

Add GW to existing AWS

Tuesday, December 4, 2018 2:29 PM

Adding a Cloud Guard cluster into an existing AWS environment

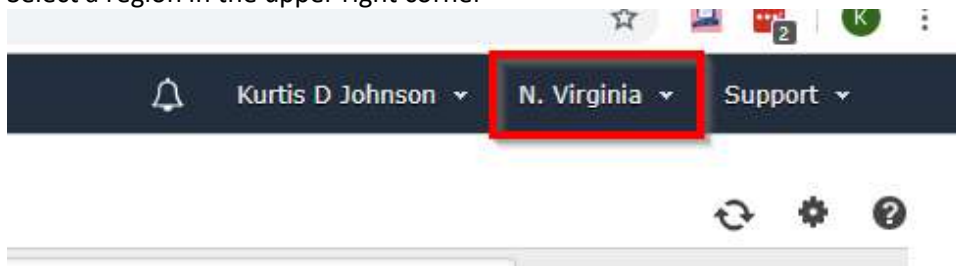
Created 11/20/2018 by Kurt Johnson (SE - KY/OH)

Section 1 - Setup or confirm the initial AWS environment

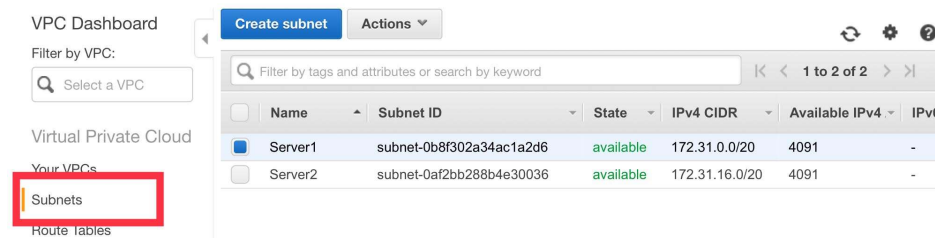
1. Log into AWS account:
<https://console.aws.amazon.com>
2. Add shortcuts to the top bar by clicking the pushpin. It may be helpful to add EC2, VPC, CloudFormation, and IAM



Select a region in the upper right corner



3. Review 'Your VPCs' if one doesn't exist with the CIDR 172.31.0.0/16, Create one.
4. Click on 'Subnets' on the left and create two of them
Server1 - 172.31.0.0/20
Server2 - 172.31.16.0/20



Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag ⓘ

VPC* ⓘ → default

| VPC CIDRs | CIDR | Status | Status Reason |
|-----------|---------------|------------|---------------|
| | 172.31.0.0/16 | associated | |

Availability Zone ⓘ

IPv4 CIDR block* ⓘ

* Required

[Cancel](#) [Create](#)

5. Create Internet Gateway (IGW)

VPC Dashboard

[Create internet gateway](#) [Actions](#)

Filter by VPC:

Filter by tags and attributes or search by keyword

You do not have any Internet gateways in this region

Click the Create Internet gateway button to create your first Internet gateway

[Create internet gateway](#)

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways **1**

Egress Only Internet Gateways

a. Attach the IGW to the VPC

[Create internet gateway](#) [Actions](#) **1**

Filter by tags and attributes

[Delete internet gateway](#)

[Attach to VPC](#) **2**

[Detach from VPC](#)

[Add/Edit Tags](#)

| Name | State | VF |
|-------------------------|----------|----|
| N. Virginia Default IGW | detached | - |

6. Create an EC2 Instance (Virtual Machine) ami-0ac019f4fcb7cb7e6

aws Services Resource Groups **EC2** **1** VPC Clo ⭐ 🔔

EC2 Dashboard

[Launch Instance](#) **3** [Connect](#) [Actions](#)

Filter by tags and attributes or search by keyword

You do not have any running instances in

First time using EC2? Check out the [Getting](#) :

Click the Launch Instance button to start you

[Launch Instance](#)

INSTANCES **2**

[Launch Templates](#)

[Spot Requests](#)

[Reserved Instances](#)

a. Search for 'ami-0ac019f4fcb7cb7e6' and select 64-bit

- b. Select the instance type - t2.micro will be fine
- c. Configure Instance and **Scroll to the bottom of the page** to add custom "User data"

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network Create new VPC
No default VPC found. Create a new default VPC.

Subnet Create new subnet
4091 IP Addresses available

Auto-assign Public IP

Placement group ☐ Add instance to placement group.

Capacity Reservation Create new Capacity Reservation

IAM role Create new IAM role

Shutdown behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy
Additional charges will apply for dedicated tenancy.

Elastic Inference ☐ Add an Elastic Inference accelerator
Additional charges apply.

Cancel Previous **Review and Launch** Next: Add Storage

- d. Before Configuring Security Groups, scroll to the Advanced Details and paste the script below:

```
==begin script==
#!/bin/bash
until sudo apt update && sudo apt -y install apache2;do
sleep 1
done
until sudo curl --output /var/www/html/vsec.jpg --url https://www.checkpoint.com/wp-content/uploads/cloudguard-iaas-236x150.png ; do
sleep 1
done
sudo chmod 666 /var/www/html/index.html
sudo echo $HOSTNAME > /var/www/html/index.html
sudo echo "<BR><BR>Hello World - Check Point CloudGuard IAAS Demo<BR><BR>" >>
/var/www/html/index.html
sudo echo "<img src=\"/vsec.jpg\" height=\"25%\">" >> /var/www/html/index.html
==end script==
```

▼ Network interfaces ⓘ

| Device | Network Interface | Subnet | Primary IP | Secondary IP addresses | IPv6 IPs |
|--------|-------------------------|-------------------|-------------|------------------------|----------|
| eth0 | New network interface ▼ | subnet-0af2bb28 ▼ | Auto-assign | Add IP | Add IP |

Add Device

▼ Advanced Details ⓘ

User data ⓘ ☒ As text ☐ As file ☐ Input is already base64 encoded

```

sudo rm -rf /var/www/html/index.html
sudo echo $HOSTNAME > /var/www/html/index.html
sudo echo "<BR><BR>Hello World - Check Point CloudGuard IAAS
Demo<BR><BR>" > /var/www/html/index.html
sudo echo "<img src='/vsec.jpg' height='25%'>" > /var/www/html/index.html

```

e. Configure Security Groups: Add rules for All ICMP - IPv4 and HTTP

| Type ⓘ | Protocol ⓘ | Port Range ⓘ | Source ⓘ | Description ⓘ |
|-----------------|------------|--------------|-----------------------|----------------------------|
| SSH | TCP | 22 | Custom 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| All ICMP - IPv4 | ICMP | 0 - 65535 | Custom 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| HTTP | TCP | 80 | Custom 0.0.0.0/0 ::/0 | e.g. SSH for Admin Desktop |

Add Rule

Cancel Previous **Review and Launch**

f. Select Launch

g. If you don't already have a Key Pair in AWS, create a new one called AWS_CP_LAB

Select 'Download Key Pair'

Select 'Launch Instances'

Create a new key pair

Key pair name

AWS_CP_LAB

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel **Launch Instances**

Can you PING it? What IP address?

--No Public IP has been assigned.

7. Create/allocate and Associate a new public address to your host

a. Click on your VPC -> Elastic IPs (on the left)

b. Allocate new address

Allocate new address

Allocate a new Elastic IP address by selecting the scope in which it will be used

Scope VPC

IPv4 address pool ☒ Amazon pool
☐ Owned by me

* Required

Cancel

Allocate

c. Click on Actions -> Associate address

Allocate new address Actions

Filter by tags and attributes

| Name | Elastic IP address | Allocation ID | Instance | Private IP address | Scope |
|------|--------------------|----------------|--------------------|--------------------|-------|
| | 52.71.187.223 | ec-064a76cd... | i-0a6678a53b185... | 172.31.13.71 | vpc |

d. Bind the EIP to the Instance IP (Your IP and Instance ID will be different)

Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (52.71.187.223)

Resource type ☒ Instance

☐ Network interface

Instance i-0a6678a53b185a53d

Private IP 172.31.13.71

Reassociation ☐ Allow Elastic IP to be reassociated if already attached



Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. [Learn more.](#)

* Required

Cancel

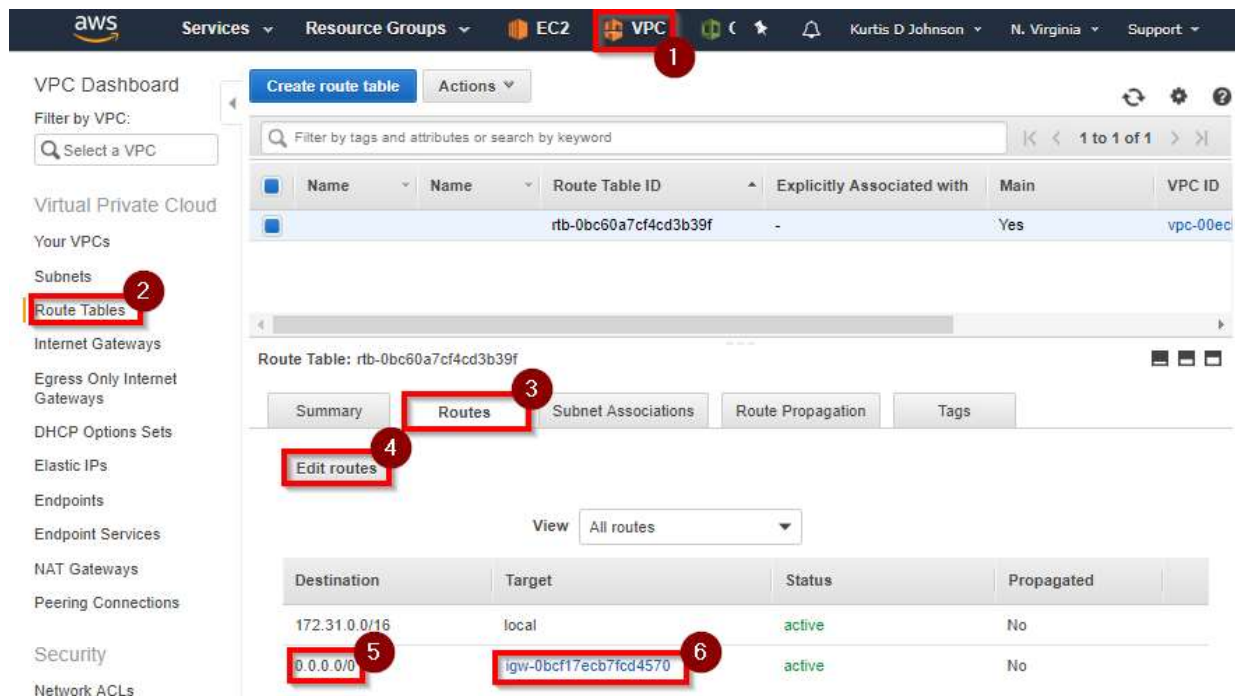
Associate

Can you PING the Elastic (public) IP now?

--Technically, the packet is getting to the host, but no packets are returning.

8. Add a default route leveraging the IGW:

- Select VPC -> Route Tables -> Routes (tab) -> Edit routes
- Add a 0.0.0.0/0 using the IGW created earlier



You should now receive replies from your PING.

You should also receive a response on HTTP

Congratulations!!! Your AWS instance is connected... to EVERYTHING on the Internet.

Section 2 - Add a Cloud Guard cluster

1. Add two new subnets: (VPC -> Subnets)
 - FW_outside - 172.31.254.0/24 - Availability Zone A
 - FW_inside - 172.31.253.0/24 - Availability Zone A

2. Launch a CloudFormation Template to deploy a cluster in an existing VPC
<https://console.aws.amazon.com/cloudformation/home?#/stacks/create/review?templateURL=https%3A%2F%2Fs3.amazonaws.com%2Fcloudformation-template%2Fcluster-into-vpc.json&stackName=Check-Point-Cluster>

- a. Enter the information below

VPC Network Configuration

| | |
|-------------------|-------------------------------|
| VPC | <the one you created earlier> |
| Availability Zone | A <same as the Subnets> |
| External subnet | FW_outside |
| Internal subnet | FW_inside |

Cluster Network Configuration

| | |
|---------------------------|---------------|
| Cluster external address | 172.31.254.10 |
| Member A external address | 172.31.254.20 |
| Member B external address | 172.31.254.30 |

| | |
|---------------------------|---------------|
| Cluster internal address | 172.31.253.10 |
| Member A internal address | 172.31.253.20 |
| Member B internal address | 172.31.253.30 |

EC2 Instance Configuration

| | |
|---------------|---------------------------|
| Instance type | C4.xlarge <default> |
| Key name | <same from Section 1-6-g> |

Check Point Settings

| | |
|-------------------------|---------------------------------------|
| License | R80.10-BYOL |
| Admin shell | /bin/bash |
| Password hash | \$1\$mX1Pn5NV\$nK6n18yxt1AvfgITZpDn.1 |
| --- | That is the hash of zaq1@WSXcde3 |
| SIC key | abcd1234 |
| Allow upload & download | true <default> |
| Primary NTP server | 169.254.169.123 <default> |
| Secondary NTP server | 0.pool.ntp.org <default> |

Capabilities

- ☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names
- ☒ I acknowledge that AWS CloudFormation might require the following capability: -----

b. Click Create

3. Wait for approximately 5 minutes and record the Elastic IP information

| Cluster info | Private IP address | Public IP address |
|--------------|--------------------|-------------------|
| VIP | 172.31.254.10 | 100.26.128.32 |
| Member A | 172.31.254.20 | 54.84.135.202 |
| Member B | 172.31.254.30 | 54.152.247.164 |

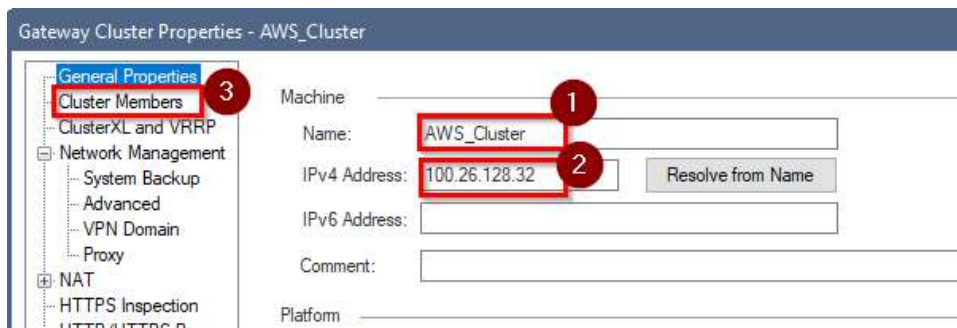
4. Create a new Cluster object using the IP addresses found on the Elastic IP section in AWS



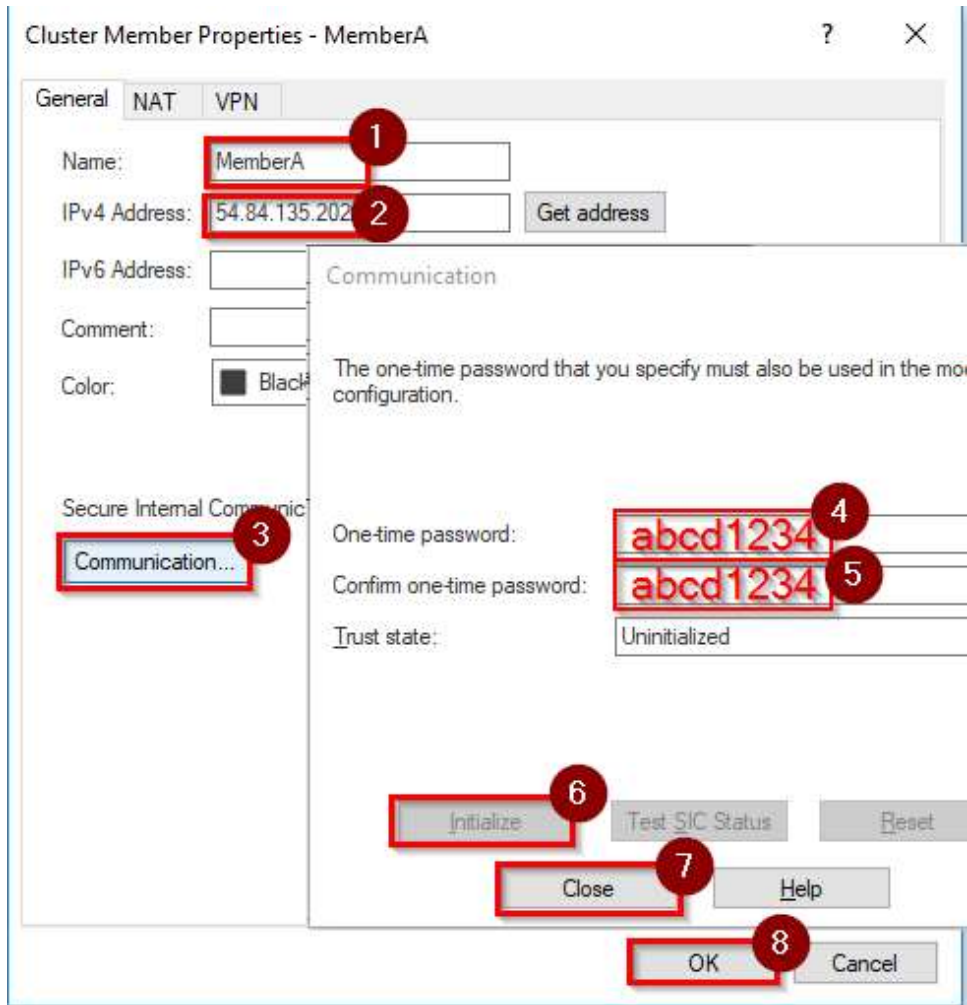
a. Select Classic mode

b. Input a Name and the public IP address tied to the VIP 172.31.254.10 from your Elastic IP information.

c. Then select Cluster Members

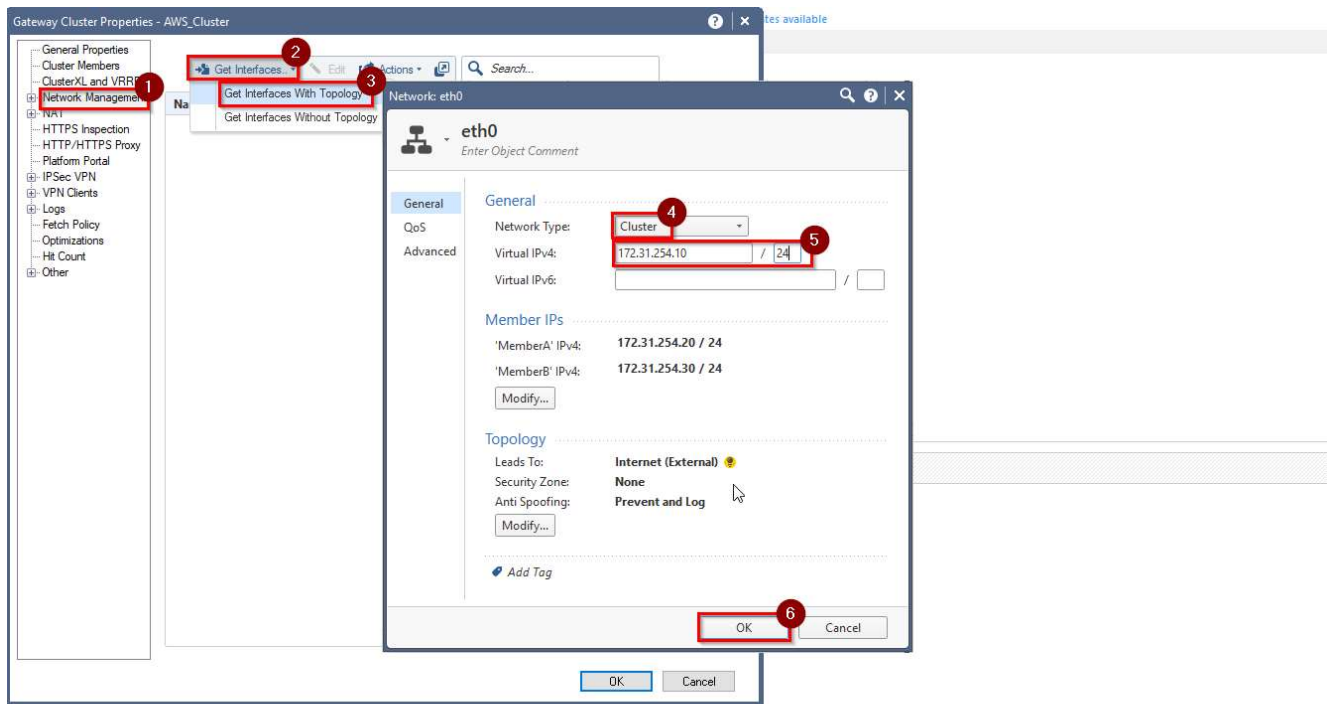


d. Add -> New Cluster Member...

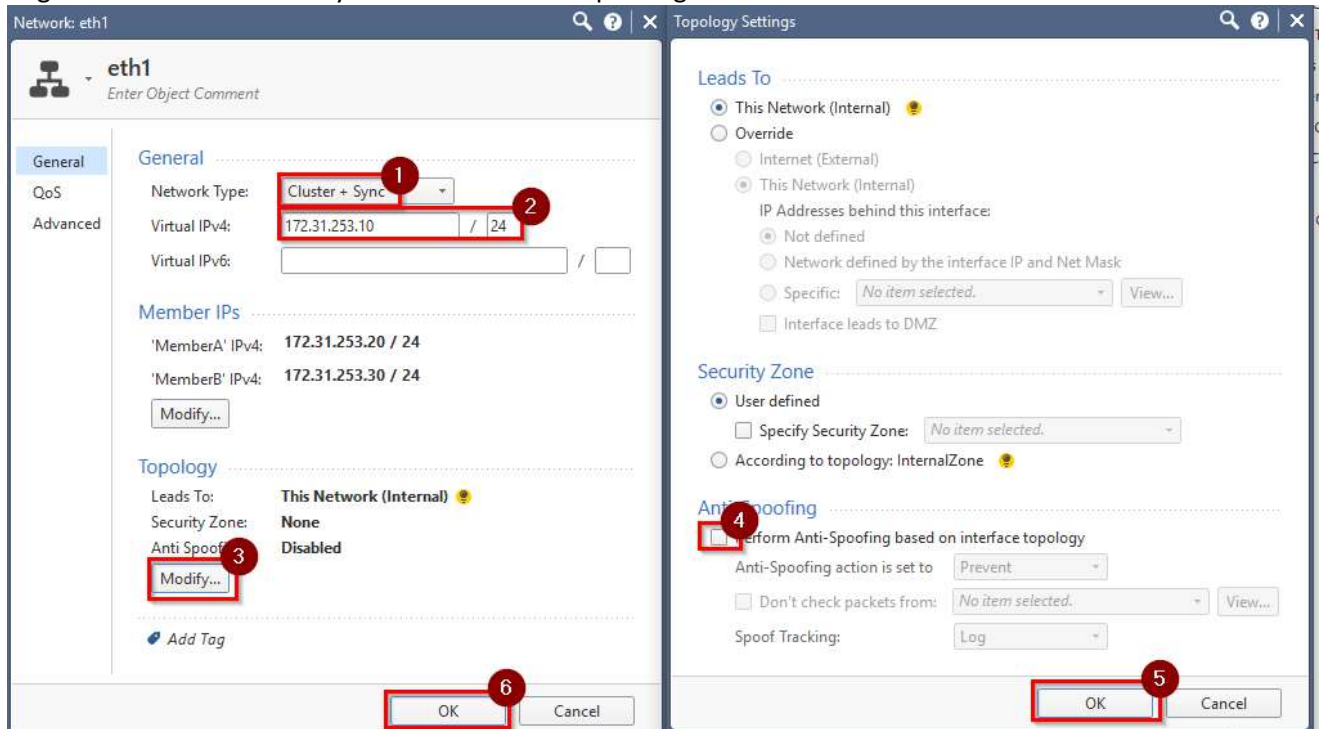


e. Repeat the above step for Member B

f. Configure Network Management for eth0 as a Cluster interface

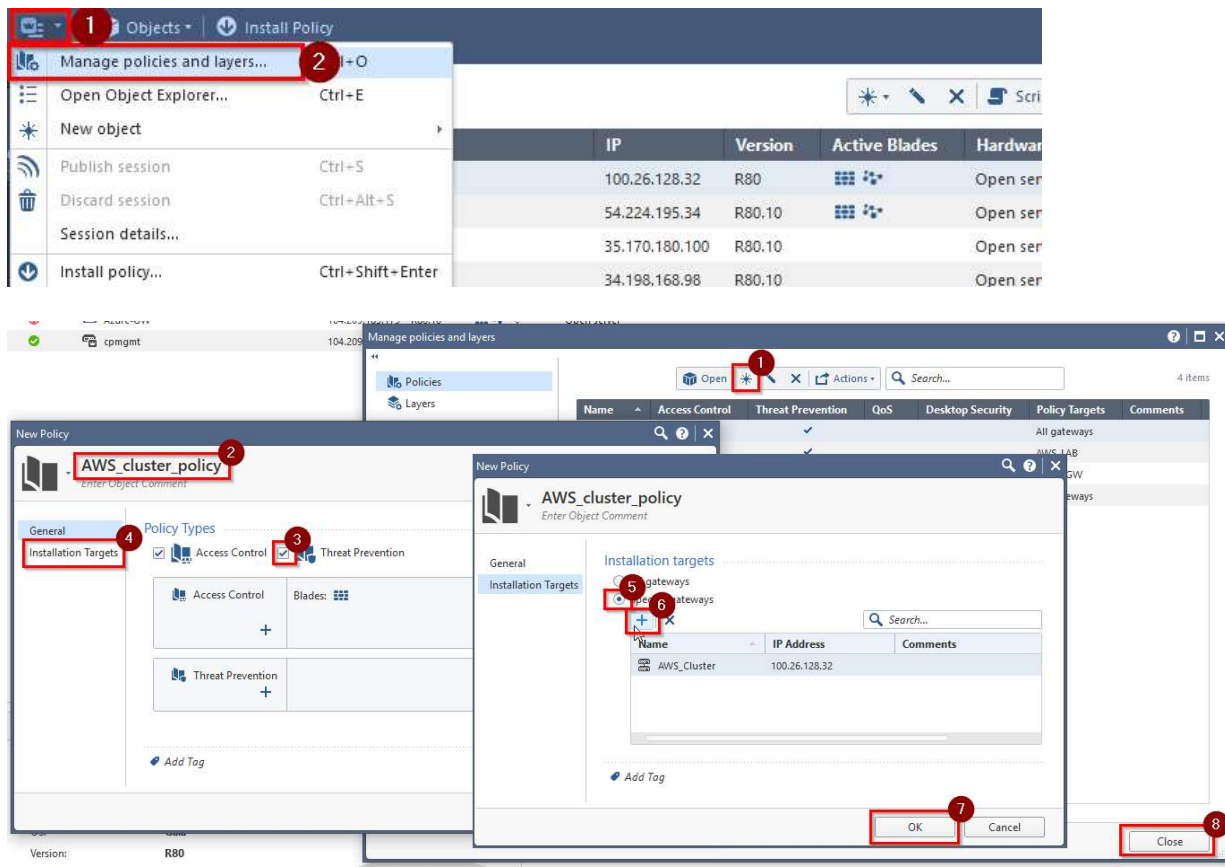


g. Edit eth1 - Cluster + Sync and disable Anti-Spoofing

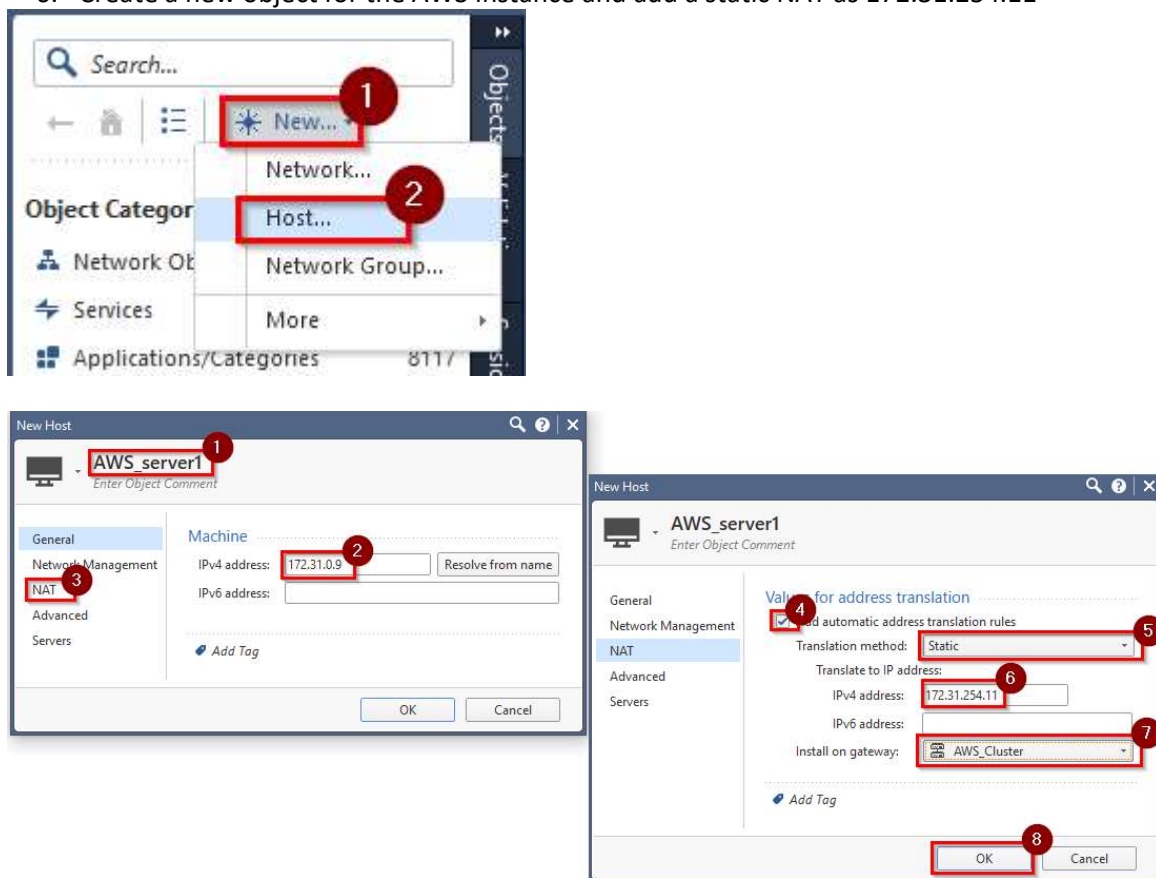


- h. Click OK to complete the Cluster setup
- i. Click Yes to the warning dialog box - VPN Link Selection

5. Create a new policy:



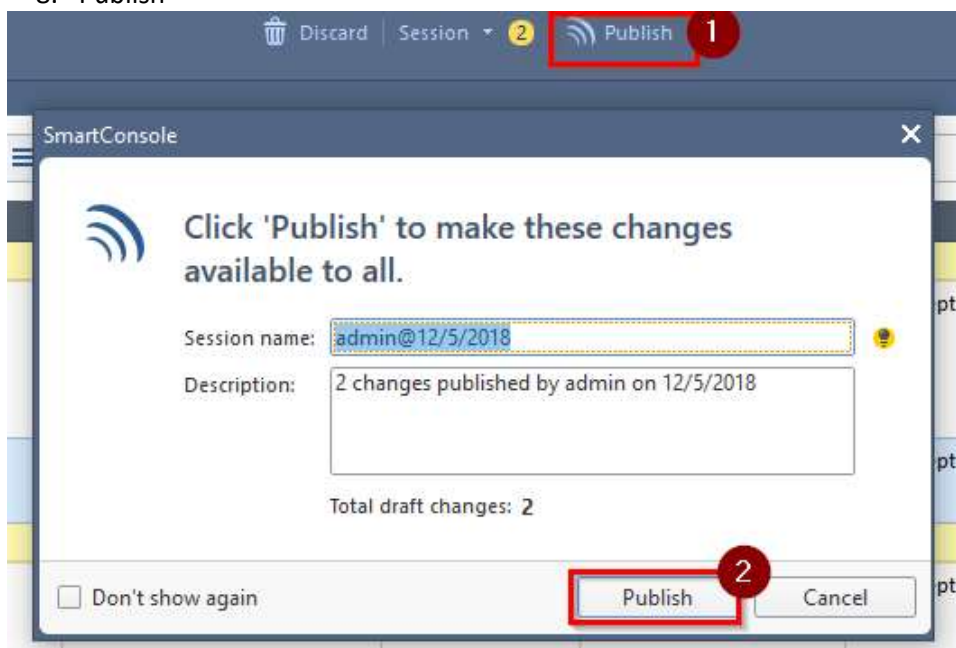
6. Create a new object for the AWS instance and add a static NAT as 172.31.254.11



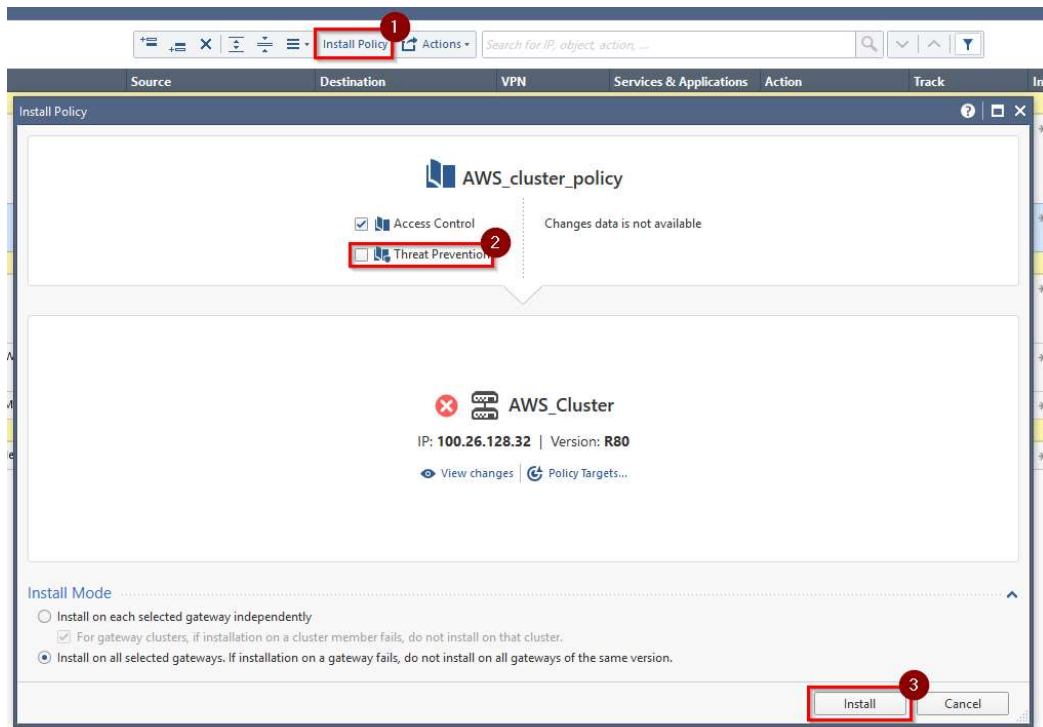
7. Create the following rulebase

| No. | Name | Source | Destination | VPN | Services & Applications | Action | Track |
|---------------|------------------|-------------|-------------|-------|---|--------|-------|
| Mgmt (1-2) | | | | | | | |
| 1 | | * Any | AWS_Cluster | * Any | http ssh_version_2 https ICMP echo-request | Accept | Log |
| 2 | | AWS_Cluster | * Any | * Any | https ICMP echo-request | Accept | Log |
| Traffic (3-5) | | | | | | | |
| 3 | | * Any | AWS_server1 | * Any | http ssh_version_2 ICMP echo-request | Accept | Log |
| 4 | Allowed WWW out | AWS_server1 | * Any | * Any | http https | Accept | Log |
| 5 | Allowed ICMP out | AWS_server1 | * Any | * Any | ICMP echo-request | Accept | Log |
| Cleanup (6) | | | | | | | |
| 6 | Cleanup rule | * Any | * Any | * Any | * Any | Drop | Log |

8. Publish



9. Install (Clear Threat Prevention for first policy install)



Section 3 - Add NAT and Routes

1. Add new address to the outside for NAT
 - a. AWS -> EC2 -> Network Interfaces (scroll to the right and edit the interface holding the 172.31.254.10 address)
 - o At click 7 <in the image below> input 172.31.254.11

The screenshot shows the AWS Management Console interface. In the top navigation bar, the **EC2** link is highlighted with a red circle 1. In the left-hand navigation pane, **Network Interfaces** is highlighted with a red circle 2. The main content area displays a list of network interfaces. The **Actions** dropdown menu is open, and **Manage IP Addresses** is selected with a red circle 5. In the **Manage IP Addresses** modal, the **Assign new IP** button is highlighted with a red circle 6. The **IPv4 Addresses** table shows a row with **172.31.254.10** highlighted with a red circle 7. The **Yes, Update** button at the bottom right is highlighted with a red circle 8. The **Close** button (X) at the top right of the modal is highlighted with a red circle 9. The **Secondary private IPv4 IPs** column in the background table shows **172.31.253.10** highlighted with a red circle 3.

b. Record the ENI of the Internal Cluster VIP 172.31.253.10 to be used in routes
eni-00da257fa0edc873a

The screenshot shows the details of a specific Network Interface. The table above the details section lists several network interfaces. The **Secondary private IPv4 IPs** column shows **172.31.253.10** highlighted with a red box. Below the table, the **Network Interface: eni-00da257fa0edc873a** details are shown. The **Network interface ID** is highlighted with a red box and contains the value **eni-00da257fa0edc873a**. Other details include VPC ID, MAC address, Security groups, Subnet ID, Availability Zone, Description, and Owner ID.

NEXT STEPS WILL CAUSE A DISCONNECT UNTIL WE ROUTE TRAFFIC
BACK THROUGH THE FIREWALL

2. Re-associate our Elastic IP from the Server1 instance to the Firewalls External Interface.

1 Resource type: Network interface

2 Network interface: eni-0beecb83c39d87f50

3 Private IP: 172.31.254.11

4 Reassociation: ☒ Allow Elastic IP to be reassociated if already attached

5 Associate address

6 Associate

| Network Interface ID | Name |
|-----------------------|--|
| eni-0beecb83c39d87f50 | am:aws:cloudformation:us-east-1:123ad236a92a |
| eni-0cc20cdc50fe1a021 | MemberInternalInterface |
| eni-0de0c22eb5d2ab244 | |
| eni-00da257fa0edc873a | Check-Point-Cluster |

ng
ssociate an Elastic IP address with your instance, your current public IP address is released. Le

3. A new Route table was created from the CloudFormation Template. Modify the Internal Routing table and edit the Subnet Associations to include Server1 - 172.31.0.0/20 and Server2 - 172.31.16.0/20. FW_inside - 172.31.253.0/24 should ALREADY be associated.

The screenshot shows the AWS VPC console. The 'Route Tables' section is active. The 'Route' table lists subnets and their associated route tables. The 'Server2' and 'Server1' subnets are highlighted. The 'Actions' menu is open, and the 'Edit subnet associations' option is selected. The 'Save' button is highlighted.

Traffic should now be flowing through the Firewall

Extra step 1:

Enable IPS, Anti-Bot, and Anti-Virus in PREVENTION mode

Install Threat Prevention Policy

SSH into the Ubuntu server (Elastic IP)

Test AV from the Ubuntu server with CURL:

curl <http://www.eicar.org/download/eicar.com> -o eicar.com.txt

Do you see a drop in the logs?

Extra step 2:

SSH into the Ubuntu server (Elastic IP) - execute:

```
while true; do curl www.google.com --max-time 5 >/dev/null; sleep 5; done
```

In a new window, SSH into the Firewall Cluster VIP - execute:

```
clusterXL_admin down
```

AWS interfaces will automatically be moved from one member to the other, but your Ubuntu session should come back with approximately 5 CURLs timed out.

Clean up:

DELETE the cluster via CloudFormation

DELETE the instance via EC2