NGIPS SOLUTION

Fortinet's NSS Labs recommended NGIPS solution integrates IPS with application control and leverages the power of FortiGuard Labs to deliver better security, more control and faster performance.

Fortinet's Next Generation IPS Solution

Better Security, More Control and Faster Performance

Introduction

Organizations are under continuous attack. Cybercriminals, motivated by previously successful high profile hacks and the highly profitable black market for stolen data, continue to increase both the volume and sophistication of their attacks on organizations. Traditional Intrusion Prevention Systems (IPS) no longer provides a wide enough range of protection. Today's threat landscape requires Next Generation IPS (NGIPS) to block a wider range of threats while minimizing false positives.

This guide discusses the need for NGIPS and demonstrates how Fortinet's NGIPS solution can help you solve this multi-faceted problem by integrating highly effective IPS with granular application control capabilities on a platform that delivers faster performance.

New Trends Challenge Traditional IPS Security

- **More Attacks against Client and Cloud Applications –** Traditionally IPS systems are used to detect attacks against servers and server based applications using signatures. Today we see many sophisticated attacks against client based applications.
- **Porous Edge Due to BYOD and Remote Workers –** Many organizations encourage BYOD and flexible working environments which has led to the explosion of anytime, anywhere data consumption. This increases the risk that sensitive data can be exposed to unauthorized access outside of corporate boundaries.

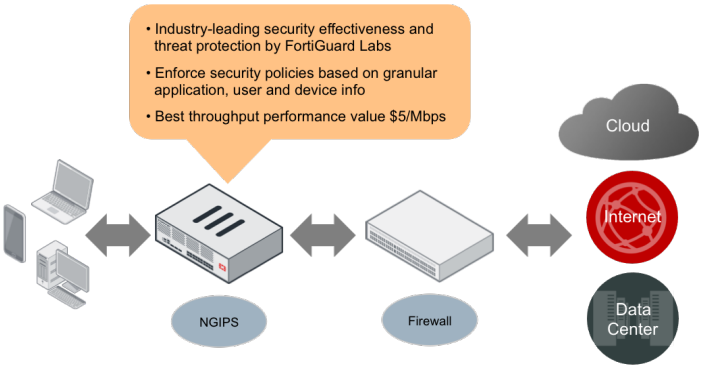
- Recommended by NSS Labs for security effectiveness and performance value
- Industry's fastest Zero-day protection provided by FortiGuard Labs
- Greater visibility and control over more types of applications, users and devices
- High level of precision and accuracy provided by IPS Filters
- Highly flexible deployment options using IPS Sensors
- Lower TCO and High Performance NGIPS achieved by purpose-built FortiASIC
- Single pane of glass management for unmatched visibility and control

What this Means for NGIPS Requirements

- **Application Visibility –** Protect against application specific attacks using IPS integrated with application control to identify, inspect and monitor thousands of applications.
- **Context Awareness –** Detect security attacks based on user identity, type of device and network behavior.
- **Performance and Reliability –** Security must be effective and it must keep up with the speed of your business. Combine deep inspection and accurate IPS filters with a high performance NGIPS platform.

Fortinet's NGIPS Solution

Fortinet's Next Generation IPS (NGIPS) meets these new requirements by combining a high-speed, highly effective IPS engine with extensive application control capabilities, user and device identification, and a performance optimized platform to set a higher standard for security, control and performance.

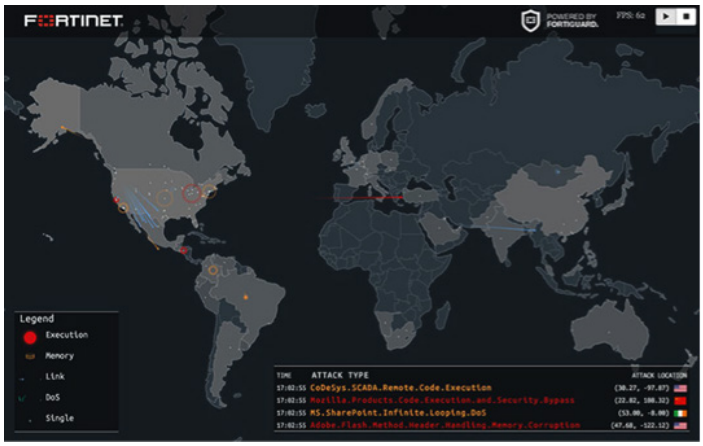


According to some leading analysts, the high end of the security market will tend to continue to use separate firewalls and IPSs driven by compliance requirements, complexity and network operational considerations. The FortiGate-based solution from Fortinet is easily deployed behind existing firewalls to deliver the full range of NGIPS capabilities including the ability to identify more applications users, and devices than other NGIPS options. This section will discuss each of the NGIPS components in more detail.

Better Security

Fortinet's NGIPS solution is Recommended by NSS Labs for top-ranked security effectiveness and the best performance value in the industry.

Fortinet's robust IPS Engine is design from the ground up to provide protection against the latest attacks by detecting and blocking threats before they reach your potentially vulnerable network devices. The combination of our IPS Engine capabilities and the real-time/zero-day threat intelligence updates provided by FortiGuard Labs, delivers the industry's best IPS protection to block more threats and better protect your organization.



Click to see attacks happening now around the world on the FortiGuard Labs live threat map

For more than 15 years FortiGuard Labs, Fortinet's industry-leading security research team, has protected organizations against attacks using:

- Real-time intelligence on the threat landscape to deliver comprehensive security updates to the entire Fortinet solution ecosystem
- 24x7x365 security updates from a Global Operations team for the latest security intelligence in real-time to deliver protection as soon as a new threat emerges.
- Industry-leading vulnerability research capabilities. FortiGuard Labs has discovered over 170 unique zero-day vulnerabilities to date and delivers millions of signature updates every month.

More Control

Fortinet's NGIPS combines IPS with Application control and more to detect threats and take action against network traffic based on contextual information derived from applications, users and devices.

- Application Control identifies more than 3500 discrete applications to enforce policies. It can inspect today's encrypted and evasive traffic as well as traffic running on new technologies such as the SPDY protocol.
- Extensive User Identity capabilities allow organizations to set granular policies for more types of users on the network with extensive directory and RADIUS integration options to deliver additional contextual controls.
- Fortinet offers deep inspection of cloud applications to give organizations more insight into who is using cloud services and how they are being used, such as what files are being

transferred or what videos are being watched. This unique granular level of information combined with integrated IPS becomes a key advantage for detecting sophisticated cybercriminal attacks.

- Organizations get greater deployment flexibility using IPS and Application control sensors to apply separate policies to different group of users and applications.
- Fortinet is the only NGIPS able to identify the type of networked device being used so you can set stronger security controls for riskier devices.

Platforms with Uncompromised Performance

Fortinet's NGIPS solution is delivered by industry-proven FortiGate appliances.

Purpose built FortiASIC processors are at the heart of the FortiGate NGIPS platform to deliver industry-leading, high performance processing. This level of performance is required for the deeper level of next generation inspection as well as the consolidation of multiple NGIPS functions onto a single appliance.

Traditional security appliances that solely use a multi-purpose CPU-based architecture become an infrastructure bottleneck. Even with multiple-core general purpose processors, network security devices cannot deliver the high performance and low latency needed for today's networks. The only way for a network security platform to deliver high-speed performance is via purpose-built ASICs to accelerate specific packet processing and content scanning functions. FortiGate technology utilizes Optimum Path Processing (OPP) to optimize the different resources available in packet flow for maximum performance.

As a result, FortiGate's integrated architecture provides extremely high throughput and exceptionally low latency, while still delivering industry-leading security effectiveness and consolidating functions.

Single Pane of Glass Management

Given the widely distributed nature of many enterprise environments, the ability to quickly provision, control and scale your security management is critical.

FortiManager allows you to control device configurations, security policies, firmware installations and content security updates from one centralized management platform.

For large distributed and campus environments with compliance requirements, FortiAnalyzer facilitates logging, reporting, in-depth visibility and event management to keep you constantly aware of your security posture. Together, FortiManager and FortiAnalyzer provide a unified administrative console to oversee your distributed security architecture.

Summary

Organizations need better security solutions to protect against today's increasingly sophisticated threats. With trends like BYOD, remote workers and the explosion of cloud applications, cybercriminals are using more advanced techniques to attack and traditional IPS alone no longer offers enough protection.

Fortinet's NGIPS significantly extends the capabilities of IPS and detects multi-vector threats based on integration with application, user, and device control based on industry-leading threat intelligence from FortiGuard Labs.

IPS Capability	Traditional IPS	Fortinet NGIPS
Inline IPS and IDS	✓	✓
Policy Management	✓	✓
Reports and Alerts	✓	✓
IPS Sensors		✓
Zero-Day Protection		✓
Custom Signatures		✓
User and Device Identity		✓
Application Control		✓

Fortinet's FortiGate line of NGIPS delivers better security, more control and faster performance than any other solution in the industry.

For more information on Fortinet's Next-Generation IPS solution, please go to : www.fortinet.com/solutions/next-gen-ips.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
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428