



Blockbit Platform

Integrated Cybersecurity, Converging Connectivity and Security

- Secure SD-WAN
- Next-Generation Firewall

blockbit.com

About Blockbit

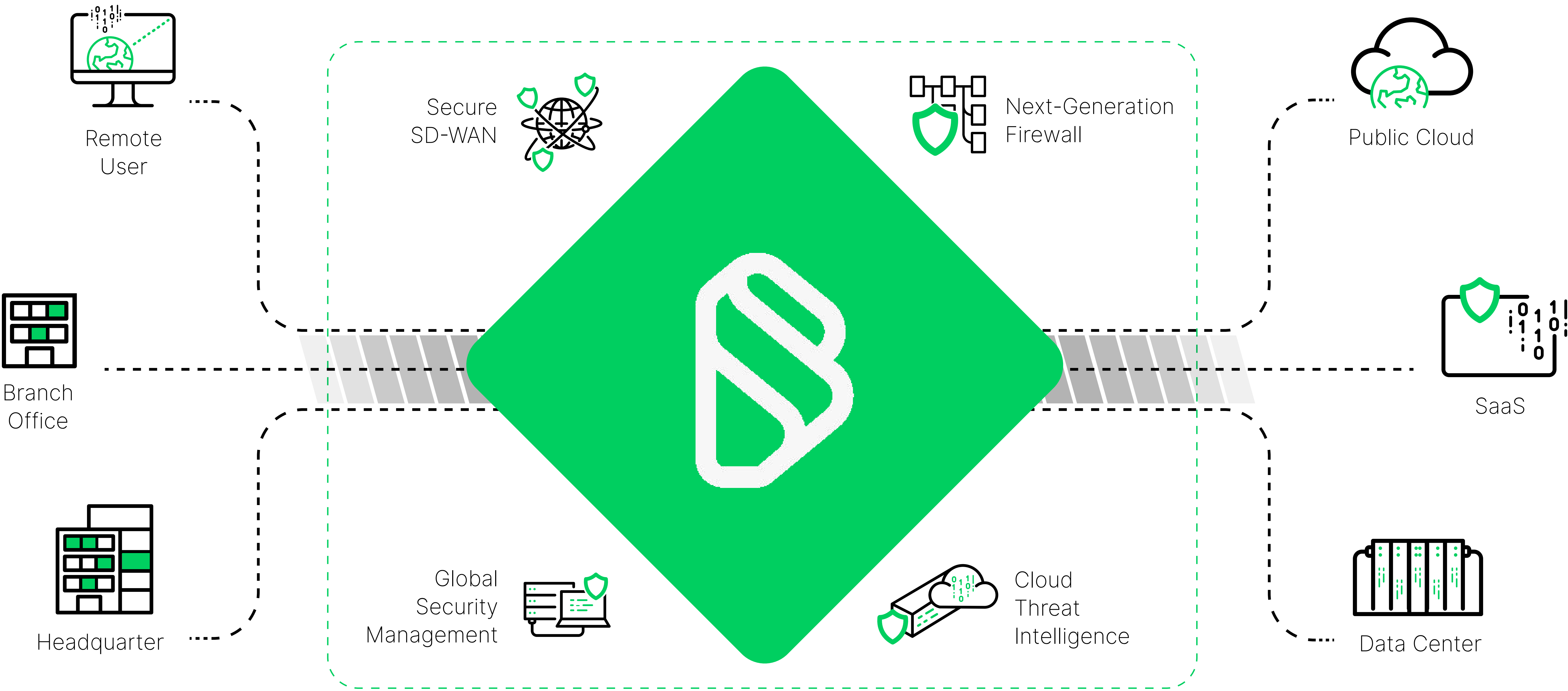
Blockbit is the Brazilian leader in cybersecurity products, protecting thousands of companies and millions of users from digital attacks and threats. With cutting-edge technologies and an advanced intelligence laboratory, Blockbit develops proprietary solutions for network protection and secure connectivity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

Discover the Blockbit Platform

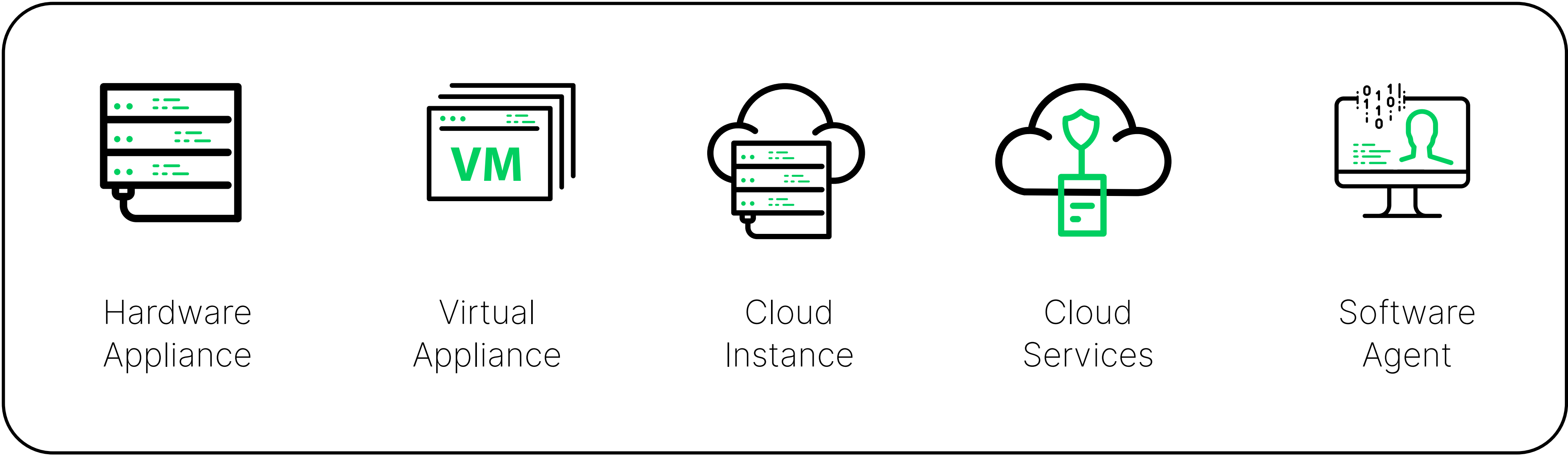
The **Blockbit Platform** is perfectly aligned with the global trend of converging connectivity with security, providing robust network protection and secure end-to-end connectivity.

Our platform comprises **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. Furthermore, **Blockbit Cloud Threat Intelligence** constantly provides advanced intelligence to the products.

The Blockbit Platform unites innovative products essential to accelerate your business securely, ensuring the desired quality and performance, all in one solution.



Deployment Options



With **Blockbit**, it's easy to be secure

The Blockbit Platform offers an advanced and robust solution with innovative features that reduce your operational time through automated configuration, centralized management, and intuitive processes. This frees up more time for you to focus on what truly matters: **your business**.

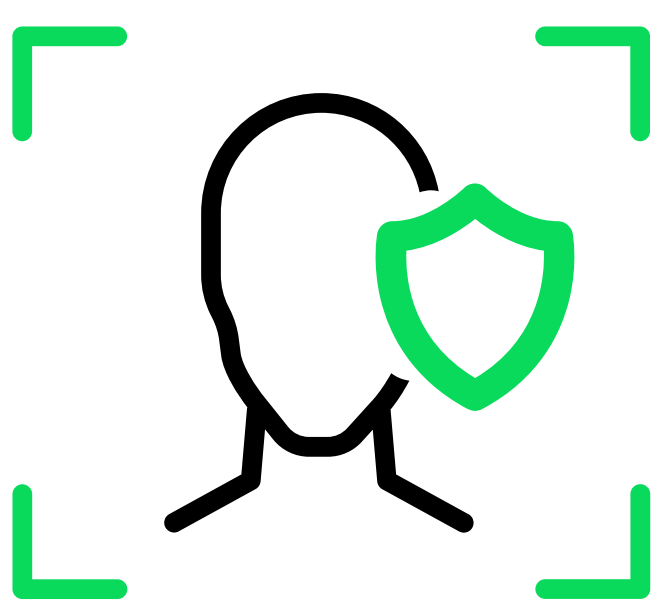
Whether it's enhancing security, optimizing performance, or saving time, Blockbit is here to simplify the path toward a more secure and efficient digital environment.



Simplify Your Network, Unifying Connectivity and Security

Our platform dramatically simplifies network complexity by harmoniously integrating connectivity and security, capable of detecting encapsulated applications and validating whether traffic matches protocol specifications.

With Blockbit, you reduce operational and administrative overhead, ensuring a consistent and robust security posture across your entire infrastructure.



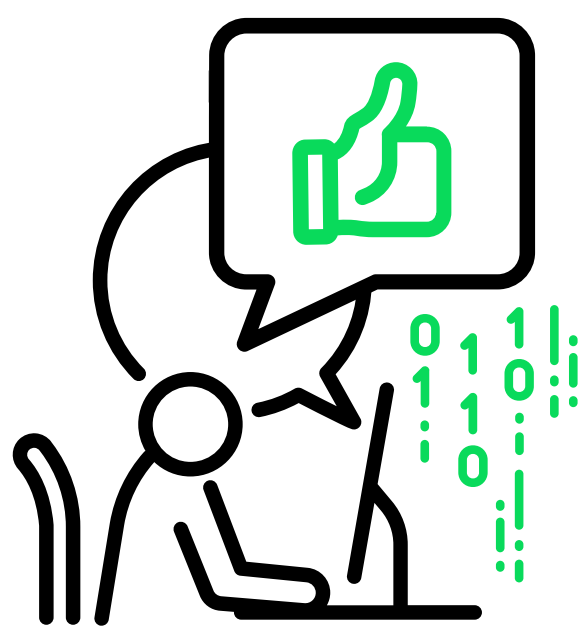
Automatically Configure Your Devices

With automatic configuration features, device deployment becomes more efficient than ever. There's no need to waste time installing our devices; Blockbit has taken care of that for you. Centralize configurations and automatically distribute them to remote assets. With the ZTP (Zero-Touch Provisioning) feature, you can reduce implementation time and cost.



Manage All Blockbit Devices from One Place

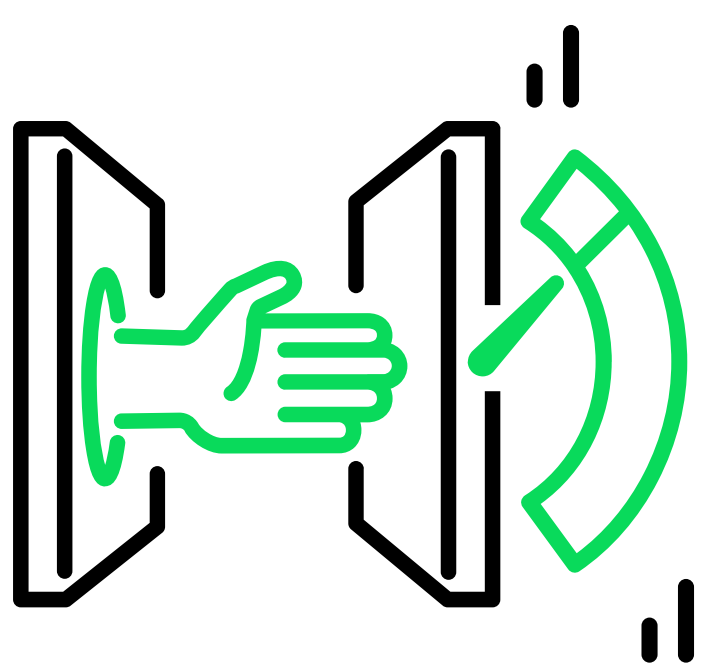
Blockbit allows you to manage all your devices and security events from a single, centralized location. This eliminates the complexity of dealing with multiple interfaces and optimizes your workflow, saving time and enabling quick actions and informed decisions.



Reduce Time with a User-Friendly and Intuitive Interface

The Blockbit Platform was designed with a user-friendly and intuitive interface, significantly reducing the time required for managing and configuring security devices.

This puts control in your hands, without the need for an extensive learning curve, and allows you to perform your functions more quickly.



Achieve Greater Quality and Performance, at an Affordable Price

Combining cutting-edge technology with performance optimization approaches, Blockbit ensures that your cybersecurity does not compromise the speed and efficiency of your network.

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

Secure SD-WAN

Blockbit Secure SD-WAN is a powerful combination of SD-WAN with all of Blockbit's advanced cybersecurity features. With this, you solve your main challenges, both in 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, unifying and minimizing continuity risks and conflicts by having a single point of control.

Monitoring of multiple links for long-distance connection, supporting connection types such as: **ADSL/DSL, Cable Modem with Ethernet or fiber, LTE/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 protection against attacks and threats, going beyond network protection to also safeguard applications and users. With this solution, you can analyze application traffic in real time, enabling more granular and efficient security policies. It can be deployed 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 the most advanced tool available to face the challenges of digital security and protect your data, users, and systems from threats and attacks.



Blockbit **SD-WAN**
Software-Defined Wide Area Network



Blockbit **NGFW**
Next-Generation Firewall

Connectivity with high quality and advanced security

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

Complete digital security with high performance

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



Global Security Management



Zero-Touch Provisioning


Blockbit Secure SD-WAN

Ensure Quality of Service for Connections and Applications, with Advanced Security

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

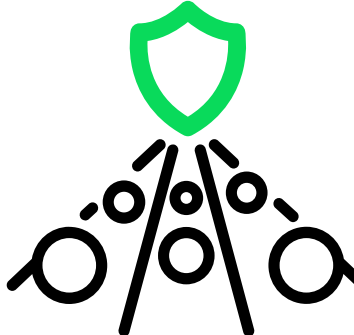
With Blockbit, the integration and management of various network connections become a reality, regardless of the vendor, technology, or connection type. For example, using features like **WAN Aggregation & Link Failover**, you can aggregate links from different providers and establish a contingency plan 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 business performance and increase resilience.



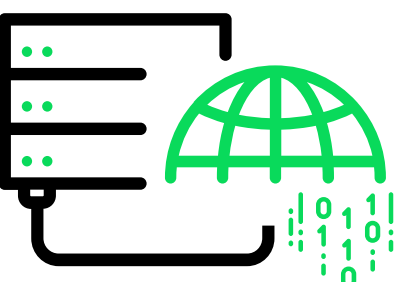
Dynamic Path Selection (DPS)

Automatically defines the best route for application traffic, based on quality of service requirements, business policy, and network conditions.



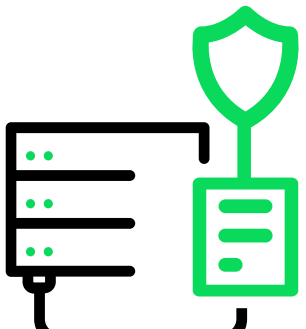
WAN Optimization

Accelerates application delivery, reducing latency, while improving bandwidth efficiency and reducing the size of transmitted packets.



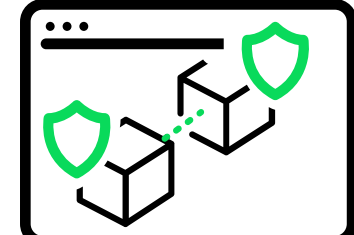
WAN Aggregation

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



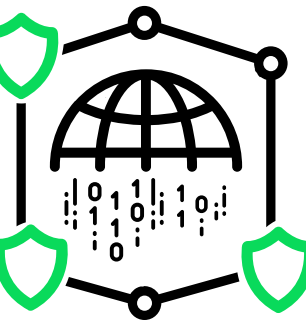
Link Failover

Provides network resilience in case of failure of one or more connections, detecting connection failure and automatically redirecting traffic to a secondary connection.




Virtual Private Network (VPN)

Enables secure and private communication between branches and employees, allowing remote access to internal information, systems, and resources.



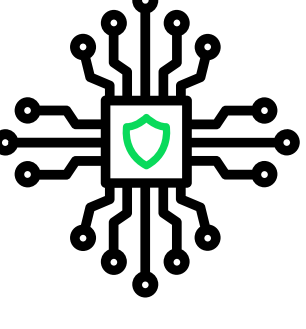
WAN Edge Security

Integrates all advanced security features into a single solution, adding ATP, IPS, and SWG modules, protecting your network and 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 Blockbit Secure SD-WAN deployment, enabling remote configuration and automated device installation.



Multi-Factor Authentication (MFA)

Provides a second authentication factor to validate user authentications, ensuring greater security for access to Blockbit resources.

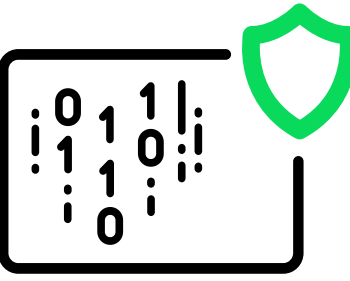
Blockbit Next-Generation Firewall

Protect Your Company with the Best Next-Generation Firewall

Blockbit NGFW is a high-performance, next-generation corporate firewall that incorporates advanced controls and protections for users, applications, and the network into a single solution.


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

Discover the Main Modules of Blockbit NGFW:



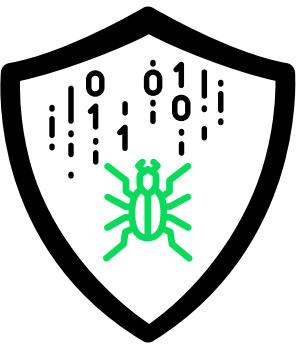
Deep Packet Inspection (DPI)

Provides deep packet inspection capabilities for both open and encrypted traffic, allowing for the identification and blocking of malicious activities, specific applications, network protocols, data types, and even hidden threats.



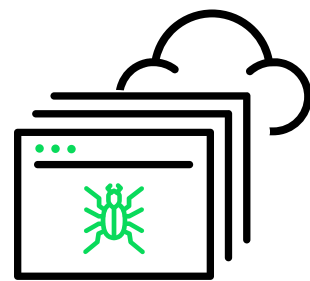
Application Control

Allows controlling and managing the use of applications and services, automatically identifying thousands of applications, controlling usage and prioritizing bandwidth, and generating analytical information on application usage.



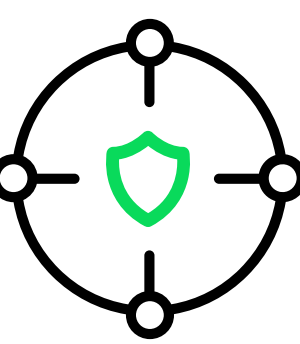
Advanced Threat and Malware Protection (ATP)

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




Cloud Sandbox

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




Intrusion Prevention System (IPS)

Creates incident logs and enhances your visibility, actively identifying and blocking malicious traffic attempting to exploit vulnerabilities in your network's applications and services.




Secure Web Gateway (SWG)

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




DNS Content Filter

Enables more granular and specific definition of internet access policies, ensuring greater security and control over Browse.




Virtual Domains (VDOM)

Allows segmenting Blockbit into multiple virtual domains, with independent administrations, for controlling and protecting multiple networks with a single device.



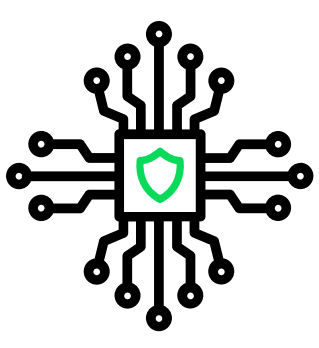
Zero Trust Network Access (ZTNA)

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



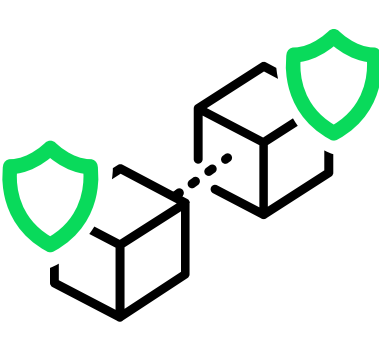
Global Security Management (GSM)

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



Zero-Touch Provisioning (ZTP)

The ZTP feature simplifies Blockbit NGFW deployment, enabling remote configuration and automated device installation.



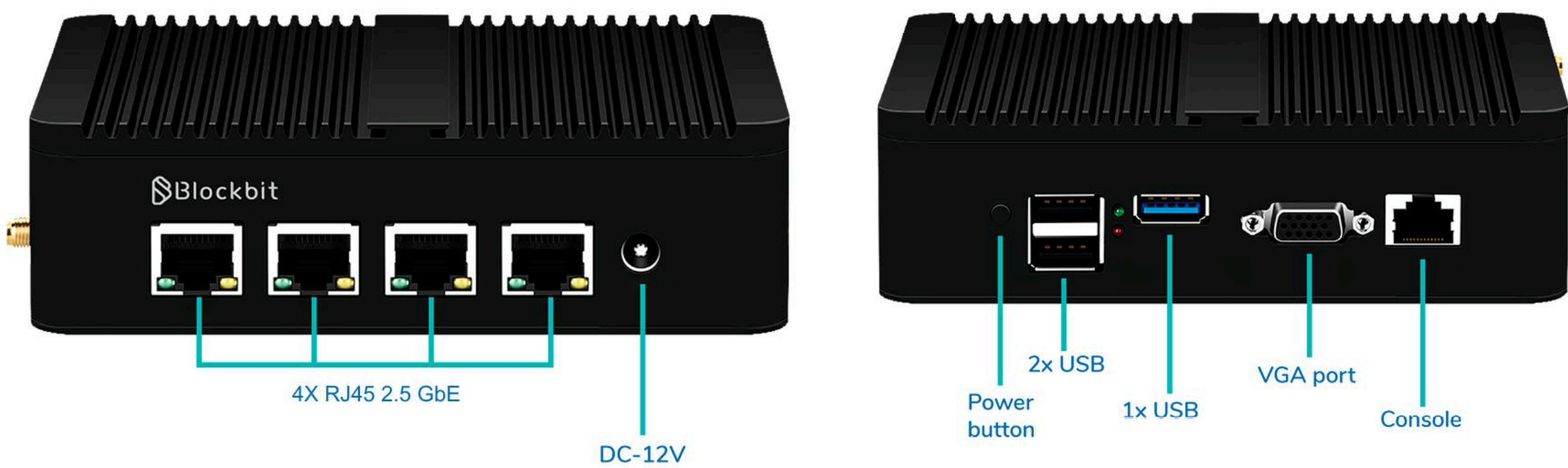
Multi-Factor Authentication (MFA)

Provides a second authentication factor to validate user authentications, ensuring greater security for access to Blockbit resources.

Blockbit Appliances

Performance and Optional Specifications

BBX40



BBX40	
Type	Desk
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	Optional
SSD Drive	64GB, 120GB or 240GB
Available Slots	*

BBX80



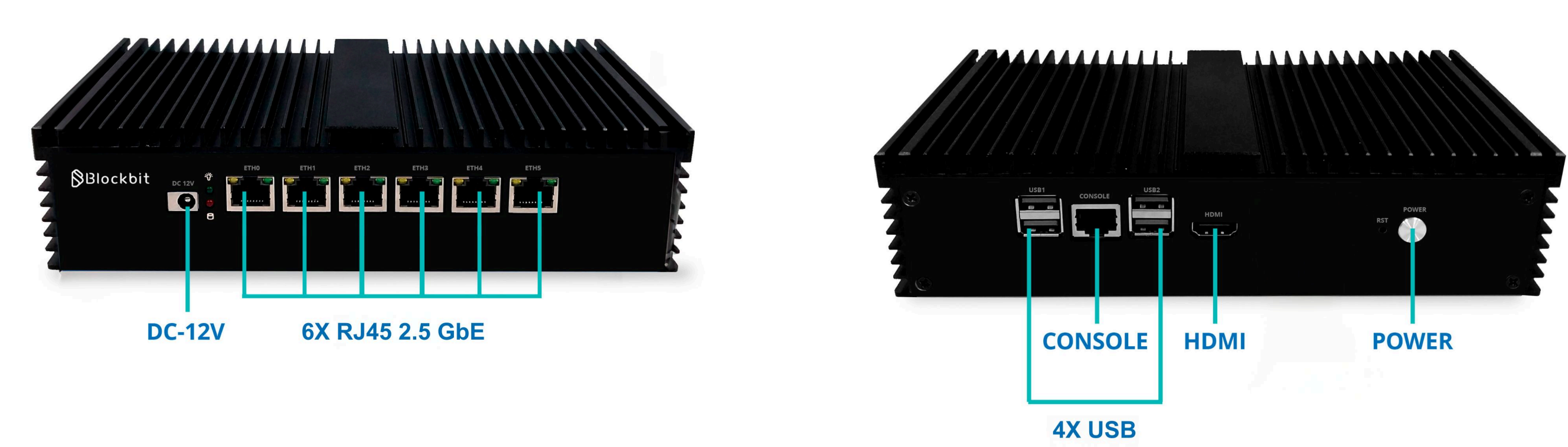
BBX80	
Type	Desk
Firewall Throughput (UDP)	10 Gbps
Concurrent Connections	6.000.000
New Connections Per Second	45.000
NGFW Throughput (IMIX)	850 Mbps
SSL Inspection Throughput	700 Mbps
IPS Throughput	1.25 Gbps
Application Control Throughput *	1.3 Gbps
Threat Protection Throughput	700 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	2.0 Gbps
SSL VPN Throughput (AES-256)	1.2 Gbps
Interfaces UTP 2.5 GbE	4
Wi-Fi	Optional
LTE 3G/4G	Optional (up to 2 modems)
SSD Drive	64GB, 120GB or 240GB
Available Slots	*

* Application Control performance uses a proxy-based methodology.

Blockbit Appliances

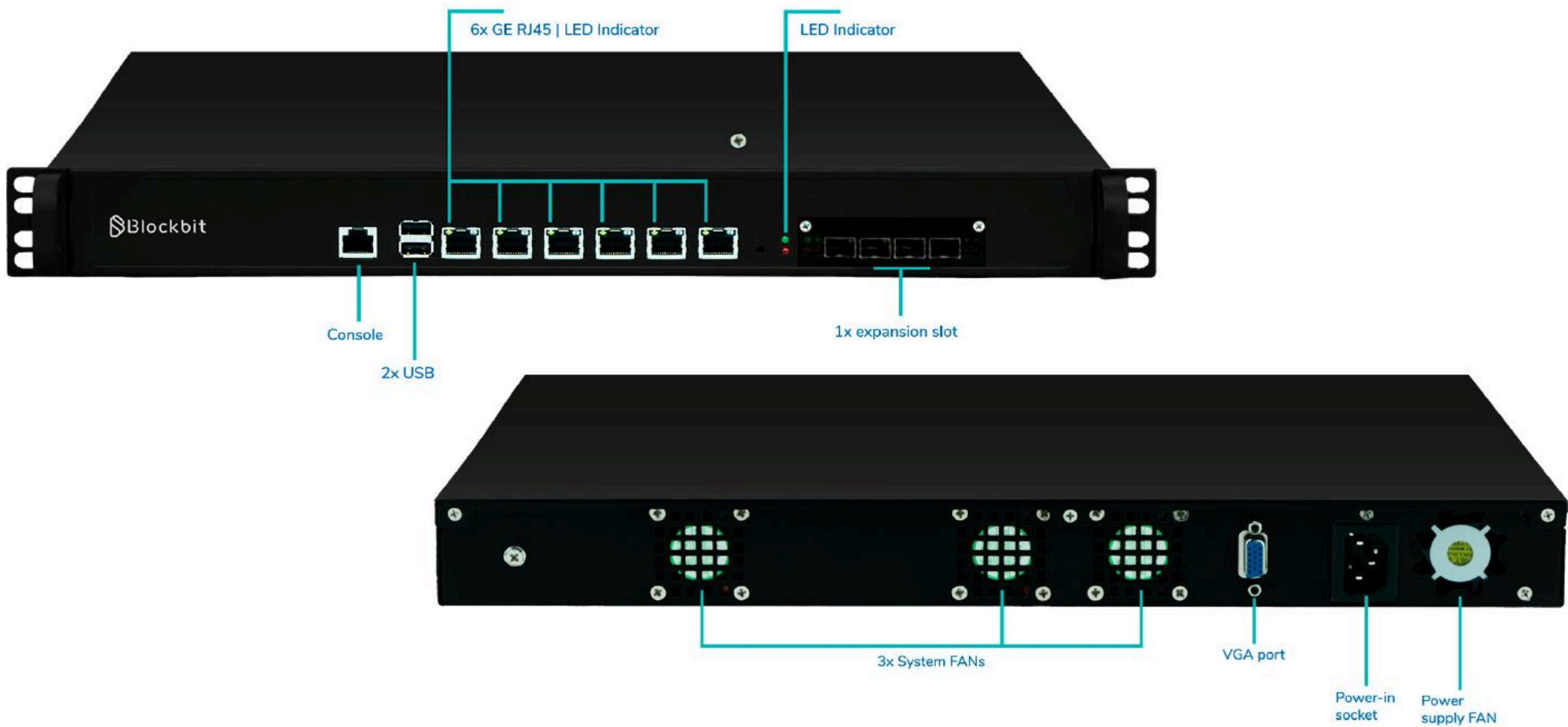
Performance and Optional Specifications

BBX140



BBX140	
Type	Desk
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	Optional
SSD Drive	120GB or 240GB
Available Slots	*

BBX200



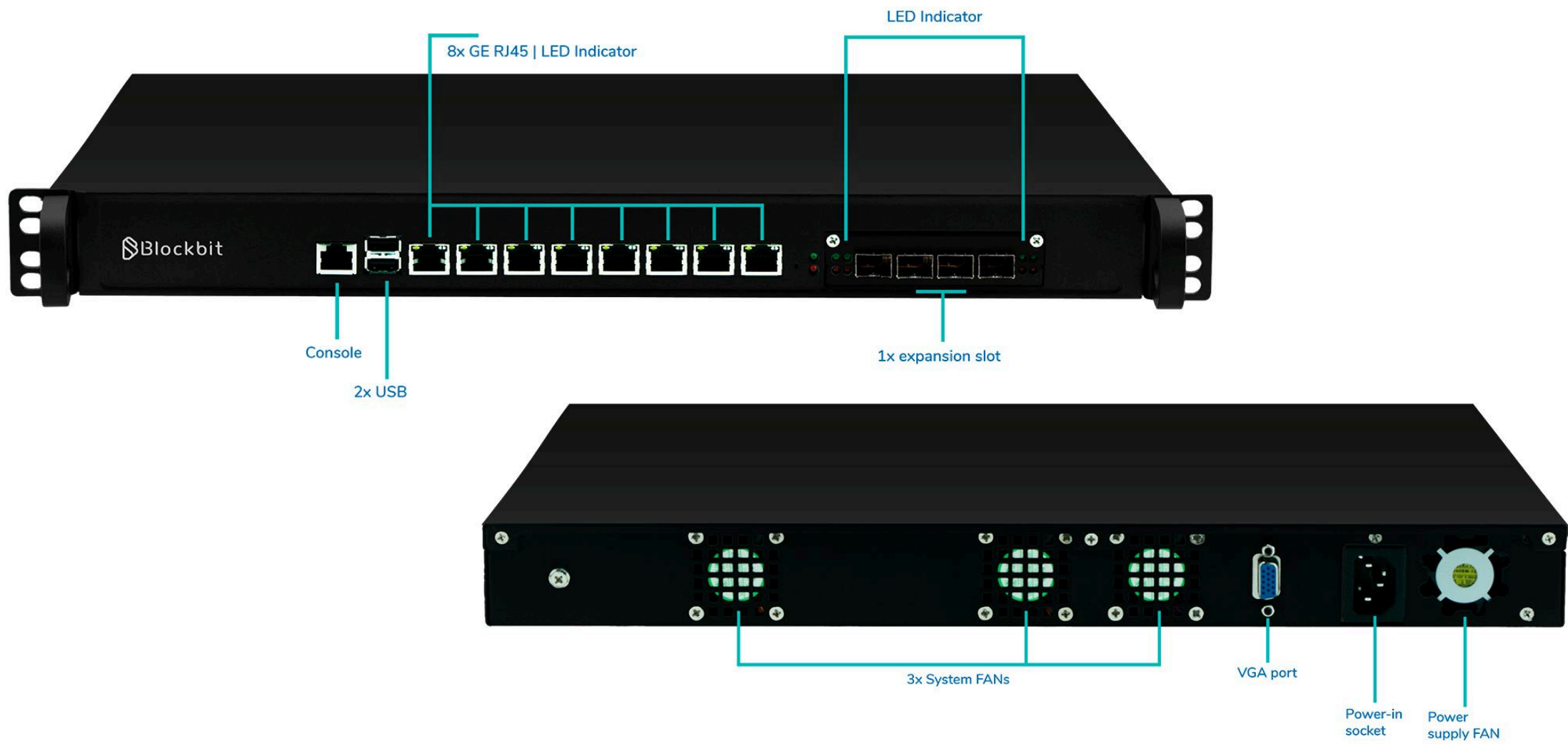
BBX200	
Type	1U - Rack 19"
Firewall Throughput (UDP)	20 Gbps
Concurrent Connections	8.200.000
New Connections Per Second	65.000
NGFW Throughput (IMIX)	2.5 Gbps
SSL Inspection Throughput	1.3 Gbps
IPS Throughput	3.0 Gbps
Application Control Throughput *	3.0 Gbps
Threat Protection Throughput	1.0 Gbps
IPSEC 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 (Optional)
Interfaces SFP+ 10 GbE	4 (Optional)
SSD Drive	120GB or 240GB
Available Slots	1x

* Application Control performance uses a proxy-based methodology..

Blockbit Appliances

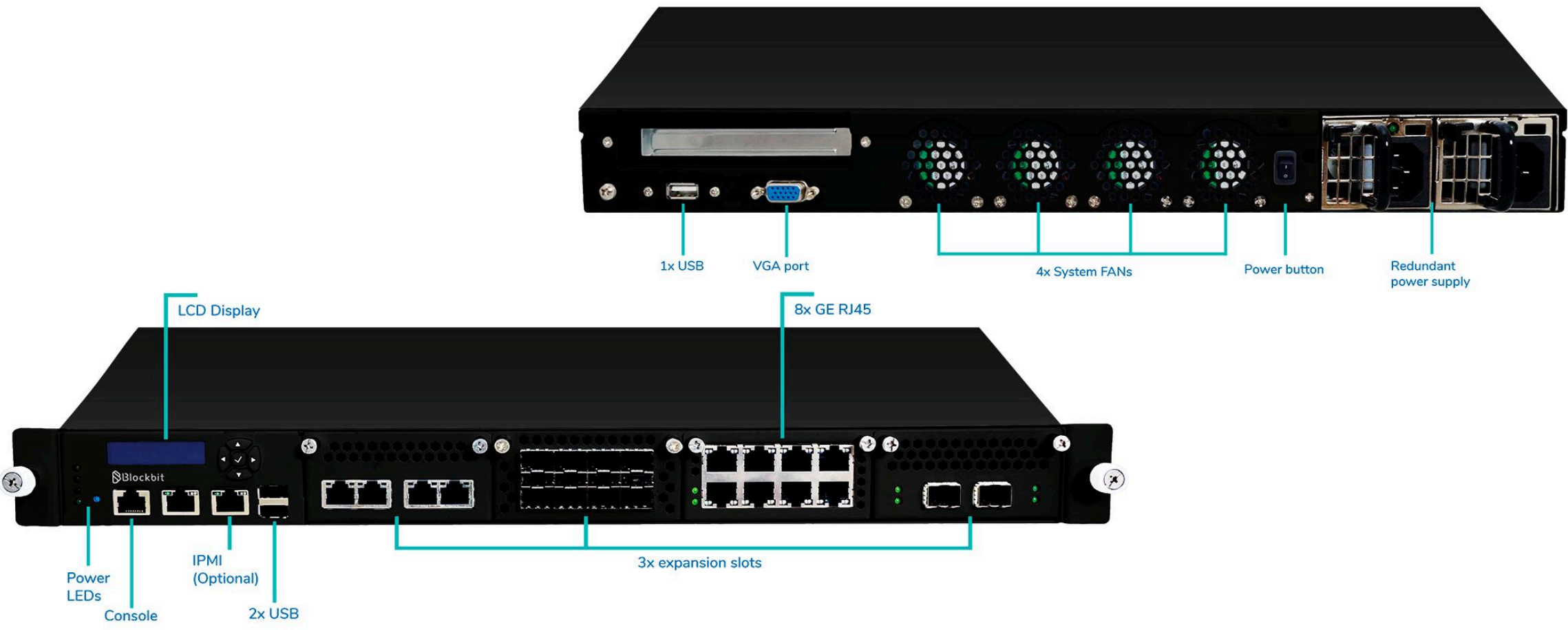
Performance and Optional Specifications

BBX700



BBX700	
Type	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 to 16 (Optional)
Interfaces SFP 1 GbE	4 (Optional)
Interfaces SFP+ 10 GbE	4 (Optional)
Power Supply 110/240V - 50~60Hz	YES
SSD Drive	240GB or 480GB
Available Slots	1x

BBX1500



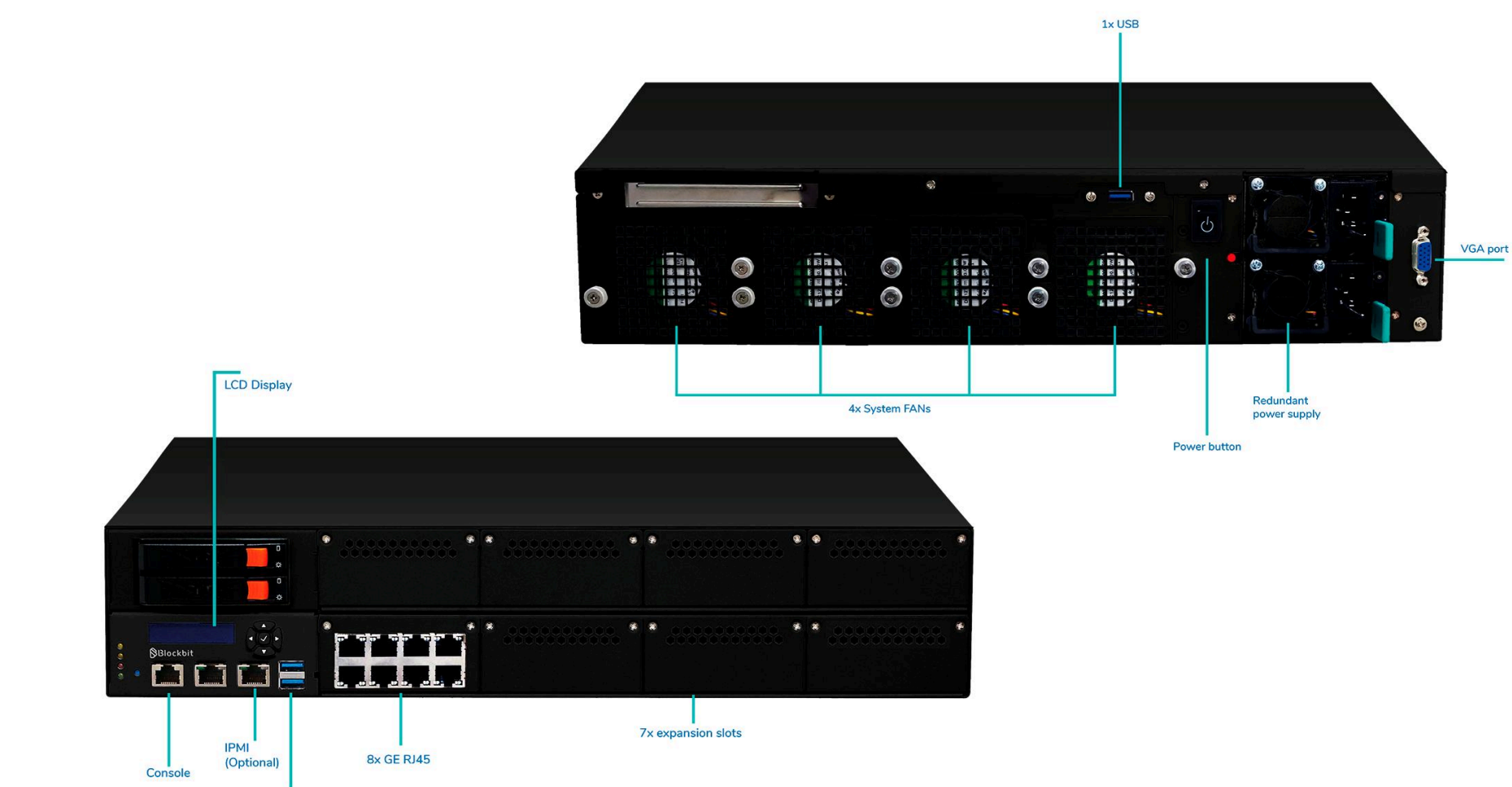
BBX1500	
Type	1U - Rack 19"
Firewall Throughput (UDP)	55 Gbps
Concurrent Connections	22.000.000
New Connections Per Second	200.000
NGFW Throughput (IMIX)	6.5 Gbps
SSL Inspection Throughput	4.5 Gbps
IPS Throughput	12 Gbps
Application Control Throughput *	10 Gbps
Threat Protection Throughput	4.5 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	10 Gbps
SSL VPN Throughput (AES-256)	5 Gbps
Interfaces UTP 1 GbE	8 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)
Redundant Power Supply - Hot Swappable - 110/240V - 50~60Hz	YES
SSD Drive	480GB or 1TB
Available Slots	3x

* Application Control performance uses a proxy-based methodology.

Blockbit Appliances

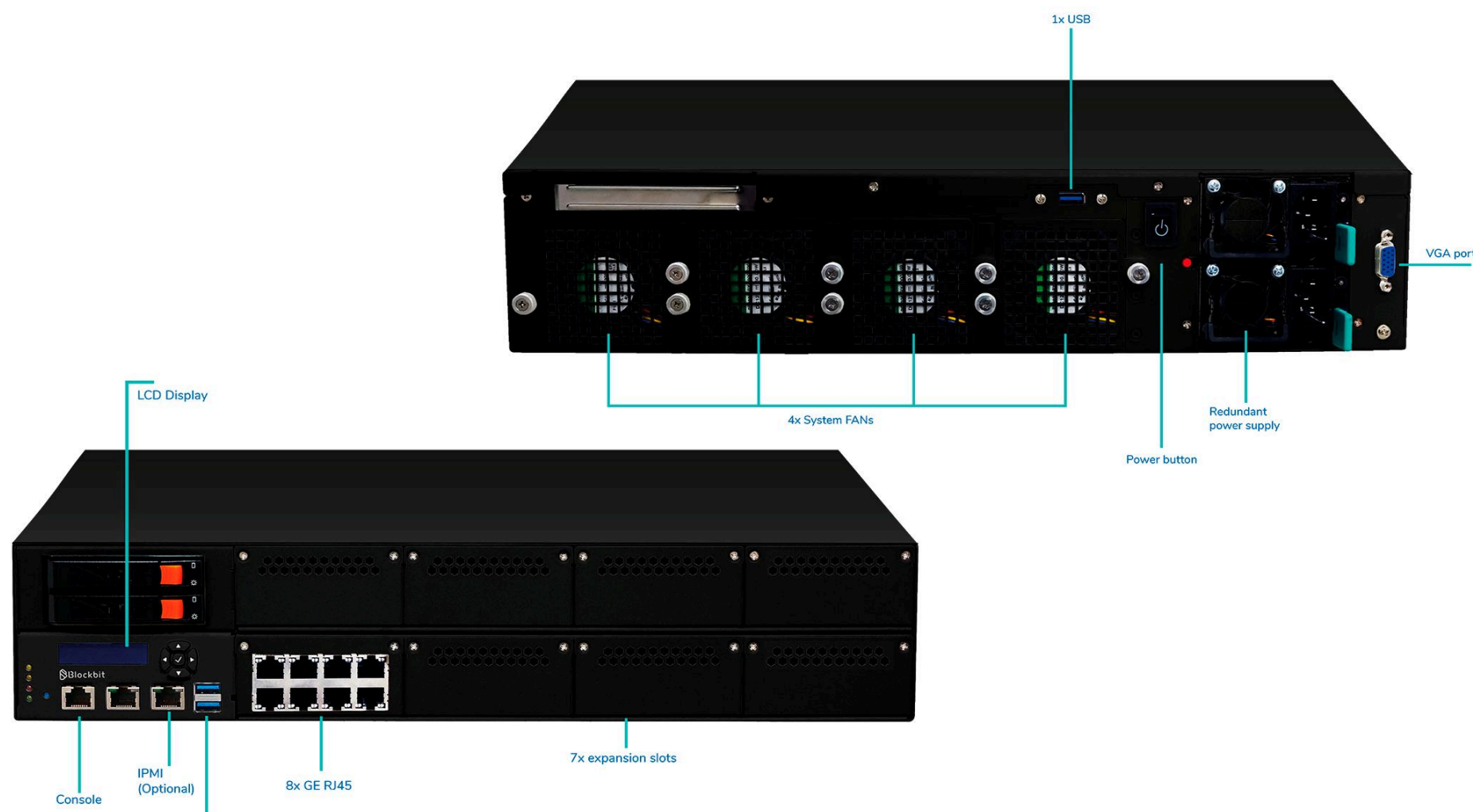
Performance and Optional Specifications

BBX3000



BBX3000	
Type	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 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)
Redundant Power Supply - Hot Swappable - 110/240V - 50~60Hz	YES
SSD Drive	1 TB or 2× 1TB in RAID 0, 1
Disk Upgrade	2TB
Available Slots	7x

BBX3600



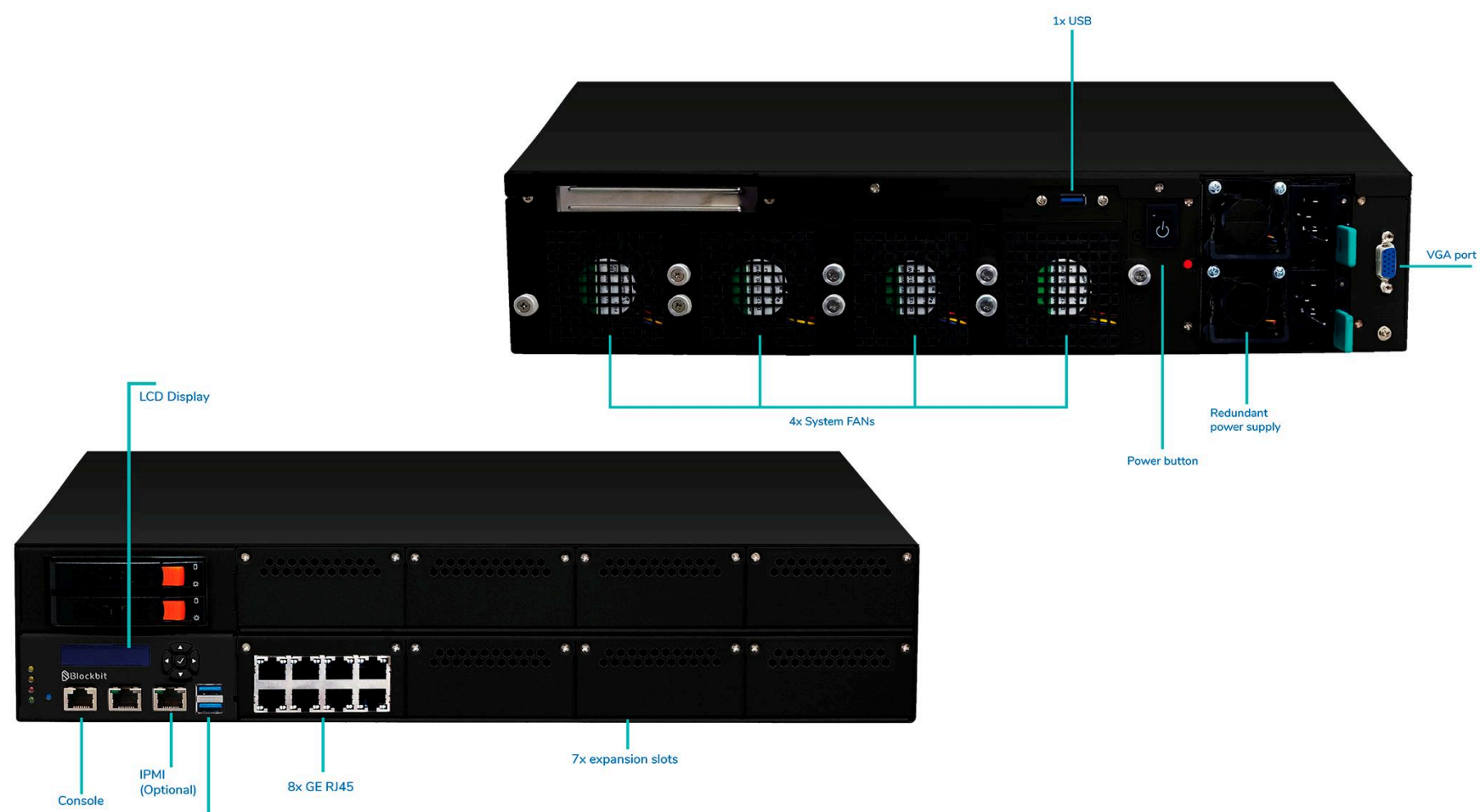
BBX3600	
Type	2U - Rack 19"
Firewall Throughput (UDP)	200 Gbps
Concurrent Connections	45.000.000
New Connections Per Second	400.000
NGFW Throughput (IMIX)	20 Gbps
SSL Inspection Throughput	12 Gbps
IPS Throughput	18 Gbps
Application Control Throughput *	18 Gbps
Threat Protection Throughput	12 Gbps
IPSEC VPN Throughput (AES-256 + SHA256)	55 Gbps
SSL VPN Throughput (AES-256)	10 Gbps
Interfaces UTP 1 GbE	8 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)
Redundant Power Supply - Hot Swappable - 110/240V - 50~60Hz	YES
SSD Drive	1 TB or 2× 1TB in RAID 0, 1
Disk Upgrade	2TB
Available Slots	7x

* Application Control performance uses a proxy-based methodology.

Blockbit Appliances

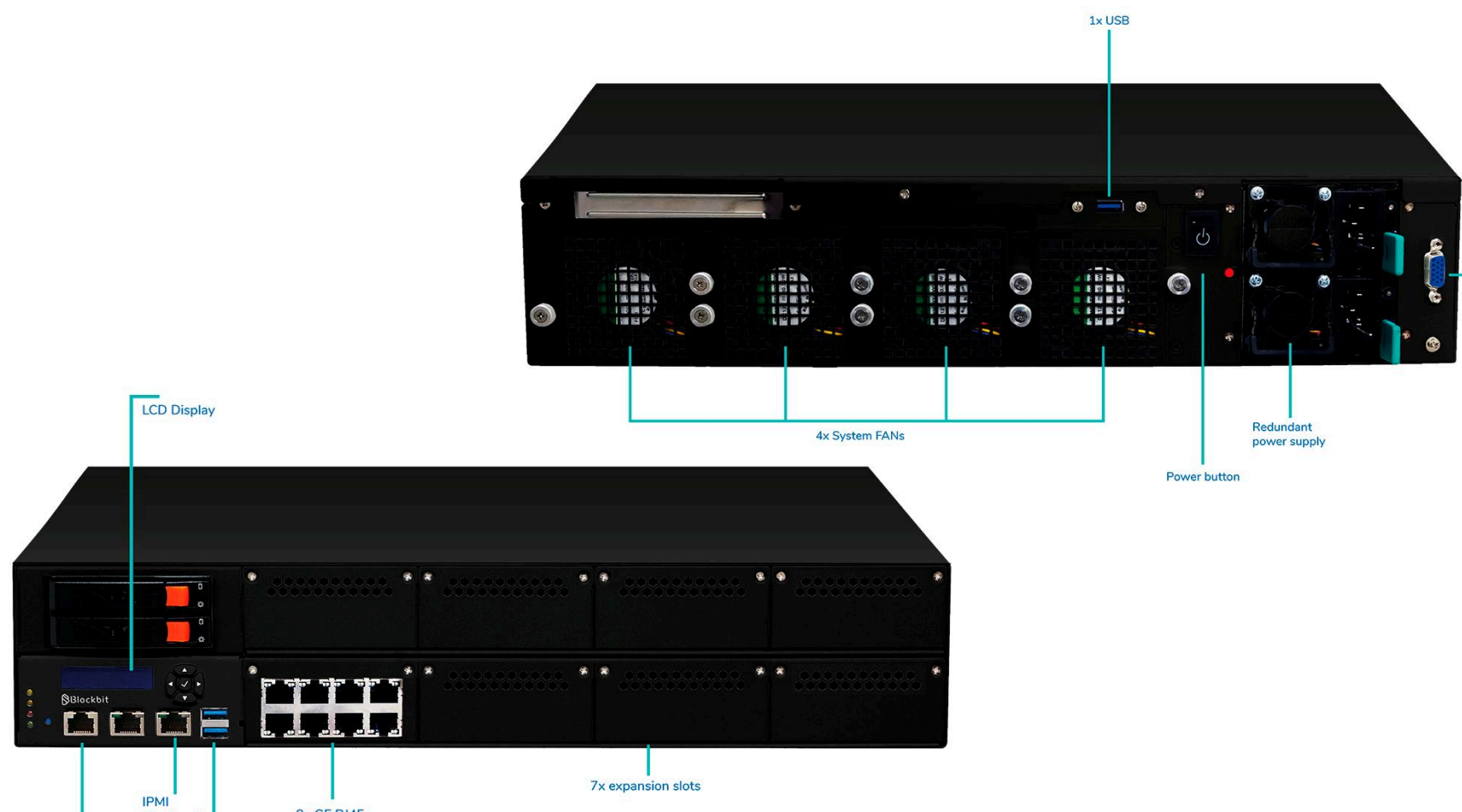
Performance and Optional Specifications

BBX4200



BBX4200	
Type	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 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)
Redundant Power Supply - Hot Swappable - 110/240V - 50~60Hz	YES
SSD Drive	1 TB or 2× 1TB in RAID 0, 1
Disk Upgrade	2TB
Available Slots	7x

BBX5000








BBX5000	
Type	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 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)
Redundant Power Supply - Hot Swappable - 110/240V - 50~60Hz	YES
SSD Drive	1 TB or 2× 1TB in RAID 0, 1
Disk Upgrade	2TB
Available Slots	7x

* Application Control performance uses a proxy-based methodology.

Technical Description

Deployment Options

Hardware Appliance	Virtual Appliance	Cloud Instance
<ul style="list-style-type: none">Maximum performanceGuaranteed stabilityQuick installationLED indicators for interface and power supplies	<ul style="list-style-type: none">Greater scalabilityFaster disaster recoveryInfrastructure optimization	<ul style="list-style-type: none">AWS, Oracle, Azure, Google and IBM <div></div>

Virtual Appliance Model Specifications

Description	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

Images for illustrative purposes only.



Technical Description

Security Policies

- Supports IPv4 and IPv6..
- Source/Destination IP, Port, and Protocol.
- Source/Destination Subnet.
- By users, groups, IPs, networks, Zone (LAN, WAN, DMZ), and country code (BR, USA, etc.).
- Application control, static and dynamic groups.
- Filtering.
- Web content, Web applications.
- Inspection Profiles: SSL, IPS, Threat Protection, Web Filter, and Application Control (implemented in a single policy and changes to one engine do not affect the others).
- QoS (bandwidth control/prioritization).
- Multiple services.
- Security rule editor (filtering policies) with scheduling capability.
- Enable and disable logs.
- Action types: allow, deny, and reject.
- Policy creation by users or groups based on authentication for all services (Firewall, VPN, IPS, Application Control, and others).
- Traffic simulator, policy locator, and validator.
- Conflicting policy detector in NGFW and GSM.
- File blocking by extension and accurate file identification by MIME type, even if the extension is renamed.
- Allows internet traffic monitoring without blocking user access.

Firewall

- Policy with authentication option, allowing log enabling or disabling.
- NAT (SNAT and DNAT), 1:1, N:1, NAT64, NAT46, NAT44, and NAT66, PAT, Source NAT, and Destination NAT simultaneously.
- Dynamic NAT (Many-to-Many and Many-to-1).
- Static NAT (1:1 and Many-to-Many) and bidirectional 1:1.
- NAT 444 (CGNAT).
- Security.
- 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, through RPF (Reverse Path Forwarding) verification.
- ICMP (controls, transmission, redirection).
- PING (Echo/Request).
- Multicast forwarding.
- Source routing, Checksum, invalid logs.
- Flow Control for dynamic applications.
- Blocking of protocol traffic on custom ports.
- Supports multicast objects and rules.
- TCP_be_liberal.
- IP spoofing.
- Protection against Man-in-the-Middle attacks.
- Connection controls for TCP/UDP/ICMP/IP.
- Supports transparent mode (layer 2), gateway mode (layer 3), and port mirroring.
- Supports real-time protocols.
- Supports GPO (SCCM) distribution via Microsoft AD for VPN client.
- Allows internet access control by domain, e.g.: gov.br, org.br, edu.br.
- Queries integrated RADIUS server (NAS); if authorized, the IP address is assigned.
- Allows limiting the maximum number of packets per second in the firewall to prevent distributed attacks or traffic anomalies caused by potential malware on the network.
- Features Stateful firewall technology.

QoS - Quality of Service

- Packet marking for traffic prioritization (TOS and DSCP).
- Priority Queue from Lowest Priority to Highest Priority.
- Traffic control and bandwidth guarantee by policy (applications, users or user groups synchronized with Windows AD or LDAP), network zone, specific host or source/destination.
- Real-time statistics for QoS classes on the WEB Management Interface.
- Supports QoS for LAG interfaces.
- Supports packet transmission without modification, with DSCP value remarking, and packet discarding for traffic exceeding specified bandwidth.
- Allows modification of DSCP values.
- Allows individually limiting the bandwidth used by P2P file-sharing programs.
- Allows defining QoS policies with up to 100% of available bandwidth.

Web Cache and Proxy

- Transparent or Explicit Proxy (customizable ports).
- Support for web services (HTTP and HTTPS versions 1.0, 1.1, 2.0, FTP, POP3, and SMTP).
- Configuration of Disk and Memory Cache size.
- Configuration of web cache in memory and disk.
- Enablement of web cache for dynamic content (Facebook, Google Maps, MSN Video, SourceForge Downloads, Windows Update, YouTube).
- Cache exceptions configurable via regular expressions.
- Proxy hierarchy with and without authentication.
- Support for HTTP Antivirus integration through proxy hierarchy.
- Blocking message for the end user.
- Supports time-based policy by schedule and/or period (day, month, year, weekday, and hour).
- Supports user groups, IPs, networks, and/or security zones.
- Enables integration with external web cache servers.
- Ability to exclude specific URLs from web cache, configurable by keyword list with support for regular expressions.
- Allows configuring the Explicit Proxy port.

IPS – Intrusion Prevention System

- Detection and prevention of attacks and intrusions based on +80k signatures grouped as Client (Applications) and Server (Servers).
- Support for Customization and upload of Signatures on 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 packets after analysis for attack identification.
- Source Session Limit with TCP Reset for session termination.
- DoS, DDoS (Flood, Scan, Session, and Sweep), PORTSCAN, Reconnaissance, Evasion, and ICMP prevention.
- Mitigation of DoS and DDoS attacks (denial of service).
- Prevention against P2P technology attacks.
- Prevention against Worm, Trojan, Backdoors, Portscans (detects and blocks the source), IP Spoofing, SYN-ICMP-UDP flood, and Spywares.
- Prevention against protocol anomalies (HTTP, SMTP, POP, IMAP, Sendmail, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, CIFS, RPC, RDP, CHARGEN, SSDP, SNMP, TCP highjacking, SSH, and Telnet).
- Prevention against Botnet, DNS Poisoning, and Escalation Privilege.
- Blocking of SSH on non-standard protocol ports and based on behavior through patterns.
- Log of incidents for each identified attack type.
- Malformed traffic and invalid headers.
- Automatic and periodic updates.
- Decodes multiple Unicode formats.
- IP fragmentation and defragmentation.
- Policies applied to interfaces or security zones.
- Alarm via email or SNMP trap.
- Supports Inline L2 (bridge/transparent mode) and L3 (firewall) implementation, and port mirroring.
- Supports exceptions by IP registered in the rules.
- Creation of Whitelist and Blacklist by IP (IPv4 and IPv6).
- Allows activating or deactivating signatures, or enabling them in monitoring mode.
- Allows analysis and log generation, blocks and quarantines the attacker's IP for a period of time.
- Allows using negation operators in the creation of custom IPS signatures, enabling the creation of exceptions with configuration granularity.
- Registers the following information about identified threats in the monitoring console: the name of the signature or attack, application, user, origin and destination of the communication, in addition to the action taken by the device.
- Appliance-based intrusion detection functionality.
- Allows defining the number of packets to be captured by IPS signatures, or allows capturing the packet that triggered the alert as well as its context, facilitating forensic analysis and identification of false positives.
- Has alarms in the administration console.
- Active response/log capability to attacks.

Threat Protection

- Antivirus and Anti-Malware with real-time analysis.
- HTTP, HTTPS, FTP, SMB, CIFS, POP3 and SMTP (natively supported by the solution).
- Protection against unauthorized applications.
- Protection against password-protected files.
- Anti-Malware quarantine.
- Report of scanned files.
- Identifies, classifies, and blocks malware such as trojans, spyware, adware, keyloggers, hijackers, worms, viruses, C&C (Command and Control) connections, and Anti-bot (Botnet).
- Allows blocking by address reputation classified into six categories: spam, reputation, malware, attacks, anonymous, and abuse.
- Automatic and periodic updates.
- Antibot features multilayer detection mechanisms, such as IP address reputation, URLs, and DNS addresses, and detects communication patterns and signatures.
- Blocks files by extension and also identifies them by MIME type, even if the extension is changed.
- Flow-based inspection, detection, and prevention.
- Specific actions for different types of malicious code.

Technical Description

SD-WAN

- Supports multiple configuration profiles and allows activation on any WAN interface (DSL, MPLS, 3G/4G LTE) and Packet Duplication (PD), with VPN aggregation capability. Supports static and dynamic routing (OSPF, BGP), IPv4/IPv6, and both dynamic and outbound NAT.
- Allows traffic forwarding definition by selected interface and supports Policy-Based Routing.
 - Failover, Load Balance, Spillover and Performance.
- Monitors link availability and protects against data link degradation.
- Supports link balancing by source and destination IP hash, by weight with configurable percentage, and supports 2 to 9 links.
- Link failure detection via TCP/UDP Echo, ICMP (ping), and HTTP protocols.
- Measures bandwidth consumption, packet loss, jitter, and latency (monitoring multiple destinations across all interfaces), with support for more than 3 targets and customizable thresholds.
- Application- and policy-based routing for multiple WAN paths, with app blocking.
- Customizable link fallback (1 to 100) and link persistence.
- Implements link load balancing without the need to create zones or use virtual instances.
- Group-based routing in SD-WAN rules, with traffic balancing by sessions and packets.
- Supports LTE (3G/4G) for link load balancing and failover.
- Allows the use of IPsec VPN to interconnect remote sites.
- SD-WAN policies dynamically adapt according to available bandwidth.
- Link check intervals can be customized in seconds.
- Allows traffic distribution based on the number of active connections or sessions per link.
- Supports traffic balancing based on volume definition.
- Enables traffic routing based on source and/or destination IP addresses.

Secure Web Gateway

- The following features are appliance-based.
- Content Filtering (without NAT).
- 88 categories (including Government, Webmail, Healthcare Institutions, News, Pornography, Restaurants, Social Networks, Sports, Education, Games, and Shopping), over 49 million cataloged URLs, login control by domain on Google, SafeSearch integration with Google, Bing, and Yahoo, and block message displayed to the end user.
- SSL inspection with invalid certificate blocking.
 - Integration with ATP inspection and Windows AD / LDAP for user and group identification.
- Blocking of social network applications such as: 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, ZohoChat, and other chat applications.
- Blocking of file types: Office, Java, JavaScript, Cookies, ActiveX, Multimedia, and Images.
- Application Recognition – DPI (Deep Packet Inspection).
- Identifies applications through SSL, HTTP, HTTPS protocols, or non-standard access ports.
- SNI-based control by category.
- Web filtering, categorization, and reclassification by URL.
- User authentication via LDAP, RADIUS, TACACS+, and Microsoft Active Directory.
- Blocking through the creation of specific filters with text-based search mechanisms.
- Custom lists (whitelist and blacklist).
- Captive Portal with social login (Facebook, Twitter, Google).
- Browsing quotas by time and/or traffic volume.
- Scheduled and automatic updates in transparent mode.
- Application recognition regardless of port or protocol.
- Detects evasive tactics used by applications attempting to use encrypted connections (e.g., Skype or TOR network).
- Customizable block message.
- Recognition of over 4,000 applications.
- More than 19 categories for application classification.
- Allows application traffic monitoring without blocking user access.
- Regular product updates occur without interrupting application control or web content filtering services.
- Includes DNS Content Filter.
- Supports detection techniques for peer-to-peer (P2P) file-sharing programs and instant messaging, including: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, WhatsApp, WeChat, Snapchat, BitTorrent, uTorrent, Vuze, eDonkey, GNUTella, Skype, and Microsoft Teams.
- Enables granular control of P2P traffic for various software (e.g., BitTorrent, eMule, etc.).
- Enables granular control of instant messaging traffic.
- Enables granular control of proxy applications.
- Allows application blocking and allowance without requiring port or protocol permissions.
 - Allows port control to be applied to all applications.
- Identifies applications through behavioral traffic analysis, including P2P and VoIP.
- Decrypts SSL traffic for payload inspection and application signature verification.
- Enables application control in all security rules (IPv4 and IPv6).
- Supports control of both known and unknown applications.
- Allows creation of custom signatures for proprietary application recognition via web interface, using regular expressions, without vendor intervention.
- Allows requests for application inclusion in the signature database via the vendor.
- Supports alert notifications when an application is blocked.
- Allows creation of static and dynamic application groups based on attributes such as risk level, technology, and category.

Interface WEB and CLI

- Granularity (read-only and read/write profiles, configuration application, etc.) of administrator access on the Web Interface with simultaneous sessions.
- CLI (Command Line Interface for management and diagnostics via SSH and serial RS-232/RJ-45).
- Proprietary Web Interface available in Portuguese, English, and Spanish, accessible via any physical interface of the product.
- Management (LAN or WAN) via WEB (HTTPS through browser) and SSHv2, using cryptographic keys of at least 16 bits.
- Supports web console access via HTTP and CLI via TELNET.
- Allows changing the default port for administration interface access via HTTP, HTTPS, and CLI.

Zero-touch Provisioning

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

Authentication

- User Authentication.
 - Local, Windows AD, LDAP, Windows SSO (Single Sign-On via Kerberos), and WMI – unified authentication, X-Auth for VPN services, authentication via RADIUS servers, RSSO (RADIUS Single Sign-On), password complexity enforcement, Token ID, and session/application-based authentication for TCP (HTTP, HTTPS, FTP, and TELNET) / UDP / ICMP.
 - TACACS+ and LDAP support for administration and firewall users.
 - User, group, and host synchronization with Windows AD and LDAP servers, including replication of established user sessions.
 - AAA (Authentication, Authorization, and Accounting).
 - AD-based identification allows the use of SSO, so users don't need to log in again to browse through the firewall.
 - Supports authentication for Firewall and VPN using Tokens, TACACS, RADIUS, LDAP/AD, and digital certificates.
 - Encrypted access control packets for authentication servers.

Networks and Interfaces

- Interfaces.
 - Ethernet (with support for FEC – Forward Error Correction).
 - VLAN (IEEE 802.1q) with up to 4094 IDs per interface.
 - VLAN Trunking with support for multiple VLANs per trunk.
 - WAN support: ADSL/DSL, MPLS, LTE (3G/4G/5G).
 - Alias (Virtual IP).
 - Link aggregation.
 - Ethernet bonding (802.3ad) LACP.
 - Dynamic Routing: BGP4/BGP4+, OSPFv2/v3, RIPv1/v2, and PIM-SM/PIM-DM.
 - Support for MD5 authentication between OSPF peers.
 - Support for multiple independent and simultaneous OSPF routing processes.
 - Supports OSPF graceful restart.
 - Support for BFD (Bidirectional Forwarding Detection) for BGP.
 - Static Routing (IPv4 and IPv6) with ECMP support.
 - Multicast Routing: supports rules and objects.
 - Native support for IPv4 and IPv6.
 - DHCP (dynamic host configuration protocol) IPv4 and IPv6.
 - Relay, Server and Client.
 - Recursive DNS.
 - Policy-Based Routing (PBR or PBF – Policy Based Forwarding).
 - Supports logical Ethernet sub-interfaces.

Monitoring

- Support for SNMP protocol v1, v2, and v3, monitoring CPU usage, memory, disk space, VPN, cluster status, and security violations.
 - Performance, simultaneous connections, DHCP lease, authenticated users, and enabled or disabled services.
 - System and Security notifications.
 - Detailed event viewing window.
 - Disk maintenance tool and real-time network traffic monitoring (Live Sessions and Traffic Monitor) with throughput and concurrent connection data.
 - Security and Threat Event Logs.
 - Allows traffic capture and download in PCAP format.
 - User logging in authentication, access, blocking, and threat events.

Data Filter

- Has a feature capable of identifying and preventing the transfer of various file types (MS Office, PDF, etc.) identified over applications (HTTP, HTTPS, FTP, SMTP).
- Capable of identifying compressed files on the data network and applying usage policies to the content of these file types.
- Supports Antispam DLP (Data Loss Prevention) feature.

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 storage with configurable number of copies.
- Scheduled Backup (Snapshot or System) through the graphical interface.

Technical Description

VPN IPSEC and VPN SSL

- VPN Tunnel (LAN-to-LAN) / Site-to-Site and Client-to-Site.
- RAS/SSL VPN (Remote Access): allows access via VPN client or directly through the browser (Web Interface), meaning SSL VPN can be used with or without an agent.
- SSL VPN Portal via HTTPS for RDP, VNC, SSH, WEB, and SMB access (no need for JAVA), with secure session connections.
- VPN client compatibility with Windows 7, 8, 8.1, 10, and 11 (32 and 64-bit), Linux, macOS, Android, and iOS.
- Authentication.
- Allows enabling, disabling, restarting, and updating IKE, Gateways, and IPsec VPN tunnels via graphical interface.
- Supports PSK (Pre-Shared Key), XAuth (AD, local LDAP, RADIUS), IKE P1 digital certificate, and EAP (MSCHAPv2).
- Tunnels can be established before user login, after login, or on demand.
- Native IPsec VPN authentication using MD5, SHA-1, SHA-256, SHA-384, SHA-512, and AES-XCBC.
- High Availability.
- Supports FQDN (Fully Qualified Domain Name) and DDNS.
- NAT-T (UDP encapsulation) and DPD (Dead Peer Detection).
- IKEv1 exchange modes: Main Mode or Aggressive Mode.
- Data compression support.
- Protocols:
 - IKEv1 e IKEv2 (Phase 1 and 2) and ESP.
 - Symmetric encryption: AES-128, AES-192, AES-256, 3DES.
 - Asymmetric encryption: 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.
- Auto-Discovery VPN (AD-VPN) support, allowing multiple devices (Spokes) with a centralized gateway (Hub) and Site-to-Site connections. Supports tunnel types such as Site-to-Site, Full Mesh, and Star.
- Supports RSA and Diffie-Hellman algorithms.
- SSL VPN with support for X.509 v3 digital certificates.
- Supports the enrollment of certification authorities via SCEP (Simple Certificate Enrollment Protocol).
- Support for Dynamic Public IP, RIPv2 routing, and OSPFv3.
- Support for certificates issued by certification authorities following the ICP-Brasil standard.
- Support for Certificate Revocation List (CRL) verification.
- Support for multiple hubs in hub-and-spoke topologies.
- Supports traffic isolation based on services and destinations (IoT, Banking Network, Guest Network).
- Appliance-based VPN functionality.
- Support for encryption algorithms: 3DES, AES-128, AES-256, AES-GCM-128.
- Includes Auto-Discovery VPN (AD-VPN) capabilities, enabling the creation of dynamic tunnels for multiple devices (spokes) with a centralized gateway (hub).
- The AD-VPN functionality supports the following tunnel types: Full-Mesh, Site-to-Site, and Star.
- Support for configuration via Virtual Interface in the setup of site-to-site VPN tunnels with SD-WAN Protection.
- The client-to-site VPN supports automatic VPN establishment over ICMP or DNS (UDP/53) if the remote client detects that the default port is being blocked.
- Includes a feature to configure multiple simultaneous tunnels in the client-to-site VPN, with optimization for traffic performance.
- SSL and IPsec VPN (client-to-site) with Blockbit Client for Windows.
- Allows DNS assignment to remote VPN clients.
- Clientless VPN (IPSec and SSL) without vendor restrictions.
- SSL certificate management (X.509).
- Allows all traffic from remote VPN users to be routed through the VPN tunnel, preventing direct communication with local devices such as proxies.
- Allows the use of IPsec VPN to interconnect remote sites.
- Offers interoperability with any vendors that use the IPsec standard.
- Allows the creation of policies for Application Control, IPS, Antivirus, Anti-Spyware, and URL Filtering for traffic from connected remote clients.
- Supports automatic distribution of the VPN agent to desktops and laptops via GPO or direct download through the portal.
- Allows applying the DiffServ code to the ESP packet.

Logs and Reports

- Netflow / IPFIX Support.
- Session Log, Authentication, and VPN Reports, per single or consolidated device.
- Customizable Analyzer report creation (native in the tool) for Firewall, Web Filter, Application Control, IPS, ATP, VPN, and User Behavior services (including IP information, user Operating System, Hostname, and "top 10" style threat classification).
- Remote Syslog for sending logs and log export via SCP, supports log sending via SSL protocol.
- Report export in multiple formats (PDF, CSV, HTML).
- Events identify the country of origin of the attack.
- Events record changes in the state and health of SD-WAN links.
- Reports with historical link health monitoring.
- Generation of historical reports by period.
- Has logs and reports of web Browse time for websites.

H.A. (High Availability)

- Mirroring of firewall sessions, user authentication, and synchronizes all configurations, sections, certificates for SSL inspection, IPsec VPN SAs (Security Associations), and all signatures for ATP, Application Control, IPS, and WEB Filter, between the primary and secondary devices so that the switchover is transparent and fast.
- Monitoring of interfaces, in case of link failure.
- High Availability Cluster system (Active-Passive/Active-Active, with identical equipment only) with maintenance of established sessions, traffic distribution, state table maintenance, session balancing in multiple availability zones.
- Server synchronization is performed via an exclusive Heartbeat interface.
- In case of primary active equipment failure, the secondary equipment takes over transparently, with no impact to the user or loss of service.
- Supports the persistence of user sessions and established connections between High Availability members.

Sandboxing - APT

- Allows mitigating advanced persistent threats (APT and Zero-Day), through dynamic analysis for the identification of unknown malware with automatic updates in a threat intelligence network database. Analyzes PDF, Microsoft Office, executable, and compressed file types.
- Capable of creating signatures and including them in the firewall's antivirus database, preventing attack reoccurrence.
- Supports including URLs identified as sources of such unknown threats in the firewall's blacklist, preventing these addresses from being accessed by network users again.
- The APT module supports file analysis by antivirus, cloud query, code emulation, sandboxing, and callback verification, and analyzes the behavior of suspicious files in a controlled environment, in real-time.
- Capable of emulating, detecting, and blocking any malware and/or malicious code.
- Emulates sandbox environments for various Microsoft versions and Office.

User Identification

- Allows the creation of policies based on URL control and URL categories.
- Allows the creation of 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.
- Compatible with Microsoft Active Directory (Windows 2003, 2012, and 2019) for identifying users and groups, machines/computers, enabling granular 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.
- Enables control, without installing client software, on devices requesting internet access, so that before browsing begins, an authentication portal hosted on the firewall is displayed (Captive Portal).
- Supports the identification of multiple users connected to the same IP address in Citrix and Microsoft Terminal Server environments, allowing granular visibility and control per user over application usage within these services.
- Allows the creation of custom user groups on the firewall, based on LDAP/AD attributes.
- Allows the creation of administration groups with different access profiles.
- Monitor Profile: Read-only.
- Operator Profile: Read/Write, no permission to disable interfaces.
- Administrator Profile: Read/Write/Modify.
- Supports multiple Authentication Servers (MS AD and/or LDAP) operating in failover mode.

GSM - Centralized Management

- Reboot or shutdown (NGFW/SD-WAN) via centralized management.
- Supports automations for management activities, e.g., rule synchronization, centralized management and orchestration.
- Centralized update and rollback.
- Supports alerts via email, SNMP, and Syslog via centralized management.
- Log centralization through centralized management.
- Supports groups for authentication servers.
- Supports authentication via X509v3 certificates.
- Supports revoked certificates (LCR).
- Supports simultaneous access by multiple administrators, with an option to block changes to prevent conflicts during concurrent sessions.
- Visualization and comparison of current and historical configurations with artificial intelligence support.
- Visualization of inventoried devices through online geolocation maps.
- Allows duplication of existing reports.
- Allows customization of graphs and reports.
- Allows the creation of customized panels (Dashboards) for traffic visibility.
- Offers drill-down functionality for real-time report detailing.
- Sending reports by email with customized recipient definition per report.
- Displays the total number of generated logs via the graphical interface.
- Allows performance analysis and problem detection based on generated logs.
- Export of logs via HTML, PDF, and CSV.
- Displays consolidated information from logs generated by a Device or group of Devices.

Technical Description

Other Features

- Proxy Services (SSH, SMB/CIFS, HTTP, FTP, SMTP, POP3).
- Supports VoIP (SIP/H.323) and RTP over IPv4/IPv6.
- Supports multiple Authentication domains.
- Supports fail-closed and optional fail-open interface (bypass).
- Transparent, automatic, periodic, and offline updates.
- Supports session authentication for all protocols and any applications.
- Resource objects.
- IP addresses, MAC addresses, port and protocol services, time tables, period and date tables, dictionaries (set of words and/or regular expressions), content types.
- Supports NTP (Network Time Protocol) servers for date and time updates.
- Option for automatic and periodic system updates for corrections and releases via web HTTPS or GSM.
- TCP Flow Optimization.
- Has packet flow in Forwarding and Control modes.
- Supports access via SSH, CLI, client, or web (HTTPS).
- Virtualization of the appliance in Public Cloud (Google Cloud®, Azure®, Oracle Cloud®, and AWS®) or Private Cloud (VmWare®, Citrix XenCenter®, and ProxMox®).
- Supports Context (Virtual Domain).
- All policies support application control.
- Supports various methods of identifying and classifying applications, e.g., signature checking and protocol decoding.
- Allows the creation of custom signatures in the WEB interface for application and IDS/IPS recognition.
- Allows requests for inclusion of applications in the standard database.
- Supports granularity in IPS, Antivirus, AntiSpam, and Anti-Spyware policies, enabling the creation of different policies per security zone, source address, destination address, service, and the combination of all these items.
- Provides protection against viruses in HTML and Javascript content, spyware, and Worms.
- Protection against involuntary downloads via HTTP of executable and/or malicious files.
- Allows the configuration of different threat and attack control policies based on firewall policies considering users, user groups, source, destination, security zones, MAC Address; each firewall policy can have a different IPS configuration, with these policies being for users, user groups, source, destination, and security zones.
- Supports Virtual Systems (VDOM) on all models.
- VDOM System allows creating virtual contexts with support for creating multiple administrators.
- Supports TLS 1.2 and TLS 1.3.
- Supports creating block or allow policies by geolocation and informs the origin and/or destination country in the logs with a flag to facilitate traffic identification.
- Supports dynamic site categorization.
- Site reclassification via the manufacturer's portal.
- Supports multiple simultaneous accesses.
- Validation of security policies to identify duplicate or overlapping rules.
- Statistical reports of simultaneous connections.
- VPN usage reports.
- Statistical traffic reports (Input and Output).
- Supports license expiration notification in the alerts window with the remaining days until the expiration date.
- Snapshot Restore without running the Wizard and without licensing.
- Any network interface of the appliance can be used for management, i.e., there is no exclusive interface for management function.
- Allows access to the web management interface via any configured network interface.
- Allows scheduling of services.
- Enables configuration of connection protocol response timeouts, and supports defining standard ICMP timeout options, TCP establishment, SYN transmission in TCP sessions.
- Has a single security policy configuration window where it's possible to insert WEB Proxy, IPS, APP control, SD-WAN, and ATP profiles.
- Allows implementing IPS filters, WEB Filter, Threat Protection, SSL Inspection, Application Control, as well as application routing by SD-WAN and DoS rate limiting by packets in a single policy.
- Displays within the policy itself which modules are enabled, without needing to edit the protection rule.
- Enables editing of linked objects without the need to recreate the policy.
- Enables policy duplication, optimizing configuration time.
- Allows access to the CLI management interface physically on the appliance.
- The USB interface supports the use of 3G/4G/LTE modems for internet link connection.
- Supports Connected Education Meter (SIMET/nic.br).

Some RFCs supported by 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 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: 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.

THE TESTS WERE CONDUCTED IN A LABORATORY ENVIRONMENT WITHOUT SUMMARIZATION BY USERS, IPS, OR SERVICES, AND WITH APPLICATION DETECTORS DISABLED. FIREWALL UDP THROUGHPUT: 1518 BYTE PACKETS. FIREWALL HTTP GET THROUGHPUT: 1280K*. IPS/ATP THROUGHPUT WITH FACTORY DEFAULT SIGNATURES ENABLED. NGFW IS MEASURED WITH FIREWALL, THREAT PROTECTION, IPS, AND APPLICATION CONTROL ENABLED, USING IMIX TRAFFIC.

Some RFCs supported by Blockbit Platform

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.

Encryption

- 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.

THE TESTS WERE CONDUCTED IN A LABORATORY ENVIRONMENT WITHOUT SUMMARIZATION BY USERS, IPS, OR SERVICES, AND WITH APPLICATION DETECTORS DISABLED. FIREWALL UDP THROUGHPUT: 1518 BYTE PACKETS. FIREWALL HTTP GET THROUGHPUT: 1280K*. IPS/ATP THROUGHPUT WITH FACTORY DEFAULT SIGNATURES ENABLED. NGFW IS MEASURED WITH FIREWALL, THREAT PROTECTION, IPS, AND APPLICATION CONTROL ENABLED, USING IMIX TRAFFIC.