DATA CENTER INTRUSION PREVENTION SYSTEM (DCIPS)

Intrusion Prevention System (IPS) technology protects your network from cyber criminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices such as key servers in the data center. 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.

Fortinet FortiOS's IPS functionality is an industry-proven network security solution that scales to 120 Gbps and beyond of in-line protection. Powered by purpose-built hardware and Fortinet Security Processing Unit (SPU), FortiOS is able to achieve attractive total cost of ownership (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.

DCIPS is designed to be highly tunable to ensure high security, performance, and availability are achieved, especially to protect the key servers in the data center. DCIPS failure can severely impact the performance and security of a data center. The following capabilities are considered essential for DCIPS products:

- Intrusion prevention
- Resistant to known evasion techniques
- Reputation awareness
- Highly resilient and stable
- Operation at Layer 2 (network transparency)

Fortinet's FortiGate products meet all these requirements by combining a high-speed, highly effective IPS engine with evasion techniques, reputation awareness, extensive application control capabilities, user and device identification, and a performance-optimized platform to set a higher standard for security, control, and performance.

NSS LABS 2016 DCIPS SVM

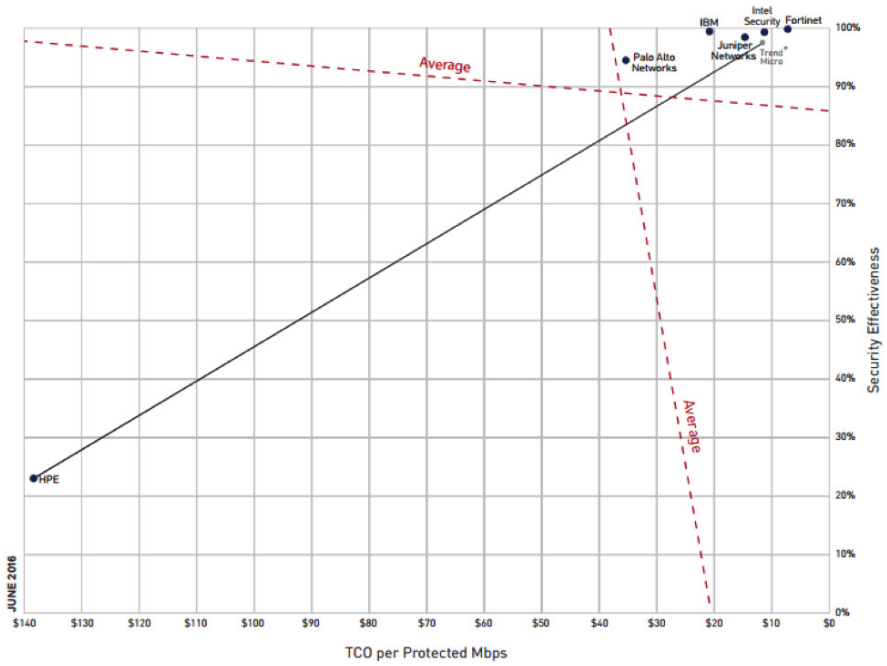
NSS Labs' Data Center Intrusion Prevention System (DCIPS) report is the industry's most comprehensive test to date with their Security Value Map revealing that Fortinet's FortiGate 3000D earned the highest ratings for Security Effectiveness, blocking 99.9 percent of exploits, and TCO per protected Mbps (Megabit per second).

- NSS Labs DCIPS Test Report FortiGate 3000D
  https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/NSS-Labs-DCIPS-Test-Report-FortiGate-3000D.pdf
- NSS Labs 2016 DCIPS Security Value Map
  https://www.fortinet.com/content/dam/fortinet/assets/certifications/NSS-Labs-2016-DCIPS-Security-Value-Map.pdf

FORTINET DCIPS HIGHLIGHTS

- Recommended by NSS Labs for security effectiveness and performance value
- Industry's fastest zero-day protection provided by FortiGuard Labs
- Optional advanced techniques, such as sandboxing, broaden detection and expose evasive threats
- High level of precision and accuracy provided by IPS filters
- Highly flexible deployment options using IPS sensors
- Lower TCO and high-performance IPS achieved by purpose-built SPU
- Single-pane-of-glass management for unmatched visibility and control

DATA CENTER INTRUSION PREVENTION SYSTEM (DCIPS)
SECURITY VALUE MAP™



FORTINET'S FORTIGATE PRODUCTS FOR DCIPS

FORTIGATE 3000 SERIES

The FortiGate 3000 Series gives you the highest performance on the market in a compact appliance form factor, now with up to 1 Tbps throughput and ultralow latency. FortiGate 3000 models are the only non-chassis security appliances on the market to support 40 GE and 100 GE connectivity—providing maximum scalability. The FortiGate 3000 Series can scale 20+ Gbps of in-line IPS throughput.

FORTIGATE 7000 SERIES

The FortiGate 7000E Series appliances are Fortinet's high-end enterprise class chassis firewalls. Available in several different configurations to meet customer needs, the 7000E Series includes the latest 7030E, 7040E, and 7060E and offers simplicity and flexibility of deployment, with ultrahigh NGFW and threat protection performance, capacity, and effortless scale to secure vast amounts of mobile and cloud traffic. The FortiGate 7000 Series can scale 60 Gbps to 120 Gbps of in-line IPS throughput.

THE FORTINET SECURITY FABRIC

The Fortinet Security Fabric is an intelligent framework connecting your security devices together for effective, efficient, and comprehensive security. Our DCIPS solution collaborates with other key solutions in the Fortinet portfolio, while allowing for open integrations (via industry-standard APIs). Fortinet is the only company with security solutions for network, endpoint, application, data center, cloud, and access designed to work together as an integrated security fabric to provide true end-to-end protection.

KEY FEATURES HIGHLIGHTS

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. 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 SPU 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 noncompliant 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.

PATTERN AND 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 signatures has a direct link to its detailed entry on the threat encyclopedia and CVE-ID references. 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 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 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 that allow organizations to proactively prevent further attacks from known attackers over a predefined duration. Quarantining by duration can be used to protect potentially vulnerable servers.

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. Organizations may use FortiConverter to easily convert Snort signatures for FortiOS use.

RESISTANT AGAINST EVASIONS

Evasion 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 advanced evasion techniques deployed by hackers, such as IP packet fragmentation, TCP stream segmentation, RPC fragmentation, URL and HTML obfuscation, and other protocol-specific evasion techniques.

INTRUSION DETECTION MODE

In out-of-band sniffer mode (or one-arm IPS mode), IPS operates as an intrusion detection system, detecting attacks and reporting them but not taking any action against them. In sniffer mode, the FortiGate unit does not process network traffic but 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 in-line mode, active traffic bypass is often desired until normal operation of the device resumes. Fortinet's FortiGate products support external bypass devices using FortiBridge. Administrators are also offered with a software fail-open option to tackle instances where the IPS engine fails. Fortinet's FortiBridge family ensures uptime and availability in case of device failure. It is very easy to add bypass functionality to FortiGates. It supports remote configuration and monitoring and a large range of network configurations including 1 GE, 10 GE, or 40 GE speeds.

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

For more information on Fortinet's Data Center IPS, please go to the following websites:

Data Center IPS:

https://www.fortinet.com/solutions/enterprise-midsize-business/data-center-security-sdn/dcips.html

FortiGate 7000 and 3000 Series Products:

https://www.fortinet.com/products/next-generation-firewall/high-end.html

FortiBridge Products:

https://www.fortinet.com/products/network-visibility/fortibridge.html

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

92950-0-0-EN June 28, 2017 11:13 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:SB-DCIPS:sb-dcips