SOLUTION BRIEF

Powerful Firewalls Need Powerful IPS Security:

FortiGate Next-Generation Firewalls

Executive Summary

Cyber, operational, and reputational risks continue to increase across all industries, impacting profitability, productivity, and brand reputation. One of the key drivers is that increasingly sophisticated and persistent threats are targeting today's expanding attack surface. However, having too many isolated security and management solutions in place (solution sprawl), combined with the ongoing cybersecurity skills gap, can make it difficult for organizations to detect and respond to these threats. Instead, IT teams spend far too much time building and maintaining workarounds to get their disparate solutions to work together, which means most organizations struggle to stay on top of cyber incidents due to the resulting fragmented visibility and control.

Addressing these challenges requires an integrated and adaptive security strategy. And the most effective approach starts with a unified next-generation firewall (NGFW) security platform. The challenge is that most NGFWs operate as isolated solutions. Today's organizations need an NGFW platform that can be deployed anywhere (campus edge, data center, cloud, branch, etc.) in any form factor (physical, virtual, container, or as-a-service) and still work together across different environments as a single, integrated system.

Even the services that run on most NGFWs operate as entirely separate solutions, often with different management tools, complicating the issue of managing siloed solutions even further. Instead, your NGFW solutions and services should all run on the same underlying OS and management console. This allows them to correlate threat intelligence and coordinate responses networkwide as a single system.

One of the most essential additions to any NGFW is a fully integrated intrusion prevention system (IPS) that can analyze all communication traffic via deep packet inspection (DPI). And given that most traffic traversing today's distributed networks is encrypted, this includes the ability to provide deep inspection of encrypted data without impacting firewall performance—including things like streaming content. Unfortunately, most of today's NGFWs cannot provide this essential service.

The average cost of a ransomware attack is now $4.5M.[1]

During the first half of 2022, FortiGuard Labs documented a 2x growth in ransomware variants.[2]

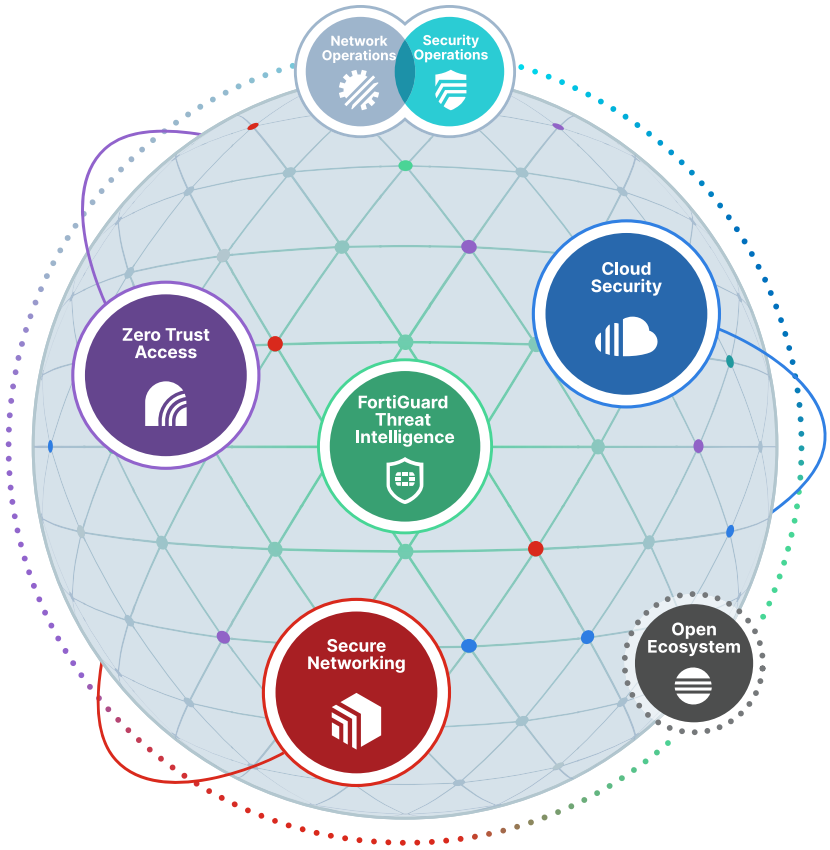
Key FortiGate IPS features and benefits:

- High performance and low latency
- Industry-leading threat intelligence
- Simplified and centralized management
- Virtual patching
- Custom IPS signatures

Additionally, an integrated IPS service must be able to initiate real-time security actions to block detected malicious activities. Given the speed of today's threats, handing off an alert to another system running on a separate OS is not good enough.

FortiGate NGFWs have been purpose-built for today's demanding and distributed networks. Every FortiGate solution runs on the same underlying FortiOS, the world's most widely distributed security operating system. And they each include a proprietary IPS processor and engine to maximize performance. In addition, our FortiGuard Labs team constantly provides near real-time threat signature updates to maximize IPS security actions.

The combination of a FortiGate firewall platform and FortiGuard Labs–powered IPS delivers a powerful and efficient NGFW solution designed for today's organizations. They blend network security and cybersecurity into a single platform that can be combined with dozens of other essential security services to mitigate risk across the Fortinet Security Fabric to better protect the way you need to do business.



FortiGate NGFW with IPS delivers:

- Insight into threats worldwide through our global network of more than 5.6 million sensors
- Deep inspection to discover and thwart advanced threats, botnets, and their command and control (C2) systems, zero-day, and targeted network attacks
- Fast and comprehensive intelligence via automated and advanced analytics (such as ML) that is applied simultaneously across the entire Security Fabric

Industry-Leading NGFW IPS by Design

Our DPI technology—part of the FortiGuard Labs IPS service—not only looks into what's inside your traffic but also provides other critical analysis services, like pattern matching and anomaly detection, in near real time so decisions can be made in microseconds to block or allow communications.

An effective IPS service must deliver high performance without adding any latency or delay to the traffic. However, providing deep inspection for today's network traffic is a challenge for most IPS solutions—and even more so for encrypted or streaming traffic. It's a design challenge that only Fortinet has managed to address.

FortiGate NGFWs leverage purpose-built custom security processors called "content processors." By offloading resource-intensive tasks like IPS to dedicated processors, FortiGate solutions provide the critical inspection services your organization needs with minimal to no impact on network performance or user experience—a process unique in the industry. As a result, FortiGate NGFWs with integrated IPS deliver the industry's highest throughput with the lowest latency to protect and secure your network.

Design and Intelligence: It's Not an Either/Or—It Must be Both

While the physical design of the NGFW is an essential consideration, so is having a robust threat intelligence service (the ability to produce and curate IPS threat signatures) if near-real-time security is a priority. Fortinet NGFWs are powered by FortiGuard Labs, which monitors the worldwide attack surface using proprietary artificial intelligence (AI) and machine learning (ML) technologies to search for new and emerging threats and then create and distribute preemptive threat signatures.

The FortiGuard Labs team includes over 500 threat researchers and analysts deployed worldwide. They leverage over 10 years of threat data, more than 5.6 million sensors (over 1.57 PB of threat samples), the world's largest dedicated security AI system, and over 200 threat intelligence partners to identify, curate, deprecate, and maximize 11,000+ threat detection signatures—all while preserving low latency for customers. This level of commitment and innovation enables FortiGuard Labs to lead the industry with 1,000+ zero-day threat discoveries.

Convergence: IPS Is Central to the Fortinet Security Fabric

The FortiGate NGFW with IPS is one of several integrated Fortinet network security services that can be combined to form the Fortinet Security Fabric. This single cybersecurity mesh architecture can span, grow, and adapt to your distributed network. To assist organizations in their struggle with security vendor and solution sprawl, lack of integrated solutions, and limited resource pool, Fortinet is committed to continuing to converge essential technologies, features, and capabilities.

By integrating products and services to create a unified platform, the Fortinet Security Fabric, you can deploy FortiGate solutions anywhere across your network, add dozens of critical services, and still have them function as a single, expansive solution. Further, FortiGate NGFWs and IPS policies can be managed centrally through a single pane of glass to better correlate threat data and initiate and automate a coordinated response.

FortiGuard Labs ingests and analyzes 100 billion events. This allows them to deliver, on average, over 1 billion daily security updates to protect enterprises against new and unknown threats. These updates are posted simultaneously across all Fortinet Security Fabric deployments—not just for your NGFW and IPS deployments but across the entire portfolio of Fortinet SD-WAN, proxy, zero trust, application controller, mail, network detection and response, cloud, secure access service edge (SASE), and endpoint solutions.

FortiGate NGFW with IPS Is a Vital Component of Your Integrated Security Strategy

Corporate risks associated with cyber events continue to grow. At the same time, companies struggle to achieve efficiency gains—especially in a time of a remote and reduced workforce—partly because it is difficult to apply security inspection and enforcement consistently across a constantly changing and distributed network. And making matters worse, this must be done without impacting productivity or user experience.

An NGFW with IPS plays a critical role in this process by virtue of its ability to detect and block malicious network traffic in real time. Advanced features, like virtual patching, combined with integrated physical, virtual, and as-a-service cloud solutions, offer faster time to protection to every worker and system, regardless of location.

As part of the extended Fortinet Security Fabric, FortiGate NGFWs with IPS can share global and local security intelligence with other Fortinet solutions and trusted third-party products, ensuring that risk assessment is coupled with the most up-to-date information to improve your overall security posture while reducing cyber risk across the network.

[1] IBM, Cost of a Data Breach 2022, accessed December 20, 2022.

[2] Fortinet Global Threat Landscape Report, August 2022.

www.fortinet.com

December 22, 2022 6:53 PM
1871846-0-0-EN