blockbit platform

Integrated cybersecurity, converging connectivity and security.

- Secure SD-WAN
- Next-Generation Firewall

It's easy to be secure

www.blockbit.com/en/

Datasheet *DEC23*

Version 2309-v10.01

About Blockbit

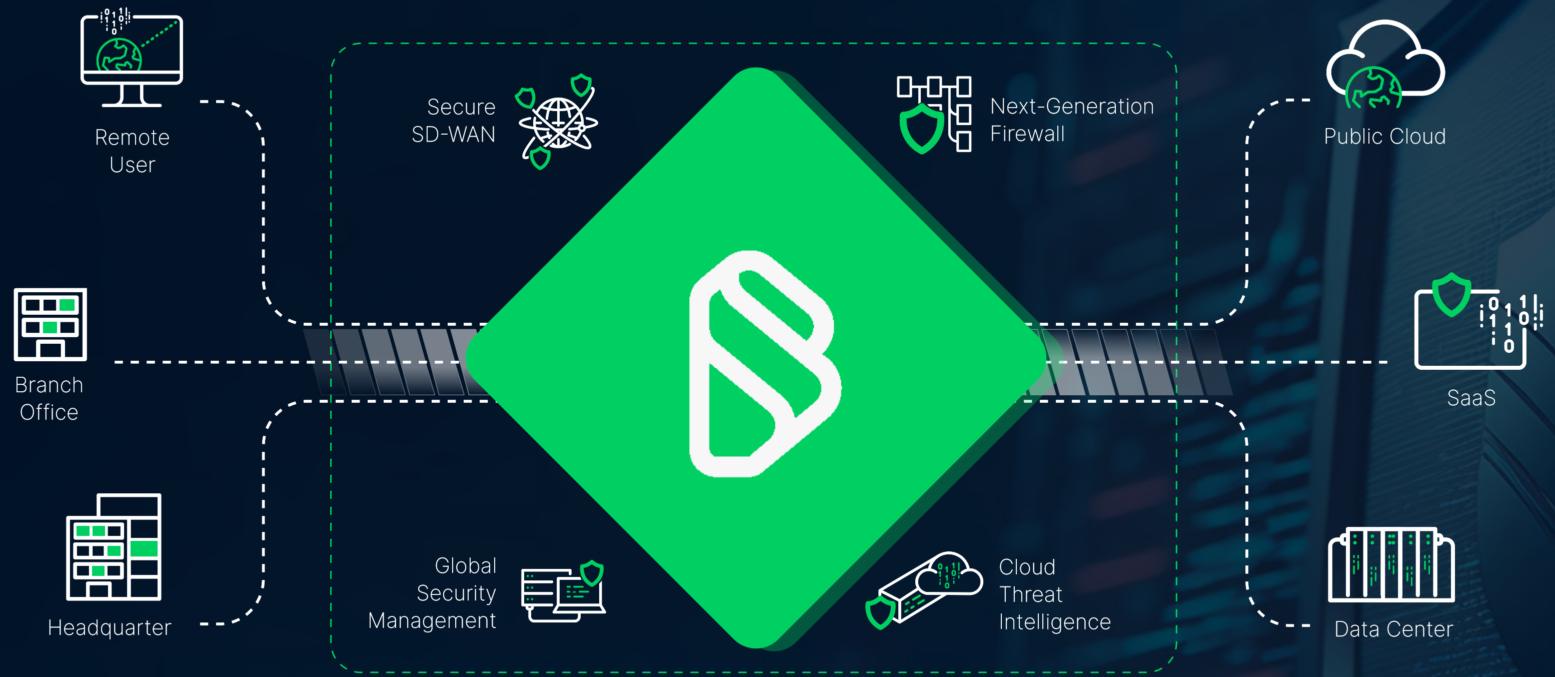
Blockbit is the Brazilian leader in cybersecurity products, protecting thousands of companies and millions of users from attacks and digital threats. With state-of-the-art technologies and an advanced intelligence laboratory, Blockbit develops proprietary solutions for network protection and secure connectivity with high quality and performance, always in line with the main global cybersecurity trends.

What is Blockbit Platform?

The Blockbit Platform is perfectly aligned with the global trend of convergence of connectivity and security, providing solid network protection and secure end-to-end connectivity.

Our platform consists of **Blockbit Secure SD-WAN** and **Blockbit NGFW** (Next-Generation Firewall), both complemented by **Blockbit GSM** (Global Security Management) for centralized and simplified management of multiple devices. In addition, **Blockbit Cloud Threat Intelligence** constantly provides advanced intelligence to products.

The Blockbit Platform unites in a single solution the innovative products essential to accelerate your business safely, ensuring the desired quality and performance.



Deployment options

Hardware Appliance
VM
Virtual Appliance
Cloud Instance
Cloud Services
Software Agent

With Blockbit, it's easy to be secure

The Blockbit Platform offers an advanced and robust solution with innovative features that reduce your uptime, such as automated setup, centralized management, and intuitive processes. With this, you have more time to focus on what really matters: **your business**. Whether it's enhancing security, optimizing performance, or saving time, Blockbit is here to simplify the path towards a more secure and efficient digital environment.

Simplify your network by unifying connectivity and security

Our platform drastically simplifies the complexity of networks, seamlessly integrating connectivity and security, being able to detect encapsulated applications and validate that the traffic matches the protocol specification.

With Blockbit, you can reduce the overhead of operation and administration, while ensuring a consistent and robust security posture across your entire infrastructure.

Automatically set up your devices

With auto-configuration capabilities, device deployment becomes more efficient than ever. No need to waste time installing our devices, Blockbit has taken care of it for you. Centralize configurations and automatically distribute them to remote assets.

With the ZTP (Zero-Touch Provisioning) feature, it is possible to reduce time and cost with implementation.

Manage all Blockbit devices from one place

Blockbit makes it possible for you to manage all your security devices and events from a single, centralized location. This eliminates the complexity of dealing with multiple interfaces and streamlines workflow, saving time, allowing for quick actions and informed decisions.

Reduce time with a user-friendly and intuitive interface

The Blockbit Platform is designed with a user-friendly and intuitive user interface, significantly reducing the time required for the management and configuration of security devices.

SSO puts control in your hands, without the need for an extensive learning curve and allowing you to perform your duties faster.

Get more quality and performance, at an affordable price

By combining cutting-edge technology with performance optimization approaches, Blockbit ensures that your cybersecurity doesn't compromise the speed and efficiency of your network.

All of this is offered at an affordable price, ensuring that quality is within the reach of all businesses.

Secure SD-WAN

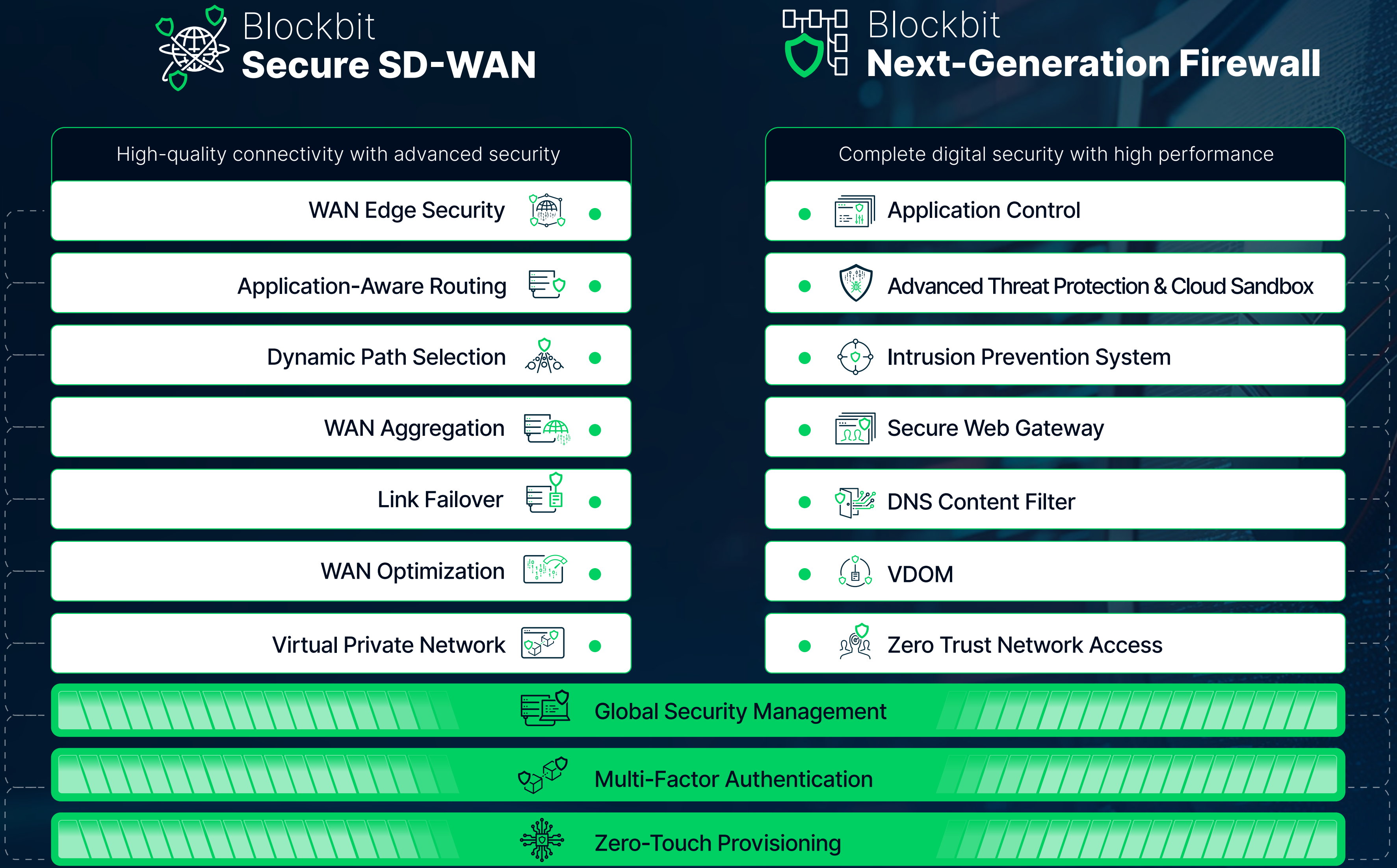
Blockbit Secure SD-WAN is a powerful combination of SD-WAN with all of Blockbit's advanced cybersecurity features. This solves your main challenges, both in terms of connectivity and security. Now you can increase the quality of service of your connections, adopt cheaper link solutions, and protect your environment, while reducing your acquisition cost and operational cost by having a single solution, while minimizing continuity risks and conflicts by having a single point of control.

Monitoring of multiple links for long distance connection, supporting connections such as: **ADSL/DSL, Cable Modem with Ethernet or fiber, LT/3G/4G/5G, MPLS, radio link, satellite link, among others.**

Next-Generation Firewall

Blockbit NGFW (Next-Generation Firewall) is the evolution of conventional firewalls and offers advanced features for attack and threat protection, and goes beyond protecting the network to protect applications and users as well. With this solution you will be able to analyze application traffic in real time, allowing more granular and efficient security policies, and can be implemented as a gateway (L2) or inline (L3), optimized for application content analysis at layer 7, providing greater control and visibility over your environment and business.

With **Blockbit NGFW**, you have at your disposal the most advanced tool to address digital security challenges and protect your data, users, and systems from threats and attacks.



Blockbit
Secure SD-WAN

High-quality connectivity with advanced security

- WAN Edge Security
- Application-Aware Routing
- Dynamic Path Selection
- WAN Aggregation
- Link Failover
- WAN Optimization
- Virtual Private Network

Blockbit
Next-Generation Firewall

Complete digital security with high performance

- Application Control
- Advanced Threat Protection & Cloud Sandbox
- Intrusion Prevention System
- Secure Web Gateway
- DNS Content Filter
- VDOM
- Zero Trust Network Access

- Global Security Management
- Multi-Factor Authentication
- Zero-Touch Provisioning

Blockbit
Secure SD-WAN

Guarantee the quality of service of connections and applications, securely advanced

Blockbit Secure SD-WAN is a complete, state-of-the-art solution for the control, advanced security and centralized management of all WAN connections. With a modern and scalable architecture, made up of innovative features, you will be able to simplify and improve your organization's network, providing greater efficiency and reliability. This gives you the flexibility to choose the best connectivity options for your company, allowing you to reduce your infrastructure costs.

With Blockbit, integration and management of multiple network connections becomes a reality, regardless of vendor, technology or connection type. For example, using features like **WAN Aggregation and Link Failover**, you can aggregate links from multiple providers and establish a contingency plan for situations where one of them fails. This functionality ensures greater redundancy and availability for your network, preventing unwanted interruptions.

Discover the main modules of Blockbit Secure SD-WAN:

Application-Aware Routing (AAR)

Prioritizes and optimizes critical application traffic to ensure performance and increase the resiliency of your business.

Dynamic Path Selection (DPS)

Allows you to automatically define the best route for application traffic, based on quality of service requirements, business policy, and network conditions.

WAN Optimization

Accelerates application delivery by reducing latency time, as well as improving bandwidth efficiency and reducing the size of transmitted packets.

WAN Aggregation

Combines multiple connections into a single logical route, increasing the bandwidth, availability, reliability, quality, and performance of your connection.

Link Failover

Provides network resiliency in the event of a failure of one or more connections by detecting connection failure and automatically redirecting traffic to a secondary connection.

Virtual Private Network (VPN)

It allows secure and private communication between branches and employees, making it possible to remotely access information, systems and internal resources.

WAN Edge Security

Integrates all advanced security features into a single solution, adding ATP, IPS, and SWG modules, protecting your network, connection from external and internal attacks and threats.

Global Security Management (GSM)

Define configuration templates for centralized management (Manager) of multiple security devices and consolidate traffic logs and events (Analyzer).

Zero-Touch Provisioning (ZTP)

Simplifies the deployment of Blockbit Secure SD-WAN by enabling remote configuration and automated installation of devices.

Multi-Factor Authentication (MFA)

It offers a second factor of authentication to validate the authentications of its users, ensuring greater security for access to Blockbit's resources.

Blockbit
Next-Generation Firewall

Protect your business with the best Next-Generation Firewall

Protect your business with the best Next-Generation Firewall

Blockbit NGFW is a state-of-the-art, high-performance enterprise firewall that incorporates advanced controls and protections for users, applications, and the network into a single solution.

The solution incorporates detailed packet inspection **(DPI)**, application control, advanced threat protection **(ATP)**, intrusion prevention system **(IPS)**, web content filtering **(SWG)**, secure remote connection **(VPN)**, centralized event management and consolidation **(GSM)**, and more. Thanks to the encrypted traffic inspection feature, which today accounts for the vast majority of traffic, The solution allows the control and blocking of threats and attacks that use encryption to hide themselves.

Discover the main modules of Blockbit NGFW:

Deep Packet Inspection (DPI)

It offers deep inspection capabilities for open and encrypted packets and traffic, allowing you to identify and block malicious activity, specific applications, network protocols, data types, and even hidden threats.

Advanced Threat and Malware Protection (ATP)

Detects and blocks cyber threats using advanced Inline Sandbox capabilities, using artificial intelligence and machine learning, to protect the environment from advanced threats and malware, including ransomware.

Intrusion Prevention System (IPS)

It creates incident log logs and increases your visibility, identifies and actively blocks malicious traffic that tries to exploit vulnerabilities in applications and services on your network.

DNS Content Filter

It enables the definition of internet access policies in a more granular and specific way, ensuring greater security and control over browsing.

Zero Trust Network Access (ZTNA)

Integrated with the VPN module, it provides granular access based on multiple security factors and only to the specific features needed by users.

Zero-Touch Provisioning (ZTP)

The ZTP feature simplifies the deployment of Blockbit NGFW by enabling remote configuration and automated installation of devices.

Application Control

It allows you to control and manage the use of applications and services by automatically identifying thousands of applications, controlling usage and prioritizing bandwidth, and generating analytical information about application usage.

Cloud Sandbox

Integrated with the ATP module and provides an additional layer for advanced protection against unknown threats by emulating and executing suspicious files in Blockbit's proprietary cloud.

Secure Web Gateway (SWG)

Manage your users' access to web resources, preventing risky or unproductive behavior within your company or remotely.

Virtual Domains (VDOM)

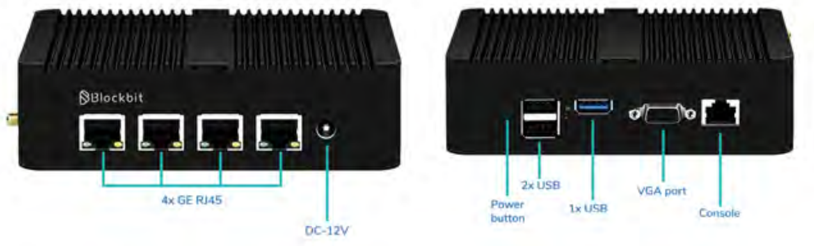
It allows you to segment Blockbit into multiple virtual domains, with independent administration, for control and protection of multiple networks with a single device.

Global Security Management (GSM)

Defines configuration templates for centralized management (Manager) of multiple security devices and consolidates traffic logs and events (Analyzer).

Multi-Factor Authentication (MFA)

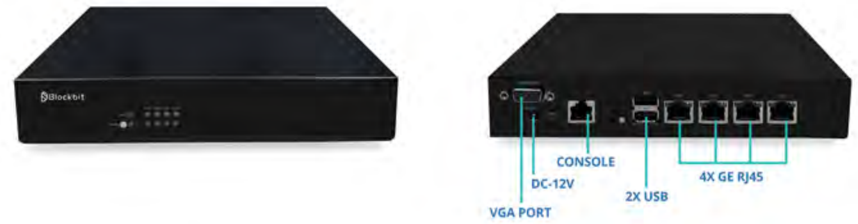
It offers a second factor of authentication to validate the authentications of its users, ensuring greater security for access to Blockbit's resources.



BBX40

Performance Specifications and Options

	BBX40
Type	Desk
Firewall Throughput (UDP)	6 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)	280 Mbps
SSL VPN Throughput (AES-256)	140 Mbps
Interfaces UTP 2.5 GbE	4
LTE 3G/4G	OPTIONAL
Disk	64GB
Solid State Drive	120GB/240GB
Available Slots	*

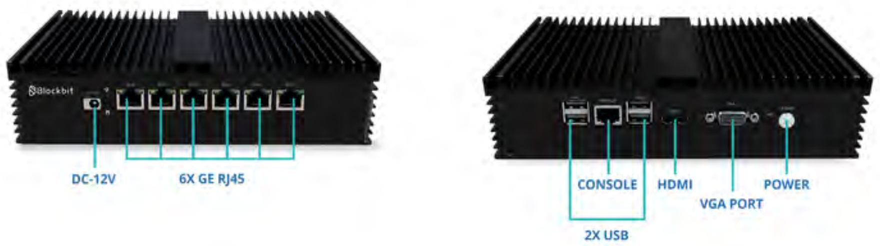


BBX80

Performance Specifications and Options

	BBX80
Type	Desk
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	670 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	2.0 Gbps
SSL VPN Throughput (AES-256)	1.2 Gbps
Interfaces UTP 2.5 GbE	4
WIFI	OPTIONAL
LTE 3G/4G	OPTIONAL
Disk	64GB
Solid State Drive	120GB/240GB
Available Slots	*

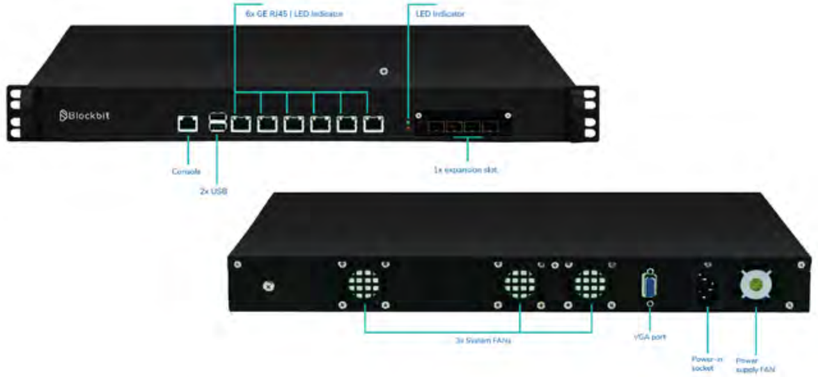
Photos for illustrative purposes only.



BBX100

Performance Specifications and Options

	BBX100
Type	Desk
Firewall Throughput (UDP)	12 Gbps
Concurrent Connections	7,000,000
New Connections Per Second	52,000
NGFW Throughput (IMIX)	1.0 Gbps
SSL Inspection Throughput	900 Mbps
IPS Throughput	1.5 Gbps
Application Control Throughput	1.6 Gbps
Threat Protection Throughput	750 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	2.5 Gbps
SSL VPN Throughput (AES-256)	1.5 Gbps
Interfaces UTP 1 GbE	6
WIFI	OPTIONAL
LTE 3G/4G	OPTIONAL
Disk	120GB
Solid State Drive	240GB
Available Slots	*

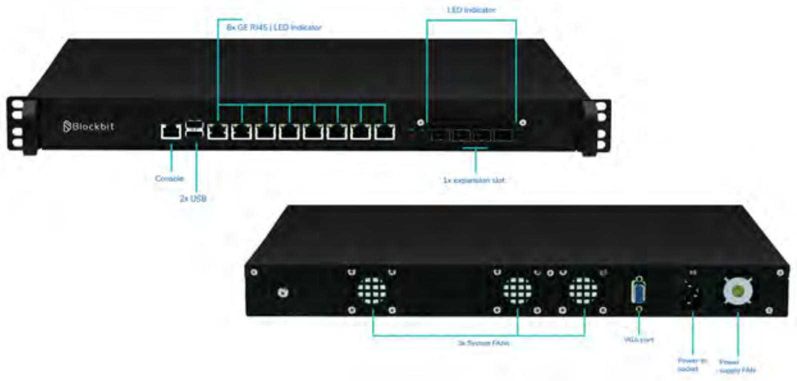


Photos for illustrative purposes only.

BBX200

Performance Specifications and Options

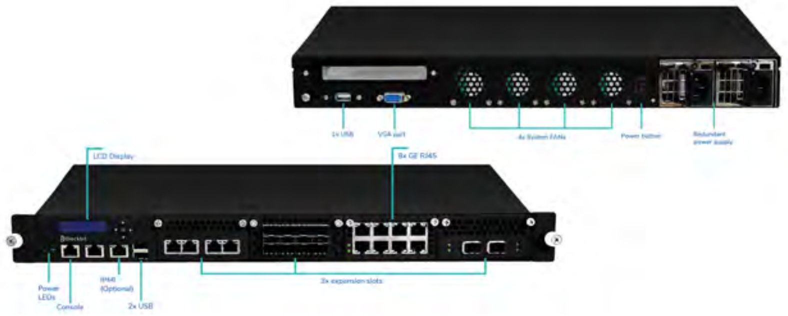
	BBX200
Type	1U
Firewall Throughput (UDP)	20 Gbps
Concurrent Connections	8,200,000
New Connections Per Second	65,000
NGFW Throughput (IMIX)	2.5 Gbps
SSL Inspection Throughput	1.3 Gbps
IPS Throughput	3.0 Gbps
Application Control Throughput	2.5 Gbps
Threat Protection Throughput	1.0 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	3.0 Gbps
SSL VPN Throughput (AES-256)	1.8 Gbps
Interfaces UTP 1 GbE	6
Interfaces SFP 1 GbE	4 (OPTIONAL)
Interfaces SFP+ 10 GbE	4 (OPTIONAL)
Disk	120GB
Solid State Drive	240GB
Available Slots	1x



BBX700

Performance Specifications and Options

	BBX700
Type	1U
Firewall Throughput (UDP)	35 Gbps
Concurrent Connections	18,000,000
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 to 16 (OPTIONAL)
Interfaces SFP 1 GbE	4 (OPTIONAL)
Interfaces SFP+ 10 GbE	4 (OPTIONAL)
Hot Swappable	OPTIONAL
Disk	240GB
Solid State Drive	480GB
Available Slots	1x

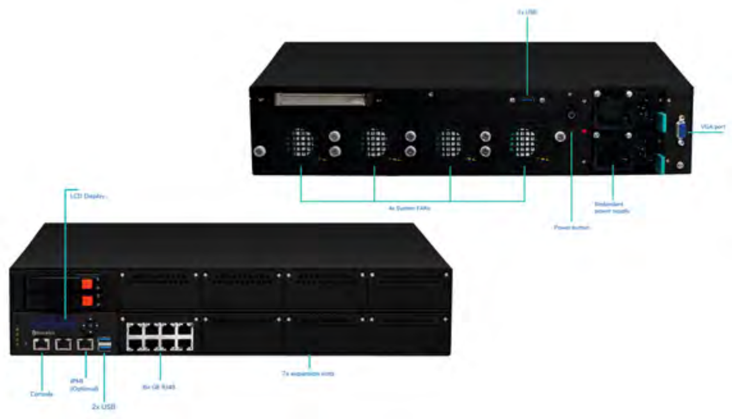


BBX1500

Performance Specifications and Options

	BBX1500
Type	1U
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 to 20 (OPTIONAL)
Interfaces SFP 1 GbE	8 (OPTIONAL)
Interfaces SFP+ 10 GbE	8 (OPTIONAL)
Interfaces 25 GbE	4 (OPTIONAL)
Interfaces 40 GbE	4 (OPTIONAL)
Hot Swappable	YES
Disk	480GB
Solid State Drive	1TB
Available Slots	3x

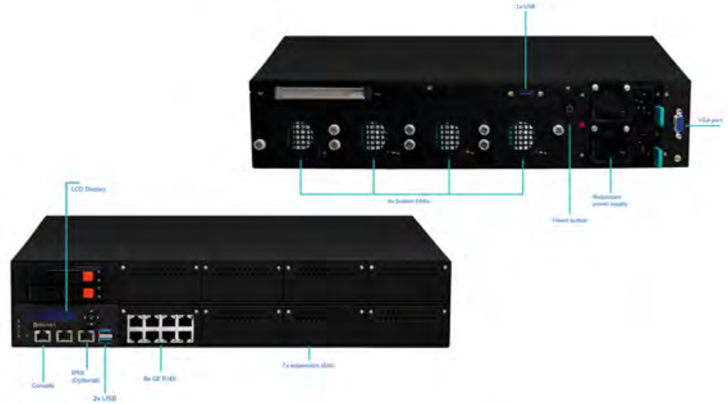
Photos for illustrative purposes only.



BBX3000

Performance Specifications and Options

	BBX3000
Type	2U
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	30,000,000
New Connections Per Second	300,000
NGFW Throughput (IMIX)	13.0 Gbps
SSL Inspection Throughput	8 Gbps
IPS Throughput	15 Gbps
Application Control Throughput	15 Gbps
Threat Protection Throughput	8 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	15 Gbps
SSL VPN Throughput (AES-256)	7 Gbps
Interfaces UTP 1 GbE	8 to 64 (OPTIONAL)
Interfaces SFP 1 GbE	32 (OPTIONAL)
Interfaces SFP+ 10 GbE	28 (OPTIONAL)
Interfaces 25 GbE	8 (OPTIONAL)
Interfaces 40 GbE	8 (OPTIONAL)
Interfaces 100 GbE	14 (OPTIONAL)
Hot Swappable	YES
Disk	1 TB or 2x 1TB in RAID 0, 1
Solid State Drive	2TB
Available Slots	7x



Photos for illustrative purposes only.

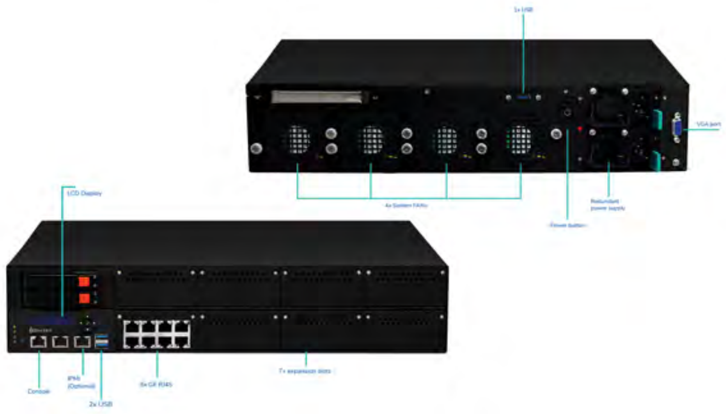
BBX3600

Performance Specifications and Options

	BBX3600
Type	2U
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	45,000,000
New Connections Per Second	400,000
NGFW Throughput (IMIX)	20 Gbps
SSL Inspection Throughput	10 Gbps
IPS Throughput	18 Gbps
Application Control Throughput	18 Gbps
Threat Protection Throughput	10 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	18 Gbps
SSL VPN Throughput (AES-256)	9 Gbps
Interfaces UTP 1 GbE	8 to 64 (OPTIONAL)
Interfaces SFP 1 GbE	32 (OPTIONAL)
Interfaces SFP+ 10 GbE	28 (OPTIONAL)
Interfaces 25 GbE	8 (OPTIONAL)
Interfaces 40 GbE	8 (OPTIONAL)
Interfaces 100 GbE	14 (OPTIONAL)
Hot Swappable	YES
Disk	1 TB or 2x 1TB in RAID 0, 1
Solid State Drive	2TB
Available Slots	7x

Photos for illustrative purposes only.

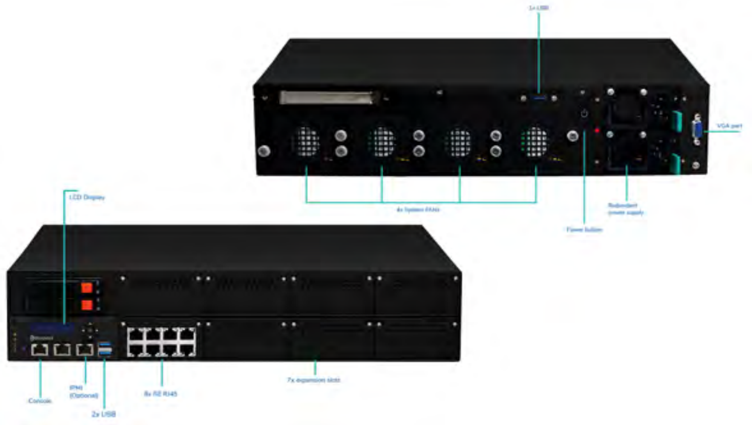
BBX4200



Performance Specifications and Options

	BBX4200
Type	2U
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	55,000,000
New Connections Per Second	520,000
NGFW Throughput (IMIX)	26 Gbps
SSL Inspection Throughput	12 Gbps
IPS Throughput	23 Gbps
Application Control Throughput	25 Gbps
Threat Protection Throughput	12 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	25.6 Gbps
SSL VPN Throughput (AES-256)	11 Gbps
Interfaces UTP 1 GbE	8 to 64 (OPTIONAL)
Interfaces SFP 1 GbE	32 (OPTIONAL)
Interfaces SFP+ 10 GbE	28 (OPTIONAL)
Interfaces 25 GbE	8 (OPTIONAL)
Interfaces 40 GbE	8 (OPTIONAL)
Interfaces 100 GbE	14 (OPTIONAL)
Hot Swappable	YES
Disk	1 TB or 2x 1TB in RAID 0, 1
Solid State Drive	2TB
Available Slots	7x

BBX5000



Performance Specifications and Options

	BBX5000
Type	2U
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	70,000,000
New Connections Per Second	700,000
NGFW Throughput (IMIX)	40 Gbps
SSL Inspection Throughput	20 Gbps
IPS Throughput	30 Gbps
Application Control Throughput	35 Gbps
Threat Protection Throughput	18 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	30 Gbps
SSL VPN Throughput (AES-256)	15 Gbps
Interfaces UTP 1 GbE	8 to 64 (OPTIONAL)
Interfaces SFP 1 GbE	32 (OPTIONAL)
Interfaces SFP+ 10 GbE	28 (OPTIONAL)
Interfaces 25 GbE	8 (OPTIONAL)
Interfaces 40 GbE	8 (OPTIONAL)
Interfaces 100 GbE	14 (OPTIONAL)
Hot Swappable	YES
Disk	1 TB or 2x 1TB in RAID 0, 1
Solid State Drive	2TB
Available Slots	7x

Deployment Options

Hardware Appliance	Virtual Appliance	Cloud Instance
• Maximum performance • Guaranteed stability • Quick installation	• Greater scalability • Faster disaster recovery • Infrastructure optimization	• AWS, Oracle, Azure, among others.

Virtual Appliance Model Specifications

Description	Overall Throughput (UDP)	NGFW Throughput (IMIX)
BBX40	6 Gbps	200 Mbps
BBX80	10 Gbps	850 Mbps
BBX100	12 Gbps	1.0 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

Photos for illustrative purposes only.

Security Policies

- Supports IPv4 and IPv6
- Source/Destination IP, Port, and Protocol
- Source/Destination Subnet
- By Users, Groups, IPs, Networks, and Zone (LAN, WAN, DMZ) and Country Code (BR, US, etc.)
- Control by applications, static and dynamic groups
- Filtration
- Web Content, Web Applications
- Inspection Profiles: SSL, IPS, Threat Protection, Web Filter and Application Control (implemented in a single policy and changing one engine does not impact others)
- QoS (bandwidth control/prioritization)
- Multiple services
- Editor of security rules (filtering policies) with the possibility of scheduling
- Inhabit and Disable Logs
- Action Types: Allow, Deny, and Reject
- Creation of policies by users or groups based on authentication for all services (Firewall, VPN, IPS, Application Control and others)
- Traffic Simulator, Locator & Policy Validator
- Conflicting Policy Detector in NGFW and GSM
- File locking by extension and allows the correct identification of the file by its MIME type, even when its extension is renamed

Web Cache and Proxy

- Transparent or Explicit Proxy (custom ports)
- Disk and Memory Cache size setting
- Web services support (HTTP and HTTPS versions 1.0, 1.1, 2.0 and FTP)
- In-memory and disk web cache configuration
- Enabling web caching of dynamic content (Facebook, Google Maps, MSN Video, Source forge Downloads, Windows Update, YouTube)
- Cache exception, configurable by regular expressions
- Proxy hierarchy with and without authentication
- Support for HTTP Anti-Virus integration via proxy hierarchy
- Blocking message to the end user
- Supports policy by time, time, and/or period (day, month, year, day of the week, and hour). Supports user groups, IPs, network, and/or security zones

Firewall

- Policy with authentication option with the ability to enable or disable logging
- NAT (SNAT and DNAT), 1:1, N:1, NAT64, NAT46, NAT44 and NAT66, PAT, Source NAT and Destination NAT and simultaneously
- Dynamic NAT (Many-to-Many and Many-to-1)
- Static (1:1 and Many-to-Many) and bidirectional 1:1 NAT
- Safety
- DoS (Denial Of Service) protection also available in Policy, PortScan, Invalid Packets, ICMP Sweep, and Brute Force
- Flood Protection (SYN, ICMP, UDP)
- Anti-spoofing protection
- ICMP (Controls, Transmission, Redirection)
- PING (Echo/Request)
- Multicast Forward
- Invalid Source Routing, Checksum, Log
- Flow Control for Dynamic Applications
- Blocking protocol traffic on custom ports
- Supports multicast objects and rules
- TCP_be_liberal
- IP spoofing
- Protection against Man-in-the-Middle attacks
- TCP/UDP/ICMP/IP Connection Controls
- Supports transparent mode (layer 2), gateway mode (layer 3), and port mirroring
- Supports real-time protocols
- Supports GPO Distribution (SCCM) by Microsoft AD from VPN Client

QoS - Quality of Service

- Packet marking for traffic prioritization (TOS and DSCP)
- Priority Queue from Lowest Priority to High Priority
- Traffic control and bandwidth assurance by policy (applications, users, or groups of users synchronized with Windows AD or LDAP), network zone, specific host, or source/- destination
- Real-time statistics for QoS classes in the Web Management Interface
- Supports QoS for LAG interfaces

IPS - Intrusion Prevention System

- Detection and prevention of attacks and intrusions based on +80k signatures grouped together as Client and Server
- Support for Customization and upload of Signatures in the web interface
- Impact Levels: Low, Medium, and High
- Protection against threats at the application layer (known exploits, Shellcode, SQL Injection, Buffer overflow, etc.)
- Protection against malformed packets
- Pattern recognition, protocol and anomaly analysis, and vulnerability blocking.
- Ability to reassemble the package after analysis to identify attacks
- Source Session Limit with TCP Reset for session termination
- DoS, DDoS (Flood, Scan, Session and Sweepe), PORTSCAN, Reconnaissance, Evasione and ICMP Prevention
- Mitigation of DoS and DDoS (denial of service) attacks
- Prevention against P2P technology attacks
- Prevention against Worm attacks, Trojans, Backdoors, Portscans (detects and blocks the source), IP Spoofing, SYN-ICMP-UDP flood and Spyware
- Prevention of protocol anomalies (HTTP, SMTP, POP, IMAP, Sendmail, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, CIFS, RPC, RDP, CHARGEN, SSDP, SNMP, TCP highjacking, SSH and Telnet)
- Botnet, DNS Poisoning, and Scalation Privilege Prevention
- SSH blocking on non-standard protocol ports and based on behavior through patterns
- Support exception configuration per source or target subscription
- Log of incidents for each type of attack identified
- Malformed traffic and invalid headers
- Automatic, periodic, and offline update
- Decodes multiple Unicode formats
- IP fragmentation and defragmentation
- Policies applied to interfaces or security zones
- Alarm via e-mail or SNMP trap
- Support Inline L2 (bridge/transparent mode) and L3 layer (firewall) implementation and port mirroring
- Supports exceptions by IP registered in the rules
- Whitelist and IP Blacklist (IPv4 and IPv6)
- Allows you to enable or disable subscriptions, or enable in monitoring mode
- It allows you to analyze and generate logs, blocks and quarantines the attacker's IP for a period of time

Threat Protection

- Antivirus and Anti-Malware with real-time analysis

- HTTP, HTTPS, FTP, SMB, CIFS, POP3, and SMTP (native in the solution)

- Protection against unauthorized applications

- (Packed, PwTool, NetTool, P2P, IRC, RAT, Tool, Spy)

- Password file protection
- Anti-Malware Quarantine
- Scanned files report
- Identifies, classifies and blocks malware such as trojans, spyware, adware, keyloggers, highjackers, worms, viruses, C&C (Command and Control) and Anti-bot (Botnet) connections
- Allows the blocking by reputation of the address classified into 6 categories: spam, reputation, malware, attacks, anonymous and abuse
- Automatic and periodic update
- Antibot has a multi-layered detection mechanism, e.g. reputation of IP address, URLs and DNS addresses and detects communication patterns and signatures
- Locks files by extension and also identifies by MIME type (even changing the extension)

SD-WAN

- Support for multiple configuration profiles and allows you to enable on any WAN interface (DSL, MPLS, 3G/4G LTE) and Packet Duplication (PD), aggregation with VPN feature, supports static and dynamic routing (OSPF, BGP). IPv4/IPv6, supports dynamic and outbound NAT
- Setting of Sending Traffic by Selected Interface, Supports Policy Based Routing

- Failover, Load Balance, Spillover and Performance

- Monitoring of link availability and protection against degradation of data links

- It supports link balancing by hash of the source and destination IP, by weight with percentage configuration and can use from 2 to 9 links
- Verification of link failure by TCP/UDP Echo protocol, ICMP (ping) and HTTP

- Measurement by bandwidth consumption, packet loss, jitter, latency (monitoring of multiple destinations and on all interfaces) with more than 3 targets, and measurement values can be changed
- Application- and policy-based routing for multiple WAN paths, with app blocking
- Customizable link failback from 1 to 100 and Link Persistence
- Implements link balancing without creating zones or using virtual instances
- Group routing in SD-WAN rules, session and packet traffic balancing

Zero-touch Provisioning

- Automatic provisioning associated with the machine's serial number
- Configures IPv4/IPv6 security templates and policies

Secure Web Gateway

- Content Filter (no NAT)
- 88 categories (including Government, Webmail, Healthcare Institutions, News, Pornography, Restaurant, Social Media, Sport, Education, Games; Shopping), +49 million cataloged URLs, login control by domain in Google, SafeSearch integration, Google, Bing and Yahoo, block message for the end user
- SSL Inspection with Invalid Certificate Lock

- Integration with ATP and Windows AD/LDAP inspection for user and group identification

- Blocking Social Media Apps like: 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 and ZohoChat and Chat Apps
- Blocking of Office, Java and Javascript files, Cookies, ActiveX, Multimedia, Images
- Application Recognition – DPI (Deep Packet Inspection)
- Identifies Applications via SSL, HTTP, HTTPS or non-standard access ports
- Category-based SNI control
- Filtering, categorizing, and reclassifying websites by URL
- User authentication in LDAP, Radius, TACACs+ and Microsoft Active Directory
- Blocking by constructing specific filters with textual search engine
- Custom lists (whitelist and blacklist)
- Captive Portal with Social Login (Facebook, Twitter, Google)
- Navigation quotas by time and/or traffic volume
- Scheduled and Automatic Update in transparent mode
- Port- and protocol-independent application awareness
- Identifies the use of evasive tactics to control applications that attempt to use encrypted connection (Skype/TOR network)

Networks and Interfaces

- Interfaces

- Ethernet (with Forward Error Correction (FEC) support
- VLAN (IEEE 802.1q) up to 4094 IDs per interface
- WAN Support: ADSL/DSL, MPLS, LTE (3G/4G/5G)
- Alias (Virtual IP)

- LTE (3G/4G) use as a link for load balancing and failover
- Link aggregation

- Ethernet bonding (802.3ad) LACP

- Dynamic routing: BGP4/BGP4+, OSPFv2/v3, RIPv2 and PIM-SM/PIM-DM
- Static routing (IPv4 and IPv6) with ECMP support
- Multicast routing: supports rules and objects
- Native IPv4 and IPv6 support
- DHCP (dynamic host configuration protocol) IPv4 and IPv6

- Relay, Server and Client

- Recursive DNS
- Policy Based Routing (PBR)
- Supports logical ethernet sub-interfaces

Authentication

- User Authentication

- On-premises, Windows AD, LDAP, SSO Windows (single sign-on via Kerberos) and WMI – unified authentication, X-Auth for VPN services, authentication on Radius servers, RSSO (radius single sign-on), password complexity identifier, Token ID, Sessions and Applications based on TCP/UDP/ICMP

- TACACS+ and LDAP support for admin users and Firewall users
- Synchronism of users and groups and hosts with Windows AD servers and LDAP servers with replication of established user sessions
- AAA (Authentication, Authorization, and Accounting)
- Identification by the AD base allows the use of SSO, so that users do not have to log back into the network to navigate through the Firewall
- Supports authentication for Firewall and VPN: Tokens, TACACS, RADIUS LDAP/AD, and digital certificates

IPSec VPN and SSL VPN

- Tunnel VPN (LAN to LAN) / Site-to-Site and Client-to-Site VPN
- RAS/SSL VPN (remote access allows VPN client access or direct support at the clientless station - Web Interface), i.e. you can use SSL VPN with or without agent
- SSL Portal VPN (via HTTPS) for RDP, VNC, SSH, WEB and SMB accesses
- VPN client compatible with Win7, 8/8.1, 10 and 11 (32 and 64-bit), Linux and MacOS, Android and IOS
- Authentication
- Allows you to enable, disable, restart, and update IKE, Gateways, and IPSec VPN tunnels from the GUI
  - PSK (Pre-Shared Key), X-Auth (AD, LDAP, local, RADIUS), IKE PKI Digital Certificate, EAP (MSCHAPv2)
- Allows tunneling to be established before or after the user authenticates at the station and on user demand
- Native IPSec VPN authentication using MD5, SHA-1, SHA-256, SHA-384, SHA-512, and AES-XCBC
- High Availability
  - Full Quality Domain Name (FQDN) and DDNS Support
- NAT-T (UDP Encapsulation) and DPD (Dead Peer Detection)
- Exchange mode IKEv1: Main mode or Aggressive mode
- Compressed data support
- Protocols
  - IKEv1 and IKEv2 (for phase 1 and phase 2) and ESP
  - Symmetric Encryption: AES(128, 192 and 256), 3DES
  - Asymmetric Cryptography: DH - Diffie-Hellman (Group1, Group2, Group5, Group14; Group15, Group16, Group17, Group18, Group19, Group20, Group21, Group22, Group23, Group24, Group25, Group26, Group27, Group28, Group29, Group30)
  - RSA key generation, DSA parameter
- Supports Auto-Discovery VPN (AD-VPN), allows multiple devices (Spokes) with centralized gateway (hub) and Site-to-Site, Supports tunnels of type (Site-to-Site, Full Mesh, Star)
- Supports RSA and Diffie-Hellman algorithms
- SSL VPN with X.509 v3 digital certificate support
- Supports enrollment of certificate authorities via SCEP (Simple Certificate Enrollment Protocol)
- Dynamic Public IP support, RIPv2 and OSPFv3 routing
- Support for certificates issued by a certificate authority in the ICP-Brasil standard
- Certificate revocation list (CRL) verification support
- SSL and IPSec (client-to-site) VPN with Blockbit Client for Windows
- Allows you to assign DNS on remote VPN clients
- Clientless VPN (IPSec and SSL) with no restrictions from market players
- SSL Certificate Management (X.509)
- Allows all remote VPN users' traffic to flow into the VPN tunnel, preventing direct communication with local devices such as proxies

Logging and Reporting

- Netflow/IPFIX support
- Session Logging, Authentication, and VPN Reports, by single or consolidated device
- Creation of a customizable Analyzer report (native in the tool) of the Firewall, Web Filter, Application Control, IPS, ATP, VPN and User Behavior services (IP information, User Operating System, Hostname and threat classification in "top 10" style)
- Remote Syslog for sending logs and log export via SCP, supports log sending via SSL protocol
- Export of reports in multiple formats (PDF, CSV, HTML)
- The events identify the country of origin of the attack
- Events record changes in the state and health of SD-WAN links

Web Interface and CLI

- Granularity (read and read/write profiles, application of settings, etc.) of administrator access in the Web Interface with concurrent sessions
- CLI (command line interface for management and diagnostics via SSH and RS-232/RJ-45 serial
- Own web interface available in Portuguese, English and Spanish accessible by any physical interface of the product
- Management (LAN or WAN) via WEB (HTTPS per browser) and SSH

Data Filter

- It has a feature capable of identifying and preventing the transfer of various types of files (MS Office, PDF, etc.) identified on applications (HTTP, HTTPS, FTP, SMTP)
- It is capable of identifying compressed files on the data network and applying usage policies on the content of these types of files

Monitoring

- SNMP v1, v2 and v3 protocol support, monitors CPU usage, memory, disk space, VPN, cluster situation and security breaches
  - Performance, concurrent connections, DHCP lease, authenticated users, and enabled or disabled services
- System and Security Notifications
- Detailed event preview window
- Tool for disk maintenance and real-time network traffic monitoring (Live Sessions and Trafic Monitor) with throughput information and simultaneous connections
- Security and Threat Event Logs
- TCPDUMP by Feature and specific protections (allows capture and download in PCAP format)
  - Logging users into authentication, access, blocking, and threat events
  - RX/TX Counters, Packet Input and Output, Packet Drops, and Errors (CLI Command)

H.A. (High Availability)

- Mirroring firewall sessions, user authentication, and synchronizes all configurations, sections, certificates for SSL inspection, IPSsec VPN Security Associations (SA), and all ATP, Application Control, IPS, and WEB Filter signatures, between the primary and secondary devices so that the switch over is transparent and fast
- Support monitoring of 3 Heartbeat interfaces
- Interface monitoring in the event of a link failure

Backup and Restore

- Encrypted System Snapshot and Backup
- Disaster Recovery (backup/restore) via web interface
- Storage (for backup and log saving)
  - NFS / DISK(HDD) / SSH / Flash (via USB)
- Backup Rotation on Storages
- Snapshot or System Backup Schedule

SandBoxing - APT

- It allows you to mitigate advanced persistent threats (APT and Zero-Day), through dynamic analysis to identify unknown malware with automatic update in a network intelligence database. Scans PDF, Microsoft Office, executable, and compressed files
- Able to create signatures and even include them in the firewall's antivirus base, preventing the recurrence of the attack
- Supports including in the firewall the URLs identified as sources of such undiscovered threats (blacklist), preventing these addresses from being accessed again by network users
- The ATP module supports file analysis by antivirus, cloud query, code emulation, sandboxing and call-back verification and analyzes the behavior of suspicious files in a controlled, real-time environment
- Capable of emulating, detecting, and blocking any malware and/or malicious code
- Emulates SandBox of Microsoft environments in various versions and Office

User Identification

- Enables the creation of policies based on URL control and URL categories
- Allows you to create policies based on visibility and control of who is using which applications through integration with directory services, authentication via LDAP, Active Directory and local database
- It has compatibility with Microsoft Active Directory (Windows 2003, 2012 and 2019) for user and group identification, allowing granularity of control and policies based on users and user groups, supporting single sign-on

- Supports unlimited users

- Supports authentication for Firewall and VPN: Tokens, TACACS+, RADIUS, and digital certificates
- It allows the control, without installation of a software client, on equipment that requests internet output so that before starting browsing, an authentication portal resident in the firewall (Captive Portal) is expanded
- Supports the identification of multiple users logged in to the same IP address in Citrix and Microsoft Terminal Server environments, allowing granular visibility and control per user over the use of applications that are in these services
- Allows the creation of custom groups of users in the firewall, based on LDAP/AD attributes

Other Resources

- Proxy Services (SSH, SMB/CIFS, HTTP, FTP, SMTP, POP3)
- Supports VoIP (SIP/H323) and RTP over IPv4/IPv6
- Multi-domain authentication support
- Supports fail-closed and optional fail-open (by-pass) interface
- Transparent Update, automatically, periodically and offline
- Supports session authentication for all protocols and any applications
- Resource Objects

- IP Addresses, MAC Addresses, Port and Protocol Services, Timetable, Time Period and Date Table, Dictionaries (set of words and/or regular expressions), Content Types

- Network Time Protocol (NTP) server support for date and time update
- Option of automatic and periodic system updates for patches and web releases HTTPS or via GSM
- TCP Flow Optimization
- Supports access via SSH, CLI, client, or WEB (HTTPS)
- Equipment virtualization in Public Cloud (Google Cloud®, Azure®, Oracle Cloud® and AWS®) or Private Cloud (VmWare®, Citrix XenCenter® and ProxMox®)
- Context Support (Virtual Domain)
- High Availability Cluster System (Active-Passive and only with equal equipment) with maintenance of established sessions, traffic distribution, state table maintenance and session balancing
- Able to identify the network user, supports AD, LDAP, RADIUS, and TACACs+
- No installation of agents in AD or on user stations
- All policies support application control
- Supports various methods of identification and classification of applications, e.g., signature checking and protocol decoding
- Allows the creation of custom signatures on the web interface for application and IDS/IPS recognition
- Allows requests to include applications in the default base
- It is possible to differentiate different P2P traffic for different software (Bittorrent, emule, and others) with granularity in the control of the applications
- Supports granularity in IPS, Anti-Virus and Anti-Spyware policies, allows the creation of different policies by security zone, source address, destination address, service and the combination of all these items
- Allows you to use deny operators in the creation of custom IPS signatures, allowing you to create exceptions with granularity in the configurations
- Logs the following information about identified threats to the monitoring console
- Name of the signature or attack, application, user, source and destination of the communication, and the action taken by the device
- It has protection against viruses in HTML and Javascript content, spy software (spyware) and Worms
- Protection against unintentional downloads using HTTP of executable and/or malicious files
- Allows the configuration of different policies to control threats and attacks based on firewall policies considering users, user groups, source, destination, security zones, MAC Address, each firewall policy may have a different configuration of IPS, these policies being by users, user groups, source, destination, security zones
- Supports Virtual System Appliances (VDOM) on all models
- VDOM system allows you to create virtual contexts with support for the creation of multiple administrators
- Supports TLS 1.2 and TLS 1.3
- Supports the creation of blocking or release policies by geolocation and informs the country of origin and/or destination in the logs with the flag to facilitate the identification of traffic

Some RFC's supported by the 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.

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).

IPv4 and 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.

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 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.

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.

Some RFC's supported by the Blockbit Platform

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.

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 and 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.

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

Other Protocols

- 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.

Cryptography

- 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.

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.

THE TESTS WERE PERFORMED IN A LABORATORY WITHOUT SUMMARIZATION BY USERS, IPS AND SERVICES, APPLICATION DETECTORS DISABLED, FIREWALL THROUGHPUT UDP PACKAGES OF 15 18 BY TES, FIREWALL THROUGHPUT HTTP GET 1280 Kb AND PUT 12 80Kb, IPS/ATP THROUGHP UT WITH FACTORY STANDARD SIGNATURES ENABLED. NGFW IS MEASURED WITH FIREW ALL, THREAT PROTECTION, IPS AND APPLICATION CONTROL ENABLED, I MIX TRAFFIC.