FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint™ Stonesoft® Next Generation Firewall

FORCEPOINT STONESOFT NEXT GENERATION FIREWALL PROTECTS ENTERPRISE NETWORKS WITH HIGH-PERFORMANCE "INTELLIGENCE AWARE" SECURITY SUPPORTED BY REAL-TIME UPDATES. THIS ENABLES STONESOFT TO DELIVER THE INDUSTRY'S BEST DEFENSE AGAINST ADVANCED EVASIONS, ALONG WITH COMPLETE NEXT-GENERATION FIREWALL PROTECTION WHEN AND WHERE YOU NEED IT — AT REMOTE SITES, BRANCH OFFICES, DATA CENTERS, AND THE NETWORK EDGE.

Forcepoint Stonesoft Next Generation Firewall (NGFW) starts with a solid foundation of protection, including granular application control, an intrusion prevention system (IPS), built-in virtual private network (VPN), and deep packet inspection, all in an efficient, extensible, and highly scalable unified design. Then we add powerful anti-evasion technologies that decode and normalize network traffic — before inspection and across all protocol layers — to expose and block the most advanced attack methods.

BLOCK SOPHISTICATED DATA BREACH ATTACKS

Large data breaches continue to plague businesses and organizations across industry verticals. Now you can fight back with application layer exfiltration protection. This new solution enables Stonesoft NGFW to selectively and automatically block network traffic originating from PCs, laptops, servers, file shares, and other endpoint devices based on highly granular endpoint contextual data. Application layer exfiltration protection is the only solution that goes beyond typical next-generation firewalls to prevent attempted ex-filtration of sensitive data from endpoints via unauthorized programs, web applications, users, and communications channels.

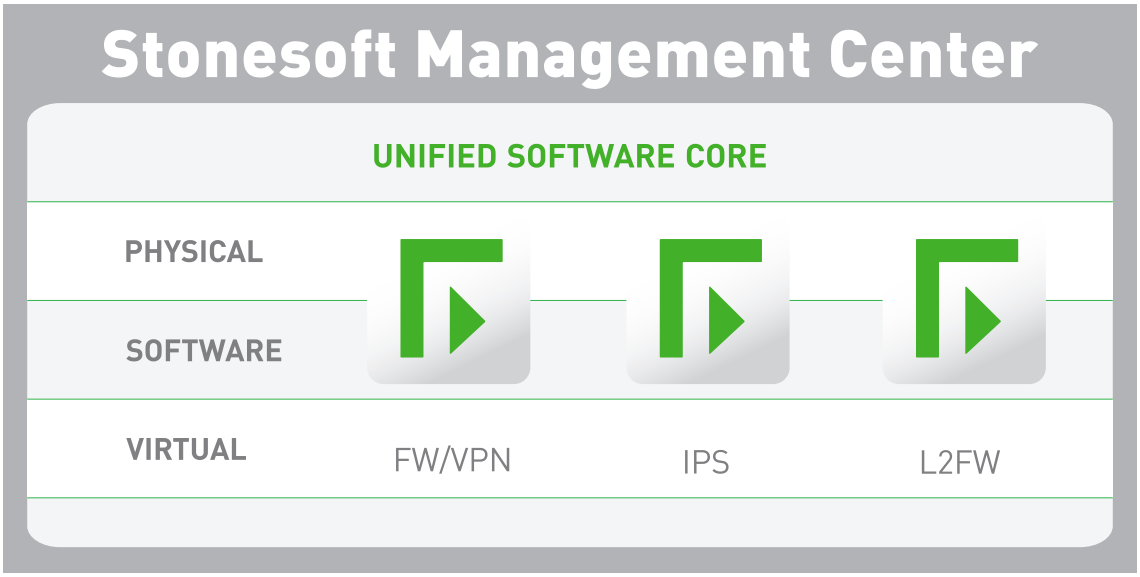
SUPERIOR FLEXIBILITY KEEPS PACE WITH YOUR CHANGING SECURITY NEEDS

A unified software core enables Stonesoft NGFW to easily change security roles, from firewall/ VPN to IPS to layer 2 firewall, in dynamic business environments. The unified software core also serves to optimize the data plane, providing a significant performance advantage regardless of security role or number of active security features. For even more flexibility, Stonesoft NGFW can be deployed in a wide variety of formats — as a physical appliance, software solution, virtual appliance, or as virtual contexts on a physical appliance.

HIGH SCALABILITY AND AVAILABILITY SECURES YOUR BUSINESS-CRITICAL APPLICATIONS

Today's businesses demand fully resilient network security solutions. Forcepoint Stonesoft NGFW delivers high scalability and availability in three powerful ways:

- Native active-active clustering: Up to 16 nodes can be clustered together, providing superior performance and resiliency when running demanding security applications, such as deep packet inspection and VPNs.
- Transparent session failover: Provides industry-leading availability and serviceability of security systems. Stonesoft NGFW even supports transparent failover for multiple software and hardware versions within the same cluster.
- Multi-Link: Extends high availability coverage to network and VPN connections. Provides the confidence of non-stop security along with high performance for every deployment.



UNMATCHED PROTECTION KEEPS YOUR BUSINESS IN BUSINESS

Every day attackers get better at penetrating enterprise networks, applications, data centers, and endpoints. Once inside, they can steal intellectual property, customer information, and other sensitive data, causing irreparable damage to businesses and reputations.

Some attackers use advanced evasion techniques (AETs) that are able to bypass most of today's security network devices. AETs deliver malware piecemeal across network layers or protocols using techniques such as masking and obfuscation. Once inside networks, threats are reassembled where they can hide, exfiltrating sensitive data for days, months, or even years.

Forcepoint Stonesoft NGFW applies layered threat discovery techniques to network traffic, identifying applications and users at a granular level so that security policies can be applied according to business rules. Then it performs specialized deep packet inspection,
including advanced techniques such as full stack normalization and horizontal data stream-based inspection. These techniques fully normalize traffic flows, enabling Stonesoft NGFW to expose AETs and traffic anomalies that evade other next-generation firewalls. Only after traffic has been fully normalized can it be properly inspected across all protocols and layers for threats and malware.

And only Stonesoft NGFW has been successfully tested against more than 800 million AETs.

KEY BENEFITS

- The best protection for your business and digital assets
- Blocks endpoint data exfiltration attempts
- Adapts easily to your security needs
- Scales effortlessly as your business grows
- Optimizes productivity of employees and customers
- Lowers TCO for security and network infrastructure

KEY FEATURES

- "Intelligence-aware" security controls
- Application layer exfiltration protection
- Advanced evasion prevention
- Unified software core design
- Many options for security and network infrastructure
- Powerful centralized management
- Built-in IPsec and SSL VPN

FORCEPOINT STONESOFT NEXT GENERATION FIREWALL SPECIFICATIONS

SUPPORTED PLATFORMS	
Appliances	Multiple hardware appliance options, ranging from branch office to data center installations
Cloud Infrastructure	Amazon Web Services
Virtual Appliance	x86 64-bit based systems; VMware ESXi and KVM virtualized environment
Supported Roles	Firewall/VPN (layer 3), IPS mode (layer 2), and Layer 2 Firewall
Virtual Contexts (License only)	Virtualization to separate logical contexts (FW, IPS, or L2FW) with separate interfaces, addressing, routing, and policies

FIREWALL/VPN FUNCTIONAL ROLE	
General	Stateful and stateless packet filtering, circuit-level firewall with TCP proxy protocol agent
User Authentication	Internal user database, LDAP, Microsoft Active Directory, RADIUS, TACACS+
High Availability	• Active-active/active-standby firewall clustering up to 16 nodes • Stateful failover (including VPN connections) • Server load balancing • Link aggregation (802.3ad) • Link failure detection
ISP Multi-Homing	Multi-Link: high availability and load balancing between multiple ISPs, including VPN connections, Multi-Link VPN link aggregation, QoS-based link selection
IP Address Assignment	• FW clusters: static, IPv4, IPv6 • FW single nodes: static, DHCP, PPoA, PPoE) IPv6 (static, SLAAC) • Services: DHCP Server for IPv4 and DHCP relay for IPv4
Address Translation	• IPv4, IPv6 • Static NAT, source NAT with port address translation (PAT), destination NAT with PAT
Routing	Static IPv4 and IPv6 routes, policy-based routing, static multicast routing
Dynamic Routing	IGMP proxy, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM-SM, PIM-SSM
IPv6	Dual stack IPv4/IPv6, ICMPv6, DNSv6
SIP	Allows RTP media streams dynamically, NAT traversal, deep inspection, interoperability with RFC3261-compliant SIP devices
CIS Redirection	HTTP, FTP, SMTP protocols redirection to content inspection server (CIS)
Geo-Protection	Control access by source/destination country or continent
IP Address List	Control access by predefined IP categories or using custom IP address list
URL List	Control access by custom URL list
Sidewinder Security Module Proxies	TCP, UDP, HTTP, SSH
TRITON AP-Web Redirect	Redirect HTTP/HTTPS traffic to the TRITON® AP-WEB Cloud via IPSec tunnel for Web content inspection

STONESOFT NEXT GENERATION FIREWALL SPECIFICATIONS CONTINUED

IPsec VPN	
Protocols	IKEv1, IKEv2, and IPsec with IPv4 and IPv6
Encryption	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES
Message Digest Algorithms	AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
Diffie-Hellman	DH group 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
Authentication	RSA, DSS, ECDSA signatures with X.509 certificates, pre-shared keys, hybrid, XAUTH, EAP
Other	• IPCOMP deflate compression • NAT-T • Dead peer detection • MOBIKE
Site-to-Site VPN	• Policy-based VPN, route-based VPN (GRE, IP-IP, SIT) • Hub and spoke, full mesh, partial mesh topologies • Stonesoft Multi-Link fuzzy-logic-based dynamic link selection • Stonesoft Multi-Link modes: load sharing, active/standby, link aggregation
Mobile VPN	• VPN client for Microsoft Windows • Automatic configuration updates from gateway • Automatic failover with Multi-Link • Client security checks • Secure domain logon
SSL VPN (LICENSE ONLY)	
Client-Based Access	Supported platforms: Android 4.0, Mac OS X 10.7, and Windows Vista SP2 (and newer versions)
Clientless Access *(Not available for 110 and 115 models)*	Web Portal access to HTTP-based services via predefined services and free form URLs

STONESOFT NEXT GENERATION FIREWALL SPECIFICATIONS CONTINUED

INSPECTION	
Anti-Botnet	• Decryption-based detection • Message length sequence analysis
Dynamic Context Detection	Protocol, application, file type
Advanced Anti-Malware	Policy-based file filtering
Sandboxing	Support for McAfee Advanced Threat Defense
File Reputation	Classification from McAfee GTI cloud service or optionally from local McAfee Threat Information Exchange
Anti-Malware Engine	Scanned protocols: FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Protocol-Specific Normalization/ Inspection/Traffic Handling	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6 encapsulation, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBios Datagram, OPC Classic, OPC UA, Oracle SQL Net ,POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP
Protocol-Independent Fingerprinting	Any TCP/UDP protocol
Evasion and Anomaly Detection	• Multilayer traffic normalization • Vulnerability-based fingerprints • Fully upgradable software-based inspection engine • Evasion and anomaly logging
Custom Fingerprinting	• Protocol-independent fingerprint matching • Regular expression-based fingerprint language • Custom application fingerprinting
TLS Inspection	• HTTPS client and server stream decryption and inspection • TLS certificate validity checks • Certificate domain name-based exemption list
Correlation	Local correlation, log server correlation
DoS/DDoS Protection	• SYN/UDP flood detection • Concurrent connection limiting, interface-based log compression • Protection against slow HTTP request methods
Reconnaissance	TCP/UDP/ICMP scan, stealth, and slow scan detection in IPv4 and IPv6
Blocking Methods	Direct blocking, connection reset, blacklisting (local and distributed), HTML response, HTTP redirect
Traffic Recording	Automatic traffic recordings/excerpts from misuse situations
Updates	• Automatic dynamic updates through Stonesoft Management Center • Current coverage of approximately 4,700 protected vulnerabilities
URL Categorization	Classify the URL in HTTP and HTTPS with the Forcepoint cloud service
Custom URL Lists	Match locally own URL sets

FORCEPOINT NEXT GENERATION FIREWALL SPECIFICATIONS CONTINUED

URL FILTERING	
Protocols	HTTP, HTTPS
Forcepoint URL categorization	Control access using category-based URL filtering from Forcepoint cloud
Database	• More than 280 million top-level domains and sub-pages (billions of URLs) • Support for more than 43 languages, 82 categories
Safe Search	Safe search usage enforcing for Google, Bing, Yahoo, DuckDuckGo web searches
MANAGEMENT & MONITORING	
Management Interfaces	• Enterprise-level centralized management system with log analysis, monitoring and reporting capabilities • See the Stonesoft Management Center datasheet for details.
SNMP Monitoring	SNMPv1, SNMPv2c, and SNMPv3
Traffic Capturing	Console tcpdump, remote capture through SMC
High Security Management Communication	256-bit security strength in engine-management communication
Security Certifications	Common Criteria Network Devices Protection Profile with Extended Package Stateful Traffic Filter Firewall, FIPS 140-2 crypto certificate, CSPN by ANSSI, (First Level Security Certification USGv6)

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

Forcepoint™ is a trademark of Forcepoint LLC. SureView®, ThreatSeeker®, TRITON®, Sidewinder®, and Stonesoft® are registered trademarks of Forcepoint LLC. Raytheon is a registered trademark of Raytheon Company. All other trademarks and registered trademarks are property of their respective owners.

[DATASHEET_NEXT_GEN_FIREWALL_EN] 100033.122016