SOLUTION BRIEF

Proactive Threat Protection with FortiGate IPS

Executive Summary

The threat landscape continues to evolve, and the attack surface for all organizations is expanding, Because the root causes of most breaches involve the exploitation of known vulnerabilities, many organizations have turned to intrusion prevention systems (IPS) to keep pace. The right IPS offers the most effective way to block threats that use known vulnerabilities.

The Fortinet FortiGate delivers best-of-breed IPS capabilities for security-driven networking infrastructure—striking a delicate balance by delivering high security efficacy without disrupting business processes. FortiGate IPS is built on a unique architecture of specialized security and network processors, which enable it to deliver unparalleled performance when paired with FortiGuard Labs, the industry's leading threat-intelligence research team.

FortiGate IPS Key Features:

- Virtual patching
- Custom-built security processors
- Industry's leading threat intelligence
- Centralized management
- Third-party connectors
- Security fabric
- Custom IPS signatures

FortiGate IPS Key Benefits:

- High security efficacy
- Breadth and depth of security coverage
- High performance and low latency
- Simplified management
- Third-party integration

Moving Beyond Standalone IPS

The expanding attack surface combined with the evolving threat landscape has resulted in enterprises deploying every security tool available to protect against the latest threats. This point product implementation approach has resulted in an explosion of security tools and vendors deployed within an organization. On average, a typical security team from a large enterprise uses over 50 different security tools from multiple vendors.[1] But that approach drives huge added cost of complexity and causes myriad issues, from a lack of automation and integration to blind spots in overall IT visibility.

Traditionally enterprises deployed standalone IPS to augment their security posture by inspecting traffic against threats. The main reason for the adoption of the standalone IPS was the inability of traditional enterprise firewalls to deliver high security effectiveness against threats under high performance without impacting network latency. Another major reason was the lack of flexibility and customization in threat coverage, which was a frequent drawback of second-generation firewalls.

Thus, many organizations struggling with the shortage of skilled staff on their security teams are in the midst of security initiatives seeking to replace their outdated IPS to stay ahead of the evolving threat and network landscape. They need a security solution that offers significant improvements in terms of simplifying security operations and management tasks, higher security effectiveness, and better visibility and control of their network. Integrating IPS within next-generation firewall (NGFW) technology effectively solves the aforementioned problems, allowing organizations to move beyond the traditional IPS and drive an integrated, much more efficient approach to network security.

Unparalleled IPS Performance

Intrusion prevention not only involves deep packet inspection, which looks into what is inside the traffic, but also provides other aspects like pattern matching, anomaly detection, and other needs that have to be done at wire speeds, with decisions made in microseconds to block or allow the traffic. A high-performing IPS solution, therefore, has to deliver a high degree of performance without adding any latency or delay to the traffic.

FortiGate NGFWs leverage purpose-built custom security processors called "content processors," which enable FortiGates to offload resource-intensive tasks like IPS to dedicated processors, which results in minimal to no impact on the performance. FortiGates, when deployed as an NGFW with the integrated IPS capability, deliver high throughput with low latency to protect the data center and the enterprise's core network.

High Security Effectiveness with Threat Intelligence

FortiGuard Labs is the global threat-intelligence and research organization at Fortinet. Its mission is to provide customers the industry's best threat intelligence to protect them from malicious cyberattacks. Using millions of global network sensors, FortiGuard Labs monitors the worldwide attack surface and employs artificial intelligence (AI) to mine that data for new threats. The efforts of the large, global team of experienced threat hunters, researchers, analysts, tool developers, and data scientists enable FortiGuard Labs to keep all Fortinet products updated with the best threat identification and protection information available. With over 860 zero-day vulnerabilities discovered to date, FortiGuard Labs creates threat-intelligence updates for Fortinet security products so that they have the latest threat protection possible. This includes threat-intelligence updates for Fortinet next-generation firewalls and IPS, as well as antivirus, antispam, sandbox, endpoint, and email security solutions. Where appropriate, this also includes reputation updates on malicious URLs, IP addresses, and domains.

Centralized Management

When it comes to network security, disparate products typically cannot share threat intelligence or coordinate responses across organizational infrastructure. This critical cybersecurity shortcoming is often compounded by a lack of skilled security personnel to manage a wide assortment of disconnected point products. But even large organizations with dedicated IT security staff still have difficulty monitoring the network to keep track of which devices are connected, who has access to the network, and which resources are needed by which applications and workflows.

A centralized management solution with a single-pane-of-glass view like the Fortinet Fabric Management Center enables streamlined visibility that reduces complexity. It allows security and network operations teams to monitor data movement and identify anomalous activity, simplifies solution optimization, and centralizes the management of security functions like policy and element management for the entire deployment. Security teams can create policy at a single point which then can be distributed across the entire IT infrastructure, whether it is an on-premises data center or both private and public clouds. It also streamlines operations for limited or under-resourced administrators and staff—requiring fewer man-hours while reducing total cost of ownership (TCO).

Summary

When it comes to delivering protection against known and zero-day vulnerabilities, Intrusion prevention systems play a critical role by virtue of their ability to use features like virtual patching to offer faster time to protection. In both standalone IPS and converged NGFW deployments, the innovative FortiGate IPS delivers proven, world-class protection. As part of the Fortinet Security Fabric, FortiGate IPS shares global and local security intelligence with other Fortinet solutions and trusted third-party products, ensuring it is assessing risk with the most up-to-date information, as well as improving overall security posture.

[1] Phil Muncaster, "CISOs Struggling With 50+ Separate Security Tools," Infosecurity Magazine, June 20, 2019.

July 14, 2020 12:27 AM

726512-0-0-EN

D:\Fortinet\Solution Briefs\Red Solution Brief\FortiGate IPS\sb-FA-proactive-threat-protection-with-fortigate-ips-7142020