

# Forcepoint Next Generation Firewall

**FORCEPOINT NEXT GENERATION FIREWALL (NGFW) CONNECTS AND PROTECTS DISTRIBUTED ENTERPRISE NETWORKS – DATA CENTERS, EDGE, BRANCHES, AND THE CLOUD – WITH THE HIGHEST EFFICIENCY, AVAILABILITY AND SECURITY. WITH FORCEPOINT NGFWs, ORGANIZATIONS CAN CUT TCO BURDENS, ELIMINATE PRACTICALLY ALL NETWORK DOWNTIME, AND SLASH THEFT WITHOUT COMPROMISING PERFORMANCE.**

**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 capabilities, performance and manageability across physical, virtual and cloud systems.

Forcepoint's unique Intelligence Inspection Engine 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 block network traffic originating from PCs, laptops, servers, file shares, and other endpoint devices based on highly granular endpoint contextual data. It goes beyond typical firewalls to prevent attempted ex-filtration of sensitive data from endpoints via unauthorized programs, web applications, users, and communications channels.

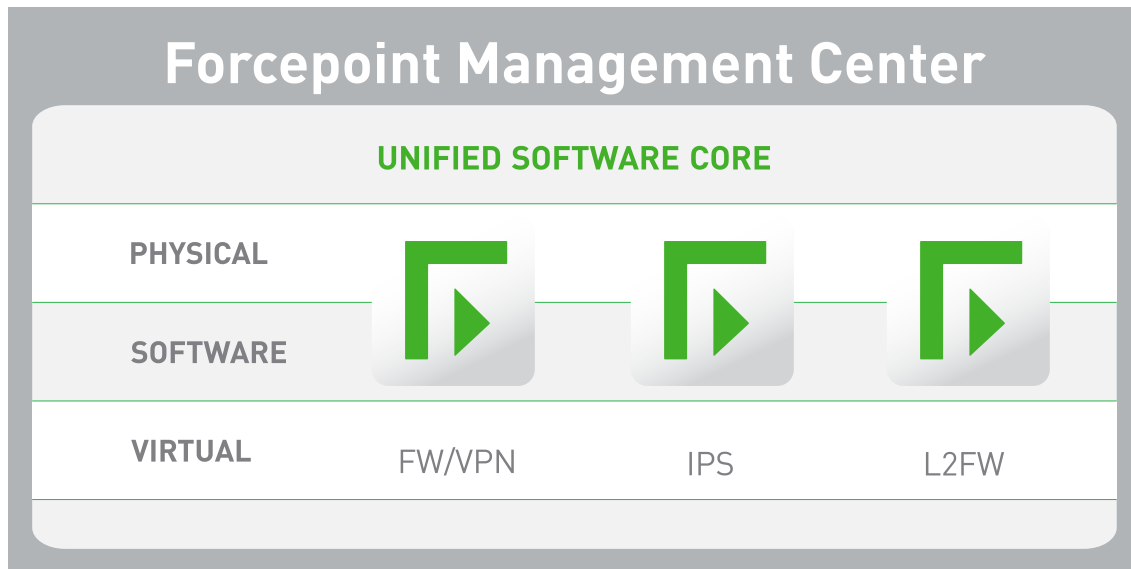
## **KEEP PACE WITH CHANGING SECURITY NEEDS**

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.

## **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.
- ▶ Transparent session failover: Provides industry-leading availability and serviceability of security systems. Policy updates and even software upgrades can be pushed to a cluster seamlessly without interrupting service.
- ▶ Multi-Link 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 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 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 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.

### 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
- 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	
<b>Appliances</b>	Multiple hardware appliance options, ranging from branch office to data center installations
<b>Cloud Infrastructure</b>	Amazon Web Services
<b>Virtual Appliance</b>	x86 64-bit based systems; VMware ESXi and KVM virtualized environment
<b>Supported Roles</b>	Firewall/VPN (layer 3), IPS mode (layer 2), and Layer 2 Firewall
<b>Virtual Contexts</b>	Virtualization to separate logical contexts (FW, IPS, or L2FW) with separate interfaces, addressing, routing, and policies
FIREWALL/VPN FUNCTIONAL ROLE	
<b>General</b>	Stateful and stateless packet filtering, transparent deep packet inspection, advanced application level proxies for HTTP and SSH, generic application level proxies for TCP and UDP
<b>User Authentication</b>	Internal user database, LDAP, Microsoft Active Directory, RADIUS, TACACS+
<b>High Availability</b>	<ul style="list-style-type: none"> <li>• Active-active/active-standby firewall clustering up to 16 nodes</li> <li>• Stateful failover (including VPN connections)</li> <li>• Server load balancing</li> <li>• Link aggregation (802.3ad)</li> <li>• Link failure detection</li> </ul>
<b>ISP Multi-Homing</b>	Multi-Link network clustering: high availability and load balancing between multiple ISPs, including VPN connections, Multi-Link VPN link aggregation, QoS-based link selection
<b>IP Address Assignment</b>	<ul style="list-style-type: none"> <li>• FW clusters: static, IPv4, IPv6</li> <li>• FW single nodes: IPv4 static, DHCP, PPPoA, PPPoE; IPv6 static, SLAAC, DHCPv6</li> <li>• Services: DHCP Server for IPv4 and DHCP relay for IPv4</li> </ul>
<b>Address Translation</b>	<ul style="list-style-type: none"> <li>• IPv4, IPv6</li> <li>• Static NAT, source NAT with port address translation (PAT), destination NAT with PAT</li> </ul>
<b>Routing</b>	Static IPv4 and IPv6 routes, policy-based routing, static multicast routing
<b>Dynamic Routing</b>	IGMP proxy, RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM-SM, PIM-SSM
<b>IPv6</b>	Dual stack IPv4/IPv6, ICMPv6, DNSv6
<b>SIP</b>	Allows RTP media streams dynamically, NAT traversal, deep inspection, interoperability with RFC3261-compliant SIP devices
<b>CIS Redirection</b>	HTTP, FTP, SMTP protocols redirection to content inspection server (CIS)
<b>Geo-Protection</b>	Control access by source/destination country or continent
<b>IP Address List</b>	Control access by predefined IP categories or using custom IP address list
<b>URL List</b>	Control access by custom URL list
<b>Sidewinder Security Proxies</b>	TCP, UDP, HTTP, SSH
<b>Forcepoint Web Security Redirect</b>	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	
<b>Protocols</b>	IKEv1, IKEv2, and IPsec with IPv4 and IPv6
<b>Encryption</b>	AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES
<b>Message Digest Algorithms</b>	AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512
<b>Diffie-Hellman</b>	DH group 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
<b>Authentication</b>	RSA, DSS, ECDSA signatures with X.509 certificates, pre-shared keys, hybrid, XAUTH, EAP
<b>Other</b>	<ul style="list-style-type: none"> <li>• IPCOMP deflate compression</li> <li>• NAT-T</li> <li>• Dead peer detection</li> <li>• MOBIKE</li> </ul>
<b>Site-to-Site VPN</b>	<ul style="list-style-type: none"> <li>• Policy-based VPN, flexible route-based VPN</li> <li>• Hub and spoke, full mesh, partial mesh topologies</li> <li>• Forcepoint NGFW Multi-Link fuzzy-logic-based dynamic link selection</li> <li>• Forcepoint NGFW Multi-Link modes: load sharing, active/standby, link aggregation</li> </ul>
<b>Mobile VPN</b>	<ul style="list-style-type: none"> <li>• VPN client for Microsoft Windows</li> <li>• Automatic configuration updates from gateway</li> <li>• Automatic failover with Multi-Link</li> <li>• Client security checks</li> <li>• Secure domain logon</li> </ul>
SSL VPN	
<b>Client-Based Access</b>	Supported platforms: Android 4.0, Mac OS X 10.7, and Windows Vista SP2 (and newer versions)
<b>Clientless Access</b> <i>(Not available for 110 and 115 models)</i>	Web Portal access to HTTP-based services via predefined services and free form URLs



**FORCEPOINT NEXT GENERATION FIREWALL (NGFW) SPECIFICATIONS** CONTINUED

INSPECTION	
<b>Anti-Botnet</b>	<ul style="list-style-type: none"> <li>• Decryption-based detection</li> <li>• Message length sequence analysis</li> </ul>
<b>Dynamic Context Detection</b>	Protocol, application, file type
<b>Protocol-Specific Normalization/ Inspection/Traffic Handling</b>	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
<b>Protocol-Independent Fingerprinting</b>	Any TCP/UDP protocol
<b>Evasion and Anomaly Detection</b>	<ul style="list-style-type: none"> <li>• Multilayer traffic normalization</li> <li>• Vulnerability-based fingerprints</li> <li>• Fully upgradable software-based inspection engine</li> <li>• Evasion and anomaly logging</li> </ul>
<b>Custom Fingerprinting</b>	<ul style="list-style-type: none"> <li>• Protocol-independent fingerprint matching</li> <li>• Regular expression-based fingerprint language</li> <li>• Custom application fingerprinting</li> </ul>
<b>TLS Inspection</b>	<ul style="list-style-type: none"> <li>• HTTPS client and server stream decryption and inspection</li> <li>• TLS certificate validity checks</li> <li>• Certificate domain name-based exemption list</li> </ul>
<b>Correlation</b>	Local correlation, log server correlation
<b>DoS/DDoS Protection</b>	<ul style="list-style-type: none"> <li>• SYN/UDP flood detection</li> <li>• Concurrent connection limiting, interface-based log compression</li> <li>• Protection against slow HTTP request methods</li> </ul>
<b>Reconnaissance</b>	TCP/UDP/ICMP scan, stealth, and slow scan detection in IPv4 and IPv6
<b>Blocking Methods</b>	Direct blocking, connection reset, blacklisting (local and distributed), HTML response, HTTP redirect
<b>Traffic Recording</b>	Automatic traffic recordings/excerpts from misuse situations
<b>Updates</b>	<ul style="list-style-type: none"> <li>• Automatic dynamic updates through Forcepoint Security Management Center (SMC)</li> <li>• Current coverage of approximately 4,700 protected vulnerabilities</li> </ul>



**FORCEPOINT NEXT GENERATION FIREWALL (NGFW) SPECIFICATIONS** CONTINUED

<b>URL FILTERING</b>	
<b>URL Categorization</b>	Classify the URL in HTTP and HTTPS with the Forcepoint cloud service
<b>Custom URL Lists</b>	Match locally own URL sets
<b>Protocols</b>	HTTP, HTTPS
<b>Forcepoint URL categorization</b>	Control access using category-based URL filtering updated from the Forcepoint cloud
<b>Database</b>	<ul style="list-style-type: none"> <li>• More than 280 million top-level domains and sub-pages (billions of URLs)</li> <li>• Support for more than 43 languages, 82 categories</li> </ul>
<b>Safe Search</b>	Safe search usage enforcing for Google, Bing, Yahoo, DuckDuckGo web searches
<b>ADVANCED MALWARE DETECTION AND FILE CONTROL</b>	
<b>Protocols</b>	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
<b>File Filtering</b>	Policy-based file filtering with efficient down selection process. Over 200 supported file types in 19 file categories
<b>File Reputation</b>	High speed cloud based Malware reputation checking and blocking. Optionally reputation checks from McAfee TIE over DxL bus.
<b>Anti-Virus</b>	Local antivirus scan engine*
<b>Zero-Day Sandboxing</b>	Forcepoint Advanced Malware Detection cloud service. Optionally file sandboxing with McAfee ATD appliance
<b>MANAGEMENT &amp; MONITORING</b>	
<b>Management Interfaces</b>	<ul style="list-style-type: none"> <li>• Enterprise-level centralized management system with log analysis, monitoring and reporting capabilities</li> <li>• See the Forcepoint Security Management Center datasheet for details.</li> </ul>
<b>SNMP Monitoring</b>	SNMPv1, SNMPv2c, and SNMPv3
<b>Traffic Capturing</b>	Console tcpdump, remote capture through Forcepoint Security Management Center
<b>High Security Management Communication</b>	256-bit security strength in engine-management communication
<b>Security Certifications</b>	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](http://www.forcepoint.com/contact)

**ABOUT FORCEPOINT**

© 2017 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

[DATASHEET\_FORCEPOINT\_NGFW\_EN] 100033.032417