FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint Next Generation Firewall

FORCEPOINT NEXT GENERATION FIREWALL (NGFW) CONNECTS AND PROTECTS DISTRIBUTED ENTERPRISE NETWORKS – DATA CENTERS, EDGE, BRANCHES, AND THE CLOUD – WITH THE STRONGEST SECURITY, SMARTEST MANAGEABILITY, AND HIGHEST AVAILABILITY. CUSTOMERS WHO SWITCH TO FORCEPOINT NGFW REPORT AN 86% DROP IN CYBERATTACKS, 53% LESS BURDEN ON IT, AND 70% LESS MAINTENANCE TIME.*

***"Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, May 2017.**

Forcepoint Next Generation Firewall (NGFW) combines fast, flexible networking with industry-leading security to connect and protect people and the data they use throughout diverse, evolving enterprise networks. Designed from the ground up for high availability and scalability as well as centralized management with full 360° visibility, Forcepoint NGFWs provide consistent security, performance and manageability across physical, virtual and cloud systems.

Forcepoint uniquely tailors access control and deep inspection to each connection to provide high performance as well as high security. It brings together granular application control, intrusion prevention system (IPS) defenses, and built-in virtual private network (VPN) control and mission-critical application proxies all in an efficient, extensible, and highly scalable design. Our powerful anti-evasion technologies 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 industries. Now you can fight back with application-layer exfiltration protection. Forcepoint NGFWs can selectively and automatically whitelist or blacklist network traffic originating from particular applications on PCs, laptops, servers, file shares, and other endpoint devices based on highly granular endpoint contextual data. It goes beyond typical firewalls to prevent attempted exfiltration of sensitive data from endpoints via unauthorized programs, web applications, users, and communications channels.

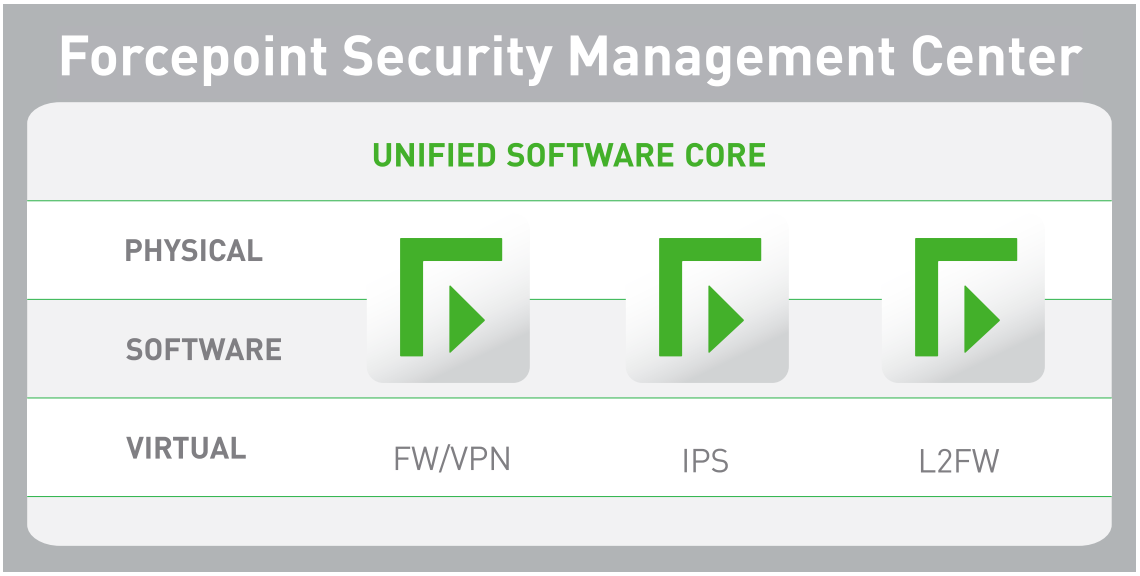
KEEP PACE WITH CHANGING SECURITY NEEDS

A unified software core enables Forcepoint NGFW to easily change security roles, from firewall/VPN to IPS to layer 2 firewall, in dynamic business environments. Forcepoint NGFWs can be deployed in a variety of ways – as physical, virtual, and cloud appliances – all managed together from a single console.

HIGH SCALABILITY AND AVAILABILITY SECURES YOUR BUSINESS-CRITICAL APPLICATIONS

Today's businesses demand fully resilient network security solutions. Forcepoint NGFW builds high scalability and availability in at all levels:

- Active-active, mixed clustering: Up to 16 nodes, of different models running different versions, can be clustered together, providing superior performance and resiliency for demanding security applications, such as deep packet inspection and VPNs.
- Seamless policy updates and software upgrades: Forcepoint's industry-leading availability and serviceability of security systems enables policy updates and even software upgrades to be pushed to a cluster seamlessly without interrupting service.
- SD-WAN network clustering: Extends high availability coverage to network and VPN connections. Provides the confidence of non-stop security that can take advantage of local broadband connections to complement or replace expensive leased lines like MPLS.



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.

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

Forcepoint 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 processes. Then it performs specialized deep inspection, including advanced techniques such as full stack normalization and horizontal data stream-based inspection. These techniques enable Forcepoint NGFW to properly inspect all protocols and layers to expose AETs and traffic anomalies that evade other next-generation firewalls.

In addition, Forcepoint NGFW provides high-performance decryption of encrypted traffic such as HTTPS web connections, combined with granular privacy controls that keep your business – and your users – safe in a rapidly changing world. It can even limit access from specific endpoint applications, to lock down devices or prevent use of vulnerable software.

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

- High-performance decryption with granular privacy controls
- Whitelisting / blacklisting by client application and version for device lockdown
- 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
- Sidewinder security proxies for mission-critical applications

FORCEPOINT NEXT GENERATION FIREWALL (NGFW) SPECIFICATIONS

SUPPORTED PLATFORMS	
Appliances	Multiple hardware appliance options, ranging from branch office to data center installations
Cloud Infrastructure	Amazon Web Services, Microsoft Azure
Virtual Appliance	x86 64-bit based systems; VMware ESXi, VMware NSX, Microsoft Hyper-V, and KVM virtualized environment
Endpoint	Endpoint Context Agent (ECA)
Supported Roles	Firewall/VPN (layer 3), IPS mode (layer 2), Layer 2 Firewall, and Layer2-Layer3 Flexible deployment
Virtual Contexts	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, transparent deep packet inspection, advanced application level proxies for HTTP, HTTPS, and SSH, generic application level proxies for TCP and UDP, and whitelisting/blacklisting by application name and version
User Authentication	Internal user database, LDAP, Microsoft Active Directory, RADIUS, TACACS+, Forcepoint User ID (FUID) Services
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 network clustering: 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: IPv4 static, DHCP, PPPoA, PPPoE; IPv6 static, SLAAC, DHCPv6 • 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
Endpoint Application Lists	Control access by application name and version
Sidewinder Security Proxies	TCP, UDP, HTTP, HTTPS, SSH
Forcepoint Web Security Redirect	Redirect HTTP/HTTPS traffic to the Forcepoint Cloud Web Security via IPSec tunnel for inbound and outbound web content inspection

FORCEPOINT NEXT GENERATION FIREWALL (NGFW) 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, flexible route-based VPN including within customer domains • Hub and spoke, full mesh, partial mesh topologies • Forcepoint NGFW Multi-Link fuzzy-logic-based dynamic link selection • Forcepoint NGFW 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	
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

FORCEPOINT NEXT GENERATION FIREWALL (NGFW) SPECIFICATIONS CONTINUED

INSPECTION	
Anti-Botnet	• Decryption-based detection • Message length sequence analysis
Dynamic Context Detection	Protocol, application, file type
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,Integrated inspection with Sidewinder Security Proxies
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/SSL 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, half-open connection limit. • Separation of Control Plane and Data Plane
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 Forcepoint Security Management Center (SMC) • Current coverage of approximately 4,700 protected vulnerabilities

FORCEPOINT NEXT GENERATION FIREWALL (NGFW) SPECIFICATIONS CONTINUED

URL FILTERING	
URL Categorization	Classify the URL in HTTP and HTTPS with the Forcepoint cloud service
Custom URL Lists	Match locally own URL sets
Protocols	HTTP, HTTPS
Forcepoint URL categorization	Control access using category-based URL filtering updated from the 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
ADVANCED MALWARE DETECTION AND FILE CONTROL	
Protocols	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
File Filtering	Policy-based file filtering with efficient down selection process. Over 200 supported file types in 19 file categories
File Reputation	High speed cloud based Malware reputation checking and blocking. Optionally reputation checks from McAfee TIE over DxL bus.
Anti-Virus	Local antivirus scan engine*
Zero-Day Sandboxing	Forcepoint Advanced Malware Detection available both as cloud and on-premise service.
MANAGEMENT & MONITORING	
Management Interfaces	• Enterprise-level centralized management system with log analysis, monitoring and reporting capabilities • See the Forcepoint Security Management Center datasheet for details.
SNMP Monitoring	SNMPv1, SNMPv2c, and SNMPv3
Traffic Capturing	Console tcpdump, remote capture through Forcepoint Security Management Center
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)

*Local anti-malware scan is not available with 110/115 appliances.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_FORCEPOINT_NGFW_EN] 100033.092917