On-Demand Security-as-a-Service with Amazon Web Services

Cloud computing as new infrastructure or resources is becoming the new normal. For many people it has become the default choice. Cloud computing fulfills rapid IT environment provisioning. It enables on-demand applications and enables companies to analyze big data as storage requirements grow. Fortinet and Amazon Web Services (AWS) deliver a cost-effective, security-as-a-service (SaaS) solution with lower operational expenses, reduced complexity, and a reduced security risk that provides advanced threat protection to varying environments including datacenter, distributed locations and branch offices. Fortinet enables enterprise posture beyond standard security offerings in the AWS environment. Fortinet security appliances seamlessly integrate with Amazon EC2 and VPC to minimize risk and mitigate security concerns over the public cloud.

Cloud Elasticity Needs Security Agility

Highlights:

- Best-in-class Enterprise AMI available: FortiGate, FortiWeb, FortiAnalyzer, and FortiManager can plug in to AWS security reference architecture instantly

- FortiGate provides comprehensive threat protection with Fortinet’s unmatched range of enterprise-grade security technologies to deliver firewall, VPN (IPsec and SSL), intrusion prevention, and antivirus/anti-spyware/anti-spam technologies
– Multiple high-availability (HA) options with config sync via FortiManager
  - FortiGuard updates to provide best-in-class security
  - URL database/filtering, including command-and-control servers and GeoIP intelligence
  - IPS signatures
  - Malware scanning

- FortiWeb for AWS class-leading Web Application firewall
  - Identifies vulnerabilities instantly in web applications without false positives
  - Many options for reverse proxy security for applications like Outlook Web Access
  - SQL injection and zero-day middleware and database protection
  - X509 certificate authentication for Single-SignOn options

- Flexible licensing for on-demand Cloud deployment usage including Bring-Your-Own-License (BYOL), Annual or Hourly metering

- FortiAnalyzer for AWS output syslog for log analytics and real-time compliance auditing

- FortiManager seamless hybrid deployment and security posture management with a single console: available in virtual machines, physical appliance, or Amazon Machine Image (AMI)

“AWS offers self-service, highly automated, highly scalable cloud infrastructure-as-a-service (IaaS), along with some platform-as-a-service (PaaS) capabilities. While it is easy to get started with these services, as customers expand their adoption, they encounter challenges in managing availability, performance, security, cost, and internal governance.” -Gartner G00268418

It’s important to remember that Security is still every IT Department’s responsibility to configure, regardless of the tools offered by AWS.

Why Fortinet in AWS

Fortinet delivers the most complete and full range 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 in AWS. All features are natively built by Fortinet and updated in real time by FortiGuard advanced threat intelligence.

Pay-As-You-Go or Bring-Your-Own-License (BYOL)

It’s not hard to see why there is such demand in AWS where you get the ability to scale up or down, without any of the overhead to manage physical servers. Fortinet realizes the security practice also needs to provide utility metering. If existing customers have purchased the licenses, Fortinet eases the licensing transition concerns in the data center or the Cloud.

Fortinet virtual appliances enable critical firewall, intrusion prevention, and web application security for AWS instances in the public cloud where hardware solutions cannot be deployed. AWS users can leverage the same Fortinet enterprise-class network security controls in AWS as they deploy in the internal data center or private cloud. In addition to Fortinet VMs in the AWS Marketplace, Fortinet provides advanced configuration options for HA design in AWS.
Hot Standby FortiGate Appliances in AWS

One of many solution differentiators is that Fortinet enables both FortiGate firewalls passing traffic at the same time using hot standby. FortiGate achieves high availability in AWS across multiple AZs leveraging FortiManager to perform a configuration sync between the two FortiGate appliances. By leveraging Route 53’s health checks, we can detect any connection failure. This solution is ideal because most of the traffic is originated from devices behind the firewall. For the application servers expected to have inbound connections, the data needs to be replicated on both the AZs.

Quickly Secure Your AWS Cloud Workloads in Varying Environments

The Fortinet agile security solution can quickly secure workloads in the AWS cloud supporting customer compliance requirements, applications, and varying environments including data center, distributed locations, and branch offices.

Fortinet uses encryption to protect sensitive data in AWS environments and simplify operations and compliance so that businesses can expend energy on what they are building.
FortiGate-VMs provide full UTM and Next-Generation Firewall functionality securing the virtual infrastructure while also providing VPN and Internet Gateway protection. The seamless integration with EC2 and VPC further mitigates security concerns and provides advanced threat protection capabilities beyond standard security offerings in the AWS environment.

For more Fortinet information on AWS, visit the product listing in AWS Marketplace.

For use case and security practices sharing, visit Fortinet Cookbook.