

DATASHEET

BT - NS Series



BYTESCREEN
CONNECT • DETECT • PROTECT

ByteSecure ByteScreen NGFW

“Secure Every Byte with Bytescreen”



Bytescreen provides a comprehensive suite of advanced network solutions designed to enhance security, connectivity, and management. Built on a hardened, crash-free OS for maximum uptime, our Next-Generation Firewall (NGFW) offers robust protection featuring multi-core intrusion prevention, AI-assisted threat detection, deep packet inspection (DPI), and precise user identification to guard against evolving cyber threats.

The BT-NS Series features a self-healing SD-WAN solution that simplifies network management through software-defined technology and zero-touch deployment, ensuring automatic failover, improved performance, and cost efficiency. Our centralized Network Management System (NMS)—FusionMaestro—allows unified orchestration and monitoring of network devices via GUI and REST APIs for proactive issue resolution. Additionally, the robust AAA framework secures network access, manages authentication, and tracks activities to maintain a secure, compliant environment. Together, these solutions empower organizations to seamlessly enhance security, streamline operations, and optimize performance.

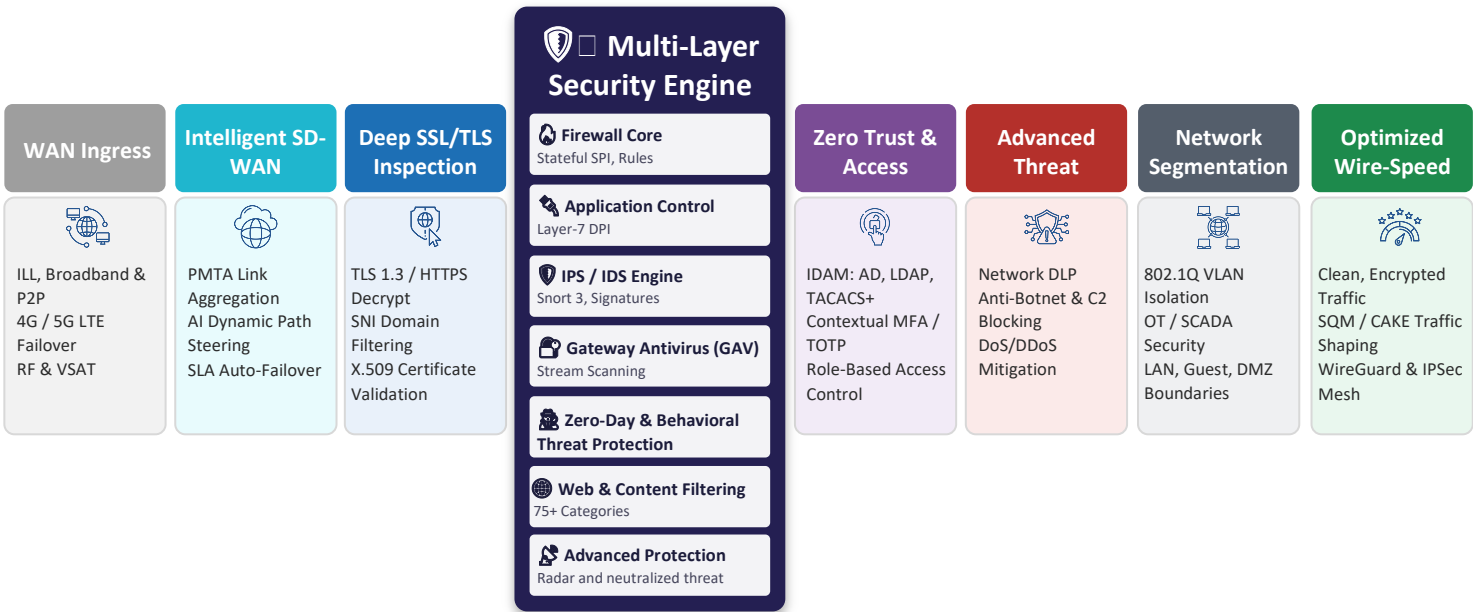
Core Platform Pillars

- **Hardened & Crash-Free OS:** Optimized for hardware resources, maximum uptime, and enterprise reliability.
- **Real-Time Threat Prevention:** Multi-core IPS, DPI, and malware protection backed by continuously updated threat intelligence.
- **Self-Healing SD-WAN & Multi-WAN:** Automatic link failover (including 4G/5G), and intelligent application-aware path optimization.
- **Advanced VPN & Encryption:** A complete secure connectivity suite including IKEv2 IPsec, SSL VPN, GRE, and WireGuard.
- **Identity & Access Control:** Centralized login via TACACS+, AD, LDAP, and robust Two-Factor Authentication (TOTP).
- **Assured Performance (QoS):** Class-based traffic shaping and Smart Queue Management to guarantee bandwidth for critical applications.
- **Fusion Maestro:** Zero-touch branch onboarding and unified fleet configuration through a single management baseline.
- **Unified Security Alerting:** Real-time operational and security events delivered via SMS, Email, WhatsApp, Telegram, and Syslog.



Single-Pass Multi-Layer Security Architecture

The Bytescreen BT-NS Series engine utilizes a hardware-accelerated, single-pass inspection pipeline designed to eliminate latency while maintaining deep threat visibility. Traffic entering via physical uplinks or SD-WAN tunnels undergoes wire-speed session parsing and SSL/TLS decryption before reaching concurrent security engines



Single-Pass Architecture:

Ingress Hardware Decryption → Concurrent Layer-7 Deep Inspection → Zero-Trust Identity Enforcement → Multi-Engine Threat Neutralization → Wire-Speed Zero-Loss Zone Delivery.

Core Pipeline Capabilities

- ◇ **Intelligent Ingress & PMTA:** Bonds multi-WAN uplinks (ILL, Broadband, 4G/5G) with real-time SLA link steering.
- ◇ **SSL/TLS Decryption:** Offloads TLS 1.2/1.3 traffic to inspect encrypted sessions at line speed.
- ◇ **Single-Pass Engine:** Scans packets concurrently across Stateful ACL, Snort 3 IPS, Gateway AV, Layer-7 DPI, and Content Filtering.
- ◇ **Zero-Trust Policy:** Enforces least-privilege access using Active Directory, LDAP, and device posture checks.
- ◇ **Advanced Threat Defenses:** Blocks zero-day exploits using inline heuristics, Network DLP, and NDR analytics.
- ◇ **Micro segmented Delivery:** Routes clean traffic into isolated corporate VLANs, DMZ clusters, and guest portals.

Unified Security Architecture

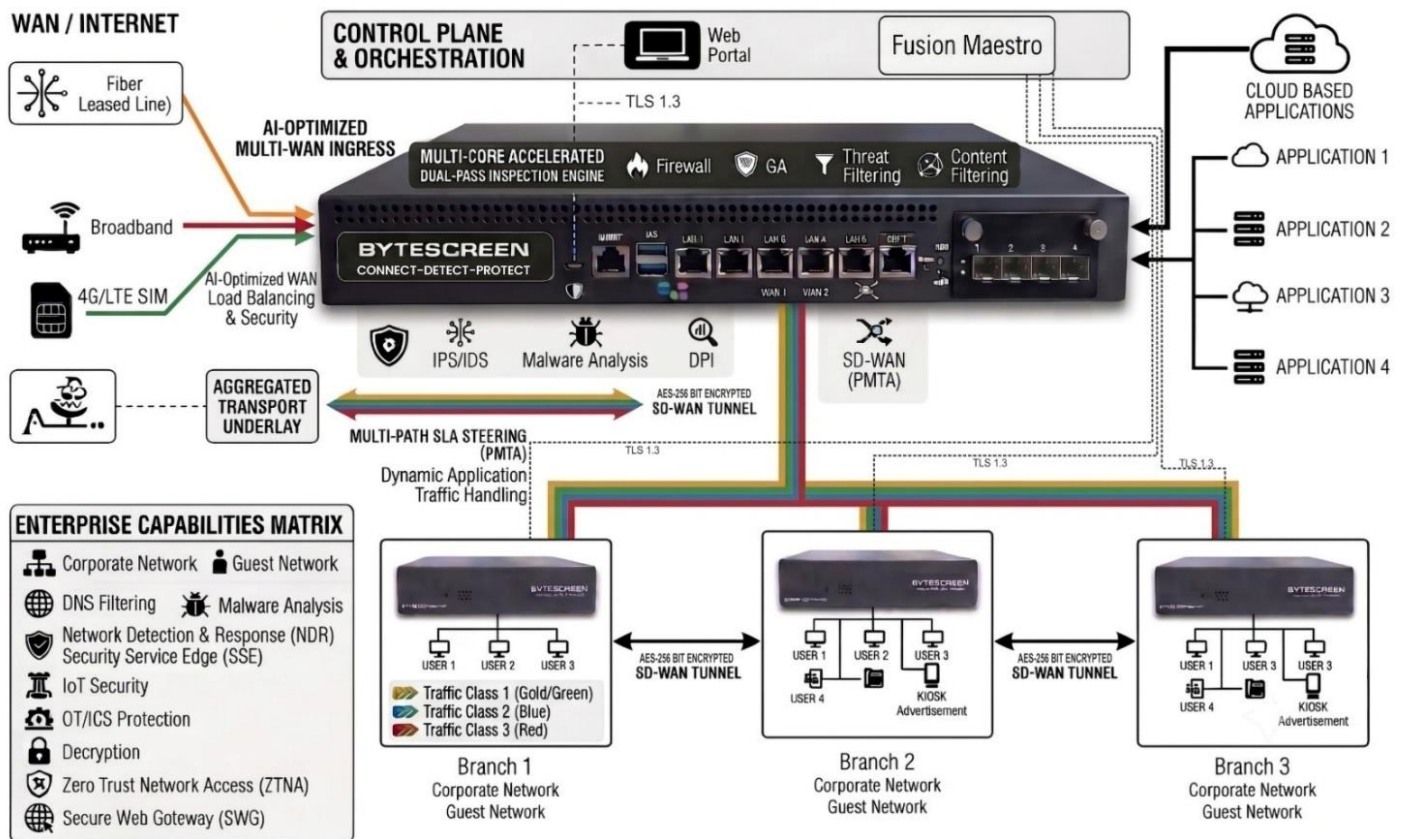
The Bytescreen BT-NS engine processes ingress packets through a single-pass inspection pipeline. Incoming WAN streams undergo zero-overhead SSL/TLS decryption and session parsing before reaching deep inspection engines. Stateful ACLs, Snort 3-based multi-core IPS/IDS, Gateway Anti-Virus, Layer-7 Application Control, and Content Filtering inspect payload data simultaneously to prevent latency accumulation while enforcing granular Zero-Trust policies across internal network zones

Self-Healing SD-WAN & Multi-Path Optimization (PMTA)

Deploying as a high-capacity hub or edge node, BT-NS automates multi-link aggregation across leased lines, broadband, and 4G/5G interfaces. Through Packet-based Multi-Tunnel Aggregation (PMTA) and real-time SLA link steering, critical application traffic dynamically routes over optimal paths while maintaining full-mesh, AES-256 encrypted overlay tunnels back to HQ and interconnected branches with zero-touch onboarding via Fusion Maestro.

BYTESCREEN NETWORK ARCHITECTURE

High Performance * Secure * Resilient * Centrally Managed



Platform: Physical Appliance | Virtual Appliance

Environment: On-Premises | Private Cloud | Public Cloud | Hybrid Cloud

Network Deployment: Gateway / Routing Mode | Bridge / Transparent Mode | High Availability (HA) | SD-WAN Deployment

BT-NS supports flexible deployment across physical and virtual environments, including on-premises, private, public and hybrid cloud infrastructures, with multiple network deployment options to meet different security and connectivity requirements.

Hardware Specifications & Performance Overview

The **Bytescreen BT-NS Series** is a scalable family of enterprise Next-Generation Firewall (NGFW) appliances designed to address a wide range of network security and deployment requirements. Built on a unified and hardened security architecture, the BT-NS platform combines purpose-built hardware, scalable processing capabilities, and consistent security functionality across its appliance portfolio.

The BT-NS portfolio includes multiple appliance series, with each series comprising different models designed to provide varying levels of performance, capacity, and scalability. This portfolio structure enables organizations to select the appropriate appliance based on network size, traffic requirements, security services, user capacity, and deployment needs.

Each appliance model within the BT-NS portfolio is engineered with a defined performance and user-capacity profile, allowing customers to select the model that best aligns with their specific network and security requirements.

BT-NS 100 Series

Product Specifications



Model	BT-NS50	BT-NS100
Ethernet Interfaces	4 x 2.5GbE	4 x 2.5GbE
SIM Support (4G / 5G)	Optional	Optional
Concurrent Sessions	1,200,000	1,500,000
New Sessions per Second	24,000	30,000
Firewall Throughput (Mbps)	1,850	2,350
NGFW Throughput (Mbps)	750	950
Firewall IMIX Throughput (Mbps)	1,100	1,400
IPS Throughput (Mbps)	850	1,100
Threat Prevention Throughput (Mbps)	500	650
SSL Inspection Throughput (Mbps)	275	350
VPN Throughput (Site-to-Site) (Mbps)	900	1,150
VPN Throughput (Remote Access) (Mbps)	400	500
VPN Tunnels (Max)	50	50
PMTA Tunnel	50	50
High Availability (HA)	YES	YES
Processor	Multi-Core	Multi-Core
RAM	8 GB	8 GB
Power Supplies	SINGLE	SINGLE
Operating Temperature	10°C to 65°C	10°C to 65°C
Operating Humidity	10% to 90%	10% to 90%

BT-NS 300 Series

Product Specifications



Model	BT-NS200	BT-NS300
Ethernet Interfaces	4 x 2.5GE, 4 x 1G SFP	4 x 2.5GE, 4 x 10G SFP+
SIM Support (4G / 5G)	1x 4G (Optional)	1x 4G (Optional)
Concurrent Sessions	4,000,000	5,000,000
New Sessions per Second	100,000	125,000
Firewall Throughput (Mbps)	8,500	18,500
NGFW Throughput (Mbps)	4,200	4,500
Firewall IMIX Throughput (Mbps)	6,800	13,500
IPS Throughput (Mbps)	5,500	6,500
Threat Prevention Throughput (Mbps)	3,000	3,200
SSL Inspection Throughput (Mbps)	2,800	3,000
VPN Throughput (Site-to-Site) (Mbps)	7,500	14,000
VPN Throughput (Remote Access) (Mbps)	2,500	2,500
VPN Tunnels (Max)	4,000	5,000
PMTA Tunnel	200	200
High Availability (HA)	YES	YES
Processor	Multi-Core	Multi-Core
RAM	8 GB	8 GB
Storage (SSD) in GB	120	120
Power Supplies	SINGLE	SINGLE
Operating Temperature	-10°C to 65°C	-10°C to 65°C
Operating Humidity	10% to 90%	10% to 90%

BT-NS 500 Series

Product Specifications



Model	BT-NS400	BT-NS500
Ethernet Interfaces	8x1GE, 4x 1G SFP	8x1GE, 4x10G SFP+
SIM Support (4G / 5G)	NO	NO
Concurrent Sessions	8,500,000	9,000,000
New Sessions per Second	120,000	130,000
Firewall Throughput (Mbps)	9,500	19,000
NGFW Throughput (Mbps)	4,000	4,200
Firewall IMIX Throughput (Mbps)	7,500	13,500
IPS Throughput (Mbps)	5,500	6,000
Threat Prevention Throughput (Mbps)	2,700	2,900
SSL Inspection Throughput (Mbps)	2,000	2,200
VPN Throughput (Site-to-Site) (Mbps)	7,800	9,500
VPN Throughput (Remote Access) (Mbps)	2,100	2,200
VPN Tunnels (Max)	6,000	6,000
PMTA Tunnel	400	500
High Availability (HA)	YES	YES
Processor	Multi-Core	Multi-Core
RAM	16 GB	16 GB
Storage (SSD) in GB	240	240
Power Supplies	SINGLE	SINGLE
Operating Temperature	-10°C to 65°C	-10°C to 65°C
Operating Humidity	10% to 90%	10% to 90%

BT-NS 1500 Series

Product Specifications

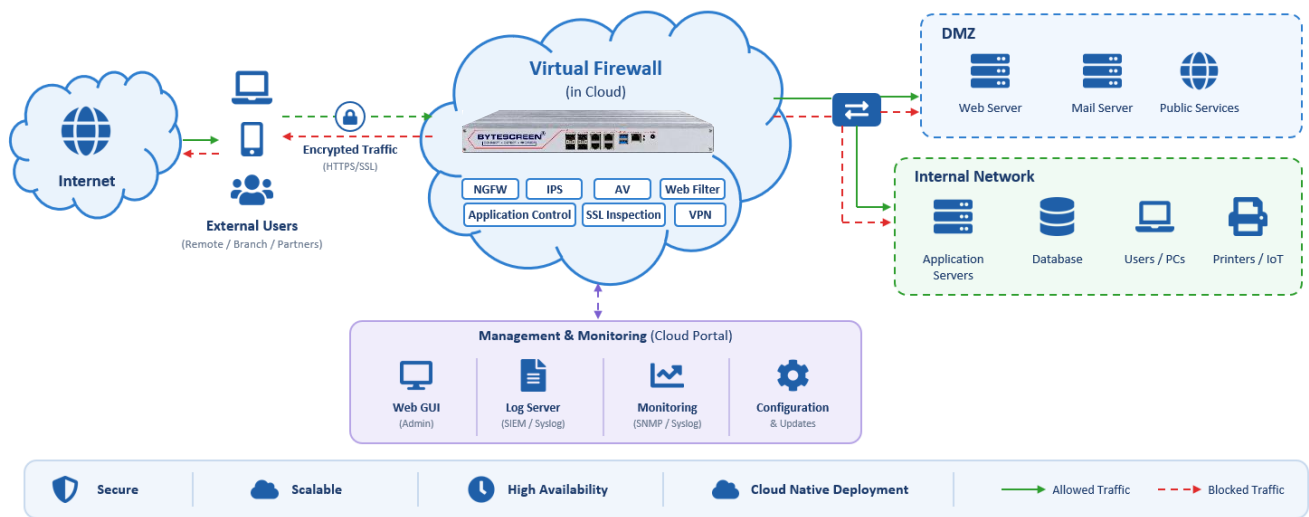


Model	BT-NS750	BT-NS1000	BT-NS1250	BT-NS1500
Ethernet Interfaces	22x1GE, 4x1G SFP	22x1GE, 4x1G SFP	22x1GE, 2x1G SF, 4 x 10G SFP+	22x1GE, 2x1G SFP, 4x10G SFP+
SIM Support (4G / 5G)	No	No	No	No
Concurrent Sessions	17,000,000	22,000,000	40,000,000	45,000,000
New Sessions per Second	380,000	400,000	420,000	500,000
Firewall Throughput (Mbps)	30,600	34,000	36,000	38,000
NGFW Throughput (Mbps)	9,775	11,000	11,500	12,000
Firewall IMIX Throughput (Mbps)	22,950	26,000	27,000	28,000
IPS Throughput (Mbps)	13,770	15,200	16,200	17,500
Threat Prevention Throughput (Mbps)	6,885	8,000	8,100	8,250
SSL Inspection Throughput (Mbps)	5,355	6,000	6,300	7,750
VPN Throughput (Site-to-Site) (Mbps)	19,890	22,400	23,400	24,000
VPN Throughput (Remote Access) (Mbps)	6,120	7,100	7,200	8,000
VPN Tunnels (Max)	14,000	15,000	18,000	20,000
PMTA Tunnel	750	750	1,000	1,000
High Availability (HA)	Yes	Yes	Yes	Yes
Processor	Multi-Core	Multi-Core	Multi-Core	Multi-Core
RAM	64 GB	64 GB	128 GB	128 GB
Storage (SSD) in GB	240	240	240	240
Power Supplies	Dual	Dual	Dual	Dual
Operating Temperature	-10°C to 65°C	-10°C to 65°C	-10°C to 65°C	-10°C to 65°C
Operating Humidity	10% to 90%	10% to 90%	10% to 90%	10% to 90%

BT-NS Virtual Series

The Bytescreen BT-NS Virtual Series extends the BT-NS security platform to virtualized and cloud environments, delivering Next-Generation Firewall (NGFW) capabilities through software-based virtual appliances. Designed for flexible deployment across supported virtualization platforms, private clouds, public clouds, and hybrid cloud environments, the series provides an alternative to dedicated physical firewall appliances while maintaining the core security capabilities of the BT-NS platform.

The virtual appliance portfolio comprises multiple models with defined performance and capacity profiles, enabling organizations to select the appropriate appliance based on network traffic, user capacity, security requirements, and available virtual infrastructure. The BT-NS Virtual Series includes BT-NS100V, BT-NS200V, BT-NS300V, BT-NS500V, and BT-NS1000V models



Virtual Product Specifications

Specification	BT-NSV100	BT-NSV200	BT-NSV500
Deployment Environment	Virtual / Private / Public / Hybrid Cloud	Virtual / Private / Public / Hybrid Cloud	Virtual / Private / Public / Hybrid Cloud
Virtual CPU (vCPU)	4	6	8
Memory (vRAM) (GB)	8	8	16
Storage (GB)	100	200	500
Virtual Network Interfaces	2	2	2
Specification	BT-NSV1000	BT-NSV2000	BT-NSV5000
Deployment Environment	Virtual / Private / Public / Hybrid Cloud	Virtual / Private / Public / Hybrid Cloud	Virtual / Private / Public / Hybrid Cloud
Virtual CPU (vCPU)	12	16	24
Memory (vRAM) (GB)	32	64	128
Storage (GB)	500	500	1000
Virtual Network Interfaces	2	4	4

Performance Testing Methodology

1. Test Environment: All throughput and capacity benchmarks are measured in a controlled laboratory environment under optimal conditions using industry-standard traffic generators adhering to RFC 2544, RFC 3511, and IMIX standards. 2. Firewall Throughput: Measured using HTTP traffic with 512 KB response size adhering to RFC 3511 test criteria. 3. Firewall IMIX: Measured using standard Enterprise UDP Traffic Mix (64-byte, 570-byte, and 1518-byte packets). 4. IPS & Application Control: Measured with multi-threaded inspection engines, standard production signature database, and logging enabled. 5. NGFW Throughput: Measured with Stateful Firewall, IPS, and Application Control concurrently active under Enterprise Mixed Traffic. 6. Threat Prevention: Measured with Firewall, IPS, Application Control, Gateway Antivirus (stream-based scanning), and Threat Intelligence feeds actively inspecting payload data. 7. SSL / TLS Deep Inspection: Measured with full SSL/TLS decryption (man-in-the-middle) across HTTPS sessions using TLS 1.2 / TLS 1.3 with AES-128-GCM cipher suites. 8. IPsec VPN Throughput: Measured across multi-tunnel Site-to-Site connections using AES-256-GCM / SHA256 encryption. 9. SD-WAN & Multi-Link Aggregation: Measured with multi-tunnel link aggregation, packet-level bonding, and session load balancing enabled. 10. Performance & Lab Conditions

Disclaimer: All stated throughputs, concurrent session capacities, and connection rates represent maximum benchmark numbers achieved under laboratory test conditions. Actual real-world performance may vary depending on live network topology, real-time traffic composition, packet size distribution, cipher complexity, active security policies, and system logging configurations.

Features

Hardened and Secure Operating System	Advanced IPS/IDS with Signature-Based Threat Detection
Stateful Packet Inspection (SPI) Firewall	IPS/IDS with Snort 3 Inspection Engine
Zone-Based Firewall Policies for Segmented Trust Boundaries	50,000+ Default IPS Signatures with Custom Signature Support
Granular Traffic Rules for Fine-Grained Allow/Deny Control	Multiple Segmentation-Based IPS Policies
Flexible LAN/WAN Port Assignment	Deep Packet Inspection (DPI) for Layer-7 Application Identification and Traffic Analysis
Multi-WAN Support including 4G/5G LTE Networks	Application Identification and Layer-7 Application Filtering
Multi-WAN Aggregation across P2P, MPLS, ILL, DHCP, PPPoE, RF, VSAT, 4G and 5G	Gateway Anti-Virus with Inline Malware Scanning and Zero-Hour Protection
High Availability (Active/Passive) with Automatic Device Failover	Packet Payload Inspection for Malware Detection
VLAN Segmentation (802.1Q) for Logical Network Isolation	Hash-Based Malware Detection
WAN and LAN Virtual Segmentation	Heuristic and Fuzzy File Analysis for Advanced Threat Detection
LAN Micro-Segmentation for Granular Network Isolation	Zero-Day Threat and Attack Protection
Layer-2 Bridging Support	Network Data Loss Prevention (DLP)
MAC Address Filtering for Device-Level Access Control	Network Anomaly Detection
Access Control Lists (ACL) for Policy-Based Network Access Control	Botnet Traffic Detection and Blocking
Port Forwarding (DNAT) for Secure Internal Service Publishing	DoS/DDoS Protection against SYN Flood, UDP Flood and Other Network Flood Attacks
Full NAT Support including SNAT, DNAT and PAT	Malicious URL Detection and Blocking
Carrier-Grade NAT (CGNAT)	Web, Domain and Content Filtering
Static and Policy-Based Routing Support	75+ Web and Content Filtering Categories
BGP Routing Support	Weight-Based Content Filtering
OSPFv2 and OSPFv3 Routing Support	Keyword, File Extension and URL Pattern Blocking
RIPv2 Routing Support	URL Blocking Based on Web Patterns and Categories
PIM-SM Multicast Routing Support	Search Engine Protection and Safe Search Enforcement
VRRPv3-Based Gateway Redundancy	SNI-Based HTTPS Domain Filtering
Virtual Routing and Forwarding (VRF) for Network Isolation	Security Intelligence for IP, URL and Domain Reputation
NTP Synchronization for Network-Wide Time Accuracy	DGA Detection for Algorithmically Generated Domain Identification
Local DHCP and DNS Services	Typo squatting and Look-Alike Domain Protection
DHCP Server and DHCP Client Support	Newly Registered Domain (NRD) Detection and Domain-Age-Based Security
ACL-Based DHCP Server	Dynamic FQDN-Based Firewall Policies with Automatic Address Updates
DHCP Reservation	Geo-Fencing and Geo-IP Traffic Filtering
Network Abuse Protection for Detecting and Blocking Malicious Network Activity	Automatic Geo-IP Database Updates
HTTP Web Proxy Mode Support	IPSec and SSL VPN Support
Upstream Parent Proxy Integration	IKEv2 IPSec VPN with Tunnel Health Monitoring and Auto-Recovery
True SDN-Based SD-WAN Architecture	WireGuard VPN Support
PMTA (Packet-Based Multi-Tunnel Aggregation) with Multi-WAN Link Aggregation, Packet Redundancy and Failover	GRE Tunnel Support
AI-Based WAN Path Selection and Link Optimization	PPTP & L2TP VPN Support

ISP Internet Link Health Monitoring and SLA-Based Failover	IPSec Path MTU Discovery for Tunnel Fragmentation Prevention
Multi-Path Multi-Direction (MPMD) Support	AES-128/256-Bit Per-Session Encryption and Compression
Intelligent Packet Redundancy through Packet Duplication	Dynamic Time-Based Encryption Key Rotation
SD-WAN Tunnel Data Compression	Built-in PKI and X.509 Certificate Management
SD-WAN Tunnel Rate Limiting	Centralized Policy and Configuration Management
Multi-Link Bandwidth Aggregation and Intelligent Traffic Steering	Configuration Backup and Restore
Zero-Touch Provisioning (ZTP) for Automated Remote Branch Deployment	Configuration Rollback and Version Management
MPLS over 4G/LTE with Private APN Support	Scheduled Configuration Backup
4G/5G LTE WAN Failover	Administrator Login and Activity Audit Logging
Identity and Access Management (IDAM)	Administrator Session Management and Timeout Control
Zero Trust Network Protection	Password Policy and Administrator Account Management
Network Access Server (NAS) Support	Secure Web GUI and CLI Administration
Role-Based Administration and Access Control	REST API-Based Administration and Integration
Multi-Level Administrator Privileges and Delegated Administration	Firmware Upgrade and Rollback Management
Directory Services Integration with AD, LDAP, TACACS+ and RADIUS	Role-Based Access to Logs, Reports and Network Analytics
Centralized Administrator Authentication	IPv6 Network Translation Support
Multi-Factor Authentication with TOTP/HOTP	464XLAT Support for IPv4/IPv6 Network Translation
Single Sign-On (SSO) Support	NAT64 Support for IPv6-to-IPv4 Connectivity
802.1X Port-Based Network Access Control	DNS64 Support for IPv6 Network Environments
Hardened SSH Access with Key-Based Authentication	Integrated Wi-Fi Controller with Multi-Brand Access Point Support
Quality of Service (QoS) and Traffic Prioritization	Integrated Captive Portal for Guest and User Access
Application-Aware QoS with Policy-Based Traffic Prioritization	PMS-Based Guest Provisioning and Authentication
Class-Based Traffic Shaping using Hierarchical Token Bucket (HTB)	Customizable Branded Guest Web Portal
Smart Queue Management (SQM) with fq_codel/CAKE	Voucher-Based Guest Authentication and Access
Unified Traffic Shaping Engine	SCADA/ICS Protocol Support
Time-Based Security Policy Scheduling	Modbus TCP Protocol Inspection and Monitoring
Traffic Flow Analyzer with Connected Device Visibility	Industrial/OT Network Traffic Visibility and Access Control
VLAN-Level Traffic Visibility and Monitoring	Industrial Network Segmentation and Policy-Based Access Control
Per-Interface and VLAN-Level Traffic and Packet Statistics	Centralized Security and System Logging
Automatic Discovery and Monitoring of LAN-Connected Devices	Syslog Support
Automatic ISP and SIM Information Discovery	SNMP v1/v2/v3 Monitoring and Management
Device Resource and System Visibility including CPU, RAM, Storage, Applications and System Services	Advanced Logs, Analytics and Reports
Endpoint Visibility including OS Type, Installed Patches, Browser, Applications, Versions and Installation Details	Security and Network Event Reporting
Real-Time Network Health and Performance Monitoring	WAN SLA Monitoring and Alerts
WAN, LAN and VLAN Traffic Analytics	Post quantum cryptography security
Centralized Network Management System (NMS)	Power Outage Alerts
Centralized Network and Service Management	SMS-Based Auto-Reboot and Remote Device Recovery

Centralized Fleet Configuration with Role-Based Access Control	Multi-Channel Alerts via SMS, Email, WhatsApp and Telegram
Centralized Network and Security Policy Orchestration	Role-Based Access to Logs, Reports and Network Analytics
Centralized Configuration and Policy Synchronization	Vulnerability Assessment Dashboard
Centralized Firmware Management and OTA Update Orchestration	LAN Security Audit and Analysis
Automated Branch Provisioning and Deployment	Advanced GUI-Based Network Diagnostics and Troubleshooting Tools
Unified Device, Network and Security Management	Network Security Event Monitoring
Intelligent WAN Path Selection and Automatic Failover	Threat Detection and Security Analytics
Self-Healing Network Operations and Automated Link Recovery	Security Audit and Compliance Visibility
Historical Performance and Security Analytics	Configuration Health and Operational Diagnostics

Standards & Compliance

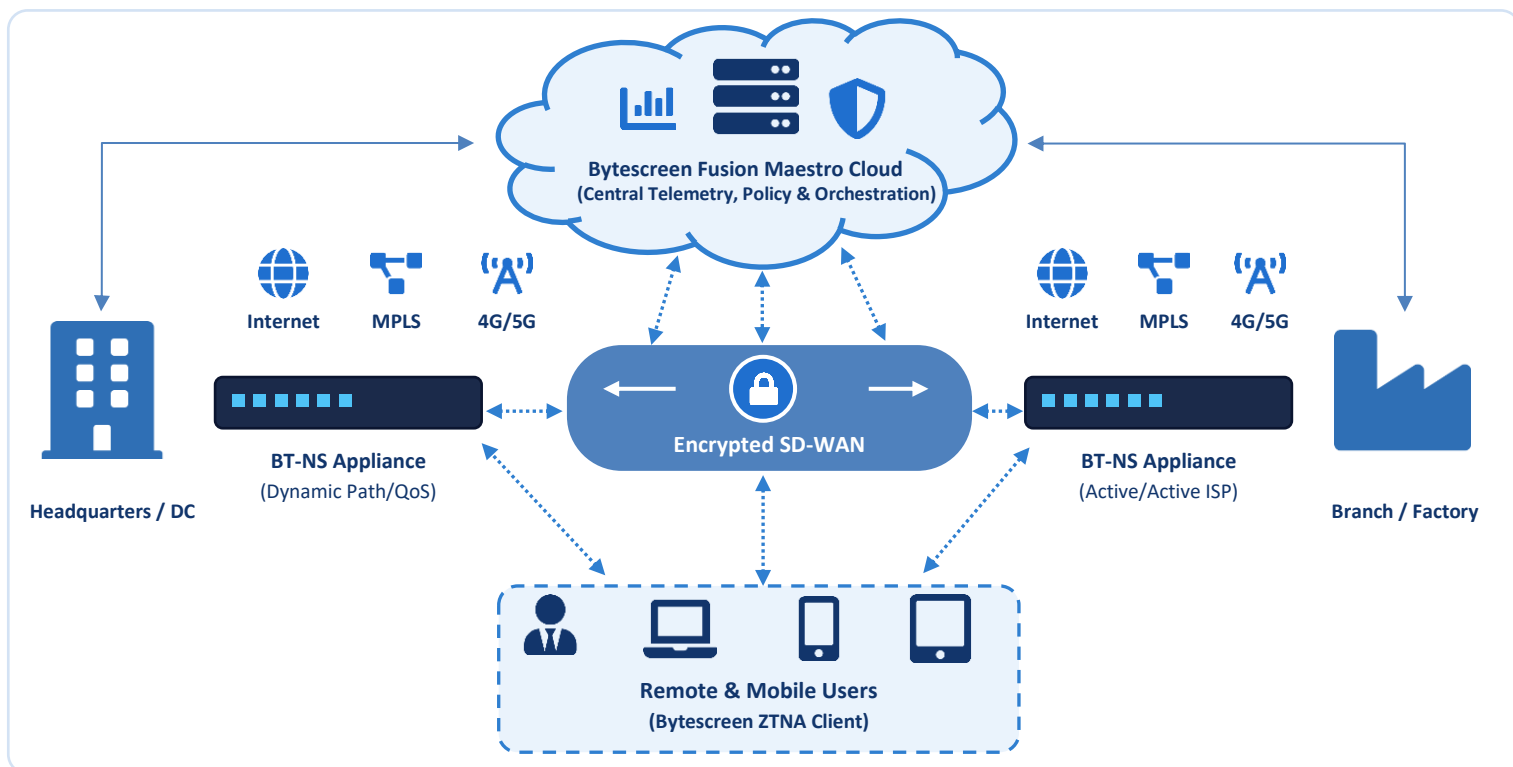
Bytescreen BT-NS Series Next-Generation Firewalls comply with international networking, security, and cryptographic standards defined by the IETF, IEEE, and industry consortia

Domain	Standards / Protocols	Implementation Scope
Ethernet, IP & Transport	IEEE 802.3; RFC 791, RFC 1812, RFC 9293, RFC 768, RFC 792, RFC 4443, RFC 8200, RFC 8201	Ethernet connectivity, IPv4/IPv6 forwarding and routing, TCP/UDP, ICMP/ICMPv6 and Path MTU Discovery
DHCP, DNS & Time Services	RFC 2131, RFC 2132, RFC 8415, RFC 1034, RFC 1035, RFC 5905	DHCPv4/DHCPv6, DNS resolution/forwarding and NTP synchronization
NAT, IPv6 Transition & Segmentation	RFC 3022, RFC 4787, RFC 5382, RFC 5508, RFC 6888, RFC 6877, RFC 6146, RFC 6147, IEEE 802.1Q, VRF implementation	NAT44/NAPT/PAT, CGNAT, 464XLAT, NAT64, DNS64, VLAN segmentation and VRF-based traffic isolation
Dynamic Routing & Redundancy	RFC 4271, RFC 2328, RFC 5340, RFC 2453, RFC 5798, RFC 7761	BGP-4, OSPFv2/v3, RIPv2, VRRPv3 and PIM-SM
IPsec, VPN & Tunnelling	RFC 4301, RFC 4303, RFC 7296, RFC 2784, RFC 2890, RFC 2661, WireGuard Protocol	IPsec, ESP, IKEv2, GRE, L2TP and WireGuard VPN
TLS, SSL VPN & PKI	RFC 5280, RFC 5246, RFC 8446, OpenVPN Protocol	X.509/PKIX certificates, TLS 1.2/1.3 and SSL VPN
Identity & Authentication	RFC 8907, RFC 2865, RFC 2866, RFC 4510, RFC 4511, RFC 4226, RFC 6238, IEEE 802.1X	TACACS+, RADIUS, LDAP, HOTP/TOTP and 802.1X network access control
Network Management & Monitoring	RFC 1157, RFC 3411–3418, RFC 5424, RFC 5425	SNMP monitoring, Syslog logging and secure log transport
REST API & Integration	RFC 9110, RFC 9112, RFC 8259	HTTP/REST API communication and JSON-based integration
QoS & Traffic Management	RFC 2474, RFC 2475, RFC 8290	DSCP/DiffServ traffic classification and FQ-CoDel queue management
Email Notification	RFC 5321, RFC 5322	SMTP-based system and security notifications
Industrial / OT Networking	Modbus Application Protocol Specification, applicable SCADA/ICS protocols	Modbus TCP inspection, SCADA/ICS traffic visibility and industrial network security

Enterprise Architecture: Secure SD-WAN & Zero-Trust (ZTNA)

Hybrid Work & Multi-Cloud Connectivity

The Bytescreen BT-NS Series consolidates software-defined WAN and identity-driven access into a single operating architecture, eliminating the performance penalties and complexity of multi-box deployments.



1 Intelligent Application-Aware SD-WAN



Dynamic Multi-Path Optimization

Measures latency, packet loss and jitter continuously across multiple broadband, DIA and 4G/5G uplinks.



SLA-Based Traffic Steering

Directs latency-sensitive traffic (VoIP, video, ERP) to the healthiest connection and routes bulk traffic over commodity internet.



Sub-Second Failover

Keeps active sessions alive without dropping connections during ISP degradation or brownouts.



SaaS Acceleration

Local breakout policies eliminate hair-pinning back to HQ, improving cloud application responsiveness.

2 Built-in Zero Trust Network Access (ZTNA)



Identity-First Security

Replaces broad-access legacy IPsec/SSL VPNs with least-privilege, application-level perimeters.



Continuous Posture Assessment

Checks user identity (MFA, SAML, Azure AD) and device health (OS patches, disk encryption, AV status) before and during active sessions.



Micro-Segmentation

Limits authorized users strictly to their assigned enterprise applications, stopping internal lateral threat movement.

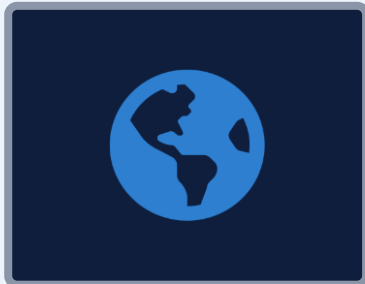


Universal Access Gateway

Delivers uniform access controls whether employees connect from home, branch offices or the corporate campus.

Central Orchestration & NaaS Delivery Framework

Centralized Control with Fusion Maestro



BYTESCREEN FUSION MAESTRO CONSOLE



Zero-Touch Provisioning

Ships pre-configured to branch; connects on boot



Global Policy Templates

Push compliance & firewall rules in seconds



Threat Telemetry & AI

Real-time anomaly detection & automated response



Log Consolidation

Audit-ready compliance reporting (ISO, SOC2, PCI)

Fusion Maestro Platform Capabilities



Zero-Touch Provisioning (ZTP)

Onboard branch appliances remotely. Connect power and WAN; auto-download config and security policies.



Unified Template Management

Push changes to security rules, IPS policies and routing tables across thousands of appliances in minutes.



Automated Patch Management

Schedule firmware updates, vulnerability rollouts and threat signature patches with automated rollback safeguards.



Consolidated Compliance Audits

Generate reports for PCI-DSS, ISO 27001 and enterprise frameworks with automated log aggregation and event correlation.

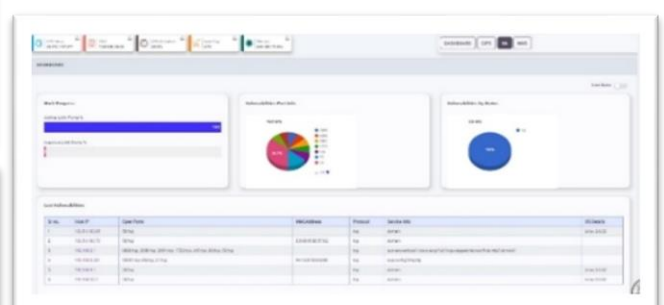
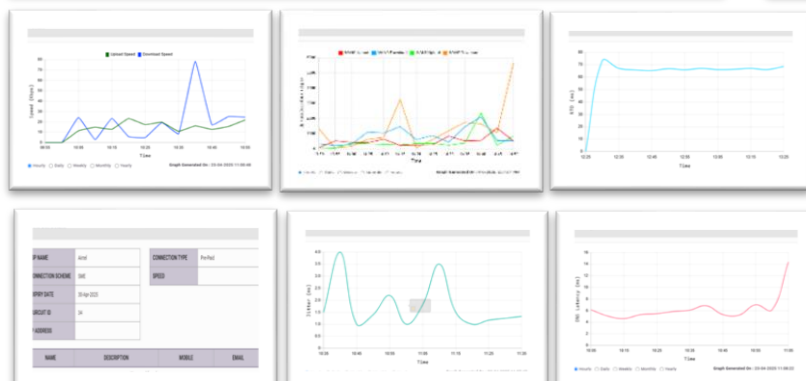
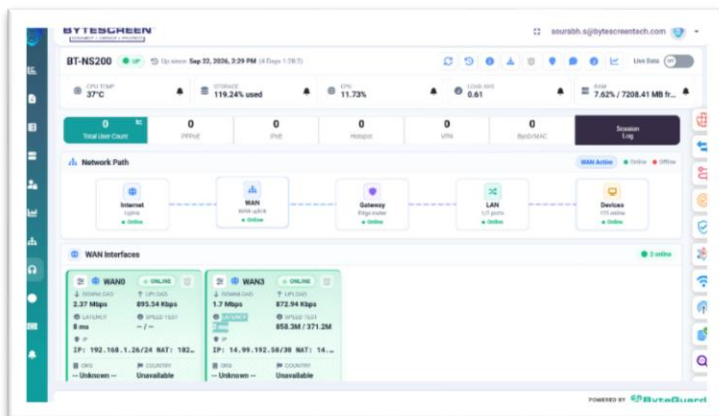
Network-as-a-Service (NaaS) Commercial Model



NaaS

Hardware + Licensing + Support
as a Service

Feature Area	Traditional CAPEX	Bytescreen NaaS Model
 Procurement	Large upfront capital expense	Predictable OPEX recurring subscription
 Hardware Refresh	Manual replacement every 3–5 years	Built-in continuous hardware lifecycle upgrades
 Licensing	Disjointed module renewals & add-ons	All-inclusive threat defense and SD-WAN licensing
 TAC Support	Varying response tiers & SLA gaps	24x7 Enterprise TAC with Next-Business-Day RMA
 Scalability	Fixed-capacity appliances	Flexible expansion as bandwidth demands grow



Ordering Information

Model	Part Code	Description
BT-NS50	BT-NS50A	BT-NS50, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN, 4 x 2.5 GBE Port, Online Activation Warranty via Cloud Controller
BT-NS100	BT-NS100A	BT-NS100, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN, 4 x 2.5 GBE Port, Online Activation Warranty via Cloud Controller
BT-NS200	BT-NS200A	BT-NS200, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN, 4 x 2.5GE, 4 x 1G SFP Port, Online Activation Warranty via Cloud Controller
BT-NS300	BT-NS300A	BT-NS300, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN, 4 x 2.5GE, 4 x 10G SFP+ Port, Online Activation Warranty via Cloud Controller
BT-NS400	BT-NS400A	BT-NS400, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN, 8 x 1GE, 4x 1G SFP Port, Online Activation Warranty via Cloud Controller
BT-NS500	BT-NS500A	BT-NS500, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN. 8 x 1GE, 4x 10G SFP+ Port, Online Activation Warranty via Cloud Controller
BT-NS750	BT-NS750A	BT-NS750, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN. 22 x 1GE, 4 x 1G SFP Port, Online Activation Warranty via Cloud Controller
BT-NS1000	BT-NS1000A	BT-NS1000, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN. 22 x 1GE, 4 x 1G SFP Port, Online Activation Warranty via Cloud Controller
BT-NS1250	BT-NS1250A	BT-NS1250, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN. 22 x 1GE, 2x1G SFP, 4 x 10G SFP+ Port, Online Activation Warranty via Cloud Controller
BT-NS1500	BT-NS1500A	BT-NS1500, Basic Appliance, Including, WAN Optimization, LAN Microsegmentation, LAN Visibility, & VPN. 22 x 1GE, 2x1G SFP, 4 x 10G SFP+ Port, Online Activation Warranty via Cloud Controller

Licensing Type

License	Part Code	Description
Protect Base	BT-ProtectBE1YB BT-ProtectBE3YB BT-ProtectBE5YB	Protect Base Bundle License includes Stateful firewall, WAN Optimization, SD-WAN, Domain Filter, Application Control, Country Filter, VPN, IDAM, Threat Intel, CIPS & IPS/IDS, VA, Gateway Antivirus, Cloud Fusion Maestro Access with Standard Support
Protect Pro	BT-ProtectPro1YB BT-ProtectPro3YB BT-ProtectPro5YB	Protect Pro Bundle License includes Stateful firewall, WAN Optimization, SD-WAN, Domain Filter, Content Filter, URL Filter, Malicious URL detection, Network DLP, Application Control, Country Filter, VPN, IDAM, Threat Intel, CIPS & IPS/IDS, VA, Gateway Antivirus, Zero-Day Protection, Multi AP Management, Cloud Fusion Maestro Access with Standard Support

www.bytescreentech.com

.....

BYTESCREEN Tech Pvt Ltd delivers high-performance, resilient networking and security solutions designed for modern enterprise environments. We combine robust hardware with an advanced software architecture to ensure your network remains secure, optimized, and easy to manage. Backed by our dedicated expert OEM support team, we empower businesses to secure their infrastructure without compromising on performance.

Try It Now for Free: 30-Day Enterprise Evaluation

Experience the enterprise-grade performance, deep packet inspection, and threat defenses of the Bytescreen BT-NS Series in your own operational environment with zero commitment.

- Full-Featured Enterprise Guard Suite: Evaluate Next-Gen IPS, Gateway Anti-Virus, Layer 7 Application Visibility, Dynamic URL Filtering, and Cloud Sandboxing.
- Live SD-WAN & ZTNA Validation: Test dynamic link steering, multi-WAN load balancing, and identity-aware application access policies under real traffic conditions.
- Fusion Maestro Central Access: Explore centralized orchestration, live threat telemetry, and zero-touch configuration management.
- Flexible Delivery Options: Available as a dedicated physical hardware Proof-of-Concept (POC) unit or an instant-deploy Virtual Appliances

Register your 30-day evaluation online:

For inquiries, collaboration opportunities, or to learn more about how BYTESCREEN Tech can elevate your network infrastructure, please don't hesitate to reach out to us

Contact Details:

sales@bytescreentech.com

www.bytescreentech.com

Need Help? Get BYTESCREEN Expert Support

Bytescreen offers direct OEM assistance through experienced professionals for product configuration and support. TAC advises customers on security best practices to enhance network reliability and prevent hacking attempts.

For Technical Assist:
support@bytescreentech.com