SOLUTION BRIEF

Mitigating Vulnerabilities: A FortiGate IPS Overview

Executive Summary

According to Verizon's *2020 Data Breach Investigations Report,* nearly half (43%) of all successful data breaches can be traced back to an application vulnerability—a share that more than doubled year over year.[1] Vulnerabilities can be exploited through many different forms of attack—such as hacking, social engineering, malware, and bots. An effective intrusion prevention system (IPS) can help protect both known and predisclosed (zero-day) vulnerabilities from exploitation. FortiGate next-generation firewalls (NGFWs) include IPS capabilities and can even be deployed as a dedicated IPS solution. Powered by purpose-built security processors that accelerate performance and industry-leading threat intelligence from FortiGuard Labs, FortiGate IPS provides fast and effective vulnerability protection.

While over 100 billion lines of new software code are written each year, the number of security vulnerabilities has remained the same over the last two decades—an average of 26.7 critical vulnerabilities per application.[3]

Vulnerabilities vs. Exploits

"Vulnerability" has generally come to be associated with unpatched software and misconfigurations.[2] It can refer to a bug or weakness in the code of an application, application programming interface (API), firmware, or operating system which can then be used to gain unauthorized access to the underlying system.

Successful exploitation of a vulnerability enables attackers to run unverified and malicious code on the system and access the system's memory, or to gain system-level administrator access to install malware. Attackers use various different techniques—including injection (e.g., SQL, NoSQL expression language), buffer overflows, cross-site scripting (XSS), Java obfuscation, and other techniques to conceal malicious code.

"Exploit" refers to the tool used to maliciously attack a vulnerability. The exploit itself is typically a piece of software, a chunk of data, or a sequence of commands that takes advantage of an application or system to cause unintended or unanticipated behavior to occur. Exploit kits (or exploit packs) are automated programs used by attackers to exploit known vulnerabilities in systems or applications. They can be used to secretly launch attacks while victims are browsing the web, with the goal being to download and execute some type of malware. Sophisticated exploit kits are capable of attacking an assortment of different vulnerabilities across multiple applications.

A single vulnerability can be exploited in different ways. It can have a one-to-many relationship with exploits—where multiple exploits can target a single vulnerability in different ways. Or it can have a many-to-one relationship—where a single exploit may be capable of leveraging multiple different vulnerabilities simultaneously.

Since vulnerabilities continue to be a leading cause of breaches, most enterprises continuously monitor and patch vulnerabilities to prevent exploitation. When a new vulnerability is discovered, the software developer must quickly develop and release a patch to correct the problem. An organization's IT department must then act quickly to ensure the patch is deployed across all instances of the application throughout the infrastructure. This window can offer malicious actors all the time they need to customize and launch an attack against the disclosed vulnerability.

Even worse, there are also predisclosed (or zero-day) vulnerabilities—undiscovered bugs or flaws where no patch is available. Exploits against a zero-day vulnerability may take days or months before they are discovered—which can give an attacker ample time to do serious damage to an organization.[4] Subsequently, even the most rigorous patch management strategies cannot fully address the risks of either known or zero-day vulnerabilities.

FortiGate IPS Protects Vulnerabilities Against Exploitation

To protect both known and zero-day vulnerabilities from exploitation, organizations need a next-generation **intrusion prevention system (IPS)** that works as an integrated part of their broader security architecture. Fortinet delivers industry-validated IPS capabilities via the FortiGate platform—using an existing FortiGate NGFW with the FortiGate IPS service or by deploying a dedicated FortiGate as a standalone IPS solution.

FortiGate IPS combines the performance of FortiGate security processors with multiple inspection engines, threat-intelligence feeds, and advanced threat capabilities to defend vulnerabilities against attacks. This includes virtual patching, which protects vulnerabilities at the network level using IPS signatures. With over 13,000 IPS signatures (and real-time updates from FortiGuard Labs), FortiGate IPS helps organizations respond to the latest threats faster, while offering complete protection across all types of vulnerabilities.

First and foremost, FortiGate IPS is built for speed. Protection happens at line speed—the same as standalone IPS devices. Fortinet's IPS engine automatically inspects packets and applies filters to content passing through the FortiOS operating system. Once the IPS engine identifies a pattern, it then offloads the full signature-matching process to FortiGate's content processor in order to maintain optimal line-speed protection.

Fast Signature Delivery Powered by FortiGuard Labs

Fast signature delivery is another key advantage that Fortinet offers. FortiGate IPS benefits from the artificial intelligence (AI)-driven threat research done by FortiGuard Labs on both known and new vulnerabilities. Based on the latest telemetry data, FortiGuard Labs creates proactive signatures to detect any exploits of the vulnerability before the vendor has released a patch. This enables FortiGuard Labs to inform FortiGate IPS (and all the other integrated components of the Fortinet Security Fabric) with the latest threat intelligence.

FortiGate IPS signatures are updated on a daily basis, after a rigorous testing and validation process to minimize false positives. In most cases, a signature for any new critical vulnerability is delivered within 48 hours of discovery. For many competing solutions, weekly updates are the norm—which extends the window of potential exploitation.

FortiGate IPS also uses machine learning (ML) to perform automated signature analysis for advanced protection against botnet attacks. With literally millions of botnet signatures coming in, ML offers an intelligent tool for detecting vulnerabilities that may be prone to bot-based attacks.

A Complement to Comprehensive Security

Fortinet earned a third consecutive "Recommended" rating from the most recent NSS Labs Next Generation IPS (NGIPS) Test Report.[5] NSS Labs also noted that FortiGate IPS offered the best total cost of ownership (TCO)—an important consideration when trying to protect an enterprise from the latest threat exposures with limited resources.

As part of the Fortinet Security Fabric, FortiGate IPS helps secure an organization's entire infrastructure from end to end. FortiGate IPS benefits from intelligence sharing with other Fortinet products as well as Fabric-Ready Partner products. For example, FortiGate IPS works with solutions such as FortiClient (endpoint protection) and FortiSandbox (sandboxing) to uncover unknown vulnerabilities in the wild (such as new malware variants) and then convert them into known threats—with the help of the FortiGuard Labs research team. FortiGate IPS also utilizes advanced analytics and policy workflows through FortiAnalyzer.

These key integrations make investigation and incident response more productive, as they can take place in the context of the whole Security Fabric architecture instead of as isolated data from a standalone IPS appliance or firewall sensor. Additionally, FortiGate IPS is a rich source of forensic details that are equally available to other Security Fabric solutions—which in turn helps fortify the organization's overall security posture. In this pursuit, FortiGate IPS gives enterprises the ability to detect, isolate, and remediate critical vulnerabilities wherever they are found.

1 "2020 Data Breach Investigations Report," Verizon, May 2020.

2 Rich Campagna, "The 9 Types of Security Vulnerabilities," Security Boulevard, May 28, 2020.

3 "Malware and ransomware attack volume down due to more targeted attacks," Help Net Security, February 5, 2020.

4 Jack Wallen, "What is a zero-day vulnerability?," TechRepublic, October 18, 2019.

5 Thomas Williams and Matt Wheeler, "Next Generation Intrusion Prevention System (NGIPS) Test Report: Fortinet FortiGate-100F," NSS Labs, October 18, 2019.

FORTINET

www.fortinet.com

July 16, 2020 3:15 PM

729177-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:sb - FortiGate IPS Overview:sb-FortiGate-IPS-Overview-071620-330pm