EVANCED.NET

Configuring a Palo Alto Firewall in AWS

Version 1.0 10/19/2015

GRANT CARMICHAEL, MBA, CISSP, RHCA, ITIL

For contact information visit EVANCED.NET

Table of Contents

This tutorial assumes you already have an AWS account, security keys and know how to use a SSH client to access the AWS servers. For this exercise PuTTY, Pageant, and PuTTYgen will be used to access the AWS servers.

NOTE: Charges may apply when using AWS services. Before proceeding, be sure to read and understand Amazon's user agreement and the respective charges. Secondly, this tutorial is intended to be a quick reference for setting up the Palo Alto in AWS, and in no way recommends, implies or suggests best practice for securing the environment.

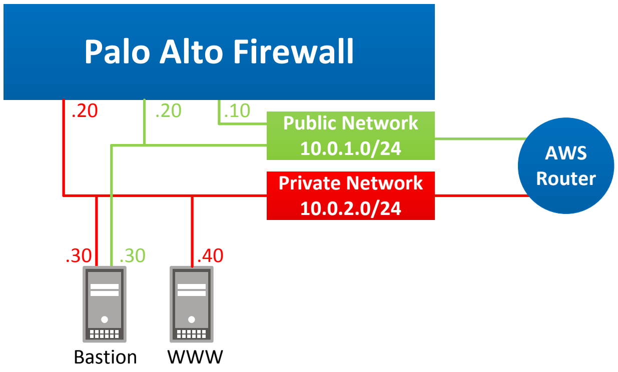
The Network Design

In this tutorial you will create a web server farm behind a Palo Alto firewall in AWS. Web servers will be built in a private DMZ network. An Internet Gateway will be created for Internet access, and Elastic IPs will be used to associate (or NAT) to the public network.

PRIVATE IP LIST
10.0.1.10 : PAN Management NIC
10.0.1.20 : PAN Public NIC
10.0.1.30 : Bastion Public NIC
10.0.2.20 : PAN Private NIC
10.0.2.30 : Bastion Private NIC
10.0.2.40 : Web Server NIC

Public IP/Private IP
X.X.X.X/10.0.1.10 PAN MGT
X.X.X.X/10.0.1.20 PAN Public
X.X.X.X/10.0.1.30 Bastion Public

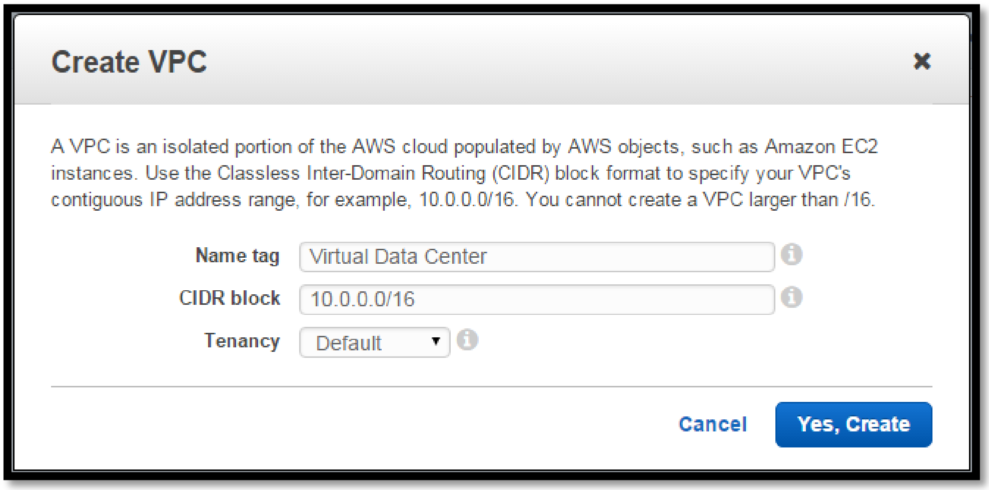
VPC Network
10.0.0.0/16



Step 1 – Building the AWS network

Let's get started by creating our Virtual Private Cloud (VPC) network, which is our virtual network where virtual resources will be launched.

Browse to **VPC > Your VPCs** and select **Create VPC.**



Create VPC

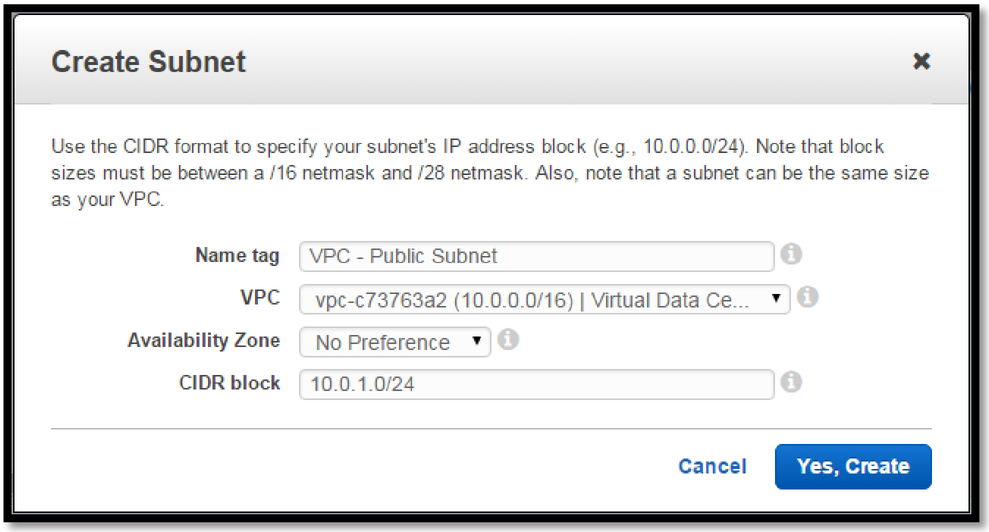
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. Use the Classless Inter-Domain Routing (CIDR) block format to specify your VPC's contiguous IP address range, for example, 10.0.0.0/16. You cannot create a VPC larger than /16.

Name tag	Virtual Data Center
CIDR block	10.0.0.0/16
Tenancy	Default

Next, create subnets within your VDC – one for the public side of your VDC and the other for the private.

Browse to **VPC > Subnets** and select **Create Subnet**

Create the **VPC – Public Subnet**

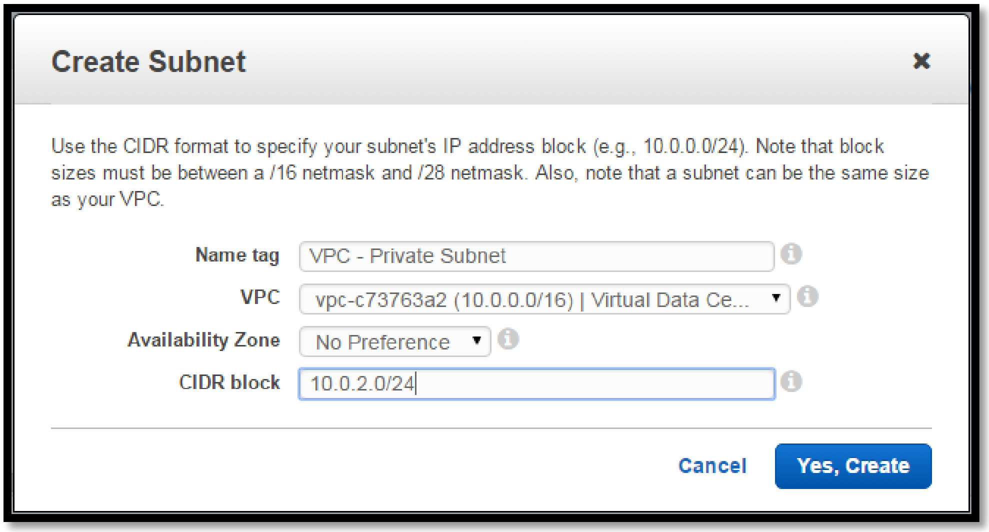


Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag	VPC - Public Subnet
VPC	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Ce...
Availability Zone	No Preference
CIDR block	10.0.1.0/24

Create the **VPC – Private Subnet**



Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

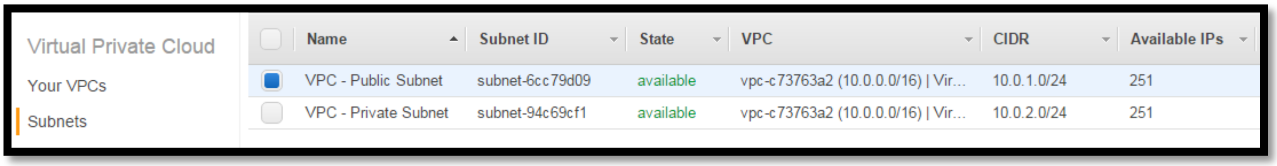
Name tag: VPC - Private Subnet

VPC: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Ce...

Availability Zone: No Preference

CIDR block: 10.0.2.0/24

Here is the final result

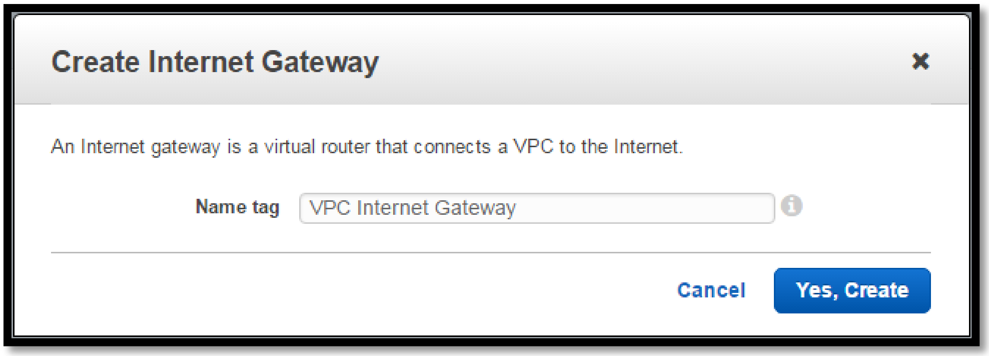


	Name	Subnet ID	State	VPC	CIDR	Available IPs
☑	VPC - Public Subnet	subnet-6cc79d09	available	vpc-c73763a2 (10.0.0.0/16) | Vir...	10.0.1.0/24	251
☐	VPC - Private Subnet	subnet-94c69cf1	available	vpc-c73763a2 (10.0.0.0/16) | Vir...	10.0.2.0/24	251

Building the Internet Gateway

Now we need to create the Internet Gateway, which allows instances, i.e. servers, to communicate with the Internet. The Internet Gateway is the Internet router for your VPC.

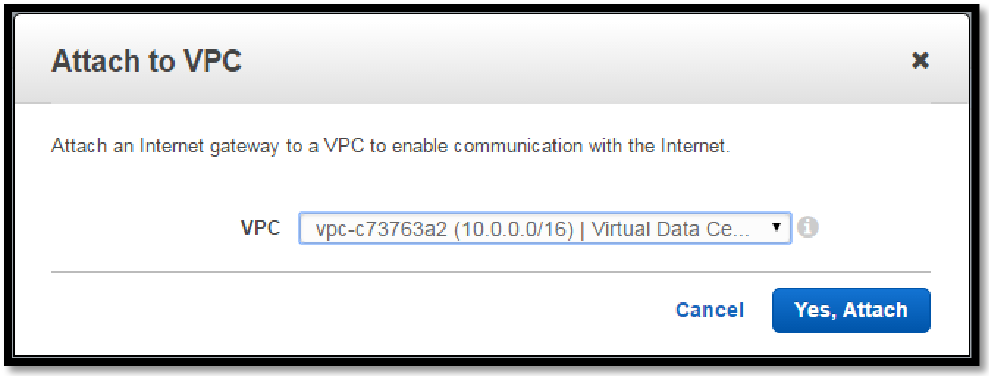
Browse to **VPC > Internet Gateways** and select **Create Internet Gateway**



An Internet gateway is a virtual router that connects a VPC to the Internet.

Name tag: VPC Internet Gateway

Select **Attach to VPC**

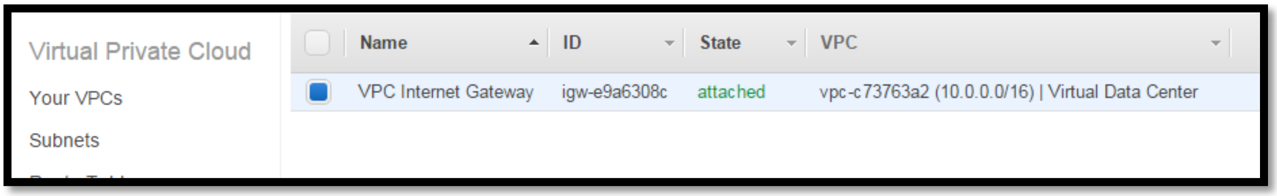


Attach to VPC

Attach an Internet gateway to a VPC to enable communication with the Internet.

VPC: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Ce...

Here is the final result for the Internet Gateway



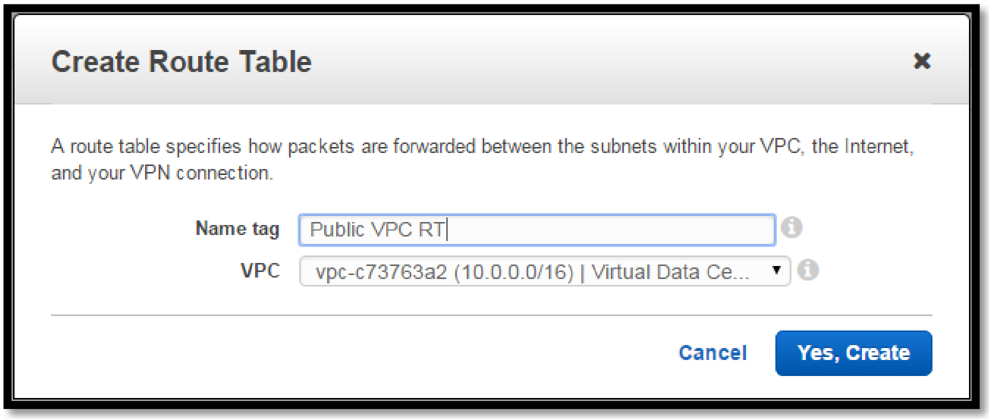
	Name	ID	State	VPC
■	VPC Internet Gateway	igw-e9a6308c	attached	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center

Creating the Route Tables for the Public and Private VPC subnets

Create two new routes for the VPC subnets and then associate the respective subnet to the route.

Browse to **VPC > Route Tables** and select **Create Route Table**

Create the **Public VPC RT**



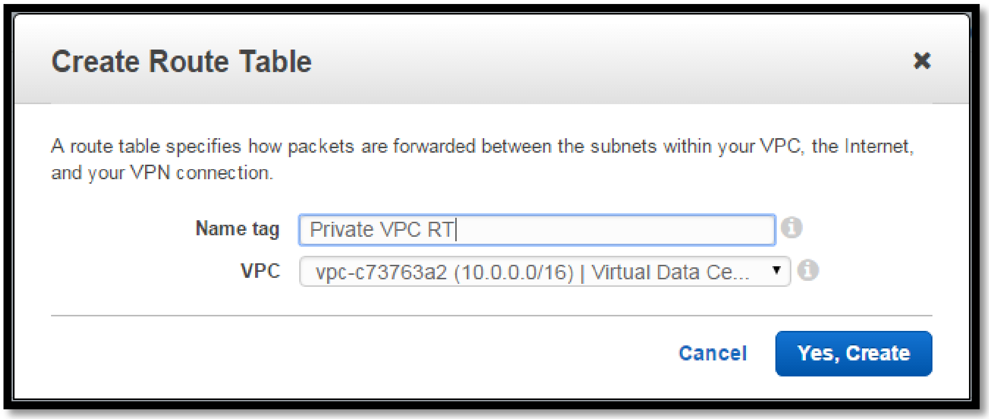
Create Route Table

A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag: Public VPC RT

VPC: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Ce...

Create the **Private VPC RT**



Create Route Table

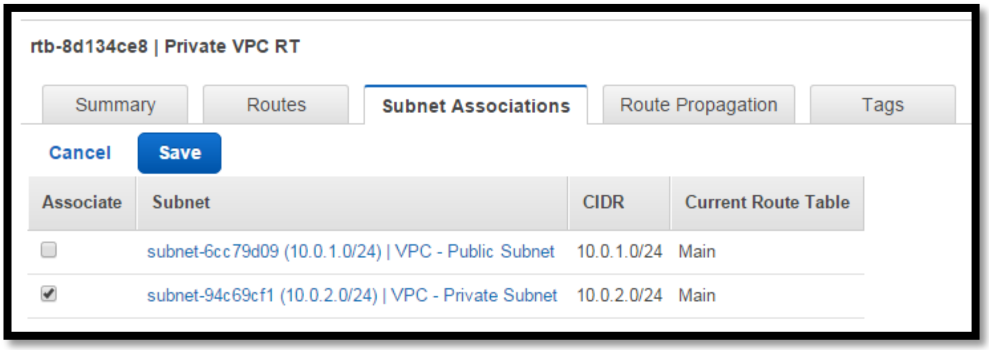
A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag: Private VPC RT

VPC: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Ce...

Now associate subnets to the new routes.

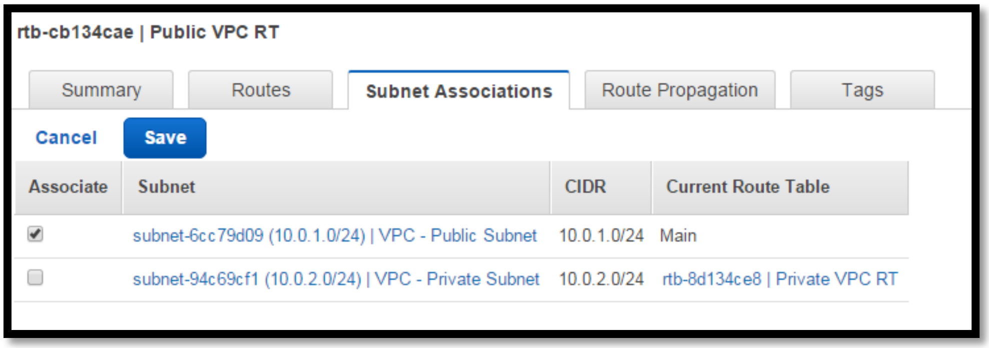
Select **Private VPC RT**, select the **Subnet Associations** tab and click **Edit.** Select the **Private Subnet** and click **Save**.



rtb-8d134ce8 | Private VPC RT

Associate	Subnet	CIDR	Current Route Table
□	subnet-6cc79d09 (10.0.1.0/24) | VPC - Public Subnet	10.0.1.0/24	Main
☑	subnet-94c69cf1 (10.0.2.0/24) | VPC - Private Subnet	10.0.2.0/24	Main

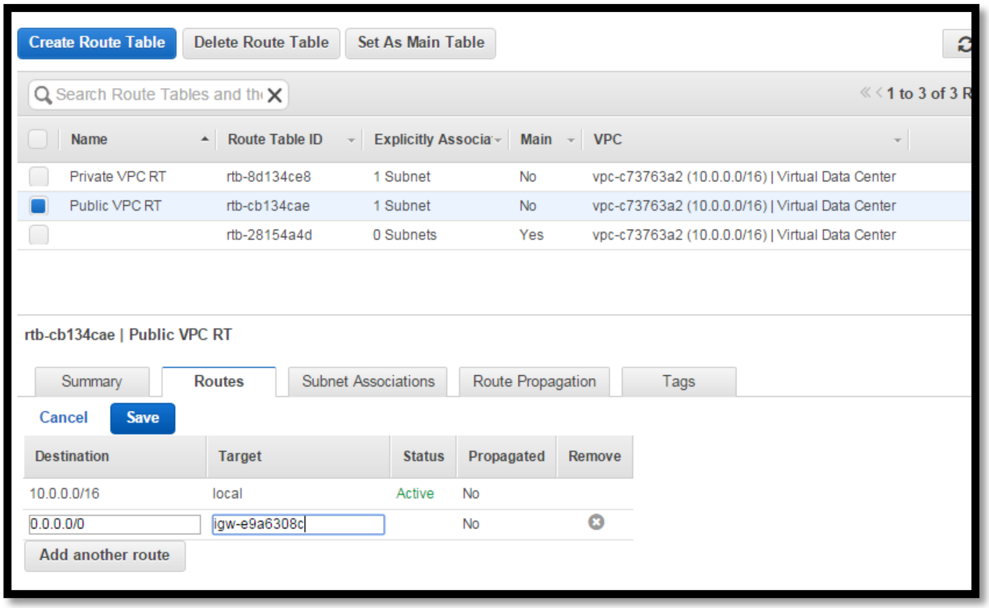
Repeat the same steps to associate the **Public VPC RT** with the **Public Subnet**



rtb-cb134cae | Public VPC RT

Associate	Subnet	CIDR	Current Route Table
☑	subnet-6cc79d09 (10.0.1.0/24) | VPC - Public Subnet	10.0.1.0/24	Main
□	subnet-94c69cf1 (10.0.2.0/24) | VPC - Private Subnet	10.0.2.0/24	rtb-8d134ce8 | Private VPC RT

Next create a default route on the **Public VPC RT** to the Internet Gateway

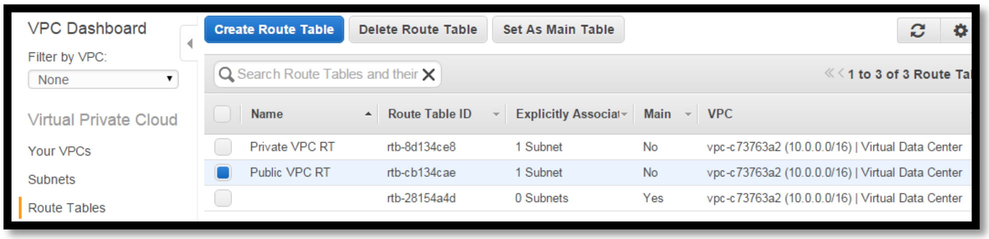


	Name	Route Table ID	Explicitly Associa	Main	VPC
□	Private VPC RT	rtb-8d134ce8	1 Subnet	No	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center
■	Public VPC RT	rtb-cb134cae	1 Subnet	No	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center
□		rtb-28154a4d	0 Subnets	Yes	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center

rtb-cb134cae | Public VPC RT

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	igw-e9a6308c		No	⊗

Here is a look at the new routes



	Name	Route Table ID	Explicitly Associa	Main	VPC
□	Private VPC RT	rtb-8d134ce8	1 Subnet	No	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center
■	Public VPC RT	rtb-cb134cae	1 Subnet	No	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center
□		rtb-28154a4d	0 Subnets	Yes	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center

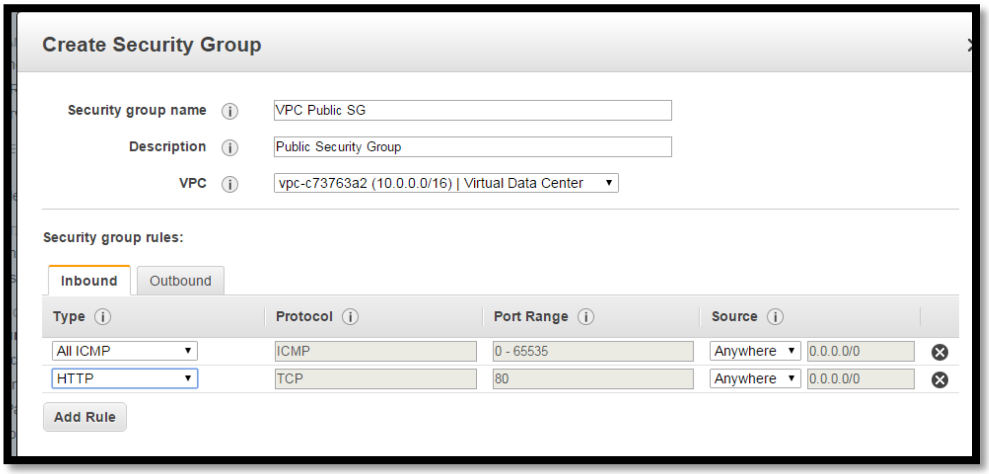
At this point, the network is almost complete. As we create the Palo Alto instance and the Linux servers, we will come back and add a few Elastic IPs.

Step 2 – Building the Palo Alto Network (PAN)

Creating Security Groups

When creating a new instance, you can add Security Groups on the fly, but we are going to create them now.

Create the Public Security Group that allows ICMP and HTTP. ICMP will be allowed so that server instances in the Security Group can be pinged for troubleshooting.



Create Security Group

Security group name: VPC Public SG

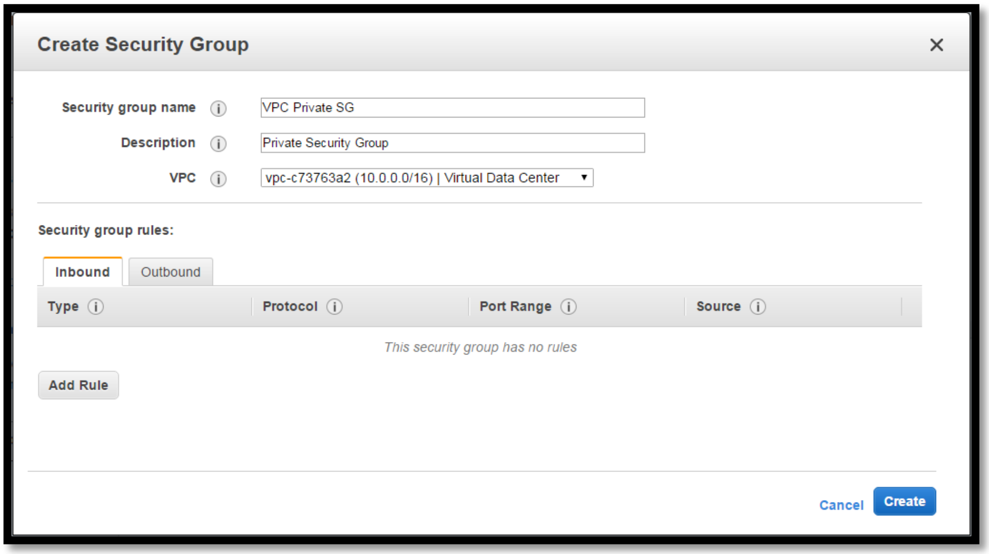
Description: Public Security Group

VPC: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center

Security group rules:

Type	Protocol	Port Range	Source	
All ICMP	ICMP	0 - 65535	Anywhere	0.0.0.0/0
HTTP	TCP	80	Anywhere	0.0.0.0/0

Create the Private Security Group, but don't add any inbound rules just yet.



Create Security Group

Security group name: VPC Private SG

Description: Private Security Group

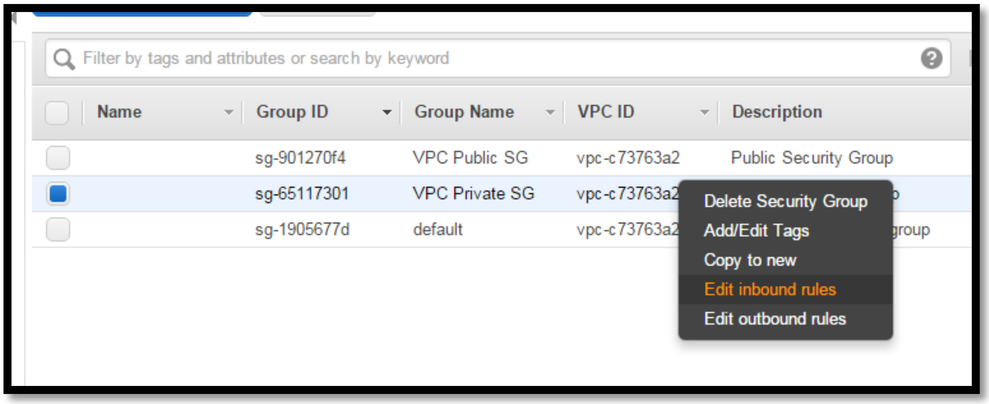
VPC: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center

Security group rules:

Type	Protocol	Port Range	Source

This security group has no rules

Now right-click on the VPC Private SG and select **Edit inbound rules.**



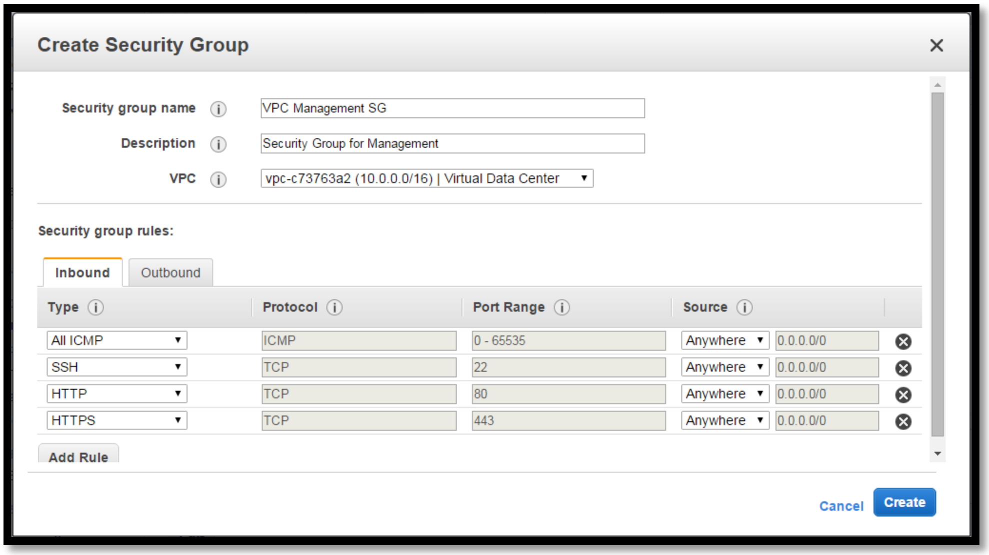
Filter by tags and attributes or search by keyword

	Name	Group ID	Group Name	VPC ID	Description
□		sg-901270f4	VPC Public SG	vpc-c73763a2	Public Security Group
☑		sg-65117301	VPC Private SG	vpc-c73763a2	p
□		sg-1905677d	default	vpc-c73763a2	group

Add a rule that allows all traffic (or any traffic you want) to the VPC Private SG that originates from the VPC Private SG. This allows hosts inside the VPC Private SG to communicate. There could be instances where you need more granular ACLs, but for this tutorial let's keep it simple.

Now create a VPC Management Security Group that will allow access to the PAN management interface, which is where you will login and manage the firewall.

NOTE: Again, I'm using ACLs that are quite liberal. I wouldn't recommend this for a production environment. I would restrict the ACLs to allow SSH and HTTPS only from your corporate network block or IP.



Create Security Group

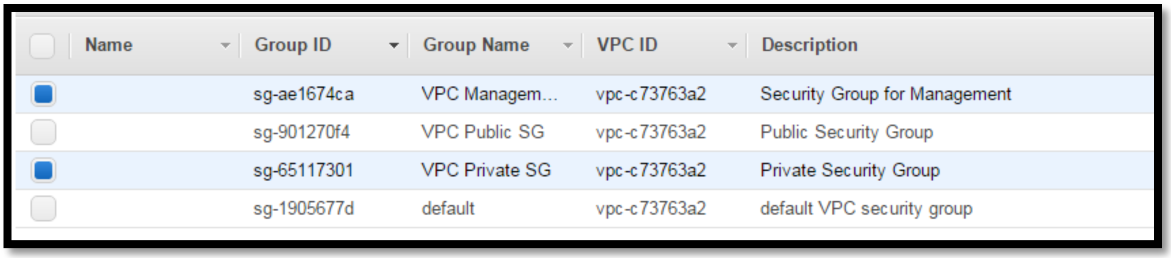
Security group name	VPC Management SG
Description	Security Group for Management
VPC	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center

Security group rules:

Inbound | Outbound

Type	Protocol	Port Range	Source	
All ICMP	ICMP	0 - 65535	Anywhere	0.0.0.0/0
SSH	TCP	22	Anywhere	0.0.0.0/0
HTTP	TCP	80	Anywhere	0.0.0.0/0
HTTPS	TCP	443	Anywhere	0.0.0.0/0

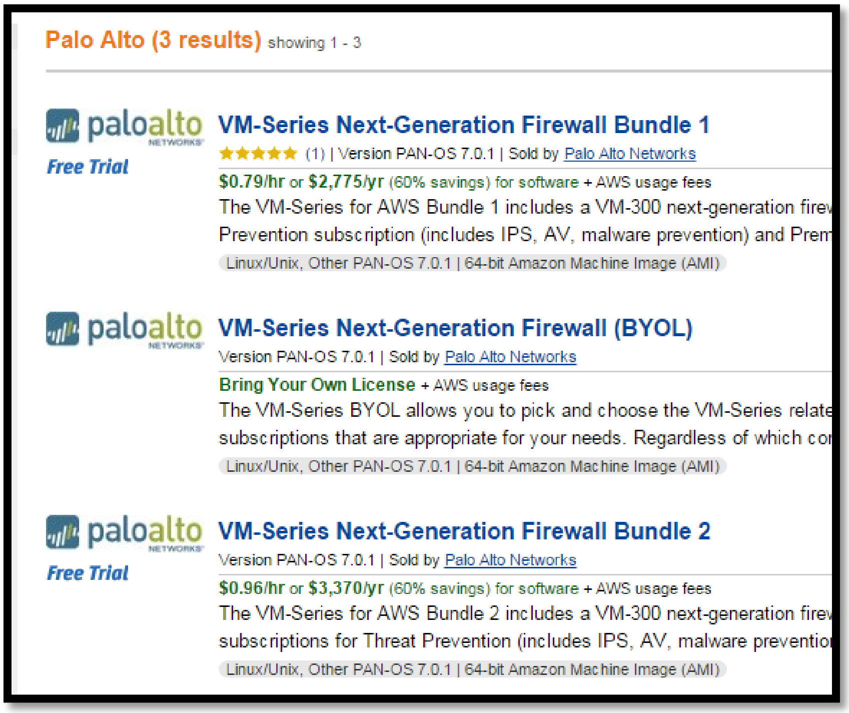
Here is the final result for the Security Groups



□	Name	Group ID	Group Name	VPC ID	Description
☑		sg-ae1674ca	VPC Managem...	vpc-c73763a2	Security Group for Management
□		sg-901270f4	VPC Public SG	vpc-c73763a2	Public Security Group
☑		sg-65117301	VPC Private SG	vpc-c73763a2	Private Security Group
□		sg-1905677d	default	vpc-c73763a2	default VPC security group

Add the Palo Alto Firewall Instance

Browse over to the AWS MarketPlace, which is located at https://aws.amazon.com/marketplace. Search for Palo Alto and select a firewall. I've selected one that is a free trial, but select the firewall that fits your requirements.



Palo Alto (3 results) showing 1 - 3

VM-Series Next-Generation Firewall Bundle 1

★★★★★ (1) | Version PAN-OS 7.0.1 | Sold by Palo Alto Networks

$0.79/hr or $2,775/yr (60% savings) for software + AWS usage fees

The VM-Series for AWS Bundle 1 includes a VM-300 next-generation firev

Prevention subscription (includes IPS, AV, malware prevention) and Prem

Linux/Unix, Other PAN-OS 7.0.1 | 64-bit Amazon Machine Image (AMI)

VM-Series Next-Generation Firewall (BYOL)

Version PAN-OS 7.0.1 | Sold by Palo Alto Networks

Bring Your Own License + AWS usage fees

The VM-Series BYOL allows you to pick and choose the VM-Series relate

subscriptions that are appropriate for your needs. Regardless of which co

Linux/Unix, Other PAN-OS 7.0.1 | 64-bit Amazon Machine Image (AMI)

VM-Series Next-Generation Firewall Bundle 2

Version PAN-OS 7.0.1 | Sold by Palo Alto Networks

$0.96/hr or $3,370/yr (60% savings) for software + AWS usage fees

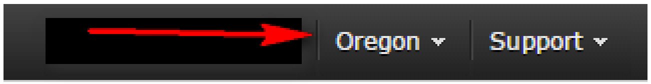
The VM-Series for AWS Bundle 2 includes a VM-300 next-generation firev

subscriptions for Threat Prevention (includes IPS, AV, malware preventio

Linux/Unix, Other PAN-OS 7.0.1 | 64-bit Amazon Machine Image (AMI)

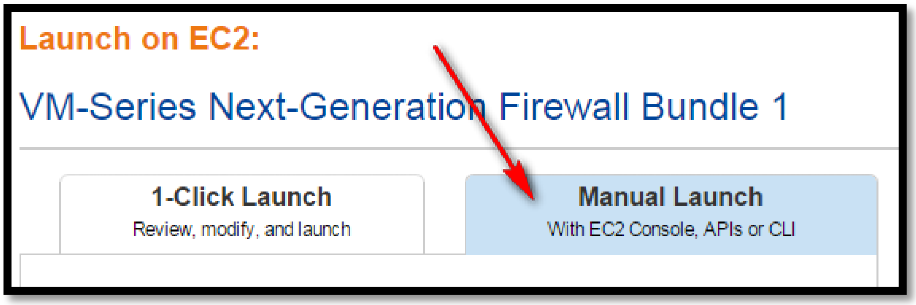
I'm going to place the PAN in the US West (Oregon) region which is where I've been doing my work.

When logged into the AWS console, you can view your region at the top left corner of your screen.

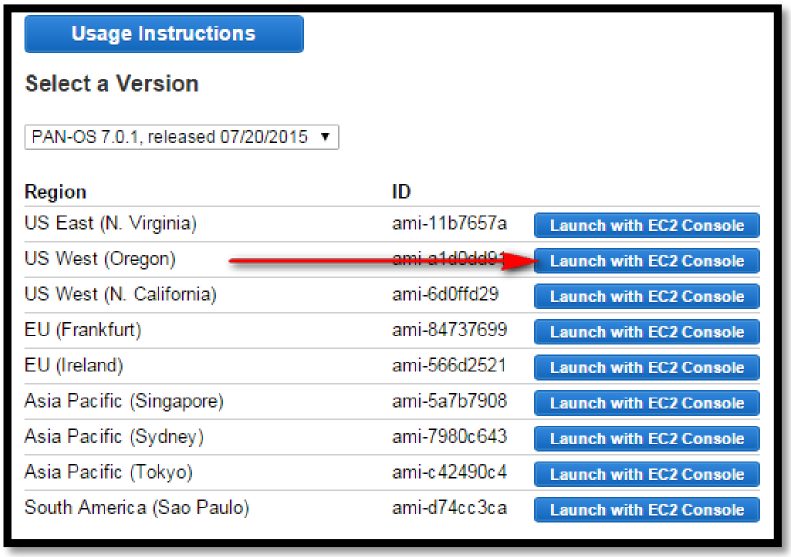


[redacted]

From the Marketplace, select **Manual Launch**. The Manual Launch option provides granular control over the PAN options.


Launch on EC2:
VM-Series Next-Generation Firewall Bundle 1
1-Click Launch
Review, modify, and launch
Manual Launch
With EC2 Console, APIs or CLI

Next, select **Launch with EC2 Console** in the proper region. In this example, I use Oregon.



Select a Version

PAN-OS 7.0.1, released 07/20/2015 ▼

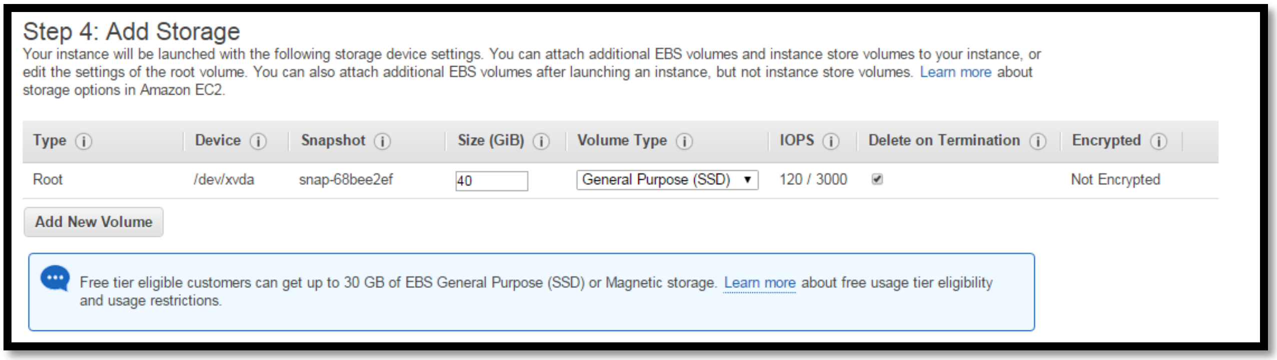
Region	ID	
US East (N. Virginia)	ami-11b7657a	Launch with EC2 Console
US West (Oregon)	ami-a1d0dd91	Launch with EC2 Console
US West (N. California)	ami-6d0ffd29	Launch with EC2 Console
EU (Frankfurt)	ami-84737699	Launch with EC2 Console
EU (Ireland)	ami-566d2521	Launch with EC2 Console
Asia Pacific (Singapore)	ami-5a7b7908	Launch with EC2 Console
Asia Pacific (Sydney)	ami-7980c643	Launch with EC2 Console
Asia Pacific (Tokyo)	ami-c42490c4	Launch with EC2 Console
South America (Sao Paulo)	ami-d74cc3ca	Launch with EC2 Console

For the Instance Type, select the option that meets your needs **and is a Palo Alto supported EC2 Instance Type. If you don't select a supported instance type, the launch will fail.**

I used a **c3.xlarge** for the Palo Alto firewall.

Configure the details of the instance. Select the proper Network, Subnet, and Enable Auto-Assign Public IP. Be sure to add the management IP (10.0.1.10) to eth0.

Click **Next: Add Storage**. I checked **Delete on Termination** because I want the EBS storage to be terminated along with the instance.



Step 4: Add Storage

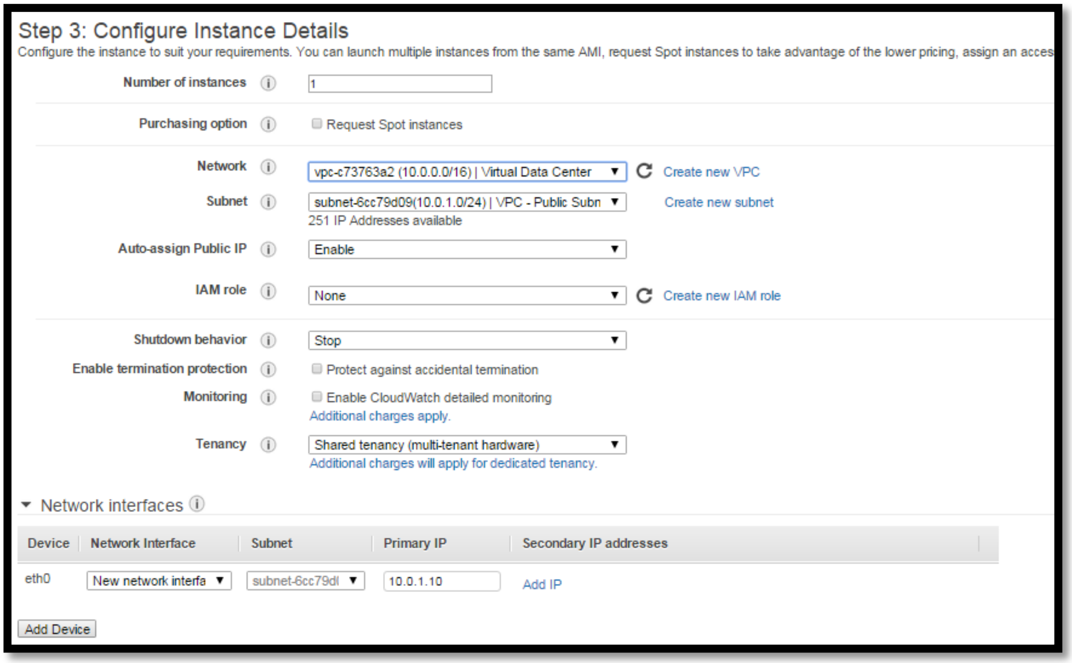
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/xvda	snap-68bee2ef	40	General Purpose (SSD)	120 / 3000	☑	Not Encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Click **Next: Tag Instance.** Click **Next: Configure Security Group.**

Click **Select an existing security group**, and then select **VPC Management SG**. Click the **Review and Launch** button.



Step 3: Configure Instance Details

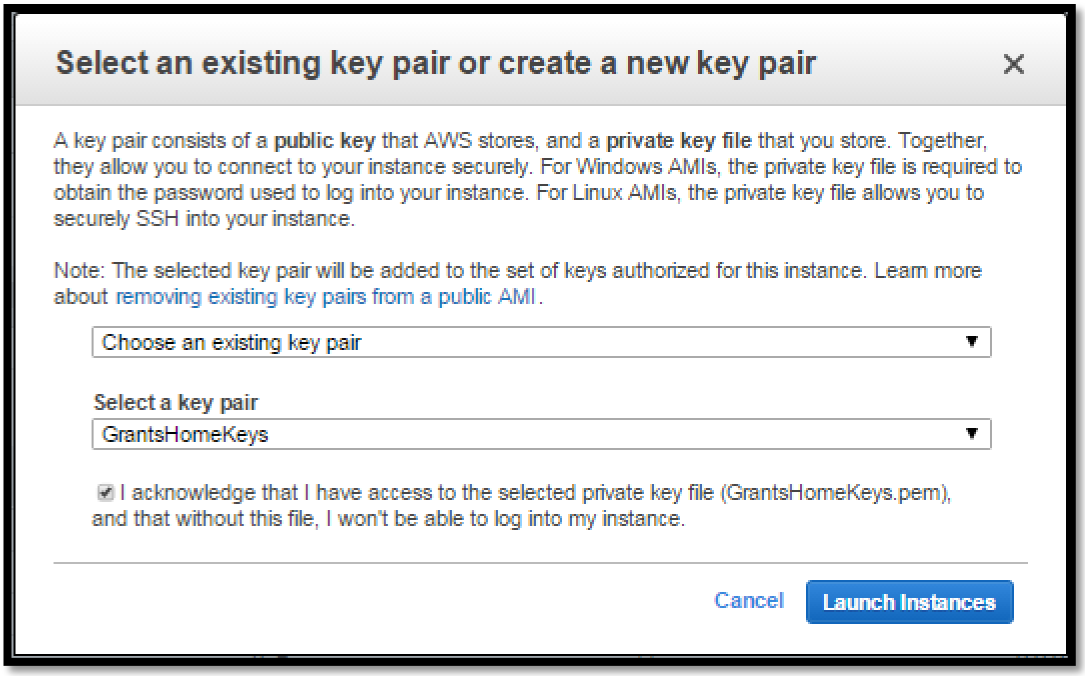
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an acces

Number of instances	1
Purchasing option	□ Request Spot instances
Network	vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center
Subnet	subnet-6cc79d09(10.0.1.0/24) | VPC - Public Subn 251 IP Addresses available
Auto-assign Public IP	Enable
IAM role	None
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared tenancy (multi-tenant hardware) Additional charges will apply for dedicated tenancy.

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfa	subnet-6cc79d(	10.0.1.10	Add IP

Click **Launch.** Select your key pair, select the checkbox and then click **Launch Instances**.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

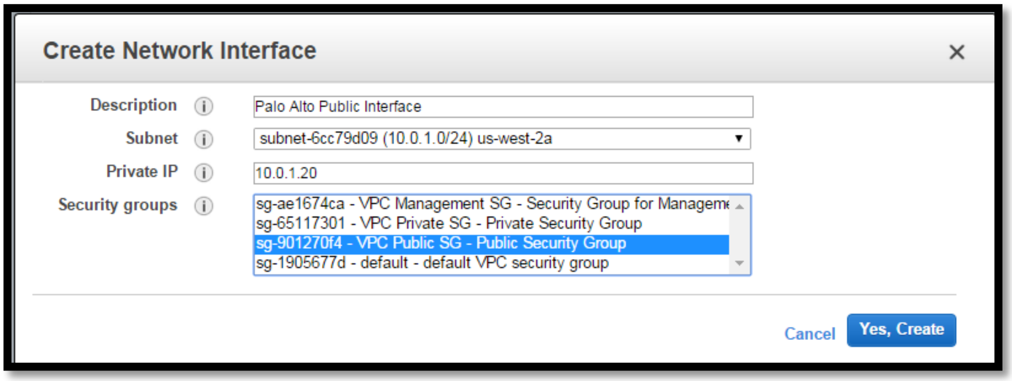
Choose an existing key pair

Select a key pair: GrantsHomeKeys

☑ I acknowledge that I have access to the selected private key file (GrantsHomeKeys.pem), and that without this file, I won't be able to log into my instance.

Back at the EC2 Dashboard, the new Palo Alto instance will be launching. When complete, select the new instance and view the details.

It's time to add two additional interfaces to the firewall. Browse to **EC2 > Network Interfaces** and select **Create Network Interface.** Do this two times, once for the Public interface and one form the Private interface. Assign the proper Private IP and Security Group for each.



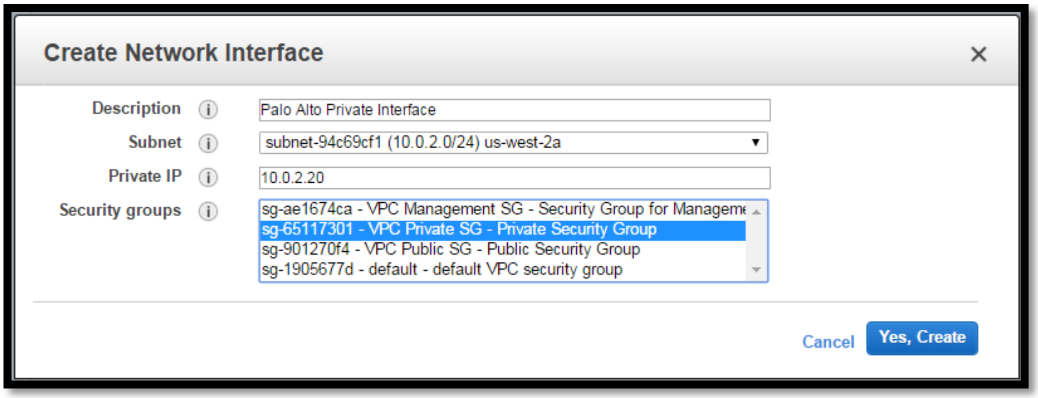
Create Network Interface

Description: Palo Alto Public Interface

Subnet: subnet-6cc79d09 (10.0.1.0/24) us-west-2a

Private IP: 10.0.1.20

Security groups:
- sg-ae1674ca - VPC Management SG - Security Group for Manageme
- sg-65117301 - VPC Private SG - Private Security Group
- sg-901270f4 - VPC Public SG - Public Security Group
- sg-1905677d - default - default VPC security group



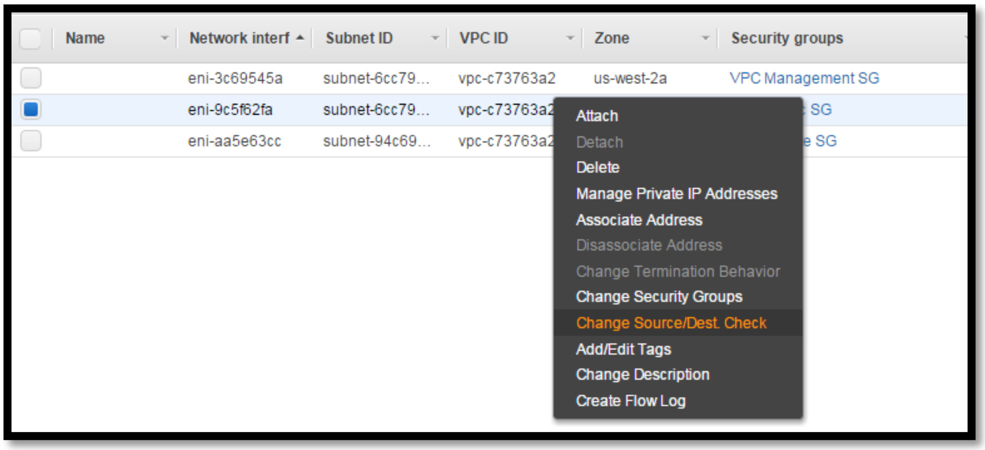
Description: Palo Alto Private Interface

Subnet: subnet-94c69cf1 (10.0.2.0/24) us-west-2a

Private IP: 10.0.2.20

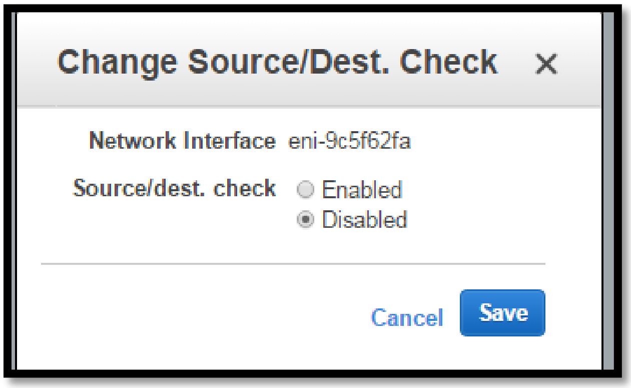
Security groups:
- sg-ae1674ca - VPC Management SG - Security Group for Manageme
- sg-65117301 - VPC Private SG - Private Security Group
- sg-901270f4 - VPC Public SG - Public Security Group
- sg-1905677d - default - default VPC security group

For the Public and Private interface, right-click and select **Change Source/Dest. Check.**



	Name	Network interf	Subnet ID	VPC ID	Zone	Security groups
□		eni-3c69545a	subnet-6cc79...	vpc-c73763a2	us-west-2a	VPC Management SG
■		eni-9c5f62fa	subnet-6cc79...	vpc-c73763a2		SG
□		eni-aa5e63cc	subnet-94c69...	vpc-c73763a2		e SG

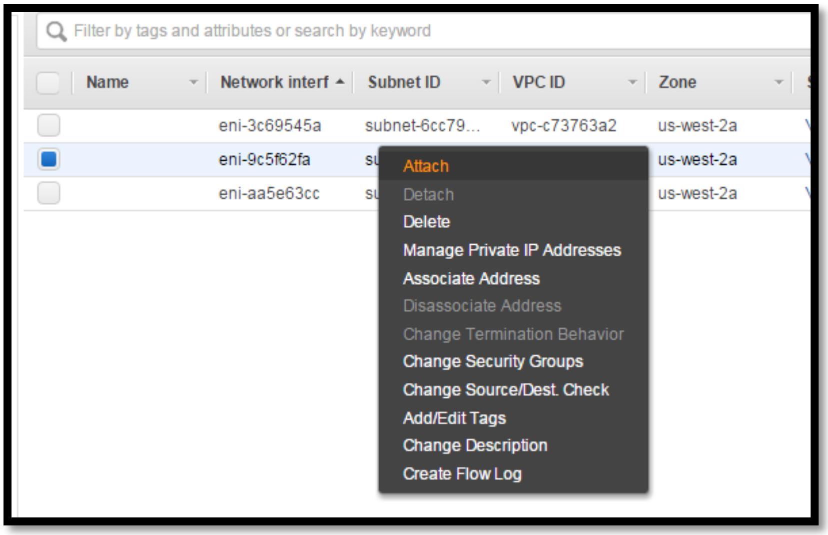
Disable the Source/dest. check for the Public and Private interface.



Network Interface eni-9c5f62fa

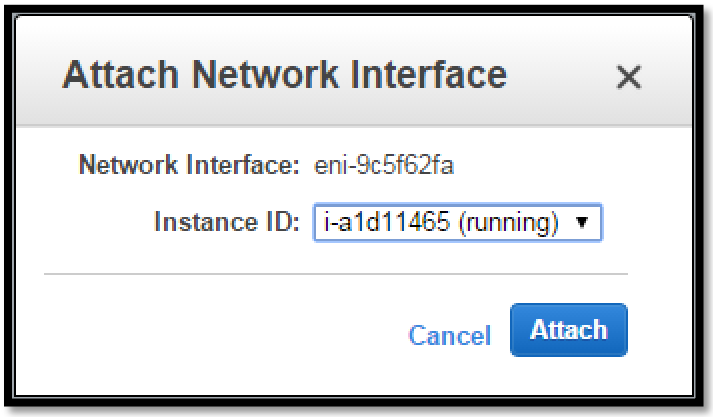
Source/dest. check ○ Enabled
● Disabled

Attach the newly created Public and Private interface to the firewall by right clicking on the interface and selecting **Attach**.


Filter by tags and attributes or search by keyword
Attach
Detach
Delete
Manage Private IP Addresses
Associate Address
Disassociate Address
Change Termination Behavior
Change Security Groups
Change Source/Dest. Check
Add/Edit Tags
Change Description
Create Flow Log

	Name	Network interf	Subnet ID	VPC ID	Zone
□		eni-3c69545a	subnet-6cc79...	vpc-c73763a2	us-west-2a
☑		eni-9c5f62fa	su		us-west-2a
□		eni-aa5e63cc	su		us-west-2a

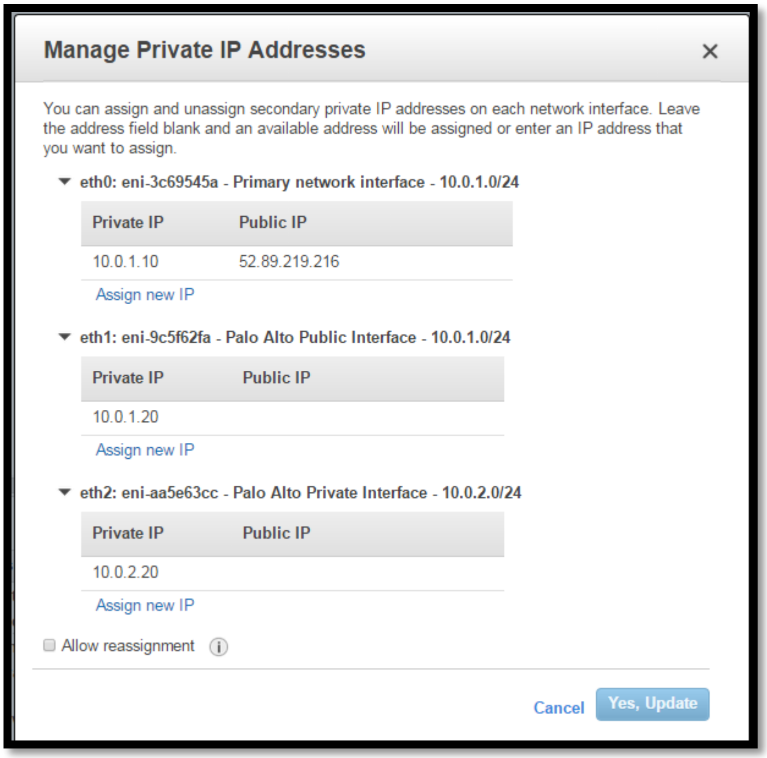
Attach the interfaces to the firewall Instance. <u>Don’t forget to do both the Public and Private Interface</u>.



Network Interface: eni-9c5f62fa

Instance ID: i-a1d11465 (running) ▼

I can view the firewall Private IP addresses by right-clicking my EC2 Palo Alto instance and selecting **Manage Private IP Addresses**.



Manage Private IP Addresses ×

You can assign and unassign secondary private IP addresses on each network interface. Leave the address field blank and an available address will be assigned or enter an IP address that you want to assign.

▼ eth0: eni-3c69545a - Primary network interface - 10.0.1.0/24

Private IP	Public IP
10.0.1.10	52.89.219.216

Assign new IP

▼ eth1: eni-9c5f62fa - Palo Alto Public Interface - 10.0.1.0/24

Private IP	Public IP
10.0.1.20	

Assign new IP

▼ eth2: eni-aa5e63cc - Palo Alto Private Interface - 10.0.2.0/24

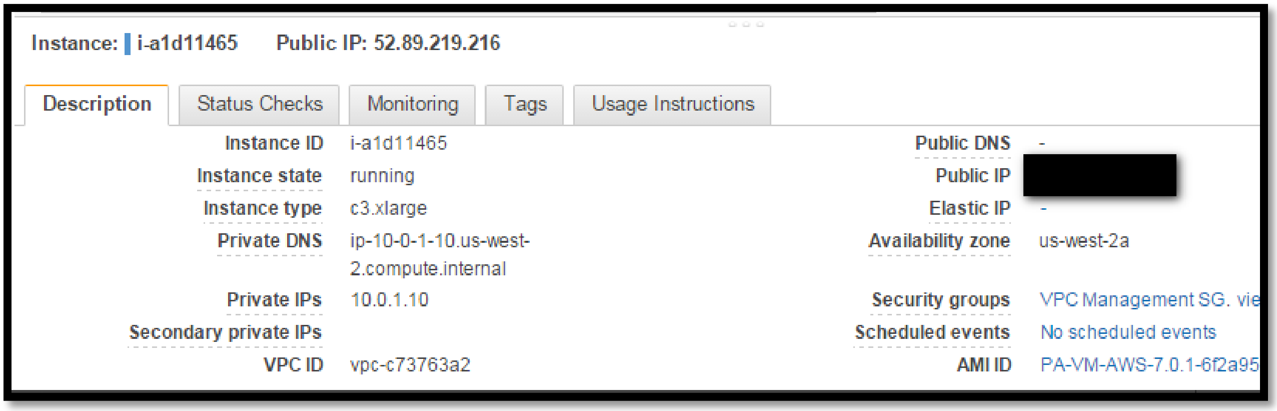
Private IP	Public IP
10.0.2.20	

Assign new IP

□ Allow reassignment

Configure the Palo Alto Firewall

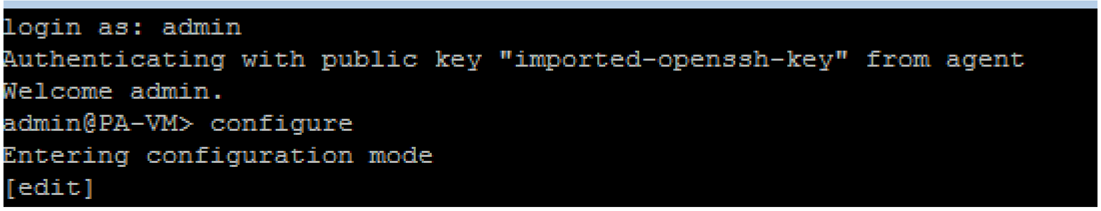
View the instance details of the firewall and get the Public IP.



Instance: i-a1d11465 Public IP: 52.89.219.216

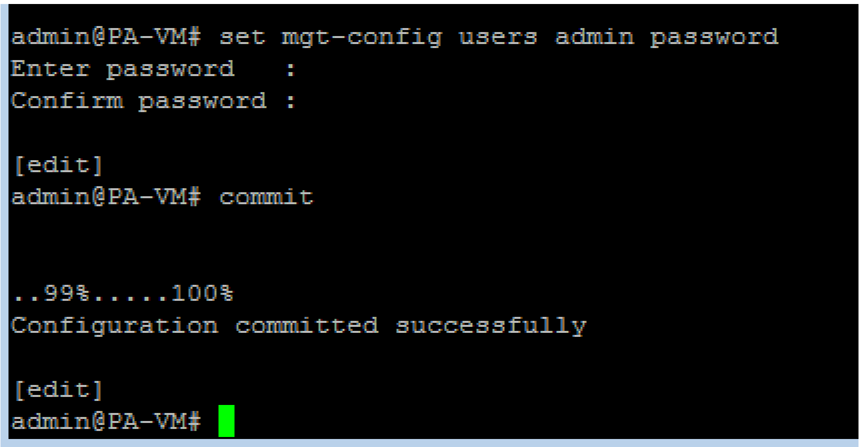
Instance ID	i-a1d11465	Public DNS	-
Instance state	running	Public IP	[redacted]
Instance type	c3.xlarge	Elastic IP	-
Private DNS	ip-10-0-1-10.us-west-2.compute.internal	Availability zone	us-west-2a
Private IPs	10.0.1.10	Security groups	VPC Management SG. vie
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-c73763a2	AMI ID	PA-VM-AWS-7.0.1-6f2a95

Open a SSH client that is configured with the proper Key Pair, and connect via SSH to the PAN's Public IP address - it's time to reset the admin password. Login as admin, and type configure at the prompt.



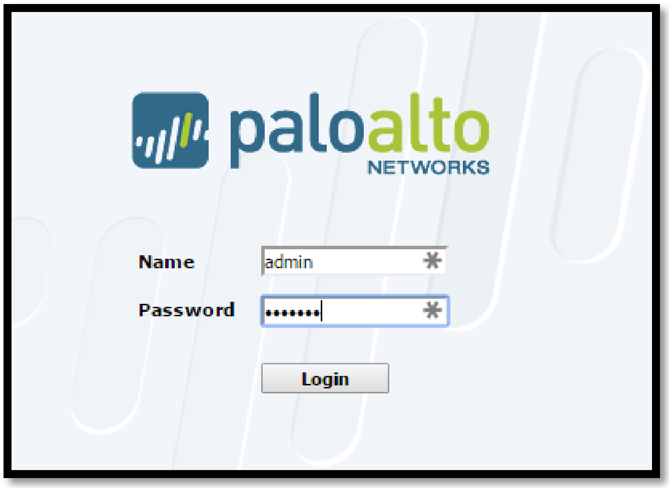
```
login as: admin
Authenticating with public key "imported-openssh-key" from agent
Welcome admin.
admin@PA-VM> configure
Entering configuration mode
[edit]
```

Set the admin password and commit the change



```
admin@PA-VM# set mgt-config users admin password
Enter password   :
Confirm password :

[edit]
admin@PA-VM# commit


..99%.....100%
Configuration committed successfully

[edit]
admin@PA-VM#
```

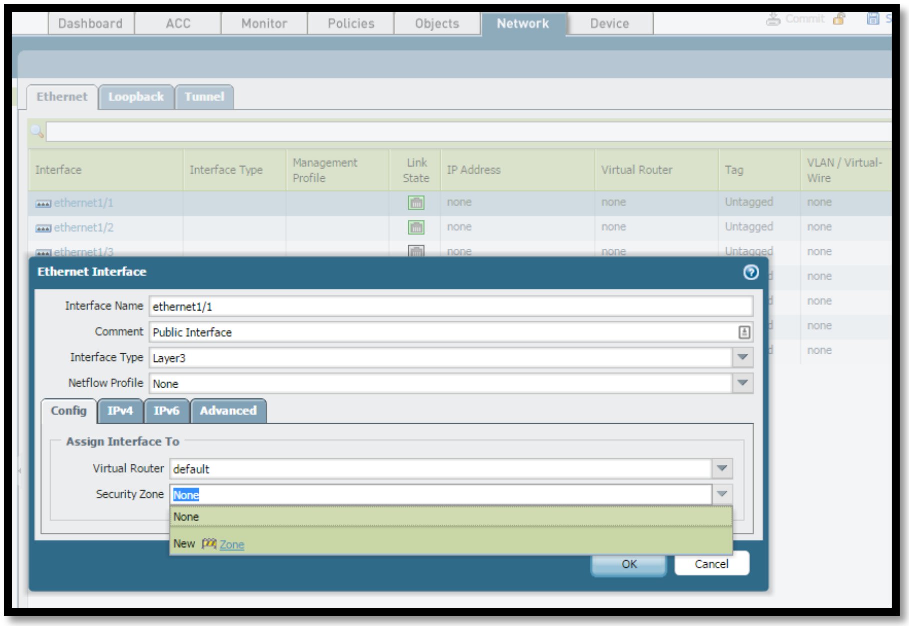
Login via HTTPS via your Internet browser using the new admin password.



Name: admin

Password: •••••••

It’s time to setup the interfaces on the Palo Alto firewall by selecting **Network** and then selecting **ethernet1/1**. Configure ethernet1/1 as seen below. When adding the Security Zone, select new zone.



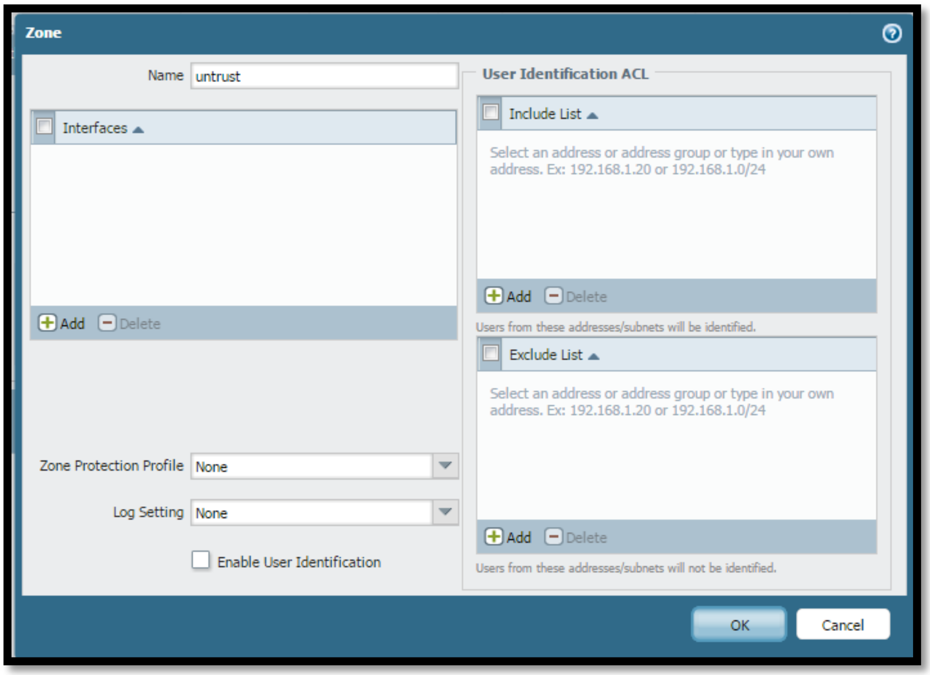
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire
ethernet1/1				none	none	Untagged	none
ethernet1/2				none	none	Untagged	none
ethernet1/3				none	none	Untagged	none

Ethernet Interface

Interface Name: ethernet1/1
Comment: Public Interface
Interface Type: Layer3
Netflow Profile: None

Assign Interface To
Virtual Router: default
Security Zone: None

Name the new zone **untrust** and select **OK**.


Zone

Name: untrust

Zone Protection Profile: None
Log Setting: None
□ Enable User Identification

User Identification ACL

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

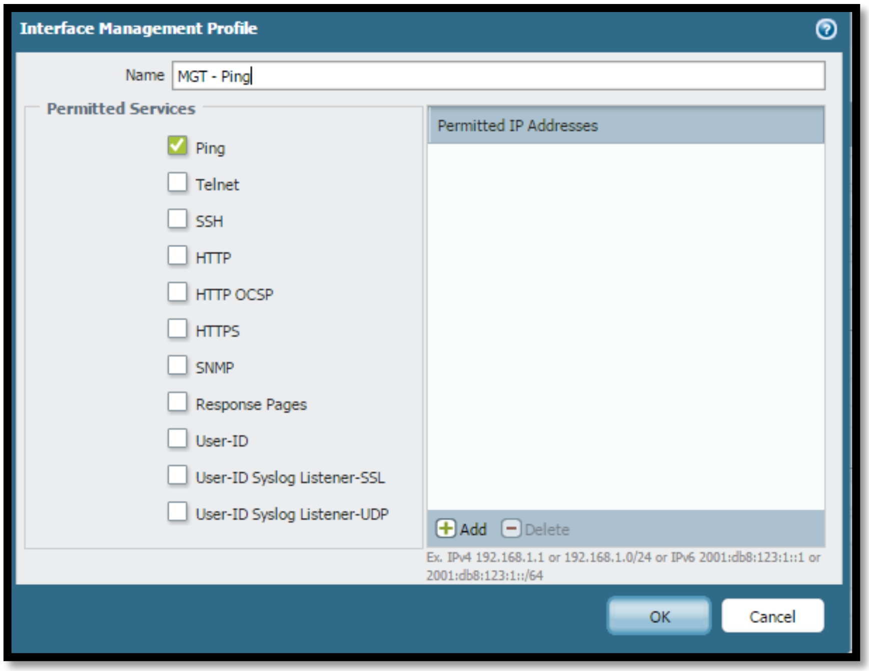
Users from these addresses/subnets will be identified.

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Select the IPv4 tab and select **DHCP Client**.

Select the **Advanced** tab and then the **Other Info** tab. Select **Management Profile** and **New Management Profile**. Create a new management profile for the Ping service.



Interface Management Profile

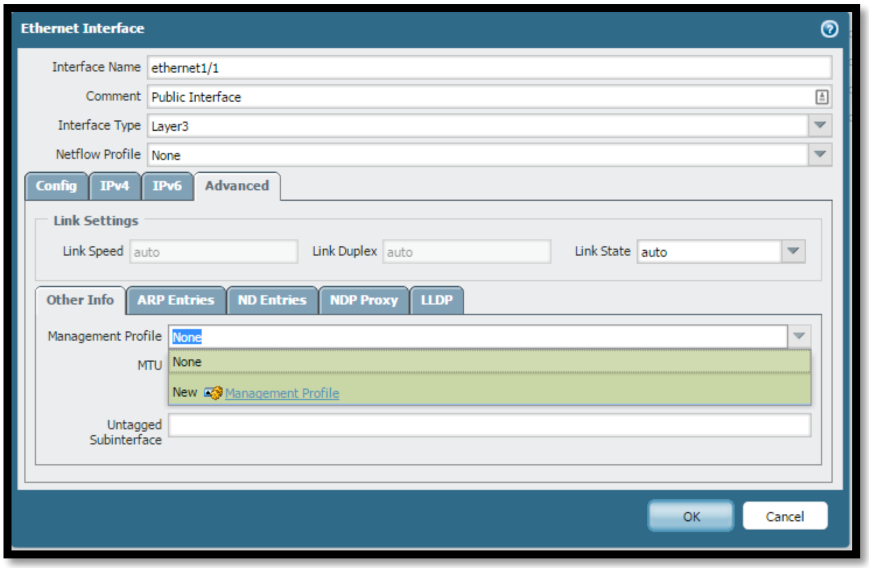
Name: MGT - Ping

Permitted Services

- ☑ Ping
- □ Telnet
- □ SSH
- □ HTTP
- □ HTTP OCSP
- □ HTTPS
- □ SNMP
- □ Response Pages
- □ User-ID
- □ User-ID Syslog Listener-SSL
- □ User-ID Syslog Listener-UDP

Permitted IP Addresses

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64



Ethernet Interface

Interface Name: ethernet1/1

Comment: Public Interface

Interface Type: Layer3

Netflow Profile: None

Link Settings

Link Speed: auto

Link Duplex: auto

Link State: auto

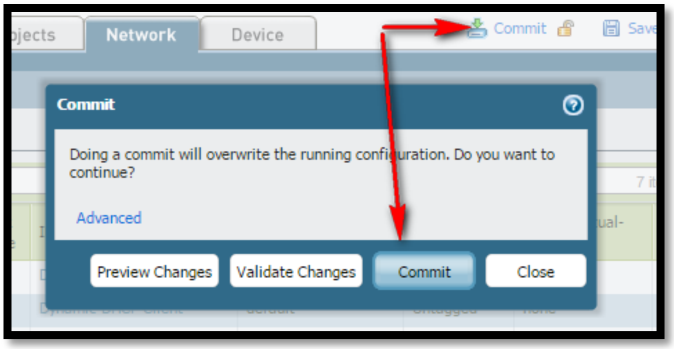
Management Profile: None

MTU

Untagged Subinterface

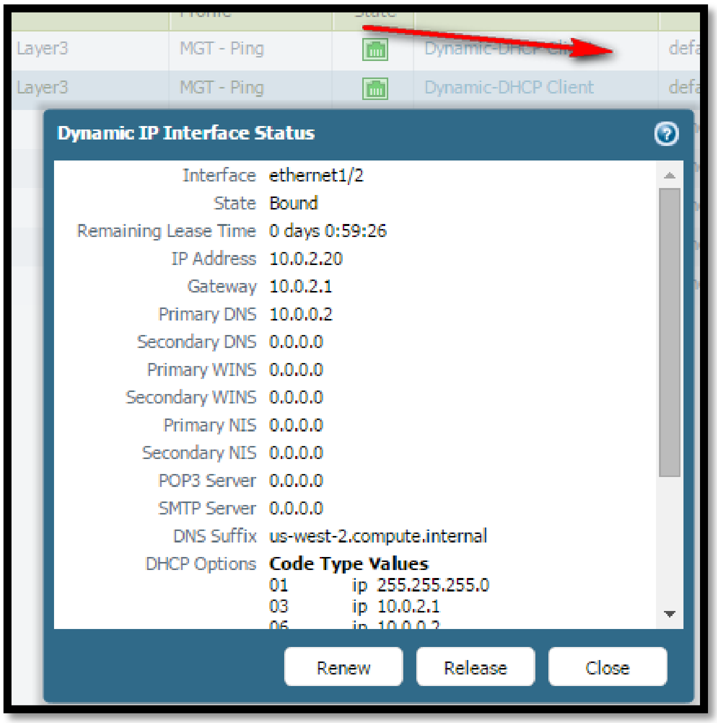
Select **OK** and then **OK** again.

Select **ethernet1/2** and configure this interface the same way for the private network. This time, however, create a new Security Zone named trust. Uncheck **automatically create default route pointing to default gateway provided by server**. Add the MGT-Ping management profile and select OK and then OK again. Commit the changes



Doing a commit will overwrite the running configuration. Do you want to continue?

By selecting just left of **Dynamic-DHCP Client** you can view the interface details

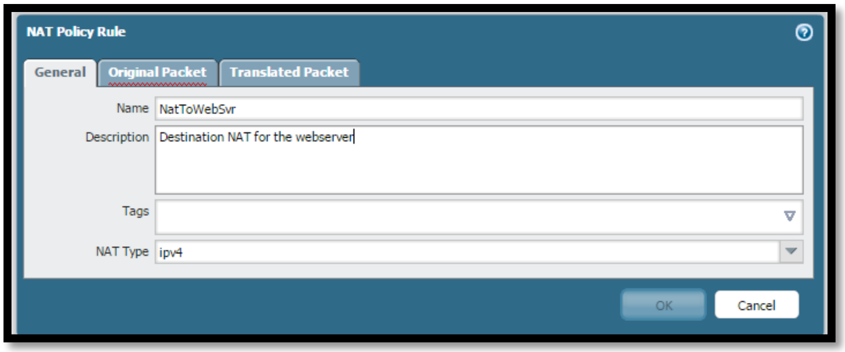


```
         Interface  ethernet1/2
             State  Bound
Remaining Lease Time  0 days 0:59:26
        IP Address  10.0.2.20
           Gateway  10.0.2.1
       Primary DNS  10.0.0.2
     Secondary DNS  0.0.0.0
      Primary WINS  0.0.0.0
    Secondary WINS  0.0.0.0
       Primary NIS  0.0.0.0
     Secondary NIS  0.0.0.0
       POP3 Server  0.0.0.0
       SMTP Server  0.0.0.0
        DNS Suffix  us-west-2.compute.internal
      DHCP Options  Code Type Values
                    01       ip  255.255.255.0
                    03       ip  10.0.2.1
                    06       ip  10.0.0.2
```

Creating the Source and Destination NAT rules

Select **Policies > NAT > Add**

Create the Destination NAT to the Webserver



Name NatToWebSvr

Description Destination NAT for the webserver

Tags

NAT Type ipv4

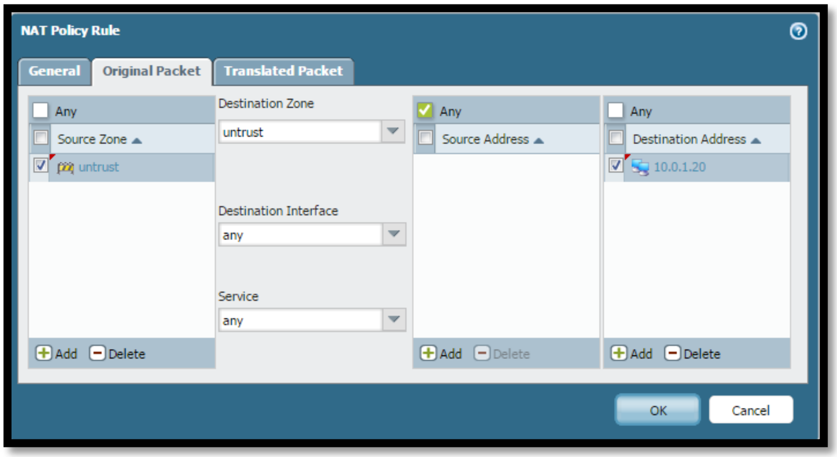
Source Zone: untrust

Destination Zone: untrust

Source Address: Any

Destination Address: 10.0.1.20

The destination address is the public IP of the public interface.



☐ Any

☐ Source Zone ▲

☑ untrust

Destination Zone untrust

Destination Interface any

Service any

☑ Any

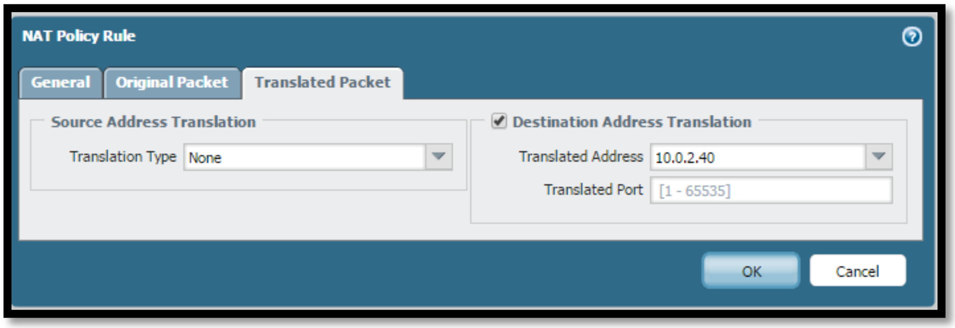
☐ Source Address ▲

☐ Any

☐ Destination Address ▲

☑ 10.0.1.20

Add the destination address translation. The translated address is the IP address of the web server.



Source Address Translation

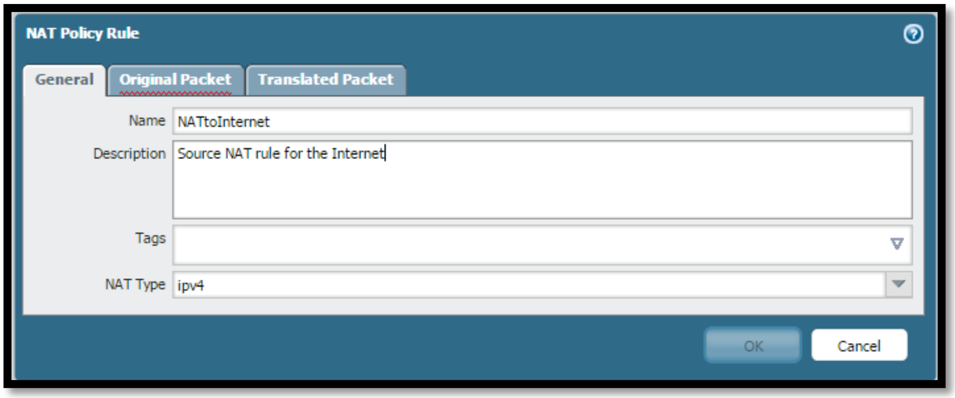
Translation Type None

☑ Destination Address Translation

Translated Address 10.0.2.40

Translated Port [1 - 65535]

Now add a source NAT for the web server.

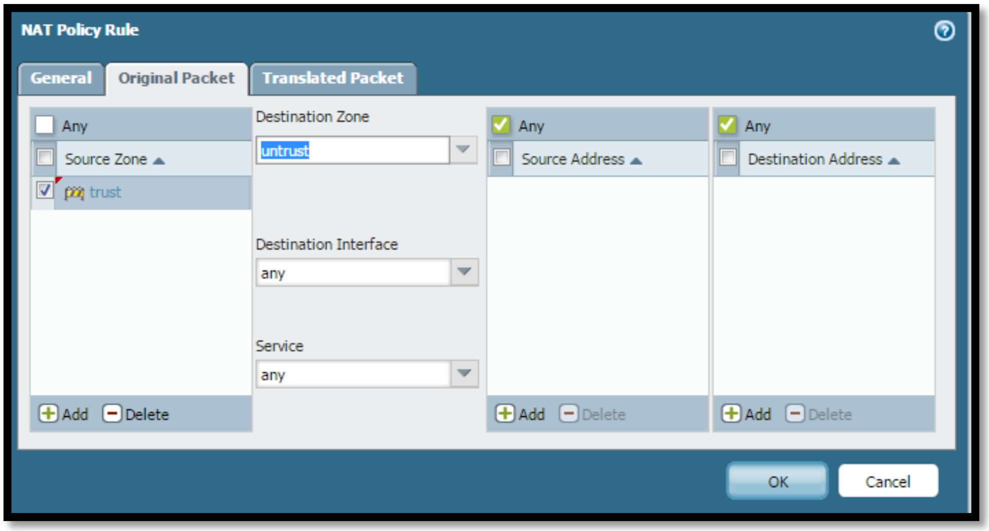


Name: NATtoInternet

Description: Source NAT rule for the Internet

Tags:

NAT Type: ipv4



☐ Any

Source Zone

☑ trust

Destination Zone: untrust

Destination Interface: any

Service: any

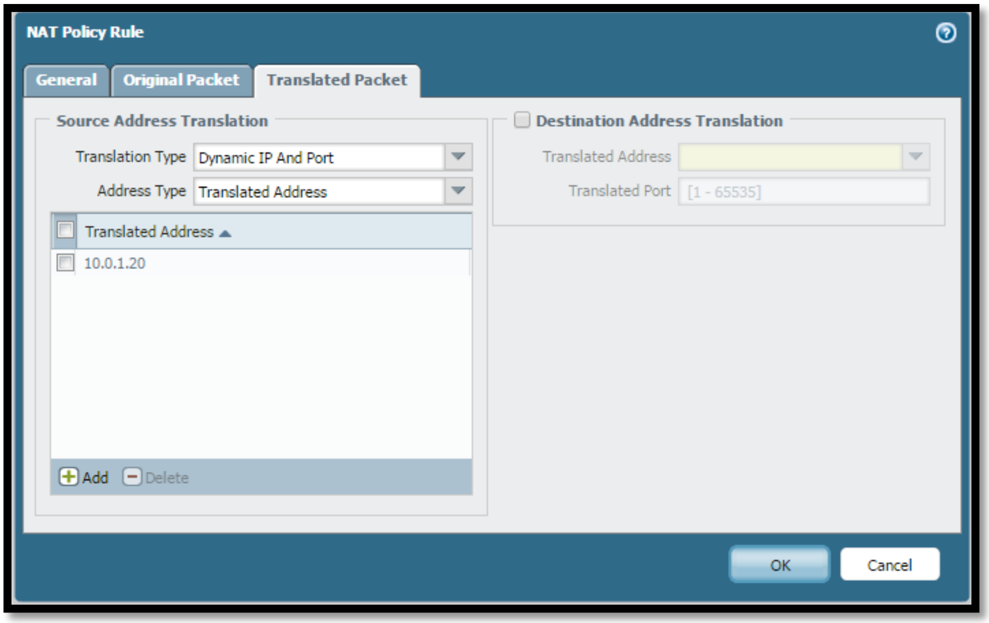
☑ Any

Source Address

☑ Any

Destination Address

Add the Translated Packet rule using the public interface of the Palo Alto firewall, which is 10.0.1.20 in this tutorial.



Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Translated Address

□ Translated Address ▲
□ 10.0.1.20

Add Delete

□ Destination Address Translation

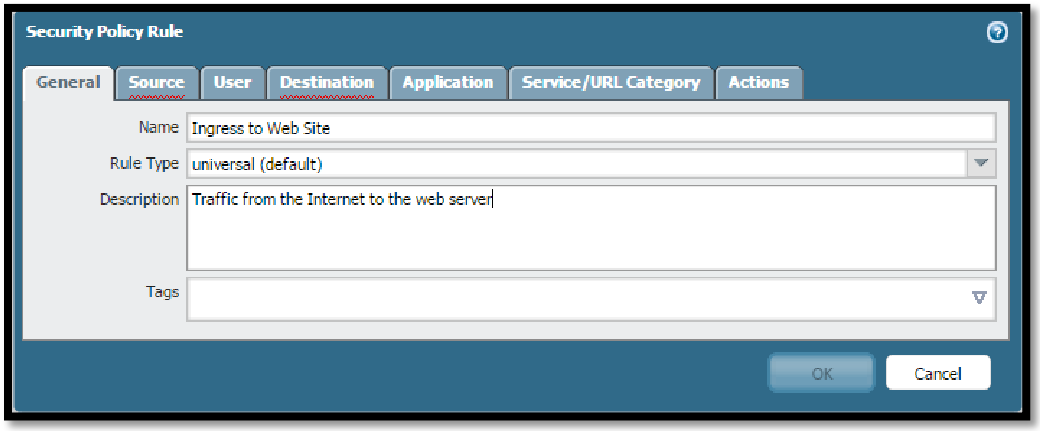
Translated Address

Translated Port [1 - 65535]

Commit the changes

Adding the Security Policies

Browse to **Policies > Security** and click Add. Begin adding the first rule to allow traffic to the web server.

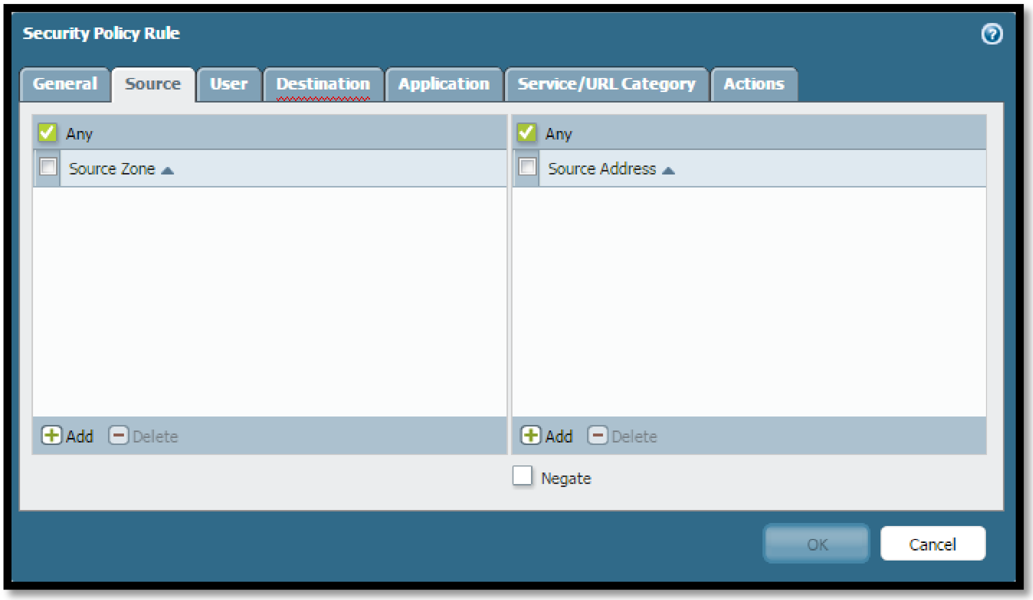


Name: Ingress to Web Site

Rule Type: universal (default)

Description: Traffic from the Internet to the web server

Tags



Security Policy Rule

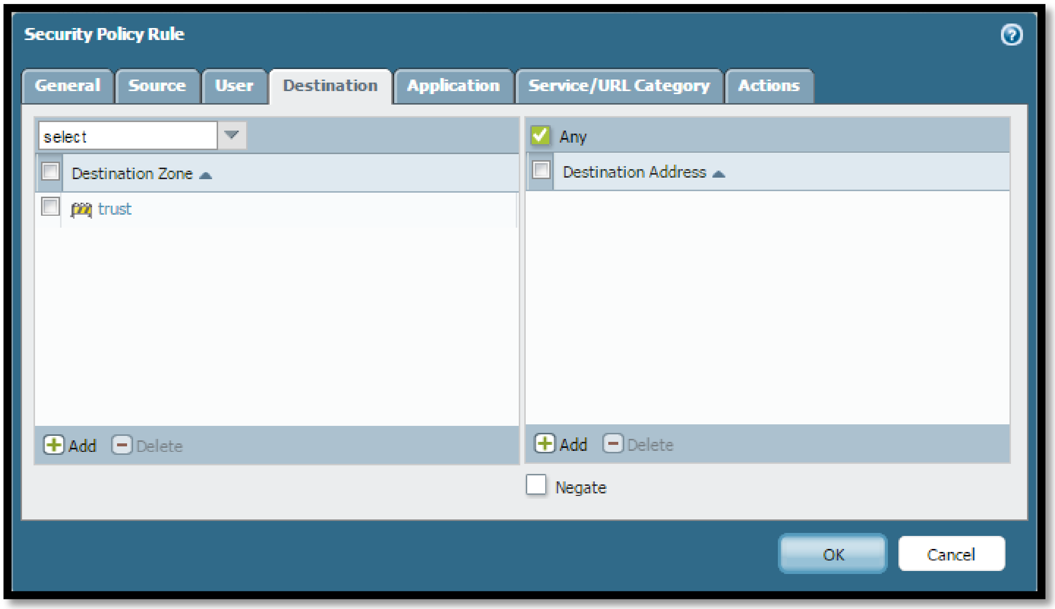
☑ Any

□ Source Zone ▲

☑ Any

□ Source Address ▲

□ Negate



Security Policy Rule

select

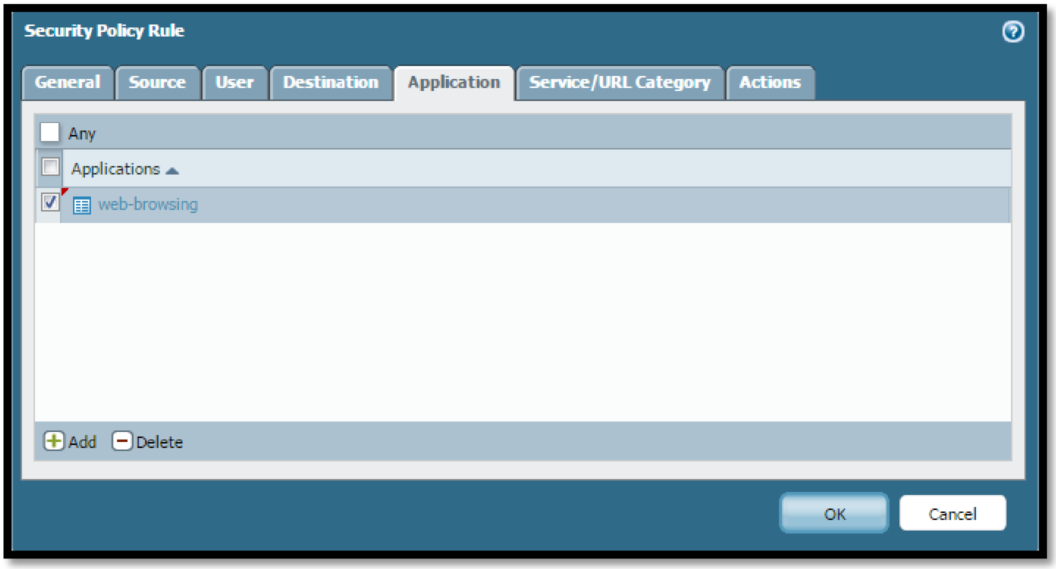
□ Destination Zone ▲

□ trust

☑ Any

□ Destination Address ▲

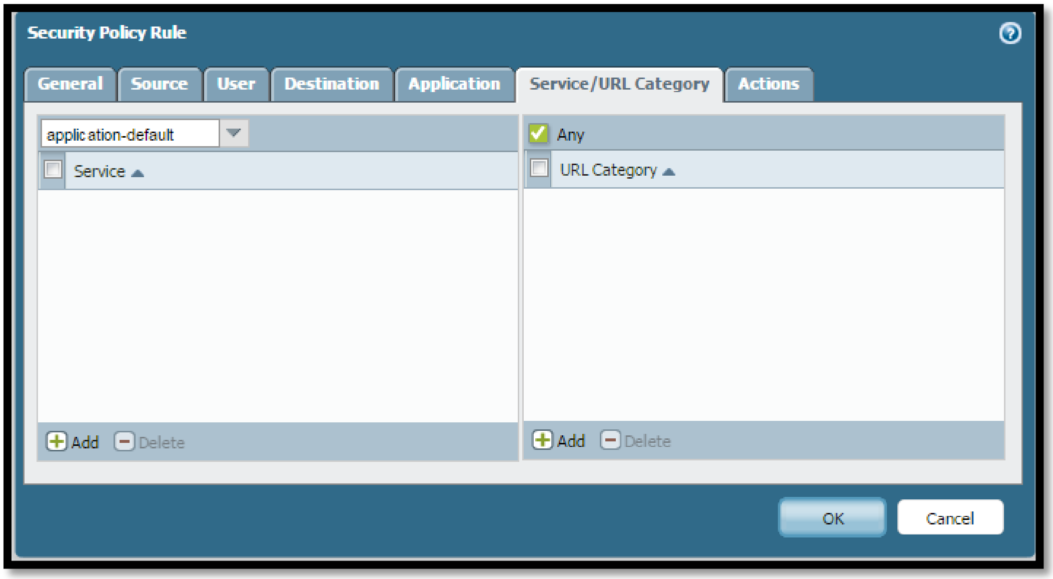
□ Negate



□ Any

□ Applications

☑ web-browsing

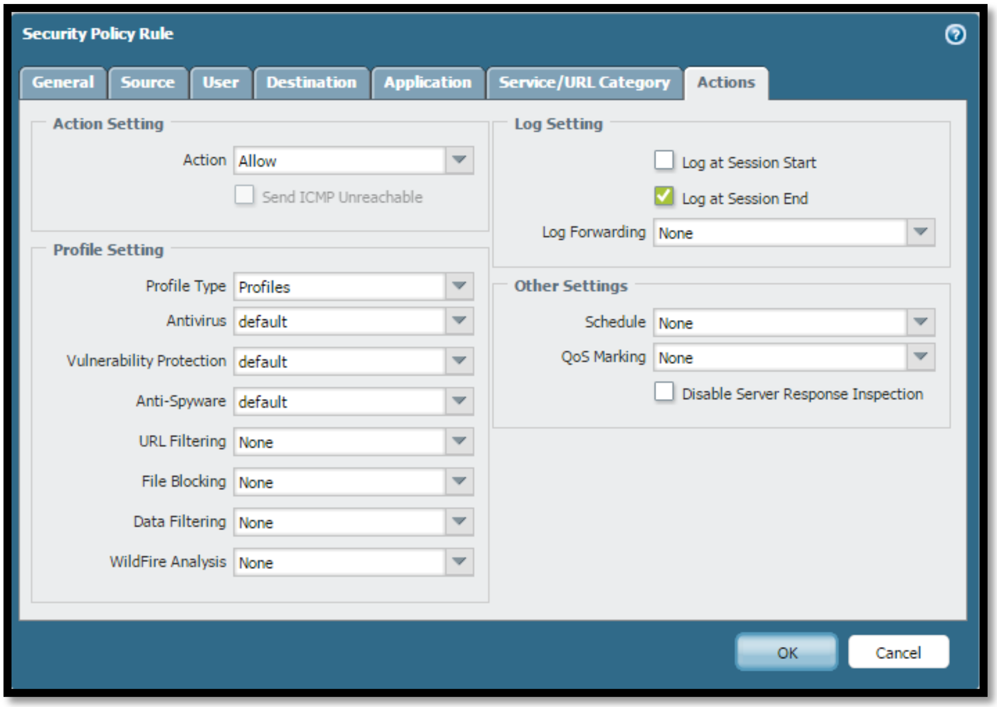


applic ation-default

□ Service

☑ Any

□ URL Category



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: default

Anti-Spyware: default

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

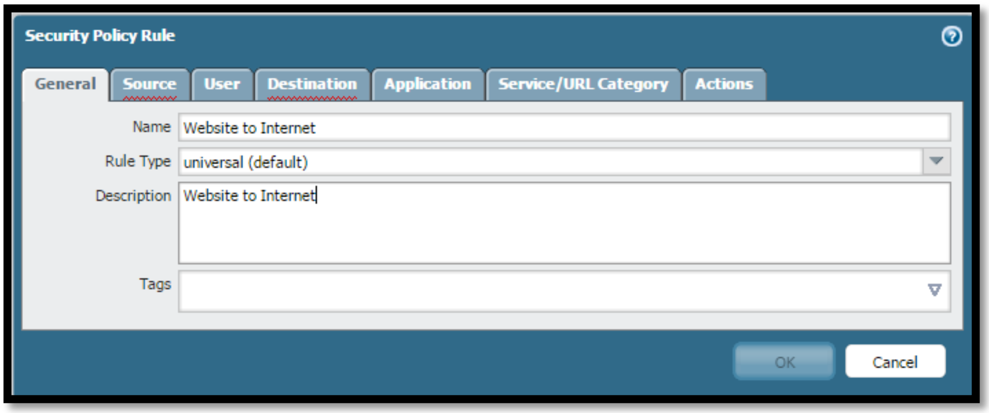
Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

Now let’s add a rule to allow the web server to the Internet

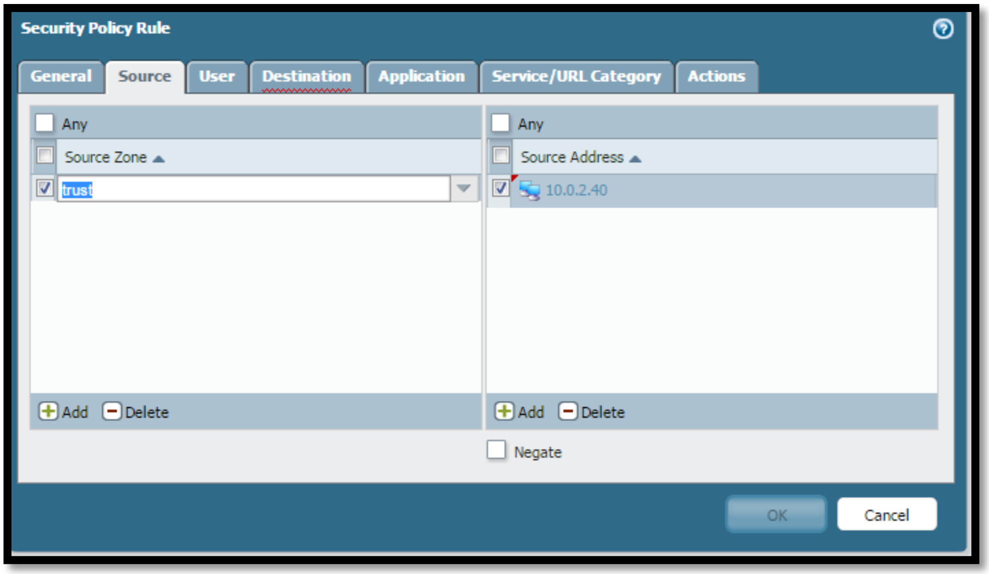


Name: Website to Internet

Rule Type: universal (default)

Description: Website to Internet

Tags:



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

□ Any

□ Source Zone ▲

☑ trust

Add | Delete

□ Any

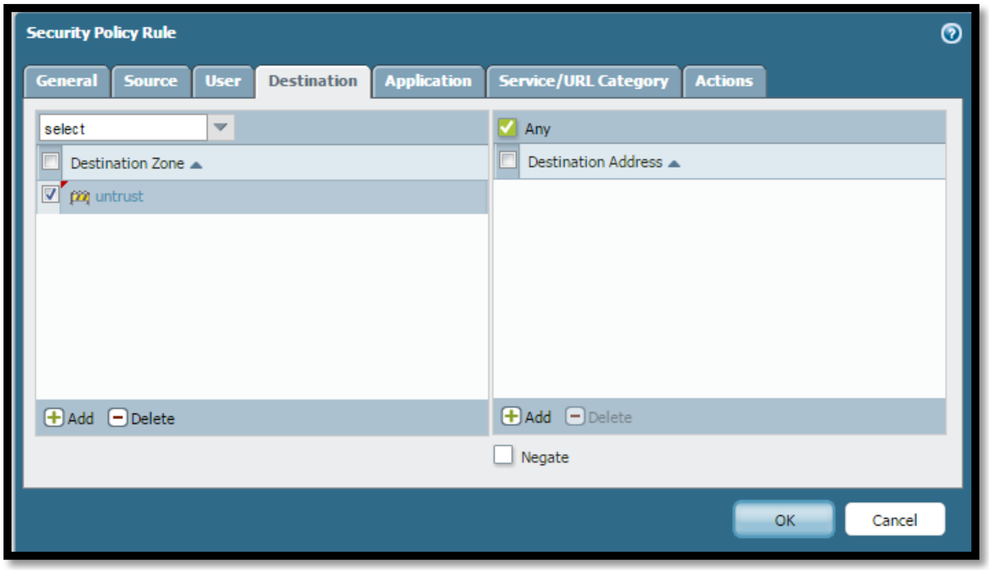
□ Source Address ▲

☑ 10.0.2.40

Add | Delete

□ Negate

OK | Cancel



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

select

□ Destination Zone ▲

☑ untrust

Add | Delete

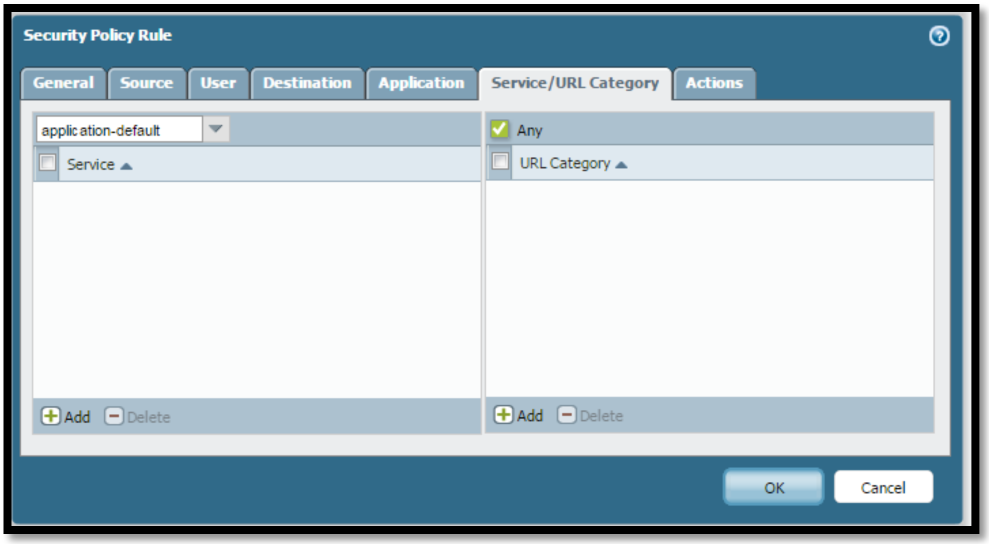
☑ Any

□ Destination Address ▲

Add | Delete

□ Negate

OK | Cancel

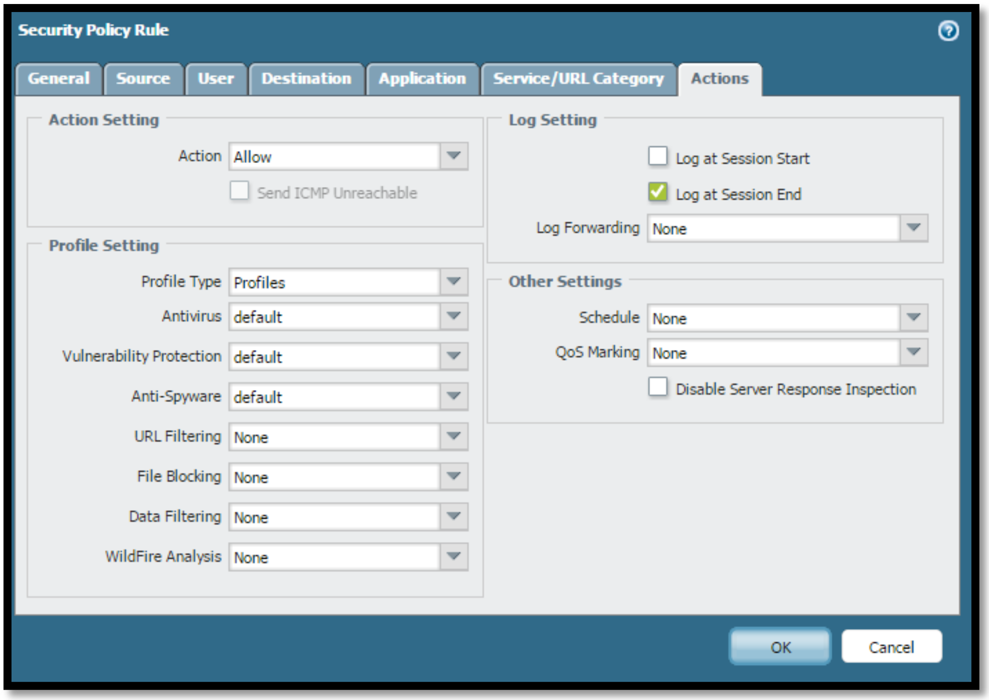


application-default

□ Service

☑ Any

□ URL Category



Action Setting

Action: Allow

□ Send ICMP Unreachable

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: default

Anti-Spyware: default

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: None

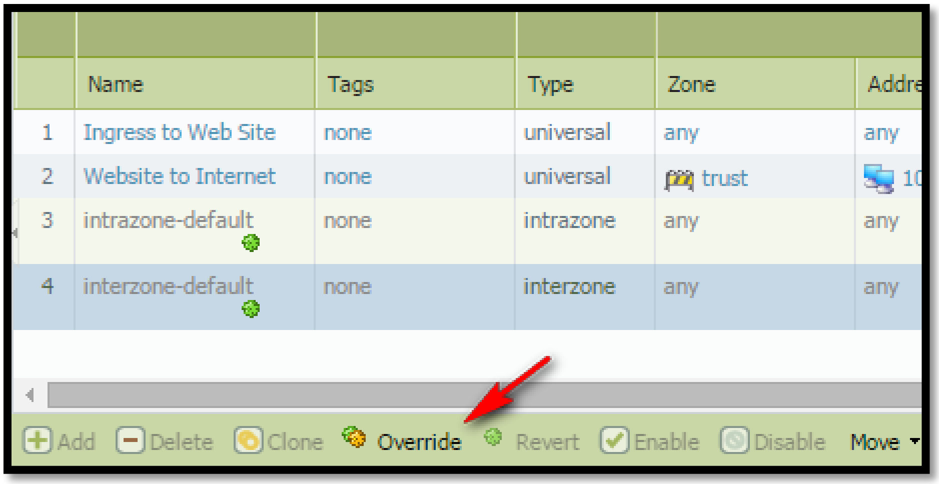
Other Settings

Schedule: None

QoS Marking: None

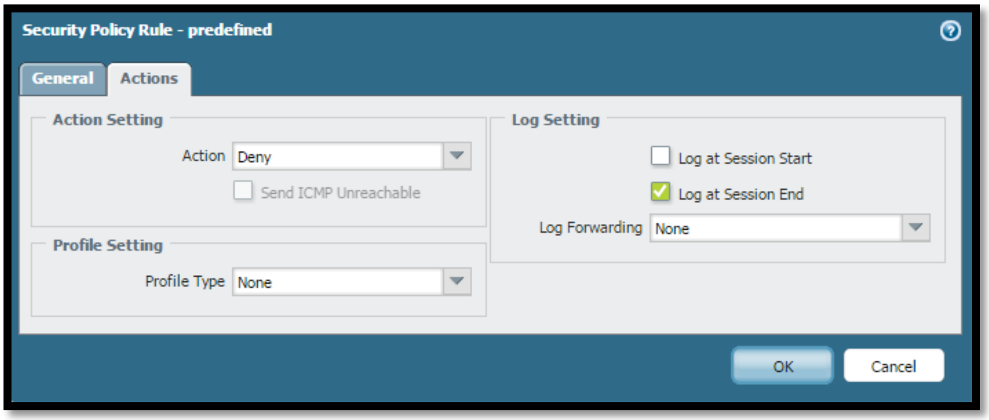
□ Disable Server Response Inspection

Now let’s adjust the implicit deny rule to log traffic that is getting blocked. Click on the **interzone-default** rule and click **Override**.



	Name	Tags	Type	Zone	Addre
1	Ingress to Web Site	none	universal	any	any
2	Website to Internet	none	universal	trust	10
3	intrazone-default	none	intrazone	any	any
4	interzone-default	none	interzone	any	any

Select the **Actions** tab and check **Log at Session End**



Security Policy Rule - predefined

Action Setting

Action: Deny

□ Send ICMP Unreachable

Profile Setting

Profile Type: None

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding: None

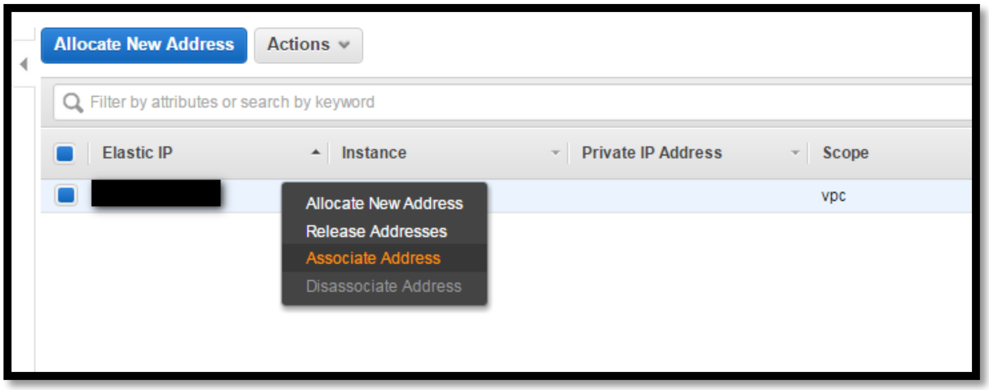
Finally, **Commit** the changes.

Step 3 – Creating the EC2 Linux servers behind the PAN

We need to create an Elastic IP for the web server's real-world IP address that will point to the Public interface of the Palo Alto (10.0.1.20).

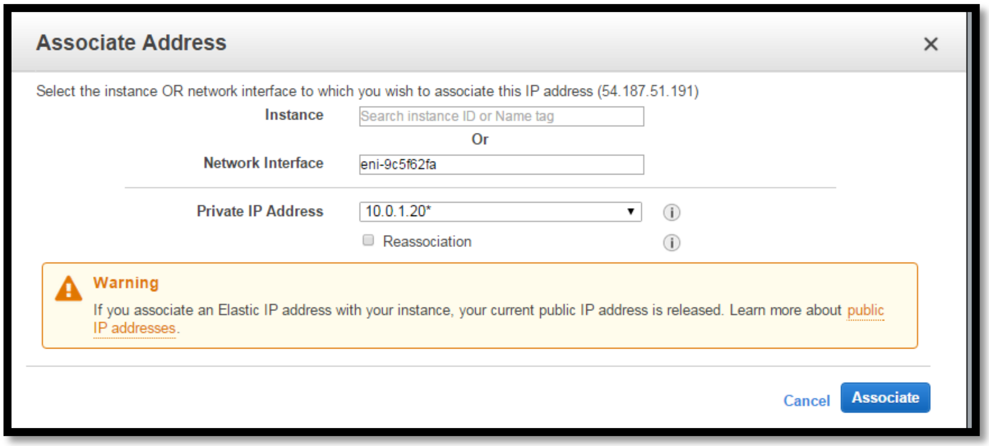
Browse to **EC2 > Elastic IPs** and select **Allocate New Address** and work through the instructions.

Then right click the new Elastic IP and select **Assocaite Address**.



Elastic IP	Instance	Private IP Address	Scope
[redacted]			vpc

Select the network interface that matches the public side of the PAN and ensure the Private IP matches the IP for the public side of the PAN.



Associate Address

Select the instance OR network interface to which you wish to associate this IP address (54.187.51.191)

Instance: Search instance ID or Name tag

Or

Network Interface: eni-9c5f62fa

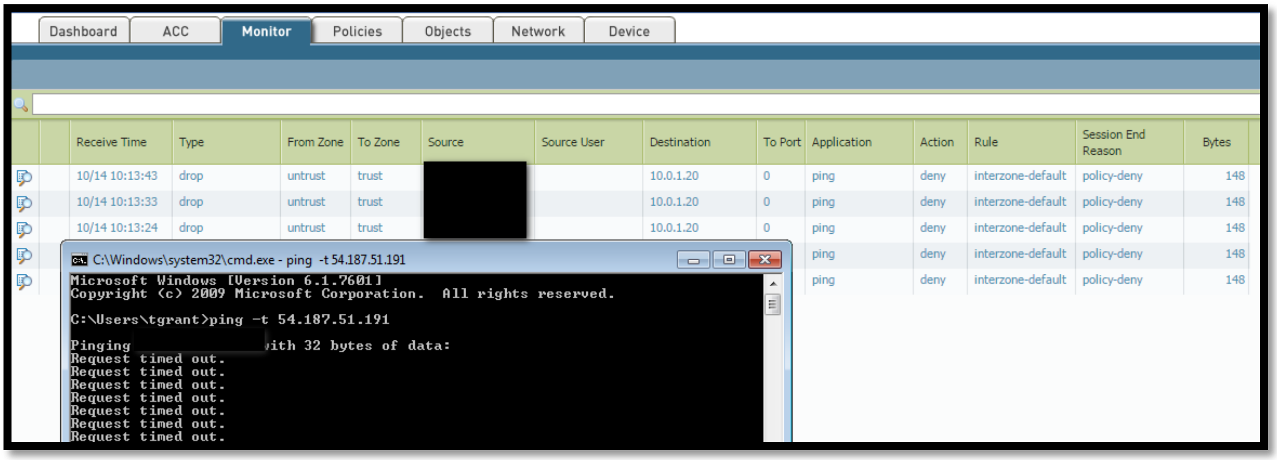
Private IP Address: 10.0.1.20*

☐ Reassociation

Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more about public IP addresses.

At this point, you should be able to ping the Elastic IP from your workstation, and since we didn't allow ICMP to security policy, the Traffic Monitor on the Palo Alto will show packets being dropped.



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
10/14 10:13:43	drop	untrust	trust	[redacted]		10.0.1.20	0	ping	deny	interzone-default	policy-deny	148
10/14 10:13:33	drop	untrust	trust	[redacted]		10.0.1.20	0	ping	deny	interzone-default	policy-deny	148
10/14 10:13:24	drop	untrust	trust	[redacted]		10.0.1.20	0	ping	deny	interzone-default	policy-deny	148
								ping	deny	interzone-default	policy-deny	148
								ping	deny	interzone-default	policy-deny	148

C:\Windows\system32\cmd.exe - ping -t 54.187.51.191

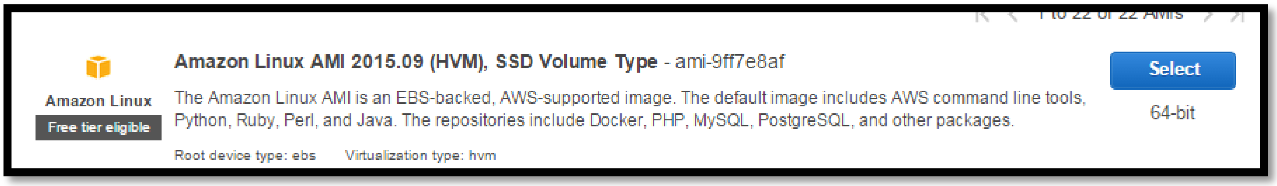
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\tgrant>ping -t 54.187.51.191

Pinging [redacted]ith 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Building the Bastion Host

Launch the bastion host instance that will be used to enter into the private subnet. Create this host in the Public Security Group and with two NICs - one NIC in the public subnet and another in the private subnet.

Browse to **EC2 > Instances** and select **Launch Instance**

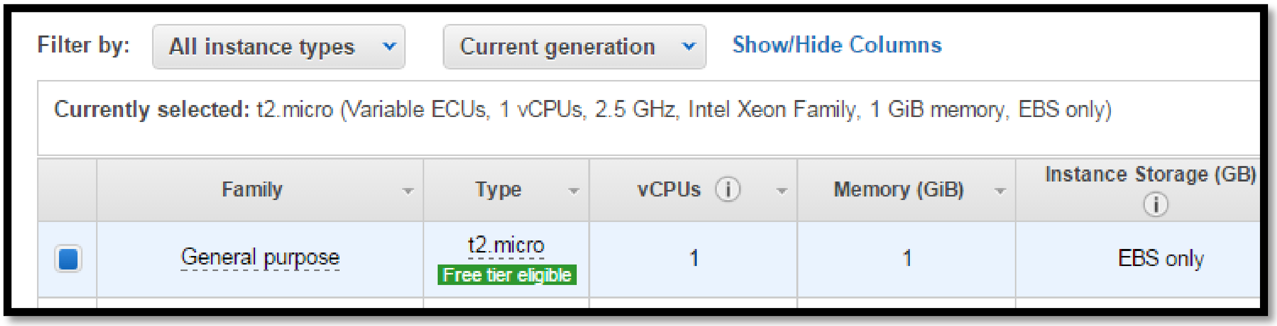
Select one of the cheaper Linux instances.



Amazon Linux AMI 2015.09 (HVM), SSD Volume Type - ami-9ff7e8af

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs   Virtualization type: hvm



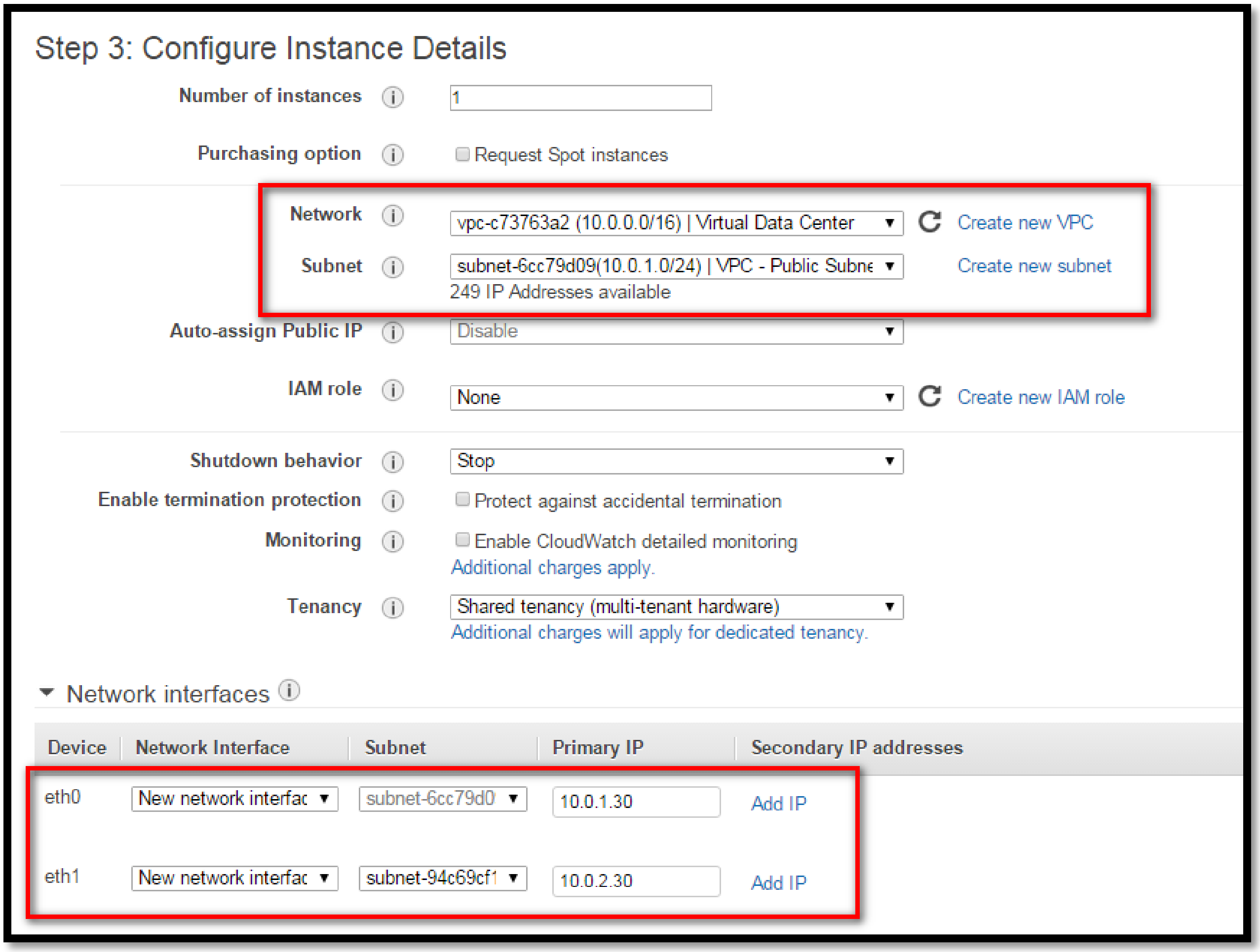
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs ⓘ	Memory (GiB)	Instance Storage (GB) ⓘ
■	General purpose	t2.micro Free tier eligible	1	1	EBS only

Select **Next: Configure Instance Details**

Make sure the VDC is 10.0.0.0/16 and the subnet is the public subnet 10.0.1.0/24.

Secondly make sure you have two NICs. One in the public subnet with the bastion host public IP, and one in the private subnet with the bastion host private IP.



Step 3: Configure Instance Details

Number of instances: 1

Purchasing option: □ Request Spot instances

Network: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center ▼ Create new VPC

Subnet: subnet-6cc79d09(10.0.1.0/24) | VPC - Public Subne ▼ Create new subnet
249 IP Addresses available

Auto-assign Public IP: Disable ▼

IAM role: None ▼ Create new IAM role

Shutdown behavior: Stop ▼

Enable termination protection: □ Protect against accidental termination

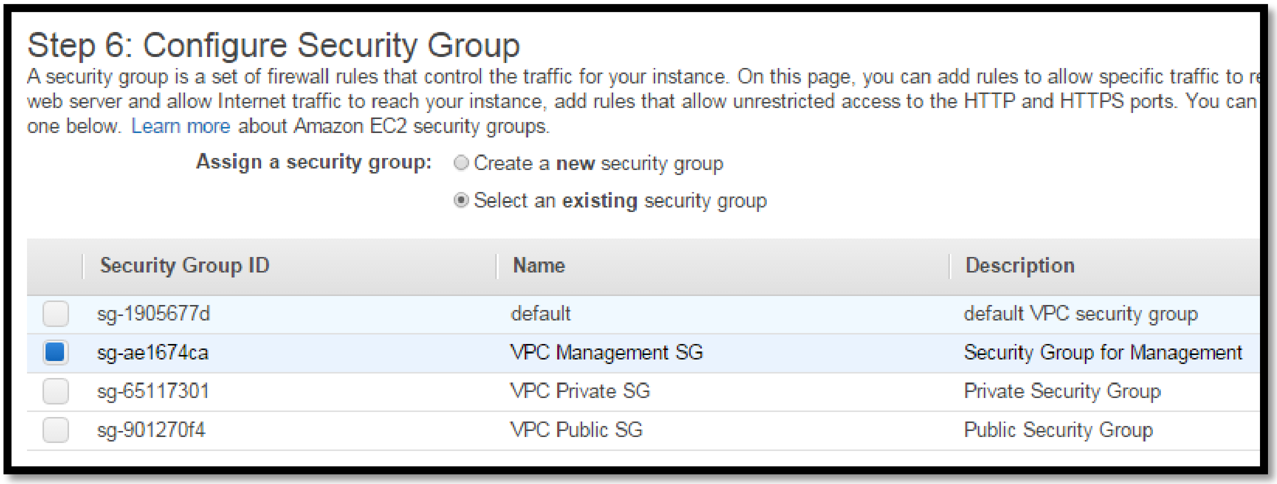
Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared tenancy (multi-tenant hardware) ▼
Additional charges will apply for dedicated tenancy.

▼ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfac ▼	subnet-6cc79d0 ▼	10.0.1.30	Add IP
eth1	New network interfac ▼	subnet-94c69cf1 ▼	10.0.2.30	Add IP

Click **Next:** until you get to **Configure Security Group** and place the instance in the **VPC Management SG** Security Group.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to r web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

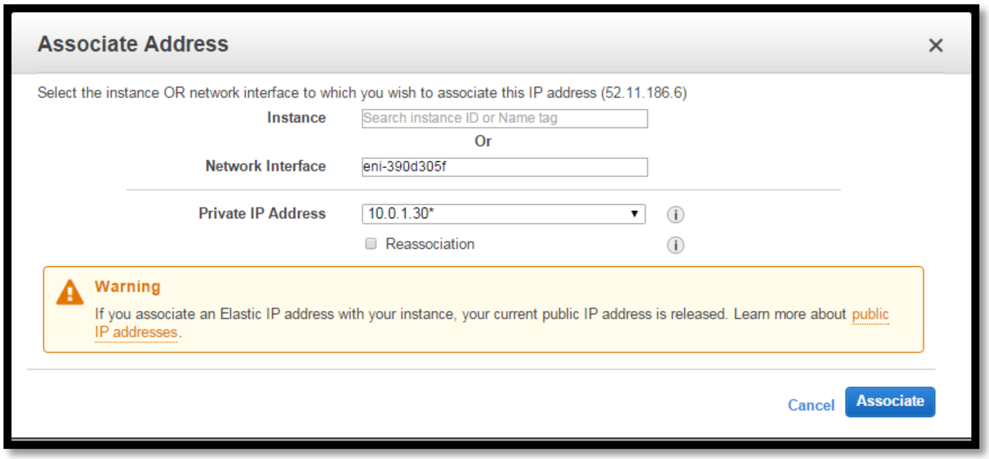
	Security Group ID	Name	Description
□	sg-1905677d	default	default VPC security group
☑	sg-ae1674ca	VPC Management SG	Security Group for Management
□	sg-65117301	VPC Private SG	Private Security Group
□	sg-901270f4	VPC Public SG	Public Security Group

Select **Review and Launch** and then **Launch.** Finally select the security key you want to use for authentication to the server. While the instance is building, assign the Elastic IP for the bastion host, so that it is accessible from the Internet.

This is a good time to mention security for the bastion host. In a production environment, you would want to only allow explicit access to the host from your corporate network block. For example, only allow SSH to the bastion host public IP from the corporate source NAT of your network.

Browse to **EC2 > Elastic IPs** and allocate a new Address

Select the new Elastic IP and use the **Actions** menu to associate a new address. Select the Network Interface with the public NIC of the bastion host.



Associate Address

Select the instance OR network interface to which you wish to associate this IP address (52.11.186.6)

Instance: Search instance ID or Name tag

Or

Network Interface: eni-390d305f

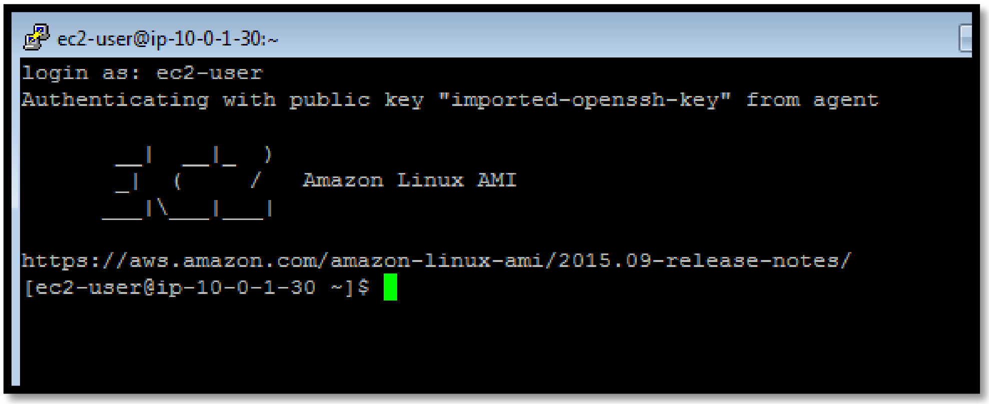
Private IP Address: 10.0.1.30*

□ Reassociation

Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more about public IP addresses.

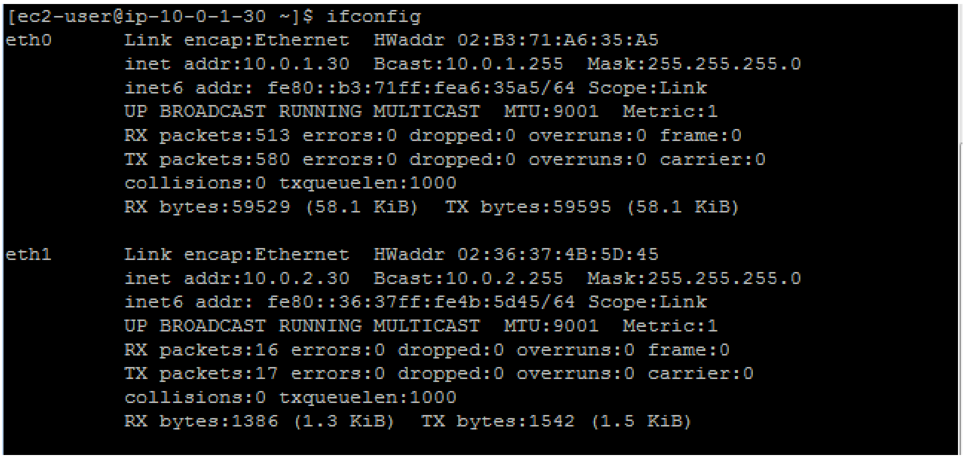
SSH to the new Elastic IP of the bastion host and login as user **ec2-user**



ec2-user@ip-10-0-1-30:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key" from agent

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/
[ec2-user@ip-10-0-1-30 ~]$
```

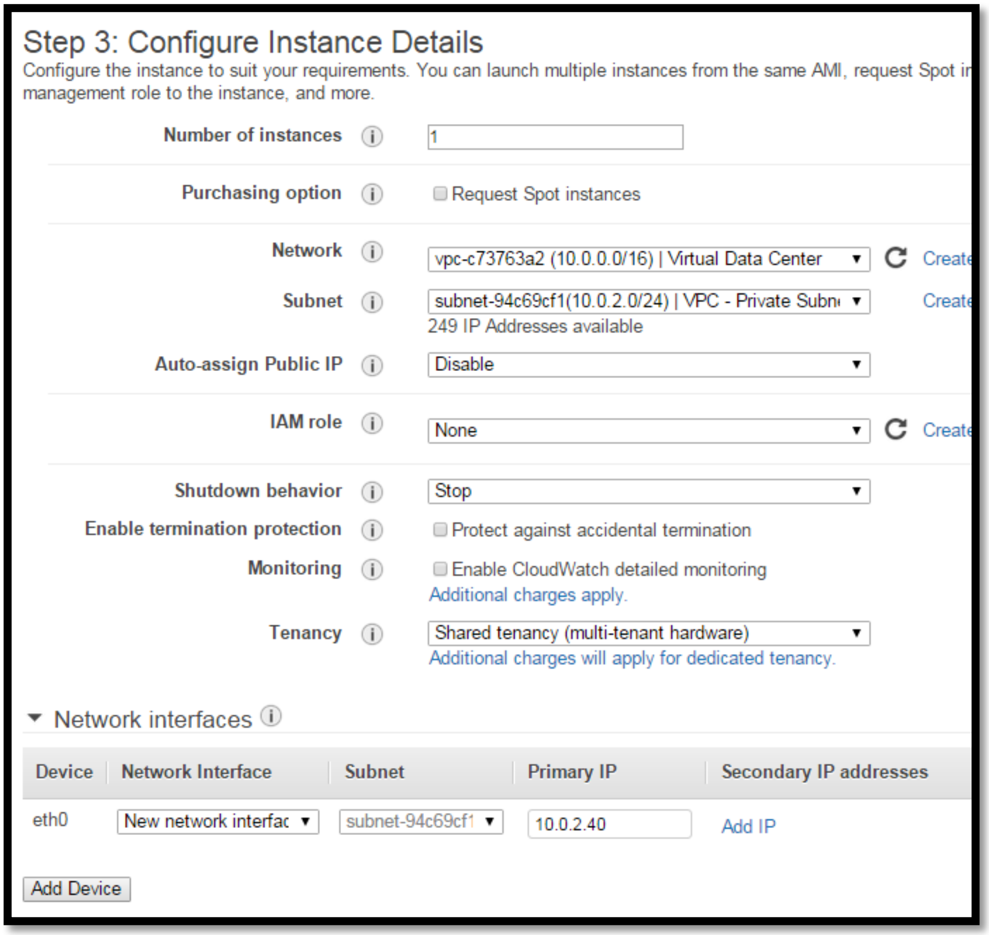
Use **ifconfig** to verify the server has 2 NICs and the correct IPs are configured



```
[ec2-user@ip-10-0-1-30 ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:B3:71:A6:35:A5
          inet addr:10.0.1.30  Bcast:10.0.1.255  Mask:255.255.255.0
          inet6 addr: fe80::b3:71ff:fea6:35a5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:513 errors:0 dropped:0 overruns:0 frame:0
          TX packets:580 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59529 (58.1 KiB)  TX bytes:59595 (58.1 KiB)

eth1      Link encap:Ethernet  HWaddr 02:36:37:4B:5D:45
          inet addr:10.0.2.30  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::36:37ff:fe4b:5d45/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1386 (1.3 KiB)  TX bytes:1542 (1.5 KiB)
```

Creating the Web Server Instance

Like the bastion host, launch another Linux instance. This time, however, place the server in the private subnet and assign the private IP of 10.0.2.40.



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot i management role to the instance, and more.

Number of instances: 1

Purchasing option: □ Request Spot instances

Network: vpc-c73763a2 (10.0.0.0/16) | Virtual Data Center ▼ Create

Subnet: subnet-94c69cf1(10.0.2.0/24) | VPC - Private Subn ▼ Create
249 IP Addresses available

Auto-assign Public IP: Disable ▼

IAM role: None ▼ Create

Shutdown behavior: Stop ▼

Enable termination protection: □ Protect against accidental termination

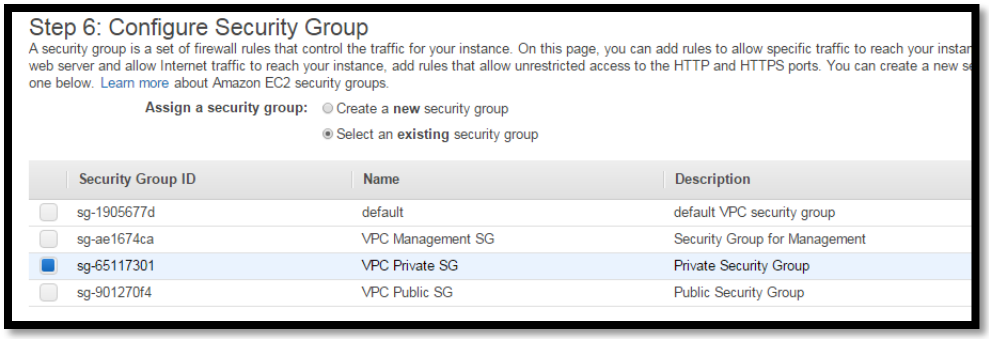
Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared tenancy (multi-tenant hardware) ▼
Additional charges will apply for dedicated tenancy.

▼ Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interfac ▼	subnet-94c69cf1 ▼	10.0.2.40	Add IP

Add the web server to the **Private Security Group**



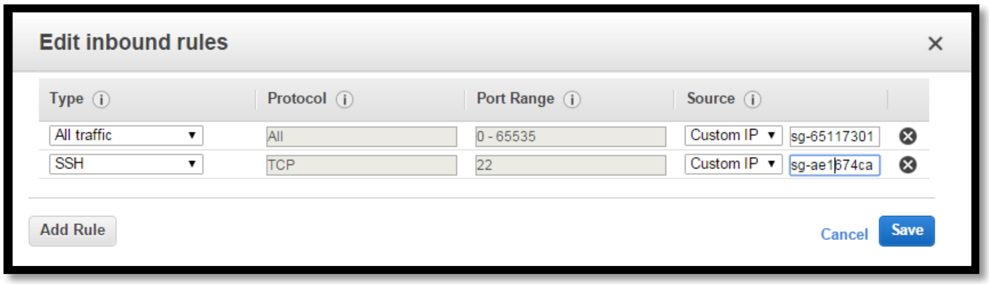
Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instar web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new s one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description
□	sg-1905677d	default	default VPC security group
□	sg-ae1674ca	VPC Management SG	Security Group for Management
☑	sg-65117301	VPC Private SG	Private Security Group
□	sg-901270f4	VPC Public SG	Public Security Group

Now, we need to ensure the bastion host in the management network can talk to the servers in the VPC Private Security Group. Browse to **EC2 > Security Groups**, right-click on the VPC Private SG and select **Edit inbound security rules**. Select **Add Rule**, and add the **VPC Management SG's Group ID** as the Custom IP.



Edit inbound rules

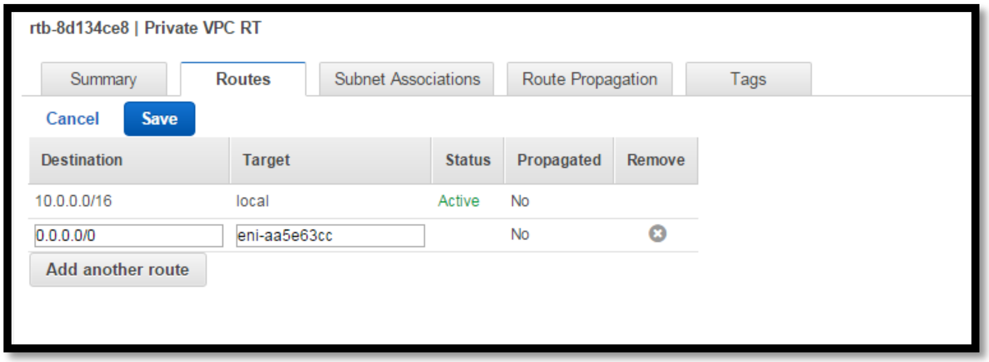
Type	Protocol	Port Range	Source	
All traffic	All	0 - 65535	Custom IP	sg-65117301
SSH	TCP	22	Custom IP	sg-ae1674ca

Proving you have Pageant running, and your security key added to it, you can SSH to the bastion's public IP, and then SSH to 10.0.2.40, the web server. Pageant loads the key automatically, so that you do not have to store the key on the bastion host – that would be a bad idea!

You'll notice, however that you can't ping out to the Internet form the web server. We need to do a couple of things first! We need to change the route for the private subnet and update the default gateway on the web server. Granted, I've read there are other ways to route through the Palo Alto, but I haven't explored those at this time.

Browse to **EC2 > Network Interfaces** and copy the **Network interface ID** for the **Palo Alto Private Interface**, which should have the IP of 10.0.2.20.

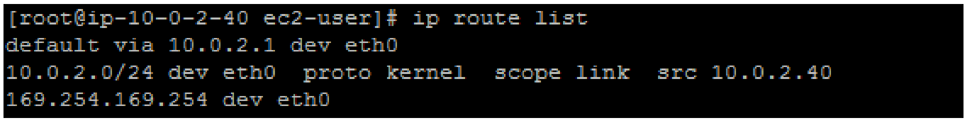
Browse to **VPC > Route Tables** and select **Private VPC RT**. Select the **Routes** tab and **Edit**. Add the destination 0.0.0.0/0 to the Network interface ID of the Palo Alto Private Interface. Click **Save.**



rtb-8d134ce8 | Private VPC RT

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-aa5e63cc		No	⊗

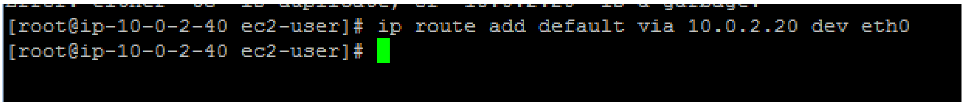
Login vis SSH to the bastion host, and then SSH to the web server, which is 10.0.2.40. Use the command **ip route list** to show the current routing table.



```
[root@ip-10-0-2-40 ec2-user]# ip route list
default via 10.0.2.1 dev eth0
10.0.2.0/24 dev eth0  proto kernel  scope link  src 10.0.2.40
169.254.169.254 dev eth0
```

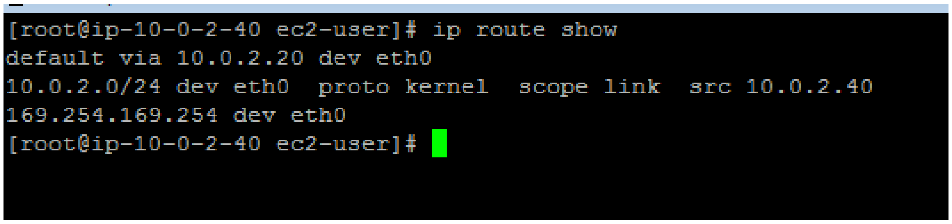
Make sure you are root by running the command **sudo su**

Then use **ip route del default** to delete the default route and then **ip route add default via 10.0.2.20 dev eth0**, which makes the default route to the Palo Alto private IP. If you reboot the server, you will need to delete the default route and add the new default route again. If needed, make the routing change persistent.



```
[root@ip-10-0-2-40 ec2-user]# ip route add default via 10.0.2.20 dev eth0
[root@ip-10-0-2-40 ec2-user]#
```

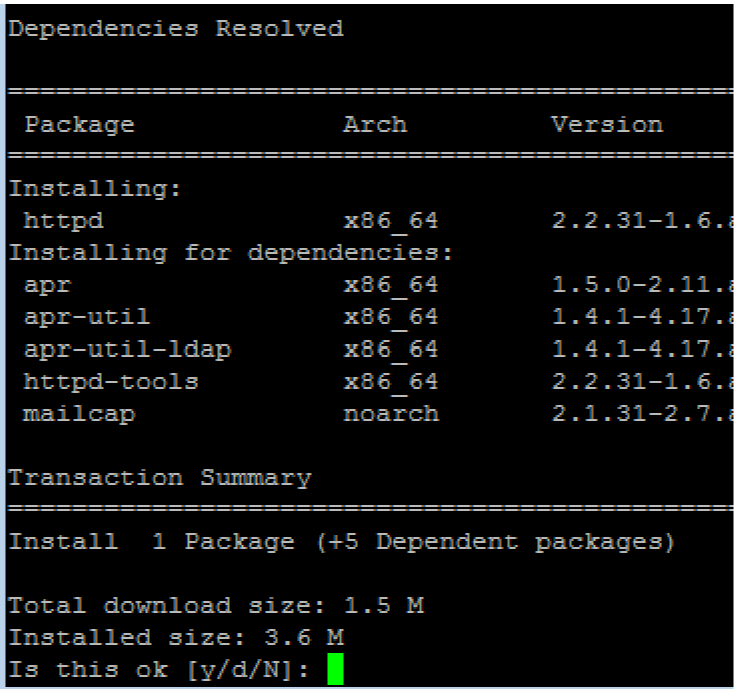
The routing table should look like this



```
[root@ip-10-0-2-40 ec2-user]# ip route show
default via 10.0.2.20 dev eth0
10.0.2.0/24 dev eth0  proto kernel  scope link  src 10.0.2.40
169.254.169.254 dev eth0
[root@ip-10-0-2-40 ec2-user]#
```

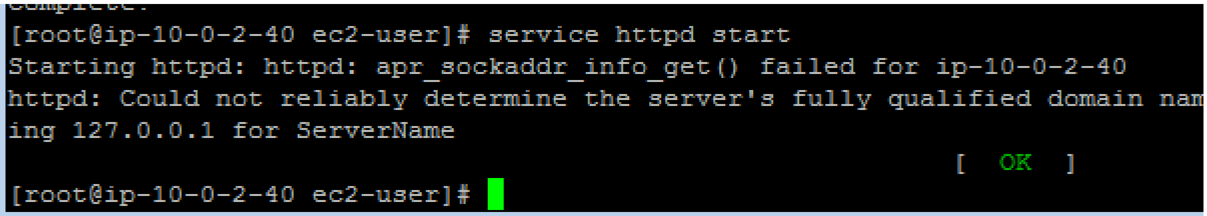
Now let's install the apache web server by running **yum install httpd**

When prompted, enter **y** and hit the enter key



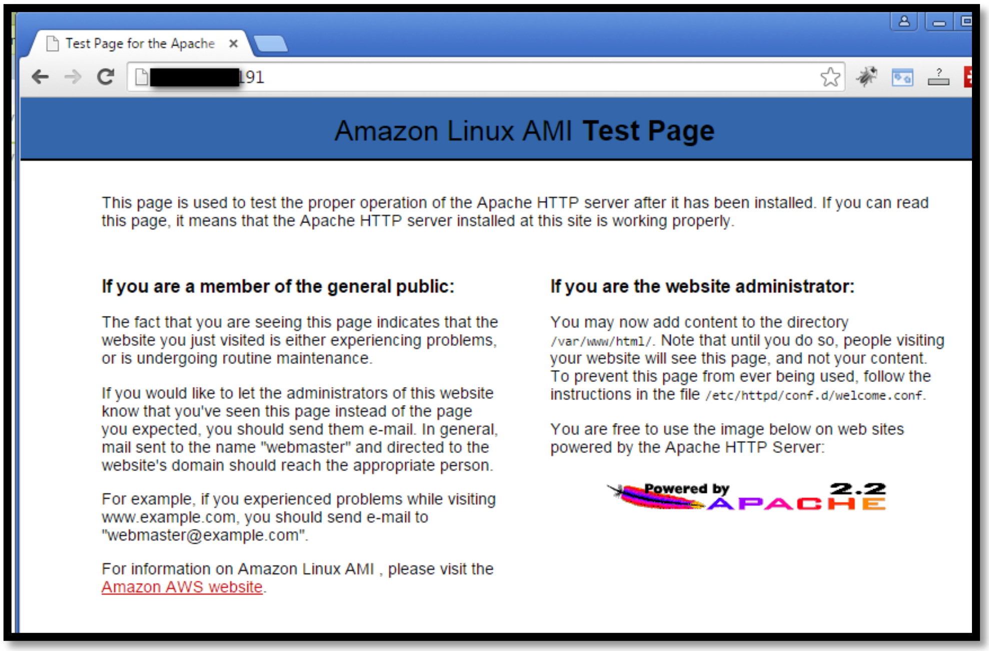
```
Dependencies Resolved

=============================================
 Package                Arch          Version
=============================================
Installing:
 httpd                  x86_64        2.2.31-1.6.
Installing for dependencies:
 apr                    x86_64        1.5.0-2.11.
 apr-util               x86_64        1.4.1-4.17.
 apr-util-ldap          x86_64        1.4.1-4.17.
 httpd-tools            x86_64        2.2.31-1.6.
 mailcap                noarch        2.1.31-2.7.

Transaction Summary
=============================================
Install  1 Package (+5 Dependent packages)

Total download size: 1.5 M
Installed size: 3.6 M
Is this ok [y/d/N]:
```

Start apache with **service httpd start**



```
Complete.
[root@ip-10-0-2-40 ec2-user]# service httpd start
Starting httpd: httpd: apr_sockaddr_info_get() failed for ip-10-0-2-40
httpd: Could not reliably determine the server's fully qualified domain nam
ing 127.0.0.1 for ServerName
                                                           [  OK  ]
[root@ip-10-0-2-40 ec2-user]#
```

Now browse via an Internet browser to the Elastic IP that was created for the web server, and your webpage should pull up!



Amazon Linux AMI **Test Page**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on Amazon Linux AMI , please visit the Amazon AWS website.

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server: