SOPHOS

Security made simple.

Sophos UTM on AWS

Overview Guide

Document date: Tuesday, January 31, 2017

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to nsg-docu@sophos.com.

Contents

1 Introduction

Sophos Unified Threat Manager (UTM) makes security simple by providing integrated security tools into one solution. Protection like NextGen Firewall, Intrusion Prevention System (IPS), Web Application Firewall (WAF), and Virtual Private Network (VPN) connections are available out of the box in Sophos UTM to help you decrease your security costs and increase your security without requiring you to be a security expert. Sophos UTM on AWS continues with this goal by integrating with AWS services that customers use the most and need help in securing your cloud workloads. You can deploy Sophos UTM in different scenarios and with little effort ensure your AWS environment is secure. The goal of this document is to provide an overview of Sophos UTM on AWS and help customers use Sophos products in AWS for supported use cases.

For information on installing and managing Sophos UTM, see the Sophos UTM Administration Guides.

2 Amazon Web Services (AWS)

Amazon Web Services (AWS) is a collection of remote computing and web services that together make up the Amazon Cloud Computing platform. The more popular AWS services cover storage and virtual computing, but AWS offers more services such as database, mobile, analytics, and Internet of Things (IoT).

Together these services allow customers to reduce time and efforts associated with deploying business applications, provide a highly secure, scalable, flexible, and redundant computing platform. These services along with the Pay As You Go (PAYG) pricing provide businesses a way to replace up front capital infrastructure investments with variable operating costs and dramatically decrease the time and efforts associated with deployment.

With this move, customers need a simple solution that ensures their data and infrastructure are secure. This is where Sophos UTM on AWS can help. This document will list the reasons why customers need additional protection like Sophos UTM on AWS and then how the solution can help you secure your AWS environment.

Discussion of all the available AWS services is outside the scope of this document, but this document will briefly discuss services used by Sophos UTM on AWS so you can understand how the solution is integrated.

For information on all AWS services, see What is AWS.

2.1 Shared Responsibility Model

AWS provides Infrastructure as a Service (IaaS), which allows customers to build systems on top of the secure AWS Cloud infrastructure. AWS puts great focus on securing the data centers it operates and built in security tools to secure endpoints, encrypt data storage, and segregate customers' virtual networks and applications. This is referred to as "Security of the cloud."

Customers are responsible for using the supplied tools to properly secure access to their environments and create security policies for services running in AWS. This is referred to as "Security in the cloud."

Sophos UTM on AWS helps customers comply with their responsibility by integrating with the security tools already provided by AWS and providing additional tools to have a complete security solution.

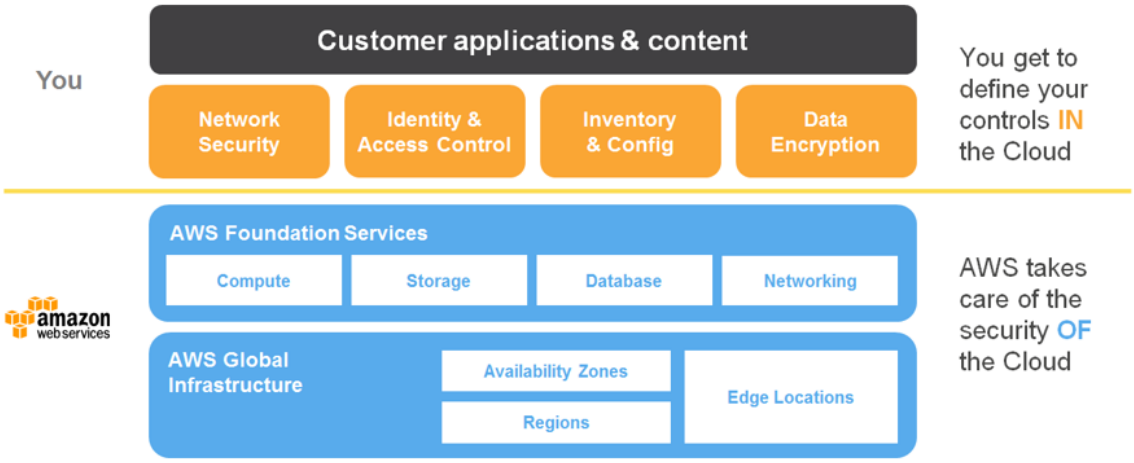


Figure 1 Shared Responsibility Model

For more information, see the Shared Responsibility Model.

2.2 Amazon Elastic Cloud Compute (EC2)

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity. You can use EC2 to launch virtual servers that host applications, run on-demand workloads, or extend your data center for your business. These virtual servers are called EC2 instances and come prepackaged with different options for CPU, RAM, storage, network throughput, and more.

For more information on EC2, see What is Cloud Computing.

2.3 AWS Elastic Load Balancing (ELB)

AWS Elastic Load Balancing (ELB) distributes incoming application traffic across multiple EC2 instances and serves as a public entry point into your AWS environment. ELB uses Amazon CloudWatch and Auto Scaling to ensure that applications running in AWS can meet increased demand per the rules you define. Auto Scaling helps you ensure that you have the correct number of EC2 instances available to handle load for your application. You create collections of EC2 instances, called Auto Scaling groups, and these groups scale up and down automatically according to the metrics you define, e.g., CPU load, storage, network traffic, etc. You can create a scaling policy that uses Amazon CloudWatch alarms to determine when your Auto Scaling group should scale up or scale down. Each CloudWatch alarm watches a single metric and sends messages to Auto Scaling when the metric breaches a threshold that you specify. Sophos UTM works with ELB, Auto Scaling, and CloudWatch to ensure that your security scales alongside your application. As new EC2 instances are spun up, Sophos UTM deploys copies of itself called UTM Workers that safeguard these new EC2 instances and automatically terminate when they are no longer needed.

For more information on Auto Scaling, see What is Auto Scaling.

2.4 Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (S3) is a storage service that allows you to store data into S3 buckets. S3 buckets can be used for public or private access alone or together with other AWS services. Sophos UTM on AWS uses S3 to store logs, system images, and configuration changes for all UTMs in your AWS environment. Using Amazon Simple Notification Service (SNS), you can upload UTM configuration changes to S3, which then sends SNS push notification to all subscribing UTMs. The UTMs then pull down new configuration changes to ensure your rules or changes are deployed in your AWS environment.

For more information, see What is Amazon S3 and What is Amazon Simple Notification Service.

2.5 AWS Virtual Private Cloud (VPC)

AWS Virtual Private Cloud (VPC) enables you to launch EC2 instances and other resources into a virtual network that you define. This virtual network closely resembles a traditional network in a data center. Within your VPC, you can define IP address ranges, subnets, route tables, and gateways. VPC also allows you to configure security rules called Network Access Control Lists (NACLs) that act as firewall rules for controlling traffic in and out of one or more subnets. Similar to Security Groups, NACLs allow or deny traffic based on simple firewall rules but at the subnet layer rather than at the EC2 instance. Sophos UTM is designed to deploy into your VPC and work in conjunction with your NACLs.

2.6 Regions and Availability Zones (AZs)

AWS services are hosted in multiple, world-wide locations called Regions. Each Region contains multiple distinct locations called Availability Zones (AZs), which are engineered to be isolated from failures in other AZs. By launching services in separate AZs, you can protect your applications from the failure of a single location. Sophos UTM supports deployments within all supported AWS Regions and allows you to deploy across multiple AZs to ensure your security is also fault tolerant.

For more information, see Regions and Availability Zones.

2.7 AWS Marketplace

AWS Marketplace is an online store where you can find, buy, and quickly deploy software that runs on AWS. The software is available in the form of Amazon Machine Images (AMIs), which contain all the information necessary to boot an EC2 instance

with the UTM software. Sophos UTM on AWS can be found in the AWS Marketplace and is delivered as AMIs for easy deployment into AWS.

For more information on AWS Marketplace, see What is AWS Marketplace?.

2.8 AWS CloudFormation

AWS CloudFormation is a service that helps set up different AWS resources so that you do have to manually configure or enable those services. CloudFormation uses templates that describe all the AWS resources that are used, e.g., ELB, S3, SNS, etc., and CloudFormation takes care of provisioning and configuring those resources for you. Sophos UTM uses CloudFormation to help you deploy the solution in the most common configuration such as High Availability (HA), Auto Scaling, and Outbound Gateway (OGW). These templates can be found on the Sophos GitHub repository or from the AWS Marketplace (under *CloudFormation Template (View)*).

For more information, see What is AWS CloudFormation.

2.9 Amazon WorkSpaces

Amazon WorkSpaces is a Virtual Desktop Infrastructure (VDI) that allows customers to run remote desktops in AWS. Customers purchase WorkSpaces bundles that come predefined with capacity for CPU, storage, software applications, and Operating Systems (OS). Sophos UTM can protect WorkSpaces by acting as the default gateway for Internet browsing. This allows you to configure which websites and categories your end users can visit as well as setting browsing quotas to help keep costs under control.

For more information on Amazon WorkSpaces, see Amazon WorkSpaces FAQs.

2.10 AWS GovCloud

AWS GovCloud (US) is an isolated AWS region designed for customers that need to meet US government compliance requirements like the International Traffic in Arms Regulations (ITAR) and Federal Risk and Authorization Management Program (FedRAMP). Unlike the other AWS regions, GovCloud does not have an AWS Marketplace where customers can select ISV solutions like Sophos UTM. To support AWS customers who use GovCloud, Sophos publishes a UTM release specifically for GovCloud.

For information on how to deploy Sophos UTM in AWS GovCloud, see the Sophos Knowledgebase.

3 Sophos UTM on AWS Use Cases

Sophos UTM is an all-in-one solution that provides security tools like NextGen Firewall, Intrusion Prevention System (IPS), Web Application Firewall (WAF), Web Protection (content filtering), and Virtual Private Network (VPN) connection. Sophos UTM provides this protection by using multiple integrated security applications to scan both inbound and outbound traffic that identify malware, potential threats, and anomalies. This all in one security approach avoids the need for installing multiple security products to protect your environment, which helps save on costs and simplifies deployment.

Sophos UTM on AWS supports the following common use cases:

- NextGen Firewall for application level control
- IPS with deep packet inspection and automatic updates from SophosLabs
- VPN Gateway to securely connect remote users and locations
- Integrated WAF with reverse authentication and certificate management support
- Outbound security controls to protect connections from EC2 and WorkSpaces

Sophos UTM is built to provide advanced security without requiring expert level knowledge.

3.1 Sophos UTM and the AWS Shared Responsibility Model

Sophos UTM on AWS works with the Shared Security Model by providing you with tools that are integrated with AWS foundation services and control over your applications and content. For example, the Shared Responsibility Model for EC2 states that AWS will manage the security of the following assets:

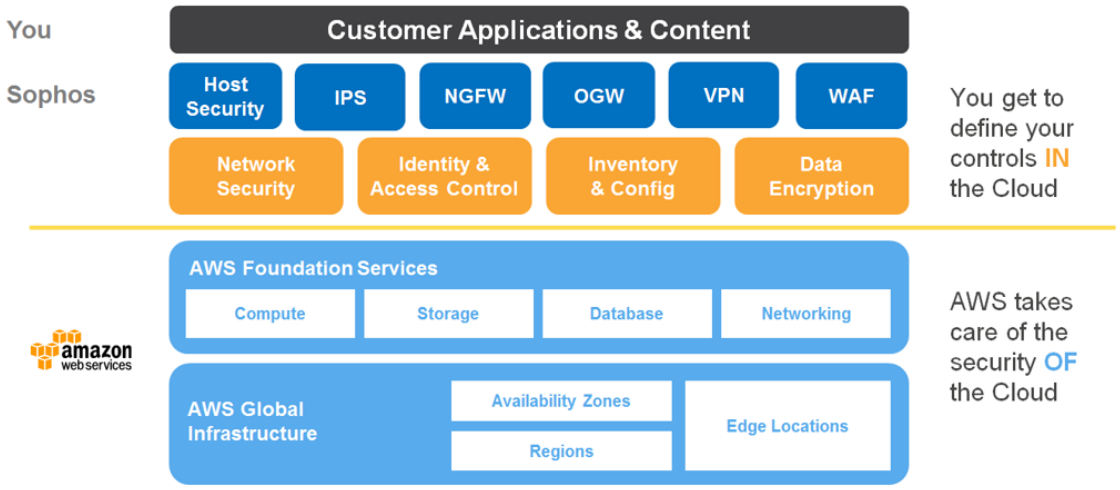
- Facilities
- Physical security of hardware
- Network infrastructure
- Virtualization infrastructure

You as the customer are responsible for protecting the following assets:

- AMIs
- OS
- Applications
- Data in transit
- Data at rest

- Data stores
- Credentials
- Policies and configuration

While AWS protects the data centers that host your applications, you can use Sophos protect applications, data, and access control. The following figure shows which areas you can use Sophos UTM for security in the cloud.



Shared Responsibility Model with Sophos UTM

Additionally Sophos has obtained the Amazon Partner Network (APN) Infrastructure Security Competency Program, which is designed to highlight solutions that have technical proficiency and proven customer success in security solutions.

For more information, see the AWS Security Best Practices whitepaper.

3.2 NextGen Firewall

In addition to creating IP and port based rules for your infrastructure, Sophos UTM provides tools that allow you to control which applications and protocols are allowed in your infrastructure. With the Network Protection module, customers can create rules that augment Security Groups and NACLs by blocking specific countries, only allowing certain applications to run, validating packet length, discarding invalid packets, preventing network broadcasts, tracking connections, and masquerading internal assets.

For information on configuring Sophos UTM, see the Sophos UTM Administration Guides.

3.3 Intrusion Prevention System (IPS)

The Intrusion Prevention System (IPS) analyzes every packet destined for VPC subnets listed in Sophos UTM. Based on over 18,000 definitions, Sophos UTM can protect your applications by either silently dropping or terminating connections to your AWS

infrastructure. Every packet can be evaluated against signatures that are updated automatically on a continuous basis by SophosLabs which analyzes data in real time. Users can also set thresholds for packets per second to prevent Distributed Denial of Service (DDoS) attacks like TCP floods, UDP floods, and ICMP floods.

For information on configuring Sophos UTM IPS, see the Sophos UTM Administration Guides.

3.4 Virtual Private Connection (VPN)

Within your VPC, you can use Sophos UTM to create VPN connections that support connections to VPC from your own data center or in between VPCs that span Regions. Because AWS does not provide cross-region VPC connectivity solution, customers can achieve this by using Sophos UTM which can import and use your AWS access keys.

For information on creating VPN connections for AWS, see Site-to-Site VPN configurations for Amazon VPC.

3.5 Web Application Firewall (WAF)

Sophos UTM WAF can secure your web applications against common attacks patterns including SQL injection, cross-site scripting and directory traversal. Because Sophos UTM is integrated with Auto Scaling, WAF can automatically scale up to inspect all HTTP/S requests during peak traffic times. The Webserver Protection module also scans all inbound files and content with dual antivirus agents to prevent infected files from entering your AWS environment. Additionally you can enable Reverse Proxy Authentication to authenticate end users to your web applications hosted in AWS and create or store X.509 certificates on UTM.

For information on deploying Sophos UTM WAF in AWS, see the Sophos Knowledgebase.

3.6 Outbound Gateway (OGW)

Outbound Gateway (OGW) is an additional feature within Sophos UTM that acts as an outbound load balancer. OGW serves two main purposes, first to scale Sophos UTMs to handle increasing outbound traffic loads and second to establish Internet routes for EC2 instances that are located within VPCs without Internet gateways. Typical use cases for the OGW include Virtual Desktop Infrastructure (VDI) access to the Internet (e.g. Amazon WorkSpaces) and Server instance access to the Internet (including web access).

For information on deploying OGW, see the Sophos UTM on AWS Quick Start Guide.

4 Sophos UTM Listings in AWS Marketplace

As of this writing, there are five AMIs for Sophos UTM in AWS Marketplace. Each AMI supports different pricing and deployment models depending on your cause. This section reviews each AMI in order to assist you in selecting the right option.

4.1 Sophos UTM 9 (PAYG)

Sophos UTM 9 (PAYG) runs on a single EC2 instance with support for Pay As You Go (PAYG) pricing. PAYG allows you to deploy Sophos UTM without any software licenses. You pay an hourly usage fee based on the pricing listed on AWS Marketplace. PAYG is managed directly through AWS who charges your usage to your AWS monthly statement. Additionally, PAYG comes preconfigured with Essential Firewall, Network Protection, Web Protection, and Web Server Protection modules enabled.

For more information on the different Sophos UTM modules, see the Sophos UTM Overview.

An optional deployment method for Sophos UTM 9 (PAYG) is High Availability (HA), which uses two EC2 instances for failover. This deployment model is detailed in chapter Stand Alone with HA (Cold and Warm Standby).

4.2 Sophos UTM 9 (BYOL)

Sophos UTM 9 (BYOL) also runs on a single EC2 instance but supports Bring Your Own License (BYOL) pricing. BYOL allows you to deploy Sophos UTM with a pre-purchased software license where you have more flexibility over which UTM modules to use to avoid hourly usage fees except for the EC2 instance. BYOL is managed via Sophos partners and provides a way to reduce your Total Cost of Ownership (TCO) by locking in prices for one, two, or three years subscriptions.

To inquire about purchasing BYOL for Sophos UTM on AWS, please email aws.-marketplace@sophos.com.

Just like Sophos UTM 9 (PAYG), an optional deployment method for Sophos UTM 9 (BYOL) is High Availability (HA), which is detailed in chapter Stand Alone with HA (Cold and Warm Standby).

4.3 Sophos UTM 9 (Auto Scaling PAYG)

Sophos UTM 9 (Auto Scaling PAYG) runs on three EC2 instances: one UTM Controller and two UTM Workers (sometimes referred to as Queen and Swarm). This deployment

model is used to support Auto Scaling for both inbound and outbound connections. You use the UTM Controller to configure your security rules while the UTM Workers enforce those rules and scale up during times of higher traffic. This deployment model is covered more in chapter Auto Scaling.

Again, with PAYG you can use Sophos UTM without any software licenses fees and pay an hourly fee to AWS based on AWS Marketplace prices. The solution comes pre-configured with Essential Firewall, Network Protection, Web Protection, and Web Server Protection modules enabled.

4.4 Sophos UTM 9 (Auto Scaling BYOL)

Sophos UTM 9 (Auto Scaling BYOL) also supports Auto Scaling for inbound and outbound connections but uses BYOL pricing. Just like the PAYG, the solution deploys three UTMs (one UTM Controller and two UTM Workers) but allows you to pre-purchase software licenses with flexibility over UTM modules and prices for yearly subscriptions. This deployment model is covered more in chapter Auto Scaling. To inquire about purchasing BYOL for Sophos UTM on AWS, please email aws.marketplace@sophos.com.

4.5 Sophos UTM Manager 4 (SUM)

Sophos UTM Manager (SUM) centrally manages multiple UTMs in AWS. SUM allows you to deploy firewall rules, WAF policies, and other configuration changes across multiple UTMs in AWS. This solution is provided free of charge except for the EC2 hourly costs for hosting the software.

Note – SUM is intended to be used with Sophos UTM 9 Stand Alone systems.

4.6 EC2 Guidelines

When deploying Sophos UTM on AWS, you can select from a list of supported EC2 instances. At the time of this writing, Sophos UTM 9 supports a total of 18 EC2 instances that generally align with the hardware equivalents of Sophos UTM. However, please be aware that selecting the right EC2 instance type for your AWS environment is dependent on a number of factors and may involve performing your benchmarking tests.

For more information, see How do I benchmark network throughput on an Amazon EC2 Linux instance.

This section provides performance numbers for common use cases that you can use as a guideline for choosing the right EC2 instance for Sophos UTM on AWS. Because AWS does specify exact network throughput numbers for EC2 instances but rather lists thresholds of “Low, Moderate, and High” these results may vary depending upon

external factors (e.g. region, time of day, network utilization, hardware specifications, etc.).

For more information, see the Instance Type Matrix.

Note – These performance results should not be compared to performance tests for Sophos UTM hardware appliances as these tests are done in a controlled lab with exact testing tools.

Note – These performance results are for VPN and IPS use cases. Performance numbers for WAF and OGW use cases will be published at a later date.

Instance	vCPU	Networking Performance	Direct Throughput (Mbps)	VPN Throughput	VPN CPU Load	IPS Throughput	IPS CPU Load
t2.small	1	Low to moderate	130	126	4%	123	50%
m3.medium	1	Moderate	300	294	4%	298	70%
m4.large	2	Moderate	449	440	3%	445	30%
m4.xlarge	4	High	744	740	3%	746	30%
c4.2xlarge	8	High	2,480	2,010	3%	1,800	30%
c4.4xlarge	16	High	2,480	2,010	3%	1,800	15%
c4.8xlarge	36	10 Gbps	9,570	2,010	2%	1,800	6%

For supported EC2 instance types not listed in the table, you can assume similar performance based on comparable CPU and Networking Performance.

5 Deployment Models

Sophos UTM on AWS supports three deployment models that include:

- Stand Alone (no redundancy)
- Stand Alone with HA (cold and warm standby)
- Auto Scaling for inbound and outbound traffic

5.1 Stand Alone

In this model, UTM is deployed on an EC2 instance into a single Availability Zone (AZ). Typically customers configure all traffic to route in and out of UTM as the perimeter gateway their Virtual Private Cloud (VPC). Sophos does not recommend this deployment model.

5.2 Stand Alone with HA (Cold and Warm Standby)

In this model, UTM is deployed on a primary EC2 instance in a single Availability Zone (AZ) with a secondary EC2 instance in a different AZ. Using AWS CloudFormation, Amazon Simple Storage Service (S3), and Health Checks for Auto Scaling instances, UTM leverages AWS services to determine the status of the primary EC2 instance. If the primary EC2 instance fails a health check, the Auto Scaling group transfers the Elastic IP Address and all configuration settings stored in S3 over to the secondary EC2 instance in a different AZ. You can select between cold standby (secondary EC2 instance has not been started) and warm standby (secondary EC2 instance is running in parallel with the primary EC2 instance but not actively inspecting traffic).

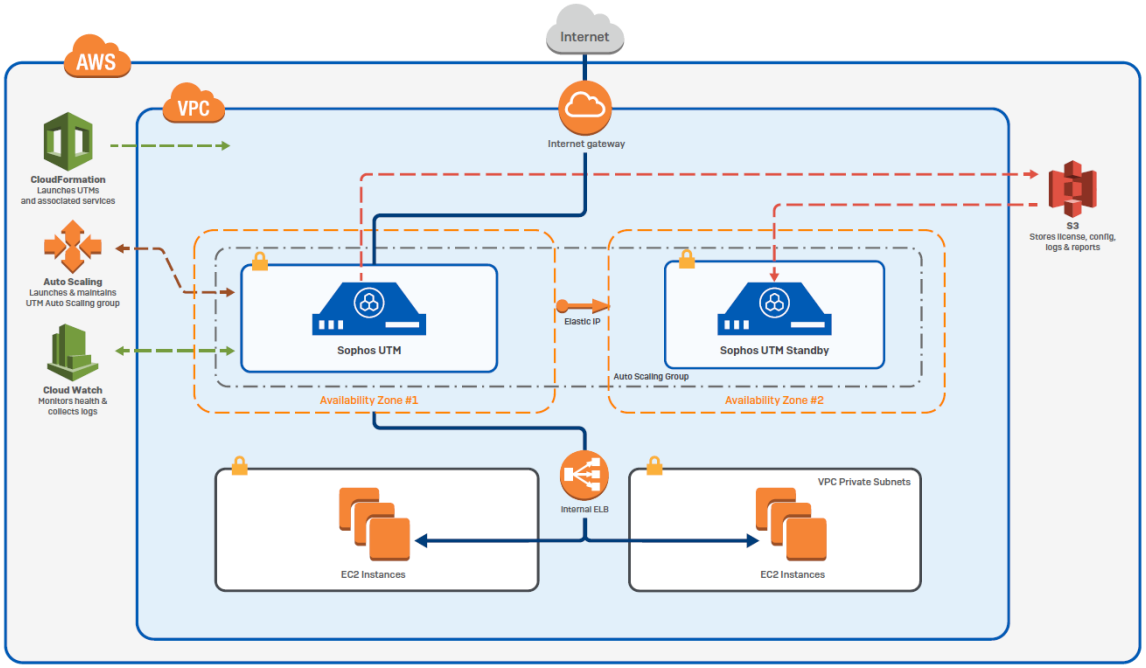


Figure 2 Stand Alone with HA

5.3 Auto Scaling

In this model, UTM is deployed via three EC2 instances: one UTM controller and two UTM workers (sometimes referred to as Queen and Swarm) that will scale depending on your traffic. The UTM controller resides in an Auto Scaling group and stores configuration details, logs, and reports to an S3 bucket. The UTM controller uses the S3 bucket to restore configuration in the event that the EC2 instance is terminated and also provides configuration details to UTM workers. The UTM workers reside in another Auto Scaling group, typically behind an external Elastic Load Balancing (ELB) Classic Load Balancer, and inspect all inbound traffic. The UTM workers pull down UTM configuration settings from S3 upon boot, if they receive a configuration change notification via the Amazon Simple Notification Service (SNS), or when they scale out depending on the traffic.

Auto Scaling UTM also offers an additional layer of security called Outbound Gateway (OGW) which allows customers to inspect and scale security based on outbound connections. OGW works by deploying gateway instances in VPC subnets (both local and remote) that forward all traffic to UTM workers via Generic Routing Encapsulation (GRE) tunnels. After inspecting the traffic, the UTM workers forward the traffic outside VPC or deny the request per the rules you configure.

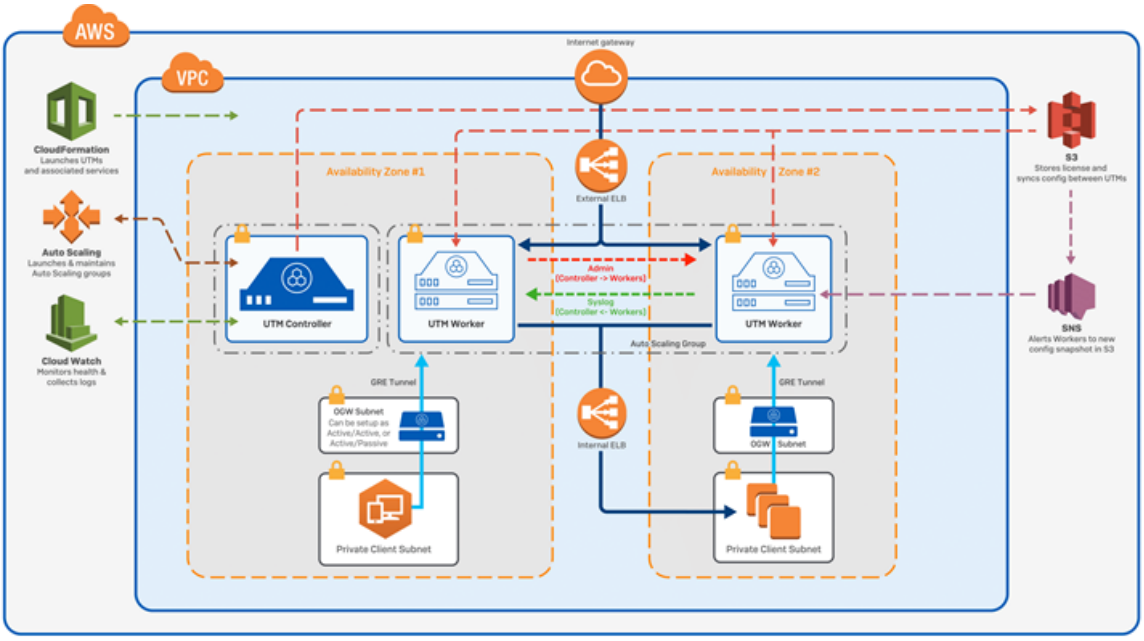


Figure 3 Auto Scaling

6 Delivery Methods

UTM supports three delivery methods:

- Single AMI
- CloudFormation Console
- Manual Launch (EC2 Console, API, or CLI)

This section summarizes the Single AMI and CloudFormation Console delivery methods. For instructions on each method, see the Sophos UTM on AWS Quick Start Guide.

6.1 Single AMI

Single AMI supports 1-Click Launch which allows you to install the Stand Alone UTM on a single EC2 and specify settings like EC2 instance type, AMI version (we recommend the latest), VPC settings, Security Groups, and Key Pair.

6.2 CloudFormation Console (Stand Alone)

The CloudFormation Console for Stand Alone allows you to install Sophos UTM on a single EC2 instance but uses a template that provides options not available in the 1-Click Launch. These options allow you to define the Elastic IP address, trusted Classless Inter-Domain Routing (CIDR) networks, and Identity and Access Management (IAM) roles.

6.3 CloudFormation Console (Auto Scaling)

The CloudFormation Console for Auto Scaling allows you to install Sophos UTM in the Auto Scaling deployment model. The template integrates the Sophos UTM deployment with ELB, CloudWatch, and Auto Scaling to support inspecting inbound and outbound connections.

The following table lists each Sophos UTM product in the AWS Marketplace with the supported delivery methods and deployment models.

Product Name	Delivery Methods	Deployment Models Supported
Sophos UTM 9 (PAYG)	Single AMI CloudFormation Console	Stand Alone UTM Stand Alone UTM with HA (cold and warm standby)

Product Name	Delivery Methods	Deployment Models Supported
Sophos UTM 9 (BYOL)	Single AMI CloudFormation Console	Stand Alone UTM Stand Alone UTM with HA (cold and warm standby)
Sophos UTM 9 (Auto Scaling PAYG)	CloudFormation Console	Auto Scaling UTM
Sophos UTM 9 (Auto Scaling BYOL)	CloudFormation Console	Auto Scaling UTM
Sophos UTM Manager 4 (SUM)	Single AMI	Stand Alone UTM

7 AWS Marketplace Product Support Connection

After you have subscribed to Sophos UTM on AWS, you are eligible to receive Sophos technical support. Sophos offers Premium support for all customers who select PAYG pricing. Premium support provides 24/7 technical support direct from Sophos support engineers. To receive this support, you'll need to register your product with the AWS Marketplace Product Support Connection (https://aws.amazon.com/marketplace/support-contacts).

In addition to the benefits of Premium, AWS customers can also purchase another level of supported called Enhanced Plus. This support tier is only available to customers who deploy Sophos UTM BYOL but gives priority case handling and VIP access to senior resources. For more information, please contact aws-marketplace@sophos.com.

8 Sophos AWS Information

For further information on Sophos AWS, see:

- http://www.sophos.com/aws
- http://aws.amazon.com

Glossary

A

Amazon WorkSpaces

Desktop computing service on the AWS cloud. Allows to provision cloud-based virtual desktops.

AMI

Amazon Machine Image

API

Application Programming Interface

APN

AWS Partner Network

Auto Scaling

Web service to launch or terminate Amazon EC2 instances automatically based on policies, schedules and health checks.

Availability Zones

Each Amazon data center location is called a region, each region contains multiple distinct locations called Availability Zones, or AZs.

AWS

Amazon Web Services

AWS CloudFormation

Free service for AWS customers which provides tools needed to create and manage the infrastructure a particular software application requires to run on AWS.

AWS Partner Network

Global partner program for Amazon Web Services, which is focused on helping partners build a successful AWS-based business.

AZ

Availability Zone

B

BYOL

Bring Your Own License

C

CIDR

Classless Inter-Domain Routing

Classless Inter-Domain Routing

Set of IP standards to create unique identifiers for networks and individual devices.

CLI

Command Line Interface

CloudFormation Console

User interface of the CloudFormation service.

CloudWatch

A component of Amazon Web Services which provides monitoring of AWS resources and applications running on the Amazon infrastructure.

E

EBS

Elastic Block Store

EC2

Elastic Compute Cloud

EC2 Instance

Compute instance in Amazon EC2 service.

EIP

Elastic IP

Elastic Compute Cloud

Amazon EC2 provides scalable computing capacity in AWS which allows users to rent virtual computers to run their own computer applications.

Elastic IP

Static IP addresses for dynamic cloud computing, which is associated with an account. You control the address until you explicitly release it.

Elastic Load Balancing

Load balancing solution which automatically scales incoming application traffic across multiple targets.

ELB

Elastic Load Balancing

G

Generic Routing Encapsulation

Tunneling protocol which provides a private, secure path for transporting packets through an otherwise public network.

GRE

Generic Routing Encapsulation

H

HA

High Availability

High Availability

System design protocol that ensures a certain absolute degree of operational continuity.

I

IAM

AWS Identity and Access Management

Identity and Access Management

Amazon web service to control who can use your AWS resources and in which way.

Intrusion Prevention System

Network security and threat prevention technology that examines network traffic flows to detect and prevent vulnerability.

N

Network Access Control List

Security layer which acts as firewall to control traffic in and out of subnets.

O

OGW

Outbound Gateway

P

PAYG

Pay As You Go

S

S3

Simple Storage Solution

S3 bucket

Logical unit which stores objects that consist of data and metadata which describe the data.

Security Group

Acts as virtual firewall for an AWS instance to control inbound and outbound traffic.

Simple Notification Service

Notification service which provides mass delivery of messages, predominantly to mobile users.

Simple Storage Service

Amazon web service which provides storage through web services interfaces.

SNS

Simple Notification Service

SSH

Secure Shell

V

Virtual Private Cloud

VPC provides secure data transfer between private enterprises and public cloud provider. Each data remains isolated from every other data both in transit and inside the cloud provider's network.

Virtual Private Network

Private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol such as PPTP or IPsec.

VPC

Virtual Private Cloud

W

WAF

Web Application Firewall

Web Application Firewall

WAF, also known as reverse proxy, applies a set of rules to an HTTP conversation and therefore protects webservers from attacks and malicious behavior like cross-site scripting (XSS), SQL injection, and others.