Forcepoint

Datasheet

Intrusion Prevention with Forcepoint Next-Gen Firewall

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 Layer 2 Intrusion Prevention System (IPS) using optional fail-open network interface modules
- Combined Intrusion Detection System (IDS) and 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 deterministic finite automata (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 provides one of the industry's top-rated IPS, delivering robust protection for distributed enterprise networks across data centers, offices, branches, and the cloud.

Forcepoint's network security solutions feature one of the industry's most secure Intrusion Prevention Systems. Highly rated in independent tests, the Forecpoint Next-Gen Firewall (NGFW) can be deployed as a standalone Layer 2 IPS device or integrated as part of a comprehensive Layer 3 NGFW, adaptable to physical, virtual, and cloud environments. It effectively blocks evasions, exploits, and malware, preventing attackers from penetrating and spreading within enterprise networks.

Unique Architecture for Efficacy and Speed

Forcepoint utilizes a dynamic, stream-based inspection method that surpasses basic packet analysis. It reconstructs and inspects actual payloads, overcoming evasion techniques that conceal exploits and malware. Additionally, high-speed, granular decryption reveals attacks concealed within SSL/TLS traffic. Forcepoint analyzes each payload stream, decoding multiple protocol layers to detect abnormal or malformed protocol setups, metadata, and headers.

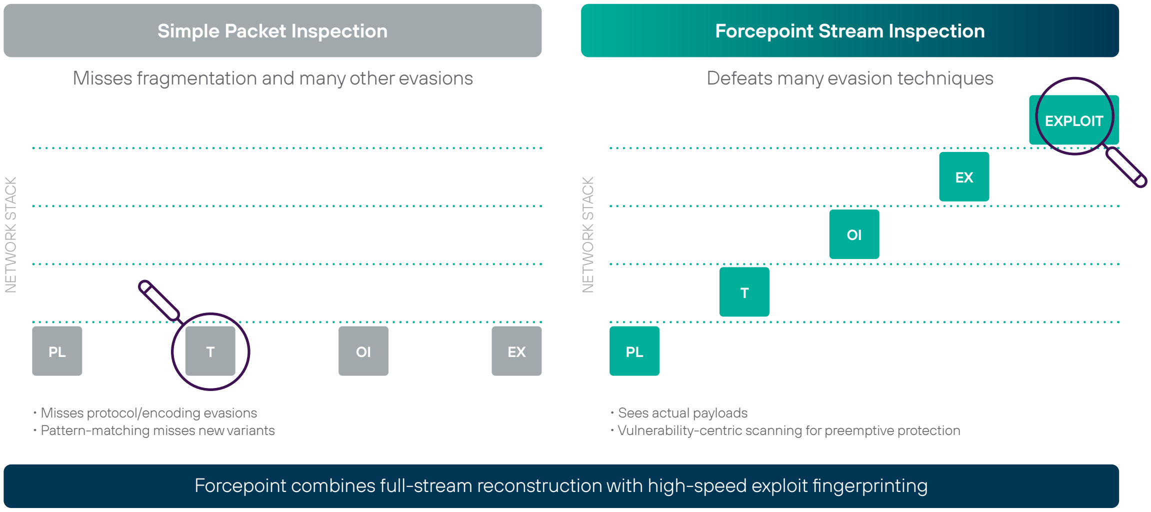
Forcepoint applies advanced methods to analyze transmission contents for exploit signs targeting various system vulnerabilities. Unlike verbose pattern-based signatures, Forcepoint's refined approach identifies these attacks with a single, precise fingerprint. Fingerprints are matched using high-speed DFA specific to each protocol, allowing new fingerprints to be integrated with minimal impact on CPU resources.

Continual Updates to Keep Ahead of Attackers

Forcepoint's global research team continuously monitors threat intelligence feeds, vulnerability reports from diverse sources, and various test systems to analyze exploits and vulnerabilities. New fingerprints are rapidly published through our cloud service and automatically updated on Forcepoint network security systems. This proactive strategy allows IT teams to review newly released patches and implement remediation efforts without the risk of immediate compromise.

Stopping Zero-Days and Unwanted Content

Forcepoint's network security products offer robust, multi-layered defense against both new and unknown threats. Files in transit undergo thorough reputation and malware scanning, while our advanced sandboxing technology detects emerging threats, including zero-day attacks. As pioneers in website and content categorization, Forcepoint's IPS devices and firewalls help organizations adhere to workplace regulations, protect personal data, and block access to harmful websites before users can reach them.



Simple Packet Inspection

Misses fragmentation and many other evasions

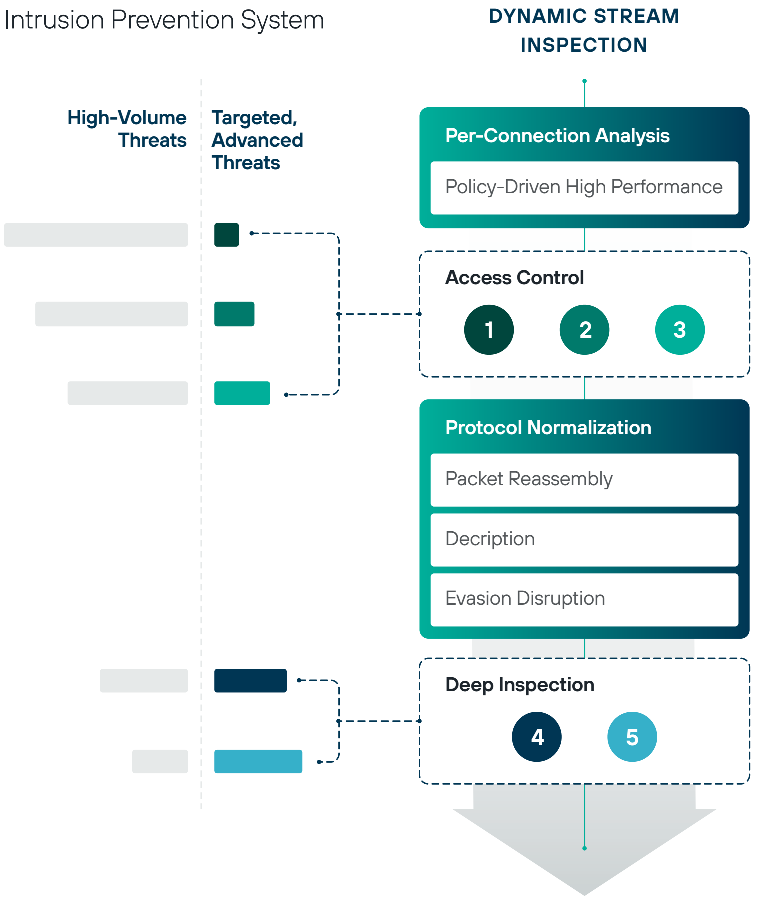
- Misses protocol/encoding evasions
- Pattern-matching misses new variants

Forcepoint Stream Inspection

Defeats many evasion techniques

- Sees actual payloads
- Vulnerability-centric scanning for preemptive protection

Forcepoint combines full-stream reconstruction with high-speed exploit fingerprinting



Intrusion Prevention System

DYNAMIC STREAM INSPECTION

High-Volume Threats

Targeted, Advanced Threats

Per-Connection Analysis

Policy-Driven High Performance

Access Control

Protocol Normalization

Packet Reassembly

Decription

Evasion Disruption

Deep Inspection

1. Connection Controls
   - Anti-spoofing
   - IP reputation
   - Geo-protection
   - Invalid connections
2. Usage Controls
   - By user, URL, or application (server & endpoint)
3. Command Controls
   - Whitelists for app versions & commands
   - Proxies to prevent direct connections
4. Vulnerability Inspection
   - Exploit & anomaly detection
   - Anti-botnet
5. Malware Inspection
   - File filtering & reputation
   - Anti-malware scanning
   - Sandboxing

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

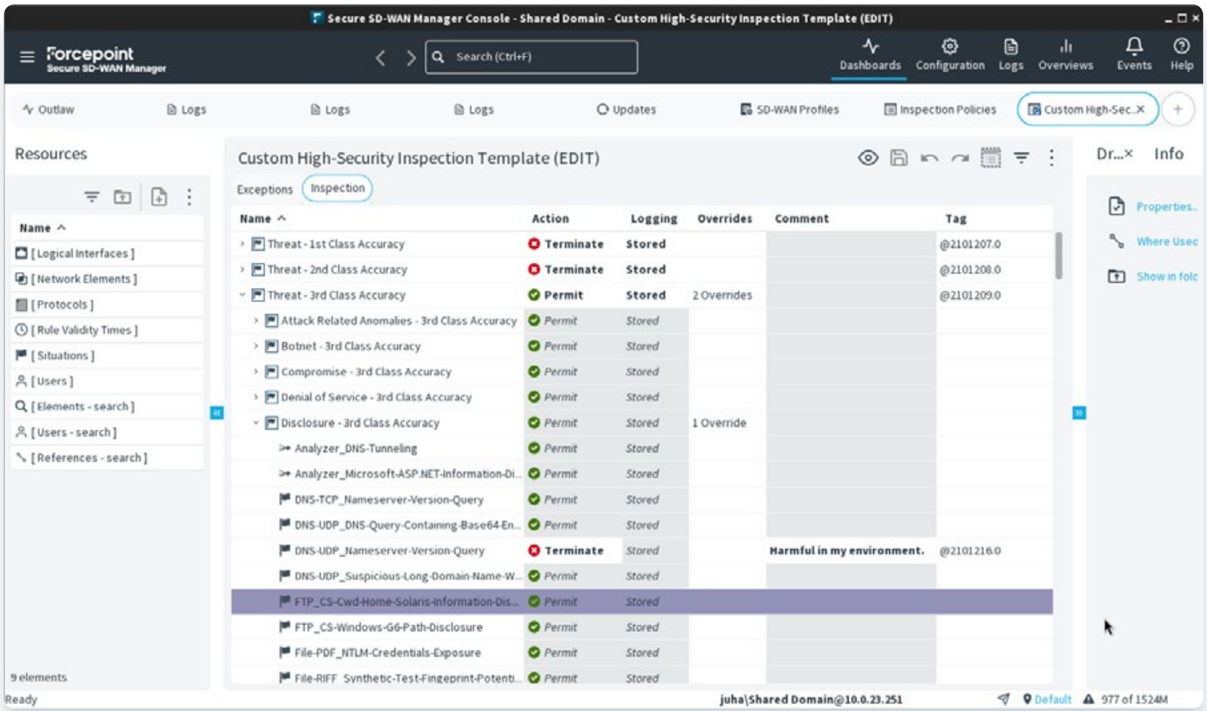
Every day, attackers grow more sophisticated in their attempts to penetrate enterprise networks, cloud environments, applications, data centers and endpoints. Once inside, they can steal intellectual property, customer information, and other sensitive data, leading to sever damage to your brand reputation and operational trust.

Today's cyber threats have evolved beyond merely exploiting vulnerabilities. Attackers are now employing advanced techniques to bypass detection by traditional security measures, including widely recognized firewall solutions.

These advanced techniques operate across multiple layers, effectively disguising exploits and malware to evade detection by conventional signature-based security tools. This means that even well-known attacks, previously mitigated, can resurface with the potential to compromise internal systems.

Forcepoint takes a highly unique and comprehensive approach to network security. Our industry-leading IPS engine is purpose-built to cover all three critical stages of defense: to defeat evasions, detect vulnerabilities exploits, and stop malware. It can be seamlessly deployed behind existing firewalls to enhance your security without causing disruptions or as part of our fully integrated NGFW for a complete, all-in-one security solution.

All Forcepoint network security products are continually updated, centrally managed, and designed to seamlessly share security policies and insights across your entire network. Whether you're protecting data centers, office networks, branch locations, or cloud environments, Forcepoint ensures your organization remains secure.



Custom High-Security Inspection Template (EDIT)

Name	Action	Logging	Overrides	Comment	Tag
Threat - 1st Class Accuracy	Terminate	Stored			@2101207.0
Threat - 2nd Class Accuracy	Terminate	Stored			@2101208.0
Threat - 3rd Class Accuracy	Permit	Stored	2 Overrides		@2101209.0
Attack Related Anomalies - 3rd Class Accuracy	Permit	Stored			
Botnet - 3rd Class Accuracy	Permit	Stored			
Compromise - 3rd Class Accuracy	Permit	Stored			
Denial of Service - 3rd Class Accuracy	Permit	Stored			
Disclosure - 3rd Class Accuracy	Permit	Stored	1 Override		
Analyzer_DNS-Tunneling	Permit	Stored			
Analyzer_Microsoft-ASP.NET-Information-Di...	Permit	Stored			
DNS-TCP_Nameserver-Version-Query	Permit	Stored			
DNS-UDP_DNS-Query-Containing-Base64-En...	Permit	Stored			
DNS-UDP_Nameserver-Version-Query	Terminate	Stored		Harmful in my environment.	@2101216.0
DNS-UDP_Suspicious-Long-Domain-Name-W...	Permit	Stored			
FTP_CS-Cwd-Home-Solaris-Information-Dis...	Permit	Stored			
FTP_CS-Windows-G6-Path-Disclosure	Permit	Stored			
File-PDF_NTLM-Credentials-Exposure	Permit	Stored			
File-RIFF_Synthetic-Test-Fingeprint-Potenti...	Permit	Stored			

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	IPS deployment will be done with Layer 2 interfaces and optional fail-open network interface modules
Virtual Context	Virtualization to separate logical contexts with separate interfaces and policies

INSPECTION	
Multi-layer Traffic Normalization / Full-Stream 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 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 and Protection 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 SMC datasheet for details)
SNMP Monitoring	SNMPv1, SNMPv2c, and SNMPv3
Traffic Capturing	Console tcp dump, remote capture through Forcepoint 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, 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 Forcepoint NGFW 60 series appliances.

Forcepoint

forcepoint.com/contact