Fortinet Managed IPS Rules for AWS Network Firewall

Essential Network Security Controls To Protect the Perimeter of Your Amazon VPCs
# Table of Contents

- Executive Overview 3
- Threat Landscape 4
- AWS Shared Responsibility Model 5
- AWS Network Firewall 6
- How AWS Network Firewall Works 7
- Fortinet Managed IPS Rules 8
- Fortinet Rulesets 10
- Getting Started 11
Executive Overview

As innovation continues to accelerate, customers expect more advanced capabilities as well as increased simplicity. This is especially true when it comes to security on the cloud. To simplify the scaling of network security across all cloud resources, Amazon Web Services (AWS) released the AWS Network Firewall. This allows users to implement customized protections to secure their workloads and comply with regulatory requirements.

However, it still requires you to provide the rules. To maintain the simplicity of its fully managed cloud backbone, you need a solution that can run in the background. That is where Fortinet Managed IPS Rules come into play.

This eBook will highlight how security teams can take full advantage of the AWS Network Firewall with Fortinet Managed IPS Rules, powered by industry-leading threat intelligence and research from FortiGuard Labs.
Threat Landscape

Threats are moving fast. You need to be faster.

Security has always been important but never as critical as today. According to a Gartner survey, 69% of corporate directors have accelerated digital transformation initiatives due to the pandemic.¹ For many, the cloud is critical to the delivery of their services. This requires additional emphasis on securing application workloads.

To keep up with the volume and variety of potential vulnerabilities, without being overburdened with managing security controls, it is imperative to establish efficient security processes across your application environments. The first step in doing so is understanding what threats exist in today's landscape.

Average impact of a breach in 2020²

- $3.86M in damages
- 280 days to identify and contain
- 59% of organizations had security automation deployed

Note: Organizations with remote working environments cited costs nearly $137K higher than the average.

Most prominent security vulnerabilities³

- 52% of data breaches are caused by malicious attacks
- 19% of malicious breaches were due to compromised credentials
- 19% of breaches were due to cloud misconfigurations
- 16% of breaches were caused by vulnerabilities in third-party software

Note: Only 59% of organizations have security automation in place, making it more difficult to respond to threats in a timely manner.
AWS Shared Responsibility Model

It is important to discern what you need to be protecting.

Security is a shared responsibility between AWS and you. AWS is responsible for the “security of the cloud,” whereas customers are responsible for “security in the cloud”:

**Security of the cloud**
AWS is responsible for protecting the infrastructure that powers your Amazon Virtual Private Clouds (VPCs). The effectiveness of its security is regularly tested and verified by third-party auditors as part of the AWS compliance programs.

**Security in the cloud**
You are responsible for managing the workloads running within your Amazon VPC, including the appropriate permissions and access levels. You are also responsible for ensuring your organization is meeting all relevant business requirements, laws, and regulations. AWS Partners, like Fortinet, offer solutions to help you enhance your security posture.
**AWS Network Firewall**

Rapidly scale your network security policies with a flexible rules engine.

AWS Network Firewall is a managed service that simplifies the deployment of essential network security controls across your Amazon VPCs.

**Managed infrastructure for high availability**

AWS Network Firewall automatically scales with your network traffic to support hundreds of thousands of connections, while offloading the build and maintenance of network security infrastructure.

**Highly flexible rules engine for broad support**

Supports thousands of custom rules, so you can establish firewall rules that meet your unique network security requirements. Rules can be based on Internet Protocol (IP), port, protocol, domain, and pattern matching—each written using common open-source rule formats.

**Consistent policy management across Amazon VPCs and accounts**

AWS Network Firewall works with AWS Firewall Manager so you can centrally manage security policies across existing accounts and VPCs. This enables you to automatically enforce security policies for newly created accounts and VPCs.
How AWS Network Firewall Works

AWS Network Firewall can be managed with three central components.

**Firewall**
Connects Amazon VPCs to the protection behavior defined in a firewall policy. For each Availability Zone you want to establish protection in, you provide the AWS Network Firewall with a public subnet dedicated to the firewall endpoint. To use the firewall, update the VPC route tables to send incoming and outgoing traffic through the firewall endpoints.

**Firewall policy**
Defines the behavior of the firewall in a collection of stateless and stateful rule groups and other settings. You can associate each firewall with only one firewall policy, but you can use a firewall policy for more than one firewall.

**Rule groups**
A collection of stateless or stateful rules that define how to inspect and handle network traffic. Rules configuration includes 5-tuple and domain name filtering. You can also provide stateful rules using a Suricata open-source rule specification.
Fortinet Managed IPS Rules

Easily filter malicious traffic at the perimeter of your Amazon VPC.

Fortinet Managed IPS Rules enhance the baseline protections provided by AWS, delivering broad coverage to address common network security use cases. These rules can be deployed in just a few clicks with no infrastructure to manage, significantly reducing complexity for your security teams.

Automatically updated by FortiGuard Labs
Fortinet Managed IPS Rules are automatically updated based on the latest information from one of the industry's largest threat intelligence and research organizations.

Rapid protection for business-critical workloads
Secure your business-critical cloud workloads against vulnerabilities, malware, and Remote Access Trojans (RATs) with just a few clicks.

Offloads network security management
On-demand provisioning that enables you to rapidly scale your network security posture without the need for deep network expertise or management overhead.

Lowers costs without sacrificing security
By leveraging pay-as-you-go (PAYG) pricing models and fully managed infrastructure, you avoid large upfront investments and can better align spend with actual resource usage.

Fortinet Managed IPS Rules
for AWS Network Firewall

Powered by FortiGuard Labs
Global Threat Research and Response
FortiGuard Labs

FortiGuard Labs is our threat intelligence and research organization. The team is comprised of experienced threat hunters, researchers, analysts, engineers, and data scientists. For more than a decade, they have been applying machine learning (ML), artificial intelligence, and advanced analytics to achieve our mission of delivering the industry's best threat intelligence. This is used to power our threat prevention products and protect customers from malicious cyberattacks around the globe.

- 215+ expert researchers and analysts around the world
- 100 billion security events gathered and analyzed daily
- 200+ security intelligence partnerships and collaborations
Fortune Rulesets

Choose from a broad range of fully managed rulesets to meet your unique security needs.

**Application, Network, and IoT Vulnerabilities**
Rules that detect attempts to exploit vulnerabilities in common applications, including desktop software, network hardware (e.g., routers), and Internet-of-Things (IoT) devices.

**Malware Detection**
Rules that detect communication attempts from malware backdoors, worms, and RATs, including command-and-control traffic.

**Server and Operating System Vulnerabilities**
Rules that detect vulnerabilities in common server applications, including Domain Name System (DNS), email, remote access, and operating systems.

**Web Client Vulnerabilities**
This ruleset detects exploits targeting vulnerabilities in web browsers, including Chrome, Firefox, Internet Explorer, Edge, etc.

**Web Application Vulnerabilities**
This ruleset detects exploits targeting vulnerabilities in common web applications, including popular CMS platforms such as WordPress and Joomla.

**Web Server Vulnerabilities**
This ruleset detects exploits targeting web server vulnerabilities, including both web servers (e.g., Apache) and proxy web servers (e.g., Squid).
Getting Started

Deploy Fortinet Managed IPS Rules

Fortinet Managed IPS Rules are made available within your AWS account. All you have to do is select your preferred rule sets and you can begin filtering malicious traffic at the perimeter of your Amazon VPCs.

Once up and running, they will be automatically updated based on the latest threat intelligence from FortiGuard Labs, so your security teams can remain focused on business-critical tasks at hand.

Need more robust security capabilities?

Check out FortiGate next-generation firewall

FortiGate next-generation firewall (NGFW) is designed to provide more advanced protection, higher performance, and centralized management of your security controls across all on-premises and cloud environments. It also integrates to AI-driven FortiGuard services to protect against known and zero-day threats.

Try for free with our 30-day trial in AWS Marketplace.
Resources


3 Ibid.