Integration Guide: SonicOS and AWS

April 2019

This document describes how SonicOS is integrated with Amazon Web Services (AWS) VPC and CloudWatch. Such integration allows SonicOS to send logs to AWS CloudWatch and synchronize Address Objects and Groups that are mapped to EC2 Instances. It also allows SonicOS to connect to Virtual Private Clouds (VPCs) and communicate with AWS Application Programming Interfaces (APIs).

Topics:

About Amazon Virtual Private Cloud and CloudWatch

Amazon Virtual Private Cloud (Amazon VPC) provides a way to access AWS resources in a private virtual network that you define, created as an isolated section of the AWS Cloud. You can control your virtual networking environment, selecting your own IP address range, subnets, route tables and network gateways. Both IPv4 and IPv6 are available for use in your VPC. You can create both public facing and private facing subnets in your Amazon VPC. Security groups and network access control lists can control access to Amazon EC2 instances in each subnet.

Amazon CloudWatch service provides monitoring and management of your applications. CloudWatch collects log events, metrics, and other data that allows you to check system health and act on changes in performance or resource utilization including applications and services that run on AWS or other servers. You can set alarms, visualize logs and metrics, create automated actions, troubleshoot issues, and see how to optimize your applications.

Creating an AWS Identity

AWS Identity and Access Management (IAM) identities, creates, and manages Users and Groups from the IAM page in the AWS Management Console. Assuming that the AWS account is already created, and that an administrator with either root access or widespread privileges is logged into that account, it is necessary to create an IAM user, if one does not already exist. The firewall needs that user to access the various AWS APIs for the services that the firewall supports.

The user needs certain permissions to access the different services. These permissions can be granted directly to the user or included in a security access policy assigned to an IAM Group and then the user is added to that group.

The security policy used, either for a group to which the user belongs to or that is attached to the user directly, must include the following mandatory permissions:

- **AmazonEC2FullAccess** – For AWS Objects and AWS VPN
- **CloudWatchLogsFullAccess** – For AWS Logs

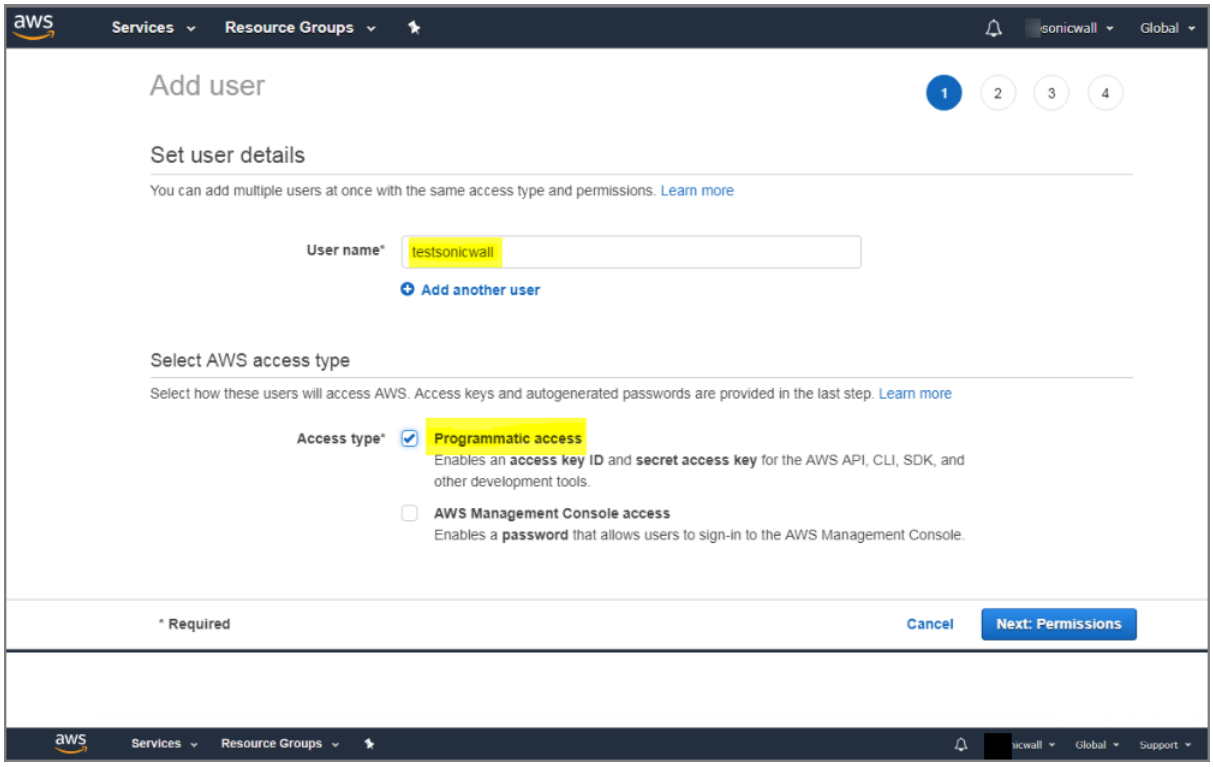
You can optionally include the below permissions:

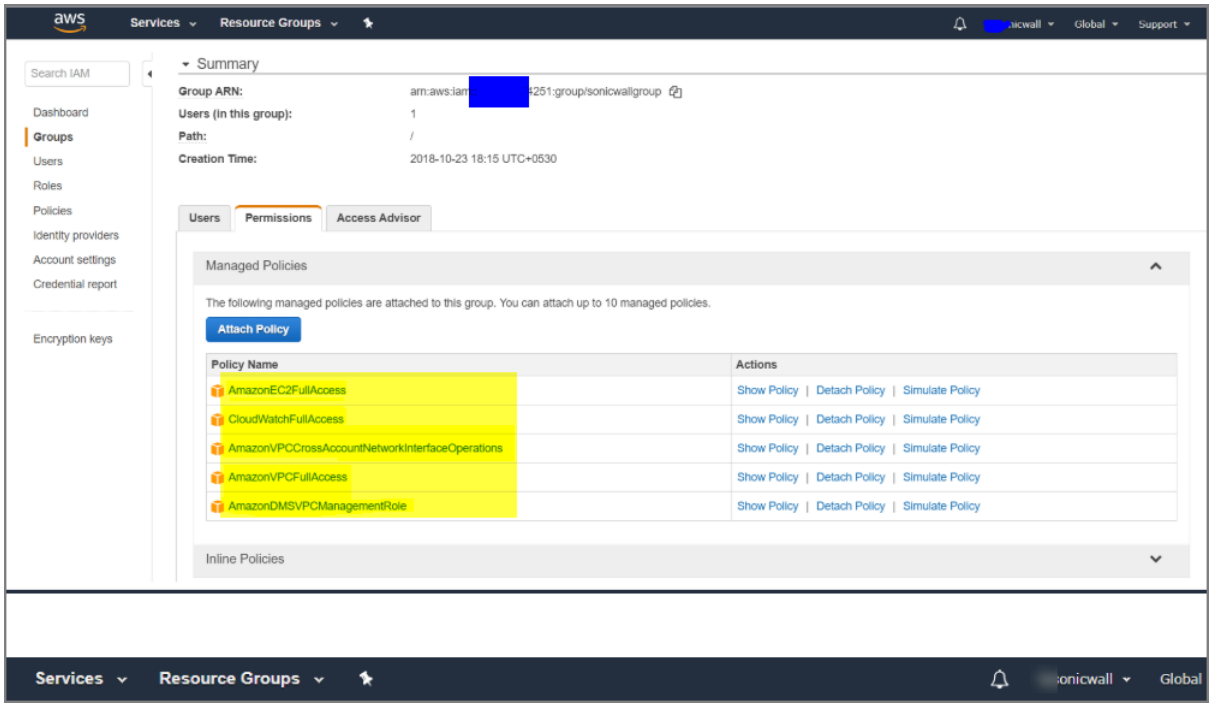
- **AmazonVPCCrossAccountNetworkInterfaceOperations**
- **AmazonVPCFullAccess**
- **AmazonDMSVPCManagementRole**

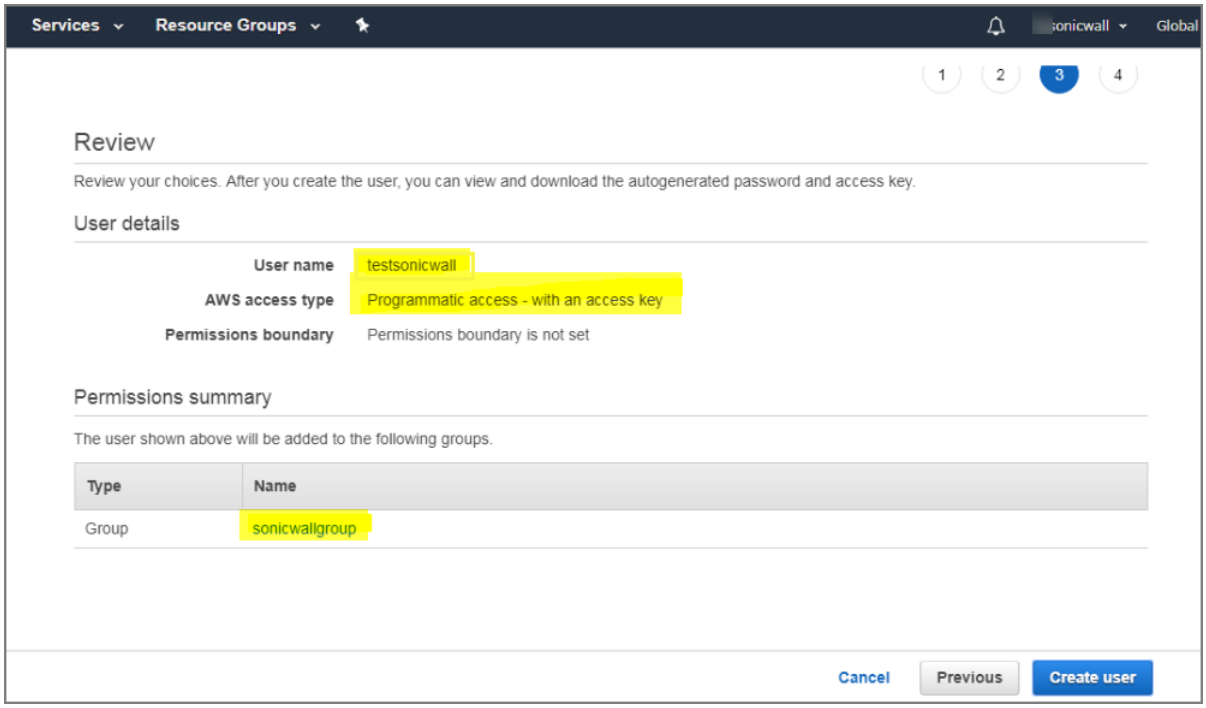
The IAM user can be created specifically to access the firewall. However, if the same user is going to access the AWS Management Console, the **Programmatic access** checkbox must be selected.

The second step of the **Add user** wizard determines which **Permissions** to assign the user. A user can be added to a group or permission managed policies can be attached to the user directly. After reviewing the user details, click **Create user** and view and download the auto-generated password and access key.

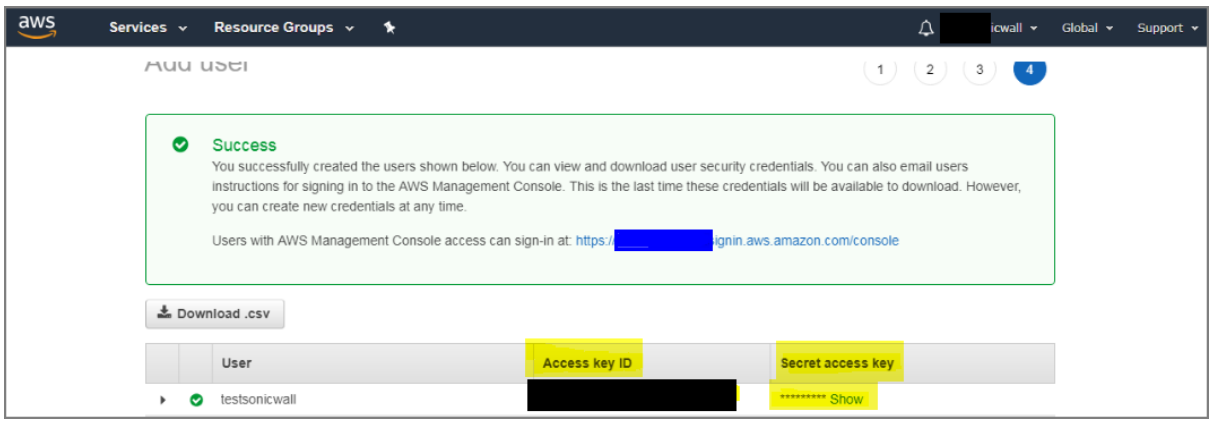
User Creation (IAM- AWS)




aws
Services
Resource Groups
Global
Support
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Summary
Group ARN:
arn:aws:iam
4251:group/sonicwallgroup
Users (In this group):
1
Path:
/
Creation Time:
2018-10-23 18:15 UTC+0530
Users
Permissions
Access Advisor
Managed Policies
The following managed policies are attached to this group. You can attach up to 10 managed policies.
Attach Policy
Policy Name
Actions
AmazonEC2FullAccess
CloudWatchFullAccess
AmazonVPCCrossAccountNetworkInterfaceOperations
AmazonVPCFullAccess
AmazonDMSVPCManagementRole
Show Policy | Detach Policy | Simulate Policy
Inline Policies


Services
Resource Groups
sonicwall
Global
1
2
3
4
Review
Review your choices. After you create the user, you can view and download the autogenerated password and access key.
User details
User name
testsonicwall
AWS access type
Programmatic access - with an access key
Permissions boundary
Permissions boundary is not set
Permissions summary
The user shown above will be added to the following groups.
Type
Name
Group
sonicwallgroup
Cancel
Previous
Create user

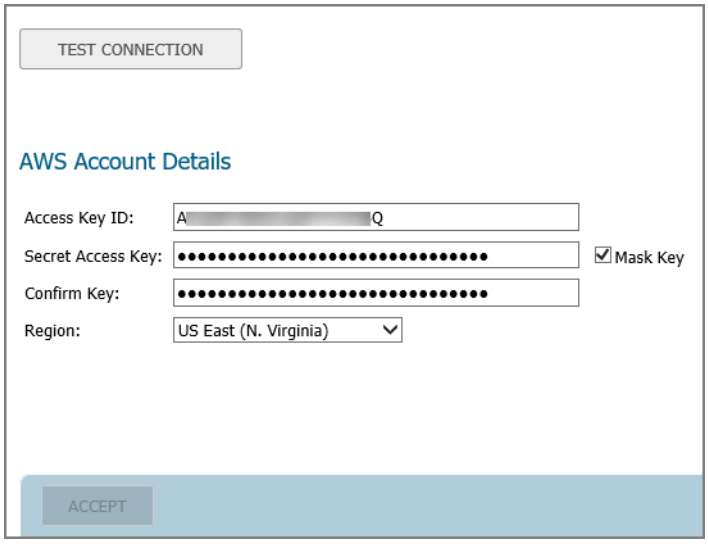
You must retrieve the user **Secret access key**. The secret access key and the **Access key ID** are used to configure the firewall. The keys are needed for all API access to AWS. Copy the key IDs to a safe location or download the CSV file with the key IDs and keep it in a secure location.



AWS Access Configuration in SonicOS

Navigate to **MANAGE | System Setup | Network > AWS Configuration** to configure SonicOS with the AWS security credentials.

The settings include an AWS AIM Access Key ID, the corresponding Secret Access Key and a default geographical region. The AWS Logs page uses the region for connection and for initialization of the AWS Objects and AWS VPN pages. You can select different regions, however, on these pages. Click **ACCEPT** to save your configuration.



AWS Logs Configuration

The firewall generates logged events that can be sent to the AWS CloudWatch Logs service. AWS hosted analysis tools, such as ElasticSearch and Kibana, can then use the data to detect threats and other suspicious activity.

The **SonicOS AWS Logs** page allows configuration of the AWS endpoint to which the logs are sent along with settings affecting the frequency with which the data is posted.

To send the logs from SonicOS to Amazon CloudWatch Logs, you must first create a Log Group and a Log Stream in AWS. Assuming that you have an AIM user account, with the appropriate permissions to access CloudWatch Logs from the AWS Console, navigate to the CloudWatch section and select the Logs item in the left navigation

menu. Ensure that you have selected the appropriate AWS region for the logs to be stored. As with many AWS services, CloudWatch Logs is region specific. First create the Log Group and then the Log Stream.

To enable AWS logs in SonicOS:

1 Navigate to **MANAGE | Logs & Reporting | Log Settings > AWS Logs**.

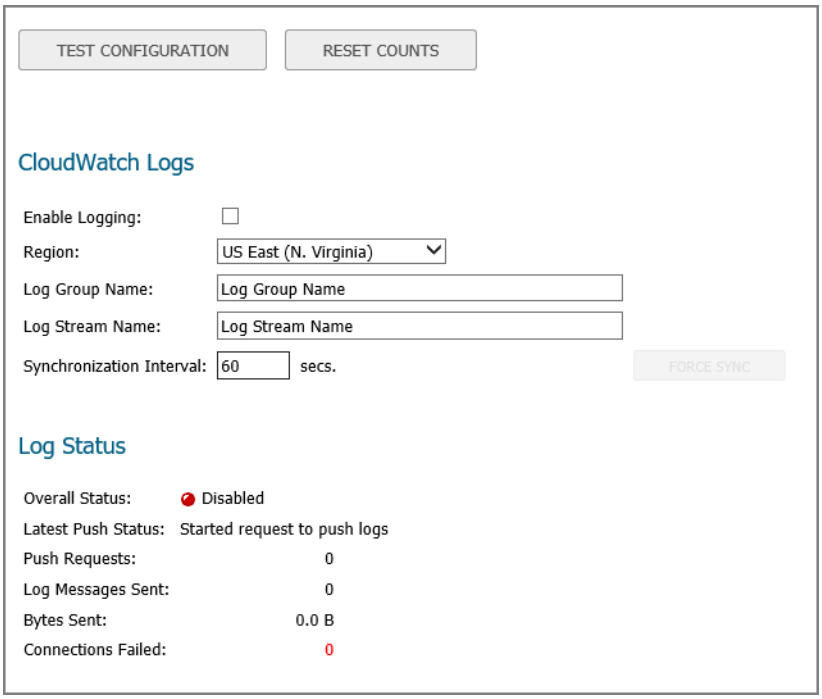
2 Select **Enable Logging**.

3 Ensure that the selected **AWS Region** is the one in which the **Log Group** and **Log Stream** were created. You can change the region that the firewall uses on this page or on the AWS Configuration page.

4 Enter the names of the Log Group and Log Stream that you created earlier and which hold the logs sent to **AWS CloudWatch Logs**.

5 The logs are sent at the specified **Synchronization Interval**. Change the Interval to suit your needs.

6 Click **ACCEPT**.



AWS Objects Configuration

The AWS Objects page is used to map the IP addresses of EC2 Instances running in the AWS Cloud with Address Objects (AOs) and Address Groups (AGs) configured on the firewall

New AOs are created for Instance IP addresses and AGs are created for all addresses of an Instance. Those Instance AGs can be added to existing AGs. And those AOs can then be used in firewall policies for networking, access control and to shape the interaction with EC2 Instances running on AWS.

In AWS, tag the EC2 Instance to then use that tag when defining Address Object Mappings in SonicOS. With the Instance selected, click on the Actions button to launch the popup menu, and then choose **Instance Settings > Add/Edit Tags**.

To create a new Address Object Mapping:

1 Navigate to **MANAGE | Policies | Objects > AWS Objects** in SonicOS.

2 Click **NEW MAPPING**.

3 Click **NEW CONDITION** to choose from the range of allowable properties from the drop-down menu.

4 For example, select **Custom Tag** for **Property**, then enter the **Key** and **Value** used in your EC2 Instance tag and click **OK**.

5 Optionally add a second mapping condition by clicking NEW CONDITION again.

6 When ready, click **OK**.

7 Click **ACCEPT** to save the mapping. Address Objects are then created for the IP addresses of each EC2 Instance that matches the mapping.

8 Select **Enable Mapping**.

9 Click **ACCEPT** to make the Address Object Mappings take effect.

With mappings in place, a Synchronization Interval set, Regions to Monitor specified, and Enable Mapping selected, you see Address Objects and Groups representing the matched EC2 Instances and their IP addresses start to appear.

On the AWS Objects page, the Address Group and the Mapped Address Groups are shown in the AWS EC2 Instances table. Expanding the relevant row reveals the Address Objects corresponding to an Instance's public and private IP addresses. You can see those same host Address Objects on the **Objects | Address Objects** page in SonicOS.

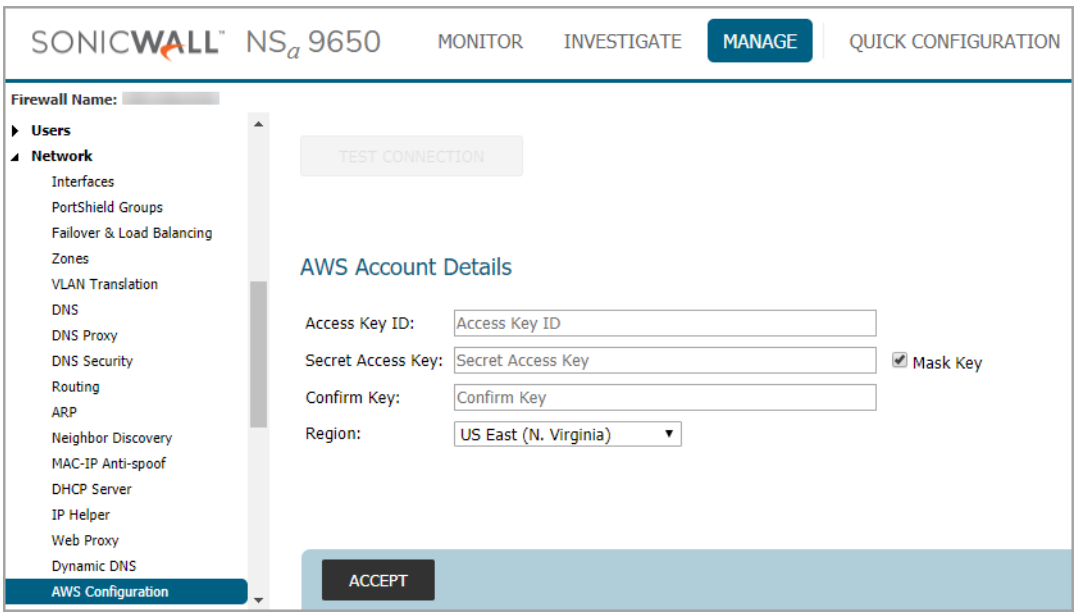
AWS VPN Configuration on SonicOS

Navigate to **MANAGE | Connectivity | VPN > AWS VPN** in SonicOS to establish and manage the connections between the computers on the Local Area Network (LAN) and those in the Virtual Private Clouds (VPCs) on AWS.

The **AWS Virtual Private Clouds** on the SonicOS AWS VPN page reflects the VPC information available on the AWS Console under the VPC Dashboard.

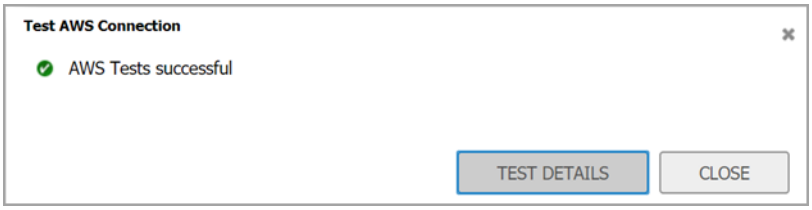
To create a new VPN connection:

1 Navigate to the **MANAGE | System Setup | Network > AWS Configuration** page in SonicOS.

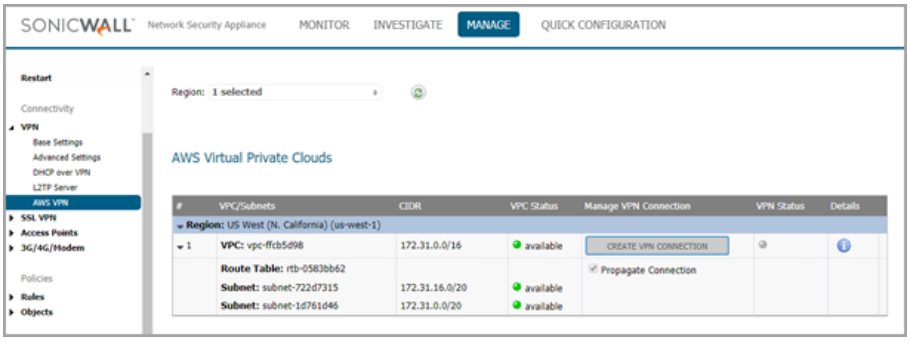


2 Input the **Access Key ID** and **Secret Access Key**. Apply the appropriate **Region** based on the content you want to access.

3 Click **TEST CONNECTION** and confirm that no errors appear:



4 Navigate to the **MANAGE | Connectivity | VPN > AWS VPN** page.



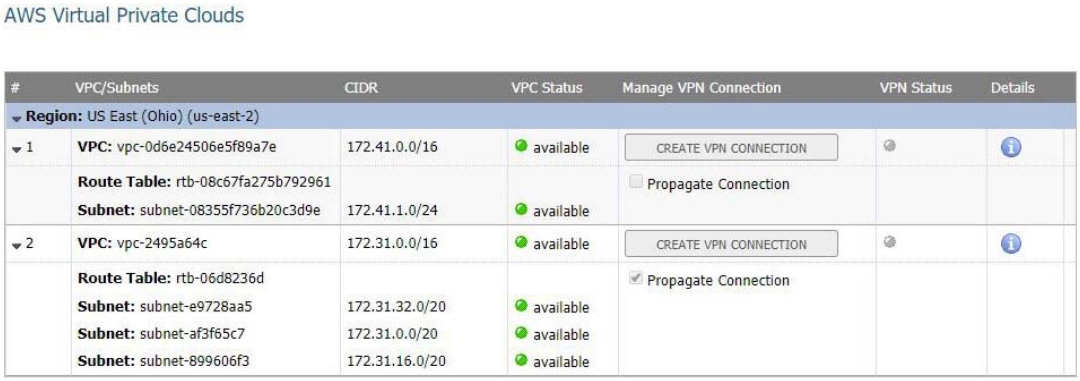
5 Click **CREATE VPN CONNECTION** in the row for the VPC you wish to connect to the firewall.

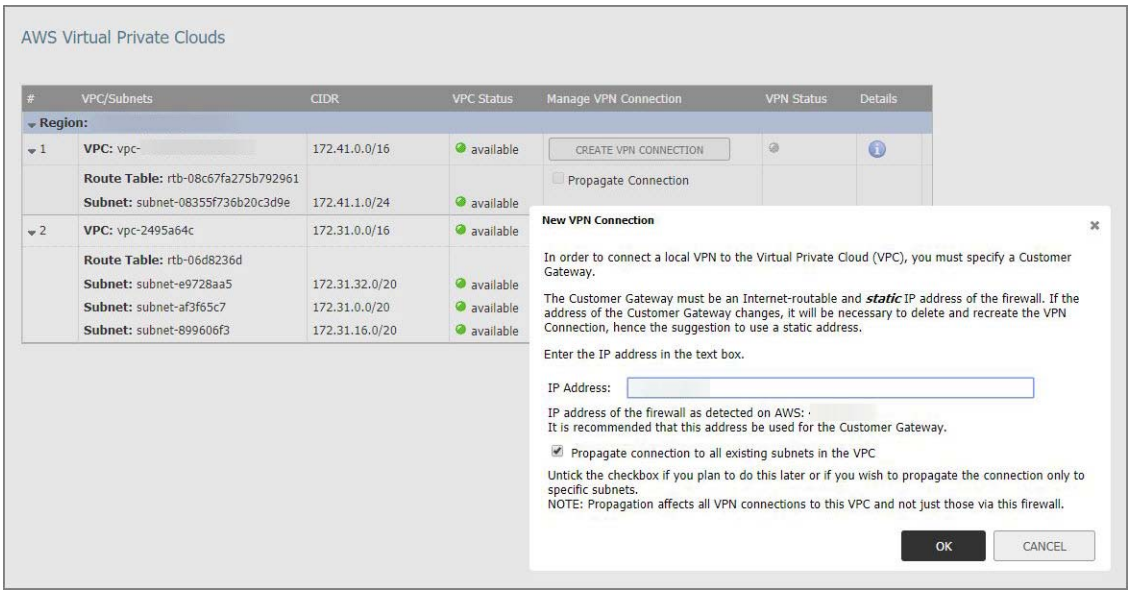
6 In the **New VPN Connection** dialog, verify that the **IP Address** field contains the public IP address of the firewall, or change it as needed. If the firewall is behind a router or some other proxy, Network Address Translation (NAT) rules should be put in place to ensure VPN traffic initiated from the AWS side can be routed back to the firewall.

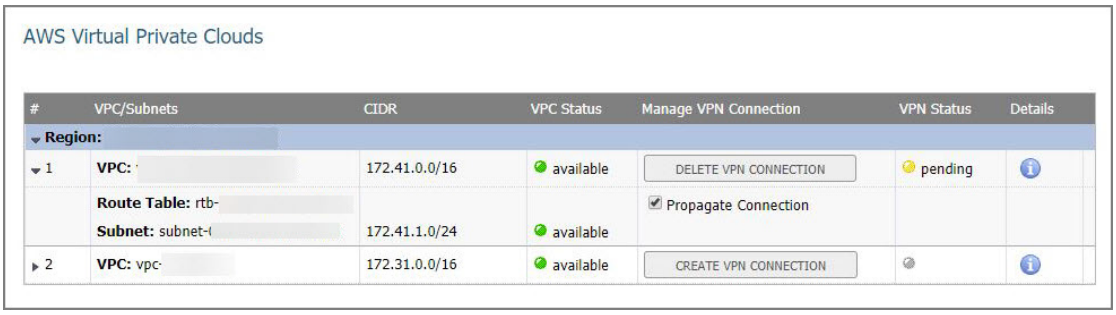
7 If the firewall detects that route propagation is disabled for one or more route tables within a VPC, the dialog includes the Propagate connection to all existing subnets in the VPC option. Select it unless you prefer to propagate the connection only to specific subnets (see Step 6).

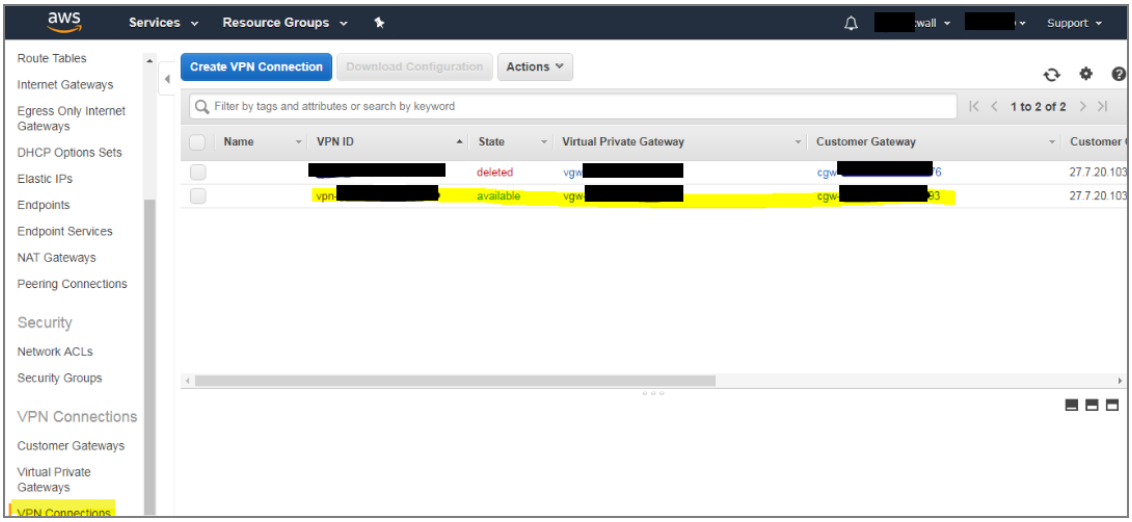
8 Click **OK**. A series of processes on the firewall and AWS configure the VPN connection between them. You can click the Information 'i' button in the table row for details about the VPN connection. Use the Refresh button on the AWS VPN page to reload the data in the table and on the associated dialogs.

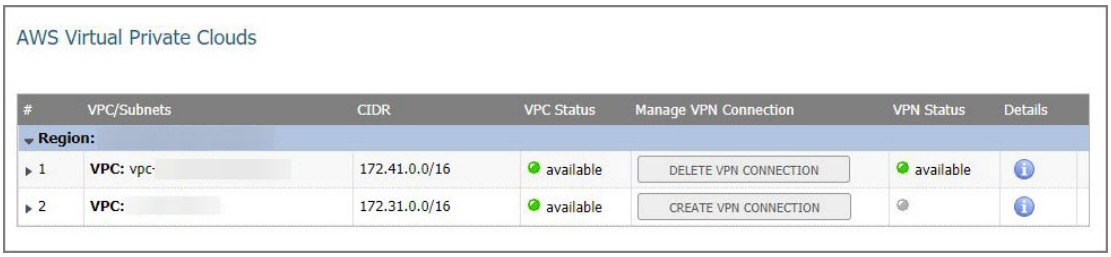
9 After the VPN Connection is established, expand the row on the AWS VPN page to display all of the subnets in that VPC, organized by the route table. Select **Propagate Connection** for each route table (unless you chose to enable propagation for all route tables in Step 4) and the associated subnets.

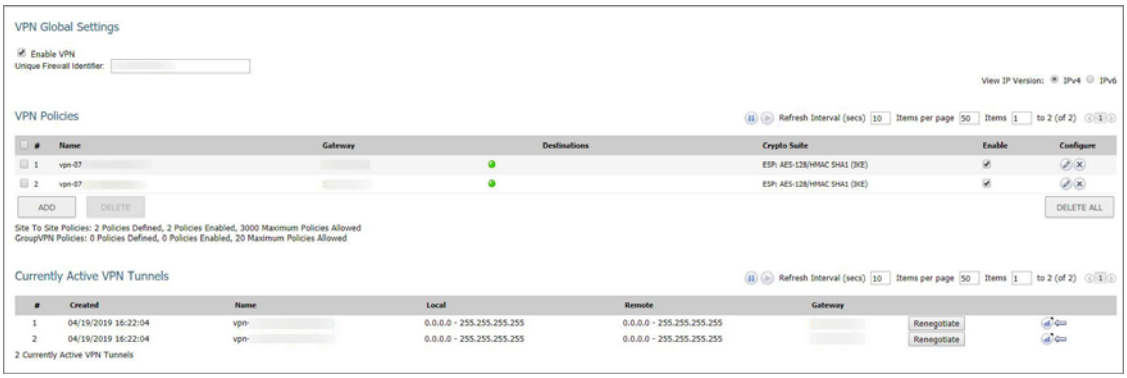




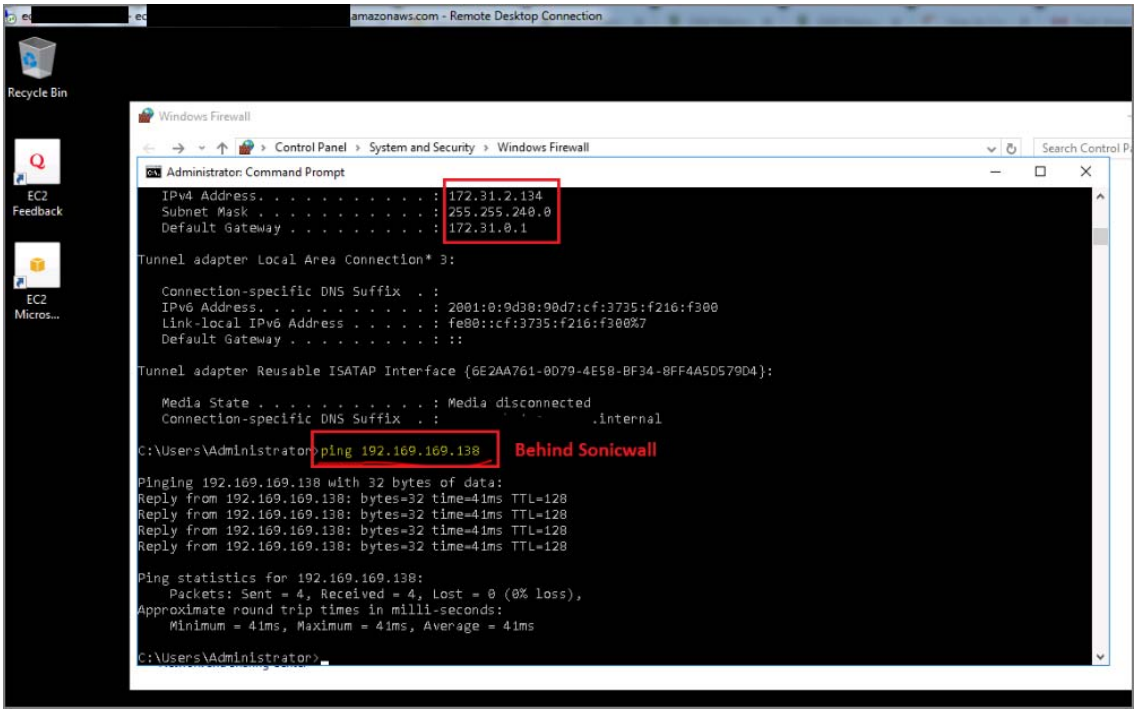



aws
Services
Resource Groups
Support
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections
Create VPN Connection
Download Configuration
Actions
Filter by tags and attributes or search by keyword
1 to 2 of 2
Name
VPN ID
State
Virtual Private Gateway
Customer Gateway
deleted
available
27.7.20.103
27.7.20.103


AWS Virtual Private Clouds
#
VPC/Subnets
CIDR
VPC Status
Manage VPN Connection
VPN Status
Details
Region:
1
VPC: vpc-
172.41.0.0/16
available
DELETE VPN CONNECTION
available
2
VPC:
172.31.0.0/16
available
CREATE VPN CONNECTION


VPN Global Settings
Enable VPN
Unique Firewall Identifier:
View IP Version: IPv4 IPv6
VPN Policies
Refresh Interval (secs) 10 Items per page 50 Items 1 to 2 (of 2)
Name
Gateway
Destinations
Crypto Suite
Enable
Configure
ESP: AES-128/HMAC SHA1 (IKE)
ADD
DELETE
DELETE ALL
Site To Site Policies: 2 Policies Defined, 2 Policies Enabled, 3000 Maximum Policies Allowed
GroupVPN Policies: 0 Policies Defined, 0 Policies Enabled, 20 Maximum Policies Allowed
Currently Active VPN Tunnels
Refresh Interval (secs) 10 Items per page 50 Items 1 to 2 (of 2)
Created
Name
Local
Remote
Gateway
04/19/2019 16:22:04
0.0.0.0 - 255.255.255.255
Renegotiate
2 Currently Active VPN Tunnels

10 Test from the EC2 Instance (AWS) to LAN Subnet behind SonicWall.



To delete a VPN connection:

1 Navigate to **MANAGE | Connectivity | VPN > AWS VPN**.

2 Click **DELETE VPN CONNECTION** in the related table row.

3 Click **YES** in the confirmation dialog. Deletion removes the associated VPN and Route Policies, and the Tunnel interfaces on the firewall. On AWS, it removes the Customer Gateway only if it is not being used elsewhere (perhaps on other VPN Connections from the same firewall, but to other VPCs). It does not delete the VPN Gateway or change the Route Propagation settings.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 4/25/19