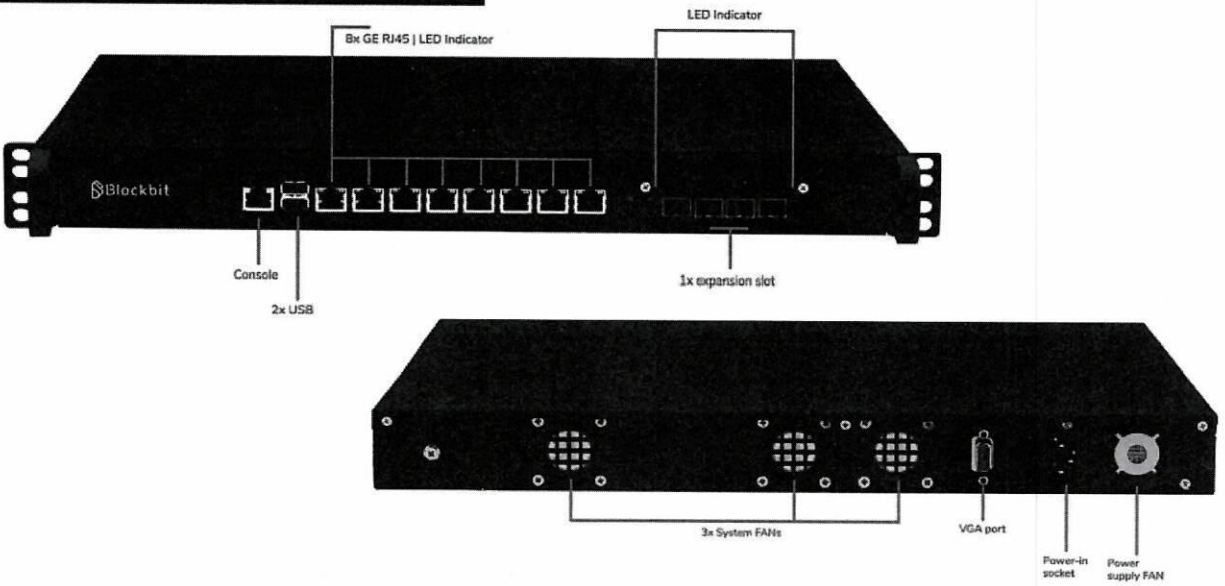
Grandes Empresas

MODELO: BB500 | BB1000



Especificações de Desempenho e Opcionais

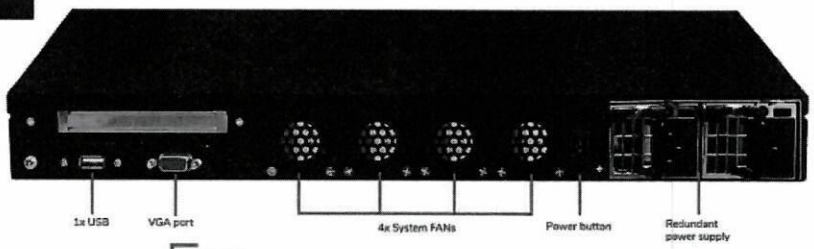
	BB500	BB1000
Firewall Throughput (UDP)	20 Gbps	35 Gbps
Conexões Simultâneas	12.000.000	18.000.000
Conexões Novas Por Segundo	80.000	120.000
NGFW Throughput (IMIX)[1]	2 Gbps	2.8 Gbps
Web Filter Throughput	4 Gbps	6 Gbps
SSL Inspection Throughput	1.4 Gbps	2.2 Gbps
IPS Throughput	4 Gbps	6 Gbps
Application Control Throughput	1.6 Gbps	2 Gbps
Threat Protection Throughput	1 Gbps	1.5 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	4 Gbps	5 Gbps
SSL VPN Throughput (AES-256)	1.6 Gbps	2 Gbps
Interfaces de Rede	8X GE RJ45	8X GE RJ45
Armazenamento	240 GB	240 GB
Característica Física	1U para Rack 19´´	1U para Rack 19´´
Alimentação	100/240V AC	100/240V AC
Dimensões (Largura x Profundidade x Altura)	360mm x 430mm x 46mm	
Temperatura Ideal de Operação	-20°C (-4°F) ~ 70°C (158°F)	

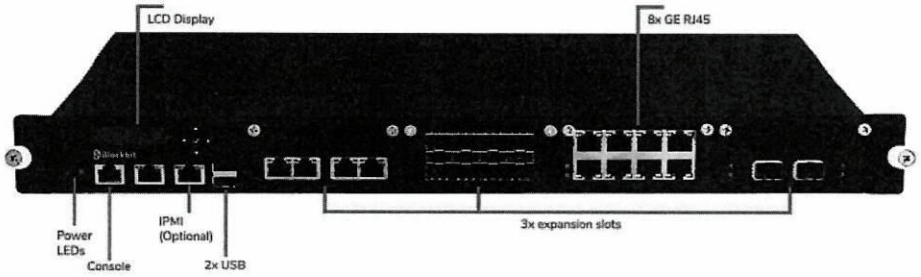
Opcionais

Unidade de Estado Sólido (SSD)	480 GB	480 GB
LTE 3G/4G	Sim	Sim
Módulo Rede 10GbE - 2 portas SFP+	Sim	Sim
Módulo Rede 1GbE - 4 portas SFP	Sim	Sim
Fonte Redundante 100-220V AC	Sim	Sim

Grandes Empresas

MODELO: BB2000





Especificações de Desempenho e Opcionais

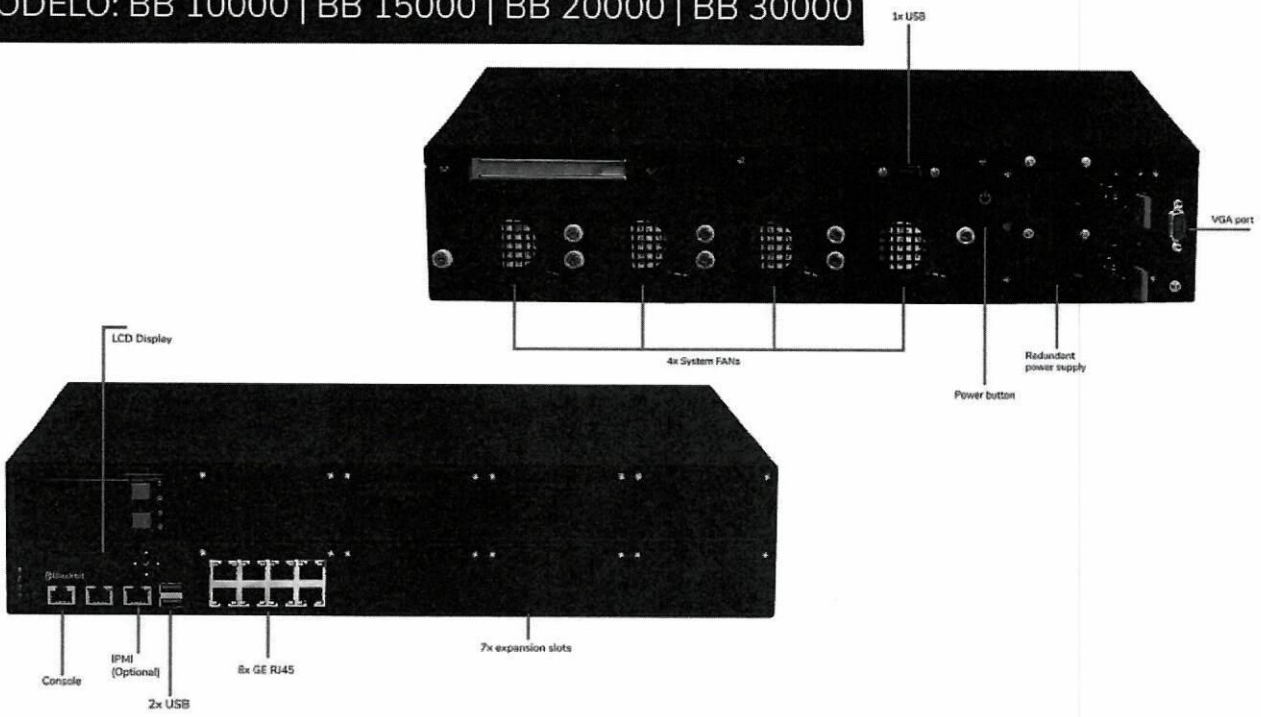
	BB2000
Firewall Throughput (UDP)	55 Gbps
Conexões Simultâneas	22.000.000
Conexões Novas Por Segundo	200.000
NGFW Throughput (IMIX)[1]	5 Gbps
Web Filter Throughput	10 Gbps
SSL Inspection Throughput	4.5 Gbps
IPS Throughput	9.0 Gbps
Application Control Throughput	5 Gbps
Threat Protection Throughput	4.5 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	10 Gbps
SSL VPN Throughput (AES-256)	6.5 Gbps
Interfaces de Rede	8X GE RJ45
Armazenamento	240 GB
Característica Física	1U para Rack 19´´
Dimensões (Largura x Profundidade x Altura)	438mm x 415mm x 44mm
Temperatura Ideal de Operação	-20°C (-4°F) ~ 70°C (158°F)
Fonte Redundante	Sim - 100/240V AC

Opcionais

Unidade de Estado Sólido (SSD)	480 GB
Módulo de Rede 10GbE - 4 portas SFP+	Sim
Módulo Rede 1GbE - 8 portas SFP	Sim
Módulo Rede 1GbE - 4 portas SFP c/ bypass	Sim
Módulo Rede 1GbE - 8 portas RJ45	Sim
Módulo Rede 1GbE - 8 portas RJ45 c/ bypass	Sim
Slots disponíveis	3x

Grandes Empresas

MODELO: BB 10000 | BB 15000 | BB 20000 | BB 30000



Especificações de Desempenho e Opcionais

	BB10000	BB15000	BB20000	BB30000
Firewall Throughput (UDP)	80 Gbps	100 Gbps	160 Gbps	200 Gbps
Conexões Simultâneas	30.000.000	45.000.000	55.000.000	70.000.000
Conexões Novas Por Segundo	300.000	400.000	520.000	700.000
NGFW Throughput (IMIX)[1]	7 Gbps	12 Gbps	20 Gbps	30 Gbps
Web Filter Throughput	12 Gbps	15 Gbps	25 Gbps	35 Gbps
SSL Inspection Throughput	6 Gbps	8 Gbps	12 Gbps	20 Gbps
IPS Throughput	12 Gbps	15 Gbps	23 Gbps	30 Gbps
Application Control Throughput	7 Gbps	10 Gbps	16 Gbps	24 Gbps
Threat Protection Throughput	6 Gbps	9.6 Gbps	12 Gbps	18 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	15 Gbps	18 Gbps	25.6 Gbps	30 Gbps
SSL VPN Throughput (AES-256)	7 Gbps	8 Gbps	11 Gbps	15 Gbps
Interfaces De Rede	8X GE RJ45	8X GE RJ45	8X GE RJ45	8X GE RJ45
Interfaces De Rede Opicionais	8x SFP / 8x SFP+	8x SFP / 8x SFP+	8x SFP / 8x SFP+	8x SFP / 8x SFP+
Fonte de Energia Redundante 110/220v	Sim	Sim	Sim	Sim
Armazenamento	480 GB	480 GB	1 TB	1 TB
Característica Física	2U para Rack 19''			
Dimensões (Largura x Profundidade x Altura)	440mm x 710mm x 880mm			
Temperatura Ideal de Operação	0°C (32°F) ~ 40°C (104°F)			

Opcionais - BB10000 | BB15000 | BB20000 | BB30000

Unidade de Estado Sólido (SSD)	1 TB	1 TB	1 TB
RAID 0/1	Sim	Sim	Sim
Módulo de Rede 40 GbE - 2 portas QSFP+	Sim	Sim	Sim
Módulo de Rede 10 GbE - 4 portas SFP+	Sim	Sim	Sim
Módulo de Rede 10 GbE - 2 portas SFP+ c/ bypass	Sim	Sim	Sim
Módulo Rede 1GbE - 8 portas SFP	Sim	Sim	Sim
Módulo Rede 1GbE - 4 portas SFP c/ bypass	Sim	Sim	Sim
Módulo Rede 1GbE - 8 portas RJ45	Sim	Sim	Sim
Módulo Rede 1GbE - 8 portas RJ45 c/ bypass	Sim	Sim	Sim
Slots disponíveis	7x	7x	7x

Virtual appliances

	Firewall Throughput (UDP)
BBV 2	3.7 Gbps
BBV 5	4 Gbps
BBV 10	6 Gbps
BBV 50	8 Gbps
BBV 100	10 Gbps
BBV 500	20 Gbps
BBV 1000	35 Gbps
BBV 2000	55 Gbps
BBV 10000	80 Gbps
BBV 15000	100 Gbps
BBV 20000	160 Gbps
BBV 30000	200 Gbps

Acessórios que acompanham os equipamentos:

- Bandejas para rack (equipamentos BB 02, BB 05, BB 10 e BB 30)
- Trilhos para montagem em Rack (BB 50, BB 100, BB 200, BB 500, BB 1000, BB 2000, BB 10000, BB 15000, BB 20000 e BB 30000)
- Cabos de energia padão IEC-320 C14
- Cabo serial RS-232/RJ-45 com adaptador RS-232/USB plug and play (sem necessidade de instalação de driver)

Todos os acessórios (bandejas e trilhos para montagem em Rack 19´´ e cabos de energia) são fornecidos pela Blockbit. Os módulos de Fibra e Rede (SFP, SFP+, QSFP+, RJ45) acompanham os transeivers (GBic) para os respectivos módulos e modelos e os cordões opticos multimodo ou monomodo conforme a necessidade do projeto.

Políticas de Segurança:

- Suporta IPv4 e IPv6
- IP de Origem/Destino, Porta e Protocolo
- Subnet de Origem/Destino
- Por usuários, grupos, IPs, redes e Zona (LAN, WAN, DMZ) e código de país (BR, EUA, etc)
- Controle por aplicações, grupos estásticos e dinâmicos
- Filtragem
- Conteúdo web, Aplicações Web
- Perfis de Inspeções: SSL, IPS, Threat Protection, Web Filter e Application Control (podendo ser implementados em uma única política e a alteração de uma engine não impacta em outras)
- QoS (controle de banda/priorização)
- Múltiplos serviços
- Editor de regras de segurança (políticas de filtragem) com possibilidade de agendamento
- Habitar e desabilitar logs
- Tipos de ação: permitir, negar e rejeitar
- Criação de políticas por usuários ou grupos baseado em autenticação para todos os serviços (Firewall, VPN, IPS, Controle de Aplicação e outros)
- Simulador de tráfego, localizador e validador de política
- Detector de Políticas conflitantes no UTM e no GSM
- Bloqueio de arquivo por extensão e permite a correta identificação do arquivo por seu tipo MIME, mesmo quando sua extensão for renomeada

Web Cache e Proxy:

- Proxy Transparente ou Explícito (portas personalizadas)
- Configuração de tamanho de Cache em Disco e Memória
- Suporte a serviços web (HTTP e HTTPS versões 1.0, 1.1, 2.0 e FTP)
- Configuração de web cache em memória e disco
- Habilitação de web cache de conteúdos dinâmicos (Facebook, Google Maps, MSN Video, Sourceforge Downloads, Windows Update, Youtube)
- Exceção de cache, configurável por expressões regulares
- Hierarquia de proxy com e sem autenticação
- Suporte à integração Antivírus HTTP através de hierarquia de proxy
- Mensagem de bloqueio para o usuário final
- Suporta política por tempo, horário e/ou período (dia, mês, ano, dia da semana e hora). Suporta grupos de usuários, IPs, rede e/ou zonas de segurança

Firewall:

- Política com opção de autenticação com possibilidade de habilitar ou desabilitar log
- NAT (SNAT e DNAT), 1:1, N:1, NAT64, NAT46, NAT44 e NAT66, PAT, NAT de Origem e NAT de Destino e simultâneamente
- NAT dinâmico (Many-to-Many e Many-to-1)
- NAT estático (1:1 e Many-to-Many) e bidirecional 1:1
- Segurança
- Proteção DoS (Denial Of Service) também disponível na Política, PortScan, Pacotes inválidos, ICMP Sweep e Brute Force
- Proteção Flood (SYN, ICMP, UDP)
- Proteção Anti-spoofing
- ICMP (controles, transmissão, redirecionamento)
- PING (Echo/Request)
- Forward de Multicast
- Source routing, Checksum, Log inválidos
- Flow Control para aplicações Dinâmicas
- Bloqueio de tráfego de protocolos em portas customizadas
- Suporta objetos e regras multicast
- TCP_be_liberal
- IP spoofing
- Proteção contra ataques Man-in-the-Middle
- Controles de conexão TCP/UDP/ICMP/IP
- Suporta modo transparente (camada 2), modo gateway (camada 3) e espelhamento de porta
- Suporta os protocolos de real time

QoS – Qualidade de Serviço

- Marcação de pacotes para priorização de tráfego (TOS e DSCP)
- Fila de Prioridade de Menor Prioridade para Maior Prioridade
- Controle de tráfego e garantia de banda por política (aplicações, usuários ou grupos de usuários sincronizados com o Windows AD ou LDAP), zona de rede, host específico ou origem/destino

IPS - Sistema de Prevenção de Intrusos:

- Detecção e prevenção de ataques e intrusões baseada em +80mil assinaturas agrupadas como Client (Aplicações) e Server (Servidores)
- Suporte a Customização e upload de Assinaturas
- Níveis de Impacto: Baixo, Médio e Alto
- Proteção contra ameaças na camada de aplicação (Exploit conhecidos, Shellcode, SQL Injection, Buffer overflow etc.)
- Proteção contra pacotes mal-formados
- Reconhecimento de padrões, analise de protocolos e anomalias e bloqueia vulnerabilidades
- Capacidade de remontagem do pacote após a análise para identificação de ataques
- Limite de Sessões de Origens (Source Session Limit) com TCP Reset para encerramento da sessão
- Prevenção DoS, DDoS (Flood, Scan, Session e Sweepe), PORTSCAN, Reconnaissance, Evasione e ICMP
- Atenuação de ataques DoS e DDoS (negação de serviços)
- Prevenção contra ataques de tecnologia P2P
- Prevenção contra ataques do tipo Worm, Trojan, Backdoors, Portscans (detecta e bloqueia a origem), IP Spoofing, SYN-ICMP-UDP flood e Spywares
- Prevenção contra anomalias de protocolos (HTTP, SMTP, POP, IMAP, Sendmail, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, CIFS, RPC, RDP, CHARGEN, SSDP, SNMP, TCP highjacking, SSH e Telnet)
- Prevenção contra Botnet, DNS Poisoning e Scalation Privilege
- Bloqueio de SSH em portas não padrão do protocolo e baseado no comportamento através de padrões
- Suporte a configuração de exceção por assinatura de origem ou destino
- Log de registro das incidências para cada tipo de ataque identificado
- Trafego mal formado e cabeçalhos invalidos
- Atualização automática, periódica e offline
- Decodifica múltiplos formatos de unicode
- Fragmentação e desfragmentação IP
- Políticas aplicadas em interfaces ou zona de segurança
- Alarme via e-mail ou trap de SNMP
- Suporte a implementação inline L2 (bridge/modo transparente) e camada L3 (firewall)
- Suporta exceções por IP cadastrado nas regras
- Criação de Whitelist e Blacklist por IP (IPv4 e IPv6)
- Permite ativar ou desativar as assinaturas, ou habilitar em modo de monitoração

Threat Protection:

- Antivírus e Anti-Malware com analise em tempo real
- HTTP, HTTPS, FTP, SMB, CIFS, POP3 e SMTP (nativo na solução)
- Proteção contra aplicações não autorizadas
- (Packed, PwTool, NetTool, P2P, IRC, RAT, Tool, Spy)
- Proteção contra arquivos com senha
- Quarentena de Anti-Malware
- Relatório de arquivos escaneados
- Identifica, classifica e bloqueia malware tais como, trojan, spyware, adware, keyloggers, highjackers, worms, vírus, conexões do tipo C&C (Command and Control) e Anti-bot (Botnet)
- Permite o bloqueio por reputação do endereço classificado em 6 categorias: spam, reputation, malware, attacks, anonymous e abuse
- Atualização automática e periódica
- Antibot possui mecanismo de detecção em multicamadas, ex: reputação de endereço IP, URLs e endereços DNS e detecta padrões de comunicação e assinaturas

SD-WAN:

- Suporte a múltiplos perfis de configuração e permite habilitar em qualquer interface WAN (DSL, MPLS, 3G/4G LTE) e Packet Duplication (PD), agregação com recurso de VPN, suporta roteamento estático, dinâmico (OSPF, BGP). IPv4/IPv6, supota NAT dinâmico e de saída
- Definição de envio de tráfego por interface selecionada, suporta Policy Based Routing
- Failover, Load Balance, Spillover e Performance
- Monitoramento da disponibilidade do link e proteção contra degradação dos links de dados
- Suporta balanceamento de link por hash do IP de origem e destino, por peso com configuraçao do percentual e podendo utilizar de 2 a 9 links
- Verificação da falha do link por protocolo TCP/UDP Echo, ICMP (ping) e HTTP
- Medição por consumo de banda, perda de pacotes, jitter, latência (monitoramento de vários destinos e em todas as interfaces) com mais de 3 alvos, podendo ser alterado os valores de medição
- Roteamento baseado em aplicação e política para múltiplos caminhos WAN, com bloqueio de app
- Failback do link personalizavel de 1 a 100 e persistência de Links
- Implementa balanceamento de links sem criar zonas ou uso de instâncias virtuais
- Roteamento por grupo em regras de SD-WAN, balanceamento de tráfego por sessão e pacotes

Zero-touch Provisioning:

- Provisionamento automático associado ao número de série do equipamento
- Configura templates de segurança e politicas IPv4/IPv6

Secure Web Gateway:

- Filtro de Conteúdo (sem NAT)
- 88 categorias (incluindo Governo, Webmail, Instituições de Saúde, Notícias, Pornografia, Restaurante, Redes Sociais, Esporte, Educação, Jogos; Compras), +49 milhões de URLs catalogadas, controle de login por domínio no Google, integração SafeSearch (busca segura), Google, Bing e Yahoo, mensagem de bloqueio para o usuário final
- Inspeção SSL com bloqueio de certificado invalido
- Integração com a inspeção ATP e Windows AD / LDAP para identificação de usuários e grupos
- Bloqueio de Aplicações de Redes Sociais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, Bold Chat, ChatON, China.com,Facebook, Flickr, FC2, Fring, Google Analytics, GoogleApp, Linkedin, Meetup, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e ZohoChat e Aplicações de BatePapo
- Bloqueio de arquivos tipo Office, Java e JavaScript, Cookies, ActiveX, Multimidias, Imagens
- Reconhecimento de Aplicação – DPI (Deep Packet Inspetion)
- Identifica Aplicações através do protocolo SSL, HTTP, HTTPS ou portas de acesso não padrão
- Controle por SNI por categoria
- Filtragem, categorização e reclassificação de sites web por URL
- Autenticação de usuários em diretório LDAP, Radius, TACACs+ e Microsoft Active Directory
- Bloqueio por construção de filtros específicos com mecanismo de busca textual
- Bloqueio de certificados inválidos
- Listas personalizadas (whitelist e blacklist)
- Captive Portal com login social (Facebook, Twitter, Google)
- Cotas de navegação por tempo e/ou volume de tráfego
- Atualização Agendada e Automática transparentes

VPN IPSec e VPN SSL:

- VPN túnel (LAN to LAN) / VPN Site-to-Site e Client-to-Site
- VPN RAS/SSL (remote access permite acesso por cliente de VPN ou suporte direto na estação sem cliente - Interface Web), ou seja, pode utilizar a VPN SSL com ou sem agente
- VPN SSL Portal (via HTTPS) para acessos RDP, VNC, SSH, WEB e SMB
- Cliente VPN compatível com Win7, 8/8.1, 10 e 11 (32 e 64 bits), Linux e MacOS
- Autenticação
- Chave PSK (Pre-Shared Key), X-Auth (AD, LDAP, local, RADIUS), certificado digital IKE PKI, EAP (MSCHAPv2),
- Permite estabelecer o túnel antes ou após o usuário autenticar na estação e sob demanda do usuário
- Alta disponibilidade
- FQDN (Full Quality Domain Name) e Suporte DDNS
- NAT-T (encapsulamento UDP) e DPD (Dead Peer Detection)
- Exchange mode IKEv1: Main mode ou Aggressive mode
- Suporte a dados compactados
- Protocolos
  - IKEv1 e IKEv2 (para fase 1 e fase 2) e ESP
- Criptografia Simétricas:
  - AES(128, 192 e 256), 3DES
- Criptografia Assimétricas:
  - DH (Diffie-Hellman - Grupo1, Grupo2, Grupo5, Grupo14; Grupo15, Grupo16, Grupo17, Grupo18, Grupo19, Grupo20, Grupo21, Grupo22, Grupo23, Grupo24, Grupo25, Grupo26, Grupo27, Grupo28, Grupo29, Grupo30) RSA key generation, DSA parameter
- Suporta Auto-Discovery VPN (AD-VPN), Permite múltiplos dispositivos (Spokes) com gateway centralizador (hub) e Site-to-Site, Suporta túneis do tipo (Site-to-Site, Full Mesh, Star)
- Suporta os algoritmos RSA e Diffie-Hellman
- VPN SSL com suporte a certificado digital X.509 v3
- Suporta a inclusão (enrollment) de autoridades certificadoras mediante SCEP (Simple Certificate Enrollment Protocol)
- Suporte a IP Público Dinâmico, roteamento RIPv2 e OSPFv3
- Suporte a certificados emitidos por autoridade certificadora no padrão ICP-Brasil
- Suporte à verificação de certificate revocation list (CRL)
- VPN SSL e IPSec (client-to-site) com Blockbit Client para Windows
- Permite atribuir DNS nos clientes remotos de VPN
- Clientless VPN (IPSec e SSL) sem restrições de players de mercado
- Gerenciamento de certificados SSL (X.509)

Redes e Interfaces:

- Interfaces
- Ethernet (com suporte a FEC - Forward Error Correction)
- VLAN (IEEE 802.1q) até 4094 por interface
- Suporte WAN: ADSL/DSL, MPLS, LTE (3G/4G/5G)
- Alias (Virtual IP)
- LTE (4G) utilização como link para load balance e failover
- Link aggregation
- Ethernet bonding (802.3ad) LACP
- Roteamento dinâmico: BGP4/BGP4+, OSPFv2/v3, RIPv2 e PIM-SM
- Roteamento estático (IPv4 e IPv6) com suporte a ECMP
- Roteamento Multicast: suporta regras e objetos
- Suporte nativo a IPv4 e IPv6
- DHCP (dynamic host configuration protocol) IPv4 e IPv6
- Relay, Server e Client
- DNS Recursivo
- Roteamento baseado em política (PBR - Policy Based Routing ou PBF – Policy Based Forwarding)
- Suporta sub-interfaces ethernet lógicas

Autenticação:

- Autenticação de Usuários
- Local, Windows AD, LDAP, SSO Windows (single sign on via Kerberos) e WMI – autenticação unificada, X-Auth para serviços de VPN, autenticação em servidores Radius, RSSO (radius single sign on), identificador de complexidade de senha, Token ID, Sessões e Aplicações baseadas em TCP/UDP/ICMP
- Suporte TACACS+ para usuários de administração e usuários de Firewall;
- Integração LDAP para administração da Blockbit Platform;
- Sincronismo de usuários e grupos e hosts com servidores Windows AD e servidores LDAP com replicação de sessões estabelecidas dos usuários
- AAA (Authentication, Authorization e Accounting)
- A identificação pela base do AD permiti o uso de SSO, de forma que os usuários não precise logar novamente na rede para navegar pelo firewall;

Log e Relatórios

- Suporte Netflow / IPFIX
- Relatórios de Log de Sessão, Autenticação e VPN
- Criação de relatório customizável do tipo Analyzer (nativo na ferramenta) dos serviços de Firewall, Web Filter, Application Control, IPS, ATP, VPN e User Behavior (informações de IP, Sistema Operacional do usuário, Hostname e classificação de ameaças em estilo "top 10")
- Syslog Remoto para envio dos logs e exportação de log via SCP, suporta envio do log via protocolo SSL
- Exportação de relatórios em múltiplos formatos (PDF, CSV, HTML)
- Os eventos identificam o país da origem do ataque
- Eventos registram alterações no estado e a saúde dos links do SDWAN

Interface WEB e CLI:

- Granularidade (perfis de leitura e leitura/escrita, aplicação de configurações etc) de acesso administrador na Interface Web com sessões simultâneas
- CLI (interface em linha de comando para gerenciamento e diagnóstico via SSH e serial RS-232/RJ-45
- Interface Web própria disponível em Português, Inglês e Espanhol acessível por qualquer interface física do produto
- Gerenciamento (LAN ou WAN) via WEB (HTTPS por browser) e SSH

Monitoramento:

- Suporte ao protocolo SNMP v1, v2 e v3, monitora o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança
- Desempenho, conexões simultâneas, lease do DHCP, usuários autenticados e serviços habilitados ou desabilitados
- Notificações de Sistema e de Segurança
- Janela de visualização de eventos detalhados
- Ferramenta para manutenção do disco e monitoramento de tráfego de rede em tempo real (Live Sessions eTrafic Monitor) com informações de throughput e conexões simultâneas
- Logs de Eventos de segurança e Ameaças
- TCPDUMP por Feature e proteções específicas (permite captura e download em formato PCAP)
- Registro de usuários nos eventos de autenticação, acesso, bloqueio e ameaças
- Contadores RX/TX, entrada e saída de pacotes, descartes de pacotes e erros (Comando CLI)

Backup e Restore:

- Snapshot e Backup do Sistema criptografado
- Disaster recovery (backup/restore) pela interface Web
- Armazenamento (para backup e salva de logs)
- NFS / DISK(HDD) / SSH / Flash (via USB)
- Backup Rotation nos armazenamentos
- Agendamento de Backup do tipo Snapshot ou de Sistema

Outros Recursos:

- Proxy Services (SSH, SMB/CIFS, HTTP, FTP, SMTP, POP3)
- Suporta Voip (SIP/H323) e RTP sobre IPv4/IPv6
- Suporte a múltiplos domínios de Autenticação
- Suporta fail-closed e opcional de interface fail-open (by-pass)
- Atualização automática, periódica e offline
- Suporta autenticação das sessões para todos os protocolos e quaisquer aplicações
- Objetos de recursos
- Endereços IP, Endereços MAC, Serviços de portas e protocolos, Tabela de horários, Tabela de períodos e datas, Dicionários (conjunto de palavras e/ou expressões regulares), Tipos de conteúdo
- Suporte a servidores NTP (Network Time Protocol) para atualização de data e hora
- Opção de atualizações automáticas e periódicas do sistema para correções e releases web HTTPS ou via GSM
- Otimização de Fluxos TCP
- Suporta acesso via SSH, CLI, cliente ou WEB (HTTPS)
- Virtualização do equipamento em Cloud Pública (Google Cloud®, Azure®, Oracle Cloud® e AWS®) ou Cloud Privada (Vmware®, Citrix XenCenter® e ProxMox®)
- Suporte a Contexto (Virtual Domain)
- Sistema de Cluster High Availability (Ativo-Passivo e Ativo/Ativo e somente com equipamentos iguais) com manutenção da sessões estabelecidas, distribuição de tráfego, manutenção da tabela de estado e balanceamento de sessão
- Suporte a dois ou mais membros no cluster
- Suporta duas interfaces de rede para sistema de cluster H.A.

Outros Recursos

- Capaz de identificar o usuário da rede, suporta AD, LDAP, RADIUS e TACACs
- Sem instalação de agentes no AD, nem nas estações dos usuários
- Todas as políticas suportam o controle de aplicações
- Suporta diversos métodos de identificação e classificação das aplicações, por exemplo, checagem de assinaturas e decodificação de protocolos
- Permite a criação de assinaturas personalizadas na interface WEB para reconhecimento de aplicações e de IPS/IPS
- Suporta cadastrar exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação
- A Blockbit permite solicitações de inclusão de aplicações na base padrão
- É possível diferenciar diferentes tráfegos P2P para diversos software (Bittorrent, emule e outros) com granularidade no controle dos aplicativos
- Possibilita a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc.), aplicações Proxies (psiphon, freegate, etc) e possui granularidade de controle e ou políticas
- Suporta granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilita a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens
- Permiti usar operadores de negação na criação de assinaturas customizadas de IPS, permitindo a criação de exceções com granularidade nas configurações
- Registra na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além
da ação tomada pelo dispositivo
- Possui proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e Worms
- Proteção contra downloads involuntários usando HTTP de arquivos executáveis e/ou maliciosos
- Permite a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, MAC Address, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança
- Suporta Sistema Virtuais (VDOM) em todos os modelos
- VDOM permite acriar contextos virtuais com suporte a criação de diversos administradores

SandBoxing - APT

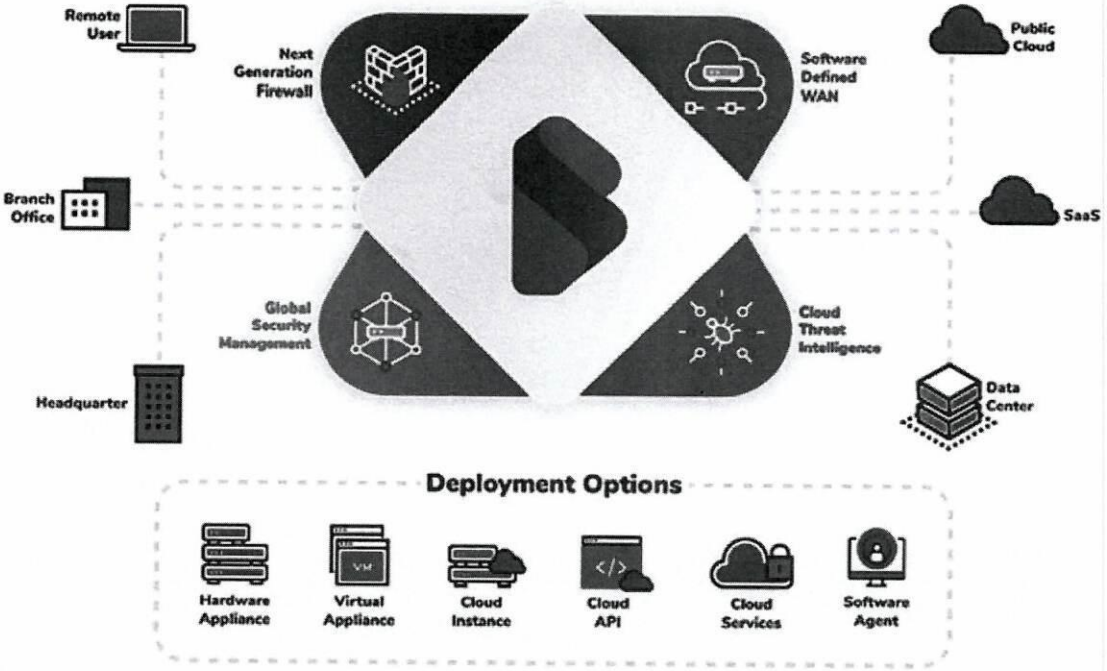
- Permite mitigar ameaças avançadas persistentes (APT e Zero-Day), através de análises dinâmicas para identificação de malwares desconhecidos com atualização automática em base de dados em rede de inteligência. Analisa arquivos do tipo PDF, Microsoft Office, executáveis e compactados;
- O SandBox Blockbit é capaz de criar assinaturas e ainda incluí-las na base de antivírus do firewall, prevenindo a reincidência do ataque
- Suporta incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Blocklist), impedindo que esses endereços sejam acessados pelos usuários de rede novamente
- O módulo de ATP suporta analisar o arquivo pelo antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back e também análisa o comportamento de arquivos suspeitos em um ambiente controlado, em tempo real
- Capaz de emular, detectar e bloquear qualquer malware e/ou código malicioso. Emula SandBox de ambientes Microsoft em versões variadas e Office

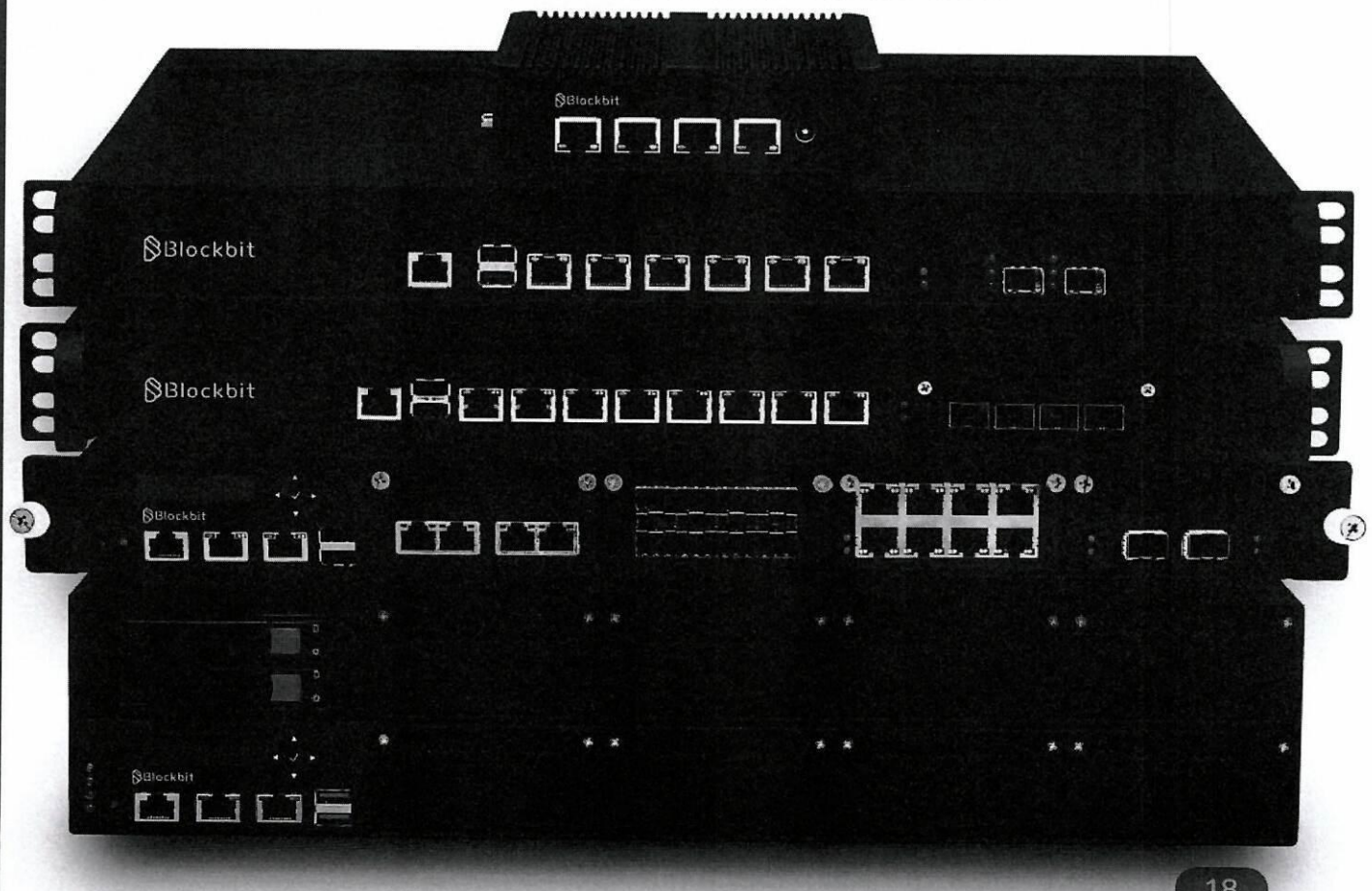
Identificação do Usuário

- Permite a criação de políticas baseadas no controle por URL e categorias de URL
- Permite criar políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local
- Possui compatibilidade com Microsoft Active Directory(Windows 2003, 2012 e 2019) para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários
- Possui integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Suporta usuários ilimitados.
- Suporta autenticação para Firewall e VPN: Tokens, TACACS, RADIUS e certificados digitais;
- Permite o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal)
- Suporta a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços
- Permite a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD

Filtro de Dados

- Possui recurso capaz de identificar e prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, HTTPS, FTP, SMTP)
- É capaz identificar na rede de dados arquivos compactados e aplicar políticas de uso sobre o conteúdo desses tipos de arquivos





Algumas RFC's suportadas pelo Blockbit Platform:

BGP:

- RFC 7911: Advertisement of Multiple Paths in BGP
- RFC 7606: Revised Error Handling for BGP UPDATE Messages
- RFC 4724: Graceful Restart Mechanism for BGP
- RFC 4456: BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 4360: BGP Extended Communities Attribute
- RFC 4271: A Border Gateway Protocol 4 (BGP-4)
- RFC 2918: Route Refresh Capability for BGP-4
- RFC 2545: Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2439: BGP Route Flap Damping
- RFC 1997: BGP Communities Attribute
- RFC 1930: Guidelines for creation, selection, and registration of an Autonomous System (AS)
- RFC 1772: Application of the Border Gateway Protocol in the Internet

OSPF:

- RFC 6860: Hiding Transit-Only Networks in OSPF
- RFC 6845: OSPF Hybrid Broadcast and Point-to-Multipoint Interface Type
- RFC 5709: OSPFv2 HMAC-SHA Cryptographic Authentication
- RFC 5340: OSPF for IPv6
- RFC 4812: OSPF Restart Signaling
- RFC 4811: OSPF Out-of-Band Link State Database (LSDB) Resynchronization
- RFC 4203: OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
- RFC 3630: Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 3623: Graceful OSPF Restart
- RFC 3509: Alternative Implementations of OSPF Area Border Routers
- RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option
- RFC 2328: OSPF Version 2
- RFC 1765: OSPF Database Overflow
- RFC 1370: Applicability Statement for OSPF

RIP:

- RFC 4822: RIPv2 Cryptographic Authentication
- RFC 2453: RIP Version 2
- RFC 2080: RIPng for IPv6
- RFC 1724: RIP Version 2 MIB Extension
- RFC 1058: Routing Information Protocol

DHCP:

- RFC 4361: Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
- RFC 3736: Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
- RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
- RFC 3456: Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 2131: Dynamic Host Configuration Protocol

Diffserv:

- RFC 3260: New Terminology and Clarifications for Diffserv
- RFC 2597: Assured Forwarding PHB Group
- RFC 2475: An Architecture for Differentiated Services
- RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

IPv4 e IPv6:

- RFC 6864: Updated Specification of the IPv4 ID Field
- RFC 5177: Network Mobility (NEMO) Extensions for Mobile IPv4
- RFC 4632: Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses
- RFC 3021: Using 31-Bit Prefixes on IPv4 Point-to-Point Links
- RFC 1812: Requirements for IP Version 4 Routers
- RFC 7761: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
- RFC 6343: Advisory Guidelines for 6to4 Deployment
- RFC 5175: IPv6 Router Advertisement Flags Option
- RFC 5095: Deprecation of Type 0 Routing Headers in IPv6
- RFC 4941: Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC 4389: Neighbor Discovery Proxies (ND Proxy)
- RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 4193: Unique Local IPv6 Unicast Addresses
- RFC 4007: IPv6 Scoped Address Architecture
- RFC 3971: Secure Neighbor Discovery (SEND)
- RFC 3596: DNS Extensions to Support IP Version 6
- RFC 3587: IPv6 Global Unicast Address Format
- RFC 3493: Basic Socket Interface Extensions for IPv6
- RFC 3056: Connection of IPv6 Domains via IPv4 Clouds
- RFC 3053: IPv6 Tunnel Broker
- RFC 2894: Router Renumbering for IPv6
- RFC 2675: IPv6 Jumbograms
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 2185: Routing Aspects Of IPv6 Transition
- RFC 1752: The Recommendation for the IP Next Generation Protocol
- RFC 8200: Internet Protocol, Version 6 (IPv6) Specification
- RFC 8201: Path MTU Discovery for IP version 6

NAT:

- RFC 7857: Updates to Network Address Translation (NAT) Behavioral Requirements
- RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC 5508: NAT Behavioral Requirements for ICMP
- RFC 5382: NAT Behavioral Requirements for TCP
- RFC 4787: NAT Behavioral Requirements for Unicast UDP
- RFC 4380: Teredo: Tunneling IPv6 over UDP through NAT
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3022: Traditional IP Network Address Translator (Traditional NAT)

SIP:

- RFC 3960: Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
- RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC 3262: Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3261: SIP: Session Initiation Protocol

LDAP:

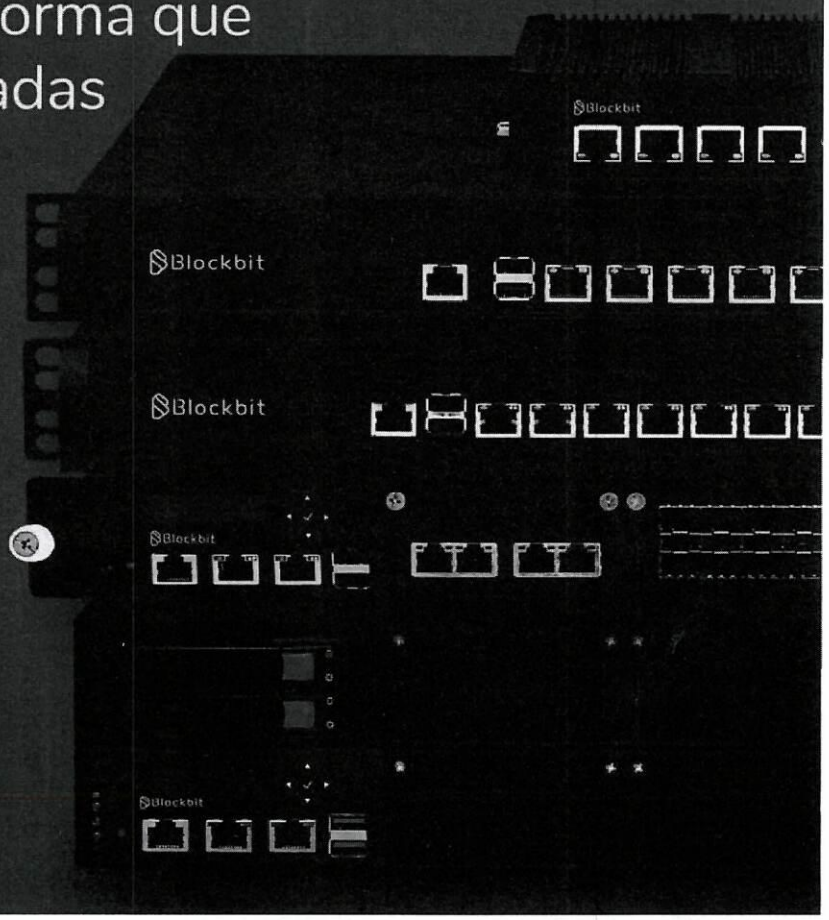
- RFC 4513: Authentication Methods and Security Mechanisms
- RFC 4512: Directory Information Models
- RFC 4511: The Protocol
- RFC 3494: Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status

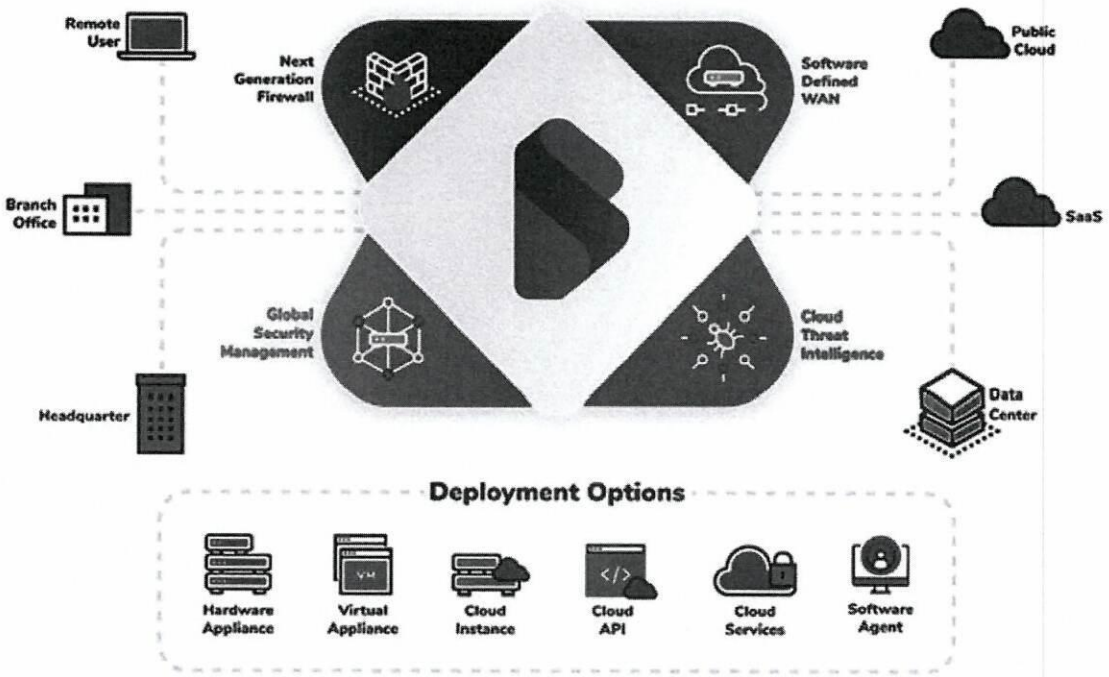
Blockbit

Blockbit Platform 2.4.0

É fácil estar seguro!

Proteja a arquitetura da sua rede com uma única plataforma que integra diversas camadas de segurança digital, sem custo de módulos adicionais.





É fácil estar seguro!

Proteja a arquitetura da sua rede com uma única plataforma que integra diversas camadas de segurança digital, sem custo de módulos adicionais.

Como fabricante global de cibersegurança, a **Blockbit oferece** uma plataforma de gestão unificada e abrangente à todas as empresas. **A Blockbit Platform** foi desenvolvida especificamente para ser um Firewall com total integração para facilitar o gerenciamento e a usabilidade do usuário final. O sistema operacional é desenvolvido pela Blockbit para garantir estabilidade e o melhor desempenho, com o que há de mais novo no mercado, nossas soluções integradas protegem todo o perímetro de rede e suas redes distribuídas.

Alterações na solução de ATP ou quaisquer outras apenas impactam no recurso alterado sem interferir nas demais regras de segurança.

Permite configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

Plataforma integrada da cibersegurança: dinâmica, moderna e funcional;

- Configure políticas de segurança, implemente recursos e ative múltiplos dispositivos automaticamente com o Zero-touch;
- Identifique e bloqueie intrusos e aplicações suspeitas antes mesmo que entrem em sua rede;
- Simplifique a gestão e a proteção de redes, usuários, conexões e múltiplos ativos;
- Bloqueie ataques sofisticados e ameaças avançadas a partir de uma única plataforma;
- Controle navegação web e promova mais produtividade para sua equipe;
- Defina políticas de segurança, conformidade e níveis de acesso;
- Habilite comunicação entre dispositivos remotos com sua rede de forma segura e criptografada.

DESTAQUES

Controle e Roteamento Avançado de Aplicações:
Gerencie facilmente o acesso à Aplicações Web como Facebook, LinkedIn, Google, Twitter, Dropbox, entre outros.

Proteção Avançada Contra Ameaças:
Segurança inovadora contra malware avançado e call-back.

Gerenciamento Centralizado:
Gerencie facilmente múltiplos dispositivos com o Blockbit GSM (Global Security Management), que tem integração nativa com o Blockbit Next-Generation Firewall.

Decodificação de Protocolo
Capaz de detectar aplicações encapsuladas e validar se o tráfego corresponde com a especificação do protocolo. O recurso também identifica funcionalidades específicas dentro de uma aplicação.

Atualizações Transparente:
As atualizações automáticas de patches de correções e subscriptions são transparentes para o cliente sem causar interrupção na rede. Possui ferramenta com os hotfixes de segurança e upgrade simplificado e sem interrupção do ambiente.

Reduza o custo e o tempo na implementação:
Centralize configurações e as distribua automaticamente para os ativos remotos. Com o recurso ZTP (Zero-Touch Provisioning) é possível reduzir tempo e custo com a implementação.

Principais Recursos

Next-Generation Firewall
A Blockbit Platform é muito mais que um firewall. Unindo a mais avançada tecnologia de gestão de redes à capacidade avançada de detecção e proteção contra ataques e ameaças digitais. O Blockbit NGFW (Next-Generation Firewall) simplifica a criação de políticas e regras de segurança complexas, podendo ser implementado como gateway ou inline, otimizada para análise de conteúdo de aplicação na camada 7, utilizando endereços, usuários, grupos de usuários, aplicações, ameaças e serviços em suas configurações, que podem ser nomeados para facilitar a compreensão das políticas e garantir controle total do seu ambiente. Possibilita a criação de regras de saída de rede baseado em endereço IP e faixa de rede de origem, endereço IP e faixa de rede de destino e porta de destino. O licenciamento é de uso perpétuo para todos os recursos NGFW, SD-WAN, App control e stateful firewall. Suporta VDOM (Virtual Domain) em todos os modelos de hardware. Suporta criar políticas de bloqueio ou liberação por geolocalização e informam nos logs o país de origem e/ou destino com a bandeira para facilitar a identificação do tráfego.

Zero-Touch Provisioning
Com o recurso ZTP (Zero-Touch Provising) é possível pré-configurar as políticas de segurança e implementá-las automaticamente no dispositivo remoto vinculado, assim que receber uma conexão de rede. Isso reduz a complexidade da instalação e, consequentemente, a economia de recursos financeiros e técnicos.

Inspeção SSL
A maioria das informações que trafegam na web usam conexões criptografadas. A Blockbit Platform conta com descriptografia de SSL para inspeção de tráfego de saída (Outbound), garantindo o controle total de acesso e aplicando recursos avançados, como ATP, Filtro de Conteúdo, Controle de Aplicação e Antimalware. Suporta TLS 1.2 e TLS 1.3. Suporta aplicação de políticas de segurança e visibilidade para as aplicações que circulam

Filtragem de Conteúdo

A Blockbit Platform possui milhões de endereços classificados em categorias específicas. Estas informações, em conjunto com a inspeção SSL, permitem controlar totalmente o acesso ao conteúdo online e na visibilidade, o que pode ser configurado por usuário, grupos de usuários, (AD ou base local) IPs, largura de banda, prioridade de conexão, links, diferentes navegadores e suas versões. Você também pode determinar limites para tamanho de arquivos para download e upload, execução de aplicações web, tempo permitido de navegação e muito mais. Permite a filtragem de arquivos e dados pré-definidos, controle de arquivos compactados e aplicar politicas no conteúdo destes.

Controle de Aplicações

O avanço da Internet permitiu a criação de aplicações como Facebook, Youtube, Google Apps, Twitter, LinkedIn e Dropbox, que se tornaram muito populares e podem impactar a produtividade de suas equipes se não utilizadas corretamente. A Blockbit Platform permite que você controle totalmente as Aplicações Web (podendo bloquear, limitar e aplicar controle de QoS) executadas com integração a diversos métodos de autenticação, restringindo ou permitindo acesso de acordo com as regras do seu negócio. Suporta controlar o uso de aplicativos por políticas e grupos estáticos de aplicações. A Blockbit é capaz de reconhecer aplicações independemente de porta e protocolo, portanto é possível [illegible]rar a aplicação sem precisar liberar porta e/ou protocolos. Identifica o uso de táticas evasivas para controlar aplicações que tentam usar conexão criptografadas (por exemplo Skype ou rede TOR).

IPS - Sistema de Prevenção de Intrusos

A Blockbit Platform protege continuamente sua rede contra o número crescente de ameaças digitais. O IPS conta com milhares de assinaturas para identificação de ameaças em um banco de dados atualizado diariamente. É possível criar múltiplos perfis de proteção para aplicá-los em diferentes tipos de tráfego de rede. Além disto, o dashboard exibe informações sobre as ameaças detectadas de maneira detalhada, permitindo uma rápida e eficiente análise de risco. São suportados as seguintes proteções: Permite analisar e gerar logs, bloqueia e envia para quarentena o IP do atacante por um período de tempo.

ATP - Proteção Avançada Contra Ameaças (Antívirus e Anti-Spyware)

A Blockbit Platform conta com tecnologias sofisticadas de segurança e inteligência que detectam e protegem sua empresa contra ameaças conhecidas e desconhecidas, inclusive em tráfego SSL. A Blockbit Platform pode detectar malware avançados como trojans e vírus, ameaças persistentes avançadas e ataques de callbacks maliciosos. O ATP também pode bloquear IPs com má reputação em diferentes categorias (abusers, anonymizers, attackers, malware, spam) além de ataques por geolocalização. Bloqueia arquivos pela extensão e também indentifica pelo tipo MIME (mesmo mudando a extensão).

VPN SSL e IPSec

A Blockbit Platform permite criar acesso seguro às aplicações de sua rede através de um portal web que pode ser configurado rapidamente e executado em qualquer navegador. A plataforma também suporta conexão do tipo client-to-site. A Blockbit Platform permite criar redes privadas virtuais com criptografia de tunelamento nativa, que garante a interoperabilidade com outros produtos e aumenta a segurança. Suporta arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site como para client-to-site (remote access). Permite que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies. Crie políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL/IPSEC

QoS & Traffic Shapping

A Blockbit Platform conta com recurso de QoS exclusivo que permite, via interface gráfica centralizada e local, priorizar tráfego e controlar a largura de banda de acordo com as políticas de segurança e conformidades configuradas, além da classificação de pacotes (Shaping). O recurso de QoS avançado categoriza conexões de acordo com sua importância e possibilita priorizar pacotes através da marcação de DSCP e TOS. Defina banda máxima e garantida por aplicação, suporta o match em categorias de URL, IPs de origem e destino, logins e portas. Regas de QoS podem ser habilitadas por horários ou intervalo de tempo.

SD-WAN

A Blockbit Platform oferece um serviço de balanceamento dinâmico de 2 até 9 links para conexão de longa distância, que permite conectar a sua empresa a qualquer local – filiais, datacenters, nuvem etc. Suporta interface física, sub-interfaces VLAN e IPSec. Suporta conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link satélite (a terminação da conectividade deve permitir conectividade com interfaces ethernet).

Você tem mais visibilidade sobre todas as atividades em qualquer local e ainda integra o SD-WAN com todos os recursos de segurança da Blockbit, podendo gerenciar todo o ambiente a partir de uma única interface, facilitando a análise de resultados e a tomada de decisões sobre otimizações na rede, em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remoto. Os appliances Blockbit possuem entrada USB compatível com modem 3G/4G permitindo que o link WAN seja utilizado nas regras de SD-WAN. Suporta o roteamento por aplicação. Permite escolher o melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação. Utilize VPN IPSec para balancear o tráfego por round robin na agregação de tráfego e definição de peso de cada túnel.

Alta Disponibilidade

A Blockbit Platform tem suporte nativo a implementações H.A. (high availability). O recurso mantém um appliance em modo backup, que entra em operação imediatamente caso o appliance primário sofra uma falha. Tamém suporta monitorar se ocorre falha no link. O suporte H.A. espelha sessões de firewall, autenticação de usuário e sincroniza todas configurações, seções, certificados para Inspenção SSL, SA (Associações de Segurança) de VPN IPSsec e todas as assinaturas de ATP, Application Control, IPS e WEB Filter, entre os dispositivos primário e secundário para que o switch over seja transparente e rápido.

Captive Portal

A Blockbit Platform facilita o gerenciamento do acesso de visitantes por meio da autenticação que o navegador web utiliza. O Captive Portal permite auto registro, personalização de políticas de acesso, controle de conteúdo, gestão de usuários, troca de senhas de acesso e relatórios personalizados. Além disso, é possível autenticar via contas de mídias sociais (Facebook, Google e Twitter), Windows AD, LDAP e RADIUS.

Gerenciamento Centralizado

O Blockbit NGFW tem integração nativa com o GSM (Global Security Management), que possibilita gerenciar múltiplos dispositivos, com conexão criptografada e autenticada por meio de um ponto central. Permite o gerenciamento centralizado e local das funcionalidades de Políticas de encaminhamento, Proxy WEB, IPS/IDS e Antimalware, monitorando seus eventos de forma integrada. Suporta envio automático dos logs para servidor externo por NFS. Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, origem e destino. Página com Indicador de Comprometimento. Usuários com utilização web suspeita: endereço IP do terminal do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça) e número de ameaças detectadas.

Recursos Habilitados*

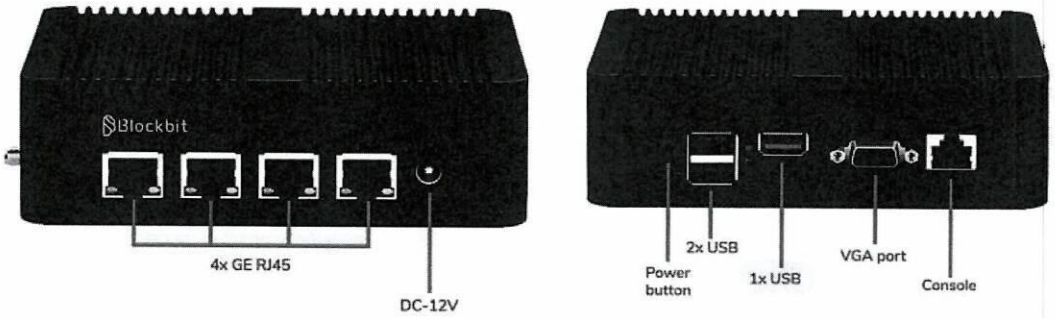
Features	Basic	Standard	Advanced
Next-Generation Firewall (NGFW)	✓	✓	✓
Secure SD-WAN	✓	✓	✓
Proxy WEB	✓	✓	✓
VPN IPSEC	✓	✓	✓
VPN SSL	✓	✓	✓
QoS	✓	✓	✓
Cluster	✓	✓	✓
Captive Portal	✓	✓	✓
DHCP SERVER/RELAY	✓	✓	✓
Garantia de Hardware	✓	✓	✓
Base de Categoria de URL		✓	✓
Intrusion Prevention System (IPS)		✓	✓
Antivírus de Gateway		✓	✓
Threat Protection		✓	✓
Suporte Remoto - 04 horas mês			✓

*LICENCIAMENTO DOS EQUIPAMENTOS DA BLOCKBIT NÃO LIMITA A QUANTIDADE DE USUÁRIOS, EQUIPAMENTO E/OU FUNCIONALIDADE.

MODELOS EQUIPAMENTOS

Pequenas Empresas

MODELO: BB2 | BB5 | BB10



Especificações de Desempenho e Opcionais

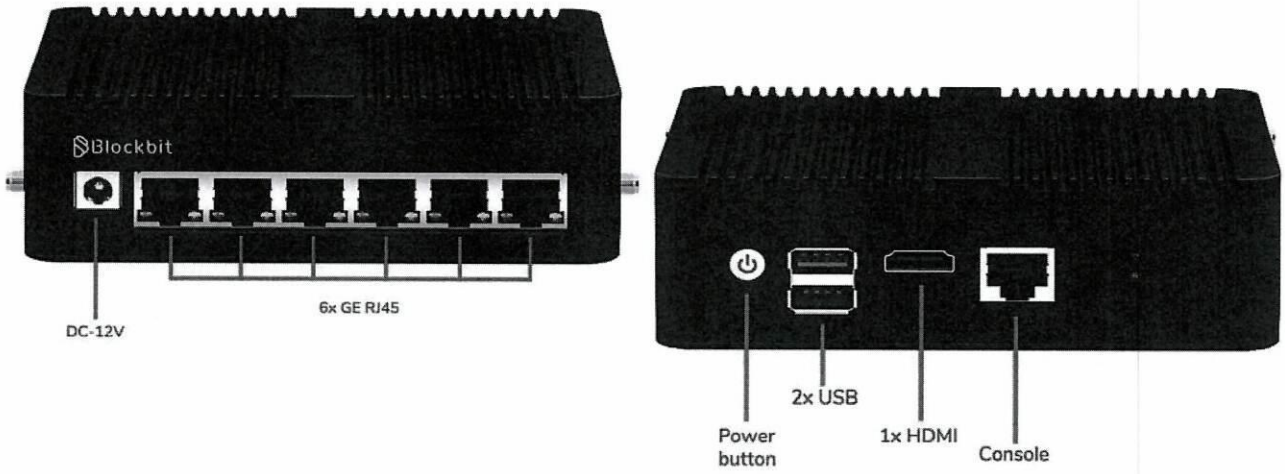
	BB2	BB5	BB10
Firewall Throughput (UDP)	3.7Gbps	4 Gbps	6 Gbps
Conexões Simultâneas	3.500.000	4.000.000	6.000.000
Conexões Novas Por Segundo	35.000	37.000	38.000
NGFW Throughput (IMIX)[1]	150 Mbps	200 Mbps	350Mbps
Web Filter Throughput	300 Mbps	400 Mbps	600 Mbps
SSL Inspection Throughput	100 Mbps	150 Mbps	200 Mbps
IPS Throughput	500 Mbps	700 Mbps	1 Gbps
Application Control Throughput	70 Mbps	100 Mbps	200 Mbps
Threat Protection Throughput	100 Mbps	150 Mbps	200 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	250 Mbps	280 Mbps	500 Mbps
SSL VPN Throughput (AES-256)	100 Mbps	140 Mbps	250 Mbps
Interfaces de Rede	4 X GE RJ45	4 X GE RJ45	4 X GE RJ45
Armazenamento	32 GB	32 GB	32 GB
Característica Física / Alimentação	1U p/ Desktop / DC 100-220V AC, 50-60hz		
Dimensões (Largura x Profundidade x Altura)	230mm x 300mm x 46mm		
Temperatura Ideal de Operação	-10°C (14 °F) ~ 60°C (140 °F)		

Opcionais

Unidade de Estado Sólido (SSD)	64/120 GB	64/120 GB	120/240 GB
LTE 3G/4G	Sim	Sim	Sim

Médias Empresas

MODELO: BB30



Especificações de Desempenho e Opcionais

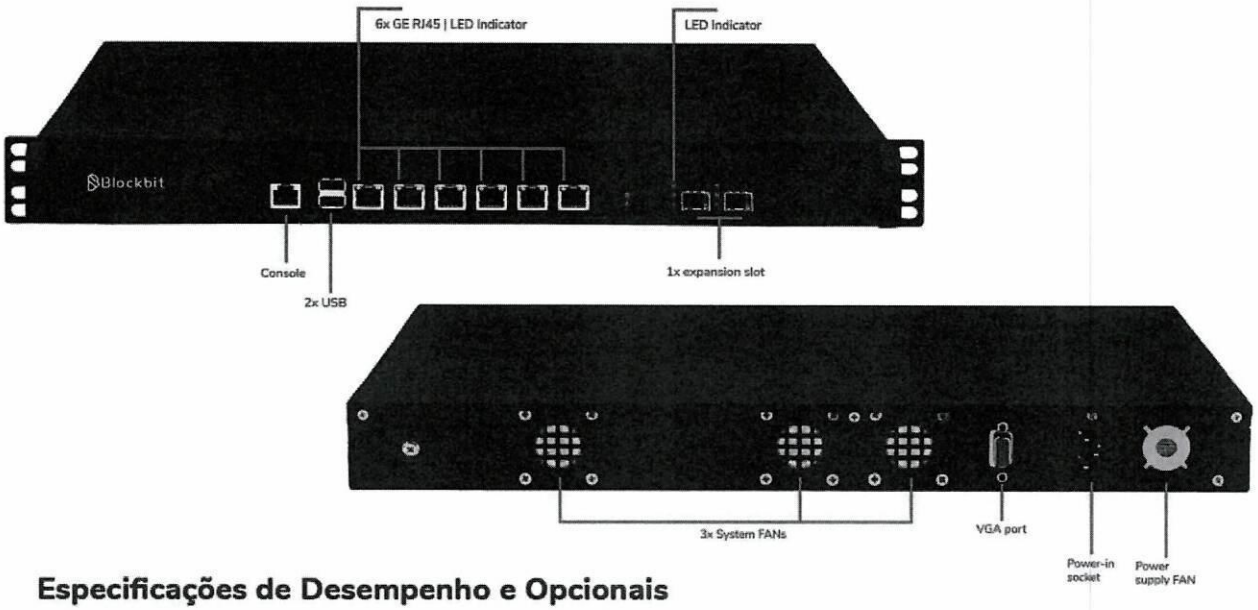
	BB30
Firewall Throughput (UDP)	6 Gbps
Conexões Simultâneas	6.000.000
Conexões Novas por Segundo	38.000
NGFW Throughput (IMIX)[1]	350 Mbps
Web Filter Throughput	600 Mbps
SSL Inspection Throughput	200 Mbps
IPS Throughput	1 Gbps
Application Control Throughput	200 Mbps
Threat Protection Throughput	200 Mbps
IPSEC VPN Throughput (AES-128 + SHA256)	500 Mbps
SSL VPN Throughput (AES-128)	250 Mbps
Interfaces de Rede	6X GE RJ45
Armazenamento	32 GB
Característica Física	1U para Desktop
Dimensões (Largura x Profundidade x Altura)	230mm x 300mm x 46mm
Temperatura Ideal de Operação	-10°C (14 °F) ~ 60°C (140 °F)

Opcionais

Unidade de Estado Sólido (SSD)	120/240 GB
LTE 3G/4G	Sim

Grandes Empresas

MODELO: BB50 | BB100



Especificações de Desempenho e Opcionais

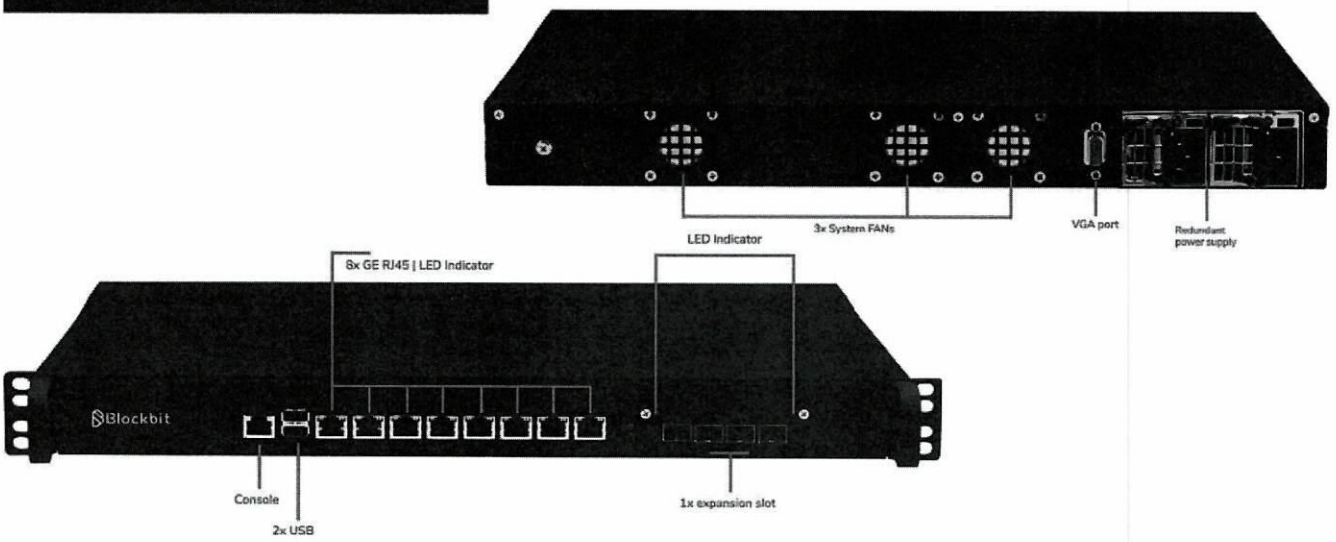
	BB50	BB100
Firewall Throughput (UDP)	8 Gbps	10 Gbps
Conexões Simultâneas	7.000.000	8.200.000
Conexões Novas Por Segundo	42.000	55.000
NGFW Throughput (IMIX)[1]	1 Gbps	1.6 Gbps
Web Filter Throughput	1.5 Gbps	2 Gbps
SSL Inspection Throughput	750 Mbps	1 Gbps
IPS Throughput	1.5 Gbps	2 Gbps
Application Control Throughput	700 Mbps	1 Gbps
Threat Protection Throughput	500 Mbps	700 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	1.5 Gbps	2 Gbps
SSL VPN Throughput (AES-256)	1 Gbps	1.5 Gbps
Interfaces de Rede	6 X GE RJ45	6X GE RJ45
Armazenamento	120 GB	120 GB
Característica Física	1U para Rack 19''	1U para Rack 19''
Alimentação	100-240V AC	
Dimensões (Largura x Profundidade x Altura)	380mm x 430mm x 46mm	
Temperatura Ideal de Operação	-20 °C (-4 °F) ~ 70 °C (158 °F)	

Opcionais

Unidade de Estado Sólido (SSD)	240 GB	240 GB
LTE 3G/4G	Sim	Sim
Módulo Rede 10GbE - 2 portas SFP+	Sim	Sim
Módulo Rede 1GbE - 2 portas SFP	Sim	Sim
Slots disponíveis	1x	1x

Grandes Empresas

MODELO: BB200



Especificações de Desempenho e Opcionais

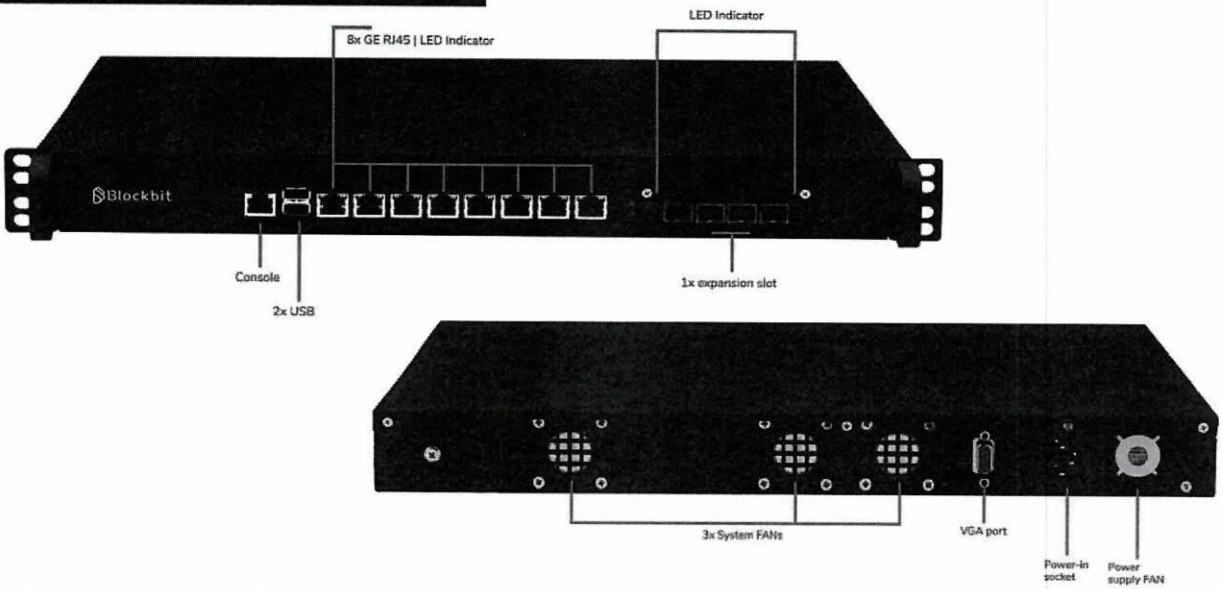
	BB200
Firewall Throughput (UDP)	15 Gbps
Conexões Simultâneas	10.200.000
Conexões Novas Por Segundo	75.000
NGFW Throughput (IMIX)[1]	1.8 Gbps
Web Filter Throughput	3 Gbps
SSL Inspection Throughput	1.2 Gbps
IPS Throughput	3 Gbps
Application Control Throughput	1.4 Gbps
Threat Protection Throughput	950 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	3 Gbps
SSL VPN Throughput (AES-256)	1.5 Gbps
Interfaces de Rede	8X GE RJ45
Armazenamento	120 GB
Característica Física	1U para Rack 19''
Alimentação	100-240 AC
Dimensões (Largura x Profundidade x Altura)	380mm x 430mm x 46mm
Temperatura Ideal de Operação	-20 °C (-4 °F) ~ 70 °C (158 °F)

Opcionais

Unidade de Estado Sólido (SSD)	240 GB
LTE 3G/4G	Sim
Módulo Rede 10GbE - 2 portas SFP+	Sim
Módulo Rede 1GbE - 2 portas SFP	Sim
Fonte Redundante - Hot Swappable 110~240VAC, 60 Hz	Sim
Slots disponíveis	1x

Grandes Empresas

MODELO: BB500 | BB1000



Especificações de Desempenho e Opcionais

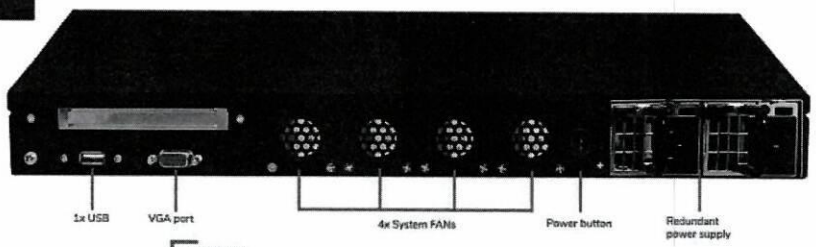
	BB500	BB1000
Firewall Throughput (UDP)	20 Gbps	35 Gbps
Conexões Simultâneas	12.000.000	18.000.000
Conexões Novas Por Segundo	80.000	120.000
NGFW Throughput (IMIX)[1]	2 Gbps	2.8 Gbps
Web Filter Throughput	4 Gbps	6 Gbps
SSL Inspection Throughput	1.4 Gbps	2.2 Gbps
IPS Throughput	4 Gbps	6 Gbps
Application Control Throughput	1.6 Gbps	2 Gbps
Threat Protection Throughput	1 Gbps	1.5 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	4 Gbps	5 Gbps
SSL VPN Throughput (AES-256)	1.6 Gbps	2 Gbps
Interfaces de Rede	8X GE RJ45	8X GE RJ45
Armazenamento	240 GB	240 GB
Característica Física	1U para Rack 19''	1U para Rack 19''
Alimentação	100/240V AC	100/240V AC
Dimensões (Largura x Profundidade x Altura)	360mm x 430mm x 46mm	
Temperatura Ideal de Operação	-20°C (-4°F) ~ 70°C (158°F)	

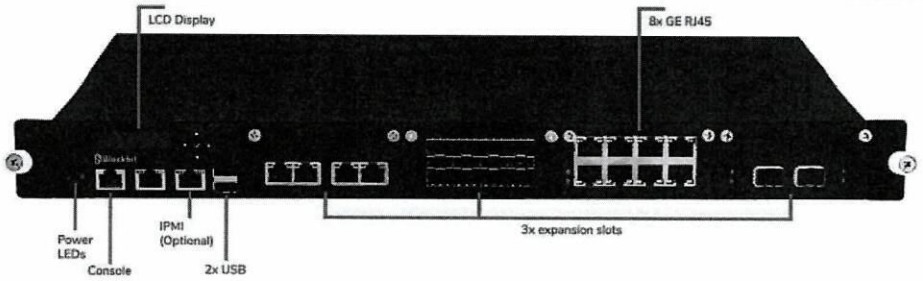
Opcionais

Unidade de Estado Sólido (SSD)	480 GB	480 GB
LTE 3G/4G	Sim	Sim
Módulo Rede 10GbE - 2 portas SFP+	Sim	Sim
Módulo Rede 1GbE - 4 portas SFP	Sim	Sim
Fonte Redundante 100-220V AC	Sim	Sim

Grandes Empresas

MODELO: BB2000





Especificações de Desempenho e Opcionais

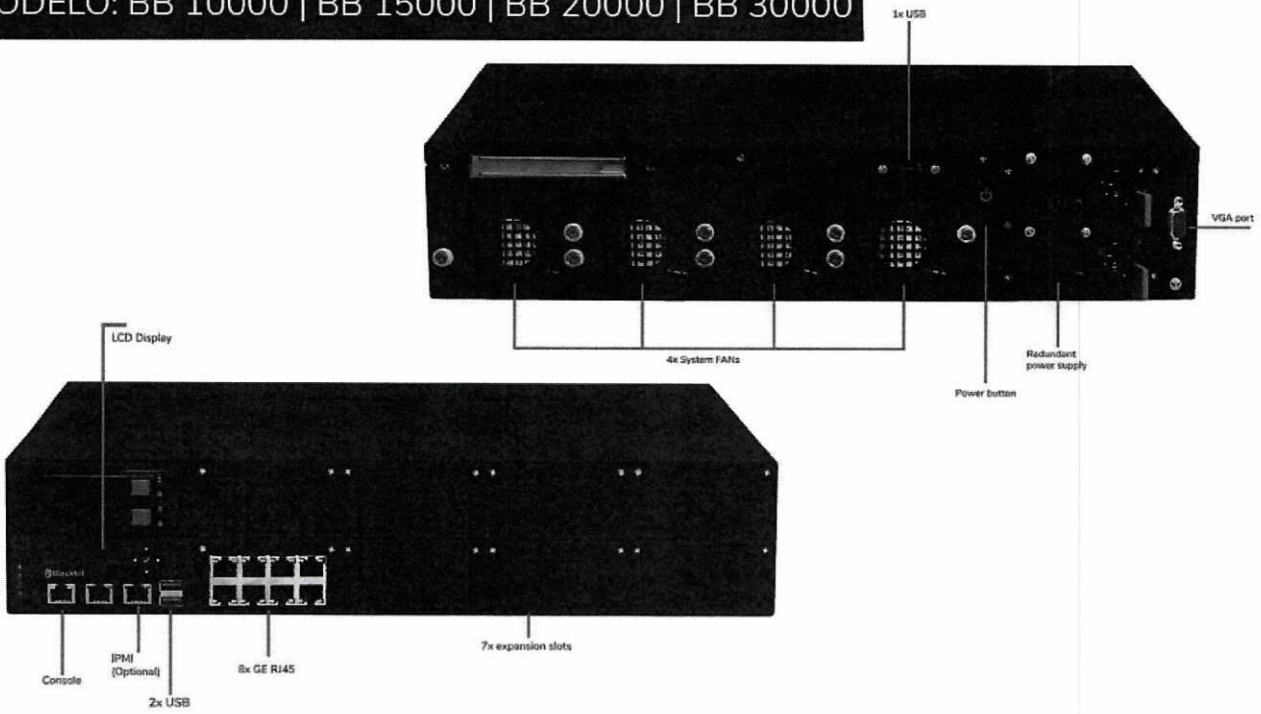
	BB2000
Firewall Throughput (UDP)	55 Gbps
Conexões Simultâneas	22.000.000
Conexões Novas Por Segundo	200.000
NGFW Throughput (IMIX)[1]	5 Gbps
Web Filter Throughput	10 Gbps
SSL Inspection Throughput	4.5 Gbps
IPS Throughput	9.0 Gbps
Application Control Throughput	5 Gbps
Threat Protection Throughput	4.5 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	10 Gbps
SSL VPN Throughput (AES-256)	6.5 Gbps
Interfaces de Rede	8X GE RJ45
Armazenamento	240 GB
Característica Física	1U para Rack 19´´
Dimensões (Largura x Profundidade x Altura)	438mm x 415mm x 44mm
Temperatura Ideal de Operação	-20°C (-4°F) ~ 70°C (158°F)
Fonte Redundante	Sim - 100/240V AC

Opcionais

Unidade de Estado Sólido (SSD)	480 GB
Módulo de Rede 10GbE - 4 portas SFP+	Sim
Módulo Rede 1GbE - 8 portas SFP	Sim
Módulo Rede 1GbE - 4 portas SFP c/ bypass	Sim
Módulo Rede 1GbE - 8 portas RJ45	Sim
Módulo Rede 1GbE - 8 portas RJ45 c/ bypass	Sim
Slots disponíveis	3x

Grandes Empresas

MODELO: BB 10000 | BB 15000 | BB 20000 | BB 30000



Especificações de Desempenho e Opcionais

	BB10000	BB15000	BB20000	BB30000
Firewall Throughput (UDP)	80 Gbps	100 Gbps	160 Gbps	200 Gbps
Conexões Simultâneas	30.000.000	45.000.000	55.000.000	70.000.000
Conexões Novas Por Segundo	300.000	400.000	520.000	700.000
NGFW Throughput (IMIX)[1]	7 Gbps	12 Gbps	20 Gbps	30 Gbps
Web Filter Throughput	12 Gbps	15 Gbps	25 Gbps	35 Gbps
SSL Inspection Throughput	6 Gbps	8 Gbps	12 Gbps	20 Gbps
IPS Throughput	12 Gbps	15 Gbps	23 Gbps	30 Gbps
Application Control Throughput	7 Gbps	10 Gbps	16 Gbps	24 Gbps
Threat Protection Throughput	6 Gbps	9.6 Gbps	12 Gbps	18 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	15 Gbps	18 Gbps	25.6 Gbps	30 Gbps
SSL VPN Throughput (AES-256)	7 Gbps	8 Gbps	11 Gbps	15 Gbps
Interfaces De Rede	8X GE RJ45	8X GE RJ45	8X GE RJ45	8X GE RJ45
Interfaces De Rede Opicionais	8x SFP / 8x SFP+	8x SFP / 8x SFP+	8x SFP / 8x SFP+	8x SFP / 8x SFP+
Fonte de Energia Redundante 110/220v	Sim	Sim	Sim	Sim
Armazenamento	480 GB	480 GB	1 TB	1 TB
Característica Física	2U para Rack 19''			
Dimensões (Largura x Profundidade x Altura)	440mm x 710mm x 880mm			
Temperatura Ideal de Operação	0°C (32°F) ~ 40°C (104°F)			

Opcionais - BB10000 | BB15000 | BB20000 | BB30000

Unidade de Estado Sólido (SSD)	1 TB	1 TB	1 TB
RAID 0/1	Sim	Sim	Sim
Módulo de Rede 40 GbE - 2 portas QSFP+	Sim	Sim	Sim
Módulo de Rede 10 GbE - 4 portas SFP+	Sim	Sim	Sim
Módulo de Rede 10 GbE - 2 portas SFP+ c/ bypass	Sim	Sim	Sim
Módulo Rede 1GbE - 8 portas SFP	Sim	Sim	Sim
Módulo Rede 1GbE - 4 portas SFP c/ bypass	Sim	Sim	Sim
Módulo Rede 1GbE - 8 portas RJ45	Sim	Sim	Sim
Módulo Rede 1GbE - 8 portas RJ45 c/ bypass	Sim	Sim	Sim
Slots disponíveis	7x	7x	7x

Virtual appliances

	Firewall Throughput (UDP)
BBV 2	3.7 Gbps
BBV 5	4 Gbps
BBV 10	6 Gbps
BBV 50	8 Gbps
BBV 100	10 Gbps
BBV 500	20 Gbps
BBV 1000	35 Gbps
BBV 2000	55 Gbps
BBV 10000	80 Gbps
BBV 15000	100 Gbps
BBV 20000	160 Gbps
BBV 30000	200 Gbps

Acessórios que acompanham os equipamentos:

- Bandejas para rack (equipamentos BB 02, BB 05, BB 10 e BB 30)
- Trilhos para montagem em Rack (BB 50, BB 100, BB 200, BB 500, BB 1000, BB 2000, BB 10000, BB 15000, BB 20000 e BB 30000)
- Cabos de energia padão IEC-320 C14
- Cabo serial RS-232/RJ-45 com adaptador RS-232/USB plug and play (sem necessidade de instalação de driver)

Todos os acessórios (bandejas e trilhos para montagem em Rack 19'' e cabos de energia) são fornecidos pela Blockbit. Os módulos de Fibra e Rede (SFP, SFP+, QSFP+, RJ45) acompanham os transeivers (GBic) para os respectivos módulos e modelos e os cordões opticos multimodo ou monomodo conforme a necessidade do projeto.

Políticas de Segurança:

- Suporta IPv4 e IPv6
- IP de Origem/Destino, Porta e Protocolo
- Subnet de Origem/Destino
- Por usuários, grupos, IPs, redes e Zona (LAN, WAN, DMZ) e código de país (BR, EUA, etc)
- Controle por aplicações, grupos estásticos e dinâmicos
- Filtragem
- Conteúdo web, Aplicações Web
- Perfis de Inspeções: SSL, IPS, Threat Protection, Web Filter e Application Control (podendo ser implementados em uma única política e a alteração de uma engine não impacta em outras)
- QoS (controle de banda/priorização)
- Múltiplos serviços
- Editor de regras de segurança (políticas de filtragem) com possibilidade de agendamento
- Habitar e desabilitar logs
- Tipos de ação: permitir, negar e rejeitar
- Criação de políticas por usuários ou grupos baseado em autenticação para todos os serviços (Firewall, VPN, IPS, Controle de Aplicação e outros)
- Simulador de tráfego, localizador e validador de política
- Detector de Políticas conflitantes no UTM e no GSM
- Bloqueio de arquivo por extensão e permite a correta identificação do arquivo por seu tipo MIME, mesmo quando sua extensão for renomeada

Web Cache e Proxy:

- Proxy Transparente ou Explícito (portas personalizadas)
- Configuração de tamanho de Cache em Disco e Memória
- Suporte a serviços web (HTTP e HTTPS versões 1.0, 1.1, 2.0 e FTP)
- Configuração de web cache em memória e disco
- Habilitação de web cache de conteúdos dinâmicos (Facebook, Google Maps, MSN Video, Sourceforge Downloads, Windows Update, Youtube)
- Exceção de cache, configurável por expressões regulares
- Hierarquia de proxy com e sem autenticação
- Suporte à integração Antivírus HTTP através de hierarquia de proxy
- Mensagem de bloqueio para o usuário final
- Suporta política por tempo, horário e/ou período (dia, mês, ano, dia da semana e hora). Suporta grupos de usuários, IPs, rede e/ou zonas de segurança

Firewall:

- Política com opção de autenticação com possibilidade de habilitar ou desabilitar log
- NAT (SNAT e DNAT), 1:1, N:1, NAT64, NAT46, NAT44 e NAT66, PAT, NAT de Origem e NAT de Destino e simultâneamente
- NAT dinâmico (Many-to-Many e Many-to-1)
- NAT estático (1:1 e Many-to-Many) e bidirecional 1:1
- Segurança
- Proteção DoS (Denial Of Service) também disponível na Política, PortScan, Pacotes inválidos, ICMP Sweep e Brute Force
- Proteção Flood (SYN, ICMP, UDP)
- Proteção Anti-spoofing
- ICMP (controles, transmissão, redirecionamento)
- PING (Echo/Request)
- Forward de Multicast
- Source routing, Checksum, Log inválidos
- Flow Control para aplicações Dinâmicas
- Bloqueio de tráfego de protocolos em portas customizadas
- Suporta objetos e regras multicast
- TCP_be_liberal
- IP spoofing
- Proteção contra ataques Man-in-the-Middle
- Controles de conexão TCP/UDP/ICMP/IP
- Suporta modo transparente (camada 2), modo gateway (camada 3) e espelhamento de porta
- Suporta os protocolos de real time

QoS – Qualidade de Serviço

- Marcação de pacotes para priorização de tráfego (TOS e DSCP)
- Fila de Prioridade de Menor Prioridade para Maior Prioridade
- Controle de tráfego e garantia de banda por política (aplicações, usuários ou grupos de usuários sincronizados com o Windows AD ou LDAP), zona de rede, host específico ou origem/destino

IPS - Sistema de Prevenção de Intrusos:

- Detecção e prevenção de ataques e intrusões baseada em +80mil assinaturas agrupadas como Client (Aplicações) e Server (Servidores)
- Suporte a Customização e upload de Assinaturas
- Níveis de Impacto: Baixo, Médio e Alto
- Proteção contra ameaças na camada de aplicação (Exploit conhecidos, Shellcode, SQL Injection, Buffer overflow etc.)
- Proteção contra pacotes mal-formados
- Reconhecimento de padrões, analise de protocolos e anomalias e bloqueia vulnerabilidades
- Capacidade de remontagem do pacote após a análise para identificação de ataques
- Limite de Sessões de Origens (Source Session Limit) com TCP Reset para encerramento da sessão
- Prevenção DoS, DDoS (Flood, Scan, Session e Sweepe), PORTSCAN, Reconnaissance, Evasione e ICMP
- Atenuação de ataques DoS e DDoS (negação de serviços)
- Prevenção contra ataques de tecnologia P2P
- Prevenção contra ataques do tipo Worm, Trojan, Backdoors, Portscans (detecta e bloqueia a origem), IP Spoofing, SYN-ICMP-UDP flood e Spywares
- Prevenção contra anomalias de protocolos (HTTP, SMTP, POP, IMAP, Sendmail, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, CIFS, RPC, RDP, CHARGEN, SSDP, SNMP, TCP highjacking, SSH e Telnet)
- Prevenção contra Botnet, DNS Poisoning e Scalation Privilege
- Bloqueio de SSH em portas não padrão do protocolo e baseado no comportamento através de padrões
- Suporte a configuração de exceção por assinatura de origem ou destino
- Log de registro das incidências para cada tipo de ataque identificado
- Trafego mal formado e cabeçalhos invalidos
- Atualização automática, periódica e offline
- Decodifica múltiplos formatos de unicode
- Fragmentação e desfragmentação IP
- Políticas aplicadas em interfaces ou zona de segurança
- Alarme via e-mail ou trap de SNMP
- Suporte a implementação inline L2 (bridge/modo transparente) e camada L3 (firewall)
- Suporta exceções por IP cadastrado nas regras
- Criação de Whitelist e Blacklist por IP (IPv4 e IPv6)
- Permite ativar ou desativar as assinaturas, ou habilitar em modo de monitoração

Threat Protection:

- Antivírus e Anti-Malware com analise em tempo real
- HTTP, HTTPS, FTP, SMB, CIFS, POP3 e SMTP (nativo na solução)
- Proteção contra aplicações não autorizadas
- (Packed, PwTool, NetTool, P2P, IRC, RAT, Tool, Spy)
- Proteção contra arquivos com senha
- Quarentena de Anti-Malware
- Relatório de arquivos escaneados
- Identifica, classifica e bloqueia malware tais como, trojan, spyware, adware, keyloggers, highjackers, worms, vírus, conexões do tipo C&C (Command and Control) e Anti-bot (Botnet)
- Permite o bloqueio por reputação do endereço classificado em 6 categorias: spam, reputation, malware, attacks, anonymous e abuse
- Atualização automática e periódica
- Antibot possui mecanismo de detecção em multicamadas, ex: reputação de endereço IP, URLs e endereços DNS e detecta padrões de comunicação e assinaturas

SD-WAN:

- Suporte a múltiplos perfis de configuração e permite habilitar em qualquer interface WAN (DSL, MPLS, 3G/4G LTE) e Packet Duplication (PD), agregação com recurso de VPN, suporta roteamento estático, dinâmico (OSPF, BGP). IPv4/IPv6, supota NAT dinâmico e de saída
- Definição de envio de tráfego por interface selecionada, suporta Policy Based Routing
- Failover, Load Balance, Spillover e Performance
- Monitoramento da disponibilidade do link e proteção contra degradação dos links de dados
- Suporta balanceamento de link por hash do IP de origem e destino, por peso com configuraçao do percentual e podendo utilizar de 2 a 9 links
- Verificação da falha do link por protocolo TCP/UDP Echo, ICMP (ping) e HTTP
- Medição por consumo de banda, perda de pacotes, jitter, latência (monitoramento de vários destinos e em todas as interfaces) com mais de 3 alvos, podendo ser alterado os valores de medição
- Roteamento baseado em aplicação e política para múltiplos caminhos WAN, com bloqueio de app
- Failback do link personalizavel de 1 a 100 e persistência de Links
- Implementa balanceamento de links sem criar zonas ou uso de instâncias virtuais
- Roteamento por grupo em regras de SD-WAN, balanceamento de tráfego por sessão e pacotes

Zero-touch Provisioning:

- Provisionamento automático associado ao número de série do equipamento
- Configura templates de segurança e politicas IPv4/IPv6

Secure Web Gateway:

- Filtro de Conteúdo (sem NAT)
- 88 categorias (incluindo Governo, Webmail, Instituições de Saúde, Notícias, Pornografia, Restaurante, Redes Sociais, Esporte, Educação, Jogos; Compras), +49 milhões de URLs catalogadas, controle de login por domínio no Google, integração SafeSearch (busca segura), Google, Bing e Yahoo, mensagem de bloqueio para o usuário final
- Inspeção SSL com bloqueio de certificado invalido
- Integração com a inspeção ATP e Windows AD / LDAP para identificação de usuários e grupos
- Bloqueio de Aplicações de Redes Sociais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, Bold Chat, ChatON, China.com,Facebook, Flickr, FC2, Fring, Google Analytics, GoogleApp, Linkedin, Meetup, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e ZohoChat e Aplicações de BatePapo
- Bloqueio de arquivos tipo Office, Java e JavaScript, Cookies, ActiveX, Multimidias, Imagens
- Reconhecimento de Aplicação – DPI (Deep Packet Inspetion)
- Identifica Aplicações através do protocolo SSL, HTTP, HTTPS ou portas de acesso não padrão
- Controle por SNI por categoria
- Filtragem, categorização e reclassificação de sites web por URL
- Autenticação de usuários em diretório LDAP, Radius, TACACs+ e Microsoft Active Directory
- Bloqueio por construção de filtros específicos com mecanismo de busca textual
- Bloqueio de certificados inválidos
- Listas personalizadas (whitelist e blacklist)
- Captive Portal com login social (Facebook, Twitter, Google)
- Cotas de navegação por tempo e/ou volume de tráfego
- Atualização Agendada e Automática transparentes

VPN IPSec e VPN SSL:

- VPN túnel (LAN to LAN) / VPN Site-to-Site e Client-to-Site
- VPN RAS/SSL (remote access permite acesso por cliente de VPN ou suporte direto na estação sem cliente - Interface Web), ou seja, pode utilizar a VPN SSL com ou sem agente
- VPN SSL Portal (via HTTPS) para acessos RDP, VNC, SSH, WEB e SMB
- Cliente VPN compatível com Win7, 8/8.1, 10 e 11 (32 e 64 bits), Linux e MacOS
- Autenticação
- Chave PSK (Pre-Shared Key), X-Auth (AD, LDAP, local, RADIUS), certificado digital IKE PKI, EAP (MSCHAPv2),
- Permite estabelecer o túnel antes ou após o usuário autenticar na estação e sob demanda do usuário
- Alta disponibilidade
- FQDN (Full Quality Domain Name) e Suporte DDNS
- NAT-T (encapsulamento UDP) e DPD (Dead Peer Detection)
- Exchange mode IKEv1: Main mode ou Aggressive mode
- Suporte a dados compactados
- Protocolos
  - IKEv1 e IKEv2 (para fase 1 e fase 2) e ESP
- Criptografia Simétricas:
  - AES(128, 192 e 256), 3DES
- Criptografia Assimétricas:
  - DH (Diffie-Hellman - Grupo1, Grupo2, Grupo5, Grupo14; Grupo15, Grupo16, Grupo17, Grupo18, Grupo19, Grupo20, Grupo21, Grupo22, Grupo23, Grupo24, Grupo25, Grupo26, Grupo27, Grupo28, Grupo29, Grupo30) RSA key generation, DSA parameter
- Suporta Auto-Discovery VPN (AD-VPN), Permite múltiplos dispositivos (Spokes) com gateway centralizador (hub) e Site-to-Site, Suporta túneis do tipo (Site-to-Site, Full Mesh, Star)
- Suporta os algoritmos RSA e Diffie-Hellman
- VPN SSL com suporte a certificado digital X.509 v3
- Suporta a inclusão (enrollment) de autoridades certificadoras mediante SCEP (Simple Certificate Enrollment Protocol)
- Suporte a IP Público Dinâmico, roteamento RIPv2 e OSPFv3
- Suporte a certificados emitidos por autoridade certificadora no padrão ICP-Brasil
- Suporte à verificação de certificate revocation list (CRL)
- VPN SSL e IPSec (client-to-site) com Blockbit Client para Windows
- Permite atribuir DNS nos clientes remotos de VPN
- Clientless VPN (IPSec e SSL) sem restrições de players de mercado
- Gerenciamento de certificados SSL (X.509)

Redes e Interfaces:

- Interfaces
- Ethernet (com suporte a FEC - Forward Error Correction)
- VLAN (IEEE 802.1q) até 4094 por interface
- Suporte WAN: ADSL/DSL, MPLS, LTE (3G/4G/5G)
- Alias (Virtual IP)
- LTE (4G) utilização como link para load balance e failover
- Link aggregation
- Ethernet bonding (802.3ad) LACP
- Roteamento dinâmico: BGP4/BGP4+, OSPFv2/v3, RIPv2 e PIM-SM
- Roteamento estático (IPv4 e IPv6) com suporte a ECMP
- Roteamento Multicast: suporta regras e objetos
- Suporte nativo a IPv4 e IPv6
- DHCP (dynamic host configuration protocol) IPv4 e IPv6
- Relay, Server e Client
- DNS Recursivo
- Roteamento baseado em política (PBR - Policy Based Routing ou PBF – Policy Based Forwarding)
- Suporta sub-interfaces ethernet lógicas

Autenticação:

- Autenticação de Usuários
- Local, Windows AD, LDAP, SSO Windows (single sign on via Kerberos) e WMI – autenticação unificada, X-Auth para serviços de VPN, autenticação em servidores Radius, RSSO (radius single sign on), identificador de complexidade de senha, Token ID, Sessões e Aplicações baseadas em TCP/UDP/ICMP
- Suporte TACACS+ para usuários de administração e usuários de Firewall;
- Integração LDAP para administração da Blockbit Platform;
- Sincronismo de usuários e grupos e hosts com servidores Windows AD e servidores LDAP com replicação de sessões estabelecidas dos usuários
- AAA (Authentication, Authorization e Accounting)
- A identificação pela base do AD permiti o uso de SSO, de forma que os usuários não precise logar novamente na rede para navegar pelo firewall;

Log e Relatórios

- Suporte Netflow / IPFIX
- Relatórios de Log de Sessão, Autenticação e VPN
- Criação de relatório customizável do tipo Analyzer (nativo na ferramenta) dos serviços de Firewall, Web Filter, Application Control, IPS, ATP, VPN e User Behavior (informações de IP, Sistema Operacional do usuário, Hostname e classificação de ameaças em estilo "top 10")
- Syslog Remoto para envio dos logs e exportação de log via SCP, suporta envio do log via protocolo SSL
- Exportação de relatórios em múltiplos formatos (PDF, CSV, HTML)
- Os eventos identificam o país da origem do ataque
- Eventos registram alterações no estado e a saúde dos links do SDWAN

Interface WEB e CLI:

- Granularidade (perfis de leitura e leitura/escrita, aplicação de configurações etc) de acesso administrador na Interface Web com sessões simultâneas
- CLI (interface em linha de comando para gerenciamento e diagnóstico via SSH e serial RS-232/RJ-45
- Interface Web própria disponível em Português, Inglês e Espanhol acessível por qualquer interface física do produto
- Gerenciamento (LAN ou WAN) via WEB (HTTPS por browser) e SSH

Monitoramento:

- Suporte ao protocolo SNMP v1, v2 e v3, monitora o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança
- Desempenho, conexões simultâneas, lease do DHCP, usuários autenticados e serviços habilitados ou desabilitados
- Notificações de Sistema e de Segurança
- Janela de visualização de eventos detalhados
- Ferramenta para manutenção do disco e monitoramento de tráfego de rede em tempo real (Live Sessions eTrafic Monitor) com informações de throughput e conexões simultâneas
- Logs de Eventos de segurança e Ameaças
- TCPDUMP por Feature e proteções específicas (permite captura e download em formato PCAP)
- Registro de usuários nos eventos de autenticação, acesso, bloqueio e ameaças
- Contadores RX/TX, entrada e saída de pacotes, descartes de pacotes e erros (Comando CLI)

Backup e Restore:

- Snapshot e Backup do Sistema criptografado
- Disaster recovery (backup/restore) pela interface Web
- Armazenamento (para backup e salva de logs)
- NFS / DISK(HDD) / SSH / Flash (via USB)
- Backup Rotation nos armazenamentos
- Agendamento de Backup do tipo Snapshot ou de Sistema

Outros Recursos:

- Proxy Services (SSH, SMB/CIFS, HTTP, FTP, SMTP, POP3)
- Suporta Voip (SIP/H323) e RTP sobre IPv4/IPv6
- Suporte a múltiplos domínios de Autenticação
- Suporta fail-closed e opcional de interface fail-open (by-pass)
- Atualização automática, periódica e offline
- Suporta autenticação das sessões para todos os protocolos e quaisquer aplicações
- Objetos de recursos
- Endereços IP, Endereços MAC, Serviços de portas e protocolos, Tabela de horários, Tabela de períodos e datas, Dicionários (conjunto de palavras e/ou expressões regulares), Tipos de conteúdo
- Suporte a servidores NTP (Network Time Protocol) para atualização de data e hora
- Opção de atualizações automáticas e periódicas do sistema para correções e releases web HTTPS ou via GSM
- Otimização de Fluxos TCP
- Suporta acesso via SSH, CLI, cliente ou WEB (HTTPS)
- Virtualização do equipamento em Cloud Pública (Google Cloud®, Azure®, Oracle Cloud® e AWS®) ou Cloud Privada (Vmware®, Citrix XenCenter® e ProxMox®)
- Suporte a Contexto (Virtual Domain)
- Sistema de Cluster High Availability (Ativo-Passivo e Ativo/Ativo e somente com equipamentos iguais) com manutenção da sessões estabelecidas, distribuição de tráfego, manutenção da tabela de estado e balanceamento de sessão
- Suporte a dois ou mais membros no cluster
- Suporta duas interfaces de rede para sistema de cluster H.A.

Outros Recursos

- Capaz de identificar o usuário da rede, suporta AD, LDAP, RADIUS e TACACs
- Sem instalação de agentes no AD, nem nas estações dos usuários
- Todas as políticas suportam o controle de aplicações
- Suporta diversos métodos de identificação e classificação das aplicações, por exemplo, checagem de assinaturas e decodificação de protocolos
- Permite a criação de assinaturas personalizadas na interface WEB para reconhecimento de aplicações e de IPS/IPS
- Suporta cadastrar exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação
- A Blockbit permite solicitações de inclusão de aplicações na base padrão
- É possível diferenciar diferentes tráfegos P2P para diversos software (Bittorrent, emule e outros) com granularidade no controle dos aplicativos
- Possibilita a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc.), aplicações Proxies (psiphon, freegate, etc) e possui granularidade de controle e ou políticas
- Suporta granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilita a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens
- Permiti usar operadores de negação na criação de assinaturas customizadas de IPS, permitindo a criação de exceções com granularidade nas configurações
- Registra na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além
da ação tomada pelo dispositivo
- Possui proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e Worms
- Proteção contra downloads involuntários usando HTTP de arquivos executáveis e/ou maliciosos
- Permite a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, MAC Address, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança
- Suporta Sistema Virtuais (VDOM) em todos os modelos
- VDOM permite acriar contextos virtuais com suporte a criação de diversos administradores

SandBoxing - APT

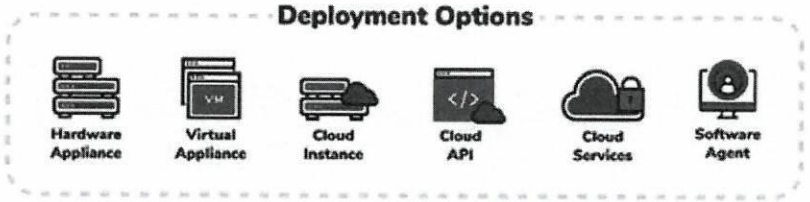
- Permite mitigar ameaças avançadas persistentes (APT e Zero-Day), através de análises dinâmicas para identificação de malwares desconhecidos com atualização automática em base de dados em rede de inteligência. Analisa arquivos do tipo PDF, Microsoft Office, executáveis e compactados;
- O SandBox Blockbit é capaz de criar assinaturas e ainda incluí-las na base de antivírus do firewall, prevenindo a reincidência do ataque
- Suporta incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Blocklist), impedindo que esses endereços sejam acessados pelos usuários de rede novamente
- O módulo de ATP suporta analisar o arquivo pelo antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back e também análisa o comportamento de arquivos suspeitos em um ambiente controlado, em tempo real
- Capaz de emular, detectar e bloquear qualquer malware e/ou código malicioso. Emula SandBox de ambientes Microsoft em versões variadas e Office

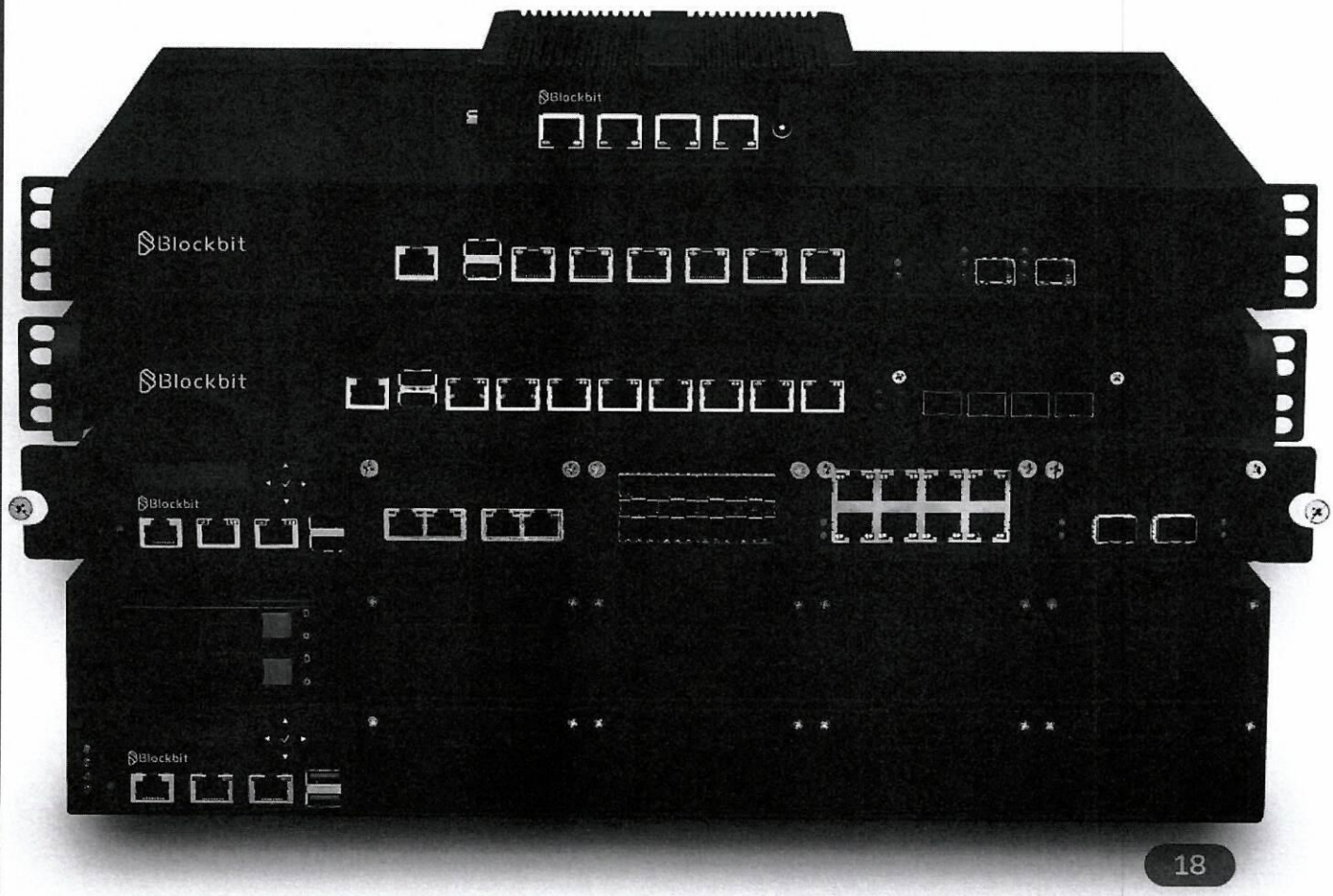
Identificação do Usuário

- Permite a criação de políticas baseadas no controle por URL e categorias de URL
- Permite criar políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local
- Possui compatibilidade com Microsoft Active Directory(Windows 2003, 2012 e 2019) para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários
- Possui integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Suporta usuários ilimitados.
- Suporta autenticação para Firewall e VPN: Tokens, TACACS, RADIUS e certificados digitais;
- Permite o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal)
- Suporta a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços
- Permite a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD

Filtro de Dados

- Possui recurso capaz de identificar e prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, HTTPS, FTP, SMTP)
- É capaz identificar na rede de dados arquivos compactados e aplicar políticas de uso sobre o conteúdo desses tipos de arquivos





Algumas RFC's suportadas pelo Blockbit Platform:

BGP:

- RFC 7911: Advertisement of Multiple Paths in BGP
- RFC 7606: Revised Error Handling for BGP UPDATE Messages
- RFC 4724: Graceful Restart Mechanism for BGP
- RFC 4456: BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 4360: BGP Extended Communities Attribute
- RFC 4271: A Border Gateway Protocol 4 (BGP-4)
- RFC 2918: Route Refresh Capability for BGP-4
- RFC 2545: Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2439: BGP Route Flap Damping
- RFC 1997: BGP Communities Attribute
- RFC 1930: Guidelines for creation, selection, and registration of an Autonomous System (AS)
- RFC 1772: Application of the Border Gateway Protocol in the Internet

OSPF:

- RFC 6860: Hiding Transit-Only Networks in OSPF
- RFC 6845: OSPF Hybrid Broadcast and Point-to-Multipoint Interface Type
- RFC 5709: OSPFv2 HMAC-SHA Cryptographic Authentication
- RFC 5340: OSPF for IPv6
- RFC 4812: OSPF Restart Signaling
- RFC 4811: OSPF Out-of-Band Link State Database (LSDB) Resynchronization
- RFC 4203: OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
- RFC 3630: Traffic Engineering (TE) Extensions to OSPF Version 2
- RFC 3623: Graceful OSPF Restart
- RFC 3509: Alternative Implementations of OSPF Area Border Routers
- RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option
- RFC 2328: OSPF Version 2
- RFC 1765: OSPF Database Overflow
- RFC 1370: Applicability Statement for OSPF

RIP:

- RFC 4822: RIPv2 Cryptographic Authentication
- RFC 2453: RIP Version 2
- RFC 2080: RIPng for IPv6
- RFC 1724: RIP Version 2 MIB Extension
- RFC 1058: Routing Information Protocol

DHCP:

- RFC 4361: Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
- RFC 3736: Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
- RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
- RFC 3456: Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 2131: Dynamic Host Configuration Protocol

Diffserv:

- RFC 3260: New Terminology and Clarifications for Diffserv
- RFC 2597: Assured Forwarding PHB Group
- RFC 2475: An Architecture for Differentiated Services
- RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

IPv4 e IPv6:

- RFC 6864: Updated Specification of the IPv4 ID Field
- RFC 5177: Network Mobility (NEMO) Extensions for Mobile IPv4
- RFC 4632: Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses
- RFC 3021: Using 31-Bit Prefixes on IPv4 Point-to-Point Links
- RFC 1812: Requirements for IP Version 4 Routers
- RFC 7761: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
- RFC 6343: Advisory Guidelines for 6to4 Deployment
- RFC 5175: IPv6 Router Advertisement Flags Option
- RFC 5095: Deprecation of Type 0 Routing Headers in IPv6
- RFC 4941: Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC 4389: Neighbor Discovery Proxies (ND Proxy)
- RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 4193: Unique Local IPv6 Unicast Addresses
- RFC 4007: IPv6 Scoped Address Architecture
- RFC 3971: Secure Neighbor Discovery (SEND)
- RFC 3596: DNS Extensions to Support IP Version 6
- RFC 3587: IPv6 Global Unicast Address Format
- RFC 3493: Basic Socket Interface Extensions for IPv6
- RFC 3056: Connection of IPv6 Domains via IPv4 Clouds
- RFC 3053: IPv6 Tunnel Broker
- RFC 2894: Router Renumbering for IPv6
- RFC 2675: IPv6 Jumbograms
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 2185: Routing Aspects Of IPv6 Transition
- RFC 1752: The Recommendation for the IP Next Generation Protocol
- RFC 8200: Internet Protocol, Version 6 (IPv6) Specification
- RFC 8201: Path MTU Discovery for IP version 6

NAT:

- RFC 7857: Updates to Network Address Translation (NAT) Behavioral Requirements
- RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC 5508: NAT Behavioral Requirements for ICMP
- RFC 5382: NAT Behavioral Requirements for TCP
- RFC 4787: NAT Behavioral Requirements for Unicast UDP
- RFC 4380: Teredo: Tunneling IPv6 over UDP through NAT
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3022: Traditional IP Network Address Translator (Traditional NAT)

SIP:

- RFC 3960: Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
- RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC 3262: Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3261: SIP: Session Initiation Protocol

LDAP:

- RFC 4513: Authentication Methods and Security Mechanisms
- RFC 4512: Directory Information Models
- RFC 4511: The Protocol
- RFC 3494: Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status

SNMP:

- RFC 4293: Management Information Base for the IP
- RFC 4273: Definitions of Managed Objects for BGP-4
- RFC 4113: Management Information Base for the User Datagram Protocol (UDP)
- RFC 4022: Management Information Base for the TCP
- RFC 3635: Definitions of Managed Objects for the Ethernet-like Interface Types
- RFC 3417: Transport Mappings for the SNMP
- RFC 3416: Version 2 of the Protocol Operations for the SNMP
- RFC 3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3413: SNMP Applications
- RFC 3412: Message Processing and Dispatching for the SNMP
- RFC 3411: An Architecture for Describing SNMP Management Frameworks
- RFC 3410: Introduction and Applicability Statements for Internet Standard Management Framework
- RFC 2863: The Interfaces Group MIB
- RFC 2578: Structure of Management Information Version 2 (SMIv2)
- RFC 1238: CLNS MIB for use with Connectionless Network Protocol (ISO 8473) and End System to Intermediate System (ISO 9542)
- RFC 1215: A Convention for Defining Traps for use with the SNMP
- RFC 1213: Management Infor mation Base for Network Management of TCP/IP-based internets: MIB-II
- RFC 1212: Concise MIB Definitions
- RFC 1157: A Simple Network Management Protocol (SNMP)
- RFC 1156: Management Information Base for Network Management of TCP/IP-based internets
- RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets

VPN:

- RFC 4761: Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
- RFC 4684: Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
- RFC 4577: OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)
- RFC 3715: IPsec-Network Address Translation (NAT) Compatibility Requirements

TLS e SSL:

- RFC 8446: The TLS Protocol Version 1.3
- RFC 6347: Datagram Transport Layer Security Version 1.2
- RFC 6066: TLS Extensions: Extension Definitions
- RFC 5746: TLS Renegotiation Indication Extension
- RFC 5425: TLS Transport Mapping for Syslog
- RFC 5246: TLS Protocol Version 1.2
- RFC 4680: TLS Handshake Message for Supplemental Data
- RFC 6176: Prohibiting Secure Sockets Layer (SSL) Version 2.0
- RFC 6101:The Secure Sockets Layer (SSL) Protocol Version 3.0

Outros Protocolos:

- RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport
- RFC 7541: HPACK: Header Compression for HTTP/2
- RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2)
- RFC 5424: The Syslog Protocol
- RFC 4960: Stream Control Transmission Protocol
- RFC 3376: Internet Group Management Protocol, Version 3
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 1928: SOCKS Protocol Version 5. Supported when explicit proxy is implemented.
- RFC 1413: Identification Protocol
- RFC 1305: NTP (Version 3) Specification, Implementation and Analysis
- RFC 959: File Transfer Protocol (FTP)
- RFC 862: Echo Protocol
- RFC 783: The TFTP Protocol (Revision 2)
- RFC 768: User Datagram Protocol
- The TACACS+ Protocol

Criptografia:

- RFC 7627: Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension
- RFC 7427: Signature Authentication in the IKEv2
- RFC 7383: IKEv2 Message Fragmentation
- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7027: Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)
- RFC 6989: Additional Diffie-Hellman Tests for the IKEv2
- RFC 6954: Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the IKEv2
- RFC 6290: A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE)
- RFC 6023: A Childless Initiation of the IKEv2 Security Association (SA)
- RFC 5723: IKEv2 Session Resumption
- RFC 5282: Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 4754: IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
- RFC 4635: HMAC SHA TSIG Algorithm Identifiers
- RFC 4492: Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
- RFC 4478: Repeated Authentication in IKEv2 Protocol
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for IKE
- RFC 2631: Diffie-Hellman Key Agreement Method
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2104: HMAC: Keyed-Hashing for Message Authentication
- RFC 2085: HMAC-MD5 IP Authentication with Replay Prevention
- RFC 1321: The MD5 Message-Digest Algorithm
- RFC 3768: Virtual Router Redundancy Protocol (VRRP)
- RFC 2787: Definitions of Managed Objects for the Virtual Router Redundancy Protocol

OS TESTES FORAM REALIZADOS EM LABORATÓRIO SEM SUMARIZAÇÃO POR USUÁRIOS, IPS E SERVIÇOS, DETECTORES DE APLICATIVOS DESABILITADOS, FIREWALL THROUGHPUT UDP PACOTES DE 1518 BYTES, FIREWALL THROUGHPUT HTTP GET 1280Kb e PUT 1280K, IPS/ATP THROUGHPUT COM ASSINATURAS PADRÃO DE FÁBRICA HABILITADAS. [1]NGFW É MEDIDO COM FIREWALL, IPS E CONTROLE DE APLICATIVO HABILITADOS, TRÁFEGO IMIX.

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Algar Telecom S/A (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Algar Telecom S/A:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To advise Algar Telecom S/A of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at and in the body of such request you must state: your previous email address, your new email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Algar Telecom S/A

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to and in the body of such request you must state your email address, full name, mailing address, and telephone number.

To withdraw your consent with Algar Telecom S/A

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to and in the body of such request you must state your email, full name, mailing address, and telephone number. . .

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Algar Telecom S/A as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Algar Telecom S/A during the course of your relationship with Algar Telecom S/A.