SOLUTION BRIEF

Automatically Scale Cloud Security With Ease on Amazon Web Services

Executive Summary

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 (SECaaS) 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.

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, virtual private network (VPN) (Internet Protocol security [IPsec] and secure sockets layer [SSL]), intrusion prevention, and antivirus/antispam/antispyware.
- 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.

Joint Solution Benefits

- Delivers top-tier security solutions
- Includes comprehensive Amazon Machine Image (AMI) security portfolio
- Preconfigures 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

FORTINET FABRIC-READY

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.

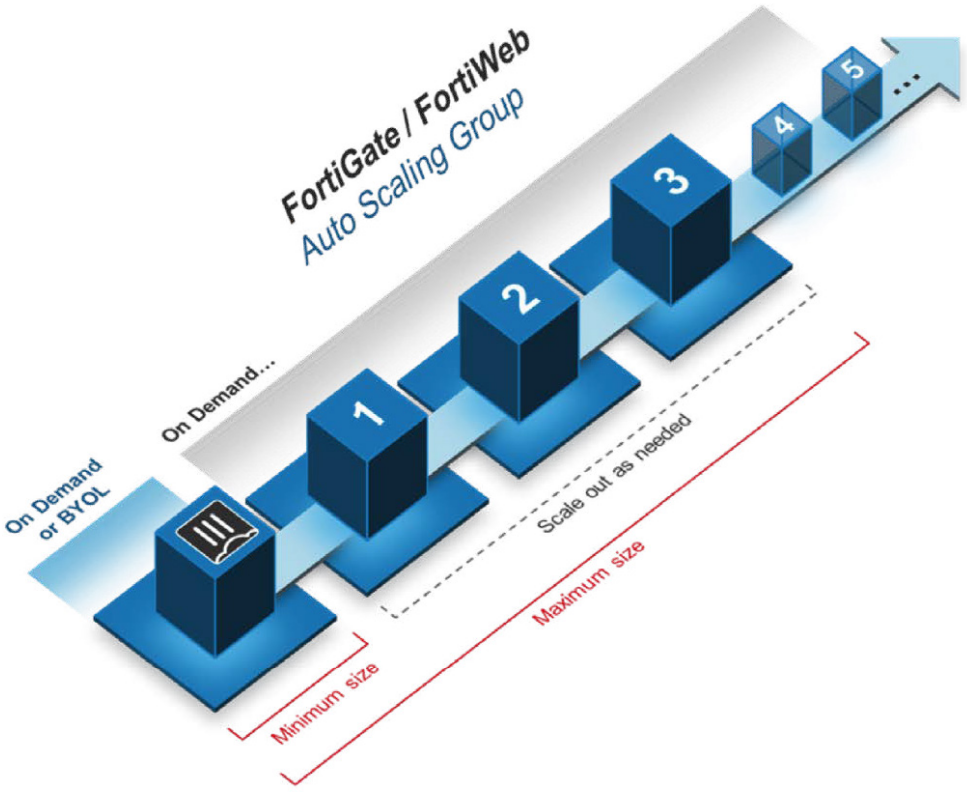
Why Fortinet in AWS

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, antispam 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 auto scaling to create a high-availability (HA) 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 (NGFW), 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 nondisruptive. 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 secure elasticity for optimal network utilization.

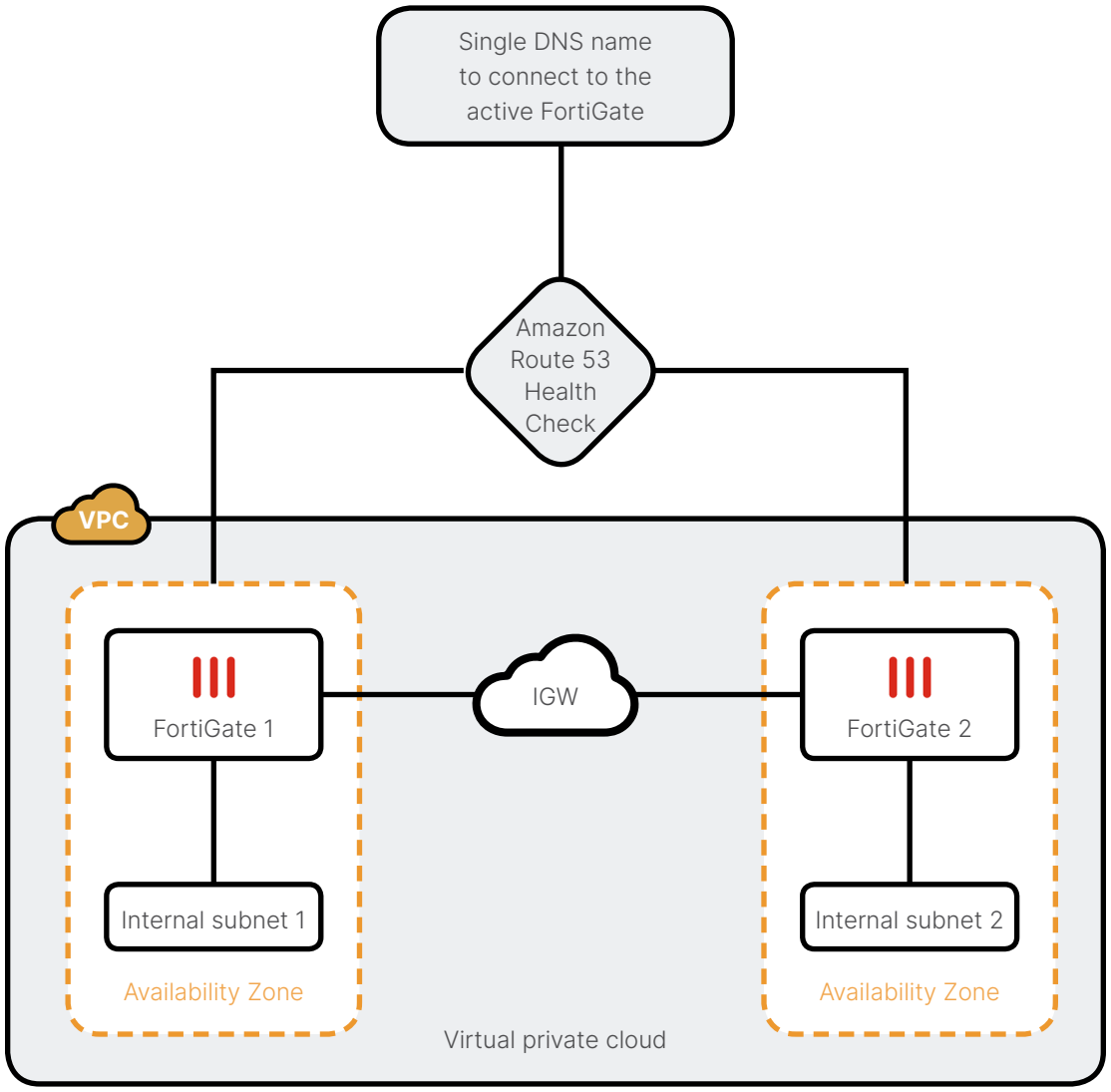


Figure 1: FortiGate using Amazon Route 53.

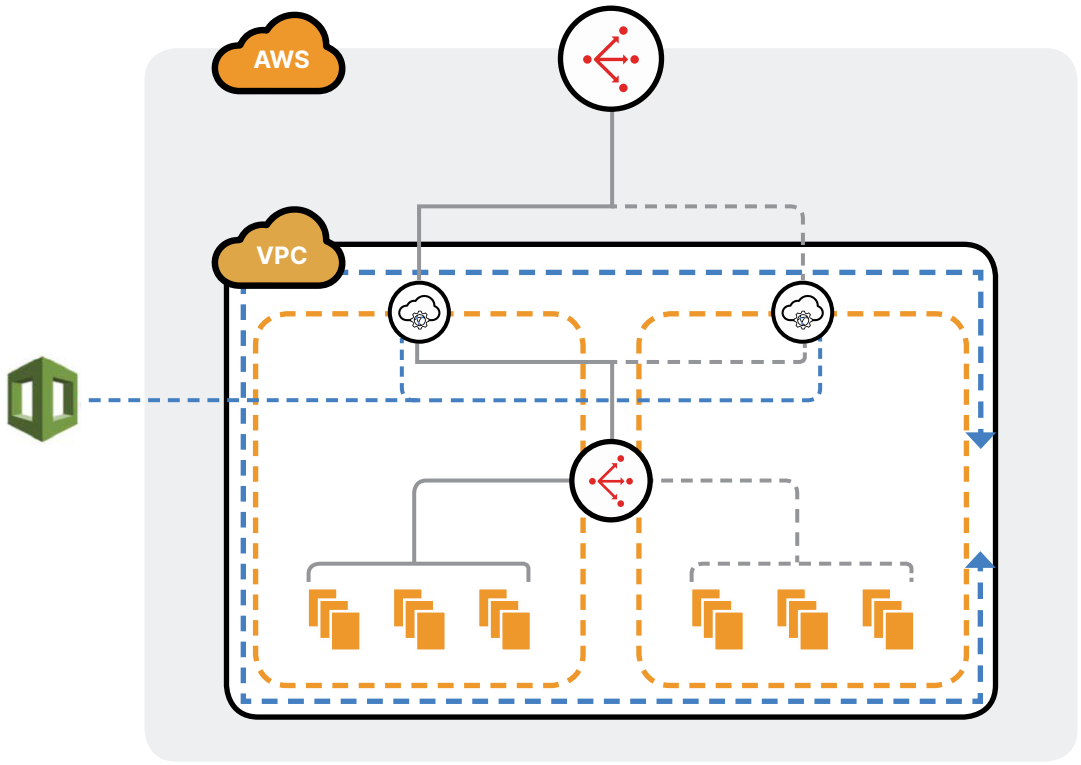


Figure 2: FortiWeb using Amazon ELB. (In this case we show an ELB Sandwich.)

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.

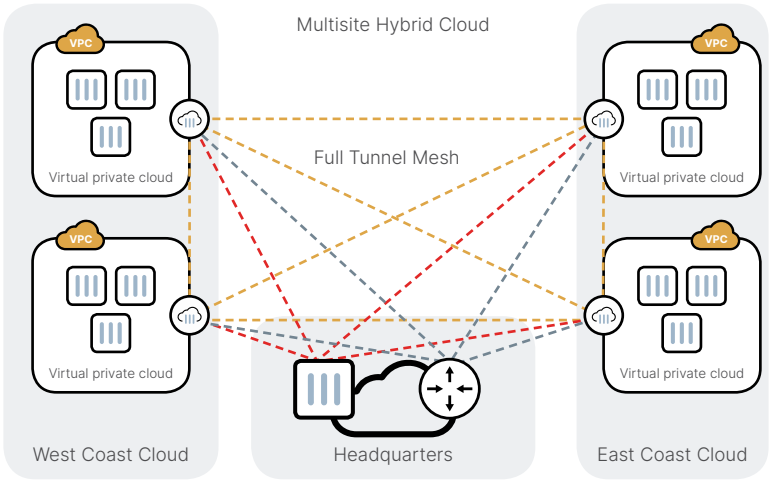


Figure 3: Full tunnel mesh connecting all VPCs with headquarters.

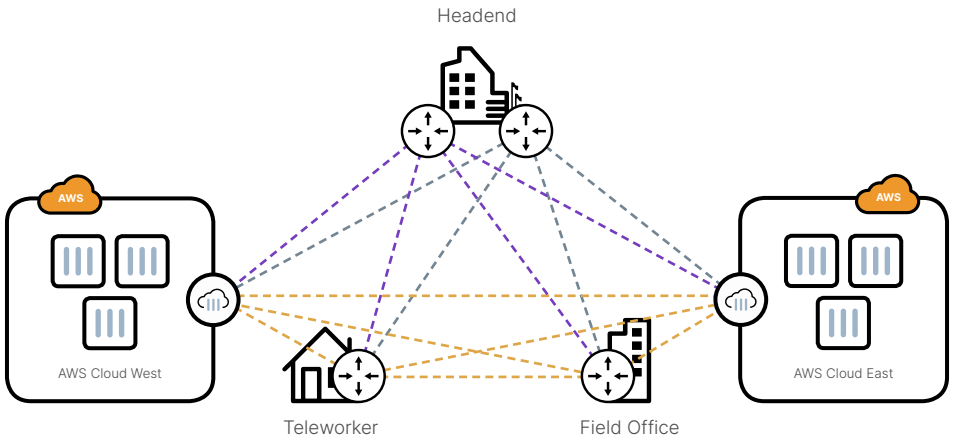


Figure 4: Enterprise distributed remote locations to create tunnels. Connecting AWS hosts to reduce bottlenecks.

FortiGate VMs provide full NGFW and unified threat management (UTM) functionality, securing the virtual infrastructure while also providing VPN and internet gateway protection. The seamless integration with Amazon EC2 and Amazon VPC further mitigates security concerns and provides advanced threat protection capabilities beyond standard security offerings on the AWS environment. For more information on Fortinet on AWS, visit the product listing in the AWS Marketplace.

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.

Fortinet FortiWeb VM Web Application Firewall

15-day Free Trial Available—Advanced protection for AWS web-based applications. Hosting on AWS is a fast and simplified method to deploy and manage web-based applications.

FortiSandbox VM On-demand

FortiSandbox identifies zero-day, advanced malware including ransomware, and generates relevant threat intelligence.

Fortinet FortiSIEM Collector VM (BYOL)

FortiSIEM Collector VM is used for data collection in AWS environments. FortiSIEM is a highly scalable multitenant security information and event management (SIEM) solution.

Fortinet FortiSIEM VM (BYOL)

FortiSIEM is a highly scalable multitenant solution that provides real-time infrastructure and user awareness for accurate threat detection, analysis, and reporting.

Fortinet FortiWeb Manager—Centralized Management

Centralized deployment and management of FortiWeb web application firewalls (WAFs). FortiWeb Manager centralizes the configuration of FortiWeb appliances on AWS or hosted in an on-premises data center.

Fortinet FortiWeb VM Web Application Firewall (BYOL)

Advanced protection for AWS web-based applications. Hosting on AWS is a fast and simplified method to deploy and manage web-based applications.

For further CloudFormation or Lambda functions, please visit the Fortinet Solution GitHub repository at https://github.com/fortinetsolutions/AWS-CloudFormationTemplates.

March 29, 2021 11:35 PM

D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\March\Branding Refresh\913517 - Update Connecting SBs\sb-FA-automatically-scale-cloud-services-3292021\sb-FA-automatically-scale-cloud-services-3292021

924001-A-0-EN