FORCEPOINT

Datasheet

FORCEPOINT Next Generation Firewall (NGFW)

Enterprise SD-WAN meets the #1 in network security

CUSTOMERS WHO SWITCH TO FORCEPOINT NGFW REPORT AN 86% DROP IN CYBERATTACKS, 53% LESS BURDEN ON IT, AND 70% LESS MAINTENANCE TIME.*

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

Always-On SD-WAN Connectivity for Enterprises

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

- **Active-active, mixed clustering.** Up to 16 nodes of different models running different versions can be clustered together. This provides superior networking performance and resilience, and enables security such as deep packet inspection and VPNs.
- **Seamless policy updates and software upgrades.** Forcepoint's industry-leading availability enables policy updates (and even software upgrades) to be seamlessly pushed to a cluster without interrupting service.
- **SD-WAN network clustering.** Extends high-availability coverage to network and VPN connections. Combines nonstop security with the ability to take advantage of local broadband connections in order to complement or replace expensive leased lines like MPLS.

Keep Pace With Changing Security Needs

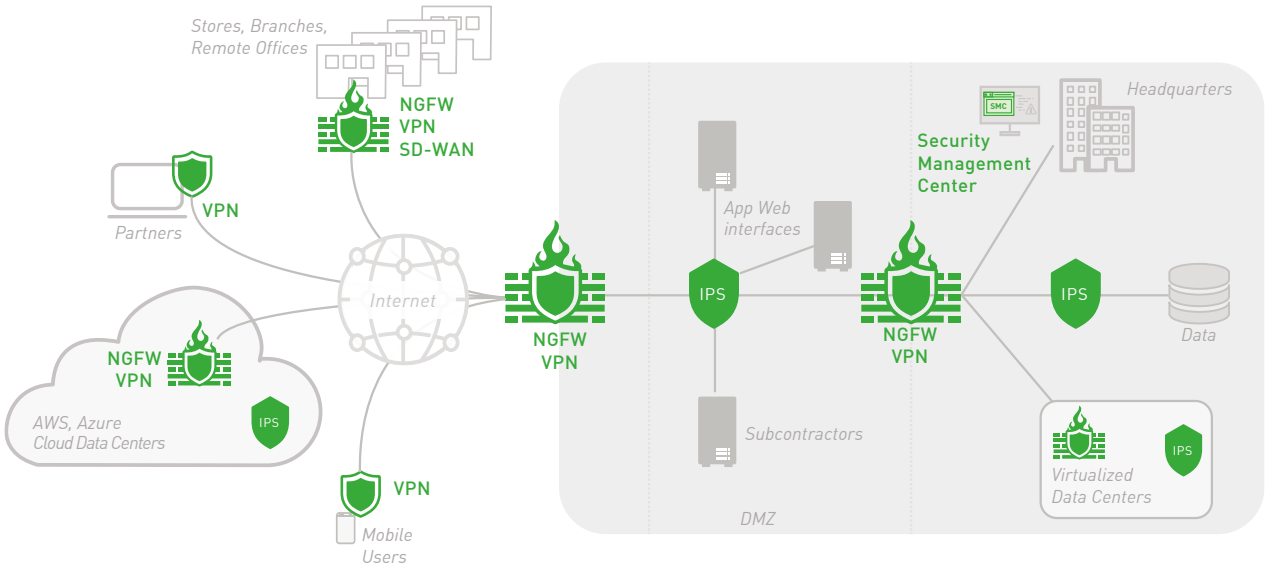
A unified software core enables Forcepoint NGFW to handle multiple security roles, from firewall/VPN to IPS to layer 2 firewall, in dynamic business environments. Forcepoint NGFWs can be deployed in a variety of ways (e.g., physical, virtual, cloud appliances), all managed from a single console.

Forcepoint uniquely tailors access control and deep inspection to each connection to provide high performance and security. It combines granular application control, intrusion prevention system (IPS) defenses, built-in virtual private network (VPN) control and mission-critical application proxies into 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 of every industry. Now you can fight back with application-layer exfiltration protection. Forcepoint NGFWs selectively and automatically whitelist or blacklist network traffic originating from specific 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.

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



One Platform with Many Deployment Options – All Managed from a Single Console

Unmatched Protection

Attackers have become experts in penetrating enterprise networks, applications, data centers and endpoints. Once inside, they steal intellectual property, customer information and other sensitive data, causing irreparable damage to businesses and their respective reputations.

New attack techniques can evade detection by traditional security network devices, including many name-brand firewalls, moving beyond the simple transmission of vulnerability exploits.

Evasions work at multiple levels to camouflage exploits and malware, making them invisible to traditional signature-based packet inspection. With evasions, even old attacks that have been blocked for years can be repackaged to compromise internal systems.

Forcepoint NGFW takes a different approach. Our industry-leading security engine is designed for all three stages of network defense: to defeat evasions, detect exploits of vulnerabilities and stop malware. It can be deployed transparently behind existing firewalls to add protection without disruption, or as full-featured NGFW for all-in-one security.

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

Business Outcomes

- **Faster rollout of branches, clouds or data centers**
- **Less downtime**
- **Greater security without disruption**
- **Fewer breaches**
- **Less exposure to new vulnerabilities while IT teams prepare to deploy new patches**
- **Lower TCO for network infrastructure and security**

Key Features

- **SD-WAN connectivity at enterprise scale**
- **High-availability clustering of devices and networks**
- **Automated, zero-downtime updates**
- **Policy-driven centralized management**
- **Actionable, interactive 360° visibility**
- **Built-in IPS with anti-evasion defenses**
- **Sidewinder security proxies for mission-critical applications**
- **Human-centric user and endpoint context**
- **High-performance decryption with granular privacy controls**
- **Whitelisting/blacklisting by client application and version**
- **CASB and Web Security integration**
- **Anti-malware sandboxing**
- **Unified software for physical, AWS, Azure, VMware deployments**

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, L2FW, or L2/L3 mixed mode) 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, Native LDAP, Microsoft Active Directory, RADIUS, TACACS+, Forcepoint User ID (FUID) Service, Client Certificate-based Authentication with Web Browser or IPsec Client
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, HTTPS, FTP, SMTP protocols redirection to content inspection server (CIS)

Forcepoint Next Generation Firewall (NGFW) Specifications *Continued*

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, FTP, TFTP, SFTP, DNS
Forcepoint Web Security Redirect	Redirect HTTP/HTTPS traffic to the Forcepoint Cloud Web Security for inbound and outbound web content inspection
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	
Multi-Layer Traffic Normalization/Full-Steam Deep Inspection	▸ Reconstructs and analyzes actual payloads to assure integrity of data streams ▸ Discards duplicate lower-level segments that could lead to ambiguities when reassembled
Anti-Evasion Defense	Stops out-of-order fragments, overlapping segments, protocol manipulation, obfuscation, encoding tricks
Dynamic Context Detection	Protocol, application, file type
Protocol-Specific Traffic Handling / Inspection	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
Granular Decryption of SSL/TLS Traffic	▸ High-performance decryption of HTTPS client and server streams ▸ Policy-driven controls to protect users' privacy and limit organizations' exposure to personal data ▸ TLS certificate validity checks and certificate domain name-based exemption list
Vulnerability Exploit Detection	▸ Protocol-independent, any TCP/UDP protocol with evasion and anomaly logging ▸ Virtual patching for both client and server CVE vulnerabilities ▸ Sophisticated fingerprint approach eliminates need for many signatures ▸ High-speed deterministic finite automata (DFA) matching engine handles new fingerprints quickly ▸ Continual update of fingerprints from Forcepoint
Custom Fingerprinting	▸ Protocol-independent fingerprint matching ▸ Regular expression-based fingerprint language with support for custom applications
Reconnaissance	TCP/UDP/ICMP scan, stealth, and slow scan detection in IPv4 and IPv6
Anti-Botnet	▸ Decryption-based detection and message length sequence analysis ▸ Automatically updated URL categorization to block or warn users away from botnet sites
Correlation	Local correlation, log server correlation
DoS/DDoS Protection	▸ SYN/UDP flood detection with concurrent connection limiting, interface-based log compression ▸ Protection against slow HTTP request methods, half-open connection limit. ▸ Separation of Control Plane and Data Plane
Blocking Methods	Direct blocking, connection reset, blacklisting (local and distributed), HTML response, HTTP redirect
Traffic Recording	Automatic traffic recordings/excerpts from misuse situations
Automatic Updates	▸ Continual dynamic updates through Forcepoint Security Management Center (SMC) ▸ Updates virtual patching and provides detection and prevention for emerging threats
URL FILTERING	
URL Categorization	Classify the URL in HTTP and HTTPS with the Forcepoint ThreatSeeker Intelligence cloud service
Custom URL Lists	Match locally own URL sets

*For more information, see Forcepoint Intrusion Prevention System datasheet.

Forcepoint Next Generation Firewall (NGFW) Specifications *Continued*

Protocols	HTTP, HTTPS
Forcepoint URL categorization	Control access using category-based URL filtering updated from the Forcepoint ThreatSeeker Intelligence
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
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 algorithm certificates, CSPN by ANSSI, (First Level Security Certification USGv6)

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

CONTACT
www.forcepoint.com/contact

[DATASHEET_FORCEPOINT_NEXTGENERATIONFIREWALL_EN] 100082.061218