FAQ

Network Intrusion Prevention Systems (IPS)

Frequently Asked Questions

Introduction

Deploying updates and patches to devices and servers in large enterprise and service provider networks can be a complex and time-consuming process. Following a patch release, it might often take weeks or even months for a large organization to deploy the fix to all affected systems. This opens a window of opportunity for external threats or even malicious insiders to penetrate unpatched systems, steal valuable information, and sabotage networks. Intrusion Detection Systems can detect attacks, but cannot act in real time to block them. Only a network Intrusion Prevention System (IPS) can detect and block attacks *before* damage has been done. Most network security vendors now offer an IPS, however many of these solutions fall short because they force customers to choose between acceptable network security and business continuity. This document provides answers to questions that are often asked about Intrusion Prevention Systems, and also details important security features that you should consider when choosing the best network security solution for your organization.

What is a network IPS and how is it different from an Intrusion Detection System?

Network IPS performs in-line inspection of network traffic in a near-real-time manner. The inspection identifies attacks using known vulnerabilities of commonly used software products and protocols, as well as known attack patterns with unusual activity based on connection sequences or traffic volume[1].

Intrusion Prevention Systems are considered extensions of Intrusion Detection Systems because both systems monitor network traffic and/or system activity for threats. The primary difference between the two systems is that Intrusion Prevention Systems are placed in-line and are therefore able to actively prevent/block intrusions that are detected. More specifically, an IPS can take such actions as sending an alarm, dropping malicious packets, resetting the connection and/or blocking traffic from an offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, defragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options[2].

Why does my organization need a network IPS?

Many enterprise network systems and end user devices remain susceptible to a myriad of known attacks due to a simple failure to patch known vulnerabilities, outdated equipment and malware signatures, or failure to properly setup and deploy security devices. Since known vulnerabilities are typically well documented, anyone can download ready-made tools to attack unpatched systems[3]. When developing a security strategy, organizations must plan to protect against not just current threats, but all threats, known and unknown.

Newer blended threats and Advanced Persistent Threats, or APTs, use multiple old and new attack methods simultaneously, targeting specific data and even individuals within organizations. Therefore, both traditional and advanced security measures working together are especially important when defending networks against these new types of multi-faceted and persistent attacks. Surveys verify the effectiveness of these new attacks, showing that in 2010, the average cost of a data breach reached $214 per compromised record, and averaged $7.2 million per data breach event, an increase of 6% over 2009[4].

---

1 Gartner Magic Quadrant for Network Intrusion Prevention Systems, December 2010

2 Computer Security: Protecting Digital Resources, Robert C. Newman, February 2009; Principles of Information Security, Michael E. Whitman, Herbert J. Mattord, 2009

3 LulzSec Disbands: The Attacks Live On, Infosec Island, June 2011

4 2010 Annual Study: Global Cost of a Data Breach, Ponemon Institute, LLC

I just installed a new IPS. Why are my users still complaining about slow connections?

According to analysts, IPS has two primary performance drivers; the handling of network traffic at near wire speeds, and the deep inspection of traffic based on signatures, rules and policy. The load on both aspects is increasing radically. Enterprise network traffic is growing in bandwidth, complexity of connections and protocols, and connections per second. Inspection load is increasing as new signatures are introduced and old ones do not go away[1].

Some network security vendors have added new inspection capabilities and features onto their IPS platforms without sufficiently upgrading the ability of their hardware to handle the added tasks and network traffic. Purpose-built hardware is now a necessity when attempting to do deep packet inspection at wire speeds in today's high speed next-generation networks. Vendors who skimp on the hardware side and try to use commodity, industry-standard servers may not have the horsepower necessary to effectively process packets in near real time[5].

What makes Fortinet® IPS better than competing solutions?

Fortinet IPS

In order to defend your network and critical data against the latest attacks, your intrusion prevention system (IPS) must be robust enough to detect and block both known and unknown threats. Fortinet IPS protects networks from both known and zero-day vulnerabilities, blocking attacks that take advantage of unpatched systems. Fortinet IPS uses a layered combination of pre-defined signatures to inspect traffic for known threats, followed by heuristic techniques and deep packet scanning with protocol decoders to expose and remove unknown zero-day and hidden attacks. This approach delivers a one-two protective punch:

1. Signature-based detection: leverages a database of over 6,500 signatures to protect networks and devices against known threats and vulnerabilities.
2. Behavior-based detection: compares any traffic anomalies against baseline conditions to detect malicious behavior and block zero-day threats.

In addition, purpose-built FortiASIC™ Security Processors, built into certain FortiGate® appliances and modules, accelerate IPS functions by offloading resource intensive tasks such as IPS signature scanning. Designed with performance in mind, FortiASIC Network Processors and Content Processors help Fortinet consolidated security appliances deliver wire-speed firewall throughput and accelerated content inspection. Available with all FortiGate and FortiWiFi™ platforms, Fortinet IPS offers a wide range of features that can be used to monitor and block malicious activity such as:

IPS sensors

IPS sensors may be configured to apply specific inspection signatures to selected traffic. Actions can be assigned to block, pass, or reset any suspicious traffic. IPS sensors may also be used to enable packet logging for each signature, or to pass traffic from certain IP addresses without further inspection. On the flip side, IPS sensors can prevent attacks from spreading by quarantining all traffic originating from an attack source, sent to an attack destination, or received by the FortiGate device.

IPS sensors are populated with filters and custom signature entries. Attributes can be set to classify traffic by severity, target (client/server), OS, protocol, application, and tags. Specifying more or fewer attributes widens or narrows the focus of the sensor. Custom signature entries can be created to include or exclude signatures on an individual basis. Custom signatures can also specify actions such as logging, packet logging and filtering, attacker quarantine, and exempt IP address settings. Fortinet IPS sensors can be accessed through the FortiGate management interface as shown below in Fig. 1.

---

[5] Market Overview: Intrusion Prevention Systems, Forrester, Q2 2011

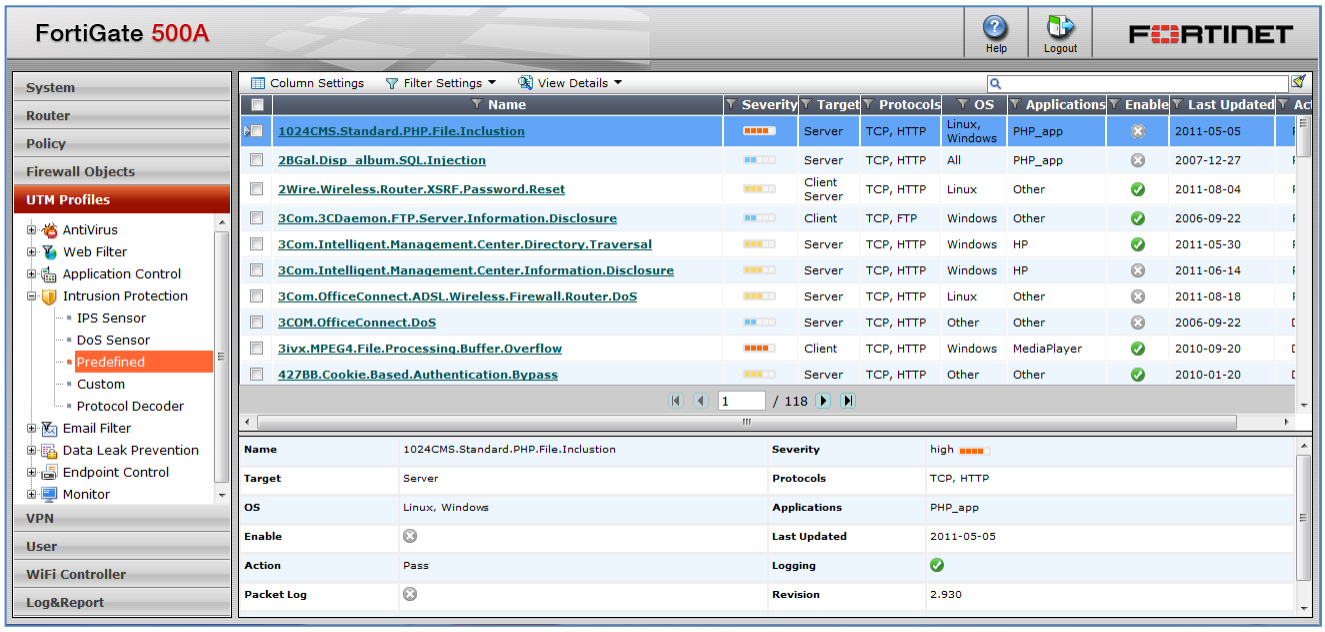

Figure 1: FortGate IPS Sensor Configuration

Predefined IPS signatures

Provided through the global FortiGuard Distribution Network, predefined IPS signatures are used by FortiGate systems to detect more than 6,500 different attack signatures – from attacks against unpatched operating system vulnerabilities to invalid checksums contained in UDP packets.

Custom IPS signatures

Organizations can also create custom IPS signatures to extend protection beyond predefined signatures. For example, custom IPS signatures can be used to protect unusual or specialized applications, or even custom platforms from known and unknown attacks. In addition, custom IPS signatures can be used for specialized network traffic analysis and pattern matching. For example, if a network is experiencing unusual or unwanted traffic, a system administrator can create a custom IPS signature to monitor and understand traffic patterns.

Protocol decoders

Protocol decoders identify abnormal traffic patterns, such as those that do not meet established protocol requirements and standards. For example, the HTTP decoder monitors network traffic to identify any HTTP packets that do not meet the HTTP protocol standard. Many Fortinet protocol decoders are able to recognize traffic by type, rather than port, eliminating the need to specify individual ports.

Packet logging and attacker quarantine

IPS packet logging can be enabled to save packets matched by one or more IPS signatures. The packets are saved as log messages and the packet contents can be viewed and analyzed using log message analysis tools. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.

IPS also provides a way to quarantine attackers and display them on a 'banned user list'. Attackers can be quarantined according to their IP address, their IP address plus the victim's IP address, or by incoming interface used. Attackers can be banned from accessing the network for hours, days, or forever.

IPS out-of-band mode

Fortinet IPS can also be deployed in 'out-of-band', or sniffer mode. This mode allows Fortinet IPS to operate as an Intrusion Detection System, detecting and reporting attacks, but not taking any action. Out-of-band mode can be useful for network diagnostics.

FortiGuard® Services

Backed by automatic, real-time updates delivered by FortiGuard Services, FortiGate IPS technology leverages a database of thousands of unique attack signatures to stop attacks that might evade conventional firewall defenses, plus anomaly-based detection that enables the system to recognize threats for which no signature has yet been developed. The combination of known and unknown threat prevention, plus tight integration with other Fortinet security technologies, enables FortiGate systems to stop attacks regardless of whether your network is wired or wireless, a partner extranet, or connected to a branch office.

Where should I deploy Fortinet IPS?

IPS systems are usually deployed at the network edge, with secondary placements in branch offices, the data center, and the internal network. Integrated with all FortiGate and FortiWiFi platforms, you can deploy Fortinet IPS at the edge of your network to block attacks, or within your network core to protect critical business applications. Following are some typical use cases showing how Fortinet IPS could be deployed to effectively block attacks:

- An administrator wants to protect their Microsoft® Exchange Server from attacks. Using Fortinet IPS sensors, the administrator selects the correct criteria and application, and Fortinet IPS automatically selects all IPS signatures associated with Exchange Server attacks.
- A new worm is released that affects a large number of hosts and a network is hit with continued attempts to infect servers and devices. Using the quarantine option, an administrator configures their FortiGate appliance to temporarily block any IP addresses that might try to infect a host on their network.
- Like all other Fortinet security features, IPS can be combined with other functions on a FortiGate appliance. If an administrator decides to create a rule allowing inbound access to a web server, IPS and antivirus could be applied on top of that rule to prevent any exploits from being run on their web server or viruses from infecting it.

Does Fortinet IPS integrate with other security technologies to detect and block attacks?

An essential component of the Fortinet next-generation security platform, Fortinet IPS works in concert with Fortinet application control and user identification technologies to ensure that only approved traffic, applications and users are given access to your network. Following are just a few of the important security features that are integral to Fortinet products, and work collaboratively with Fortinet IPS to provide complete security for your network:

Application Control

A primary requirement and driver for adoption of next-generation firewalls is application control. In order to prevent data loss and mitigate new threats, organizations must be able to effectively control legacy applications as well as the new breed of Internet-based applications. Next-generation application control must be able to detect, monitor, and control the usage of applications and any associated traffic flows at gateways and at endpoints, regardless of ports and protocols used. In addition, an association must be made between the application and the end user before the proper access rights and security policy can be assigned.

Using the Application Control feature included in FortiGate® platforms, businesses and agencies can detect and restrict the use of applications on their networks and endpoints based on application classification, behavioral analysis, and end user association. Network administrators can define and enforce policies for thousands of applications running on next-generation networks and endpoints. They can detect and control individual features of Web 2.0 applications such as Facebook, Skype, Twitter and Salesforce.com such as allowing chat but disabling the ability to download videos or following links.

Data Loss Prevention (DLP)

Trusted employees can send sensitive data into untrusted zones, either intentionally or by accident. Fortinet DLP uses sophisticated pattern matching techniques and user identity to detect and prevent unauthorized communication of sensitive information and files through the network perimeter. DLP features include fingerprinting of document files and document file sources, multiple inspection modes

(proxy and flow-based), enhanced pattern matching, and data archiving.

Numerous communication protocols - including HTTP, HTTPS, FTP, FTPS, email (POP3, POP3S, IMAP, IMAPS, SMTP, and SMTPS), NNTP and instant messaging (AIM, ICQ, MSN, and Yahoo!) – can be monitored for sensitive data. Fortinet DLP can search content based on text strings as well as enhanced pattern matching that includes wild cards and Perl regular expressions. For example, pattern matching can be used to scan network traffic for sensitive personal information such as social security and credit cards numbers.

When a match is found, sensitive content can be blocked, passed or archived, with potential leak notifications generated. DLP can be used to block sensitive information coming into the network or going out. For example, by blocking content often found in spam email messages, DLP can enhance incoming data protection measures.

Web Content Filtering

The Fortinet web content filtering solution begins with traditional URL blocking lists, but goes further by expanding these methods and allowing their use in combination with other Fortinet security functions resident on all FortiGate consolidated security appliances. Fortinet's web content filtering technology enables a wide variety of actions to inspect, rate, and control perimeter web traffic at a granular level. Using Fortinet web content filtering technology, FortiGate appliances can classify and filter web traffic using multiple pre-defined and custom categories.

To accelerate web traffic and content inspection, all FortiGate devices support web cache communication protocol (WCCP) which allows the FortiGate to operate as a router or cache engine. Acting as a router, the FortiGate intercepts web browsing requests from client web browsers and forwards them to the cache engine. The cache engine then returns web content to the client as required. When operating as a WCCP cache server, the FortiGate can communicate with other WCCP routers to cache web content, returning requested content to client web browsers as needed. Fortinet web content filtering is easily accessible through the FortiGate management interface.

Integrated Secure Wireless Controller

All FortiGate appliances include an integrated wireless controller, consolidating security policies and management of all wired and wireless network traffic into a single pane of glass. The integrated wireless controller provides unmatched visibility and control of both thick FortiWiFi and thin FortiAP™ wireless access points. The same comprehensive threat protection provided for wired networks, including firewall, VPN, intrusion prevention, application control, web filtering, traffic shaping and many other security capabilities, are extended to wireless networks.

Dual-stack IPv4 and IPv6 Support

With the recent exhaustion of the IPv4 address space, many organizations are migrating towards IPv6, the next generation Internet communication protocol. As more content and service providers begin to transition to IPv6, it's essential that organizations deploy network security devices that can deliver the same level of protection for IPv6 content as IPv4. There are mechanisms in place to enable communication between IPv6-only devices and networks with IPv4-only devices and networks.

The two most common are dual-stack and tunnelling:

- Dual-stack is preferable because it allows the security device to process each packet in either IPv4 or IPv6.
- Tunnelling, on the other hand, wraps an IPv6 packet in an IPv4 header, allowing a device to forward a packet but not inspect it. This limited IPv6 support means that it will not be able to inspect the contents for malicious code or unwanted content, allowing unwanted traffic to traverse the network.

FortiGate consolidated security appliances support a dual stack architecture that recognizes and separately routes both IPv4 and IPv6 traffic, providing the same core network security technologies simultaneously for both Internet protocols. Vital network and content protection security features, including routing, are fully supported. Fortinet adopted early support of IPv6, receiving IPv6-Ready and JITC certifications in 2008, both important to global telecommunications carriers. Fortinet also earned the USGv6 certification in 2011, important to the US government and the businesses serving them.

Centralized Management and Analysis

For large installations, FortiManager™ appliances provide centralized policy-based provisioning, configuration, and update management for FortiGate, FortiWiFi, and FortiMail™ appliances as well as FortiClient™ endpoint security agents. By locally hosting security content updates for managed devices and agents, FortiManager appliances minimize web filtering rating request response times and maximize network protection. FortiManager provides a single pane of glass interface to manage and configure all Fortinet appliances.

For additional analysis and reporting capabilities, FortiAnalyzer™ appliances securely aggregate log data from both Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of easily-customizable reports, users can filter and review log records for traffic, event, virus, attack, web content and email data. Information can be mined to determine a user's security stance and assure regulatory compliance. FortiAnalyzer also provides advanced security management functions such as quarantined file archiving, event correlation, vulnerability assessments, traffic analysis, and archiving of email, web access, instant messaging and file transfer content.

Conclusion

FortiGate consolidated security physical and virtual appliances from Fortinet are field-proven, purpose-built security platforms that include rock-solid traditional security technologies, as well as protection against next-generation threats such as Advanced Persistent Threats, or APTs, and threats targeting mobile devices. Because Fortinet develops all security technologies in-house (instead of licensing crucial security features from third parties), all FortiGate platforms include finely tuned, hardware-accelerated protective technologies that can integrate new security technologies and scale effortlessly with any size of fast-growing business and any network environment. Fortinet also provides in-depth monitoring and reporting capabilities to alert administrators and users to threats, and to allow further analysis for fine tuning. When combined with FortiGuard Services, FortiGate consolidated security appliances protect your next-generation network and your business against threats now and into the future.

About Fortinet

Fortinet delivers unified threat management and specialized security solutions that block today's sophisticated threats. Our consolidated architecture enables our customers to deploy fully integrated security technologies in a single device, delivering increased performance, improved protection, and reduced costs. Purpose-built hardware and software provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. Our customers rely on Fortinet to protect their constantly evolving networks in every industry and region in the world. They deploy a robust defense-in-depth strategy that improves their security posture, simplifies their security infrastructure, and reduces their overall cost of ownership.

About FortiOS

FortiOS™ is a security-hardened, purpose-built operating system that is the software foundation of FortiGate consolidated security platforms. FortiOS software enables high performance multi-threat security by leveraging the hardware acceleration provided by FortiASIC™ content and network processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS helps you stop the latest, most sophisticated, and dynamic threats facing your network today with expert threat intelligence delivered via FortiGuard Security Subscription Services.

FortiOS 4.0 software redefines network security by extending the scope of integrated security and networking capabilities within the FortiGate consolidated security platform. Regardless of the size of your organization, you can benefit from the most comprehensive suite of security and networking services within a single device on the market today.

FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability management, application control, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with return and replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 90-day limited software warranty.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015