SERVICE BRIEF

Fortinet Managed IPS Rules Service for AWS Network Firewall

Easily Filter Malicious Traffic at the Perimeter of Your Amazon VPC

Introduction

Enterprises are speeding digital transformation, making the cloud's role in application delivery services more important than ever. Securing virtual private cloud networks and application workloads is critical, and must not add to a security team's operational burdens.

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

Benefits

Customers

Customers benefit from easy access to private offers, frictionless procurement, ease of deployment, and consolidated invoicing through their existing partner relationship. Other benefits include:

- **Reduces operational burden:** IPS Rules sets are automatically updated based on the latest threat information by Fortinet FortiGuard Labs.
- **Removes need for expert security management staff:** On-demand provisioning enables organizations to rapidly scale their network security postures.
- **Rapidly protects business-critical workloads:** Can secure business-critical cloud workloads against vulnerabilities, malware, and remote-access trojans with just a few clicks.
- **Lowers costs without compromising security:** Leveraging a managed service infrastructure for both network firewall and IPS Rules helps to avoid large infrastructure investments.

Product, Pricing, and Support

The Fortinet Managed IPS Rules Service is available on AWS Marketplace as a Private Offer for customers. The service is an annual subscription offer priced per pair of regions sharing the rule groups. Contact your Fortinet representative to learn more and get started with better security for your AWS VPCs.

By purchasing a Fortinet rule group, customers are entitled to support from Fortinet. Contact Fortinet support directly at awsips@fortinet.com.

Partners

Fortinet Partners can serve their customers and grow their business on AWS while benefiting from prenegotiated discounts and a simple resell model.

How It Works

Fortinet Managed IPS Rules offers end-users access to 14 rule-groups in 6 categories. The categories include:

1. Application, Network, and IoT Vulnerabilities
2. Server and Operating System Vulnerabilities
3. Malware Detection
4. Web Client Vulnerabilities
5. Web Server Vulnerabilities
6. Web Application Vulnerabilities

Additional Resource

Fortinet Managed IPS Rules

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

Fortinet Managed IPS Rules is available within AWS customers' accounts. End-users should provide the Fortinet team with contact information, AWS ID, and the regions where they want to deploy the service. The end-user's AWS ID (account number) is used to share the Managed IPS Rules. Fortinet provides access to the Managed IPS Rules through the AWS Resource Access Manager. Once the Rules are shared, the end-user will receive an email from Fortinet that they have access to the service for the selected regions. Using the AWS management console, they can follow a simple workflow to activate the Managed IPS Rules.

Fortinet Managed IPS Rules is supported in 21 regions across the Americas, Europe, APAC, and EMEA. The AWS Firewall rules administration guide has the most updated information.

January 3, 2022 9:49 PM
1402151-0-0-EN