Blockbit

Blockbit Platform

Cibersegurança integrada, convergindo conectividade e segurança

- Secure SD-WAN
- Next-Generation Firewall

blockbit.com

Sobre a Blockbit

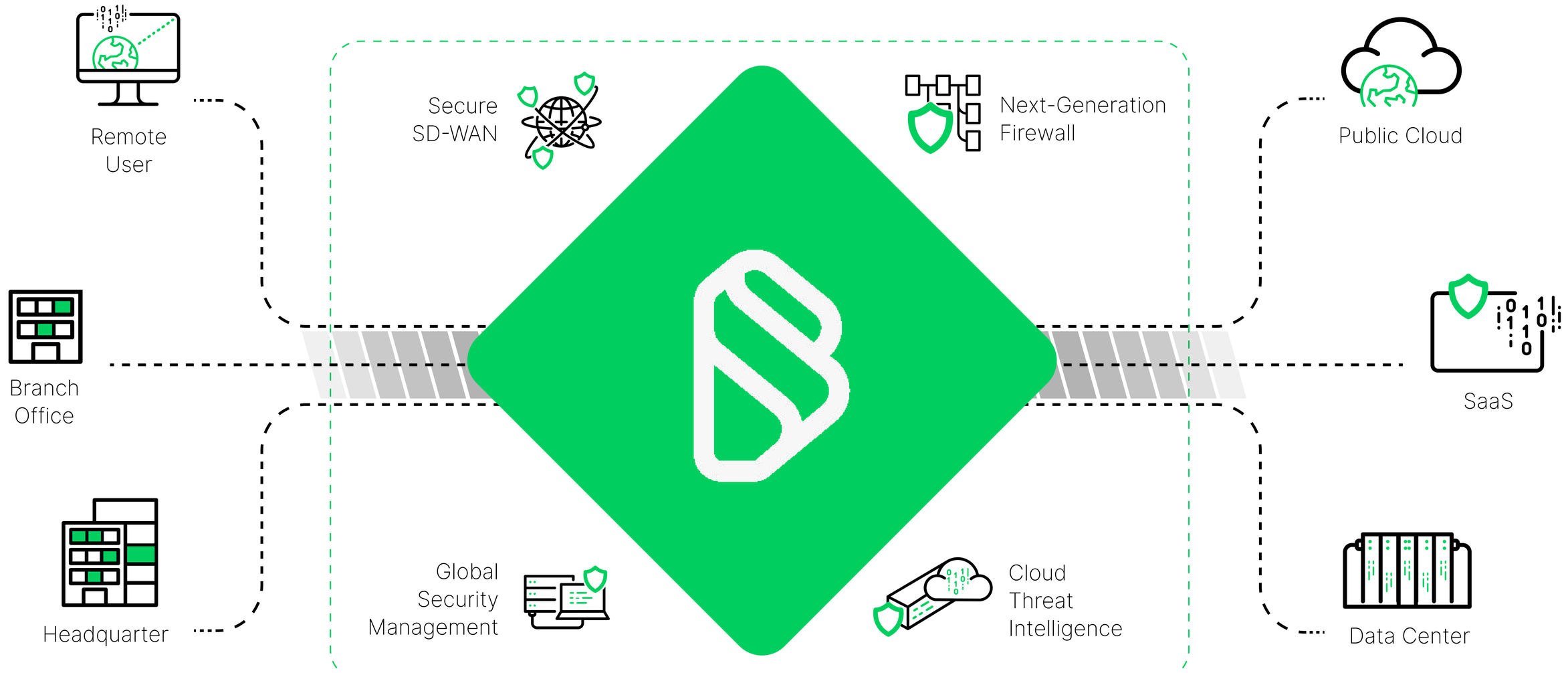
A Blockbit é a líder brasileira em produtos de cibersegurança, protegendo milhares de empresas e milhões de usuários de ataques e ameaças digitais. Com tecnologias de última geração e avançado laboratório de inteligência, a Blockbit desenvolve soluções proprietárias para proteção de redes e conectividade segura com alta qualidade e performance, sempre alinhada às principais tendências globais de cibersegurança.

Conheça a Blockbit Platform

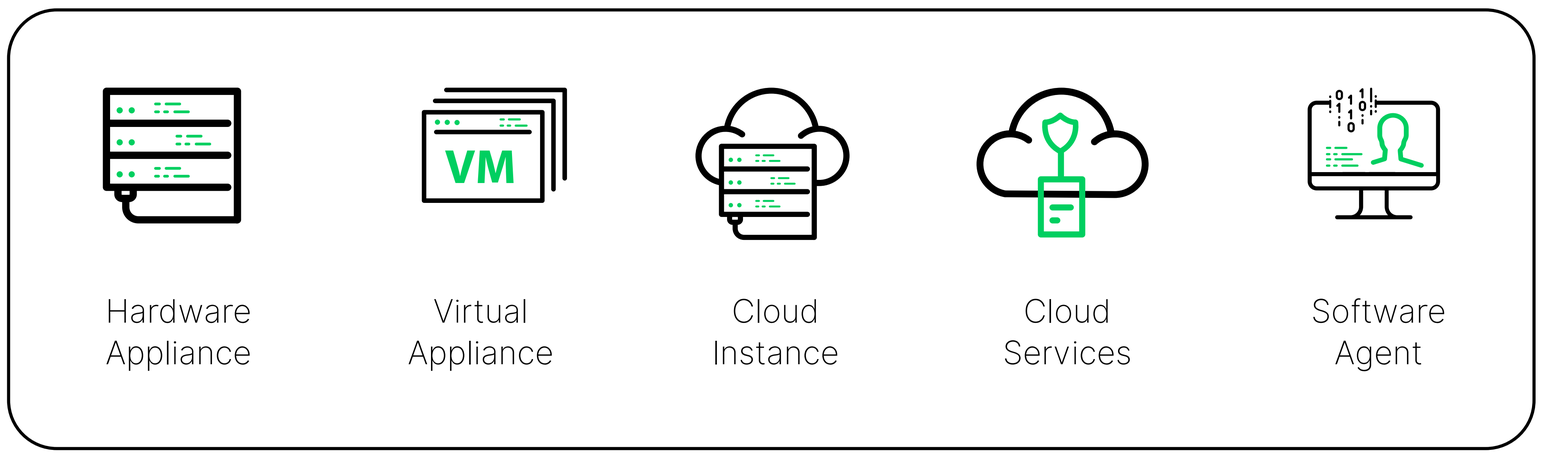
A Blockbit Platform está perfeitamente alinhada com a tendência global de convergência da conectividade com a segurança, proporcionando sólida proteção de rede e conectividade segura de ponta a ponta.

A nossa plataforma é composta pelo **Blockbit Secure SD-WAN** e pelo **Blockbit NGFW** (Next-Generation Firewall), ambos complementados pelo **Blockbit GSM** (Global Security Management) para gerenciamento centralizado e simplificado de múltiplos dispositivos. Além disso, o **Blockbit Cloud Threat Intelligence** fornece constantemente inteligência avançada aos produtos.

A Blockbit Platform une em só uma solução os produtos inovadores essenciais para acelerar o seu negócio com segurança, assegurando a qualidade e a performance desejadas.



Opções de Implantação



blockbit.com

Com a Blockbit, é fácil estar seguro

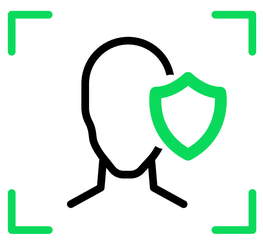
A Blockbit Platform oferece uma solução avançada e robusta com recursos inovadores que reduzem o seu tempo operacional, com configuração automatizada, gerenciamento centralizado e processos intuitivos. Com isso, você tem mais tempo para focar no que de fato interessa: **no seu negócio**.

Seja no aprimoramento da segurança, na otimização do desempenho ou na economia de tempo, a Blockbit está aqui para simplificar o caminho em direção a um ambiente digital mais seguro e eficiente.

Simplifique a sua rede, unificando conectividade e segurança

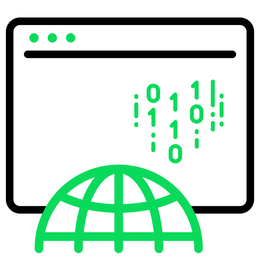
Nossa plataforma simplifica drasticamente a complexidade das redes, integrando de forma harmoniosa a conectividade e a segurança, sendo capaz de detectar aplicações encapsuladas e validar se o tráfego corresponde com a especificação do protocolo.

Com a Blockbit, você reduz a sobrecarga de operação e administração, garantindo uma postura de segurança consistente e robusta em toda a sua infraestrutura.



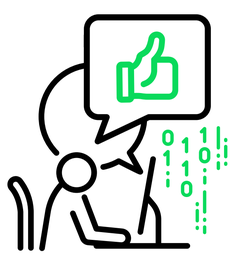
Configure automaticamente seus dispositivos

Com recursos de configuração automática, a implantação dos dispositivos torna-se mais eficiente do que nunca. Não é necessário perder tempo instalando nossos dispositivos, a Blockbit cuidou disso para você. Centralize configurações e as distribua automaticamente para os ativos remotos. Com o recurso ZTP (Zero-Touch Provisioning), é possível reduzir tempo e custo na implementação.



Gerencie todos os dispositivos da Blockbit de um só lugar

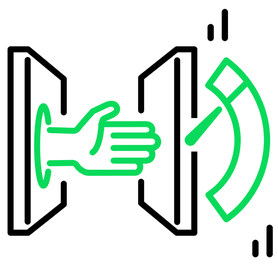
A Blockbit possibilita que você gerencie todos os seus dispositivos e eventos de segurança a partir de um único local centralizado. Isso elimina a complexidade de lidar com múltiplas interfaces e otimiza o fluxo de trabalho, economizando tempo, permitindo ações rápidas e decisões informadas.



Reduza tempo com uma interface amigável e intuitiva

A Blockbit Platform foi projetada com uma interface de usuário amigável e intuitiva, reduzindo significativamente o tempo necessário para a gestão e configuração de dispositivos de segurança.

Isso coloca o controle nas suas mãos, sem a necessidade de curva de aprendizado extensa e permitindo que você execute suas funções de forma mais rápida.



Tenha mais qualidade e performance, com preço acessível

Combinando tecnologia de ponta com abordagens de otimização de desempenho, a Blockbit garante que sua segurança cibernética não comprometa a velocidade e a eficiência da sua rede.

Tudo isso é oferecido a um preço acessível, garantindo que a qualidade esteja ao alcance de todas as empresas.

Secure SD-WAN

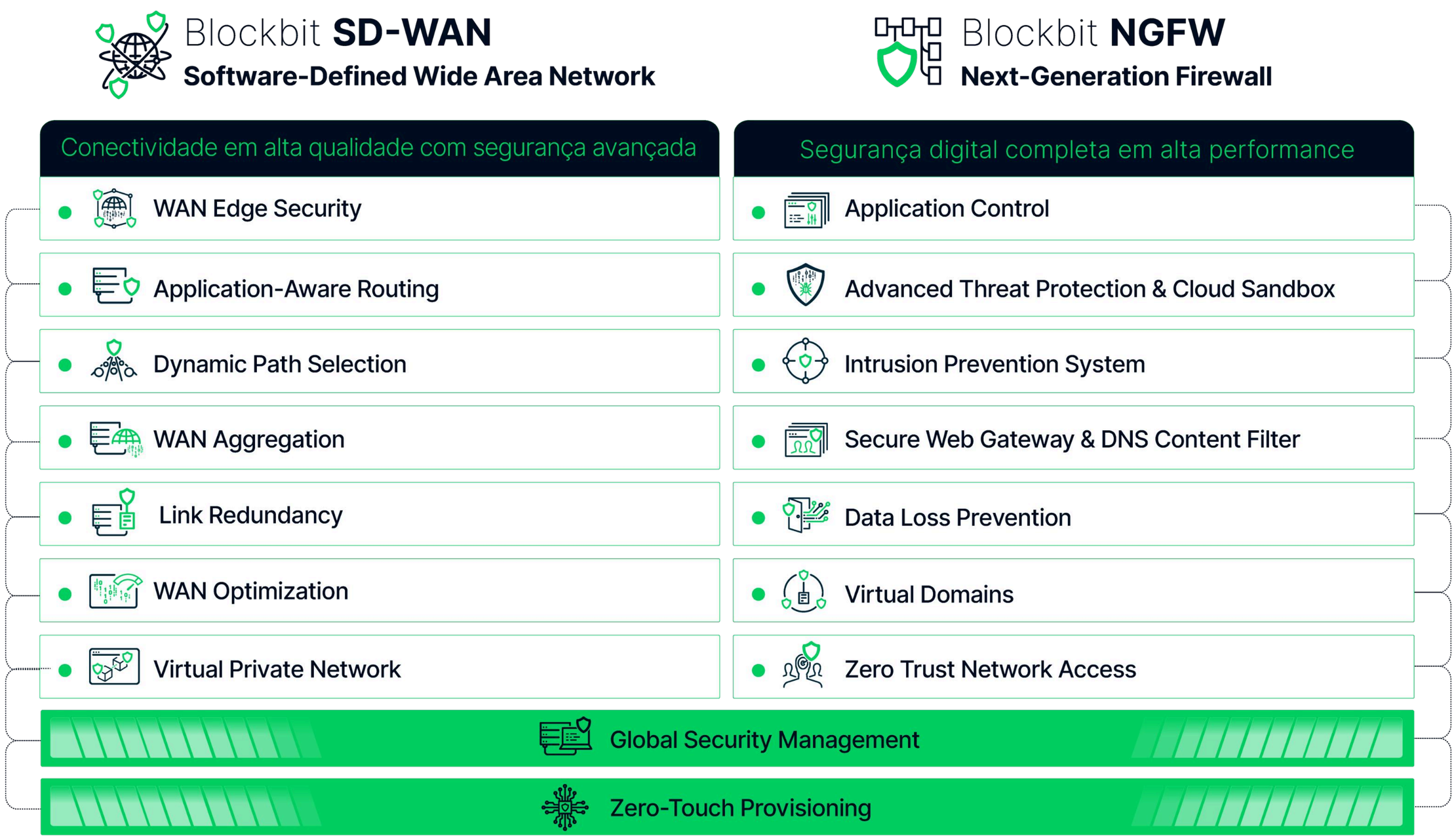
O **Blockbit Secure SD-WAN** é uma poderosa combinação do SD-WAN com todos os recursos avançados de segurança cibernética da Blockbit. Com isso, você soluciona seus principais desafios, tanto de conectividade quanto de segurança. Agora você consegue aumentar a qualidade do serviço das suas conexões, adotar soluções mais baratas de link e proteger seu ambiente, enquanto reduz seu custo de aquisição e custo operacional por ter uma solução única, unificando e minimizando riscos de continuidade e conflitos por ter um único ponto de controle.

Monitoramento de múltiplos links para conexão de longa distância, suportando conexões do tipo: **ADSL/DSL, Cable Modem com Ethernet ou fibra, LT/3G/4G/5G, MPLS, link de rádio, link satélite, entre outros.**

Next-Generation Firewall

O **Blockbit NGFW** (Next-Generation Firewall) é a evolução dos firewalls convencionais e oferece recursos avançados para proteção de ataques e ameaças, e vai além da proteção da rede protegendo também as aplicações e os usuários. Com esta solução, você poderá analisar em tempo real o tráfego de aplicativos, permitindo políticas de segurança mais granulares e eficientes, podendo ser implementado como gateway (L2) ou inline (L3), otimizada para análise de conteúdo de aplicação na camada 7, proporcionando maior controle e visibilidade sobre o seu ambiente e negócio.

Com o **Blockbit NGFW**, você tem à disposição a mais avançada ferramenta para enfrentar os desafios da segurança digital e proteger seus dados, usuários e sistemas de ameaças e ataques.



Blockbit Secure SD-WAN

Garanta a qualidade de serviço das conexões e aplicações, com segurança avançada

O **Blockbit Secure SD-WAN** é uma solução completa e de última geração para o controle, segurança avançada e gerenciamento centralizado de todas as conexões WAN. Com uma arquitetura moderna e escalável, composta pelos recursos inovadores, você poderá simplificar e aprimorar a rede de sua organização, conferindo maior eficiência e confiabilidade. Com isso, você tem a flexibilidade para escolher as melhores opções de conectividade para sua empresa, permitindo a redução de seu custo com infraestrutura.

Com a Blockbit, a integração e o gerenciamento de várias conexões de rede se tornam realidade, independentemente do fornecedor, da tecnologia ou do tipo de conexão. Por exemplo, usando recursos como o **WAN Aggregation & Link Failover**, você pode agregar links de diversos fornecedores e estabelecer um plano de contingência para situações em que algum deles falhe. Essa funcionalidade assegura uma maior redundância e disponibilidade para a sua rede, prevenindo interrupções indesejadas.

Descubra os principais módulos do Blockbit Secure SD-WAN:

Application-Aware Routing (AAR)

Prioriza e otimiza o tráfego de aplicativos críticos para garantir a performance e aumentar a resiliência do seu negócio.

Dynamic Path Selection (DPS)

Permite definir automaticamente a melhor rota para o tráfego de aplicativos, com base em requisitos de qualidade de serviço, política de negócios e condições de rede.

WAN Optimization

Acelera a entrega de aplicativos, reduzindo o tempo de latência, além de melhorar a eficiência da largura de banda e reduzir o tamanho dos pacotes transmitidos.

WAN Aggregation

Combina várias conexões em uma única rota lógica, aumentando a largura de banda, disponibilidade, confiabilidade, qualidade e performance da sua conexão.

Link Failover

Oferece resiliência à rede em caso de falha de uma ou mais conexões, detectando falha de conexão e automaticamente redirecionando o tráfego para uma conexão secundária.

Virtual Private Network (VPN)

Permite comunicação segura e privada entre filiais e colaboradores, possibilitando acessar remotamente as informações, sistemas e recursos internos.

WAN Edge Security

Integra todos os recursos de segurança avançada em uma única solução, adicionando os módulos de ATP, IPS e SWG, protegendo sua rede, conexão de ataques e ameaças externas e internas.

Global Security Management (GSM)

Defina modelos de configuração para o gerenciamento centralizado (Manager) de múltiplos dispositivos de segurança e consolide logs e eventos de tráfego (Analyzer).

Zero-Touch Provisioning (ZTP)

Simplifica a implantação do Blockbit Secure SD-WAN, permitindo a configuração remota e instalação automatizada de dispositivos.

Multi-Factor Authentication (MFA)

Oferece um segundo fator de autenticação para validar as autenticações de seus usuários, garantindo maior segurança para acessos aos recursos da Blockbit.

Blockbit Next-Generation Firewall

Proteja a sua empresa com o melhor firewall de última geração

O **Blockbit NGFW** é um firewall corporativo de última geração e alto desempenho, que incorpora em uma única solução controles e proteções avançadas para usuários, aplicações e rede.

A solução incorpora inspeção detalhada de pacotes (DPI), controle de aplicação, proteção avançada contra ameaças (ATP), sistema de prevenção de intrusão (IPS), filtro de conteúdo web (SWG), conexão remota segura (VPN), gerenciamento centralizado e consolidação de eventos (GSM), e muito mais. Graças ao recurso de inspeção de tráfego criptografado, que hoje representa a grande maioria do tráfego, a solução permite o controle e bloqueio de ameaças e ataques que utilizam a criptografia para se ocultar.

Descubra os principais módulos do Blockbit NGFW:

Deep Packet Inspection (DPI)

Oferece recursos de inspeção profunda de pacotes e tráfegos abertos e criptografados, permitindo identificar e bloquear atividades maliciosas, aplicativos específicos, protocolos de rede, tipos de dados e até mesmo ameaças ocultas.

Application Control

Permite controlar e gerenciar o uso de aplicativos e serviços, identificando automaticamente milhares de aplicativos, controlando o uso e priorizando banda, e gerando informações analíticas sobre o uso de aplicativos.

Advanced Threat and Malware Protection (ATP)

Detecta e bloqueia ameaças cibernéticas utilizando recursos avançados de Inline Sandbox, utilizando inteligência artificial e aprendizado de máquina, para proteger o ambiente de ameaças avançadas e malware, incluindo ransomware.

Cloud Sandbox

Integrado ao módulo de ATP, oferece uma camada adicional para proteção avançada contra ameaças desconhecidas, emulando e executando arquivos suspeitos na nuvem proprietária da Blockbit.

Intrusion Prevention System (IPS)

Cria logs de registro de incidências e eleva a sua visibilidade, identifica e bloqueia de forma ativa tráfegos maliciosos que tentam explorar vulnerabilidades em aplicações e serviços de sua rede.

Secure Web Gateway (SWG)

Gerencie o acesso de seus usuários aos recursos da web, prevenindo o comportamento de riscos ou improdutivo dentro da sua empresa ou remotamente.

DNS Content Filter

Possibilita a definição de políticas de acesso à internet de forma mais granular e específica, garantindo maior segurança e controle sobre a navegação.

Virtual Domains (VDOM)

Permite segmentar o Blockbit em múltiplos domínios virtuais, com administrações independentes, para controle e proteção de múltiplas redes com um único dispositivo.

Zero Trust Network Access (ZTNA)

Integrado ao módulo de VPN, fornece acesso granular baseado em vários fatores de segurança e apenas aos recursos específicos necessários aos usuários.

Global Security Management (GSM)

Define modelos de configuração para o gerenciamento centralizado (Manager) de múltiplos dispositivos de segurança e consolida logs e eventos de tráfego (Analyzer).

Zero-Touch Provisioning (ZTP)

O recurso ZTP simplifica a implantação do Blockbit NGFW, permitindo a configuração remota e instalação automatizada de dispositivos.

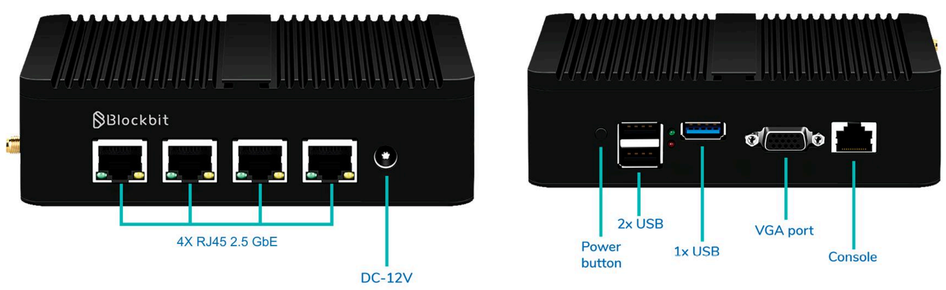
Multi-Factor Authentication (MFA)

Oferece um segundo fator de autenticação para validar as autenticações de seus usuários, garantindo maior segurança para acessos aos recursos da Blockbit.

Appliances Blockbit

Especificações de Desempenho e Opcionais

BBX40



BBX40	
Tipo	Mesa
Firewall Throughput (UDP)	7 Gbps
Concurrent Connections	4.000.000
New Connections Per Second	37.000
NGFW Throughput (IMIX)	200 Mbps
SSL Inspection Throughput	150 Mbps
IPS Throughput	320 Mbps
Application Control Throughput *	260 Mbps
Threat Protection Throughput	150 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	450 Mbps
SSL VPN Throughput (AES-256)	240 Mbps
Interfaces UTP 2.5 GbE	4
LTE 3G/4G	Opcional
Disco SSD	64GB, 120GB ou 240GB
Available Slots	*

BBX80

BBX80	
Tipo	Mesa
Firewall Throughput (UDP)	10 Gbps
Concurrent Connections	6.000.000
New Connections Per Second	45.000
NGFW Throughput (IMIX)	850 Mbps
SSL Inspection Throughput	700 Mbps
IPS Throughput	1.25 Gbps
Application Control Throughput *	1.3 Gbps
Threat Protection Throughput	700 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	2.0 Gbps
SSL VPN Throughput (AES-256)	1.2 Gbps
Interfaces UTP 2.5 GbE	4
Wi-Fi	Opcional
LTE 3G/4G	Opcional (até 2 modens)
Disco SSD	64GB, 120GB ou 240GB
Available Slots	*

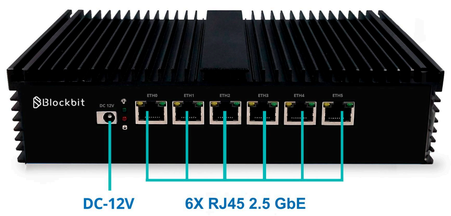
Fotos meramente ilustrativas.

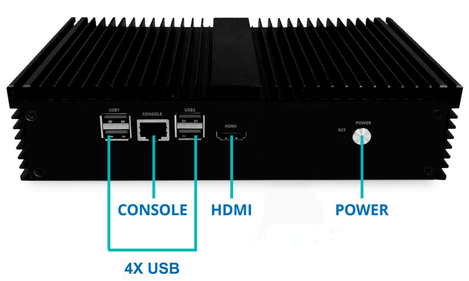
* O desempenho de Application Control utiliza a metodologia baseado em proxy (proxy based).

Appliances Blockbit

Especificações de Desempenho e Opcionais

BBX140

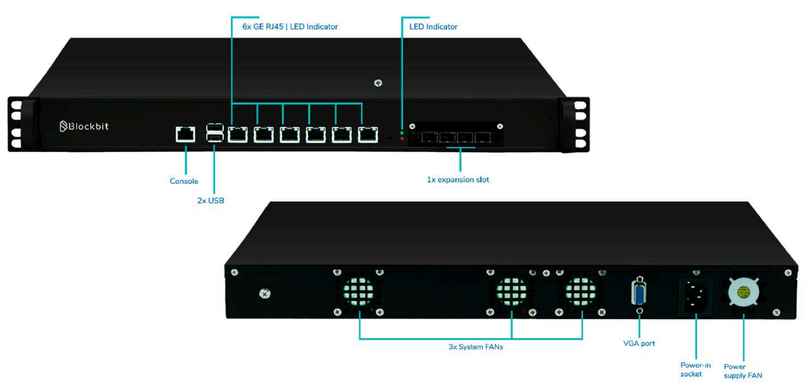




BBX140	
Tipo	Mesa
Firewall Throughput (UDP)	15 Gbps
Concurrent Connections	7.500.000
New Connections Per Second	60.000
NGFW Throughput (IMIX)	1.5 Gbps
SSL Inspection Throughput	1.2 Gbps
IPS Throughput	2.0 Gbps
Application Control Throughput *	2.0 Gbps
Threat Protection Throughput	1.0 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	3.0 Gbps
SSL VPN Throughput (AES-256)	1.7 Gbps
Interfaces UTP 2.5 GbE	6
Wi-Fi	*
LTE 3G/4G	Opcional
Disco SSD	120GB ou 240GB
Available Slots	*

Fotos meramente ilustrativas.

BBX200



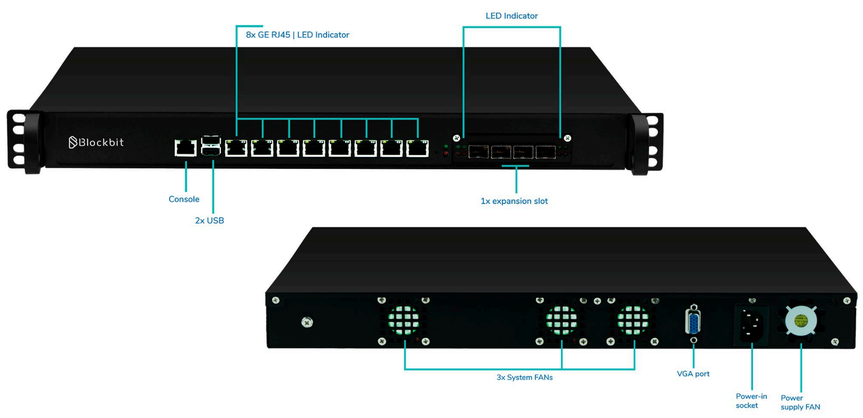
BBX200	
Tipo	1U - Rack 19”
Firewall Throughput (UDP)	20 Gbps
Concurrent Connections	8.200.000
New Connections Per Second	65.000
NGFW Throughput (IMIX)	2.5 Gbps
SSL Inspection Throughput	1.3 Gbps
IPS Throughput	3.0 Gbps
Application Control Throughput *	3.0 Gbps
Threat Protection Throughput	1.0 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	3.5 Gbps
SSL VPN Throughput (AES-256)	2.0 Gbps
Interfaces UTP 1 GbE	6
Interfaces SFP 1 GbE	4 (Opcional)
Interfaces SFP+ 10 GbE	4 (Opcional)
Disco SSD	120GB ou 240GB
Available Slots	1x

* O desempenho de Application Control utiliza a metodologia baseado em proxy (proxy based).

Appliances Blockbit

Especificações de Desempenho e Opcionais

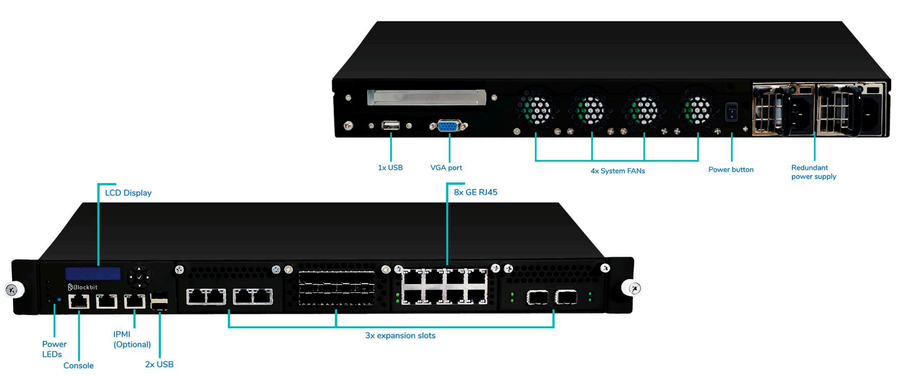
BBX700



BBX700	
Tipo	1U - Rack 19”
Firewall Throughput (UDP)	35 Gbps
Concurrent Connections	20.000.000
New Connections Per Second	120.000
NGFW Throughput (IMIX)	3.6 Gbps
SSL Inspection Throughput	2.2 Gbps
IPS Throughput	6 Gbps
Application Control Throughput *	6 Gbps
Threat Protection Throughput	1.5 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	5 Gbps
SSL VPN Throughput (AES-256)	2 Gbps
Interfaces UTP 1 GbE	8 a 16 (Opcional)
Interfaces SFP 1 GbE	4 (Opcional)
Interfaces SFP+ 10 GbE	4 (Opcional)
Fonte 110/240V - 50~60Hz	SIM
Disco SSD	240GB ou 480GB
Available Slots	1x

Fotos meramente ilustrativas.

BBX1500



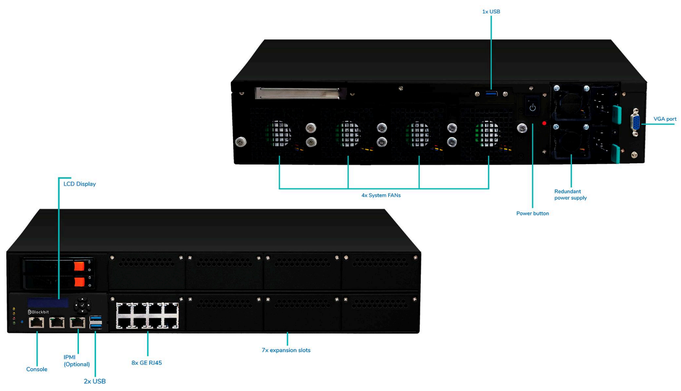
BBX1500	
Tipo	1U - Rack 19”
Firewall Throughput (UDP)	55 Gbps
Concurrent Connections	22.000.000
New Connections Per Second	200.000
NGFW Throughput (IMIX)	6.5 Gbps
SSL Inspection Throughput	4.5 Gbps
IPS Throughput	12 Gbps
Application Control Throughput *	10 Gbps
Threat Protection Throughput	4.5 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	10 Gbps
SSL VPN Throughput (AES-256)	5 Gbps
Interfaces UTP 1 GbE	8 a 20 (Opcional)
Interfaces SFP 1 GbE	8 (Opcional)
Interfaces SFP+ 10 GbE	8 (Opcional)
Interfaces 25 GbE	4 (Opcional)
Interfaces 40 GbE	4 (Opcional)
Fonte Redundante - Hot Swappable - 110/240V - 50~60Hz	SIM
Disco SSD	480GB ou 1TB
Available Slots	3x

* O desempenho de Application Control utiliza a metodologia baseado em proxy (proxy based).

Appliances Blockbit

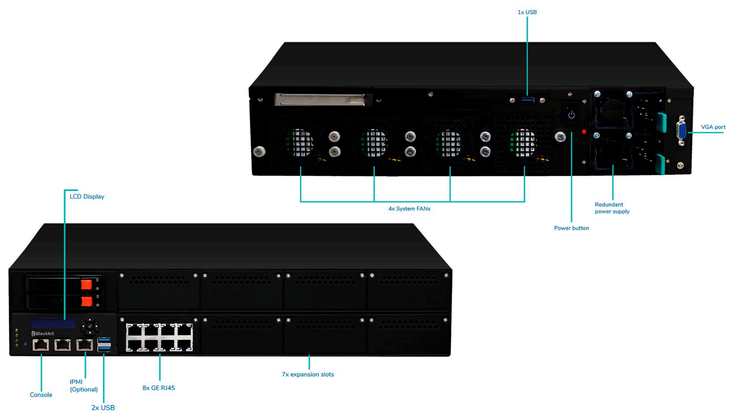
Especificações de Desempenho e Opcionais

BBX3000



BBX3000	
Tipo	2U - Rack 19”
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	30.000.000
New Connections Per Second	300.000
NGFW Throughput (IMIX)	13 Gbps
SSL Inspection Throughput	10 Gbps
IPS Throughput	15 Gbps
Application Control Throughput *	15 Gbps
Threat Protection Throughput	10 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	55 Gbps
SSL VPN Throughput (AES-256)	8 Gbps
Interfaces UTP 1 GbE	8 a 64 (Opcional)
Interfaces SFP 1 GbE	32 (Opcional)
Interfaces SFP+ 10 GbE	28 (Opcional)
Interfaces 25 GbE	8 (Opcional)
Interfaces 40 GbE	8 (Opcional)
Interfaces 100 GbE	14 (Opcional)
Fonte Redundante - Hot Swappable - 110/240V - 50~60Hz	SIM
Disco SSD	1 TB ou 2× 1TB em RAID 0, 1
Upgrade Disco	2TB
Available Slots	7x

BBX3600



BBX3600	
Tipo	2U - Rack 19”
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	45.000.000
New Connections Per Second	400.000
NGFW Throughput (IMIX)	20 Gbps
SSL Inspection Throughput	12 Gbps
IPS Throughput	18 Gbps
Application Control Throughput *	18 Gbps
Threat Protection Throughput	12 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	55 Gbps
SSL VPN Throughput (AES-256)	10 Gbps
Interfaces UTP 1 GbE	8 a 64 (Opcional)
Interfaces SFP 1 GbE	32 (Opcional)
Interfaces SFP+ 10 GbE	28 (Opcional)
Interfaces 25 GbE	8 (Opcional)
Interfaces 40 GbE	8 (Opcional)
Interfaces 100 GbE	14 (Opcional)
Fonte Redundante - Hot Swappable - 110/240V - 50~60Hz	SIM
Disco SSD	1 TB ou 2× 1TB em RAID 0, 1
Upgrade Disco	2TB
Available Slots	7x

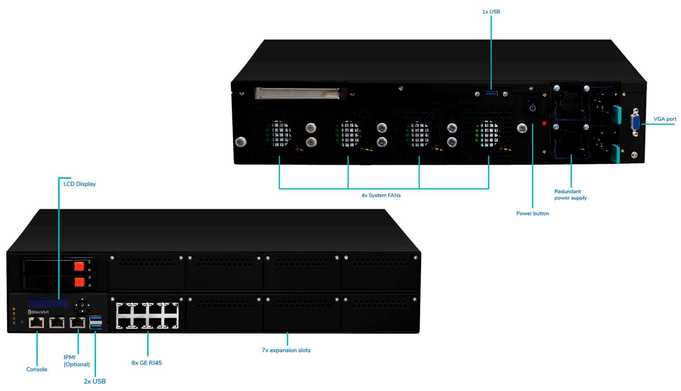
Fotos meramente ilustrativas.

* O desempenho de Application Control utiliza a metodologia baseado em proxy (proxy based).

Appliances Blockbit

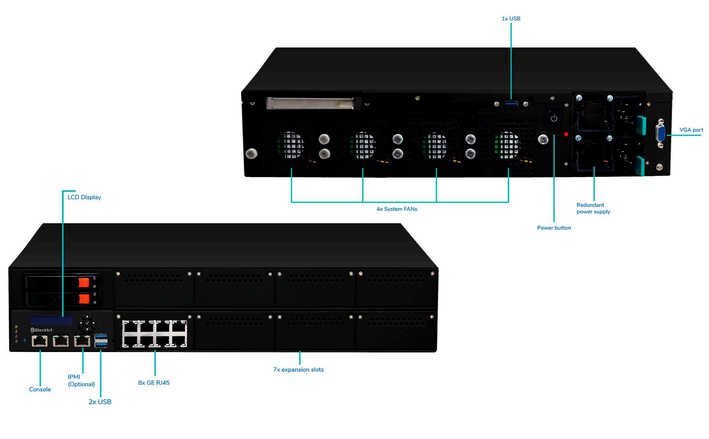
Especificações de Desempenho e Opcionais

BBX4200



BBX4200	
Tipo	2U - Rack 19”
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	55.000.000
New Connections Per Second	520.000
NGFW Throughput (IMIX)	26 Gbps
SSL Inspection Throughput	14 Gbps
IPS Throughput	23 Gbps
Application Control Throughput *	25 Gbps
Threat Protection Throughput	14 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	55 Gbps
SSL VPN Throughput (AES-256)	12 Gbps
Interfaces UTP 1 GbE	8 a 64 (Opcional)
Interfaces SFP 1 GbE	32 (Opcional)
Interfaces SFP+ 10 GbE	28 (Opcional)
Interfaces 25 GbE	8 (Opcional)
Interfaces 40 GbE	8 (Opcional)
Interfaces 100 GbE	14 (Opcional)
Fonte Redundante - Hot Swappable - 110/240V - 50~60Hz	SIM
Disco SSD	1 TB ou 2× 1TB em RAID 0, 1
Upgrade Disco	2TB
Available Slots	7x

BBX5000



BBX5000	
Tipo	2U - Rack 19”
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	70.000.000
New Connections Per Second	900.000
NGFW Throughput (IMIX)	40 Gbps
SSL Inspection Throughput	20 Gbps
IPS Throughput	32 Gbps
Application Control Throughput *	35 Gbps
Threat Protection Throughput	20 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	55 Gbps
SSL VPN Throughput (AES-256)	16 Gbps
Interfaces UTP 1 GbE	8 a 64 (Opcional)
Interfaces SFP 1 GbE	32 (Opcional)
Interfaces SFP+ 10 GbE	28 (Opcional)
Interfaces 25 GbE	8 (Opcional)
Interfaces 40 GbE	8 (Opcional)
Interfaces 100 GbE	14 (Opcional)
Fonte Redundante - Hot Swappable - 110/240V - 50~60Hz	SIM
Disco SSD	1 TB ou 2× 1TB em RAID 0, 1
Upgrade Disco	2TB
Available Slots	7x

Fotos meramente ilustrativas.

* O desempenho de Application Control utiliza a metodologia baseado em proxy (proxy based).

Descrição técnica

Opções de Implantação

Hardware Appliance	Virtual Appliance	Cloud Instance
• Desempenho máximo • Estabilidade garantida • Instalação rápida • Indicadores de LEDs para interface e fontes de alimentação	• Maior escalabilidade • Recuperação de desastres mais rápida • Otimização da infraestrutura	• AWS, Oracle, Azure, Google e IBM

Especificações dos modelos de Virtual Appliance

Descrição	Overall Throughput (UDP)	NGFW Throughput (IMIX)
BBX40	7 Gbps	200 Mbps
BBX80	10 Gbps	850 Mbps
BBX140	15 Gbps	1.5 Gbps
BBX200	20 Gbps	2.5 Gbps
BBX700	35 Gbps	3.6 Gbps
BBX1500	55 Gbps	6.5 Gbps
BBX3000	200 Gbps	13 Gbps
BBX3600	200 Gbps	20 Gbps
BBX4200	200 Gbps	26 Gbps
BBX5000	200 Gbps	40 Gbps

Fotos meramente ilustrativas.

Descrição técnica

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 estáticos e dinâmicos.
• Filtragem.
- Conteúdo web, Aplicações Web.
• Perfis de Inspeções: SSL, IPS, Threat Protection, Web Filter e Application Control (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.
- Habilitar 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 NGFW 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.
• Permite a monitoração do tráfego internet sem bloqueio de acesso aos usuários.

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 simultaneamente.
- NAT dinâmico (Many-to-Many e Many-to-1).
- NAT estático (1:1 e Many-to-Many) e bidirecional 1:1.
- NAT 444 (CGNAT).
• 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, através de verificação RPF (Reverse Path Forwarding).
- 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.
• Suporta distribuição GPO (SCCM) por AD Microsoft do cliente de VPN.
• Permite o controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br.
• Consulta o servidor RADIUS integrado (NAS), caso autorizado, é entregue o endereço IP.
• Permite limitar a quantidade máxima de pacotes por segundo no firewall, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede.
• Possui tecnologia de firewall do tipo Stateful.

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.
- Estatísticas em tempo real para classes de QoS na Interface de Gerência WEB.
- Suporta QoS para interfaces LAG.
- Suporta transmissão de pacotes sem modificação, com remarcação do valor DSCP e descarte de pacotes para tráfegos excedente da banda especificada.
- Permite modificação de valores DSCP.
- Permite limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo P2P.

Web Cache e Proxy

• Proxy Transparente ou Explícito (portas personalizadas).
- Supor te a serviços web (HTTP e HTTPS versões 1.0, 1.1, 2.0 , FTP, POP3 e SMTP).
• Configuração de tamanho de Cache em Disco e Memória.
• Configuração de web cache em memória e disco.
• Habilitação de web cache de conteúdos dinâmicos (Facebook, Google Maps, MSN Video, Source forge 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.
• Possibilita a integração com servidores de cache web externos
• Possui a capacidade de excluir URLs específicas do cache web, configurável por lista de palavras chaves com suporte inclusive a expressões regulares.
• Permite configurar a porta do Proxy Explícito.

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 na interface web.
• 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 malformados.
• Reconhecimento de padrões, análise de protocolos e anomalias e bloqueio de 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.
• Log de registro das incidências para cada tipo de ataque identificado.
• Tráfego mal formado e cabeçalhos inválidos.
• Atualização automática e periódica.
• 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) e espelhamento de porta.
• 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.
• Permite analisar e gerar logs, bloqueia e envia para quarentena o IP do atacante por um período de tempo.
• Permite 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.
• Funcionalidade de detecção de intrusão baseada em appliance.
• Permite que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permite capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.
• Possui alarmes na console de administração.
• Capacidade de resposta/logs ativa a ataques.

Threat Protection

• Antivírus e Anti-Malware com análise em tempo real.
- HTTP, HTTPS, FTP, SMB, CIFS, POP3 e SMTP (nativo na solução).
• Proteção contra aplicações não autorizadas.
• 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.
• Bloqueia arquivos pela extensão e também indentifica pelo tipo MIME (mesmo mudando a extensão).
• Inspeção, detecção e prevenção baseado em fluxo.
• Ações específicas para códigos maliciosos distintos.

Descrição técnica

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, suporta 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 configuração 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 personalizável 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.
• LTE (3G/4G) utilização como link load balance e failover.
• Permite utilizar VPN IPsec para interligar unidades remotas.

Zero-touch Provisioning

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

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 (HTTP, HTTPS, FTP e TELNET) /UDP/ICMP.
• Suporte TACACS+ e LDAP para usuários de administração e usuários de Firewall.
• 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 permite o uso de SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo Firewall.
• Suporta autenticação para Firewall e VPN: Tokens, TACACS, RADIUS LDAP/AD e certificados digitais.
• Controle de acesso criptografado em pacotes para servidores de autenticação.

Secure Web Gateway

• As funcionalidades abaixo são baseadas em appliance.
• 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 inválido.
- 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, Google App, LinkedIn, Meetup, Skype, Tinder, Tuenti, Twitter, WhatsApp, WeChat e ZohoChat e Aplicações de Bate-papo.
• Bloqueio de arquivos tipo Office, Java e Javascript, Cookies, ActiveX, Multimídias, Imagens.
• Reconhecimento de Aplicação – DPI (Deep Packet Inspection).
• Identifica Aplicações através do protocolo SSL, HTTP, HTTPS ou portas de acesso não padrão.
• Controle por SNI baseado em 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.
• 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 em modo transparente.
• Reconhecimento de aplicações independentemente de porta e protocolo.
• Identifica o uso de táticas evasivas para controlar aplicações que tentam usar conexão criptografadas (Skype/rede TOR).
• Mensagem de bloqueio customizável.
• Reconhecimento de mais de 4000 aplicações.
• Possui mais de 19 categorias para classificação de aplicações.
• Permite a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
• As atualizações regulares do produto são realizadas sem interromper a execução dos serviços de controle de aplicações e serviços de filtragem de conteúdo web.
• Possui DNS Content Filter.
• Suporte a técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, Whatsapp, WeChat, Snapchat BitTorrent, UTorrent, Vuze, eDonkey, GNUTella, Skype e Microsoft Teams.

Redes e Interfaces

• Interfaces.
- Ethernet (com suporte a FEC - Forward Error Correction).
- VLAN (IEEE 802.1q) até 4094 ID por interface.
- VLAN Trunking com suporte de VLANs por tronco.
- Suporte WAN: ADSL/DSL, MPLS, LTE (3G/4G/5G).
- Alias (Virtual IP).
• Link aggregation.
- Ethernet bonding (802.3ad) LACP.
• Roteamento dinâmico: BGP4/BGP4+, OSPFv2/v3, RIPv1/v2 e PIM-SM/PIM-DM.
- Suporte a autenticação MD5 entre os peers OSPF.
- Suporte a múltiplos processos de roteamento OSPF independentes e simultâneos.
- Suporte BFD (Bidirectional Forwarding Detection) para BGP.
• 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.

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 e Trafic Monitor) com informações de throughput e conexões simultâneas.
• Logs de Eventos de Segurança e Ameaças.
• Permite captura de tráfego e download em formato PCAP.
- Registro de usuários nos eventos de autenticação, acesso, bloqueio e ameaças.

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 SSHv2, utilizando chaves criptográficas no mínimo de 16bits.
- Suporte acesso à console web por HTTP e CLI por TELNET.
- Permite alterar a porta padrão para os acessos a interface de administração via HTTP, HTTPS e CLI.

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 de identificar na rede de dados arquivos compactados e aplicar políticas de uso sobre o conteúdo desses tipos de arquivo.
- Suporta recurso Antispam DLP (Data Loss Prevention).

Descrição técnica

VPN IPSEC e VPN SSL

- VPN Tunnel (LAN to LAN) / VPN Site-to-Site e Cliente-to-Site.
- VPN RAS/SSL (remote access) permite acesso por cliente de VPN ou suporte direto na estação sem cliente - Interface Web, ssl, popa, e/ou interface de web sem agente.
- VPN SSL Portal via HTTPS para acessos RDP, VNC, SSH, WEB e SMB (sem necessidade de utilização de JAVA).
- Cliente VPN compatível com Win7, 8,8.1, 10 e 11 (32 e 64 bits), Linux e MacOS, Android e IOS.
- Autenticação.
- Permite habilitar, desabilitar, reiniciar e atualizar IKE, Gateways e túneis de VPN IPsec a partir da interface gráfica.
- Chave PSK (Pre-Shared Key) - XAuth (AD, LDAP local, RADIUS), certificado digital IKE P1, EAP (MSCHAPv2).
- Permite estabelecer o túnel antes ou após o usuário autenticar na estação do teclado do usuário.
- Autenticação nativa de VPN IPsec utilizando MD5, SHA-1, SHA-256, SHA-384, SHA-512 e AES-XCBC.
- Alta disponibilidade.
- FQDN Full (Quality Domain Name) e Suporte DDNS.
- NAT-T (encapsulamento UDP e I/D (Dead Peer Detection).
- Exchange mode IKEv1: Main mode ou Aggressive Mode.
- Suporte a dados compactados.
- Protocolos:
  - IKEv1 e IKEv2 (na fase 1 e fase 2) e ESP.
  - Criptografia Simétrica: AES128, 192 e 256, 3DES.
  - Criptografia Assimétrica: DH - Diffie-Hellman (Group1, Group2, Group5, Group14, Group15, Group16, Group17, Group18, Group19, Group20, Group21, Group22, Group23, Group24, Group25, Group26, Group27, Group28, Group29, Group30, Group31 e Group 32).
  - RSA key generation.
- Suporte Auto-Discovery VPN (AD-VPN), permite múltiplos dispositivos (Spokes) com gateway centralizador (hub) e Site-to-Site, Suporte túneis do tipo (Site-to-Site, Full Mesh, Star).
- Suporta os algoritmos RSA e Diffie-Hellman.
- VPN SSL com suporte a certificado digital X509 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 a verificação de certificado revocation list (CRL).
- Suporte a múltiplos hubs em topologias hub-spoke.
- Suporta o isolamento de tráfego baseado em serviços e destinos (IoT, Rede Bancária, Rede Visitante).
- Funcionalidade VPN baseada em appliance.
- Suporte aos algoritmos de criptografia: 3DES, AES128, AES256, AES GCM-128.
- Possui funcionalidades de Auto-Discovery VPN (AD-VPN) capaz de permitir criar túneis dinâmicos para múltiplos dispositivos (spokes) com um gateway centralizador (hub).
- A funcionalidade de AD-VPN suporta os seguintes tipos de túneis: Full-Mesh, Site-to-Site e Star.
- Suporte a configuração via Virtual interface na configuração de túneis VPN site-to-site com SD-WAN Protection.
- A VPN client-to-site suporta o estabelecimento automático da VPN nos protocolos ICMP ou DNS (53/UDP), caso o cliente remoto identifique que a porta padrão está sendo bloqueada.
- Possui recurso para configurar vários túneis simultâneos na VPN cliente-to-site, com otimização para o desempenho do tráfego.
- 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 certicados SSL (X.509).
- 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.
- Permite utilizar VPN IPSec para interligar unidades remotas.

Log e Relatórios

- Suporte Netflow / IPFIX.
- Relatórios de Log de Sessão, Autenticação e VPN, por dispositivo único ou consolidado.
- 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 de origem do ataque.
- Eventos registram alterações no estado e a saúde dos links do SD-WAN.
- Relatórios com histórico com monitoramento da saúde do link.
- Geração de relatórios históricos por período.
- Possui logs e relatórios de tempo de navegação de sites web.

H.A. (Alta Disponibilidade)

- Espelhamento de sessões de firewall, autenticação de usuário e sincroniza todas configurações, seções, certificados para inspeção 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.
- Monitoramento de interfaces, em caso de falha do link.
- Sistema de Cluster High Availability (Ativo-Passivo/Ativo-Ativo, somente com equipamentos iguais) com manutenção das sessões estabelecidas, distribuição de tráfego, manutenção da tabela de estado, balanceamento de sessão em múltiplas zonas de disponibilidade.
- O sincronismo dos servidores é realizado por interface exclusiva de Heartbeat.
- Em caso de falha do equipamento ativo primário, o equipamento secundário assume de forma transparente, sem impacto ao usuário ou perda de serviço.
- Suporta a persistências de sessão de usuários e conexões estabelecidas, entre os membros da Alta Disponibilidade.

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 com configuração de número de cópias.
• Agendamento de Backup do tipo Snapshot ou de Sistema, através da interface gráfica.

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.
- 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 (Blacklist), impedindo que esses endereços sejam acessados pelos usuários de rede novamente.
- O módulo de APT suporta analisar o arquivo pelo antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back e analisa 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, máquina/computador, permitindo granularidade de controle e 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 client 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.
• Permite a criação de grupos de administração com diferentes perfis de acesso.
- Perfil Monitor: Somente leitura.
- Perfil Operador: Leitura/Escrita, sem permissão de desativação de interfaces.
- Perfil Administrador: Leitura/Escrita/Alteração.
• Suporta múltiplos Servidores de Autenticação (MS AD e/ou LDAP) atuando no modo failover.

GSM - Gerenciamento Centralizado

- Reboot ou desligamento (NGFW/SD-WAN) via gerenciamento centralizado.
- Suporta automações para atividades de gestão, por exemplo, sincronismo de regras, gestão e orquestração centralizada.
- Atualização centralizada e rollback.
- Suporte a alertas via gerenciamento centralizado.
- Centralização de logs através do gerenciamento centralizado.
- Suporte a grupos para servidores de autenticação.
- Suporte a autenticação através de certificados X509v3.
- Suporte a certificados revogados (LCR).

Descrição técnica

Outros Recursos

- Proxy Services (SSH, SMB/CIFS, HTTP, FTP, SMTP, POP3).
- Suporta Voip (SIP/H.323) e RTP sobre IPv4/IPv6.
- Suporte a múltiplos domínios de Autenticação.
- Suporta fail-closed e opcional de interface fail-open (by-pass).
- Atualização Transparente, de forma 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.
- Possui Fluxo de pacotes nos modos de Encaminhamento e Controle.
- 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).
- 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 IDS/IPS.
- Permite solicitações de inclusão de aplicações na base padrão.
- É possível diferenciar diferentes tráfegos P2P para diversos softwares (Bittorrent, emule e outros) com granularidade no controle dos aplicativos.
- Suporta granularidade nas políticas de IPS, Antivírus, AntiSpam 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.
- 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 para usuários, grupos de usuário, origem, destino, zonas de segurança.
- Suporta Sistema Virtuais (VDOM) em todos os modelos.
- Sistema VDOM permite criar contextos virtuais com suporte a criação de diversos administradores.
- Suporta TLS 1.2 e TLS 1.3.
- Suporta criar políticas de bloqueio ou liberar por geolocalização e informam nos logs o país de origem e/ou destino com a bandeira para facilitar a identificação do tráfego.
- Suporte a categorização dinâmica de sites.
- Reclassificação de sites via portal do fabricante.
- Suporte a múltiplos acessos simultâneos.
- Validação das políticas de segurança para identificar regras duplicadas ou que se ofusquem.
- Relatórios estatísticos de conexões simultâneas.
- Relatórios de utilização de VPN.
- Relatórios estatísticos de tráfego (Input e Output).
- Suporta notificação de vencimento da licença na janela de alertas com os dias restantes para a data de vencimento.
- Restore de Snapshot sem executar o Wizard e sem licenciamento.
- Qualquer interface de rede do equipamento pode ser utilizada como gerenciamento, ou seja, não existe interface exclusiva para função de gerenciamento.
- Permite o acesso à interface de gerenciamento web por qualquer interface de rede configurada.
- Permite o agendamento de serviços.
- Possibilita a configuração dos timeouts de resposta dos protocolos de conexão, e suporta a definição das opções do timeout padrão do ICMP, estabelecimento do TCP envio do SYN em sessões TCP.
- Possui uma única janela de configuração de política de segurança onde seja possível inserir os perfis de Proxy WEB, IPS, APP control, SD-WAN e ATP.
- Permite implementar filtros de IPS, WEB Filter, Threat Protection, SSL Inspection, Application Control, assim como roteamento de aplicativos por SD-WAN e limitação da taxa de DoS por pacotes em uma única política.
- Exibe na própria política a visualização de quais módulos estão habilitados, sem que seja necessário a edição da regra de proteção.
- Possibilita a edição de objetos vinculados, sem a necessidade de recriar a política.
- Possibilita a duplicação de uma política, otimizando tempo de configuração.
- Permite acesso a interface de gerenciamento CLI fisicamente no equipamento.
- A interface USB suporta o uso de modem 3G/4G/LTE para conexão de link de internet.
- Suporta Medidor Educação Conectada (SIMET/nic.br).

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.
- RFC 5925: BGP Session protection via TCP MD5.
- RFC 4760: Multi-Protocol Extensions para BGP-4.

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: Route 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.
- RFC 2460: Internet Protocol, Version 6 (IPv6) - Specification.
- RFC 2461: Neighbor Discovery for IP Version 6 (IPv6).
- RFC 2462: IPv6 Stateless Address Auto-Configuration.
- RFC 4884: Internet Control Message Protocol (ICMPv6) for IPv6.
- RFC 4291: IP Version 6 Addressing Architecture.

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.

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 5246: TLS Transport Mapping for Syslog.
- RFC 5245: 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.

SNMP

- RFC 4293: Management Information Base for the IP.
- RFC 4273: Definitions of Managed Objects for BGP-4.
- RFC 4113: Management Information Base for 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 Information 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.

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.

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).

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.

RIP

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

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.

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 1280k*, IPS/ATP THROUGHPUT COM ASSINATURAS PADRÃO DE FÁBRICA HABILITADAS, NGFW É MEDIDO COM FIREWALL, THREAT PROTECTION, IPS E CONTROLE DE APLICATIVO HABILITADOS, TRÁFEGO IMIX.

Algumas RFC’s suportadas pelo Blockbit Platform

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.

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.

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 IKEv2.
- RFC 6954: Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for IKEv2.
- RFC 6290: A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE).
- RFC 6032: A Childless Initiation in 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 4756: IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA).
- RFC 4355: IANA SHA1/SHA256 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 3667: 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 2409: The IKE CBC-Mode Cipher Algorithms.
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec.
- RFC 2408: The Internet Key Exchange Algorithm With PKE.
- RFC 2406: IPsec-AH and ESP.
- RFC 2104: 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.

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 3442: The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4.
- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6).
- RFC 2132: DHCP Options and BOOTP Vendor Extensions.
- RFC 2131: Dynamic Host Configuration Protocol.

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.

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 1280k*, IPS/ATP THROUGHPUT COM ASSINATURAS PADRÃO DE FÁBRICA HABILITADAS, NGFW É MEDIDO COM FIREWALL, THREAT PROTECTION, IPS E CONTROLE DE APLICATIVO HABILITADOS, TRÁFEGO IMIX.