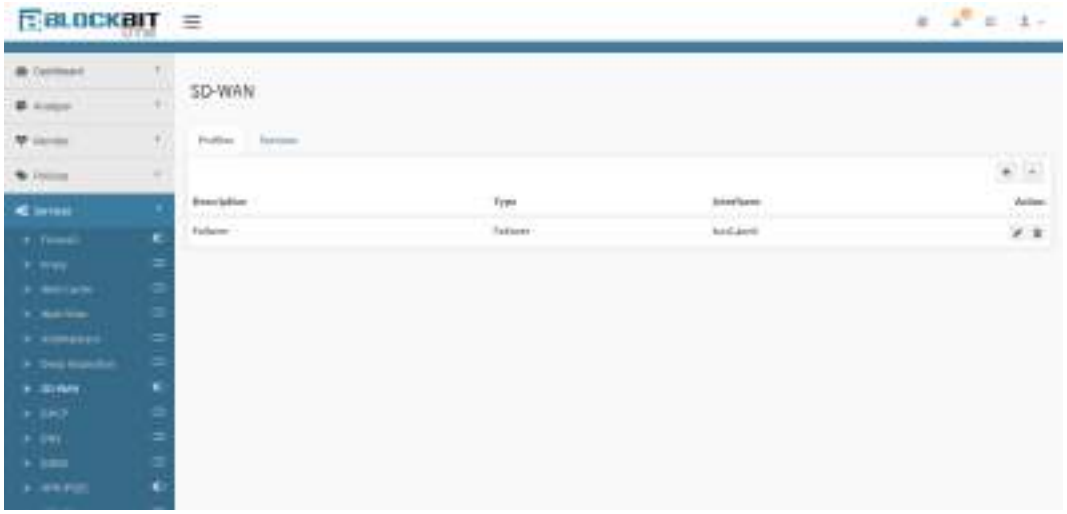
Após salvar cada perfil, para que o *VPN* entre em ação será necessário acessar a **fila de comandos [**  **]** e aplicar as alterações efetuadas. Para mais informações a respeito da fila de comandos acesse a página: UTM - Fila de comandos.

A seguir 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***.



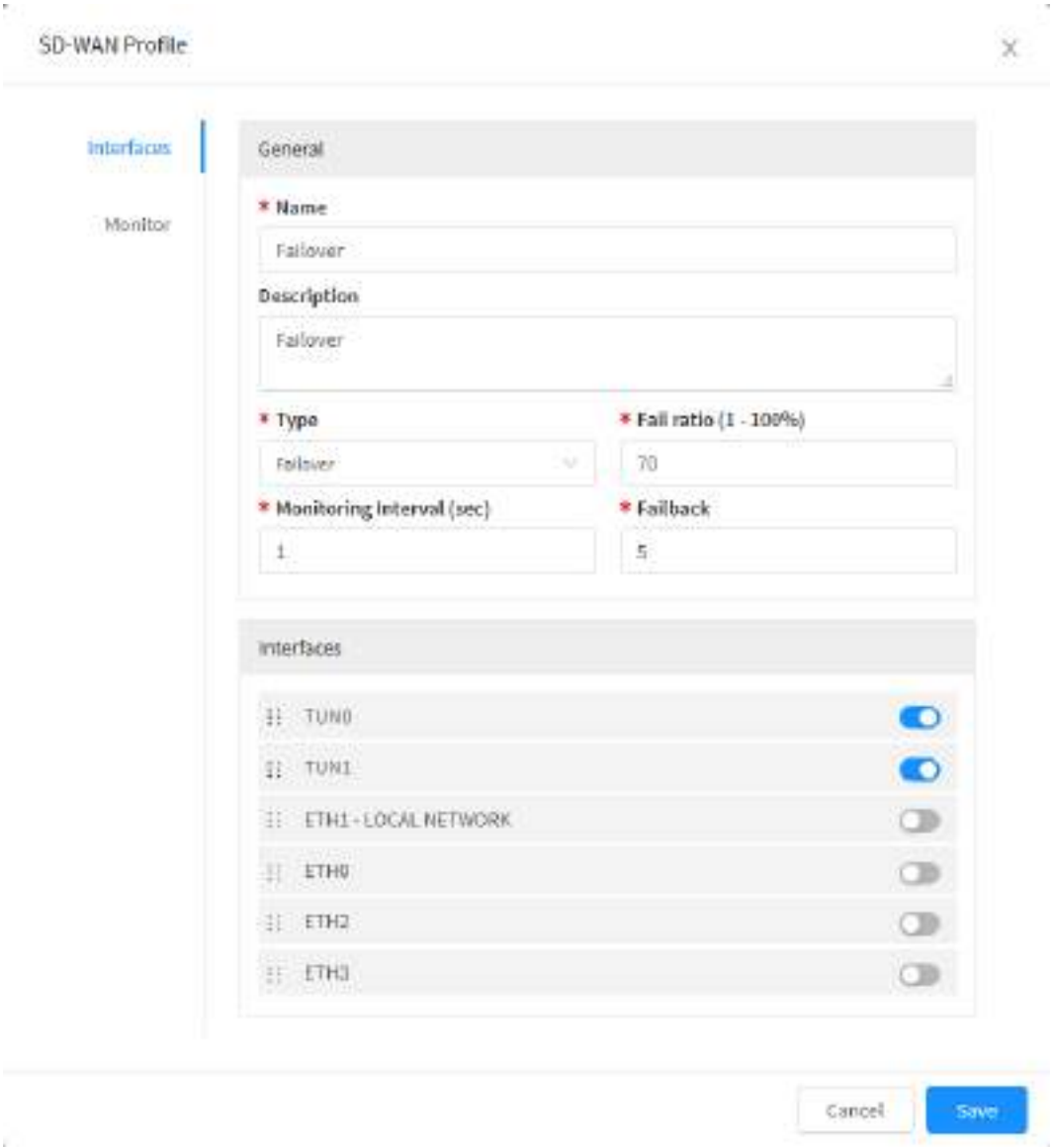
SD-WAN

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:



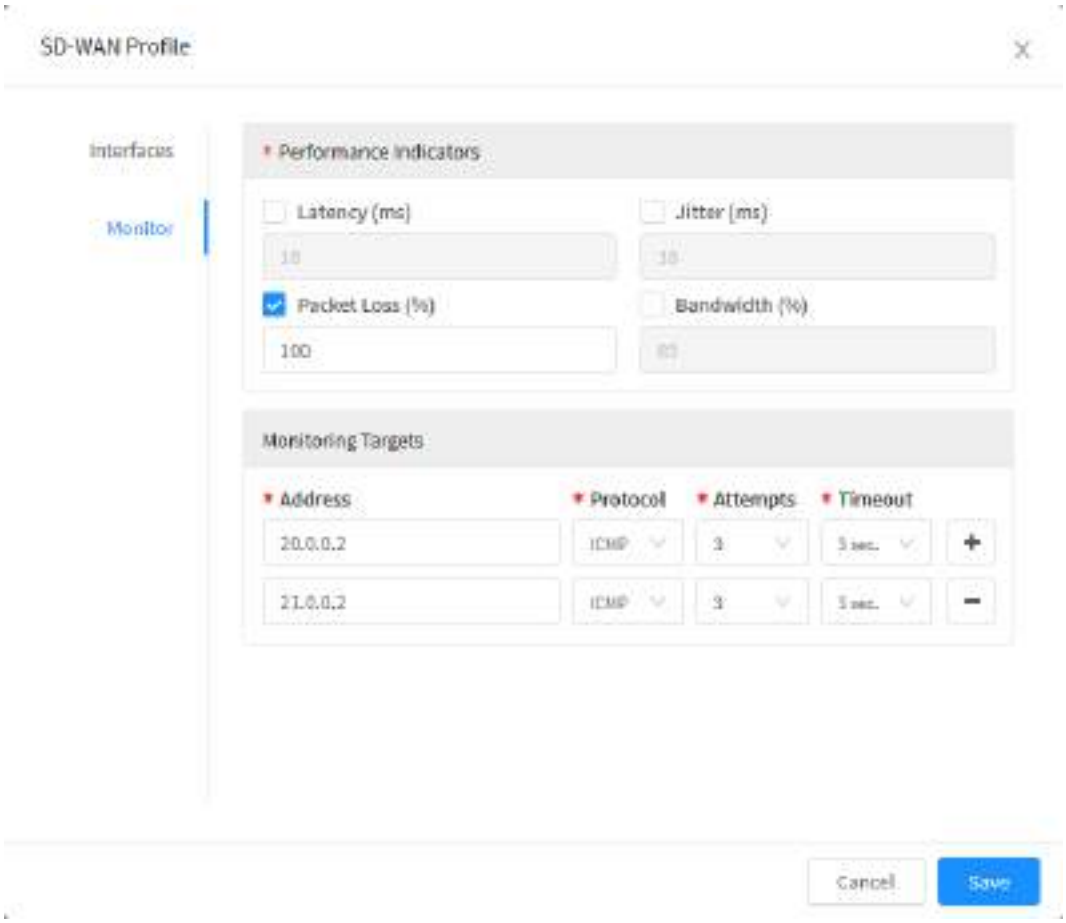
SD-WAN - Interfaces

- ***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*".

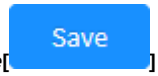
Monitors

Complete o formulário conforme exemplificado a seguir:

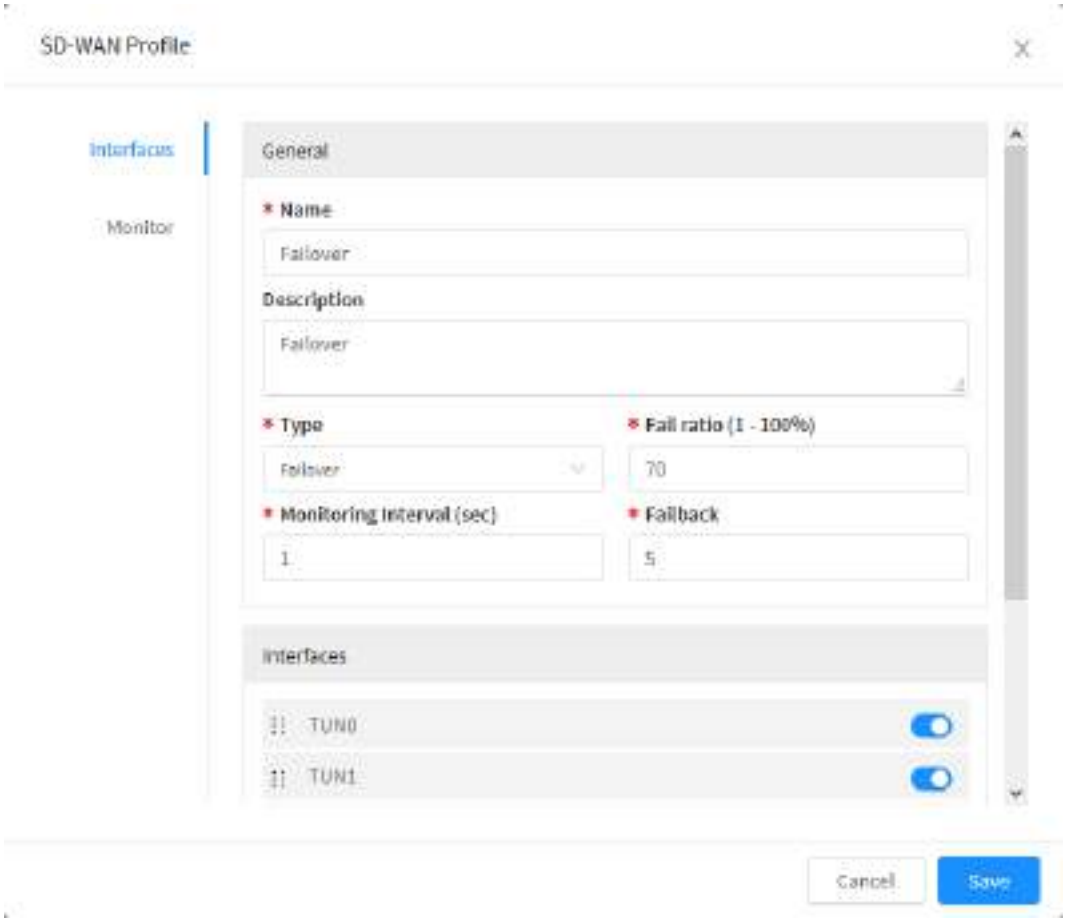


SD-WAN - Monitors

- ***Performance Indicators*:** As opções neste painel devem ser determinadas de acordo com os testes que se deseja executar. É possível selecionar qualquer tipo, porém nesta demonstração utilizaremos "*Packet Loss*" com uma taxa de "100%";
- ***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.

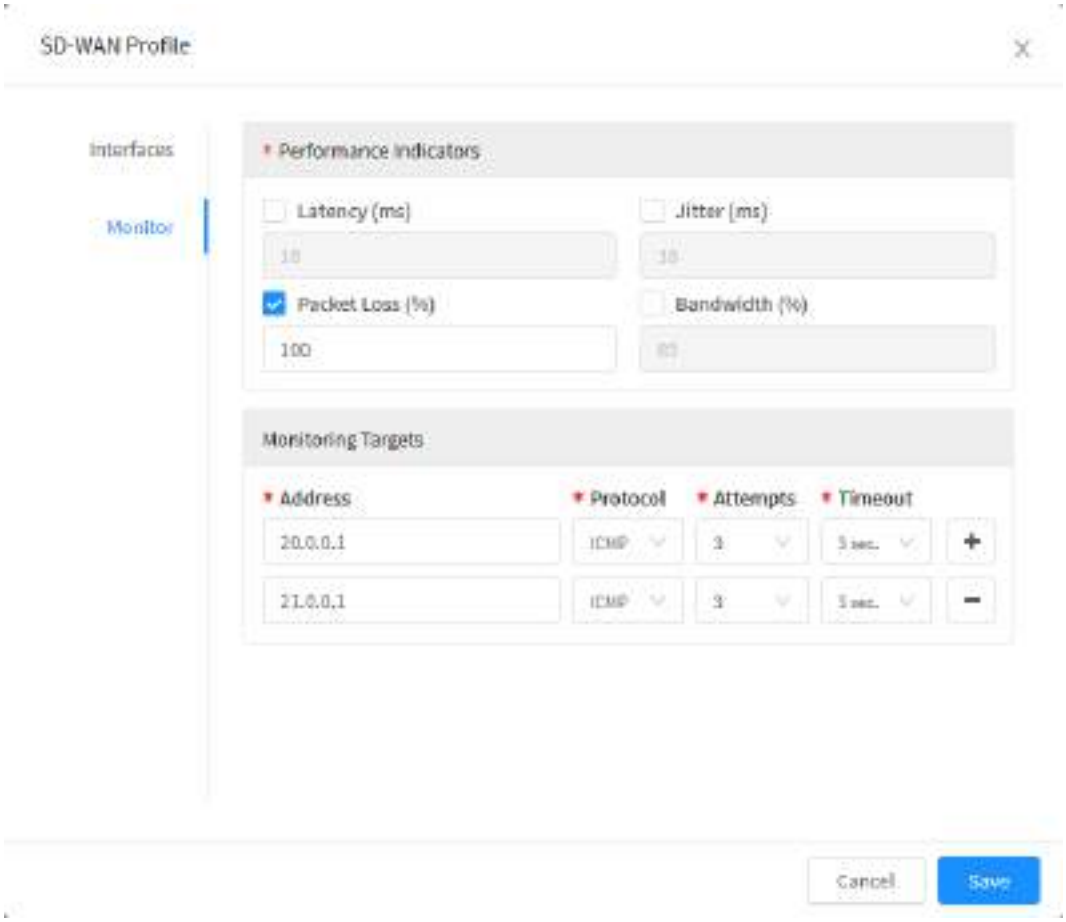
Clique no botão ***Save*[**  **]** para salvar as configurações efetuadas.

Repita esses passos no *UTM – Remote Office* a aba "*Interface*" deverá ter sido configurada conforme demonstrado pela imagem abaixo:



Remote Office - Configurações das *Interfaces*

A aba “*Monitor*” deve ficar conforme demonstrado na imagem abaixo:



Remote Office - Configurações dos *Monitors*

Após salvar cada perfil, para que o *SD-WAN* 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.

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:

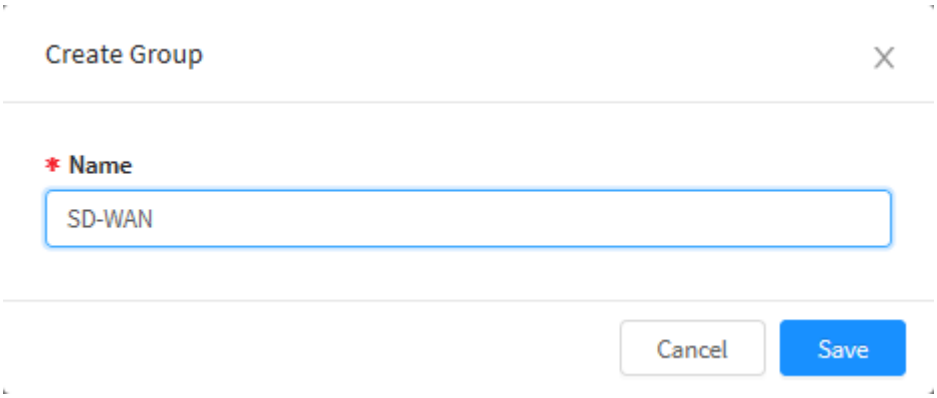
Neste exemplo será criada uma política usando IP.


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***.

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 [➕]**.



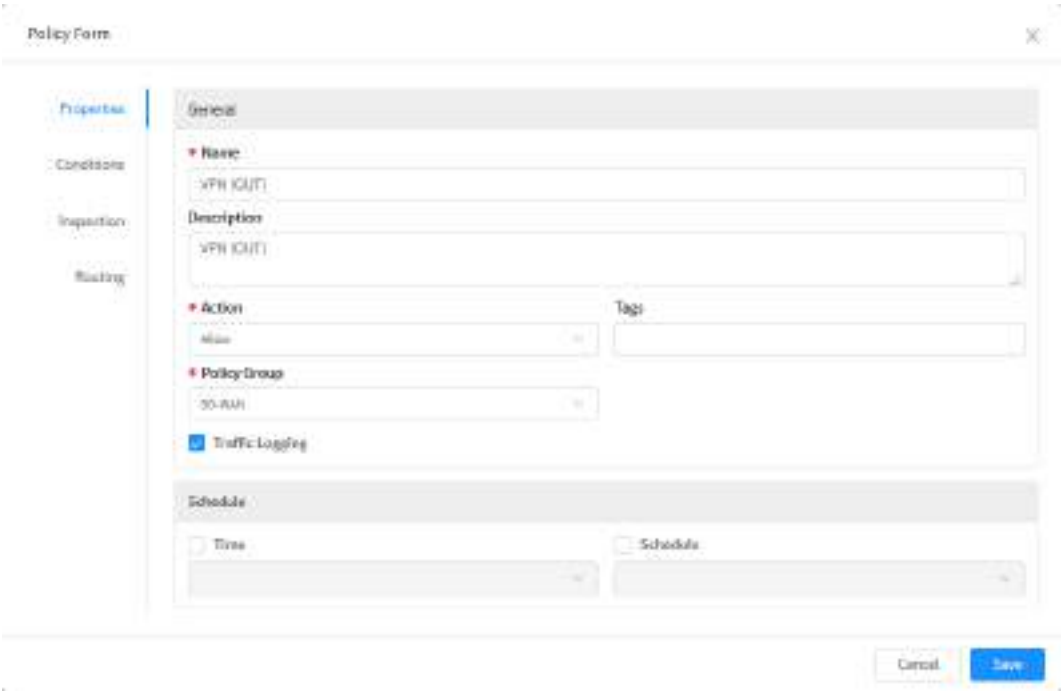
SD-WAN – Add group policies

Após esta etapa, clique em ***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:



IPv4 - Policies - Properties

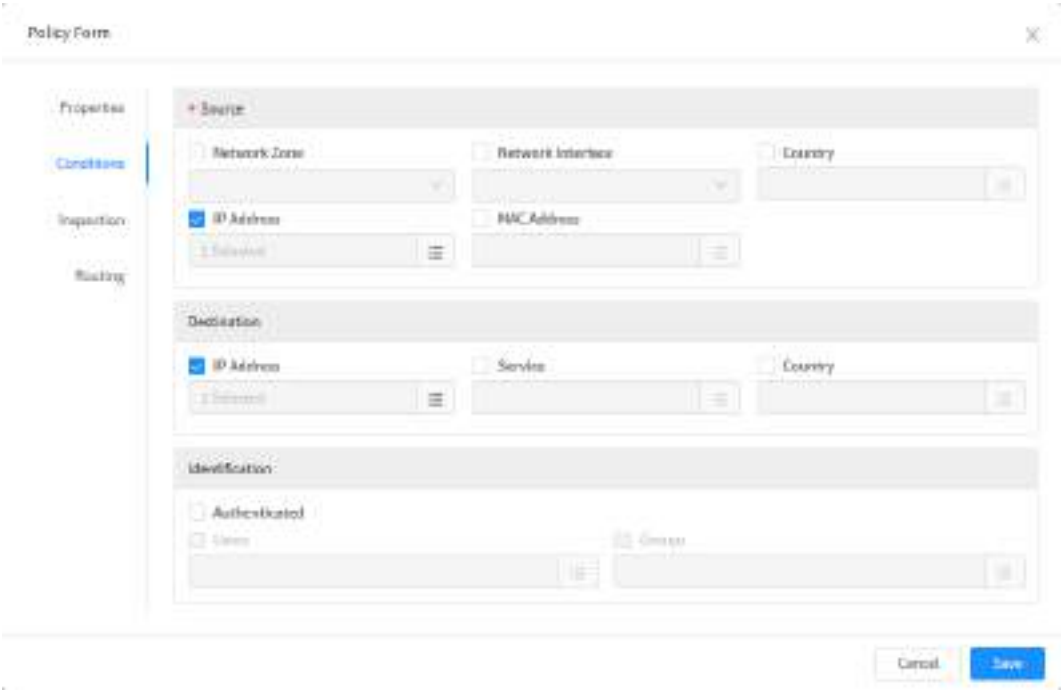
- ***Name*:** Adicione o nome da política. Nesta demonstração usaremos "*VPN* (*Out*)";
- ***Description*:** Insira a descrição desejada de forma a facilitar a identificação da interface política posteriormente. Nesta demonstração usaremos " *VPN* (*Out*)";
- ***Tags*:** Nenhuma *tag* será inserida nesta 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;
- ***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:



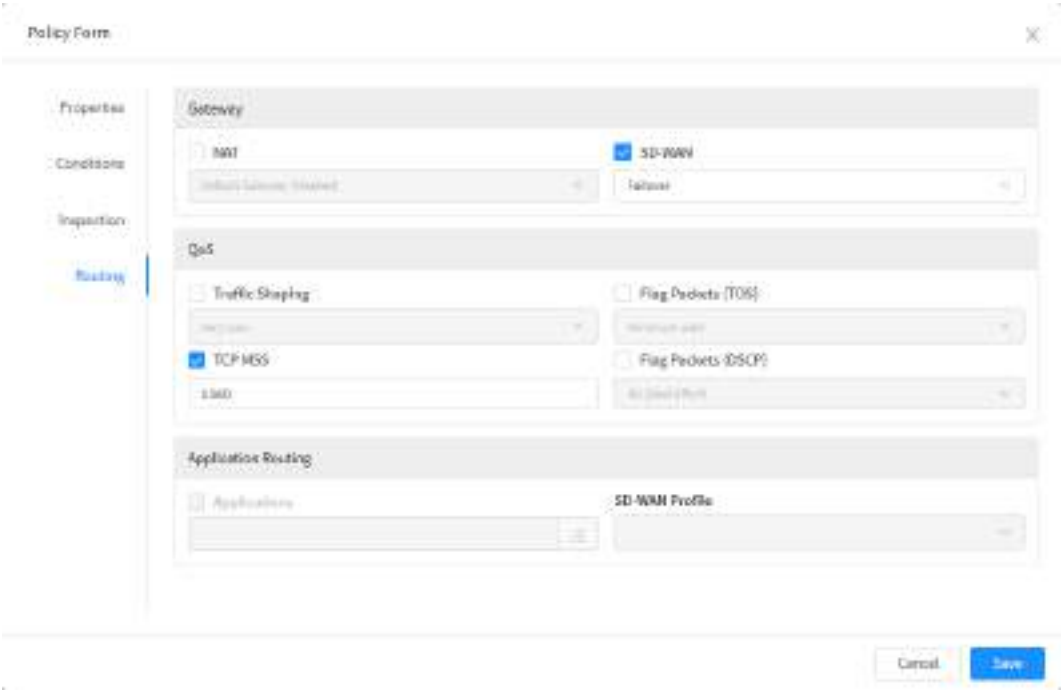
IPv4 - Policies - Connection

- ***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 "*LAN* – 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

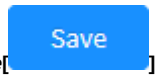
Complete o formulário conforme exemplificado a seguir:



IPv4 – Policies - Routing

- ***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*[**  **]** para registrar todas as alterações feitas.

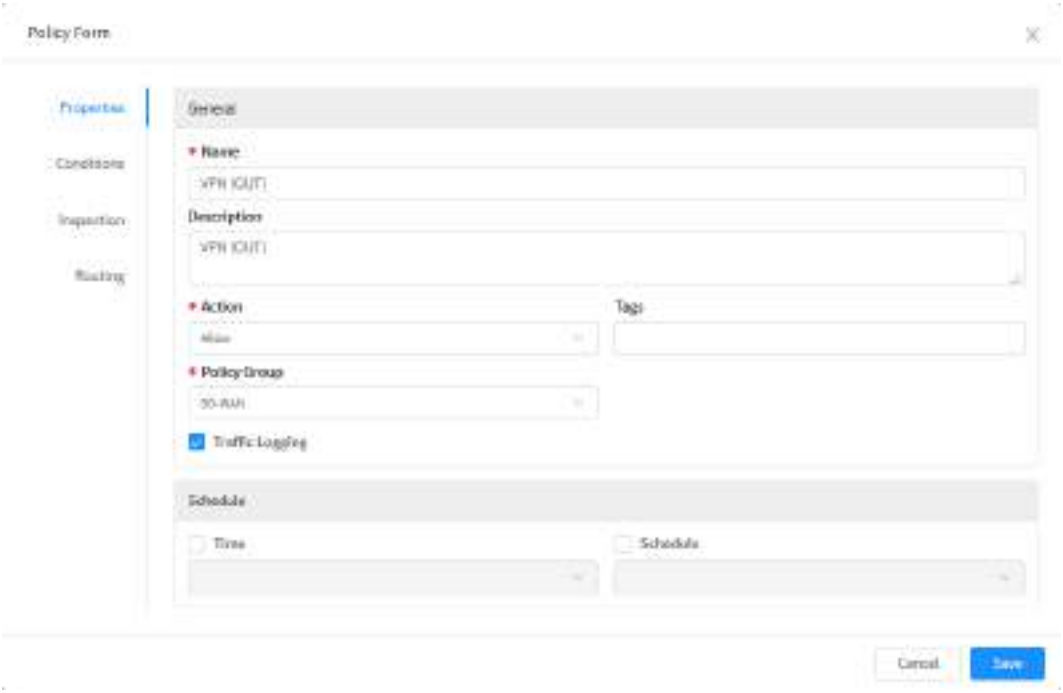
Após estes passos, teremos chego no resultado demonstrado pela imagem abaixo:

IPv4 – Policies – VPN (Out)

Repita esses passos no UTM – *Remote Office*, conforme demonstrado abaixo:

Properties

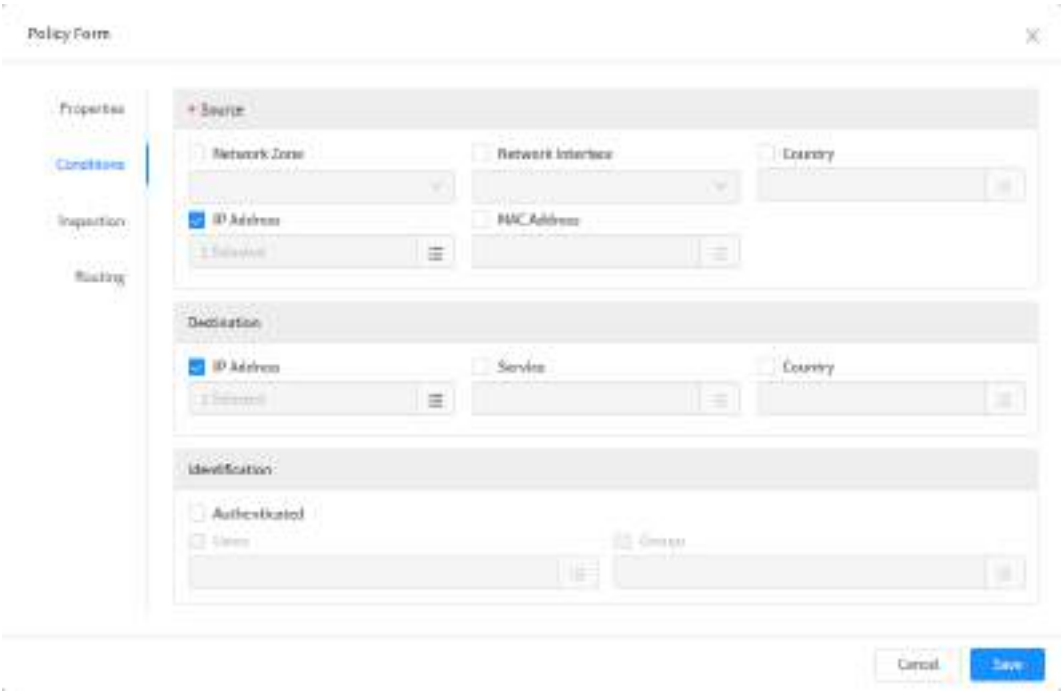
Complete o formulário conforme feito anteriormente:



IPv4 – Remote Office - Properties

Connection

Complete o formulário conforme exemplificado a seguir:



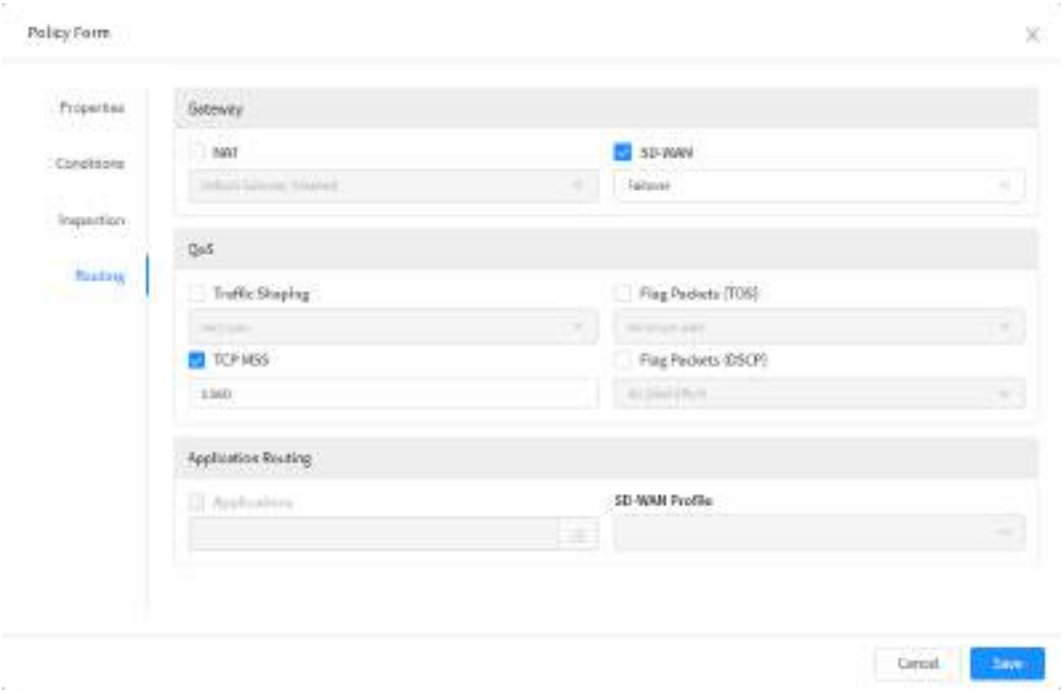
IPv4 – Remote Office - Connection

- ***Network Zone*:** Esta caixa de seleção pode ficar no padrão;
- ***Network interface*:** Esta caixa de seleção pode ficar no padrão;

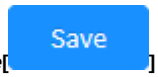
- ***Source - IP Address*:** Deve-se marcar esta caixa de seleção e selecionar o *IP* que foi configurado como interface de *LAN*. No UTM – *Remote Office* será "*LAN* – 172.17.0.0/16";
- ***Source - MAC Address*:** Esta regra não usará endereço físico e, portanto, não lidará com *MAC Address*, a seleção 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 – *Remote Office* será "Remota – 172.18.0.0/16";
- ***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.

Routing

Complete o formulário conforme feito anteriormente:



IPv4 – Remote Office - Security

Clique no botão ***save*[**  **]** para registrar todas as alterações feitas.

Após estes passos, teremos chego no resultado demonstrado pela imagem abaixo:

IPv4 – Remote Office - Policies

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.

IPv4 – *Policies* – Controle de Acesso

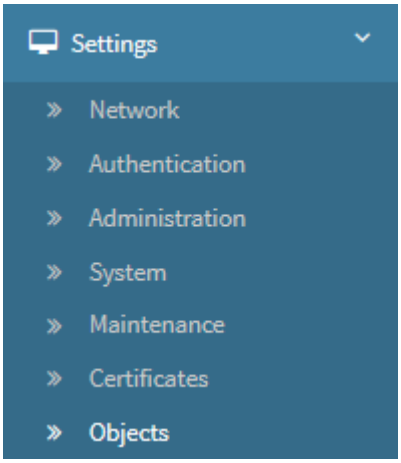
Isso conclui a configuração do *SD-WAN*.

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:

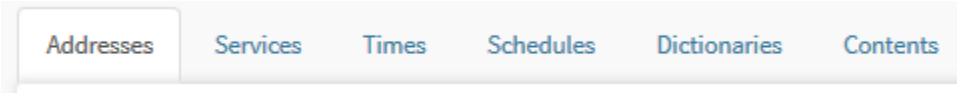
Gerando objeto *Mac Address*

No menu lateral acesse "*Settings*" e selecione a opção "*Objects*".



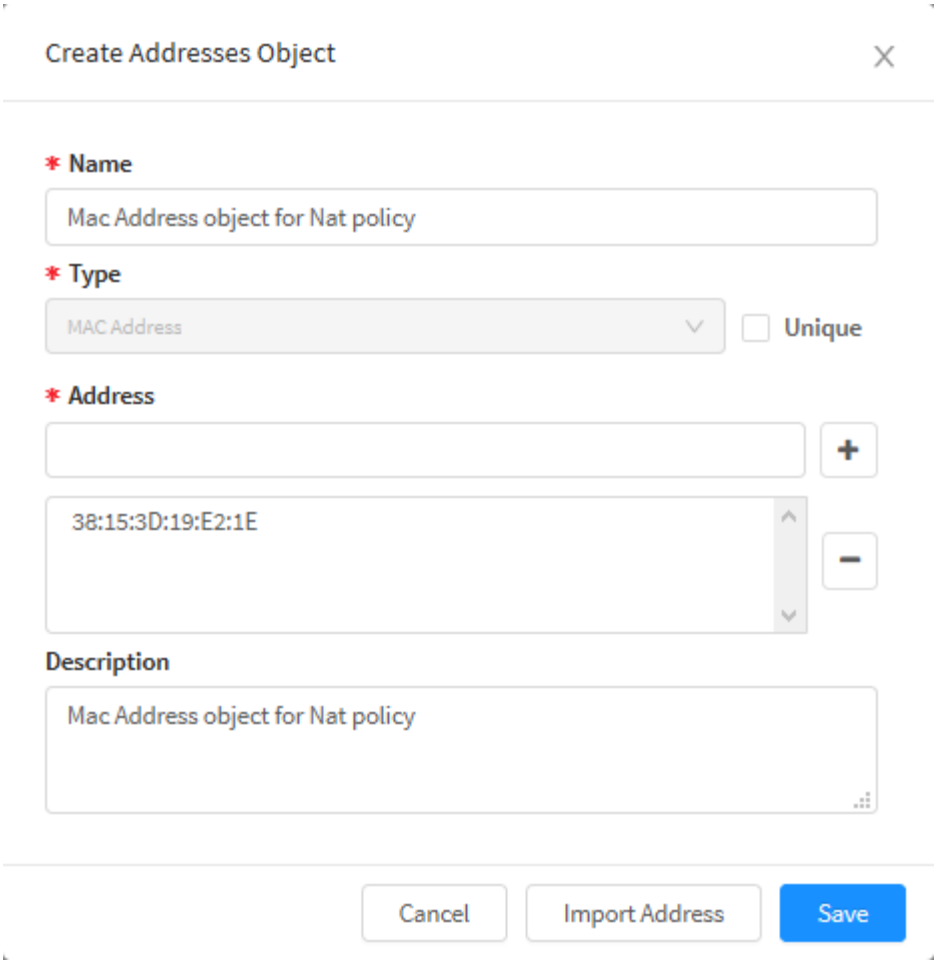
Settings - Objects

Já em "*Objects*", selecione a aba "*Addresses*".



Settings - Objects - Addresses

Crie um novo objeto de *mac address* clicando no **botão[** **+** **]** a seguinte janela será exibida e complete o formulário conforme exemplificado:



Novo objeto *Mac Address*

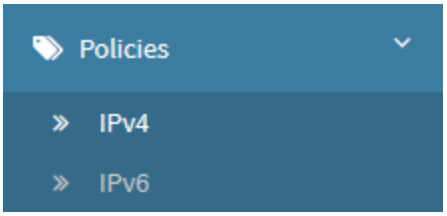
- ***Name*:** Digite o nome do objeto Mac Address. Ex.: Mac Address object for Nat policy
- ***Mac address*:** Digite o endereço físico e clique no **botão [+]** para adicioná-lo na lista. Caso deseje remover um Mac Address, selecione-o na lista e clique no **botão [−]** para remover. Ex.: 38:15:3d:19:e2:1e;
- ***Description*:** Digite a descrição do seu objeto. Ex.: Mac Address object for Nat policy*;*
- ***Group*:** Caso deseje adicionar esse mac address em um grupo, adicione-o neste campo. Neste exemplo, não adicionaremos nenhum grupo;

Para mais informações sobre como lidar com objetos, cheque o capítulo *Settings - Objects*.

Por fim, clique no botão ***Save*** **[** Save **]** para finalizar a operação.

Criando a política de *Mac Address*

No menu lateral acesse "*Policies*" e selecione a opção "*IPv4*".

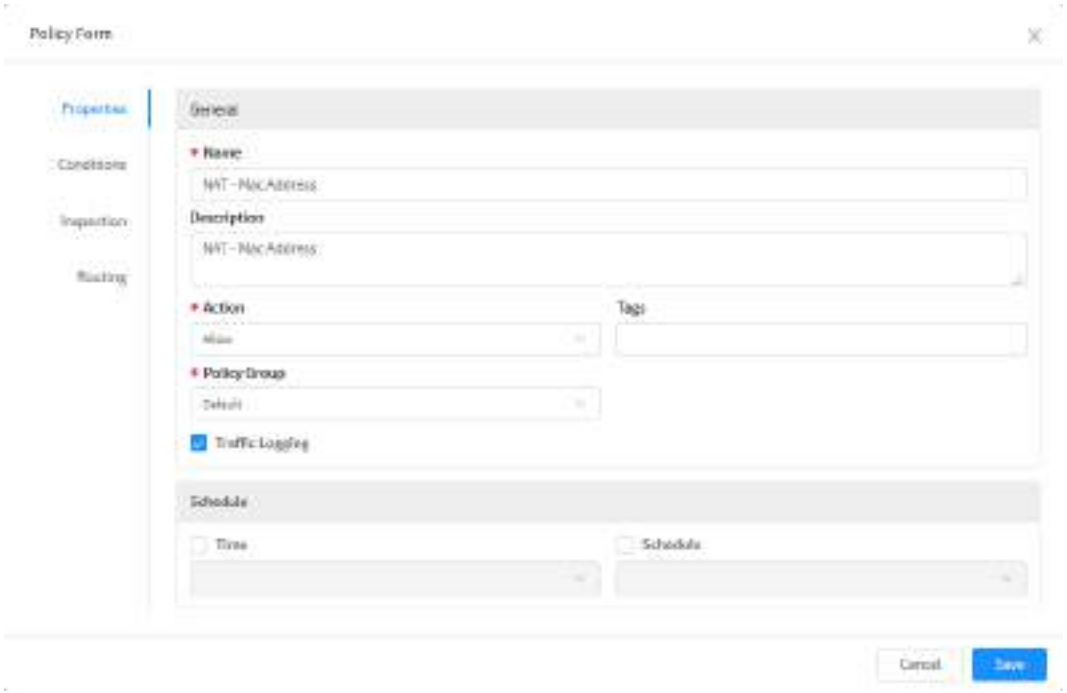


Policies - IPv4

Selecione o grupo onde se deseja criar a política, neste exemplo, usaremos o grupo "*Default*".

Policies - IPv4 - Groups

Clique na opção *Create Policy* do Menu de ações para criar uma nova política. Complete o formulário conforme exemplificado a seguir:

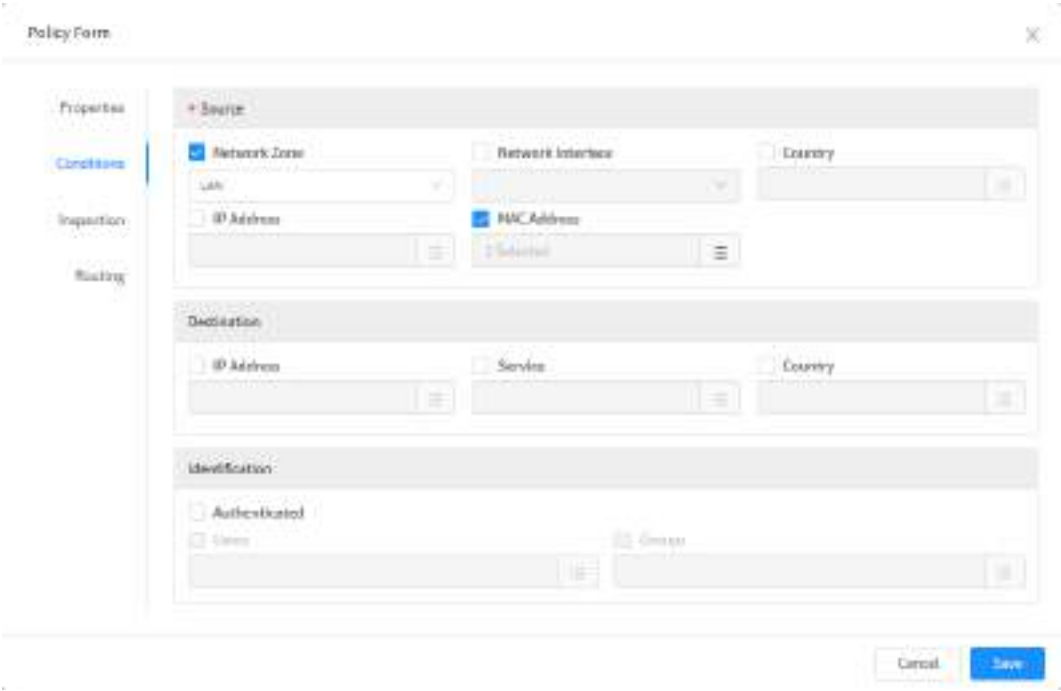


Policies - New Policy - Properties

- ***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.*

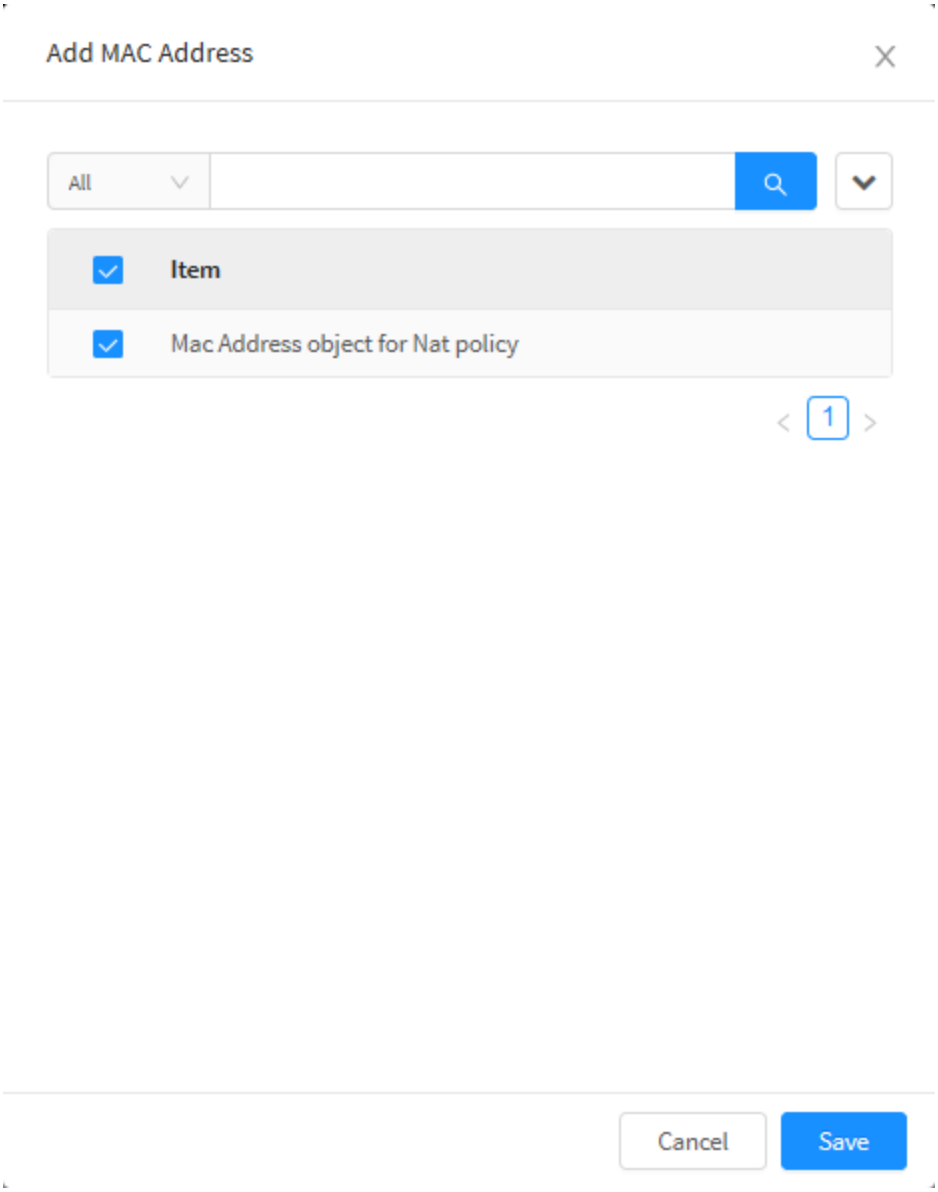
O resto das opções podem continuar como com os valores padrão.

Selecione a opção "*Conditions*" no menu lateral.



Policies - New Policy - Conditions

- ***Network Zone*:** LAN;
- ***MAC Address*:** Selecione o endereço físico, adicionado previamente, conforme demonstrado abaixo:



Policies - New Policy - 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 [** Save **]** para salvar a política.

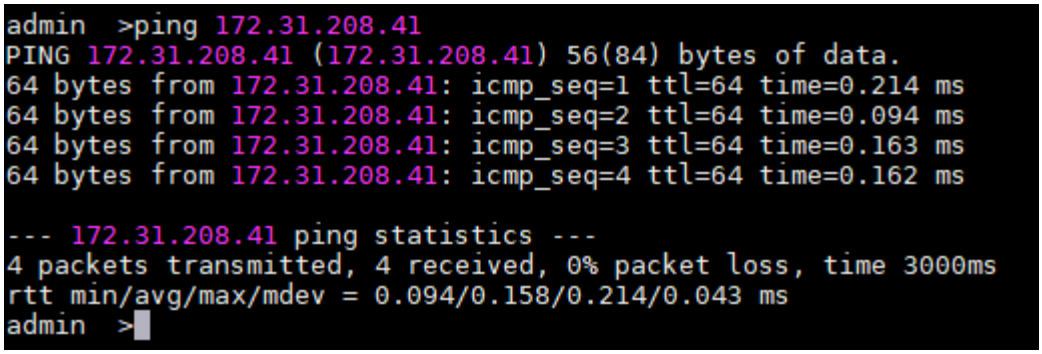
Policy - NAT - Mac Address

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:

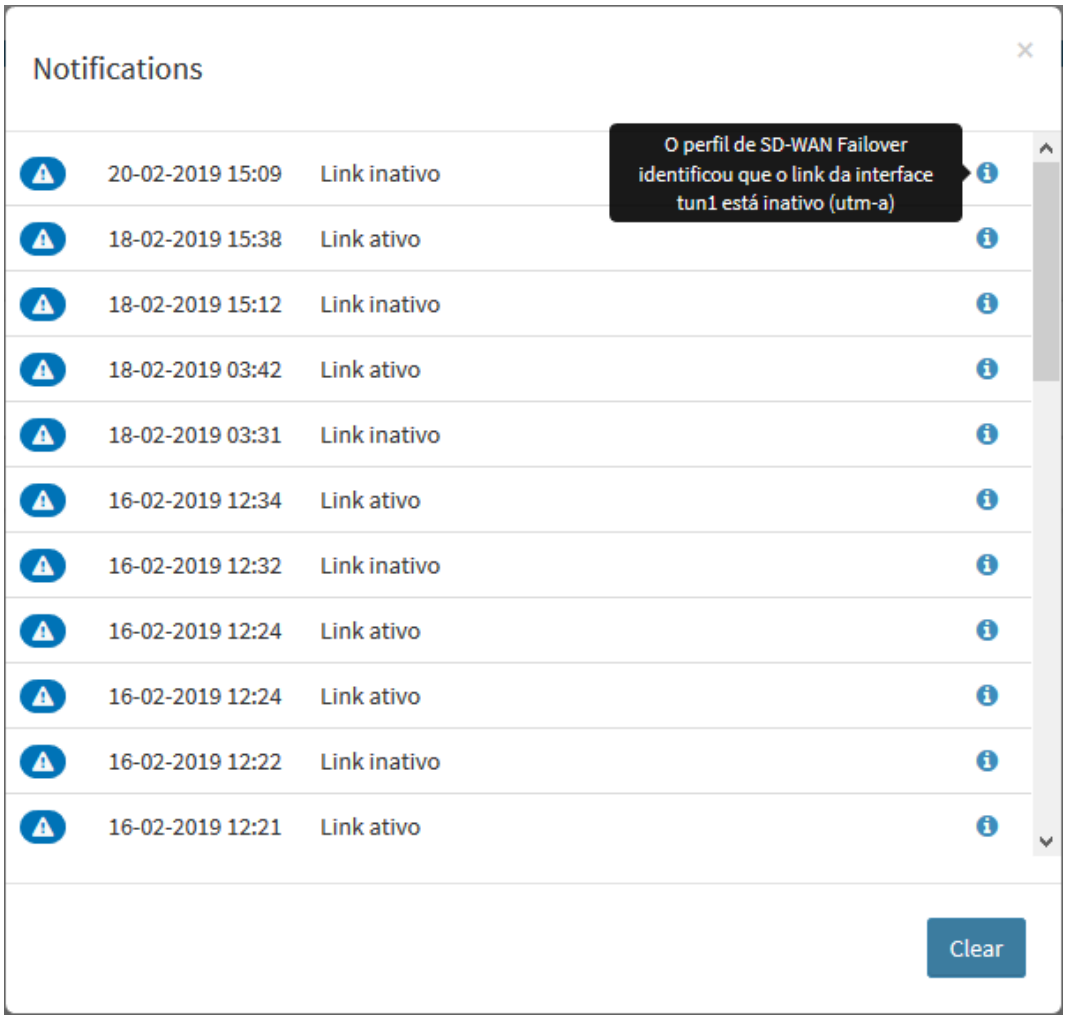


Validação por *Ping*

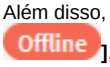
Além disso, é possível derrubar propositalmente o *link* que está sendo utilizado pelo *SD-WAN* com objetivo de checar se o *Failover* irá assumir a interface corretamente.

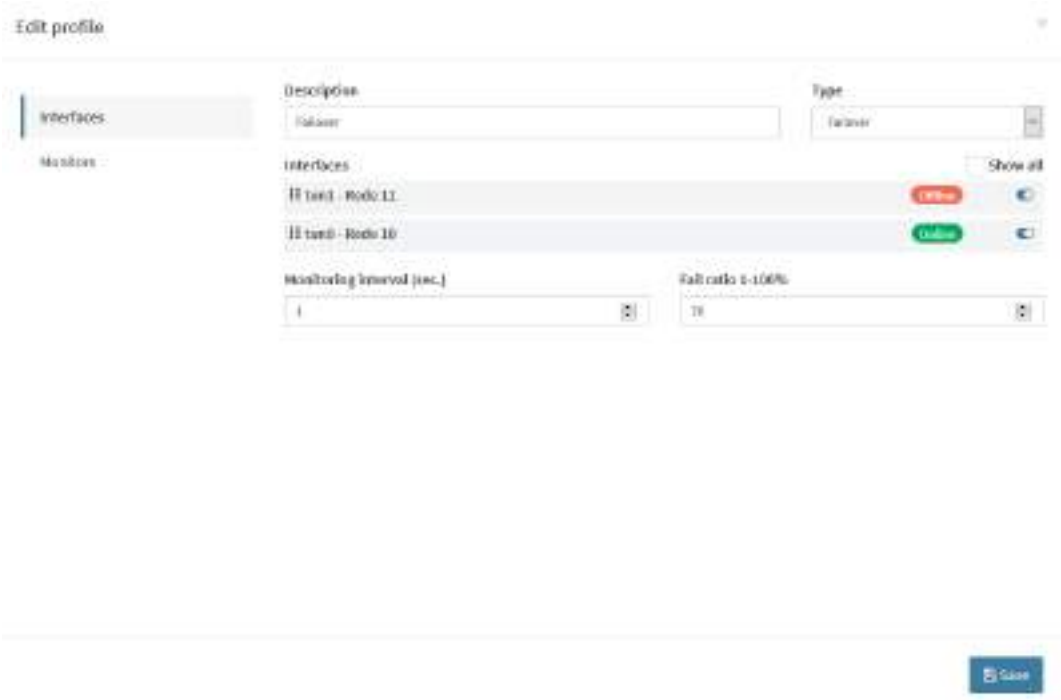
Conforme anteriormente configurado, no UTM - *HQ* a interface com prioridade no *SD-WAN* é a “tun1 – Rede 11”, assim sendo, remova o cabo de rede de forma a interromper a comunicação do dispositivo.

Na janela de notificações, será possível observar o alerta exibido, conforme exibido na imagem a seguir.



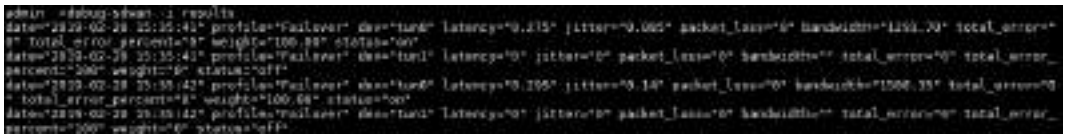
Notifications

Além disso, acesse ***Services>>SD-WAN*** e clique no botão ***edit*** **[**  **]**, será possível observar que a interface *tunnel1* está com o *status* ***offline*** **[**  **]**, conforme demonstrado na imagem abaixo.



Interface *Offline*

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*.

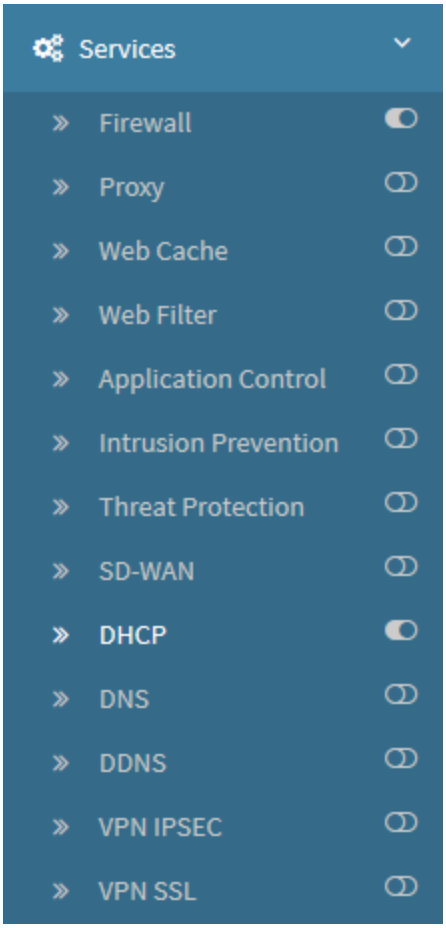
Recursos do *DHCP*:

- 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:



Serviços - DHCP

A seguinte tela será exibida:

DHCP

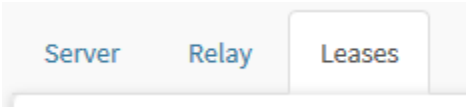
A seguir, explicaremos as demais abas da interface *DHCP em detalhe*:

- *Server IPv4*;
- Server IPv6;
- *Relay IPv4;*
- *Relay IPv6;*
- *Leases IPv4;*
- *Leases IPv6;*

DHCP - Aba Leases IPv4

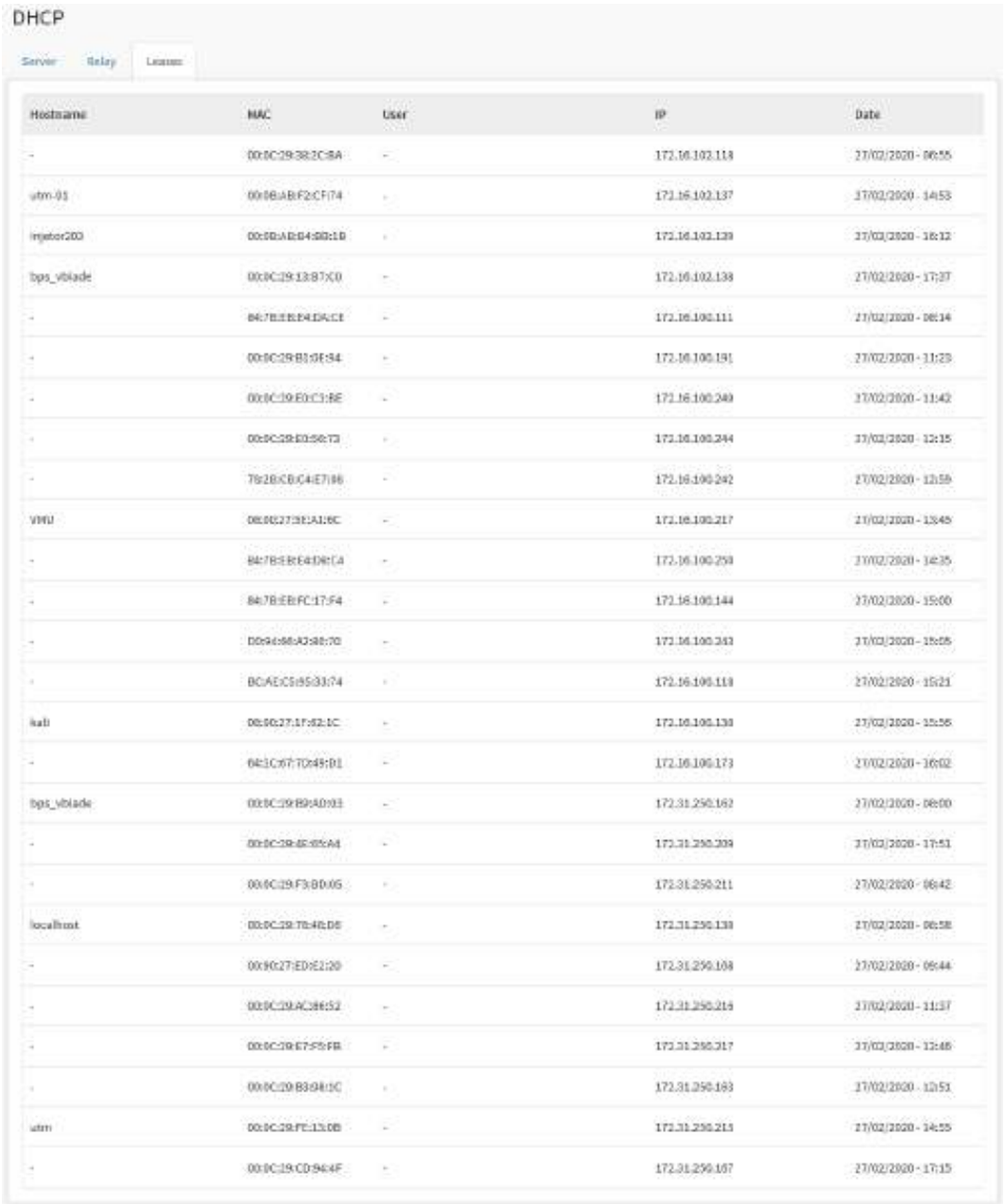
Este recurso permite ao administrador visualizar os *hostnames*, *MacAddress*, Usuários, endereços *IP* e a Data do recebimento do *IP* distribuídos pelo servidor *DHCP* do Blockbit UTM.

Para visualizar esta janela, clique na aba "*Leases*", como demonstrado abaixo.



Aba *Leases*

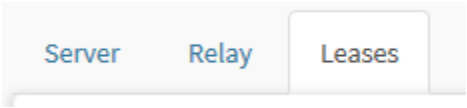
Surgirá a tela a seguir:



DHCP - Aba Leases IPv6

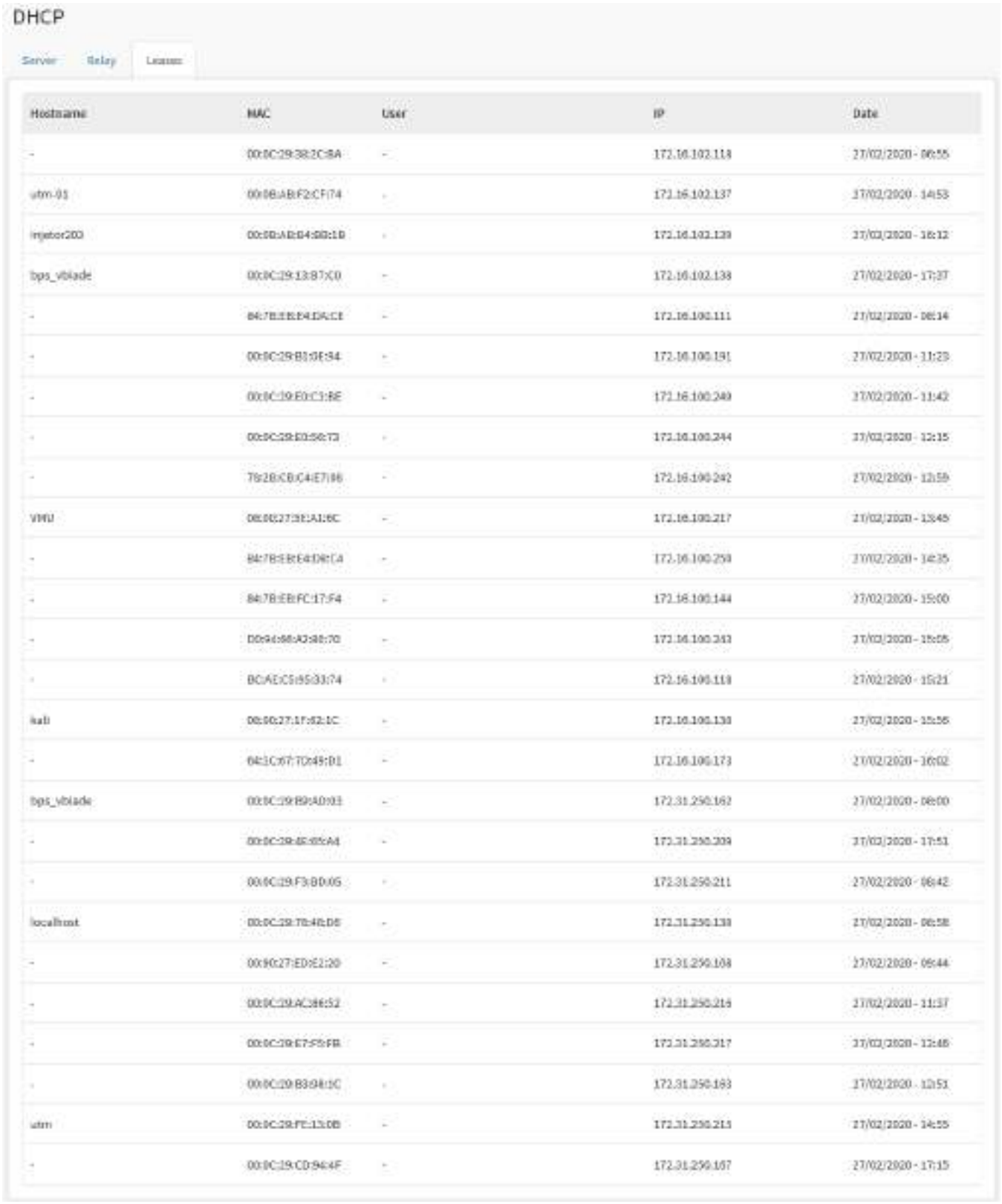
Este recurso permite ao administrador visualizar os *hostnames*, *MacAddresses*, Usuários, endereços *IP* e a Data do recebimento do *IP* distribuídos pelo servidor *DHCP* do Blockbit UTM.

Para visualizar esta janela, clique na aba "*Leases*", como demonstrado abaixo.



Aba *Leases*

Surgirá a tela a seguir:


DHCP
Server
Relay
Leases
Hostname
MAC
User
IP
Date
-
00:0C:29:38:2C:BA
-
172.16.102.118
27/02/2020 - 09:55
utm-01
00:0B:AB:F2:CF:74
-
172.16.102.137
27/02/2020 - 14:53
injetor200
00:0B:AB:B4:0D:1D
-
172.16.102.139
27/02/2020 - 16:12
bps_vblade
00:0C:29:13:B7:X0
-
172.16.102.138
27/02/2020 - 17:37
-
84:7B:EB:E4:DA:CE
-
172.16.100.111
27/02/2020 - 08:14
-
00:0C:29:B1:0F:34
-
172.16.100.191
27/02/2020 - 11:23
-
00:0C:29:E0:C1:8E
-
172.16.100.249
27/02/2020 - 11:42
-
00:0C:29:E0:58:T3
-
172.16.100.244
27/02/2020 - 12:15
-
78:2B:CB:C4:E7:86
-
172.16.100.242
27/02/2020 - 12:59
VMU
08:00:27:3E:A1:6C
-
172.16.100.217
27/02/2020 - 13:45
-
84:7B:EB:E4:D8:CA
-
172.16.100.259
27/02/2020 - 14:35
-
84:7B:EB:FC:17:F4
-
172.16.100.144
27/02/2020 - 15:00
-
D0:94:66:A2:88:70
-
172.16.100.243
27/02/2020 - 15:05
-
BC:AE:C5:65:33:74
-
172.16.100.113
27/02/2020 - 15:21
kali
08:00:27:1F:82:1C
-
172.16.100.133
27/02/2020 - 15:56
-
64:1C:67:7D:49:D1
-
172.16.100.173
27/02/2020 - 16:02
bps_vblade
00:0C:29:B9:A0:03
-
172.31.250.162
27/02/2020 - 08:00
-
00:0C:29:4F:05:A4
-
172.31.250.209
27/02/2020 - 17:51
-
00:0C:29:F3:B0:05
-
172.31.250.211
27/02/2020 - 08:42
localhost
00:0C:29:7B:4B:D8
-
172.31.250.133
27/02/2020 - 08:58
-
00:90:27:ED:E1:20
-
172.31.250.108
27/02/2020 - 09:44
-
00:0C:29:AC:86:52
-
172.31.250.216
27/02/2020 - 11:37
-
00:0C:29:E7:F5:FB
-
172.31.250.217
27/02/2020 - 12:48
-
00:0C:29:B3:94:1C
-
172.31.250.163
27/02/2020 - 12:51
utm
00:0C:29:FE:15:DB
-
172.31.250.213
27/02/2020 - 14:55
-
00:0C:29:CD:94:4F
-
172.31.250.167
27/02/2020 - 17:15

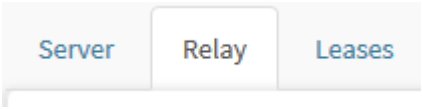
DHCP - Leases

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.

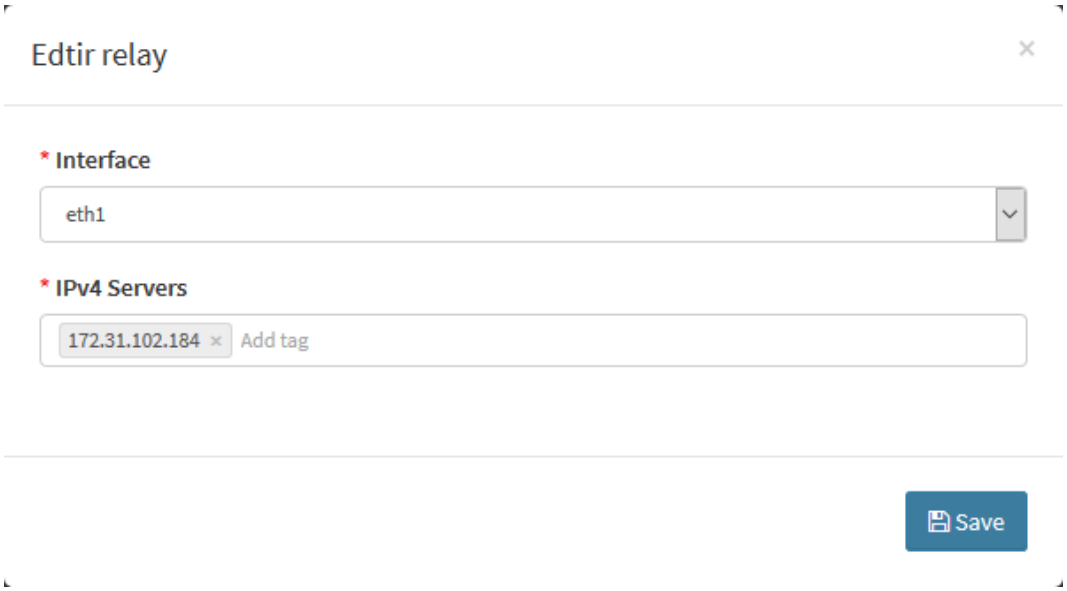


Aba *Relay*

Surgirá a tela *a seguir*, conforme demonstrado pela imagem abaixo:

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 *IP* do serviço de *DHCP*.



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 [Save] para concluir as alterações .

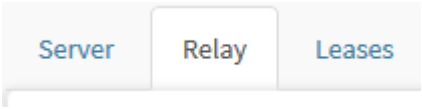
- Leases.

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.

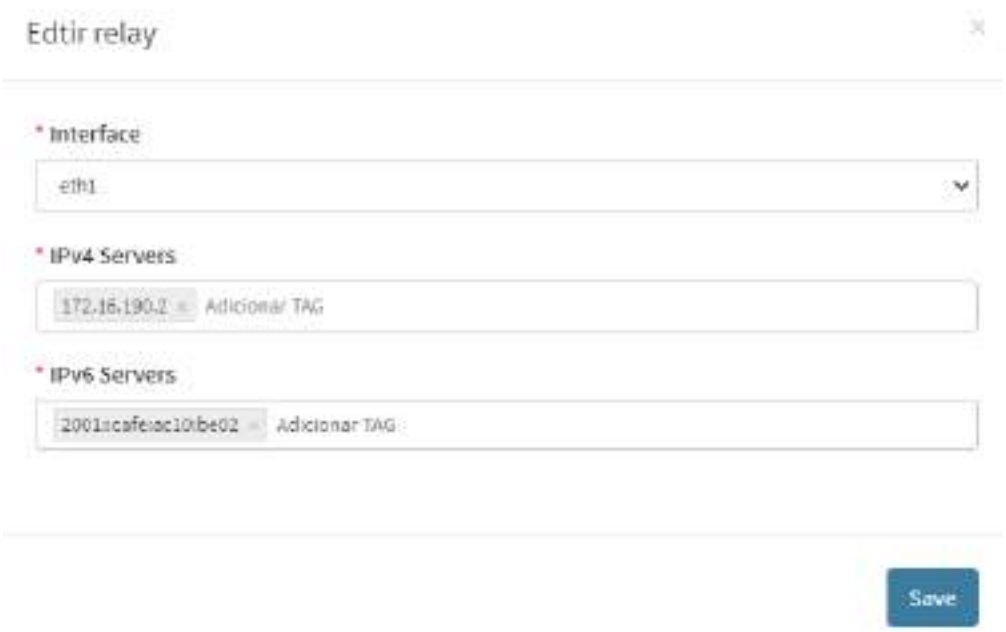


Aba *Relay*

Surgirá a tela *a seguir*, conforme demonstrado pela imagem abaixo:

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 *IP* do serviço de *DHCP*.



DHCP - Aba *Relay* - *Add Relay*

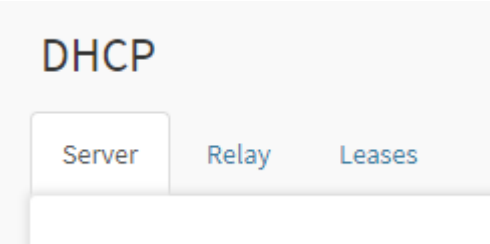
> ⚠ O campo *IPv6* aceita objetos únicos de endereço, para mais informações cheque a página de criação de Address Objects.

Depois clique em [Save] para concluir as alterações .

- Leases.

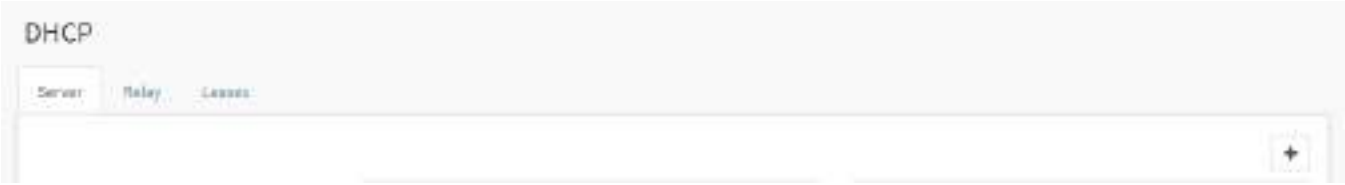
DHCP - Aba Server IPv4

Para configurar os servidores de *DHCP*, IPv4 e IPv6 selecione a aba correta:



Aba *Server*

Surgirá a tela *a seguir*, conforme demonstrado pela imagem abaixo:



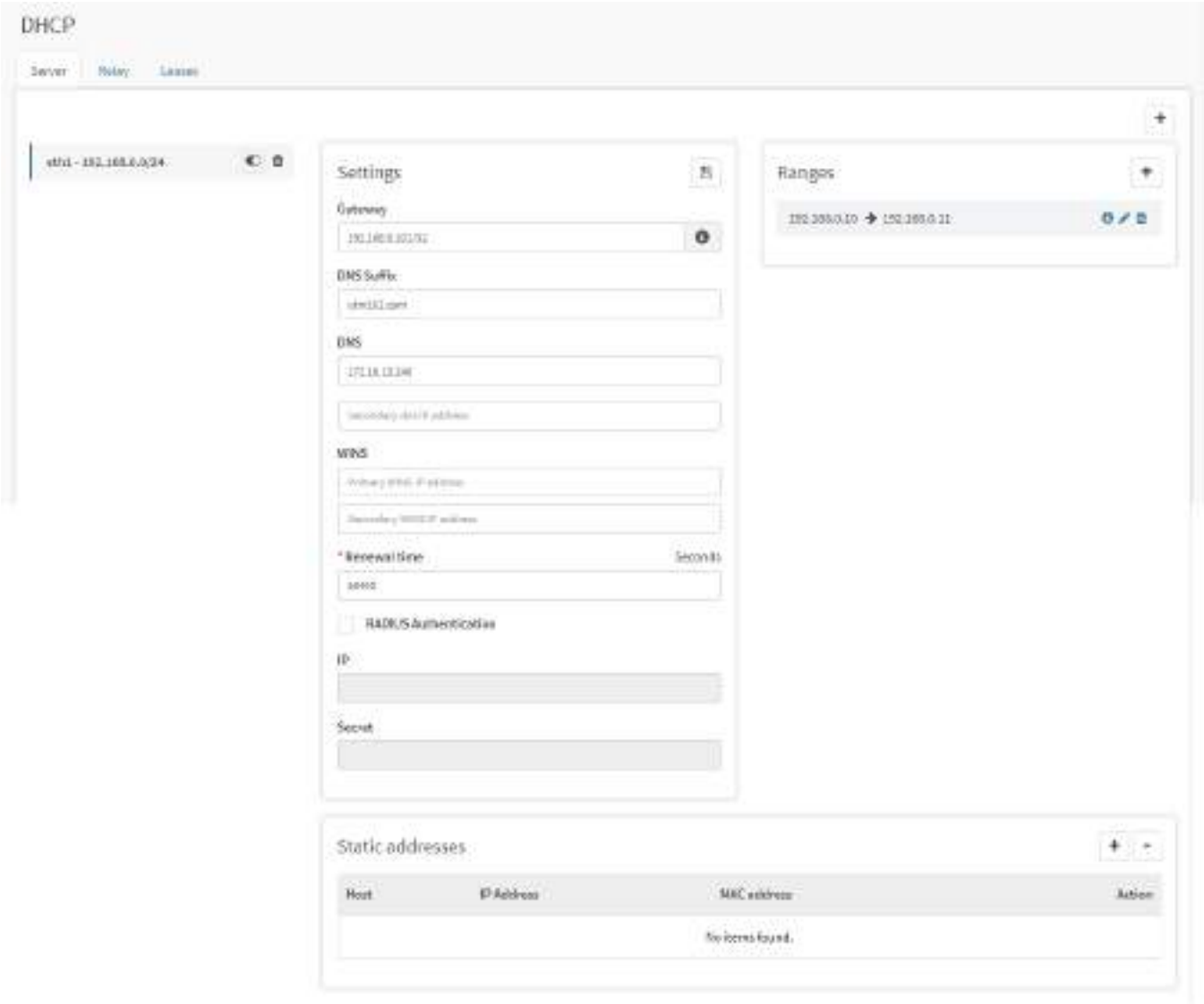
DHCP - Server

Para adicionar uma política de *DHCP*, clique em **[ ]**, e selecione um Device para distribuição de endereços *IP* na rede. Note que o default *Type* será *IPv4*.

DHCP - 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*.



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:

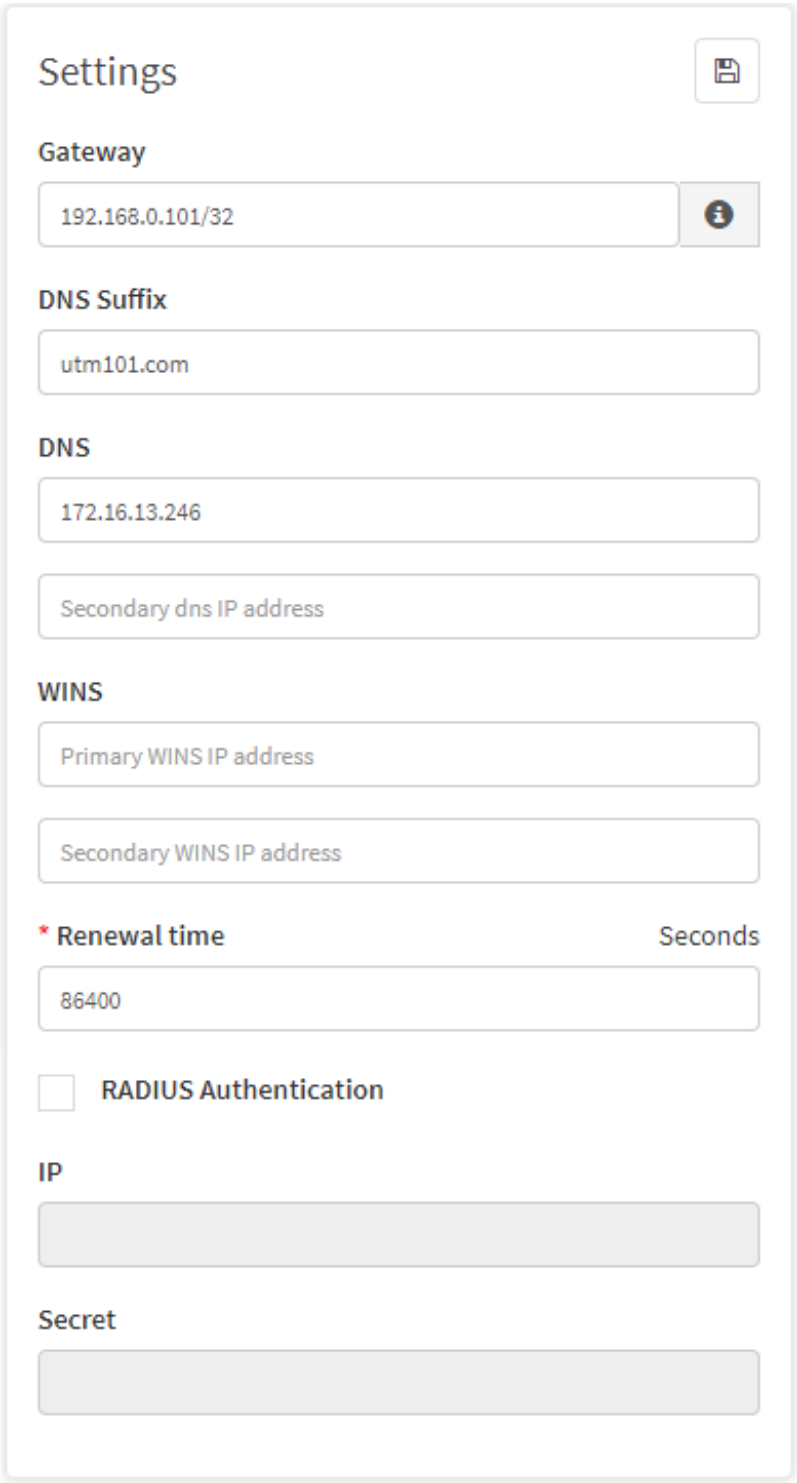
- *Settings*;
- Ranges;
- *Radius*;
- *Static Addresses*.

A seguir analisaremos cada uma delas.

DHCP Server - Settings

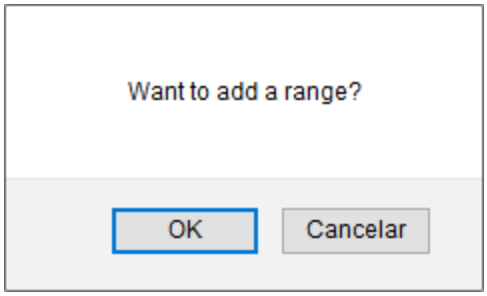
Para configuração dos parâmetros básicos para distribuição de endereços *IP*, no painel *Settings* configure os campos de acordo o formulário e os respectivos valores e endereços que pretende distribuir como válidos para o serviço *DHCP*. Depois clique em **[**  **].**

O endereço de Gateway obrigatoriamente deve estar dentro do intervalo de rede ou subnet declarada no device selecionado para configuração.



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:



DHCP - Adding a range

Ao clicar em [OK] você será automaticamente redirecionado para a interface de configurações do *range*.

A seguir, analisaremos as próximas seções:

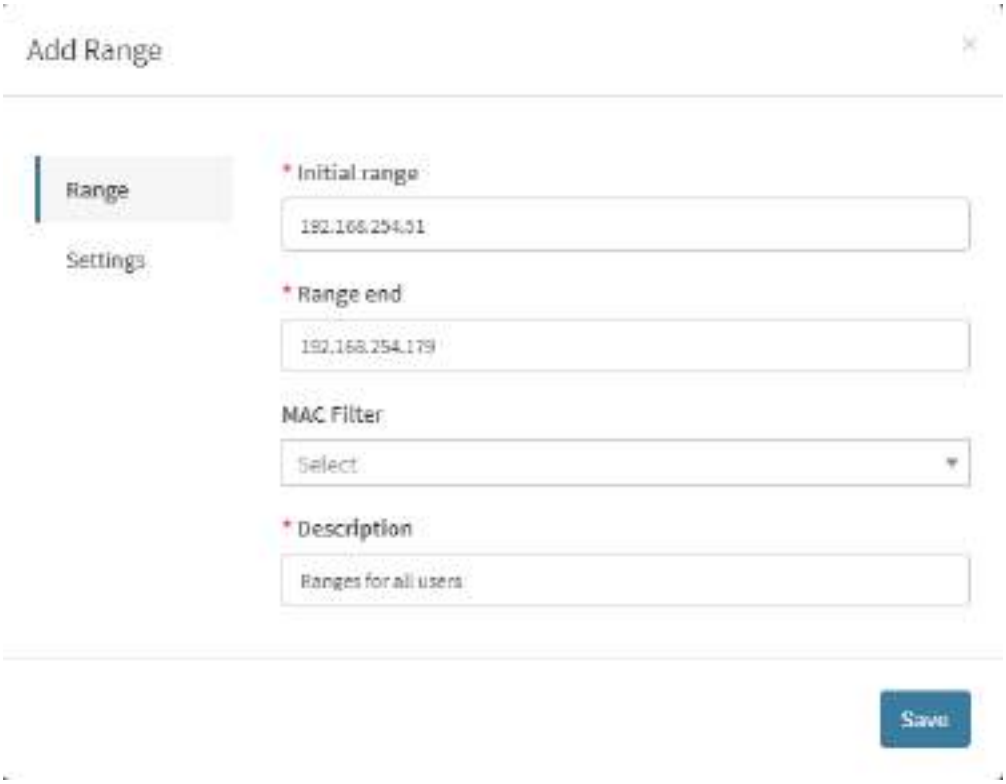
- Ranges;
- Radius;
- Static Addresses.

DHCP Server - Ranges

Nesta parte, você define qual o *“range”* ou “intervalo” de endereços *IP* que pretende distribuir pelo serviço *DHCP*.

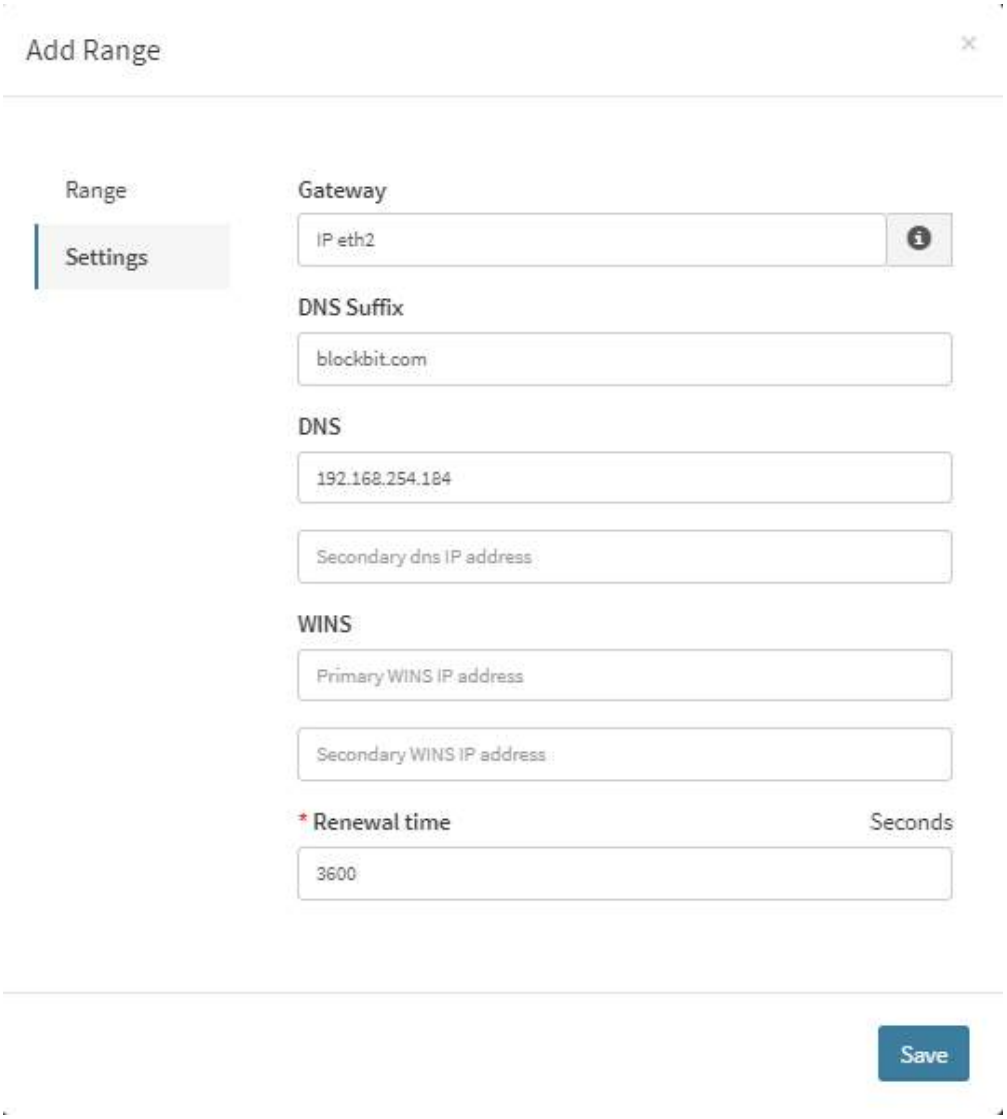
Para adicionar um *“range” ou “*intervalo” de endereço *IP*, clique em **[ ]**, e configure os campos de acordo.

Os 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.



Add Range - Range

- ***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*.



Add Range - Settings

- ***Gateway*:** Determina o *gateway* do *range*. Ex.: 192.168.254.190/32;
- ***DNS Suffix*:** Define o sufixo *DNS* do *range*. Ex.: blockbit.com;
- ***DNS*:** Determina o endereço primário e secundário do *DNS*. Ex.: 192.168.254.184;
- ***WINS*:** Define o endereço primário e secundário do servidor *WINS*;
- ***Renewal time*:** Tempo em segundos para a renovação do intervalo de *IPs*. Ex.: 3600.

Por fim, clique no botão **Save[** 

] para finalizar a criação do *range*.

A seguir, analisaremos as demais abas:

- Radius;
- Static Addresses.

DHCP Server - Radius

Autenticação DHCP por servidor RADIUS

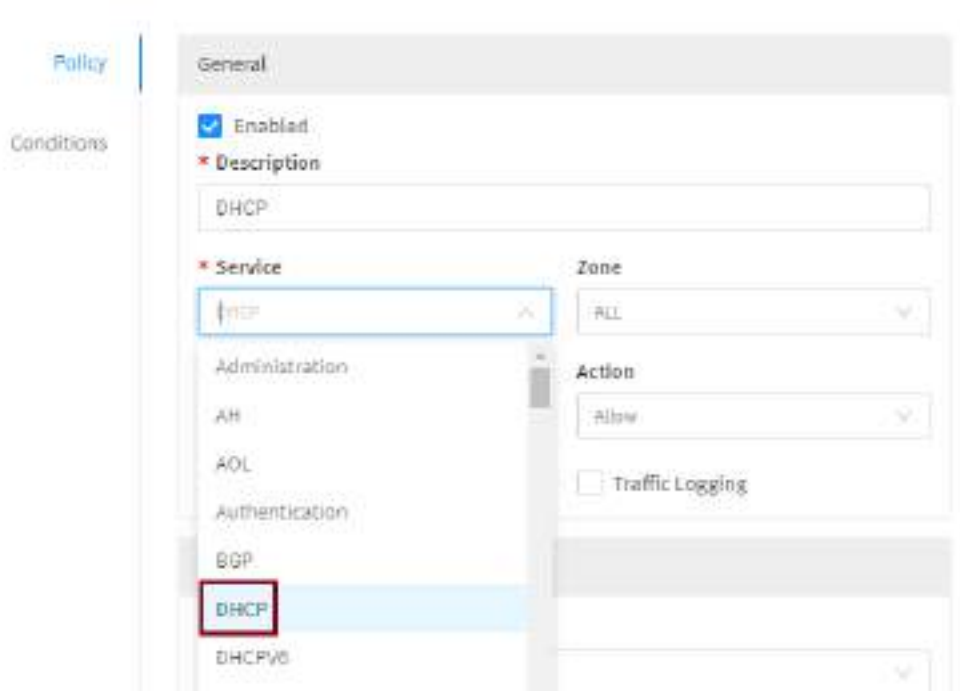
Em termos de autenticação, também é possível configurar um servidor RADIUS para a validação de usuários.

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:

Para tal, é necessário criar uma política em Zone Protection e selecionar "DHCP" entre as opções:

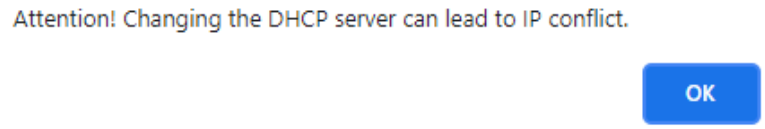


Seleção de serviço de autenticação: *Services* > *Firewall* > *Zone Protection* > Create[ ] ou Edit[ ] Zone Protection.

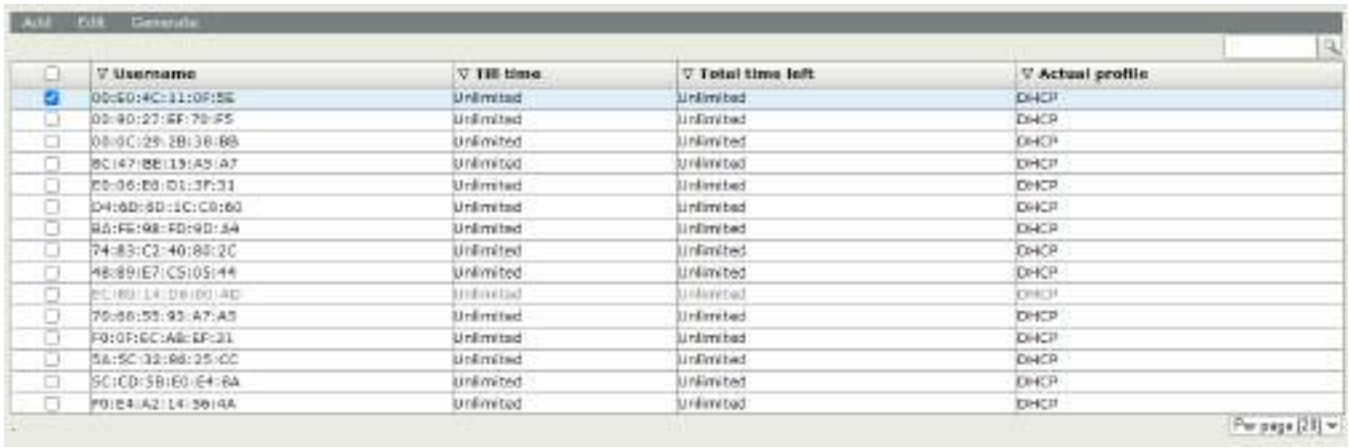
A seguir, devemos clicar na opção *DHCP* em *Services e* habilitar a opção *RADIUS Authentication:*

Tela de inserção de usuário e senha do servidor *RADIUS.*

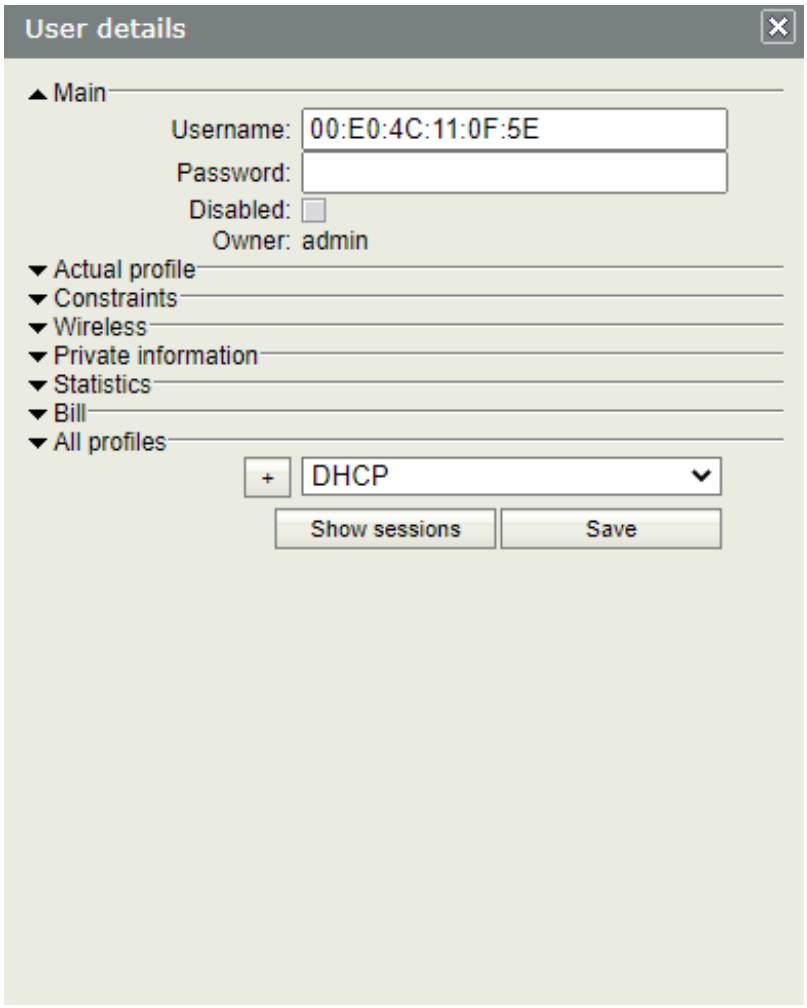
A seguinte mensagem será exibida, devemos clicar em *OK:*



É importante lembrar que o usuário no Servidor Radius (campo IP) deve ser o MAC address:



Exemplo de tela inicial de servidor Radius.



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 - Static Address

Para adicionar regras de distribuição de endereço *IP* no modo estático, por *Host*/*Mac Address*, clique em **[+]** e configure de acordo a definição de políticas para distribuição de endereços fixos na rede. Depois clique em **[Save].**

Ex.1:

- *Host: WinXen2012;*
- *IP Address: 192.168.254.184;*
- *MAC Address: 90:B1:1C:F6:2F:E2*.

DHCP reserve static address example 1

Ex.2:

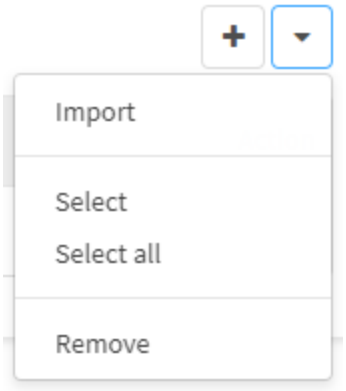
- *Host: NFS_CentOS7;*
- *IP Address: 192.168.254.202;*
- *MAC Address: 42:69:4C:3F:00.*

DHCP reserve static address example 2

Static addresses definition

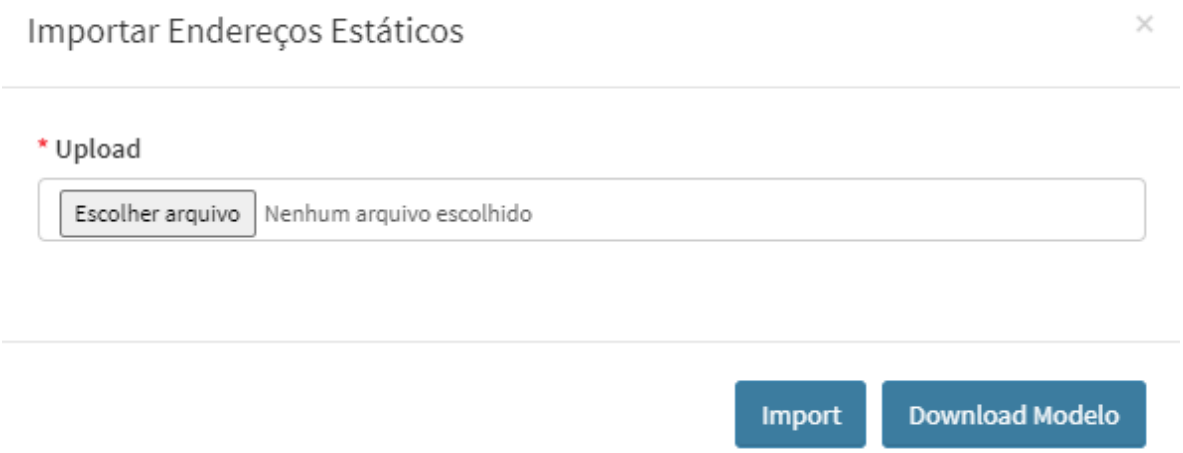
Importar múltiplos Hosts

Para importar múltiplos Hosts, basta clicar em [▾]:



Import multiple hosts

Em import, teremos a seguinte tela:



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.

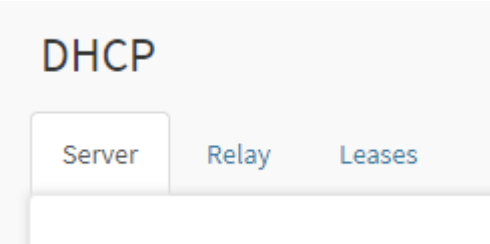
Para habilitar a distribuição automática dos endereços declarados no serviço *DHCP*, clique em habilitar **[ ]**.

A seguir analisaremos as demais abas:

- Relay;
- Leases.

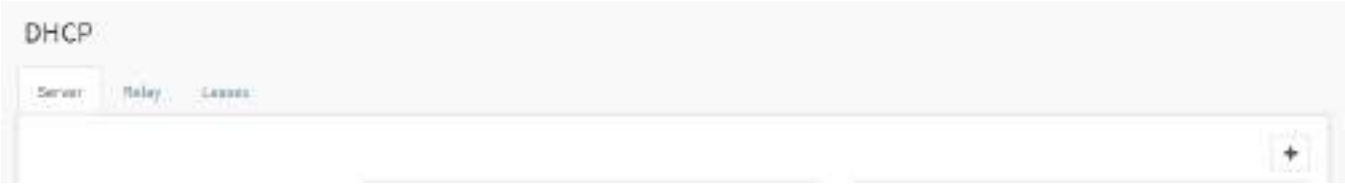
DHCP - Aba Server IPv6

Para configurar os servidores de *DHCP*, IPv4 e IPv6 selecione a aba correta:



Aba *Server*

Surgirá a tela *a seguir*, conforme demonstrado pela imagem abaixo:



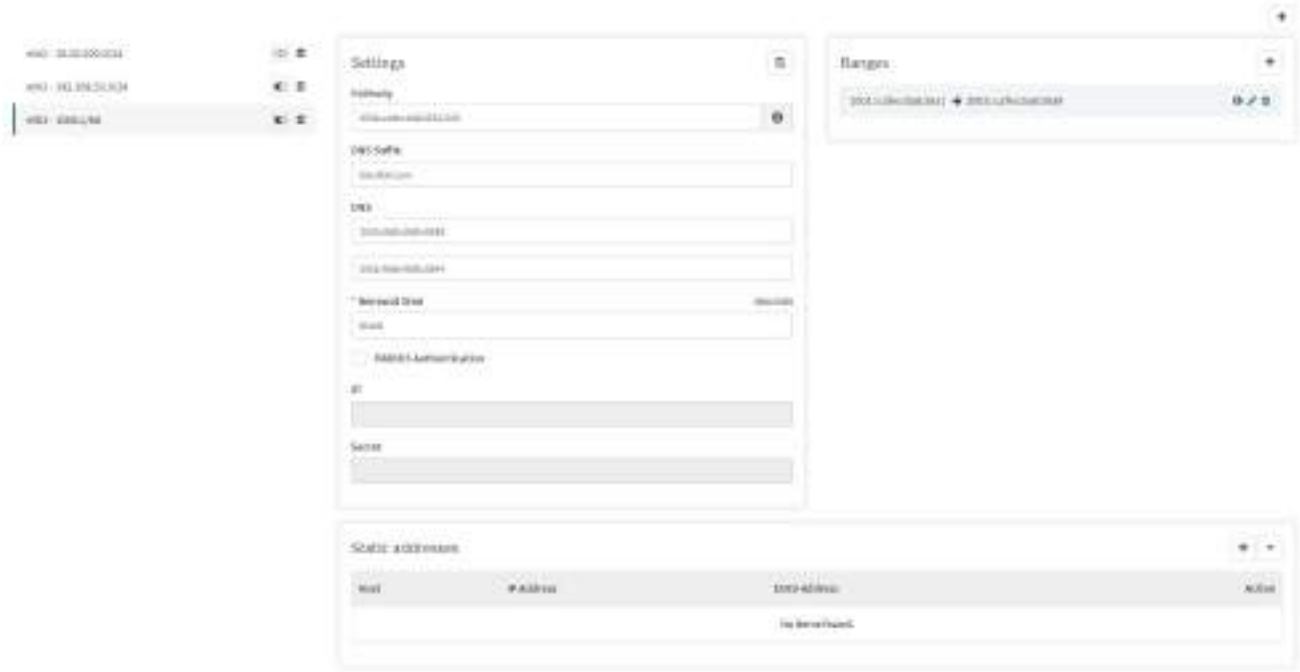
DHCP - Server

Para adicionar uma política de *DHCP*, clique em **[ ]**, e selecione um Device para distribuição de endereços *IP* na rede. Note que o default *Type* será *IPv4. Abra a lista e selecione o IPv6.*

DHCP - 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*.



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.

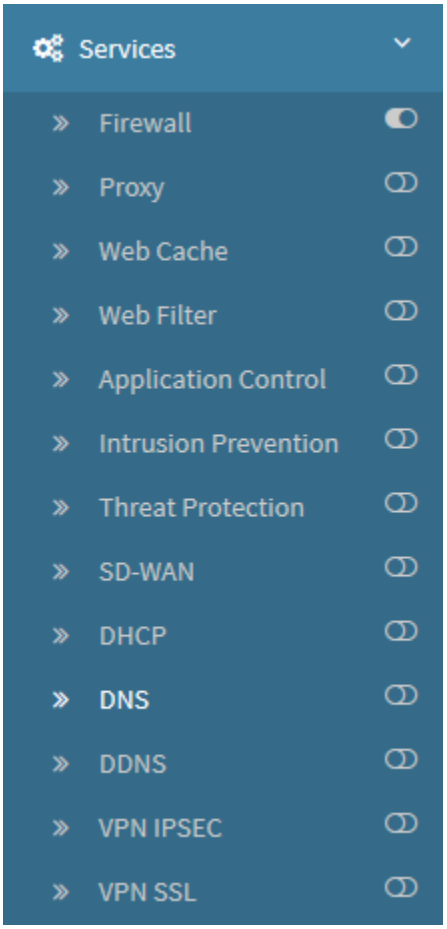
UTM - Services - DNS

O Serviço de *DNS* (Domain Name System) é o responsável em fornecer o recurso de “tradução de nomes de domínios” para seus respectivos endereços *I*
.

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.

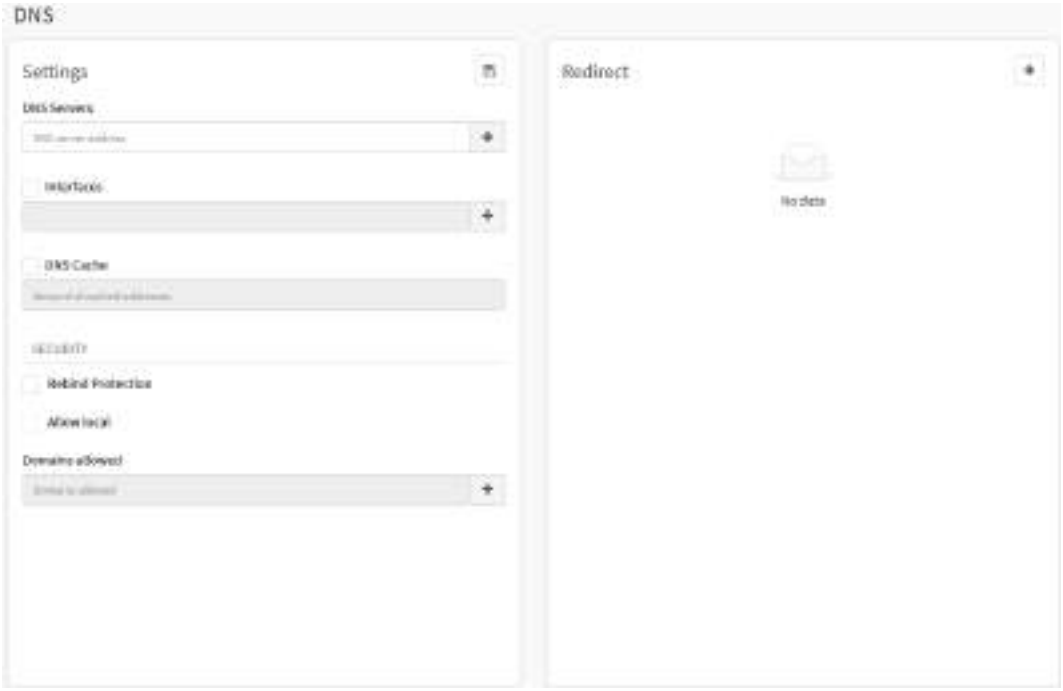
O serviço *DNS* conta com a integração ao recurso de *Caching*, lida com as consultas dos clientes *DNS* e armazena a resposta em seu *cache* local por um determinado tempo permitido pelo *TTL* dos respectivos registros dos domínios consultados. O *Cache* é usado como uma fonte para os próximos pedidos, 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:



Services - Interface DNS

A interface *DNS* está dividida nos painéis:

- *Settings*;
- *Redirect*.

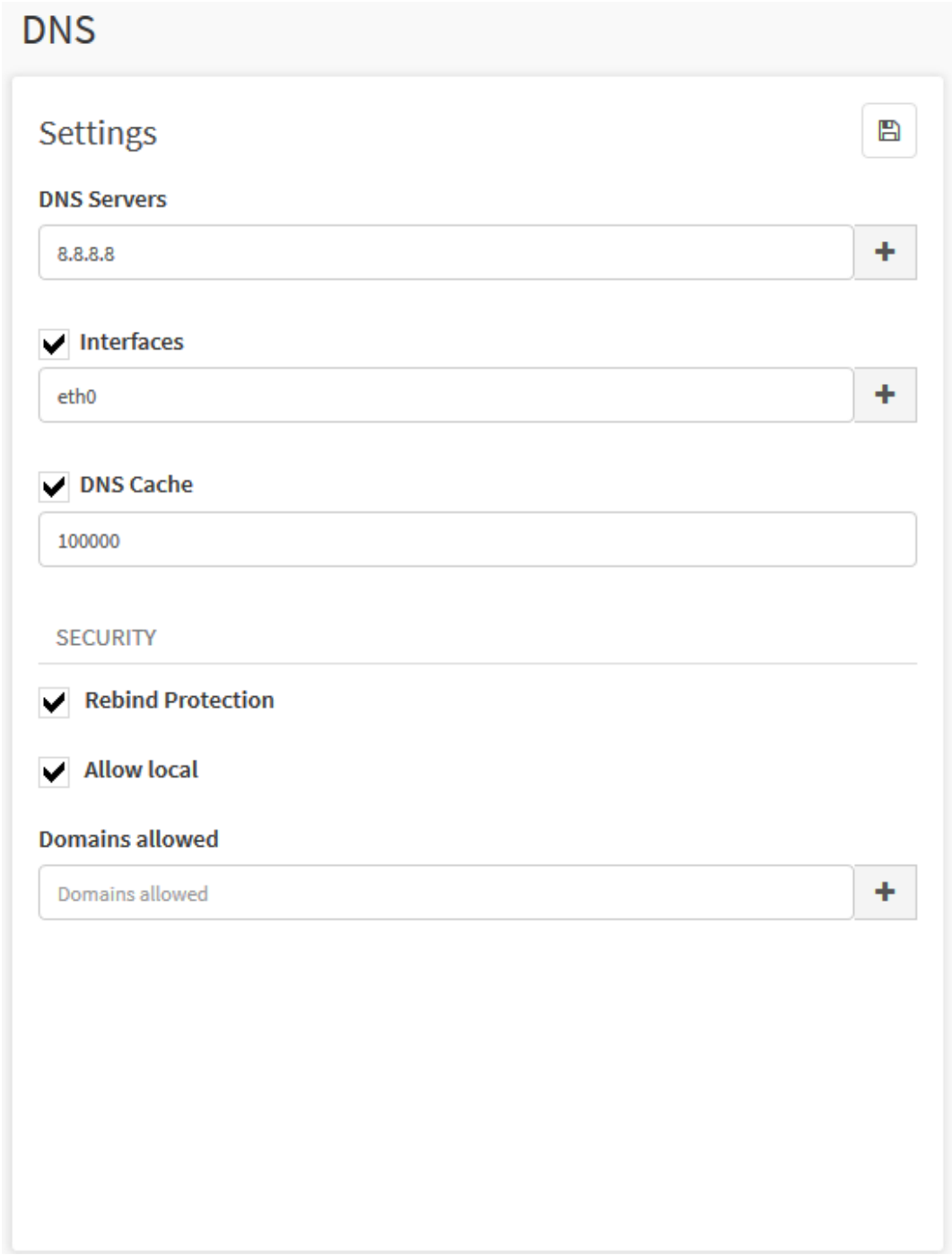
A seguir analisaremos os componentes da desta tela.

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

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 *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*** **[**  **]*:*** 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, clique no botão **[**  **]**, após ter adicionado outros domínios, clique em **[**  **]** para removê-los;

Depois de ter efetuado as configurações, clique em **[**  **]** para salvá-las.

Após salvar, para que as alterações entrem em vigor 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.

Após realizar esses procedimentos o *DNS* terá sido configurado com sucesso.

DNS - Redirect

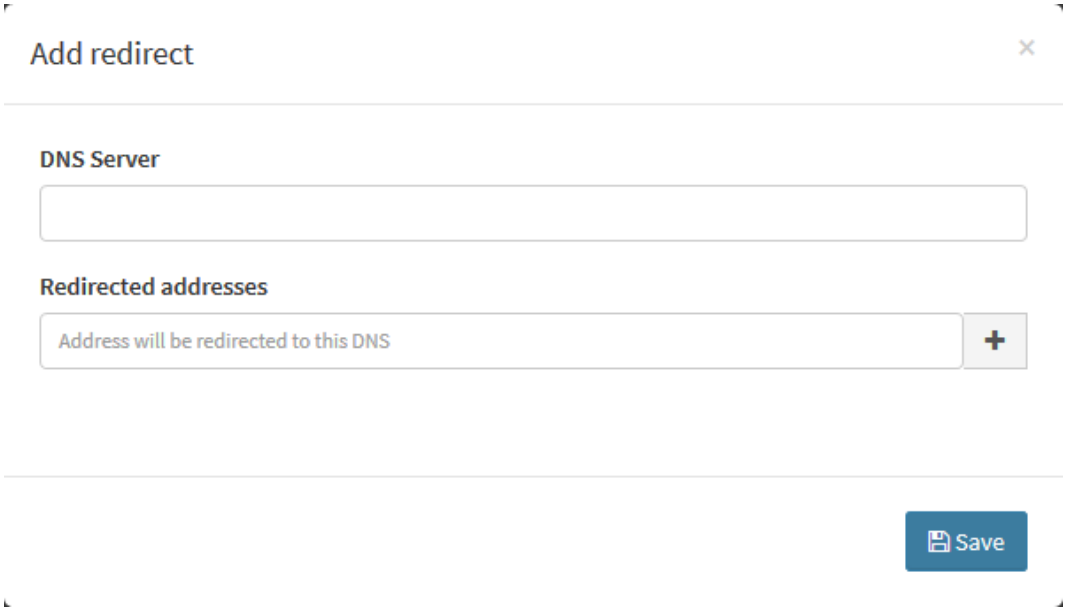
Nesta área você pode configurar o serviço de redirecionamento das requisições *DNS* para *"Que outros servidores DNS"* sejam os *"Responsáveis"* em realizar as consultas recursivas *"Exclusivas"* para uma *"lista de hosts".*

O serviço permite através da distribuição e balanceamento das pesquisas para *hosts* específicos, redirecionar o serviço para outro servidor *DNS* exclusivo para os *hosts* especificados.

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*.

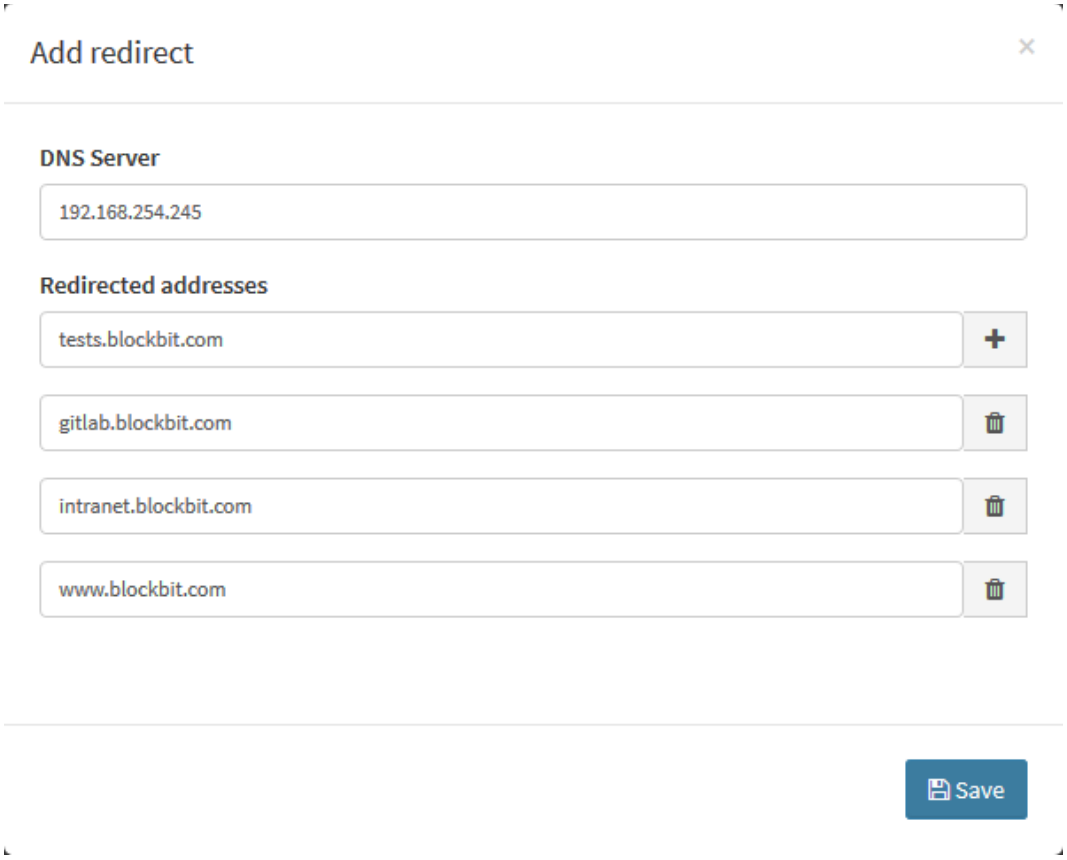
No quadro *Redirect* clique em **[ ]** e configure apontando o endereço do servidor *DNS* e adicionando a lista de *hosts* que pretende redirecionar as pesquisas recursivas.



DNS - Add redirect

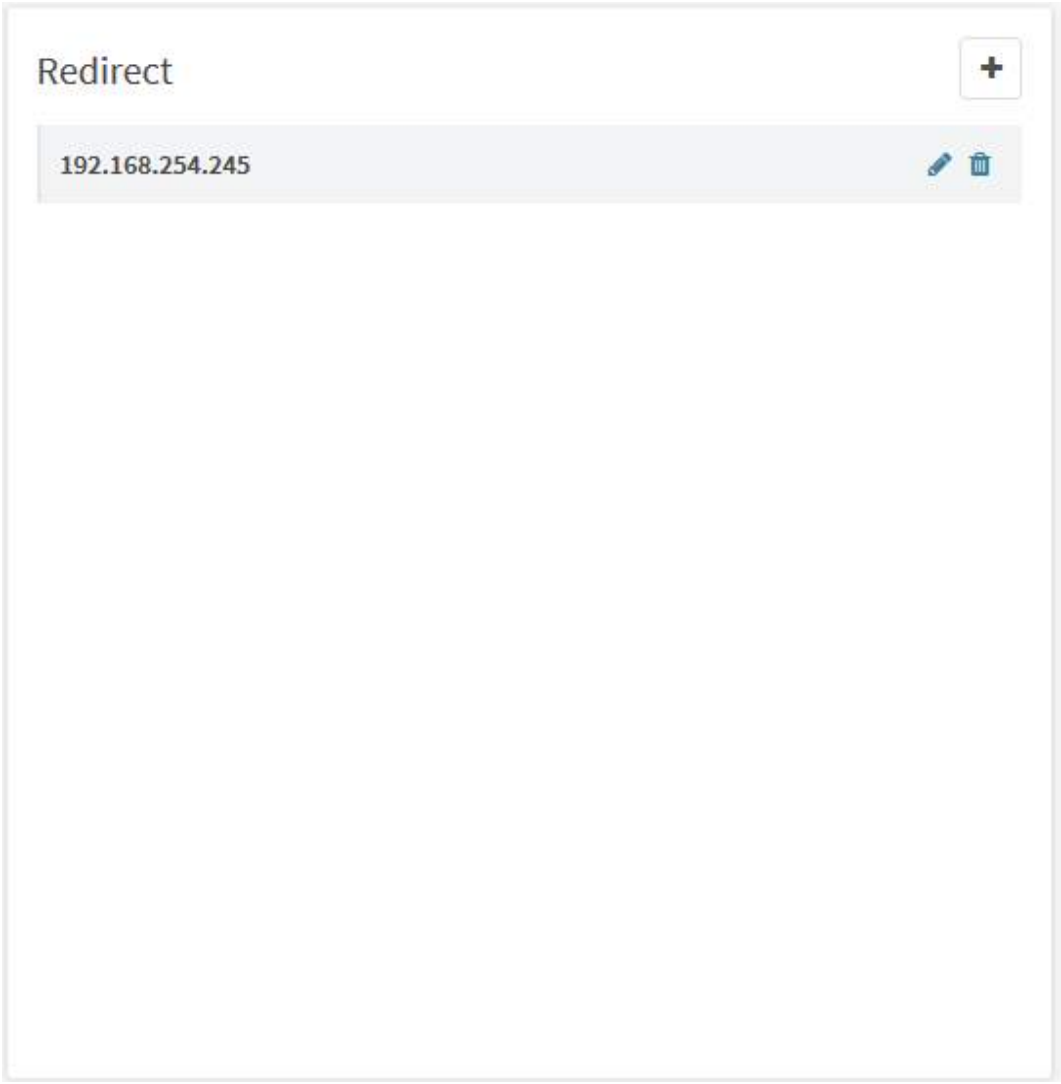
- ***DNS Server*:** Adicionar o servidor *DNS* que será utilizado. Caso queira adicionar outros domínios, clique no botão **[ ]**, após ter adicionado outros domínios, clique em **[ ]** para removê-los;
- ***Redirected addresses*:** Adicionar os endereços para onde será efetuado o redirecionamento. Caso queira adicionar endereços extras, clique no botão **[ ]**, após ter adicionado outros endereços, caso seja necessário, clique em **[ ]** para removê-los.

Vamos exemplificar a pesquisa a uma lista de *hosts* em um *DNS* Server local, conforme demonstrado pela imagem a seguir:



DNS - Add redirect - Example

Feitas as alterações, clique em [Save] para salvar todas as configurações.

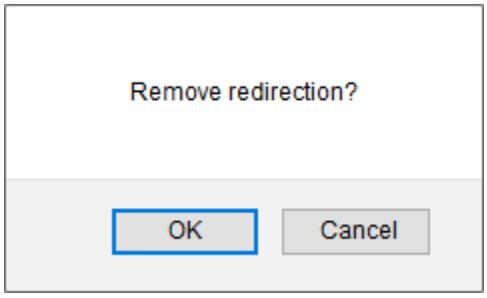


DNS - Redirect added

Após salvar, para que as alterações entrem em vigor 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.

Caso seja necessário editar os dados adicionados, clique no botão **[** **]** e efetue as configurações necessárias.

Caso pretenda removê-los clique em **[** **]**, a seguinte mensagem será exibida:



Remove redirection

Clique em [OK] para concluir a exclusão, caso contrário, clique em [Cancel] para fechar esta janela

Após estes passos, o redirecionamento de *DNS* terá sido configurado com sucesso.

UTM - Services - DDNS (DynDns)

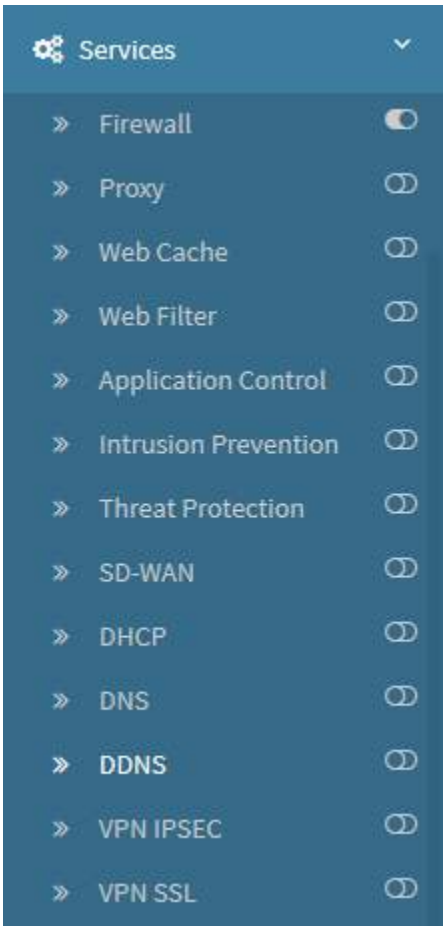
O serviço *DDNS* (*Dynamic Domain Name System*) é um gerenciador de um serviço de tradução de nomes para endereços *IP* dinâmicos. O *DDNS* é o método usado para atualizar a tabela de *IPs*/*hosts* públicos automaticamente em um servidor *DNS* em tempo real e isso com o propósito de manter ativo e publicado 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 - DDNS

A tela abaixo será exibida:

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.

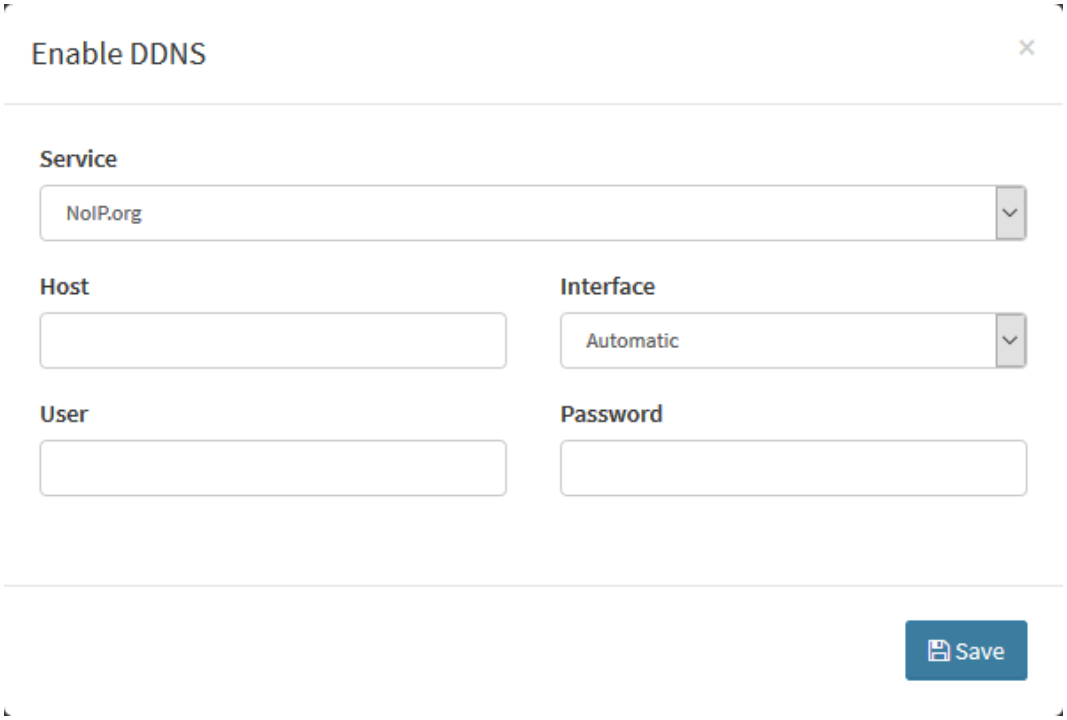
- Recursos *DDNS.*
  - Suporte aos provedores de serviço.
    - NoIP.org;
    - DynDNS.com.
  - Suporte a interfaces.
    - *Ethernet*;
    - *Vlan*;
    - *MacVlan* (Interface virtual).
  - Integração com os serviços
    - *DNS*;
    - *VPN*;
    - *Firewall*;
    - Políticas de segurança.
  - Atualização *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 um *DDNS* clique em **[ ]**. A seguinte janela será exibida:



DDNS - Enable DDNS

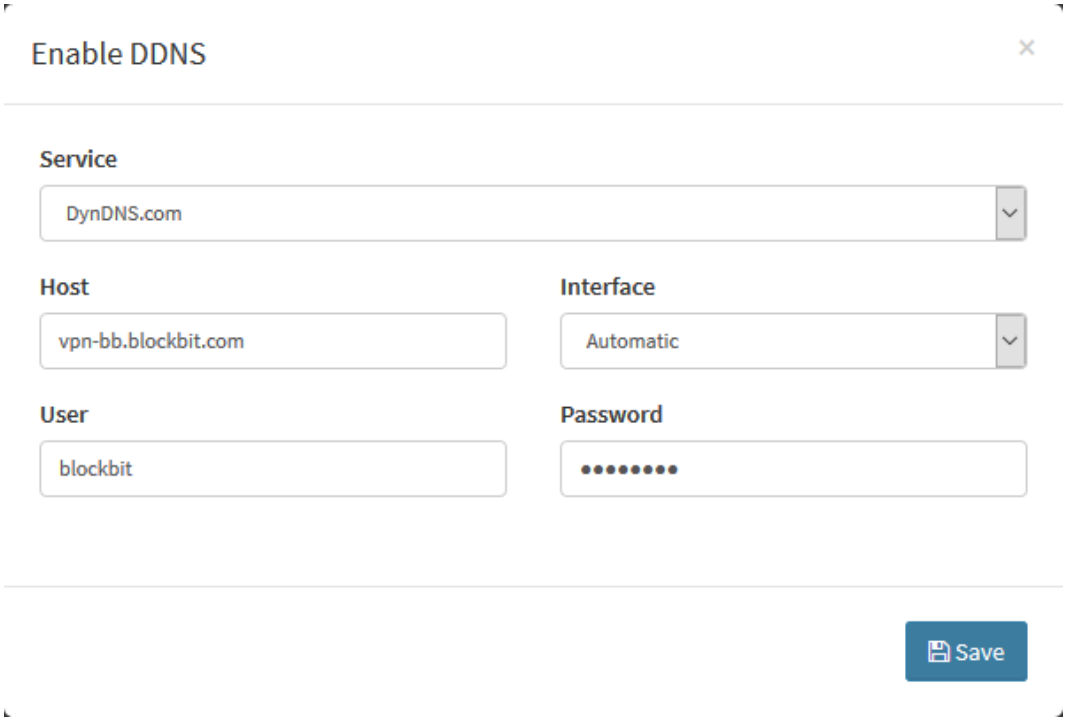
Configure o formulário de acordo as especificações para conexão com o provedor conforme o exemplo dado.

- ***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.



DDNS - Enable DDNS - Example

Depois de ter efetuado as configurações, clique em [Save] para salvá-las.

Após salvar, para que as alterações entrem em vigor 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.

Após realizar esses procedimentos o *DDNS* terá sido configurado com sucesso.

DDNS - Dynamic DNS Added

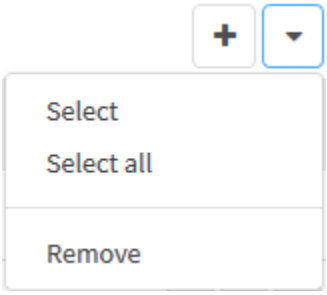
O Serviço *DDNS* já está configurado e o *host* "*vpn-bb.blockbit.com*" respondendo pelo endereço *IP* da interface de rede correspondente a rota *default*.

DDNS - Menu de ações

No topo direito da tela, ao lado do botão de adição temos o menu de ações:

DDNS – Botão do menu de ações

Ao clicar neste botão o menu abaixo é exibido:



DDNS – Menu de ações

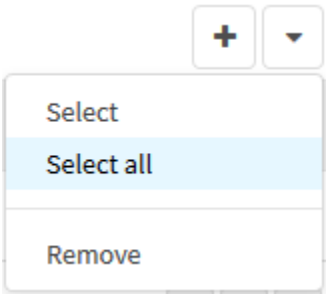
O menu é composto das seguintes opções:

- *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.

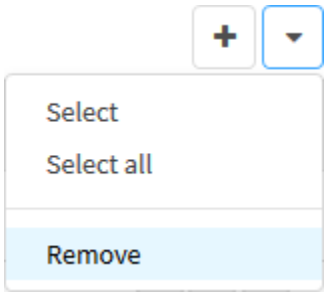
DDNS - Menu de Ações - Remove

Através do menu de ações é possível deletar vários itens ao mesmo tempo. Siga os seguintes passos:

1. Selecione os itens que deseja deletar clicando no ícone de **seleção[ ]**;

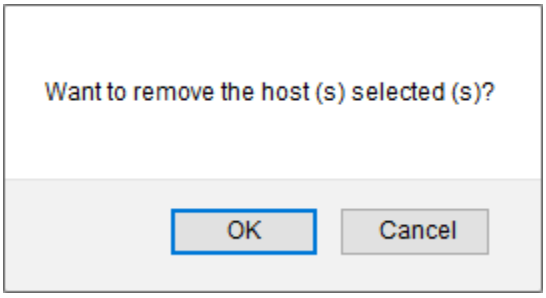
DDNS - Seleção para deleção

2. Clique no **Menu de ações[ ]** e selecione a opção “*Remove*”;



DDNS – Menu de ações – *Remove*

4. Surgirá uma tela perguntado se deseja deletar o item selecionado:



DDNS - Remove itens

Caso deseje cancelar clique no botão [Cancel]. Para concluir a deleção clique no botão [OK].

O item foi deletado com sucesso.