Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.

World Class Next Generation IPS Capabilities

Today, sophisticated and high volume attacks are the challenges that every organization must recognize. These attacks are evolving, infiltrating ever-increasing vectors and complex network environments. The result is an urgent need for network protection while maintaining the ability to efficiently provide demanding services and applications.

FortiOS's IPS functionality is an industry-proven network security solution that scales up to over 50 Gbps of in-line protection. Powered by purpose-built hardware and FortiASICs, FortiOS is able to achieve attractive TCO while meeting performance requirements. IPS is easy to set up, yet offers feature-rich capabilities, with contextual visibility and coverage. It is kept up-to-date by research teams that work 24 hours a day worldwide, in order to detect and deter the latest known threats as well as zero-day attacks.

Rich feature set for protecting your applications, data and users.

- Validated best-in-class security and capacity with proven coverage and high performance.

- Comprehensive protection provided by a signatures-based IPS engine, protocol anomaly scanning, and DDOS mitigation

- Flexible deployment options and actionable implementations for a wide array of network integration and operation requirements. .

Key Features & Benefits

High Performance IPS, powered by FortiASIC	Low latency and high capacity ensure business applications are not affected while security is enforced.
Best-in-class security with superior coverage	Protects critical digital resources from both internal exploits and external cybercriminals, even if sophisticated attacks are crafted.
Backed by FortiGuard Labs that deliver real-time protection.	Maintains up-to-date and proactive protection against latest known threats and newly discovered hacking techniques while allowing time for organizations to patch vulnerable systems.

Technical Documentation
docs.fortinet.com

Video Tuturials & Guides
video.fortinet.com

Knowledgebase
kb.fortinet.com

www.fortinet.com

Tested and Proven Protection

Not only have FortiGates been deployed in some of the largest enterprises in the world since 2002, FortiOS IPS components and FortiGuard IPS signatures are periodically tested and certified by well-known external labs. These independent certifications ensure that solutions delivered to customers are of the highest standards in performance, coverage, and accuracy.

Real-Time & Zero-day Protection

The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

FortiGuard IPS service quick facts

- Over 8,000 signatures consisting of 15,649 rules

- Approximately 190,000 network intrusion attempts resisted per minute

- Over 90 signatures are updated or added per week

- Over 140 Zero-day vulnerabilities discovered to date.

This update service is backed by a team of threat experts and a close relationship with major application vendors. The best-in-class team also uncovers significant zero-day vulnerabilities continuously, providing FortiGate units with advanced protection ahead of vendor patches.

Uncompromised Performance

The FortiASICS Content Processor (CP) accelerates content processing, which is traditionally done completely by the CPU. The CP reduces the resources required by the CPU when matching an incoming file against the signature database, thus improving system performance and stability.

Protocol Decoders and Anomaly Detection

Protocol decoders are required to assemble the packets and detect suspicious, nonconforming sessions that resemble known attacks or are non-compliant to RFC or standard implementation.

FortiOS offers one of the most comprehensive arrays of protocol decoders in the industry, providing customers with significantly wide coverage in all kinds of environments.
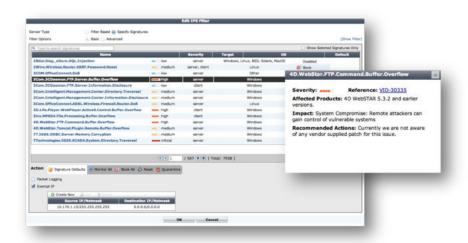
Acceleration with Content Processor

The FortiASICS Content Processor (CP) accelerates content processing traditionally performed completely by the CPU. The CP reduces the resources required by the CPU when matching an incoming file against the signature database, thus improving system performance and stability.

Pattern & Rate-Based Signatures

The pattern signature matching technique is essential in IPS implementation due to its high level of precision and accuracy. FortiOS offers administrators robust pattern signature selection using filters based on severity, target, operating system, application, and protocol. Each of the 6,000+ signatures has a direct link to its detailed entry on the threat encyclopedia. After selection, administrators are able to assign associated actions such as monitoring, blocking, or resetting the session.

Rate-based IPS signatures protect networks against application-based DoS and brute force attacks. Administrators can configure nearly 30 rate-based IPS signatures and tune them to their needs. Threshold (incidents per minute) and an action to take when the threshold is reached can be assigned to each signature. If the action is set to block, then a timeout period can be set so that the block is removed after a specified duration.

DoS and DDoS Mitigation

DoS policies can help protect against DDoS attacks that aim to overwhelm server resources. In FortiOS, the DoS scans precede the policy engine at the incoming interfaces, thus eliminating unnecessary sessions from the firewall process and state table entry during a surge of attack traffic. This helps to safeguard the firewall from overloading and allows it to perform optimally.

FortiOS DoS policies can be configured to detect and block floodings, port scans, and sweeps. Administrators can set baselines for the amount of concurrent sessions from sources or to destinations. The settings utilize thresholds and can be applied to UDP, TCP, ICMP, IP, and SCTP.

Network interfaces associated with a port attached to a Network Processor (NP) can be configured to offload anomaly checking, further offloading the CPU for greater performance. Some of the anomaly traffic dropped includes LAND attacks, IP protocol with malformed options, and WinNukes.

Quarantine Attacks

FortiOS offers sophisticated automatic attack quarantine capabilities which allow organizations to proactively prevent further attacks from known attackers over a predefined duration. Quarantining can be used to protect potentially vulnerable servers until a more permanent defense can be put in place.

Packet Logging

Administrators may choose to automatically perform IPS packet logging, which saves packets for detailed analysis when an IPS signature is matched. Saved packets can be viewed and analyzed on the FortiGate unit or by using third-party analysis tools. Packet logging is also useful in determining false positives.

Custom Signatures

Custom IPS signatures can be created to further extend protection. For example, you can use custom IPS signatures to protect unusual or specialized applications, or even custom platforms from known and unknown attacks.

Resistant Against Evasions

FoEvasion techniques attempt to fool the protocol decoders in IPS products by crafting exotic network streams that would not be handled or reconstructed by the decoders, yet still be valid enough for the target recipient to process. The robust IPS engine is capable of handling both common evasions and sophisticated AETs (Advanced Evasion Techniques) deployed by hackers such as IP Packet Fragmentation, TCP Stream Segmentation, RPC Fragmentation, URL & HTML Obfuscation, and other protocol-specific evasion techniques.

Offline Detection

In out-of-band sniffer mode (or one-arm IPS mode), IPS operates as an Intrusion Detection System (IDS), detecting attacks and reporting them but not taking any action against them. In sniffer mode, the FortiGate unit does

---

FortiGate® - High performance Network Security Platform

- **ASIC-Powered Performance**
  FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.

- **High speed and Flexible Connectivity**
  The FortiGate product family offer a variety of interfaces for today's network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.

- **Broad Product Offerings**
  The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises to high-end platforms for service providers and data centers

not process network traffic and instead is connected to a spanning or mirrored switch port, or a network tap. If an attack is detected, log messages can be recorded and alerts sent to system administrators.

Traffic Bypass

Since most IPS deployments are in transparent inline mode, active traffic bypass is often desired until normal operation of the device resumes. Some FortiGates offer inbuilt active bypass interfaces while others may use external bypass switches.

Monitoring, Logging, and Reporting

FortiOS empowers organizations to implement security best practices that require continuous examination of their threat status and adaptation to new requirements. The FortiView query widgets provide useful analysis data with detailed and contextual session information, which can be filtered, ranked, and further inspected. System events can also be archived via logs, which in turn can generate useful trending and overview reports.

ADDITIONAL REFERENCES

Resource	URL
The FortiOS Handbook - The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/
Product Datasheets & Matrix	http://www.fortinet.com/resource_center/datasheets.html
Fortinet Solution Page	http://www.fortinet.com/solutions

GLOBAL HEADQUARTERS

Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE

120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE

300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE

Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480