Intrusion Prevention System
1100 Series

For regional offices, 3-6 Gbps inspection throughput

Traditional network security is no match for today's sophisticated threat landscape. Thwart attackers' attempts to evade detection using the industry's most secure intrusion prevention system (IPS). The Forcepoint 1100 Series IPS is ideal for regional offices that require best-in-class protection without sacrificing performance.

Key features

- Deploy as a layer 2 IPS or as part of a layer 3 NGFW
- Full-stream deep inspection of payloads
- Industry-leading anti-evasion defense
- Anti-botnet protection
- Protocol abnormality and misuse detection
- Reconnaissance detection
- DoS/DDoS protection
- Granular decryption of SSL/TLS traffic
- Centralized management for up to 2,000 IPS and NGFW appliances across all types of deployments
- Security policy updates with just a few clicks
- Access and security policies updates with just a few clicks
- URL Filtering and Advanced Malware Detection (sandboxing) options

Keep one step ahead of cyber threats

Internet attacks are moving beyond the simple exploit of vulnerabilities. Increasingly, new techniques are being used to evade detection by traditional network devices, including many brand-name firewalls.

Forcepoint takes a different approach. The 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 the full-featured NGFW for all-in-one security.

Forcepoint uses dynamic stream-based technology that goes beyond simple packet inspection to reconstruct and examine payloads in order to defeat evasions and malware. High-speed granular decryption unmasks attempts to hide within SSL/TLS traffic, and zero day attacks are uncovered using advanced sandboxing technology.

Greater security without disruption

Resilience is built into every level of Forcepoint IPS to keep your business running. Forcepoint IPS can be deployed in serial clusters to keep the network running in the event of a service disruption to a single device, which means device software, security patches, and policies can be updated at any time without dropped packets. It also supports a range of modular network interface cards, including fail-open interfaces that keep traffic running even if the IPS loses power.

Reduce the time spent on managing network security

Forcepoint makes it simple to manage network security in highly distributed environments. With the Forcepoint Security Management Center (SMC), network security teams can manage up to 2,000 Forcepoint IPS and NGFW appliances from one centralized location, regardless of them being physical, virtual, or cloud-based. Zero-touch deployment allows IPS installation at remote locations without an on-site technician, and security policies can be updated across all appliances with just a few clicks.

INSPECTION	
Multi-layer traffic normalization/ full stream deep inspection	• Reconstructs and analyzes 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 by 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

PERFORMANCE[1]	N1101	N1105
NGFW/NGIPS throughput (HTTP 21kB payload)	1.5 Gbps	3 Gbps
Max inspection throughput UDP 1518 byte	3 Gbps	6 Gbps
TLS 1.2 inspection performance (44kB payload)	800 Mbps	1.6 Gbps
Concurrent inspected TCP connections	500,000	1 Million
Max number of concurrent inspected HTTP connections	450,000	1 Million
Virtual contexts default/maximum	5/25	10/100

[1] Performance values reflect maximums measured under test conditions and may vary based on configuration and features enabled

NETWORK INTERFACES	N1101 & N1105
Fixed Ethernet interfaces	8 x GE RJ45, 2 x 10Gbps SFP+
Gigabit Ethernet - copper ports	8-16
10 gigabit Ethernet ports	2-6
Fail-open interfaces	1 GbE: 0-4, 10GbE: 0-2
Connectors	3 x USB, 1 x serial, VGA, IPMI Ethernet

Contact: forcepoint.com/contact

FORCEPOINT

[IPS-1100 SERIES-GLOBAL-DATASHEET-US-EN] 100105.100919