Sophos Outbound Web Proxy on the AWS Cloud

Quick Start Reference Deployment

Sophos IaaS team
Cameron Worrell, Alex Tomic, Nick Matthews, and Tony Vattathil — AWS

October 2017
# Contents

About This Guide .................................................................................................................................................. 3
Quick Links .......................................................................................................................................................... 3
Overview ............................................................................................................................................................ 4
Sophos Outbound Proxy on AWS .......................................................................................................................... 4
Cost and Licenses .................................................................................................................................................. 4
AWS Services ....................................................................................................................................................... 5
Sophos Component Definitions ............................................................................................................................ 6
Architecture ......................................................................................................................................................... 6
Outbound Proxy Solution Considerations .............................................................................................................. 9
Best Practices ....................................................................................................................................................... 9
Prerequisites ......................................................................................................................................................... 10
Deployment Steps ................................................................................................................................................. 10
  Step 1. Prepare Your AWS Account .................................................................................................................. 11
  Step 2. Accept Software Terms for the Sophos UTM AMI .............................................................................. 14
  Step 3. Launch the Sophos UTM Stack ............................................................................................................ 15
  Step 4. Configure Sophos UTM ....................................................................................................................... 19
  Step 5. Test Outbound Web Filtering Functionality ......................................................................................... 25
  Step 6. (Optional) Configure URL Whitelist .................................................................................................. 26
Troubleshooting .................................................................................................................................................. 29
Additional Sophos Web Filtering Options ............................................................................................................ 30
  Web Filtering Modes ......................................................................................................................................... 30
  Transparent Mode Skiplist ............................................................................................................................... 31
  Whitelisting AWS Endpoints ........................................................................................................................... 31
  AWS IP Address Ranges ............................................................................................................................... 31
Security ................................................................................................................................................................. 31
Additional Resources .......................................................................................................................................... 32
GitHub Repository ............................................................................................................................................... 33
Document Revisions ......................................................................................................................................... 33
This Quick Start deployment guide was created by Sophos, Ltd. in collaboration with Amazon Web Services (AWS).

**Quick Starts** are automated reference deployments that use AWS CloudFormation templates to deploy key technologies in the AWS Cloud, following AWS best practices.

**About This Guide**

This Quick Start deployment guide describes how to deploy a Sophos outbound proxy solution on the AWS Cloud, using [AWS CloudFormation](https://aws.amazon.com/cloudformation/) templates that automate the deployment.

This guide is for IT infrastructure architects, administrators, and DevOps professionals who are planning to provide a transparent outbound web proxy on the AWS Cloud. The outbound proxy use case highlighted in this guide is to whitelist AWS API calls without allowing internet access. You can also use this example to enable other proxy use cases with Sophos Unified Threat Management (UTM).

**Quick Links**

The links in this section are for your convenience. Before you launch the Quick Start, please review the architecture, configuration, network security, and other considerations discussed in this guide.

- If you have an AWS account, and you’re already familiar with AWS services and Sophos UTM, you can [launch the Quick Start](https://aws.amazon.com/cloudformation/) to build the architecture shown in Figure 2 in a new virtual private cloud (VPC). The deployment takes approximately 20 minutes. If you’re new to AWS or to Sophos UTM, please review the implementation details and follow the [step-by-step instructions](https://aws.amazon.com/cloudformation/) provided later in this guide.

- If you want to take a look under the covers, you can view the AWS CloudFormation templates that automate the deployment by viewing the [GitHub repository](https://github.com/awslabs/aws-quick-start-sophos-outbound-proxy) for this Quick Start.
Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying a Sophos outbound web filtering proxy on the AWS Cloud. The solution uses the Sophos UTM virtual appliance to provide a transparent outbound proxy for Amazon Elastic Compute Cloud (Amazon EC2) instances deployed in a VPC. In addition, it uses a Sophos feature called Outbound Gateway to extend the security of the solution to multiple VPCs.

EC2 instances often require access to external resources such as software repositories and web services. Many organizations require restricting internet connections to authorized websites. Web filtering proxies are commonly used to enforce web policies for internet access.

This Quick Start uses the Sophos UTM virtual appliance, which is available in AWS Marketplace. Alternative web proxy solutions may use open-source solutions such as Squid or Apache Traffic Server, but aren’t covered in this document.

This Quick Start uses CloudFormation templates to deploy two new VPCs for proxy and client functionality. You may wish to modify the CloudFormation templates for your specific needs or split them into modular building blocks for more extensive architectures.

Sophos Outbound Proxy on AWS

Sophos UTM provides multiple security functions, including firewall, intrusion prevention (IPS), VPN, and web filtering. Sophos Outbound Gateway provides a distributed, fault-tolerant architecture to provide visibility, policy enforcement, and elastic scalability to outbound web traffic.

This guide provides configuration and guidance for one use case: allowing AWS API calls from a VPC. It doesn’t cover general installation and software configuration tasks for Sophos UTM. For general guidance and best practices, consult the Sophos UTM Administration Guide.

Cost and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start. You can use the Simple Monthly Calculator to view typical costs for default template settings and adjust the configuration based on your deployment. Additional cost for licensing will vary based on the consumption model (BYOL or hourly) as well as instance sizes.
Prices are subject to change. See the pricing pages for each AWS service you will be using in this Quick Start for full details.

This deployment supports both the Bring Your Own License (BYOL) model and the hourly model for the Sophos UTM software. If you already have a license for the Sophos UTM, you can select the BYOL option and upload your license file after deployment.

This Quick Start launches Amazon Machine Images (AMIs) for the Sophos UTM Controller and Worker instances as well as the bastion host and Linux testing instances, which enable you to test and familiarize yourself with the solution.

**AWS Services**

The core AWS components used by this Quick Start include the following services. (If you are new to AWS, see [Getting Started](#) on the AWS website.)

- **Amazon VPC** – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

- **Amazon EC2** – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing AMIs or import your own virtual machine images.

- **Amazon EBS** – Amazon Elastic Block Store (Amazon EBS) provides persistent block-level storage volumes for use with EC2 instances in the AWS Cloud. Each EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. EBS volumes provide the consistent and low-latency performance needed to run your workloads.

- **AWS CloudFormation** – AWS CloudFormation gives you an easy way to create and manage a collection of related AWS resources, and provision and update them in an orderly and predictable way. You use a template to describe all the AWS resources (e.g., EC2 instances) that you want. You don’t have to create and configure the resources or figure out dependencies; AWS CloudFormation handles all of that.

- **Auto Scaling** – Auto Scaling helps maintain high availability and manage capacity by automatically increasing or decreasing the EC2 instance fleet. You can use Auto Scaling to run your fleet at optimal utilization by increasing instance capacity during demand spikes and decreasing capacity during down times.
Sophos Component Definitions

This Quick Start uses the following Sophos software.

- **Sophos UTM 9 virtual appliance** – Sophos UTM is a security platform that helps you secure your infrastructure in AWS. Sophos UTM provides multiple security tools like Next-Gen Firewall (NGFW), Web Application Firewall (WAF), Intrusion Prevention System (IPS), and Advanced Threat Protection (ATP).

- **Sophos UTM Queen (Controller)** – The Queen Controller is an UTM instance that provides administrative control and configuration management for UTM Workers.

- **Sophos UTM Workers** – The UTM Workers terminate the Generic Routing Encapsulation (GRE) tunnels from the Outbound Gateways and proxy the traffic to the destination based on the policy configured within the Controller.

- **Sophos Outbound Gateway (OGW) for AWS** – The OGW is an instance that resides within an Availability Zone where clients need to connect out through the proxy.

Architecture

Deploying this Quick Start with **default parameters** builds the environment shown in Figures 1 and 2 in the AWS Cloud.

To understand how to centralize proxy functionality, let’s see how the Sophos Outbound Gateway uses GRE to tunnel outbound network traffic between VPCs.
Figure 1: Sophos outbound proxy on AWS – high-level traffic pattern
Here’s a detailed view of the architecture on AWS:

**Figure 2: Sophos outbound proxy on AWS architecture – detailed diagram**

The AWS CloudFormation template sets up the virtual network and creates the networking resources and EC2 instances needed for the Sophos outbound proxy solution.
The template deploys a highly available architecture that includes a Sophos UTM Queen Controller, Sophos UTM Workers, and Sophos Outbound Gateways for AWS. In total, the Quick Start deploys seven instances, including one Queen Controller, two Workers in an Auto Scaling group, two Outbound Gateways, one bastion host, and one client test EC2 instance. In order to centralize the proxy service for the clients, the Queen Controller and Workers are deployed into a dedicated proxy VPC. You can use this architecture in environments with many VPCs, which simplifies operations and reduces costs.

This Quick Start deploys one additional application VPC for the proxy clients. The Outbound Gateway for AWS is also deployed into the application VPC to support the connections from the clients. Finally, the bastion host and tester instances are deployed into the application VPC. You can use these instances to test and become familiar with the outbound web proxy functionality.

You can extend the Quick Start architecture to include your existing VPCs and clients by adding an Outbound Gateway in other VPCs. This process is covered in the Sophos UTM Administration Guide.

Outbound Proxy Solution Considerations
Although outbound proxy solutions are used widely, there are implications you should consider before you implement proxies in your architecture. The Sophos web filtering engine operates in transparent or standard mode. When deployed in transparent mode with URL whitelisting, your client applications will need to support the Server Name Indication (SNI) specification to access SSL/TLS endpoints. In standard mode, your client applications will need to be “proxy aware” and explicitly direct requests through the Sophos Outbound Gateway. Sophos provides additional options to control traffic such as the ability to bypass filtering by source or destination IP. To learn more about this and other considerations, see the Sophos UTM Administration Guide.

Best Practices
The architecture built by this Quick Start supports AWS best practices for high availability and security:

- The Queen Controller and Workers reside in individual Auto Scaling groups.
- The Workers are deployed across two Availability Zones.
- A separate Outbound Gateway is deployed for each Availability Zone in each VPC where proxy clients are based.
Prerequisites

Before you launch the Quick Start, you should take care of the following:

- Determine the licensing model you want to use for Sophos UTM. Available options are hourly and BYOL. If you’re using the BYOL option, you’ll need your license file. You can place the file in an Amazon Simple Storage Service (Amazon S3) bucket and specify it by using the **S3 Bucket Containing Licenses (optionalLicensePool)** parameter when you launch the Quick Start. You can also upload your license file after deployment, in the Sophos UTM application.

- Confirm that your AWS account limits allow for provisioning two VPCs and one Elastic IP address.

- Identify the CIDR ranges you want to use for the proxy and application VPC and subnets. The Quick Start provides default values as an option for testing purposes.

- In order to administer the Sophos UTM, you will need access to TCP port 4444 from your browser.

Deployment Steps

The procedure for deploying the Sophos UTM Outbound Proxy architecture on AWS consists of the following steps. For detailed instructions, follow the links for each step.

**Step 1. Prepare an AWS account**

Sign up for an AWS account, choosing a region, creating a key pair, and requesting increases for account limits, if necessary.

**Step 2. Accept software terms in AWS Marketplace**

Accept terms for the Sophos UTM AMIs in AWS MarketPlace.

**Step 3. Launch the stack**

Launch the AWS CloudFormation template into your AWS account, specify parameter values, and create the stack.

**Step 4. Configure the Sophos UTM**

Log in to the Sophos UTM Controller, define your networks and Outbound Gateway hosts, and set up web filtering.

**Step 5. Test outbound web filtering**

Connect to the bastion host and the internal Linux tester host to test the deployment.
Step 6. (Optional) Configure whitelist URLs

To prevent access to unauthorized sites, limit externally accessible websites to approved URLs.

Step 1. Prepare Your AWS Account

1. If you don’t already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy Sophos UTM on AWS (see the list of supported Regions).

   Regions are dispersed and located in separate geographic areas. Each Region includes at least two Availability Zones that are isolated from one another but connected through low-latency links. Deploying your cloud applications across multiple Availability Zones helps you achieve high availability, even in the face of natural disasters that might impact a single Availability Zone. For more information, see Regions and Availability Zones.

   ![Figure 3: Choosing an AWS Region](image)

Consider choosing a region closest to your data center or corporate network to reduce network latency between systems running on AWS and the systems and users on your corporate network.
This Quick Start currently supports the following AWS Regions:

- Asia Pacific (Tokyo)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- AWS GovCloud (US)
- EU (Frankfurt)
- EU (Ireland)
- South America (São Paulo)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

**Note** This Quick Start uses the C4 instance type for the Sophos UTM portion of the deployment. In AWS Regions where the C4 instance type is not available, it uses C3 or M4 instances instead.

3. Create a **key pair** in your preferred region. To do this, in the navigation pane of the Amazon EC2 console, choose **Key Pairs, Create Key Pair**, type a name, and then choose **Create**.
Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To log in to your instances, you must create a key pair. On Linux, the key pair is used to authenticate SSH login.

4. If necessary, request a service limit increase for the creation of additional VPCs or Elastic IP addresses. To do this, in the AWS Support Center, choose Create Case, Service Limit Increase, VPC or Elastic IPs, and then complete the fields in the limit increase form. The current default limit is 5 VPCs and 5 Elastic IP addresses per AWS Region.

You might need to request an increase if you already have existing deployments, and you think you might exceed the default VPC and Elastic IP address limits with this reference deployment. It might take a few days for the new service limit to become effective. For more information, see the Amazon EC2 User Guide.
Step 2. Accept Software Terms for the Sophos UTM AMI

This Quick Start uses AWS Marketplace software from Sophos and requires that you accept the terms within the AWS account where the Quick Start will be deployed.

1. Log in to the AWS account that you’re planning to use to deploy the Quick Start.

2. Open the AWS Marketplace page for the Sophos UTM 9 AMI:
   - For hourly licensing, open the page for the [Sophos UTM 9 (Auto Scaling PAYG)](https://aws.amazon.com/marketplace/solutions/012954593506021052) software.
   - For BYOL licensing, open the page for the [Sophos UTM 9 (Auto Scaling BYOL)](https://aws.amazon.com/marketplace/solutions/012954593506021053) software.

3. Choose **Continue**.

4. Choose **Manual Launch**, and then choose **Accept Software Terms**.
Figure 6: Accepting software terms in AWS Marketplace

5. Exit out of AWS Marketplace without further action. **Do not** provision the software from AWS Marketplace.

**Step 3. Launch the Sophos UTM Stack**

This automated AWS CloudFormation template deploys Sophos UTM into multiple Availability Zones in a VPC. Please make sure that you’ve completed the prerequisites before launching the stack.

1. **Launch the Quick Start** into your AWS account. The CloudFormation templates for this Quick Start are available on GitHub.

2. Check the AWS Region that’s displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for Sophos UTM will be built. The template is launched in the US West (Oregon) Region by default. (See the list of supported Regions earlier in this guide.)

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other

**Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.
parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose Next.

Parameters are grouped in six major categories and described in the following tables.

**Instance Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI ID (awsAMI)</td>
<td>autodetect</td>
<td>The AMI ID for the Sophos UTM software. By default, the Quick Start automatically detects the latest AMI based on the license type.</td>
</tr>
<tr>
<td>Pricing Option (awsLicenseType)</td>
<td>Hourly</td>
<td>License type (BYOL or hourly billing). This parameter has no effect if the AMI parameter is set to an AMI ID.</td>
</tr>
<tr>
<td>Instance Type of UTM Controller (utmControllerInstanceSize)</td>
<td>default for region</td>
<td>EC2 instance type for the Sophos UTM Controller. The default type is c4.large, if it's available in the deployment region. Otherwise, a similar instance type is used.</td>
</tr>
<tr>
<td>Instance Type of UTM Worker (utmWorkerInstanceSize)</td>
<td>default for region</td>
<td>EC2 instance type for the Sophos UTM Workers. The default type is c4.large, if it's available in the deployment region. Otherwise, a similar instance type is used.</td>
</tr>
<tr>
<td>Instance Type for Outbound Gateway (OGWInstanceSize)</td>
<td>default for region</td>
<td>EC2 instance type for the Outbound Gateway instances. The default type depends on the deployment region.</td>
</tr>
<tr>
<td>Authentication Token (AuthToken)</td>
<td>Requires input</td>
<td>Authentication token for API access. This token would be used as a shared secret for API communication between the Outbound Gateway and UTM instances. The token is an 8-64 character alphanumeric string. You'll use this token in step 4, when configuring Sophos UTM.</td>
</tr>
</tbody>
</table>

**Proxy Infrastructure Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TWO Availability Zones (AvailabilityZones)</td>
<td>Requires input</td>
<td>The Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.</td>
</tr>
<tr>
<td>Prefix for VPC CIDR Block (awsNetworkPrefix)</td>
<td>10.15</td>
<td>The /16 CIDR block to be used by the proxy VPC. Only the first two octets are required. For example, for the network 10.6.0.0/16, specify 10.6.</td>
</tr>
<tr>
<td>Trusted Network CIDR (awsTrustedNetwork)</td>
<td>Requires input</td>
<td>CIDR IP range that is permitted to access ports 22 and 4444; for example, 11.22.33.0/24. We recommend that you set this value to a trusted IP range. For example, you might want to grant only your corporate network access to the software.</td>
</tr>
<tr>
<td>Existing Elastic IP (optionalExistingElasticIP)</td>
<td>Optional</td>
<td>Elastic IP address to assign to the UTM instance. If you don't specify an IP value, a new Elastic IP address will be allocated automatically.</td>
</tr>
</tbody>
</table>
### Parameter label (name) | Default | Description
---|---|---
**S3 Bucket for UTM Synchronization and Backup** (optionalExistingS3Bucket) | Optional | S3 bucket for storing and restoring backups. If you don’t specify a bucket name, a new bucket will be created automatically.

**S3 Bucket Containing Licenses** (optionalLicensePool) | Optional | If you’re using the BYOL option, specify the S3 bucket that contains the license file. (This parameter is used only if there is at least one running UTM instance that’s already using this license.) If you have a BYOL license but you don’t specify the S3 bucket location, you can specify the license after deployment, using the Sophos UTM UI.

### Application VPC Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
**CIDR for Application VPC** (ApplicationVPCRange) | 10.100.0.0/16 | CIDR block for the application VPC. This VPC hosts your application servers and Sophos Outbound Gateway instances. |
**Public Subnet in AZ1** (ApplicationPublicSubnet1) | 10.100.1.0/24 | CIDR block for the public subnet located in the first Availability Zone. |
**Public Subnet in AZ2** (ApplicationPublicSubnet2) | 10.100.2.0/24 | CIDR block for the public subnet located in the second Availability Zone. |
**Private Subnet (Proxy client network 1) in AZ1** (ApplicationPrivateSubnet1) | 10.100.101.0/24 | CIDR block for the private subnet located in the first Availability Zone. |
**Private Subnet (Proxy client network 2) in AZ2** (ApplicationPrivateSubnet2) | 10.100.102.0/24 | CIDR block for the private subnet located in the second Availability Zone. |

### Settings for Initial UTM Setup:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
**Hostname** (basicHostname) | Requires input | Hostname for the Sophos UTM application. The hostname can only contain a maximum of 64 characters, including lowercase and uppercase letters, numbers, periods (.), and hyphens (-), and must begin with a letter or a number. |
**Admin E-Mail Address** (basicAdminEmail) | Requires input | Email address for administrative notifications from Sophos UTM. |
**Admin Password** (basicAdminPassword) | Requires input | Password for admin login to the UTM Controller. This must be an 8-64 character string that contains uppercase and lowercase letters, numbers, hyphens (-), underscores (_), and exclamation marks (!). |
**Organization** (basicOrganization) | Requires input | Your organization name, for SSL key generation. This must be a 1-64 character string that contains uppercase and lowercase...
<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>City (basicCity)</td>
<td>Requires input</td>
<td>Your city name, for SSL key generation. This must be a 1-64 character string that contains uppercase and lowercase letters, numbers, hyphens (-), and periods (.), and must begin with a letter or number.</td>
</tr>
<tr>
<td>Country (basicCountry)</td>
<td>Requires input</td>
<td>Your country name, for SSL key generation.</td>
</tr>
<tr>
<td>SSH Key (awsKeyName)</td>
<td>Requires input</td>
<td>Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.</td>
</tr>
</tbody>
</table>

**Debug Settings:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug Mode (debugMode)</td>
<td>off</td>
<td>Set to on to enable debug logging on the UTM instances. By default, debug logging is disabled.</td>
</tr>
</tbody>
</table>

**Other Parameters:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Start S3 Bucket Name (QSS3BucketName)</td>
<td>aws-quickstart</td>
<td>S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you’ve created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.</td>
</tr>
<tr>
<td>Quick Start S3 Key Prefix (QSS3KeyPrefix)</td>
<td>quickstart-sophos-outboundproxy/</td>
<td>The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.</td>
</tr>
</tbody>
</table>

5. On the Options page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you’re done, choose Next.

6. On the Review page, review and confirm the template settings. Under Capabilities, select the check box to acknowledge that the template will create AWS Identity and Access Management (IAM) resources.

7. Choose Create to deploy the stack.
8. Monitor the status of the stack. When the status is `CREATE_COMPLETE`, the Sophos UTM environment is ready. Note that provisioning process typically takes 20 minutes to complete.

9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

**Step 4. Configure Sophos UTM**

When the CloudFormation stack has been deployed successfully, you can log in to the Sophos UTM Controller to configure UTM.

1. In the AWS CloudFormation console **Outputs** tab, use the IP address specified in the **AdminURL** key to open `https://<ip_address>:4444`. Note that it could take a few minutes for the Controller to initiate the console. You should also confirm that TCP port 4444 is not being filtered from your client browser.

   **Note** The website uses a self-signed certificate, so your browser might display an exception warning. You’ll need to bypass this warning to proceed to the login.

2. In the login window, use **admin** as your user name, and enter the password you supplied in the **Admin Password** parameter in step 3.

   ![Figure 7: Sophos UTM login page](image)
3. If you selected the BYOL option for the Sophos UTM, choose Management, Licensing, Installation. Locate your license file and choose Start Upload. When your license has been uploaded, choose Apply.

**Note** We recommend that you complete this step even if you already specified the location of your license file during deployment, through the S3 Bucket Containing Licenses (optionalLicensePool) parameter.

![License settings in the Sophos UTM user interface](image)

**Figure 8: License settings in the Sophos UTM user interface**

4. Define the network where proxy clients are deployed. This will be a /24 IP block, but cannot overlap with the network where the OGW is deployed.

   a. The Quick Start provisions the tester host in the application VPC, in the private subnet of Availability Zone 1. In the CloudFormation stack Outputs tab, note the value of ProxyClients1.

   b. In the UTM console, choose Definitions & Users, Network Definitions, New Network Definition, and enter the value from (a) in the IPv4 address field, to define a network called Proxy-Clients-1.

**Note** If you did not use the default CIDR assignments in the application VPC, update the IPv4 address field to match your CIDR range.
c. Choose Save.

d. Repeat this process to create a second network definition named Proxy-Clients-2. For the IPv4 field, use the CIDR block for the private subnet in Availability Zone 2 of the application VPC. This value is listed in the CloudFormation stack Outputs tab as ProxyClients2.

5. Define the Outbound Gateway (OGW) host:

a. In the CloudFormation stack Outputs tab, locate the value of OGW1IP.

b. In the UTM console, choose Definitions and Users, Network Definitions, New Network Definition, and change the type to Host.

c. Add a network definition named OGW1. In the IPv4 address field, enter the IP address from (a) for OGW1IP, and then choose Save.
d. Repeat this process to create a second network definition named **OGW2** by using the **OGW2IP** value from the CloudFormation stack **Outputs** tab.

6. Add the Outbound Gateway for AWS:
   a. In the UTM console, select **AWS Management, Outbound Gateway, New Outbound Gateway**. Clear the **Resource Management** box.
   b. In the **Networks** section, choose the folder icon and select your network definition for **Proxy-Clients-1**. Note that you can drag and drop the network definitions into the configuration fields.
   c. Under **Advanced**, in the **Gateway** section, choose the folder icon and select your **OGW1** host definition.
   d. Enter the **Authentication Token** you configured in the template parameters.
   e. Choose **Save**.

![Figure 10: Creating a new host definition](image)

Image of creating a new host definition in the UTM console.
f. Repeat this process and create a second Outbound Gateway named OGW2 using the network definitions for Proxy-Clients-2 and OGW2.

7. Click the switch to enable the OGWs and confirm that the status changes to Up.

Note  You may need to refresh the console by using the refresh button in the top right for the status to update.
8. Enable web filtering protection. In the UTM console, select **Web Protection, Web Filtering**. Clear the **Resource Management** box. Select the **Web Filtering Status** button to move it to the enabled state.

9. Add the **Proxy-Clients-1** and **Proxy-Clients-2** network definitions to the **Allowed Networks** in the **Default Web Filter Profile**. Leave the default settings for the additional options, and then choose **Apply**.

---

**Figure 12: Enabling OGWs**

![Diagram showing OGWs configuration]

---
Step 5. Test Outbound Web Filtering Functionality

The Quick Start provisions a bastion host and an internal Linux tester host for testing purposes. In order to test the solution, you will need to first SSH to the bastion host, and then SSH from the bastion host to the tester host. Follow these steps:

1. Open an SSH session to the bastion host. You can get the IP of this instance from the **BastionHostIP** entry on the **Outputs** tab of the CloudFormation stack.

2. Configure your SSH key on the bastion host, and then SSH into the Linux test host from there. You can get the IP of this instance from the **TesterHostIP** entry in the **Outputs** tab of the CloudFormation stack.

3. Once you have connected to your internal host, use the **curl** command to access an external website; for example:

   ```
   $ curl https://aws.amazon.com
   ```

You have now completed the basic setup of the Sophos Outbound Proxy. For additional guidance and resources for Sophos UTM, see the [Sophos UTM Administration Guide](#).
Step 6. (Optional) Configure URL Whitelist

To prevent access to unauthorized sites, you may wish to limit externally accessible websites to approved URLs. In this example, we will only allow access from your proxy clients to the AWS API endpoints. This is a common use case where you may require access to external resources such as Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS), or Amazon Simple Storage Service (Amazon S3). Perform these steps from the tester host. In order to test the solution, you will need to first SSH to the bastion host, and then SSH from the bastion host to the tester host, as described in step 5.

1. In the UTM console, under Web Protection, choose Web Filter Profiles, and then choose the Filter Actions tab and edit the Default content filter block action.

![Figure 14: Editing the default content filter block action](image)

2. In the Websites tab, add the amazonaws.com domain to the Allow These Websites list. Select the Include subdomains option.
Choose **Save** in the **Edit whitelist/blacklist object** box, and then save the filter action.

3. In the UTM console, under **Web Protection**, choose **Web Filtering**, choose the **Policies** tab, and then assign the **Default content filter block action** to the **Filter action**.
Choose **Save** in the **Edit Filter Assignment** box, and then save the filter action.

4. Use the tester host to verify whitelist functionality. The IAM role associated with the tester host instance is configured to allow access to the [Landsat public dataset](https://landsat.usgs.gov) stored in Amazon S3. Use the following command to list the contents of the S3 bucket.

```
$ aws s3 ls s3://landsat-pds/c1/L8/203/001/LC08_L1GT_203001_20170608_20170608_01_RT/
```

Download one of the objects from this S3 location with the following command, replacing `<objectname>` with the file you want to download for testing purposes.

```
$ aws s3 cp s3://landsat-pds/c1/L8/203/001/LC08_L1GT_203001_20170608_20170608_01_RT/<objectname> ./
```

To confirm that sites that aren’t whitelisted cannot be accessed, you can test against additional sites.

```
$ curl https://aws.amazon.com
```

This command should not be successful because we didn’t include `aws.amazon.com` in the whitelist.
You have now completed the basic whitelisting setup of the Sophos Outbound Proxy. You can add any additional domains that require whitelisting by using the process above. For additional guidance and resources for Sophos UTM, see the Sophos UTM Administration Guide.

**Troubleshooting**

**Q.** I encountered a CREATE_FAILED error when I launched the Quick Start.

**A.** If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.)

**Important** When you set **Rollback on failure** to **No**, you’ll continue to incur AWS charges for this stack. Please make sure to delete the stack when you’ve finished troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

**Q.** I encountered an error message when I was configuring Sophos UTM.

**A.** If you run into a problem configuring Sophos UTM after the CloudFormation stack has successfully reached the CREATE_COMPLETE state, confirm that you’ve used the correct parameters from the stack outputs in the configuration steps. In the UTM console, under **AWS Management**, **Outbound Gateway** and **Web Protection**, **Web Filtering**, you can also choose **Open Live Log** to get more information about errors. The following table lists some typical configuration errors.

<table>
<thead>
<tr>
<th>Error message</th>
<th>Possible cause</th>
<th>What to do</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudFormation QueenScalingGroup creation fails with error “Received 0 SUCCESS signal(s) out of 1...”</td>
<td>You did not accept software terms.</td>
<td>Confirm that you’ve accepted the software terms in AWS Marketplace for the Sophos UTM AMI. Refer to step 2 for additional details.</td>
</tr>
<tr>
<td>Unable to connect to UTM Console on port 4444</td>
<td>TCP port 4444 is blocked.</td>
<td>Confirm that access to port 4444 isn’t blocked by a security device such as a firewall.</td>
</tr>
<tr>
<td>Tester Host not able to curl External URL with no whitelist</td>
<td>The UTM wasn’t configured properly.</td>
<td>Confirm that Outbound Gateway for AWS has the status “Up” and that all network definitions match AWS CloudFormation outputs. Confirm that web filtering is enabled with allowed networks for proxy clients.</td>
</tr>
<tr>
<td>Error message</td>
<td>Possible cause</td>
<td>What to do</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tester Host not able to curl</td>
<td>Whitelisted URLs aren’t configured properly.</td>
<td>Confirm that the base policy references Default content filter block action, and that allowed URLs are present in the block action Websites tab.</td>
</tr>
<tr>
<td>External URL with whitelist</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For additional information, see Troubleshooting AWS CloudFormation on the AWS website. If the problem you encounter isn’t covered on that page or in the table, please visit the AWS Support Center for AWS-specific issues or Sophos Support for UTM-related issues.

Q. I encountered a size limitation error when I deployed the AWS Cloudformation templates.

A. We recommend that you launch the Quick Start templates from the location we’ve provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Additional Sophos Web Filtering Options

Sophos UTM includes a range of options for web traffic filtering. For details, see the Sophos documentation.

Web Filtering Modes

- **Standard mode**: In standard mode, the web filter will listen for client requests on port 8080 by default and will allow any client from the networks listed in the Allowed Networks box to connect. When used in this mode, clients must have specified the web filter as an HTTP proxy in their browser configuration.

- **Transparent mode**: In transparent mode, all connections made by client browser applications on port 80 (and port 443 if SSL is used) are intercepted and redirected to the web filter without client-side configuration. The client is entirely unaware of the web filter server. The advantage of this mode is that no additional administration or client-side configuration is necessary for many installations. However, only HTTP requests can be processed. Therefore, when you select the transparent mode, the client’s proxy settings will become ineffective.
Transparent Mode Skiplist

In the UTM console, the transparent mode skiplist is under Web Protection, Filtering Options, Misc.

Using this option is meaningful only if the web filter runs in transparent mode. Hosts and networks listed in the Skip transparent mode hosts/nets boxes will not be subject to the transparent interception of HTTP traffic. There are separate boxes for source and destination hosts/networks. To allow HTTP traffic (without proxy) for these hosts and networks, select the Allow HTTP/S traffic for listed hosts/nets check box. If you do not select this check box, you must define specific firewall rules for the hosts and networks listed here.

Whitelisting AWS Endpoints

A common use case for the outbound proxy is to allow traffic only to AWS API endpoints. This allows proxy clients to communicate with AWS services that have public endpoints such as Amazon SNS and Amazon SQS, but will block requests to other sites.

AWS IP Address Ranges

AWS publishes its current IP address ranges in JSON format. This information can be useful when whitelisting AWS endpoints within the Sophos web filtering policy. To view the current ranges, download the JSON file. For more information, see AWS IP Address Ranges in the AWS documentation.

Security

Moving your IT infrastructure to AWS services creates a model of shared responsibility between you and AWS. This shared model can help reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. You assume responsibility and management of the guest operating system (including updates and security patches), other associated applications, and the configuration of the AWS-provided security group firewall.

You should carefully consider the services you choose as your responsibilities may vary depending on the services used, the integration of those services into your IT environment, and applicable laws and regulations. You can enhance security and meet your more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection/prevention, encryption, and key management. The nature of
this shared responsibility also provides the flexibility and customer control that permits the deployment of solutions that meet industry-specific certification requirements.

**Additional Resources**

**AWS services**

- Amazon EBS
- Amazon EC2
- AWS CloudFormation
  [https://aws.amazon.com/documentation/cloudformation/](https://aws.amazon.com/documentation/cloudformation/)
- Amazon VPC
  [https://aws.amazon.com/documentation/vpc/](https://aws.amazon.com/documentation/vpc/)
- AWS IP address ranges

**Sophos UTM documentation**

- Sophos UTM administration guide
- Sophos Knowledge Base
  [https://community.sophos.com/kb](https://community.sophos.com/kb)
- Sophos Technical Support

**Quick Start reference deployments**

- AWS Quick Start home page
  [https://aws.amazon.com/quickstart/](https://aws.amazon.com/quickstart/)
GitHub Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2017</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>

© 2017, Amazon Web Services, Inc. or its affiliates, and Sophos, Ltd. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.