AUTO SCALING SECURITY ON AWS

Maintaining a Dynamic Security Posture on the Cloud

April 2017

TABLE OF CONTENTS

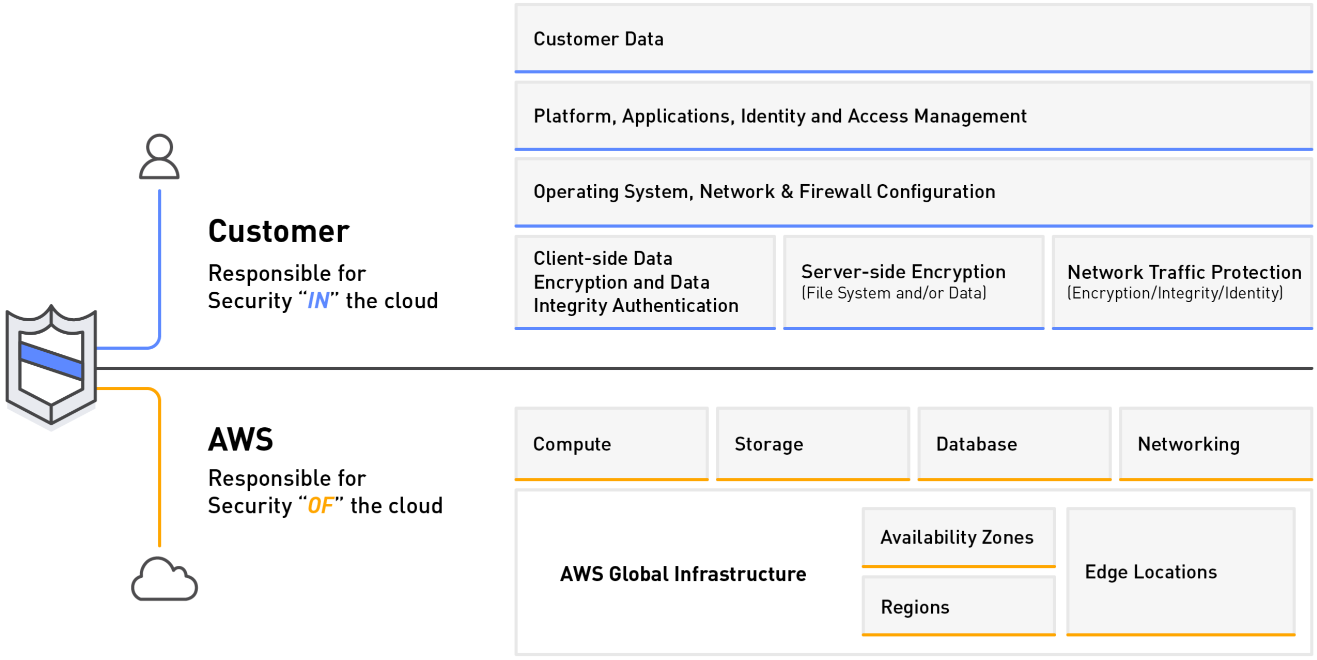
Maintaining Application Availability on the Cloud

Increased operational efficiency is one of the primary reasons most organizations are migrating applications to the cloud. The efficiency afforded by public cloud environments comes in many forms, a key one being the ability to eliminate the over-provisioning of resources. After undertaking a cloud migration, organizations no longer have to go through the time and expense of buying, deploying, and integrating servers to accommodate for spikes in network traffic. Instead, they can dynamically scale compute resources as demands change, paying only for what they use.

On the Amazon Web Services (AWS) Cloud, you can utilize AWS Auto Scaling, which automatically provisions additional Amazon Elastic Compute Cloud (Amazon EC2) capacity to keep applications available and maintain performance while optimizing costs.

Securing Workloads on the AWS Cloud

Security is essential to the successful operation of cloud environments. In order to maintain a strong security posture on the cloud, the resources that support security applications must scale up and down as dynamically as those supporting line-of-business applications. The AWS Shared Responsibility Model defines how security responsibility is shared between AWS and the customer. AWS shoulders responsibility for the security of the cloud, which includes the global infrastructure that supports the cloud such as hardware, software, networking, and the facilities that house AWS services. Customers are responsible for security on the cloud, which includes anything they put into the cloud like content, platform, applications, systems, and networks.



Customer Data

Platform, Applications, Identity and Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption and Data Integrity Authentication

Server-side Encryption (File System and/or Data)

Network Traffic Protection (Encryption/Integrity/Identity)

Customer

Responsible for Security "*IN*" the cloud

AWS

Responsible for Security "*OF*" the cloud

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Next Generation Firewalls: Providing Security "in" the Cloud

Traditionally, firewalls have been utilized to protect workloads from outside attacks. As IT architectures have become more complex and organizations have made the decision to migrate workloads to the cloud, they've realized the need to extend the same robust firewall capability that existed in their data center to their cloud-based assets. This has led to the deployment of powerful next generation firewalls (NGFWs) on public clouds like AWS.

NGFWs combine the elements of a traditional firewall like network- and port-address translation (NAT), stateful inspection, virtual private network (VPN) support, and packet filtering with more advanced filtering functions such as:

- VPN (IPsec and SSL)
- Intrusion prevention and detection (IPS/IDS)
- Data loss prevention (DLP)
- TLS/SSL encrypted traffic inspection
- Website filtering
- Antivirus/anti-spyware/anti-spam technologies

Next generation firewalls provide more granular inspection capabilities, which in turn offers organizations more robust protection against attacks and malware than traditional firewalls.

FortiGate Next Generation Firewall

Fortinet's FortiGate is a dynamic next generation firewall (NGFW) capable of delivering enterprise-grade protection across your entire hybrid network. Offering consistent security capability in both physical and virtual form factors, FortiGate delivers effective cybersecurity protection across private and public cloud domains.

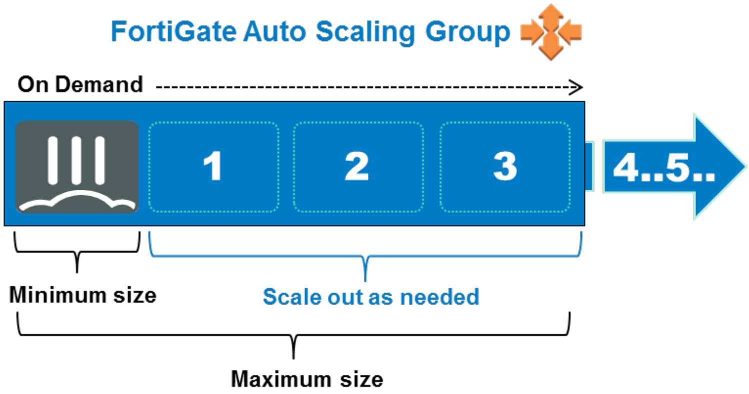
FortiGate:

- Operates the fastest global on-premises platform, scaling to 1Tbps in hybrid cloud environments
- Performs consistent and coordinated policies across both your bare metal and virtualized on-premises resources and cloud environments
- Is backed by industry-leading threat research and intelligence
- Integrates multiple security features in one common platform for a unified security posture across your entire environment

Fortinet's FortiGuard Research Labs is the largest threat research team in the world, composed of over 200 dedicated staff and logging over 40M events every second of every day. They discover more zero-day attacks than any other organization in the world, and this expertise is built into Fortinet solutions, including the FortiGate Next Generation Firewall.

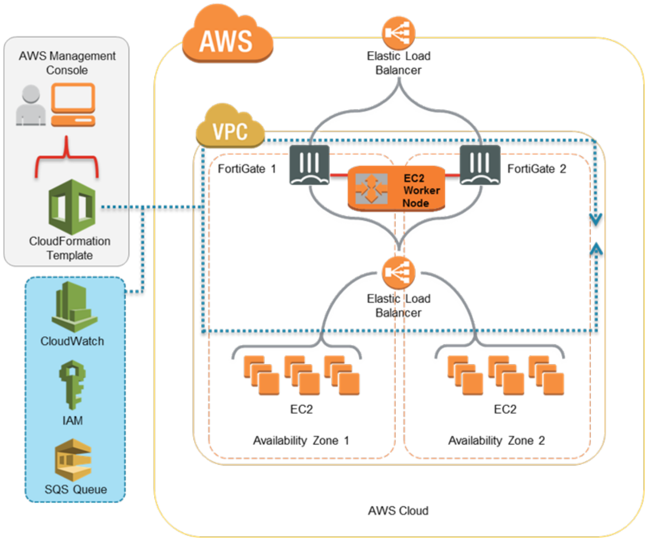
Enhancing Cloud Security with AWS Auto Scaling and FortiGate NGFW

AWS Auto Scaling ensures that an organization always has the correct number of Amazon EC2 instances available to handle the load of your application. To simplify deployment of FortiGate inside an optimal architecture, FortiGate uses an AWS CloudFormation template that uses AWS Auto Scaling to dynamically scale with your applications, maximizing resource efficiency. As the customer, you define the minimum and maximum sizes to scale and the firewalls flex to the parameters. You can further align FortiGate to your needs by adjusting other criteria, including CPU utilization, memory utilization, and concurrent sessions/session setup rate.

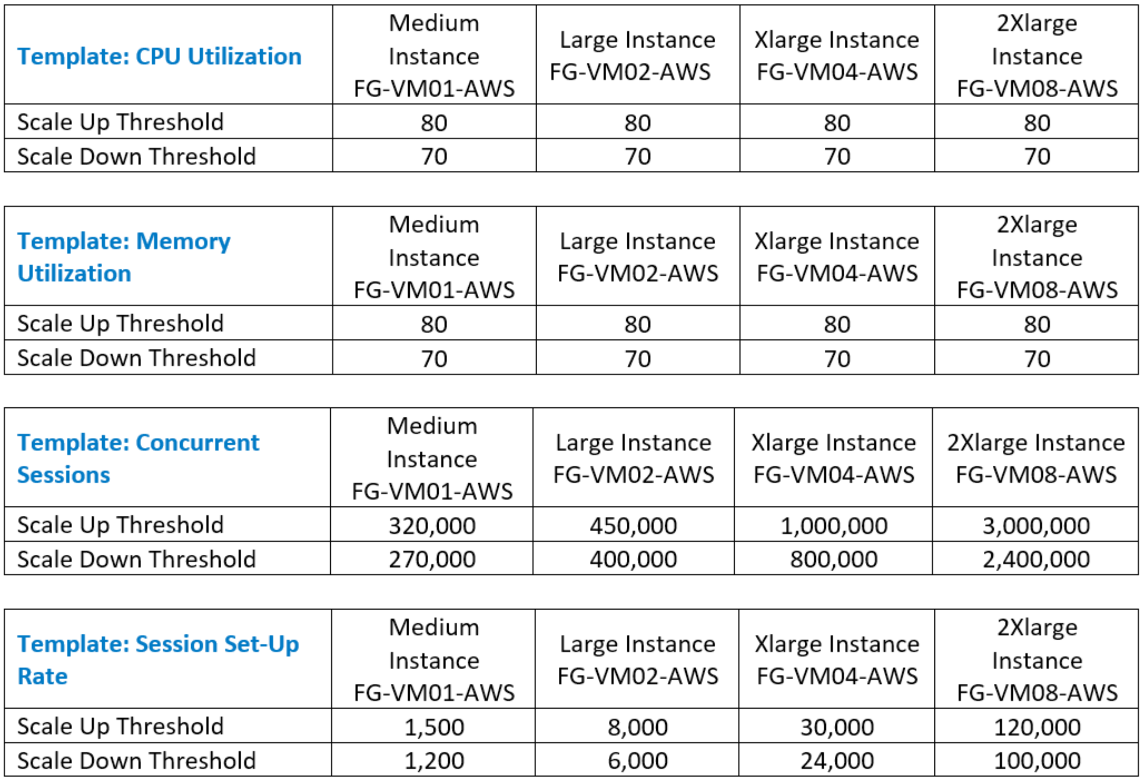


Solution Highlights

- Provides timely protection as workloads scale horizontally
- Delivers automatic scaling for best-in-class advanced security on AWS
- Pre-tunes “minimum” and “maximum” security parameters to provide refined security policies
- Minimizes cloud instance over-subscription and OpEx spending
- Eliminates error-prone manual intervention in security configurations



Auto Scaling Guidelines (FortiGate On-Demand c3/c4/m3 Instances) with suggested Scale Up/Scale Down criteria parameters:



Template: CPU Utilization	Medium Instance FG-VM01-AWS	Large Instance FG-VM02-AWS	Xlarge Instance FG-VM04-AWS	2Xlarge Instance FG-VM08-AWS
Scale Up Threshold	80	80	80	80
Scale Down Threshold	70	70	70	70

Template: Memory Utilization	Medium Instance FG-VM01-AWS	Large Instance FG-VM02-AWS	Xlarge Instance FG-VM04-AWS	2Xlarge Instance FG-VM08-AWS
Scale Up Threshold	80	80	80	80
Scale Down Threshold	70	70	70	70

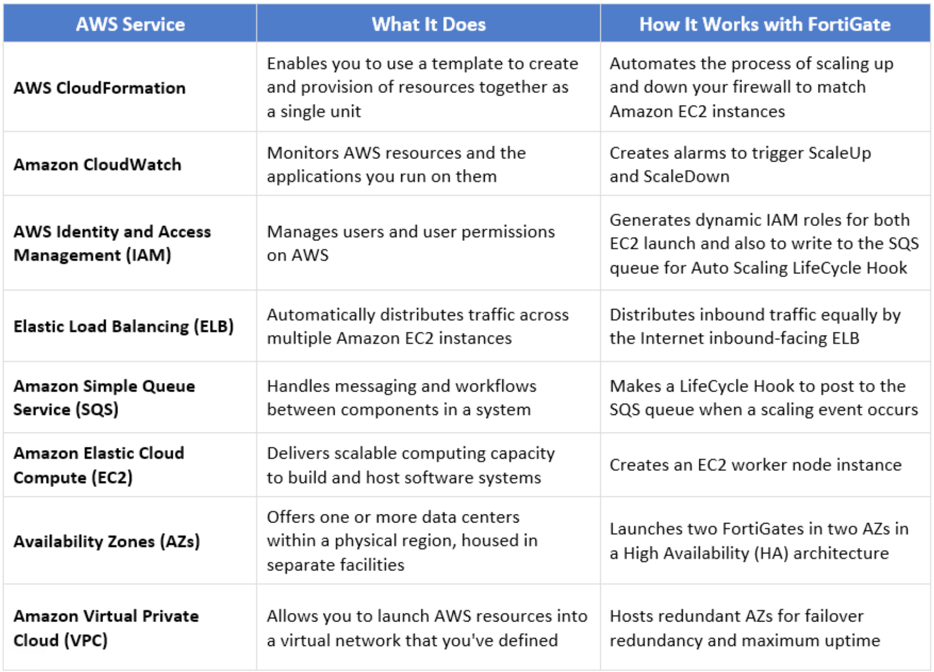
Template: Concurrent Sessions	Medium Instance FG-VM01-AWS	Large Instance FG-VM02-AWS	Xlarge Instance FG-VM04-AWS	2Xlarge Instance FG-VM08-AWS
Scale Up Threshold	320,000	450,000	1,000,000	3,000,000
Scale Down Threshold	270,000	400,000	800,000	2,400,000

Template: Session Set-Up Rate	Medium Instance FG-VM01-AWS	Large Instance FG-VM02-AWS	Xlarge Instance FG-VM04-AWS	2Xlarge Instance FG-VM08-AWS
Scale Up Threshold	1,500	8,000	30,000	120,000
Scale Down Threshold	1,200	6,000	24,000	100,000

High Availability (HA)

AWS recommends that organizations architect redundant Availability Zones (AZs) in each Amazon VPC for failover redundancy and maximum uptime in the event of an instance failure. In an Active/Passive FortiGate HA AWS environment, if the Active firewall has an issue and is unable to process traffic, a manual change is necessary for the route table to go through the Passive firewall. To eliminate the manual steps involved in maintaining security redundancy, Fortinet has created a script which monitors both firewalls and will automate route table changes if it detects an issue. Automating this process reduces errors that typically stem from manual intervention in security configurations. This HA implementation is built into the FortiGate Auto Scaling AWS CloudFormation template.

FortiGate integrates seamlessly into AWS and utilizes a number of AWS native tools, templates, and infrastructures to enable repeatable, scalable, and resilient architectures to meet any organization’s security needs.



AWS Service	What It Does	How It Works with FortiGate
AWS CloudFormation	Enables you to use a template to create and provision of resources together as a single unit	Automates the process of scaling up and down your firewall to match Amazon EC2 instances
Amazon CloudWatch	Monitors AWS resources and the applications you run on them	Creates alarms to trigger ScaleUp and ScaleDown
AWS Identity and Access Management (IAM)	Manages users and user permissions on AWS	Generates dynamic IAM roles for both EC2 launch and also to write to the SQS queue for Auto Scaling LifeCycle Hook
Elastic Load Balancing (ELB)	Automatically distributes traffic across multiple Amazon EC2 instances	Distributes inbound traffic equally by the Internet inbound-facing ELB
Amazon Simple Queue Service (SQS)	Handles messaging and workflows between components in a system	Makes a LifeCycle Hook to post to the SQS queue when a scaling event occurs
Amazon Elastic Cloud Compute (EC2)	Delivers scalable computing capacity to build and host software systems	Creates an EC2 worker node instance
Availability Zones (AZs)	Offers one or more data centers within a physical region, housed in separate facilities	Launches two FortiGates in two AZs in a High Availability (HA) architecture
Amazon Virtual Private Cloud (VPC)	Allows you to launch AWS resources into a virtual network that you've defined	Hosts redundant AZs for failover redundancy and maximum uptime

Summary

The effectiveness of your security in a cloud environment is determined not only by the efficacy of the security solution that has been put in place but also by the ability of the security solution to fully protect your workloads on the cloud. As workloads on AWS have the ability to scale dynamically with consistent High Availability performance, an organization's security posture must be able function the same way. Next Generation Firewalls such as FortiGate roll all the necessary features like High Availability and Auto Scaling into one dynamic security solution that protects data across public and private cloud domains.

Launching on AWS

The FortiGate Auto Scaling AMI is available in AWS Marketplace and supported across all AWS Marketplace Regions that support on-demand. Customers can also start with a 15-day free trial, to get a feel for the dynamic protection that FortiGate provides. After the trial, FortiGate offers affordable annual or hourly, pay-as-you-go pricing through AWS Marketplace). If you already have an existing FortiGate virtual appliance and are looking to move it from your on-premises environment to AWS, you can also deploy a bring-your-own-license (BYOL) Amazon Machine Image (AMI) from AWS Marketplace.

FortiGate Auto Scaling is based on AWS On-Demand:

- On-demand is a subscription-based transaction via AWS Marketplace (Annual/Hourly)
- Scaling instances, which scale in and out per selected criteria, are also on-demand
- Auto Scaling is supported with v5.4.2 only
- Bring Your Own License (BYOL), the Fortinet-AWS-VM perpetual license, is not yet supported in this Auto Scaling solution. Look for this support in subsequent Auto Scaling AWS CloudFormation templates from Fortinet

About Fortinet

Fortinet provides top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Their unique security fabric combines purpose-built ASICs, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control—while providing easier administration.

About Amazon Web Services

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 90 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 42 Availability Zones (AZs) across 16 geographic regions in the U.S., Australia, Brazil, Canada, China, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS services are trusted by millions of active customers around the world monthly—including the fastest growing startups, largest enterprises, and leading government agencies—to power their infrastructure, make them more agile, and lower costs.

For More Information:

FortiGate in AWS Marketplace

More about Fortinet

More about Amazon Web Services