AUTOMATICALLY SCALE CLOUD SECURITY WITH EASE ON AMAZON WEB SERVICES

Leveraging cloud computing instead of buying new infrastructure is becoming the new normal. In fact, for many organizations, it has become the default choice. Cloud computing fulfills rapid IT environment provisioning needs, allows use of on-demand applications, and enables companies to analyze big data as storage requirements grow. AWS Partner Network (APN) Advanced Technology Partner Fortinet delivers a cost-effective Security-as-a-Service (SaaS) solution on AWS that can help lower operational expenses and reduce security complexity, helping customers fulfill their duties of the AWS Shared Responsibility Model. Fortinet provides advanced threat protection to a variety of environments including data centers, environments with distributed locations, and branch offices. Security appliances from Fortinet seamlessly integrate with Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Virtual Private Cloud (Amazon VPC) to minimize risk and mitigate security threats for workloads running on the public cloud.

HIGHLIGHTS

- Delivers top-tier security solutions
- Includes comprehensive Amazon Machine Image (AMI) security portfolio
- Pre-configures AWS CloudFormation Template for instant high-availability (HA) and Auto Scaling deployment
- Allows for flexible licensing of on-demand cloud deployment, annual or hourly metering
- Protects physical, virtual, and cloud workloads across your entire network with one solution

COMPREHENSIVE, AGILE SECURITY

Fortinet delivers a best-in-class enterprise security AMI portfolio including FortiGate, FortiWeb, FortiMail, FortiAnalyzer, and FortiManager:

- FortiGate provides comprehensive threat protection — through Fortinet’s unmatched range of enterprise-grade security technologies to deliver firewall, VPN (IPsec and SSL), intrusion prevention, and antivirus/anti-spam/anti-spyware.

- FortiWeb AWS is a leading Web Application Firewall:
  - Identifies vulnerabilities instantly in web applications without false positives
  - Offers many options for reverse proxy security for applications like Outlook Web Access
  - Protects against SQL injection and zero-day middleware and database attacks
  - Includes X.509 certificate authentication for single sign-on options

- FortiMail drives comprehensive mail security and ensures all-in-one inbound and outbound security protection
  - FortiSandbox provides the zero-day advanced threat detection with the indicators of compromise (IOC) verdicts that intelligence can be shared across Fortinet Security Fabric products.

- FortiAnalyzer delivers log analytics and real-time compliance auditing

- FortiManager streamlines hybrid deployment and security posture management via single-pane-of-glass management
FortiGuard Labs provides near real-time threat intelligence updates:
- URL database filtering, including command-and-control servers
- GeoIP intelligence
- IPS signatures
- Malware scanning

It’s important to remember that security is still every IT department’s responsibility to configure, regardless of the tools offered by AWS and APN Partners.

WHY FORTINET IN AWS
Fortinet delivers a unified security posture across all types of environments through its suite of network security features including firewall, intrusion prevention (IPS), antivirus (AV), application control, WAN optimization, data loss prevention (DLP), web filtering, anti-spam filtering, and explicit proxy on AWS. All features are natively built by Fortinet and are updated in real time by FortiGuard advanced threat intelligence, plus can leverage autoscaling to create a high-availability environment.

PAY-AS-YOU-GO
By using AWS, you get the ability to scale up or down without any of the associated overhead costs required to manage physical servers. Fortinet leverages cloud security practices by offering both hourly and annual consumption.

Fortinet virtualized appliances deliver next-generation firewall, intrusion prevention, and web application security for Amazon EC2 instances in the public cloud where hardware solutions cannot be deployed. AWS users can leverage the same Fortinet enterprise-class network security controls on AWS as they deploy on their internal data centers or private clouds. In addition to Fortinet Virtual Machines (VMs) on AWS Marketplace, Fortinet provides advanced configuration options for HA design in AWS.

AUTOMATE CLOUD SECURITY WITH AUTO SCALING
Dynamic cloud workloads have peak and off-peak hours. You can no longer manually hairpin your security process to reliably ensure your security posture and business operations are non-disruptive. As you scale out your storage, network, and compute, you should scale out your security simultaneously. Automating security is not trivial, however. Fortinet has developed an AWS CloudFormation template that leverages Auto Scaling to add FortiGate enterprise firewall instances automatically based on user defined criteria while using AWS integrated scripts and templates to maintain a familiar user interface (UI) and initiate security elasticity for optimal network utilization.

FORTIGATE USING AMAZON ROUTE 53
To ensure availability and optimization of FortiGate advanced threat protection over the entire Auto Scaling group, Fortinet maps your AWS security postures to scale up and down with your Amazon EC2 workload via an AWS CloudFormation template. This template can be held in a repository, making it reproducible and easily deployable as new instances require secure elasticity.

HOT STANDBY FORTIGATE APPLIANCES ON AWS

Fortinet’s agile security solutions can quickly secure workloads and applications, plus support customer compliance requirements across the AWS Cloud and varying environments including data centers, distributed locations, and branch offices. Fortinet uses encryption to protect sensitive data on AWS environments and simplify operations and compliance so that businesses can expend energy on what they are building.
SOLUTION BRIEF: AMAZON WEB SERVICES

FORTINET PRODUCT LISTINGS ON MARKETPLACE

**Fortinet FortiGate-VM**
15 Day Free Trial Available - Fortinet FortiGate-VM firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.

**Fortinet FortiGate-VM (BYOL)**
Fortinet FortiGate-VM firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features.

**Fortinet FortiManager-VM Centralized Security Management**
Fortinet FortiManager Security Management appliances allow you to centrally manage any number of Fortinet Network Security devices, from several to thousands, including FortiGate, FortiWiFi, and FortiCarrier.

**Fortinet FortiMail-VM (BYOL)**
Fortinet FortiMail-VM provides a single solution to protect against inbound attacks - including advanced malware - as well as outbound threats and data loss with a wide range of top-rated security capabilities.

**Fortinet FortiAnalyzer-VM Centralized Security Logging and Reporting**
Fortinet FortiAnalyzer-VM securely aggregates log data from Fortinet devices and other syslog-compatible devices.

**Fortinet FortiAnalyzer-VM Centralized Logging/Reporting On-Demand**
15 Day Free Trial Available - Fortinet FortiAnalyzer-VM securely aggregates log data from Fortinet devices and other syslog-compatible devices.

For further CloudFormation or Lambda functions, please visit Fortinet Solution Github repository at https://github.com/fortinet/solutions/AWS-CloudFormationTemplates

---

Copyright © 2017 Fortinet, Inc. All rights reserved. FortiGate®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant herein, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

About AWS: For 10 years, Amazon Web Services has been the world’s most comprehensive and broadly adopted cloud platform. AWS offers over 70 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 33 Availability Zones (AZs) across 12 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, and Singapore. AWS services are trusted by more than a million active customers around the world – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit http://aws.amazon.com.

February 13, 2018 3:30 PM