SOLUTION BRIEF

Enhance AWS Network Firewall with Fortinet Managed IPS Rules

Executive Summary

Fortinet Managed IPS Rules for AWS Network Firewall, powered by FortiGuard AI-Powered Security Services, provides AWS customers with advanced, continuously updated intrusion prevention capabilities without requiring additional infrastructure or management overhead. This managed rule service extends Fortinet's industry-leading threat intelligence and protection directly into AWS Network Firewall environments, helping organizations automatically block exploits, malware, and command-and-control activity at scale.

Designed for simplicity and scalability, the solution empowers cloud security teams to protect dynamic workloads and applications with the same proven FortiGuard threat intelligence trusted by thousands of global enterprises. Continuous updates, automated protection, and seamless AWS integration help customers meet compliance mandates, reduce operational burden, and strengthen their overall cloud security posture.

Built-In Threat Protection for Cloud-First Security

Over **97 billion exploitation attempts** were recorded by FortiGuard's intrusion-prevention sensors in 2024, reflecting how adversaries are scaling attacks broadly.[1]

Meeting Today's Cloud Security Challenges

The growing attack surface in AWS environments

Modern enterprises rely on AWS for agility and scalability, but every new VPC, workload, and region increases the attack surface. Traditional network defenses often can't keep pace with the dynamic nature of cloud-native environments.

Security complexity slows innovation

Managing intrusion prevention policies across distributed AWS accounts, VPCs, and hybrid networks introduces operational complexity. Security teams face mounting pressure to maintain consistent protection without slowing cloud adoption.

Compliance and visibility gaps

AWS best practices and regulatory frameworks, such as PCI DSS, HIPAA, and ISO 27001, recommend inline intrusion prevention to safeguard sensitive data. However, building and maintaining robust IPS capabilities in the cloud requires time, resources, and specialized expertise.

Fortinet Managed IPS Rules: Continuous, AI-Driven Protection for AWS

Fortinet Managed IPS Rules for AWS Network Firewall delivers preconfigured, continuously updated intrusion prevention powered by FortiGuard AI-Powered Security Services. This service enables organizations to strengthen AWS Network Firewall deployments with intelligence-backed protection against known and emerging threats without manual tuning or maintenance.

Key capabilities:

- **AI-driven threat intelligence:** FortiGuard Labs analyzes billions of threat samples daily to generate real-time IPS updates across thousands of attack signatures.
- **Automated rule delivery:** New rules are continuously published to AWS Network Firewall, ensuring up-to-date protection without manual configuration.
- **Comprehensive coverage:** Managed IPS Rules protects against exploits targeting applications, operating systems, web servers, and client software.
- **Seamless AWS integration:** Deployed natively within AWS Network Firewall, Managed IPS Rules aligns with AWS best practices for inline inspection and compliance.
- **Flexible consumption:** The solution is available directly from AWS Marketplace with Pay-As-You-Go pricing or through multi-year private offers.

Simplified deployment and management

Customers can activate Fortinet Managed IPS Rules directly within the AWS Management Console—no new VMs, licenses, or complex configurations required. Once enabled, rule updates are automatically synchronized, ensuring continuous protection with zero operational friction.

Continuous Intelligence. Continuous Protection.

FortiGuard Labs delivers AI-driven security updates every five minutes to protect against new and emerging threats.[2]

Strengthen AWS Security, Simplify Operations, and Accelerate Compliance

Fortinet Managed IPS Rules helps organizations achieve stronger security outcomes while maintaining cloud agility and operational simplicity.

Key benefits:

- **Accelerated compliance:** Meet AWS reference architecture guidance for PCI DSS and other frameworks with managed inline IPS protection.
- **Reduced management burden:** Automatically receive the latest protections from FortiGuard Labs without manual tuning or updates.
- **Proven threat efficacy:** Managed IPS Rules is backed by the same FortiGuard intelligence that protects hundreds of thousands of customers globally.
- **Operational efficiency:** It enables cloud and SecOps teams to focus on innovation, not rule maintenance.

Organizations using Fortinet Managed IPS Rules gain a simplified, scalable path to strengthen their AWS Network Firewall deployment, closing the gap between speed and security in the cloud.

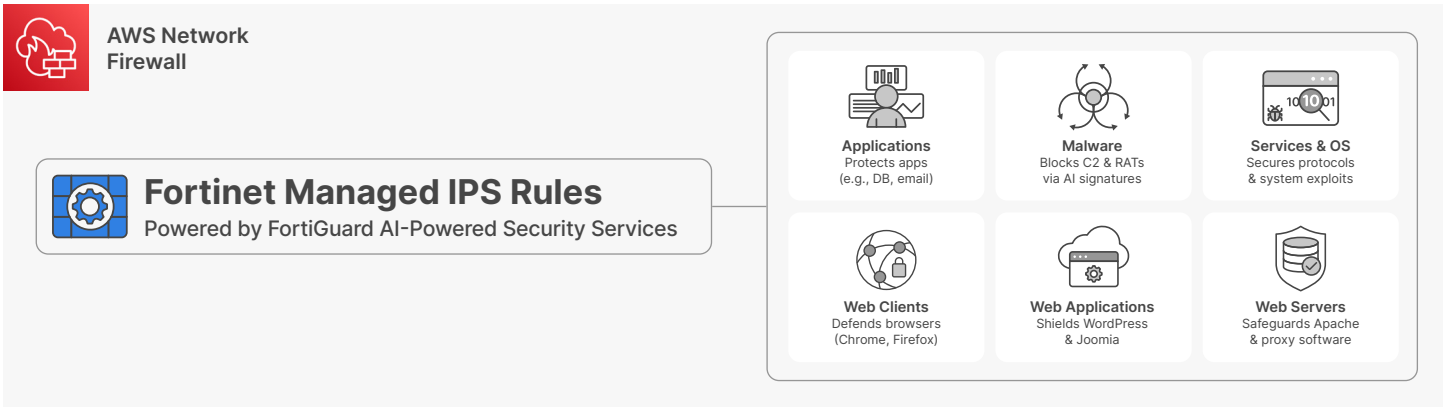

Figure 1: Fortinet Managed IPS Rules includes multiple rulesets

Conclusion: Enterprise-Grade Intrusion Prevention Simplified for the Cloud

By combining AI-driven threat intelligence with seamless AWS integration, organizations gain always-on protection against exploits and malware, accelerated compliance, and reduced operational overhead. With Fortinet, customers can secure their AWS environments at the speed of innovation.

Visit AWS Marketplace to learn more.

[1] Fortinet. "Fortinet Threat Report Reveals Record Surge in Automated Cyberattacks as Adversaries Weaponize AI and Fresh Techniques." April 28, 2025. https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2025/fortinet-threat-report-reveals-record-surge-in-automated-cyberattacks

[2] Fortinet, "FortiGuard AI-Powered Security Services for Applications." Accessed Nov. 13, 2025. https://www.fortinet.com/solutions/enterprise-midsize-business/security-as-a-service/fortiguard-subscriptions/application-security

FORTINET

www.fortinet.com

November 19, 2025 1:52 PM / MKTG-2517-0-0-EN