Forcepoint

Datasheet

Intrusion Prevention with Forcepoint Next-Gen Firewall

Forcepoint offers one of the industry's highest-rated Intrusion Prevention System (IPS) for protecting distributed enterprise networks – across data centers, offices, branches, and the cloud.

Forcepoint's network security solutions offer one of the industry's most secure Intrusion Prevention Systems. Top-rated in independent tests, Forcepoint Next-Gen Firewall's can be deployed as a standalone Layer 2 IPS device or as part of a full-featured Layer 3 Next-Gen Firewall in physical, virtual, and cloud environments. It defeats evasions, exploits, and malware that attackers use to penetrate and spread within enterprise networks.

Unique Architecture for Efficacy and Speed

Forcepoint Next-Gen Firewall's uses a dynamic stream-based approach to inspection that goes beyond simple packet inspection. It reconstructs and examines the actual payloads, defeating evasion techniques that camouflage exploits and malware.

In addition, high-speed, granular decryption unmasks attacks that attempt to hide within SSL/TLS traffic. Forcepoint analyzes each payload stream, decoding the various layers of protocols to look for abnormal or malformed protocol setup, metadata, and headers.

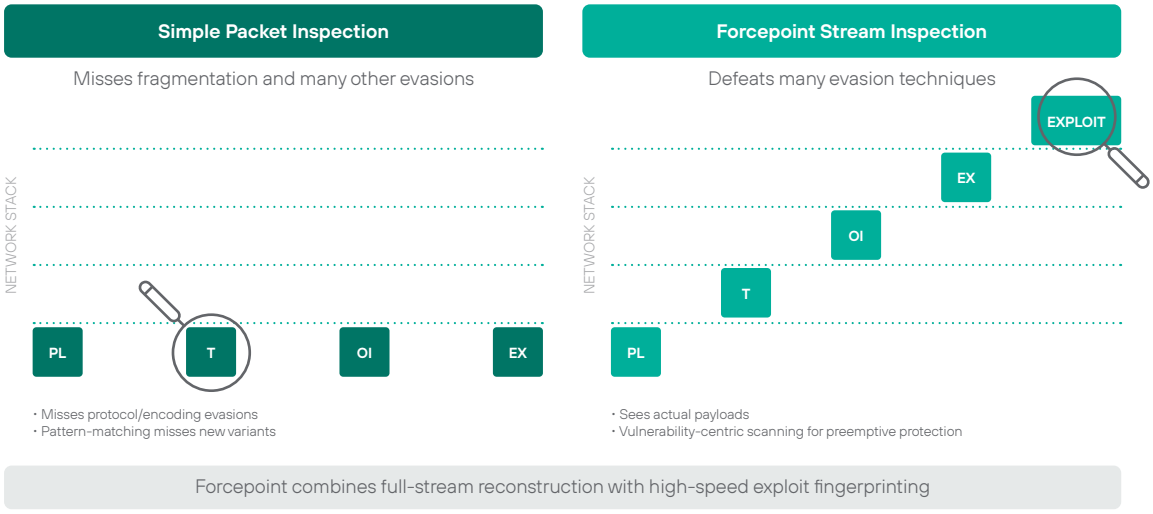
Forcepoint then applies advanced techniques to examine transmission contents for signs of exploits against vulnerabilities in many types of systems. Unlike verbose pattern-based signature mechanisms, Forcepoint's more sophisticated approach enables such attacks to be identified with a single, concise fingerprint. Fingerprints are matched using high-speed deterministic finite automata (DFA) tailored to each protocol context, enabling new fingerprints to be incorporated with almost no impact on CPU resources.

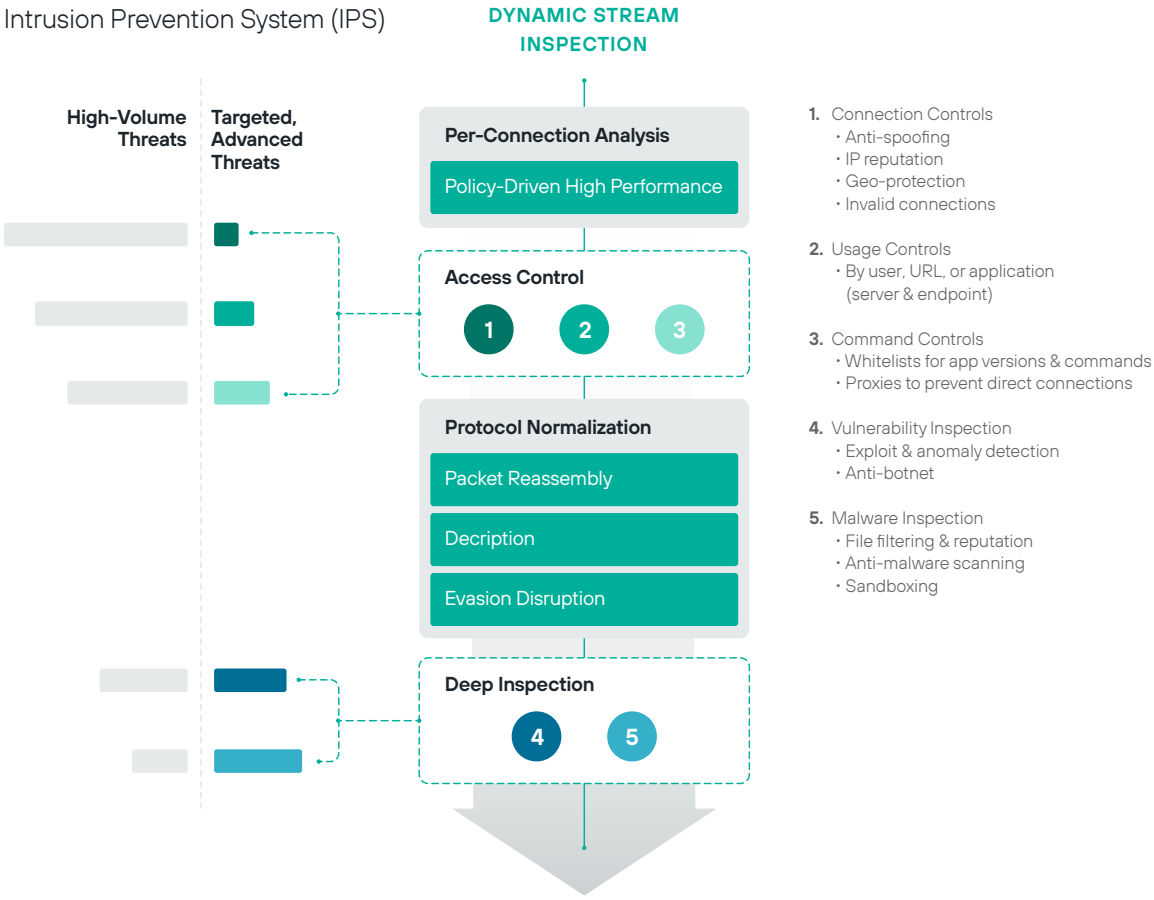
Continual Updates to Keep Ahead of Attackers

Forcepoint's global research team is constantly examining threat intelligence feeds, vulnerability reports from different sources, and a variety of test systems to analyze exploits and vulnerabilities. New fingerprints are published as needed through our cloud service and are automatically downloaded by Forcepoint network security systems. This proactive approach gives IT teams time to analyze newly published patches and implement remediation efforts without fear of immediate compromise.

Stopping Zero-Days and Unwanted Content

Forcepoint's network security products also provide multiple layers of defense against previously unknown attacks and undesirable content. Transmitted files go through rigorous reputation and malware scanning, and new threats like zero-day attacks can be uncovered with our advanced sandboxing technology. Forcepoint is one of the pioneers in categorizing and filtering websites and content; with our IPS devices and firewalls, organizations can more easily comply with workplace regulations, limit exposure to personal data, and prevent users from going to websites with dangerous content in the first place.





Fail-Open Resilience

Forcepoint's appliances support a range of modular network cards, including fail-open interfaces that keep traffic running even if the Next-Gen Firewall loses power.

Protection to Keep Your Organization Running

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 your trust and reputations.

Internet attacks are moving beyond simply transmitting exploits of vulnerabilities. Increasingly, new techniques are being used to evade detection by traditional security network devices, including many name-brand firewalls.

These 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 suddenly be used to compromise internal systems.

Forcepoint takes a different approach. Our industry–leading IPS 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 part of our full-featured Next-Gen Firewall for all-in-one security.

All Forcepoint network security products are continually updated, centrally managed, and can seamlessly share security policies and dashboards throughout your network. With Forcepoint, you can keep your organization safe–reliably, consistently, and efficiently–throughout your data centers, office networks, branch locations, or cloud environments.

Outcomes

- Fewer breaches
- Greater security without disruption
- Less exposure to new vulnerabilities while IT teams prepare to deploy new patches
- Safer rollout of branches, clouds, or datacenters
- Lower Total Cost of Ownership (TCO) for security and network infrastructure

Key Features

- Deployment as a Layer 2 IPS, Layer 2 Next-Gen Firewall or as part of a Layer 3 Next-Gen Firewall
- Combined Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to both protect and defend
- Stream inspection that examines actual payloads
- Pioneer in anti-evasion defenses
- High-speed decryption with granular privacy controls
- Protocol abnormality and misuse detection
- Exploit and malware detection via high-speed DFA
- Denial of Service (DoS) detection
- Anti-bot defenses
- Zero-day sandboxing via cloud or on-premises appliance
- Industry-leading URL Filtering
- Modular fail-open network interfaces for appliances

Forcepoint Next-Gen Firewall Specifications

SUPPORTED PLATFORMS	
Appliances	Multiple series of modular appliances for deployment in data centers, at network edges, and in branches
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
Deployment Modes	Standalone IPS (layer 2, with optional fail-open network interface modules), part of NGFW (layer 3)
Virtual Context	Virtualization to separate logical contexts with separate interfaces and policies

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 detection and protection › Support for Snort signature integrations to customize and enhance overall security posture › 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

Forcepoint Next-Gen Firewall Specifications, continued

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
File Anti-Virus Scanning	Local anti-virus scan engine*
Zero-Day Sandboxing	Forcepoint Advanced Malware Detection available for Forcepoint NGFW as a cloud, on premise, or even an air-gapped service similar to as used by Forcepoint Web Security, Forcepoint Email Security, and Forcepoint CASB

URL FILTERING	
URL Categorization	Powered by Forcepoint ThreatSeeker Intelligence, same as used by Forcepoint Web Security and Forcepoint Email Security
Automatic Updates	Continually updated as new sites are analyzed
Enforcement of Category-based Access Policies	Forcepoint NGFW URL Filtering available as an add-on subscription

MANAGEMENT & MONITORING	
Management Interfaces	Enterprise-level centralized management system with log analysis, monitoring, and reporting capabilities (see 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
Endpoint Context Agent	Whitelisting and blacklisting of client applications running on hosts and end user devices. Can prevent untrusted files from making outbound connections and enables granular controls that can be customized to fit your organization needs.

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