

TECH NOTE

# Palo Alto Networks VM-Series Firewalls on Xi

---

# Copyright

Copyright 2022 Nutanix, Inc.

Nutanix, Inc.  
1740 Technology Drive, Suite 150  
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Nutanix and the Nutanix logo are registered trademarks of Nutanix, Inc. in the United States and/or other jurisdictions. All other brand and product names mentioned herein are for identification purposes only and may be trademarks of their respective holders.

# Contents

1. Executive Summary.....	4
Document Version History.....	4
2. Use Case 1: Multisite VPN Between Xi and On-Premises Firewall.....	5
Use Case 1: Set Up the Nutanix Xi VPC.....	5
Use Case 1: Deploy and Configure VM-Series on Xi.....	10
Use Case 1: Deploy and Configure VM-Series on On-Prem 1.....	45
Use Case 1: Deploy and Configure VM-Series on On-Prem 2.....	67
3. Use Case 2: Full-Mesh VPN Between Xi and On-Premises Firewall.....	77
Use Case 2: Set Up the Nutanix Xi VPC.....	78
Use Case 2: Deploy and Configure VM-Series on Xi-VPN-VM1 and VM2.....	78
Use Case 2: Deploy and Configure VM-Series on On-Prem 1.....	82
Use Case 2: Deploy and Configure VM-Series on On-Prem 2.....	83
About Nutanix.....	85
List of Figures.....	86

---

# 1. Executive Summary

Nutanix customers can set up a secure virtual private network (VPN) connection to connect their on-premises datacenter or remote user device to Xi Cloud Services using a Palo Alto Networks firewall. A VPN solution enables secure communication between the on-premises Prism Central instance and the production virtual private cloud (VPC) in Xi Cloud Services.

This deployment guide describes two use cases.

1. Multisite VPN between Xi and an on-premises Palo Alto Networks VM-Series firewall.
  2. Full mesh VPN between Xi and an on-premises Palo Alto Networks VM-Series firewall.
- 

## Document Version History

Version Number	Published	Notes
1.0	October 2019	Original publication.
1.1	January 2021	Updated Nutanix overview.
1.2	July 2021	Updated the Use Case 1: Deploy and Configure VM-Series on Xi section.
1.3	August 2022	Refreshed content.

## 2. Use Case 1: Multisite VPN Between Xi and On-Premises Firewall

Datacenters in multiple on-premises sites can connect to Xi Cloud Services through an External Border Gateway Protocol (eBGP) running over an IPSec tunnel in the Palo Alto Networks VM-Series firewall.

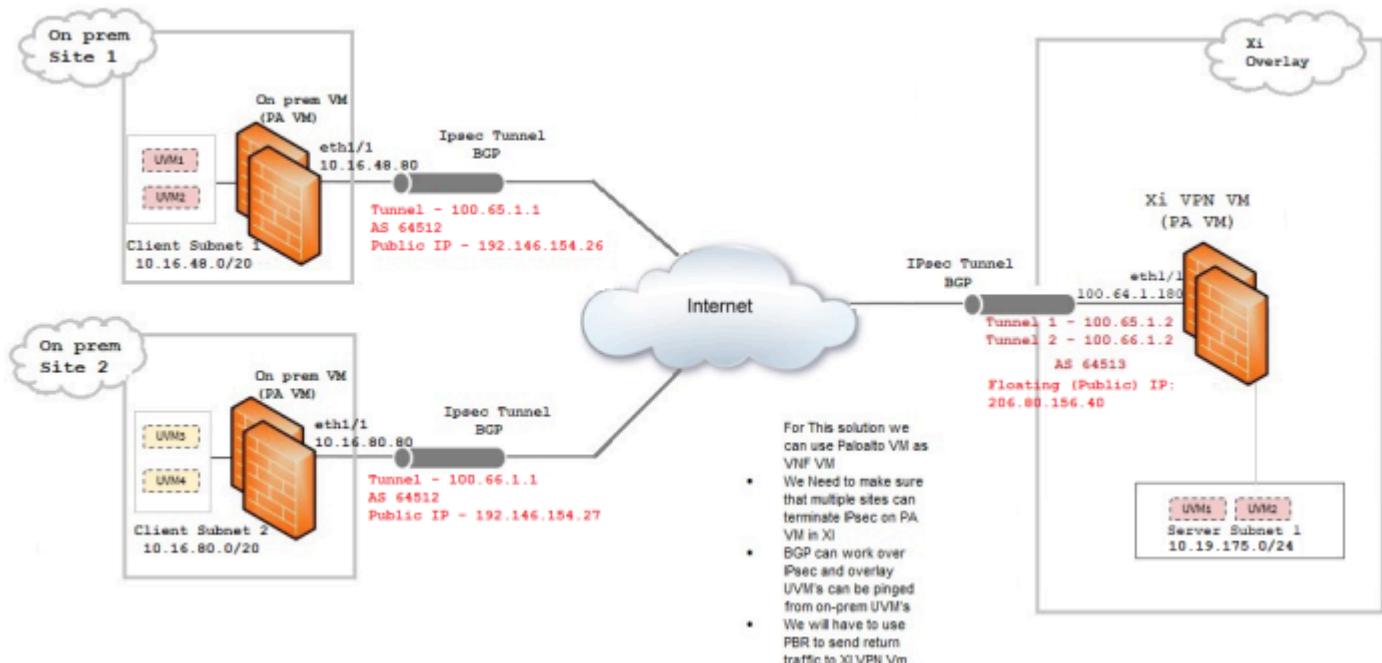


Figure 1: VPN Between Xi and On-Premises Firewall Deployment

### Use Case 1: Set Up the Nutanix Xi VPC

Sign in to the Xi portal and upload the VM-Series kernel-based VM (KVM) image:

- Click Images in the Explore tab of the Xi portal, then click Add Image.

The screenshot shows the 'Explore' tab selected in the top navigation bar. Below it, the 'Entities' section displays two items: 'VIRTUAL INFRASTRUCTURE' with a count of 41 and 'Images' with a count of 14. A blue button labeled 'Add Image' is visible on the right. A search bar with the placeholder 'Type name to filter by' is also present.

Figure 2: Xi Dashboard Images Pane

- In the Add Images pane that opens, select Image File, then click the Add File button. Add the VM-Series KVM image from your computer and click Save.

The screenshot shows the 'Add Images' dialog box. Under 'Image Source', the 'Image File' radio button is selected. A large input field with a '+ Add File' button is available for selecting a file. At the bottom, there are 'Cancel' and 'Save' buttons.

Figure 3: Xi Dashboard Add Images Pane

- In the search bar, type the name of the KVM image you just uploaded and press Enter.

**Entities**

**VIRTUAL INFRASTRUCTURE**

VMs	31
<b>Images</b>	<b>12</b>

**NETWORKING**

Virtual Private Clouds	2
Floating IPs	4

**ADMINISTRATION**

**Name contains P... Type name to filter by**

**1 Total Images**

<input type="checkbox"/>	▲ Name
<input type="checkbox"/>	PA-VM-KVM-8.1.3.qcow2

Figure 4: Use the Search Bar to Find Specific Images

Two VPCs, Production and Test, are available by default in the Xi Cloud Services portal. You can't add new VPCs in Xi Cloud Services, but you can create virtual subnets in the VPCs for hosting VMs and configure policies to secure them. You can update the VPCs to specify settings such as DNS and DHCP.

2 Total Virtual Private Clouds			
	Name	On Prem Access	SNAT IP
<input type="checkbox"/>	Production	-	206.80.156.2
<input type="checkbox"/>	Test	-	206.80.156.45

Figure 5: Xi Dashboard Virtual Private Clouds

Create two subnets in the Production VPN: Nutanix-vpn-internal and Prod Xi. Use Nutanix-vpn-internal as both a data interface on the VM-Series (associated with a floating IP) and a management interface.

Note: If you need to save, save on a public IP.

Use Prod Xi for user VMs running on Xi.

Note: Users can access floating IP addresses from the internet, so associate them with the private IP address of the VM's virtual network interface controller (vNIC). The association allows you to access the VM from the internet. Create and use floating IPs based on your needs.

Navigate to the Explore tab in your Xi dashboard and click Virtual Private Clouds, then Production, then Add Subnet.

Note: We created the Nutanix-vpn-internal subnet with the specifications in the following image as an example. Be sure to fill in the information for your subnets as appropriate for your environment.

Update Subnet ? X

---

Subnet Name  
Nutanix-vpn-internal

Availability Zone  
US-EAST-1B

IP Range  
100.64.1.0/24

Default Gateway IP  
100.64.1.1

**DHCP IP Pool**

These IP addresses will be given out to VMs on this subnet by the DHCP service

[+ IP Pool](#)

START ADDRESS	END ADDRESS	ACTIONS
100.64.1.2	100.64.1.254	<a href="#"></a> <a href="#"></a>

[Cancel](#) [Save](#)

Figure 6: Create Nutanix-vpn-internal Subnet

Repeat this process to create the Prod Xi subnet.

In the Production VPC, you should see two available subnets, as in the following figure.

The screenshot shows a list of subnets in the 'Production' VPC. There are two entries:

Name	IP Range	DHCP IP Pool	Default Gateway IP	Actions
Nutanix-vpn-internal	100.64.1.0/24	100.64.1.2 - 100.64.1.254	100.64.1.1	Edit · Delete
Prod Xi	10.19.175.0/24	10.19.175.100 - 10.19.175.200	10.19.175.1	Edit · Delete

Figure 7: Available Production VPC Subnets

## Use Case 1: Deploy and Configure VM-Series on Xi

Sign in to the Xi portal and create a VM-Series VM with two vNICs (also called interfaces in Palo Alto documentation). Use the two subnets you created in the Production VPC to create these VM vNICs. Assign Prod Xi as the VM's management vNIC. You can associate a floating IP with Prod Xi and then use the management vNIC to manage the Xi VM-Series. Assign Nutanix-vpn-internal to the VM's ethernet1/1 vNIC (associated with a floating IP). Use ethernet1/1 for data traffic and to manage the Xi VM-Series externally.

Note: Because the floating IP is a public IP, change the default admin credentials on VM-Series after the configuration to prevent unauthorized access.

- To create a VM, click VMs in the Explore tab in the Xi dashboard.
- In the search bar, type in the name of the VM-Series KVM image you uploaded earlier and press Enter to display the image.

The screenshot shows the Nutanix Xi Dashboard interface. At the top, there are three navigation tabs: 'Dashboard', 'Explore' (which is currently selected), and 'Alerts'. Below the tabs, the title 'Entities' is displayed. Under the 'VIRTUAL INFRASTRUCTURE' section, there are two items: 'VMs' (count 41) and 'Images' (count 14). To the right of these items is a search bar with the placeholder 'Name contains PA x' and a dropdown menu. A large blue button labeled 'Create VM' is prominently displayed.

Figure 8: VMs Pane in Xi Dashboard

- In the Select Disk Image(s) dropdown menu, select the KVM image you uploaded earlier and click Next.

The screenshot shows the 'Create VM' pane. At the top, it says 'Create VM' and has two numbered steps: '1 Browse images' (which is highlighted in blue) and '2 Deploy VM'. Below this, there is a section titled 'Select Disk Image(s)' with a note '1 image selected · Deselect All'. A search bar contains the text 'PA-VM-KVM-8.1.3.qcow2'. Below the search bar is a list of disk images:

- PA-VM-KVM-8.1.3.qcow2 (selected, indicated by a checked checkbox)
- 03/21/2019

At the bottom of the pane are two buttons: 'Cancel' and 'Next'.

Figure 9: Create VM Pane in Xi Dashboard

- In the General Settings pane, we entered the following specifications for the VM as an example. Be sure to use the appropriate individual specifications for your environment.
  - › Name: XiPA
  - › Timezone: Select the correct time zone.
  - › Disks: Ensure there is a disk called scsi.0 with the DISK type and 60 GB.
  - › Network: Check Production, then Nutanix-vpn-internal, then Associate Floating IP and select the floating IP from the dropdown. Select the Prod Xi checkbox, but don't select Associate Floating IP.
  - › Configuration: Under CPU, type 2 (vCPU). Under Memory, type 8 (GB).

**GENERAL SETTINGS**

Name  
XiPA

Timezone  
(UTC -07:00) America/Los\_Angeles

**Disks**  
Add new blank disks to this VM.  
+ New Disk

BOOT FROM	NAME	TYPE	SIZE (GB)	ACTIONS
<input type="radio"/>	scsi.0	DISK	60	

**Network**

NAME
<input checked="" type="checkbox"/> Production
<input checked="" type="checkbox"/> Nutanix-vpn-internal
<input checked="" type="checkbox"/> Associate Floating IP 206.80.156.40
<input checked="" type="checkbox"/> Prod Xi
<input type="checkbox"/> Associate Floating IP 206.80.156.10
<input type="checkbox"/> 3900
<input type="checkbox"/> Associate Floating IP 206.80.156.10
<input type="checkbox"/> Test

**Configuration**  
Configure the CPU and Memory for this VM.

CPU	MEMORY
2 VCPU	8 GB

**Categories**  
Search for a category

**Buttons**  
Cancel Save

Figure 10: General Settings for VM-Series VM

Start the VM-Series firewall and configure the following settings on ethernet1/1:

- Make sure ethernet1/1 has a maximum transmission unit (MTU) set to less than 1,500.
- Use SSH to connect to the public IP (associated floating IP) with administrator credentials and run the following command to set the MTU to 1,310.

```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set network interface ethernet ethernet1/1 layer3 mtu 1310
```

Figure 11: Set MTU to 1,310

- If you are using a VM-Series version earlier than 9.1, run the following command from the Palo Alto Networks CLI to disable the Data Plane Development Kit (DPDK) on the VM:

```
set system setting dpdk-pkt-io off
```

```
admin@PA-VM> set system setting dpdk-pkt-io off
Enabling/disabling DPDK Packet IO mode requires a device reboot. Do you want to
continue? (y or n)

Device is now in non-DPDK IO mode, please reboot device
admin@PA-VM> _
```

Figure 12: Disable DPDK on VM-Series with Version Earlier Than 9.1

Note: DPDK is supported with PAN-OS versions 9.1.0 and later. You don't need to run the command to disable DPDK on VM-Series running on Xi if you are using a supported version. Refer to Palo Alto Networks documentation (<https://docs.paloaltonetworks.com/compatibility-matrix/vm-series-firewalls/vms-series-hypervisor-support.html>) for more information.

- Commit to save the changes.

With this configuration, you can use the public floating IP to access the Xi web portal firewall. Now you can start setting up the VM-Series.

## Create Interfaces and Zones on VM-Series

Refer to Palo Alto's [Configure Interfaces guide](#) for more information.

Note: Palo Alto Networks VM-Series documentation sometimes refers to vNICs as interfaces.

Here we provide the steps to set up a VPN connection that allows you to connect two local area networks (LANs), one in the Nutanix Xi cloud and the other on-premises. This configuration is a route-based VPN tunnel that connects Palo Alto Networks firewalls at two sites. The firewall makes a routing decision based on the traffic's destination IP address.

Before you configure a VPN tunnel, you must configure the Ethernet interface, tunnel interface, zone, and virtual router.

#### [Configure Ethernet Interface on VM-Series](#)

Before you can configure the ethernet1/1 interface, you must create the management profile allow-test and enable it to ping to test connectivity. Open the Palo Alto WebGUI and complete the following steps.

- Navigate to the Network tab, then Network Profiles, then Interface Management.
- In that pane, click Add, which opens the Interface Management Profile window. Configure the allow-test profile as shown in the following image.

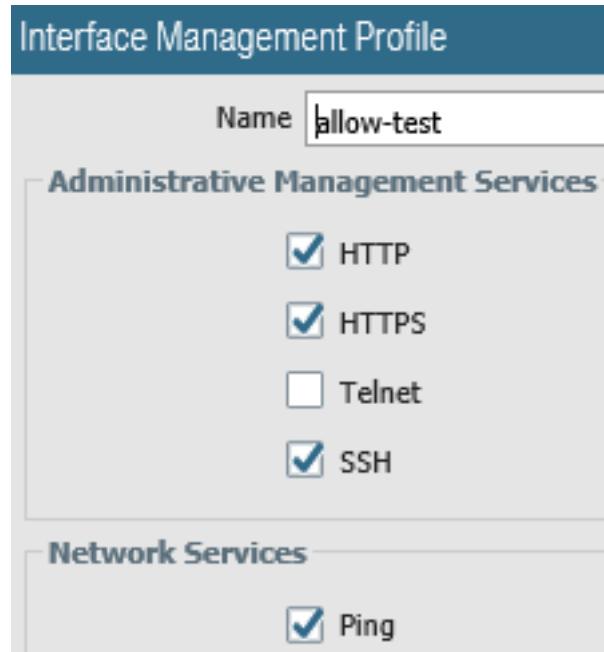


Figure 13: Add Interface Management Profile

Now, configure the Ethernet interface:

- In the Palo Alto WebGUI, navigate to Network, Interfaces, then Ethernet. Click ethernet1/1, which opens the Ethernet Interface window.
- Leave the interface name set to ethernet1/1, select Layer3 as the interface type, and use None as the Netflow Profile.
- In the Config tab, create a new security zone called test and use the default virtual router. (See the later section Create Zone on VM-Series for in-depth instructions.)

## Ethernet Interface

Interface Name	ethernet1/1		
Comment			
Interface Type	Layer3		
Netflow Profile	None		
Config	IPv4	IPv6	Advanced
<b>Assign Interface To</b>			
Virtual Router	default		
Security Zone	test		

Figure 14: Internet ethernet1/1 Configuration

- In the IPv4 tab, select Static as the Type in the IPv4 tab and choose a static IP address from the Nutanix-vpn-internal subnet.

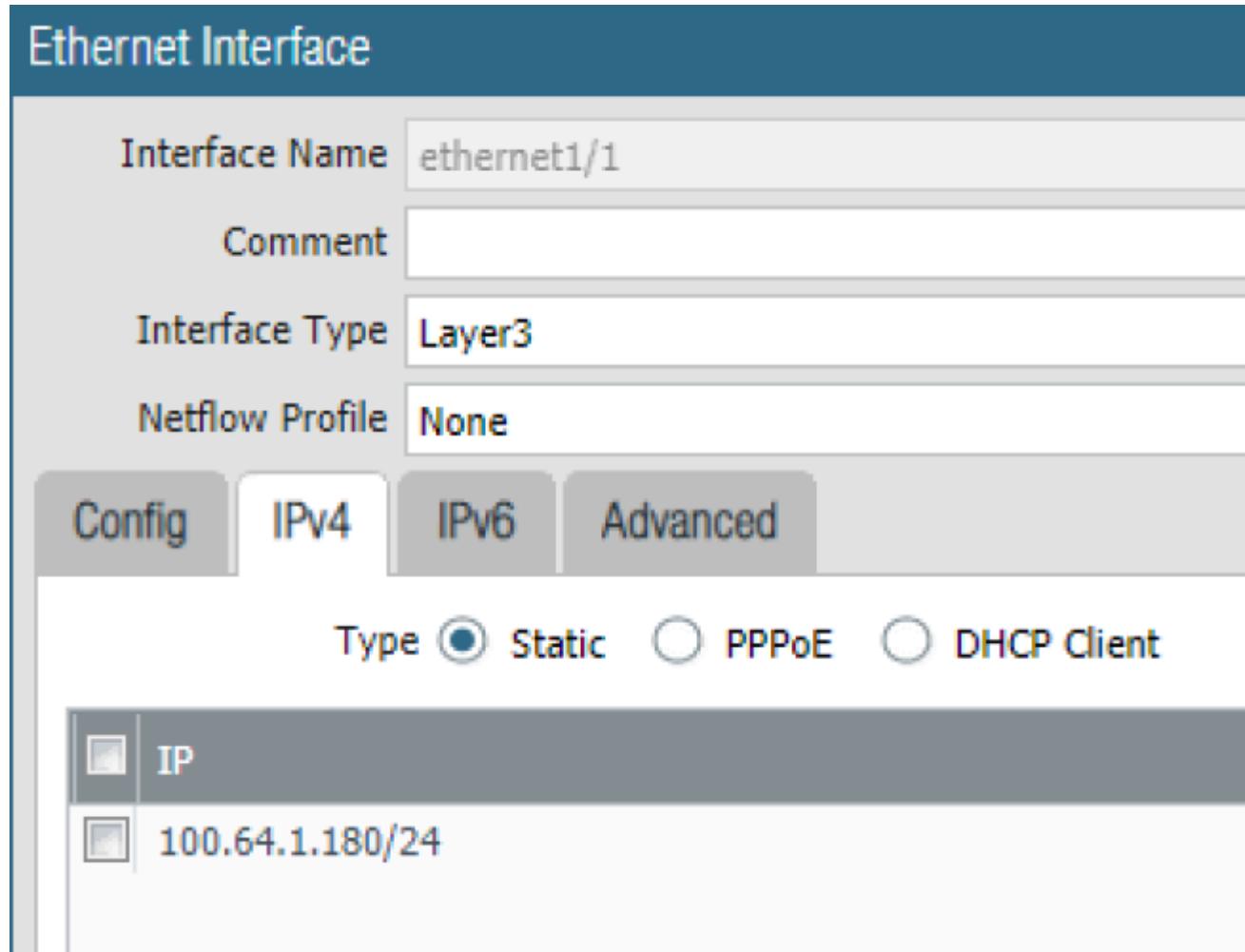


Figure 15: Ethernet Interface IPv4 Settings

- In the Advanced tab, leave the Link Speed value set to auto and type allow-test in the Management Profile box. Leave the MTU set to the default value. Select the checkbox beside Adjust TCP MSS, type 300 in the IPv4 MSS Adjustment box, and type 60 in the IPv6 MSS Adjustment box.

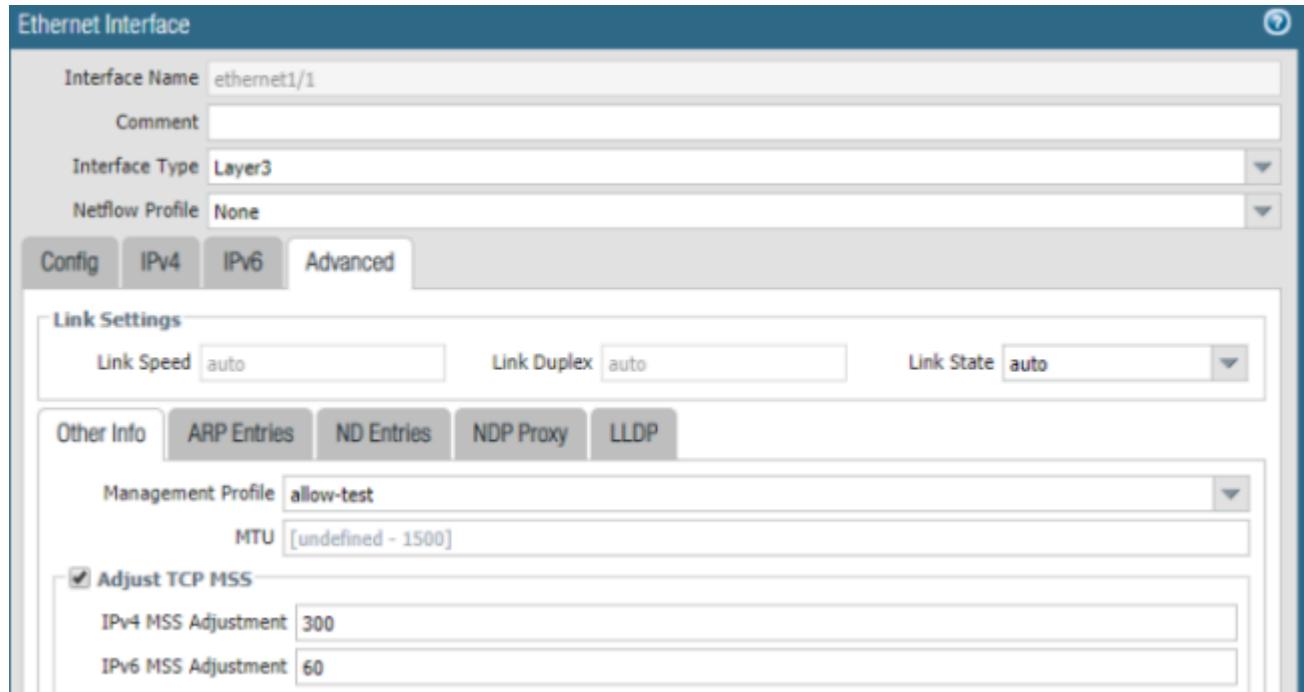


Figure 16: Ethernet Interface Advanced Settings

### Configure Tunnel Interfaces on VM-Series

This configuration has one tunnel interface for each site: tunnel.1 and tunnel.2.

- In the Palo Alto WebGUI, navigate to the Network tab, then Interfaces, then Tunnel. Click Add.
- Leave the Interface Name set to tunnel.1 and leave Netflow Profile set to None.
- Under the Config tab, set the Virtual Router to default and the Security Zone to test.

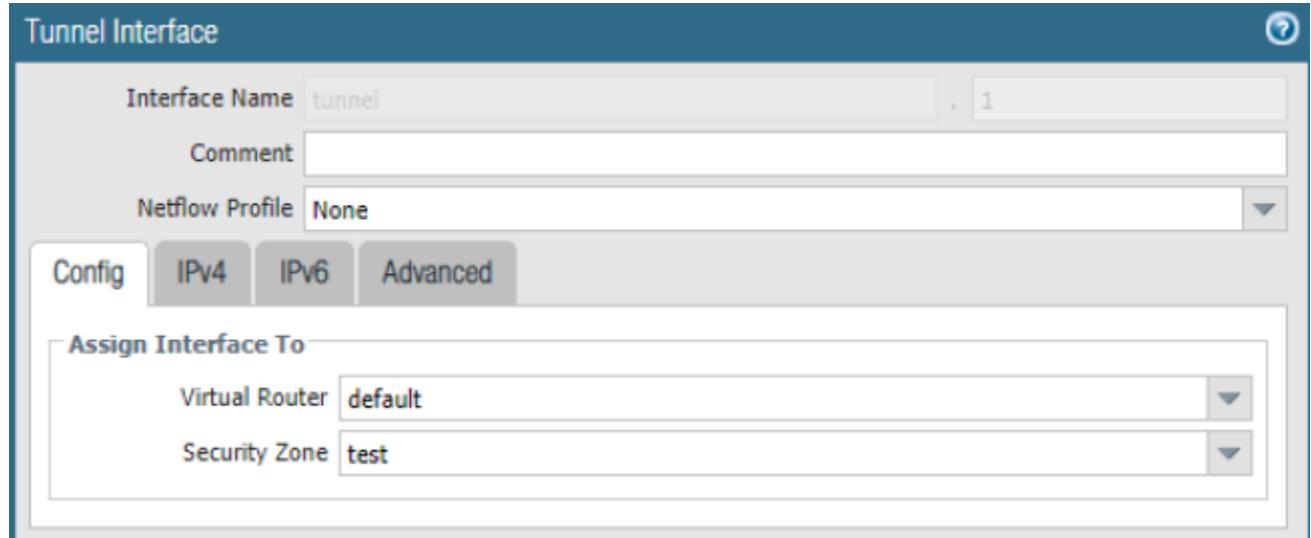


Figure 17: Tunnel Interface Configuration

- In the IPv4 tab, select the checkbox beside one of the /30 IP addresses you created (click Add and provide the IP address for the tunnel interface).

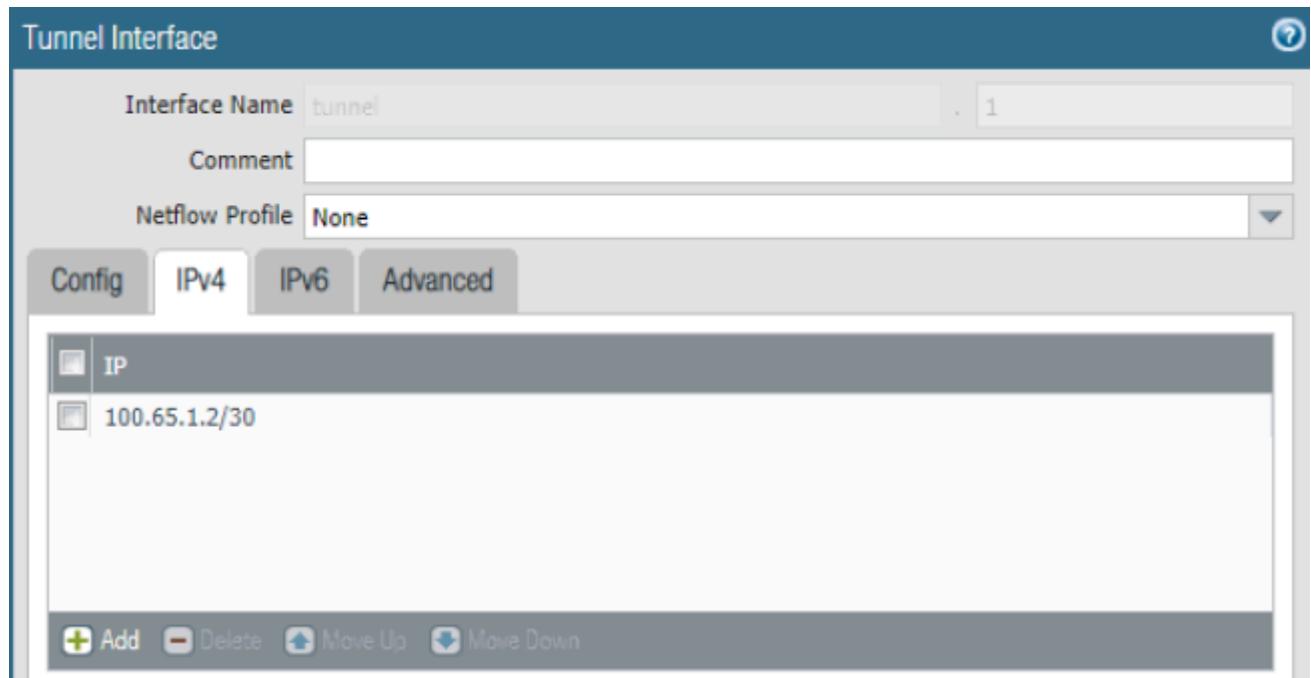


Figure 18: Tunnel Interface IPv4 Settings

- Repeat this process to create tunnel.2, using the other /30 IP address you created.

If multiple sites have VPNs terminating on the same Xi VM-Series, create additional tunnel interfaces to accommodate them.

#### [Create Zone on VM-Series](#)

- In the Palo Alto WebGUI, navigate to Network, then to Zones, then click Add Zone.
  - › Name the zone test.
  - › For Log Setting, select None.
  - › For Type, select Layer3.
  - › In the Interfaces section, click Add and add all three interfaces you created (ethernet1/1, tunnel.1, and tunnel.2).

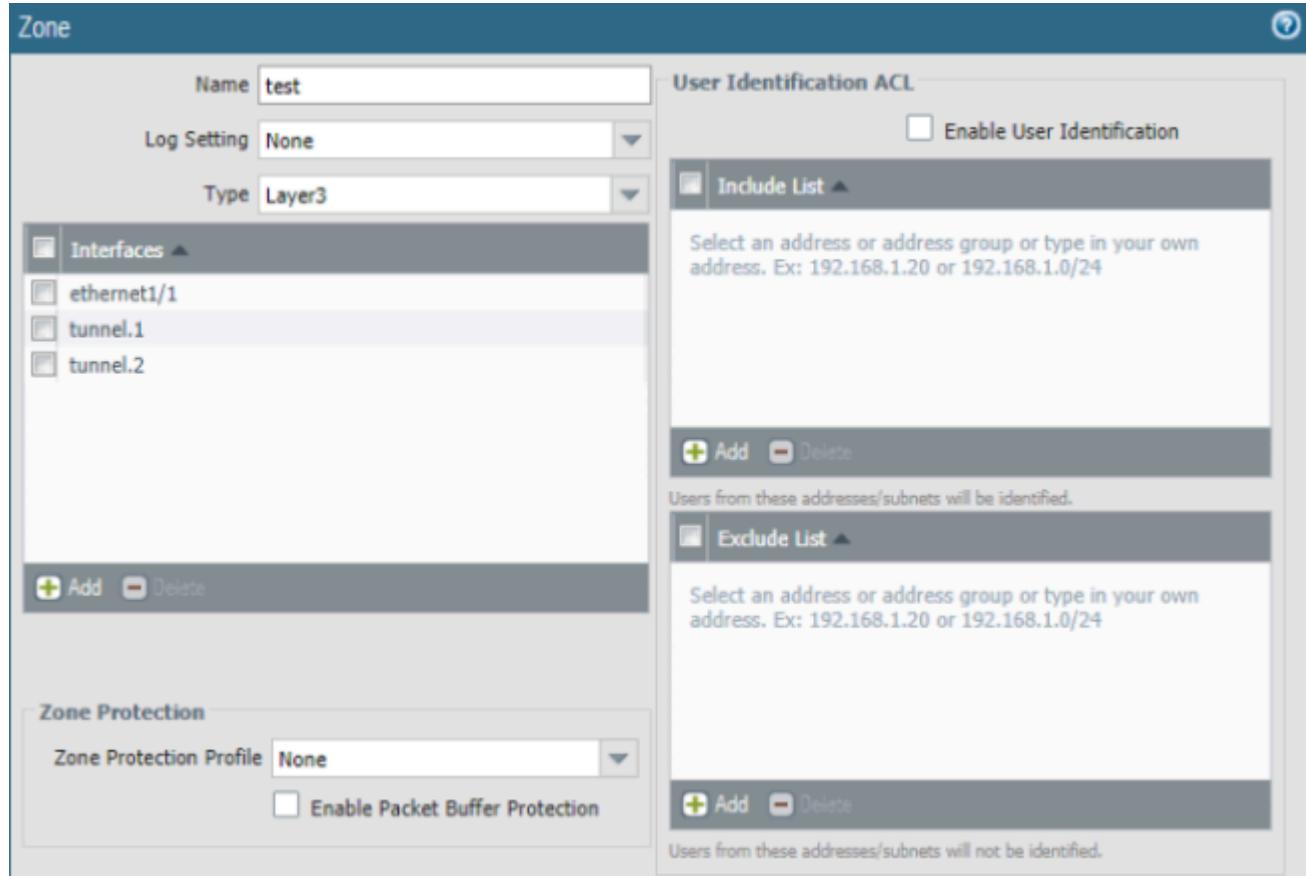


Figure 19: Zone Configuration

### Configure Virtual Router on VM-Series

In the Palo Alto WebGUI, use the default router (or create a new one) and add all the Ethernet and tunnel interfaces to it.

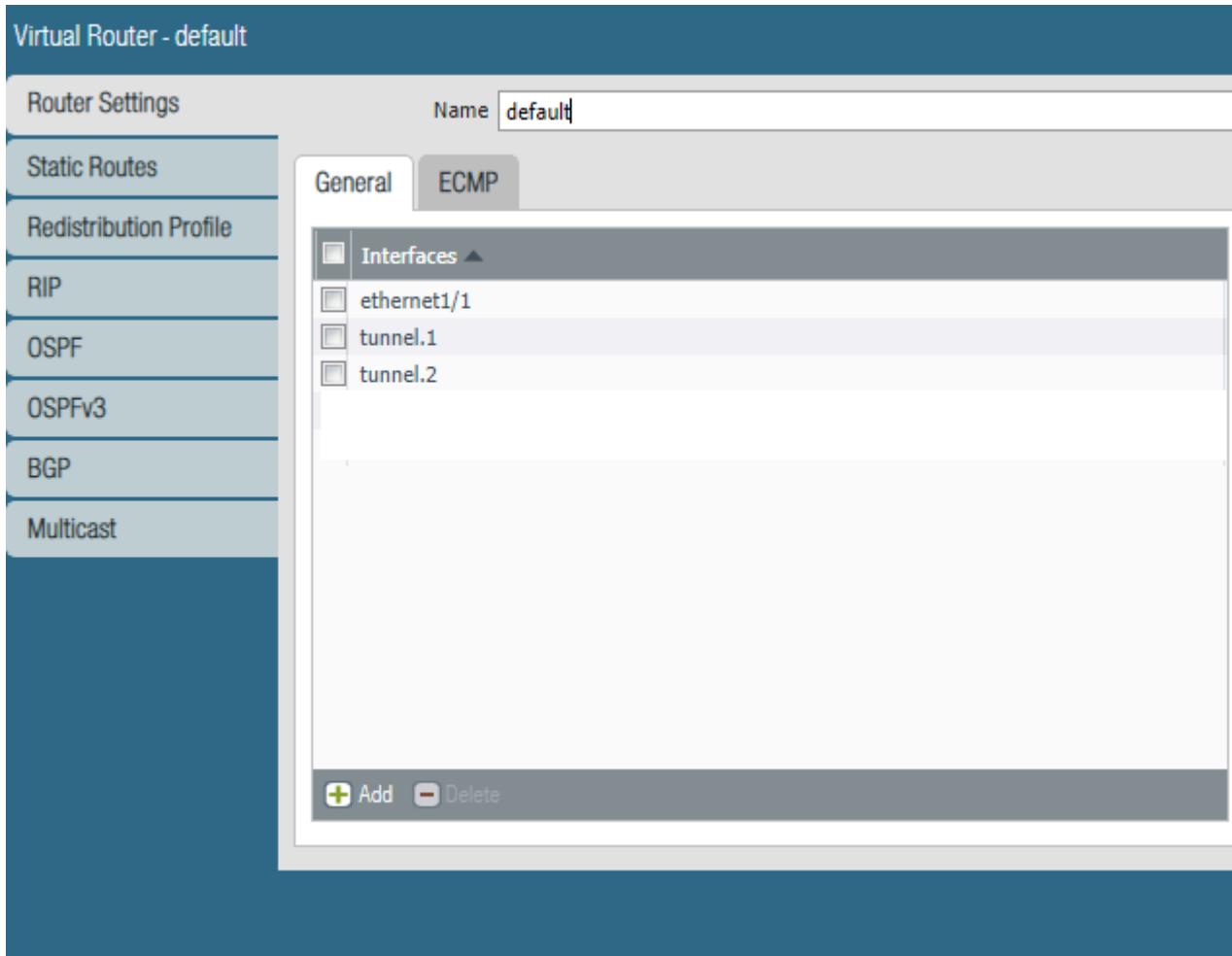


Figure 20: Virtual Router General Settings

## Configure VPN on VM-Series

Refer to [the Palo Alto VPN Deployments document](#) for additional information on how to configure VPNs.

### Create IKE Crypto Profile on VM-Series

In the Palo Alto WebGUI, navigate to Network, then Network Profiles, then IKE Crypto. Click Add to open the IKE Crypto Profile window and create a new IKE crypto profile with the following specifications:

- Name: Suite-B-GCM-256

- DH Group: group20
- Encryption: aes-256-cbc
- Authentication: sha384
- Under Timers, select Hours for Key Lifetime and type 8. Type 0 for IKEv2 Authentication Multiple.

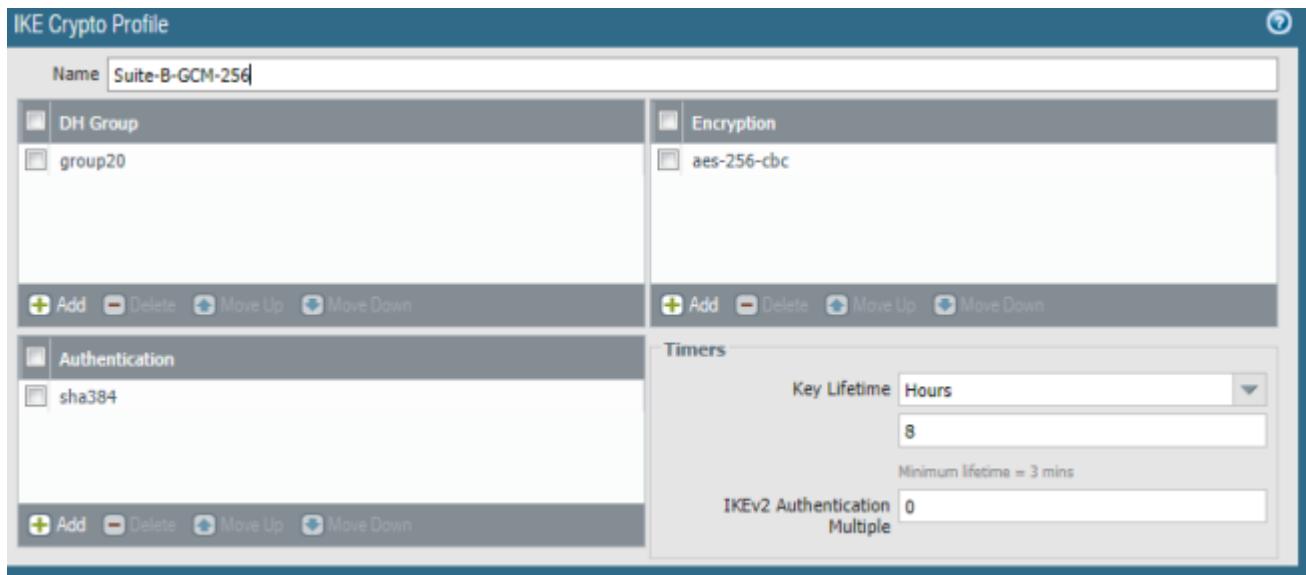


Figure 21: IKE Crypto Profile Configuration

### Create IKE Gateway on VM-Series

In the Palo Alto WebGUI, navigate to Network, then Network Profiles, then IKE Gateway. Click Add to open the IKE Gateway window and configure a new IKE gateway.

- In the General tab, enter the following configuration:
  - › Name: on-prem-IKE
  - › Version: IKEv2 only mode
  - › Address Type: IPv4
  - › Interface: ethernet1/1
  - › Local IP Address: IP address of ethernet1/1
  - › Peer IP Address Type: IP
  - › Peer Address: public IP of the remote or branch site
  - › Authentication: Pre-Shared Key
  - › Local Identification: Select FQDN (hostname) and xi-pa.nutanix.com
  - › Peer Identification: Select FQDN (hostname) and onprem-pa.nutanix.com

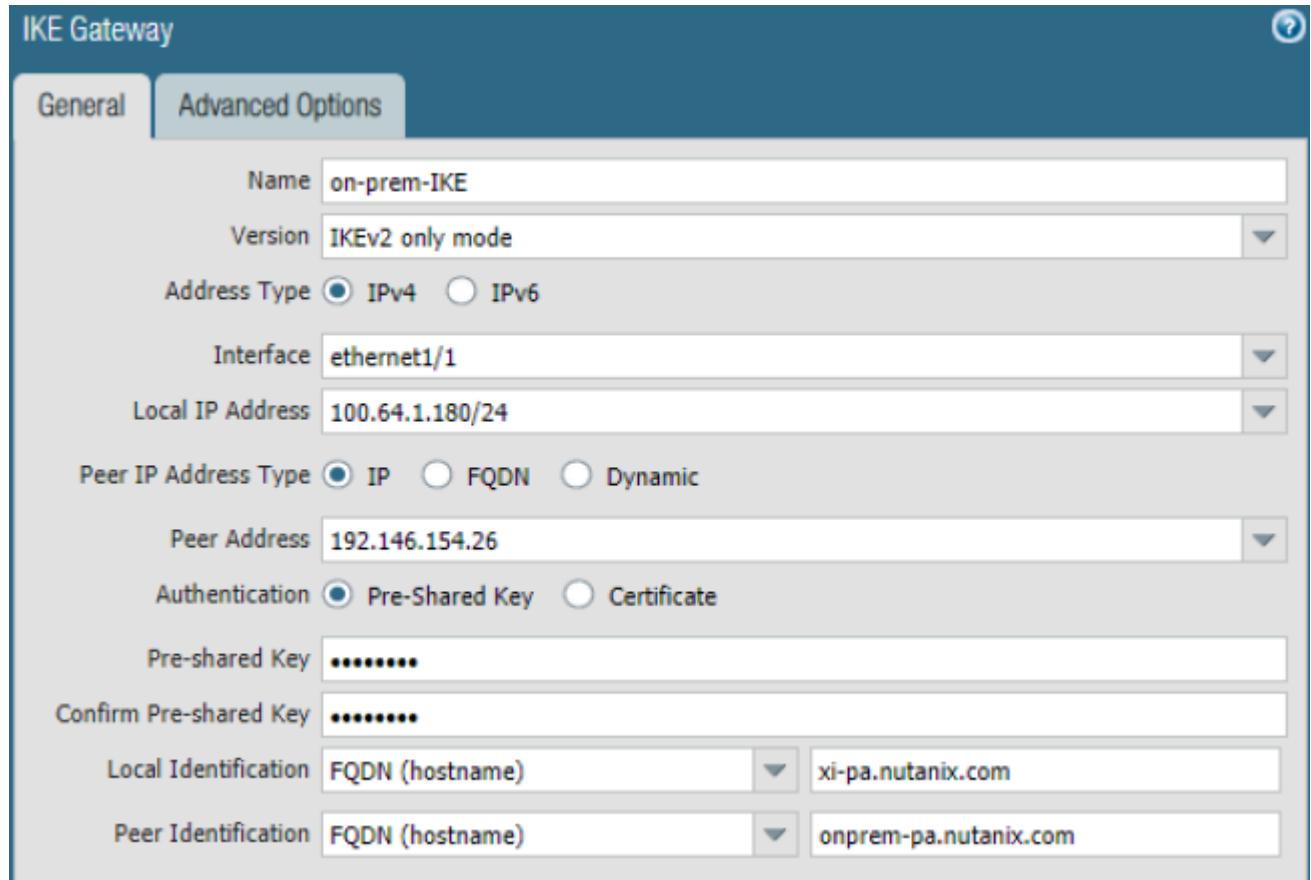


Figure 22: IKE Gateway General Configuration

- In the Advanced Options tab, select the checkboxes for Enable Passive Mode and Enable NAT Traversal on the Xi VM-Series. Select Suite-B-GCM-256 for the IKE crypto profile, select the checkbox for Liveness Check, and type 5 for the Interval (sec).

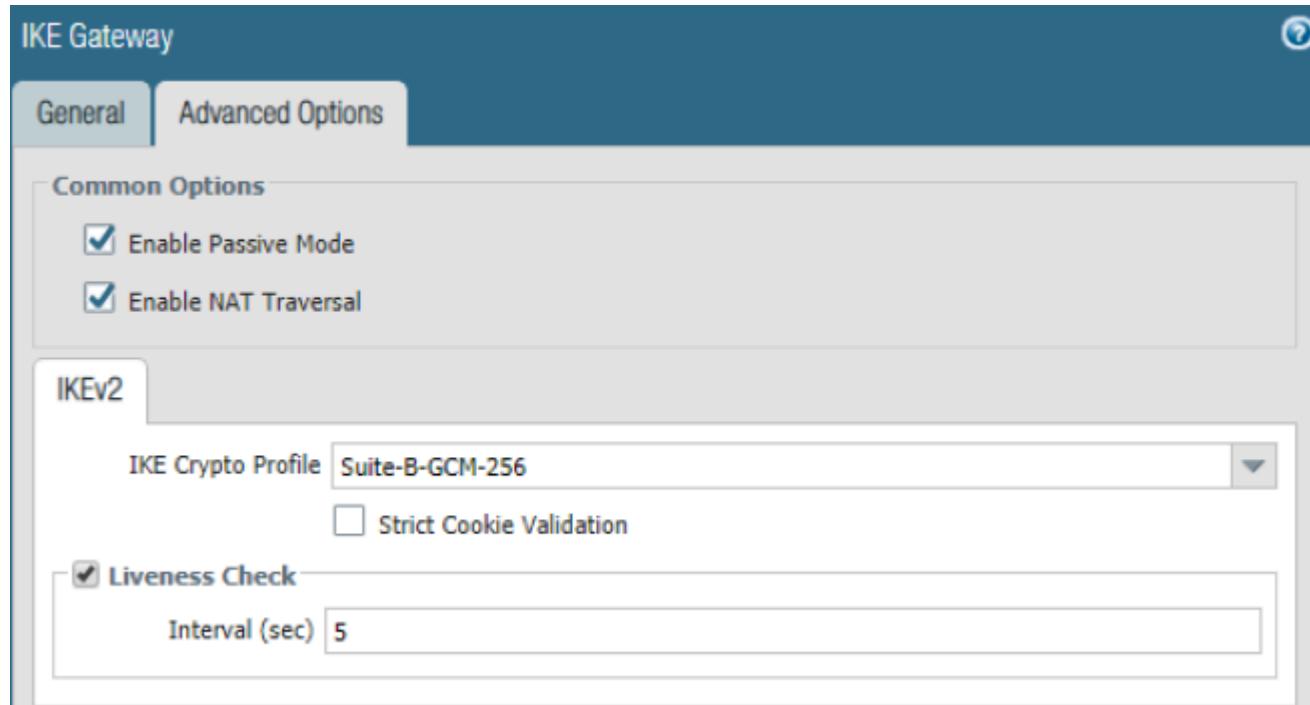


Figure 23: IKE Gateway Advanced Options

For additional remote sites, repeat this configuration, changing the peer address.

#### Create IPSec Crypto Profile on VM-Series

In the Palo Alto WebGUI, navigate to Network, then Network Profiles, then IPSec Crypto. Click Add to open the IPSec Crypto Profile window and configure a new IPSec crypto profile with the following configuration:

- Name: Suite-B-GCM-256
- IPSec Protocol: ESP
- DH Group: group20
- Encryption: aes-256-gcm
- Lifetime: Hours, 1
- Leave the Authentication and Enable sections cleared.

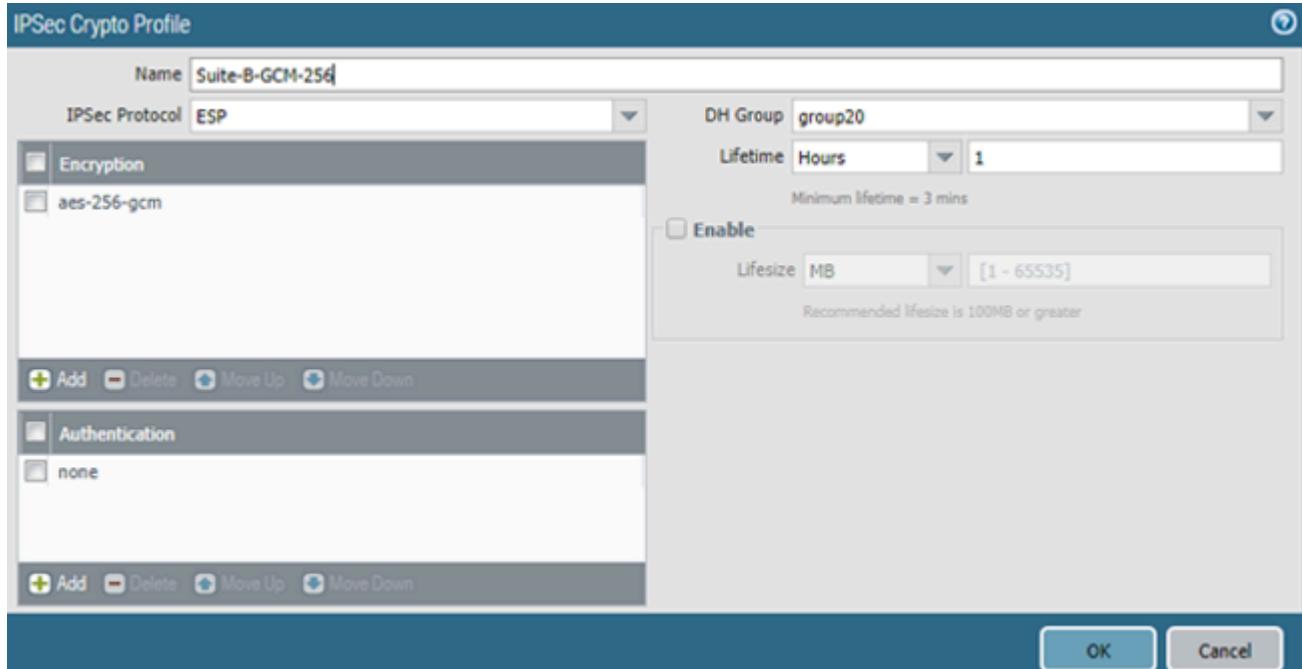


Figure 24: IPSec Crypto Profile Configuration

### Create IPSec Tunnels on VM-Series

In the Palo Alto WebGUI, navigate to Network, then IPSec Tunnels. Click Add to open the IPSec Tunnel window and create an IPsec tunnel to each on-premises VM-Series VM.

- In the General tab, enter the following specifications:
  - › Name: on-prem-ipsec
  - › Tunnel Interface: Select the same tunnel interface you used to connect to the on-premises series VM.
  - › Type: Auto Key
  - › Address Key: IPv4
  - › IKE Gateway: Select the IKE gateway you created in the Create IKE Gateway on VM-Series section.
  - › IPSec Crypto Profile: Select the IKE crypto profile you created in the Create IKE Crypto Profile on VM-Series section.

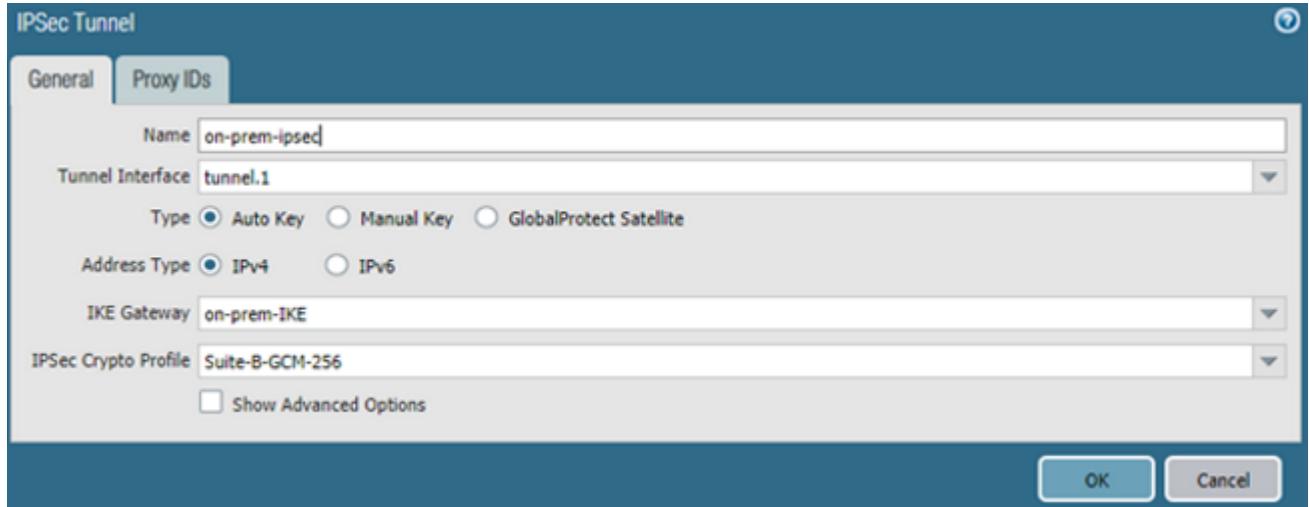


Figure 25: IPSec Tunnel on-prem-ipsec

- Repeat this process to create on-prem2-ipsec, changing the name and using the other tunnel interface.

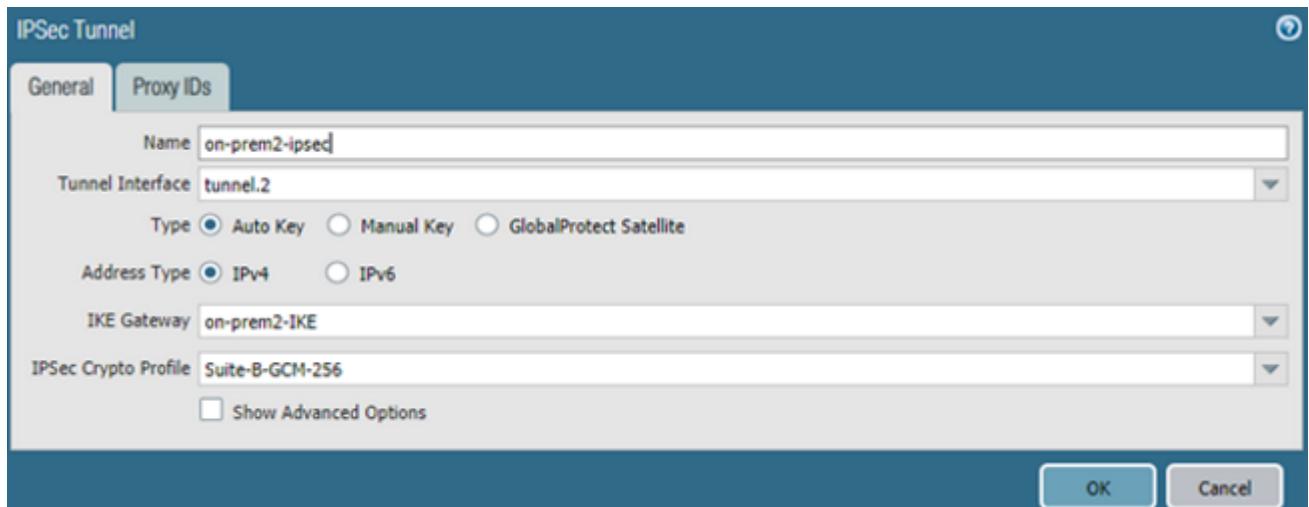


Figure 26: IPSec Tunnel on-prem2-ipsec

## Configure Routing on VM-Series

Refer to the [Palo Alto Border Gateway Protocol \(BGP\) document](#) for more information on configuring BGPs.

In the Palo Alto WebGUI, navigate to Network, then Virtual Router. Click default to open the default Virtual Router window. At the top of the BGP tab, enter the following configuration:

- Select Enable.
- Use the IPv4 address for Router ID to ensure the router ID is unique.
- Assign an AS Number between 1 and 4,294,967,295.

Then configure the settings in the General BGP tab:

- Don't select Reject Default Route; this setting ignores any default routes advertised by BGP peers.
- Select Install Route to update the global routing table with BGP routes.
- Select Aggregate MED to enable route aggregation even when routes have different multiexit discriminator (MED) values.
- Specify a Default Local Preference (used to determine preferences among different paths).
- Select the AS Format that supports interoperability for your deployment.
- Leave the Always Compare MED checkbox cleared.
- Select Deterministic MED comparison.

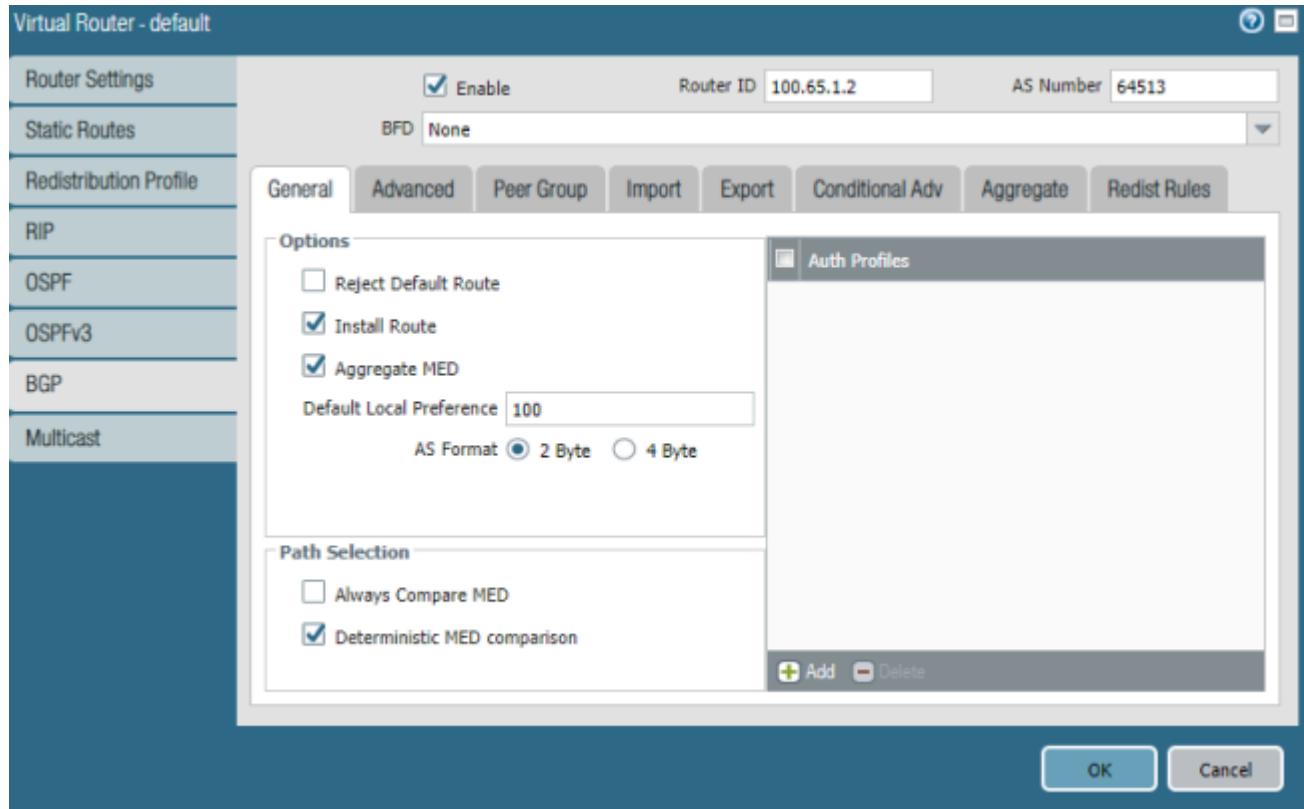


Figure 27: BGP General Settings

In the Advanced tab:

- First AS for EBGP is enabled by default; keep this default setting.
- Select Graceful Restart and enter 120 for Stale Route Time (sec), Local Restart Time (sec), and Max Peer Restart Time (sec).
- Under Dampening Profiles, select the checkbox in the Enable column for Profile Name default.

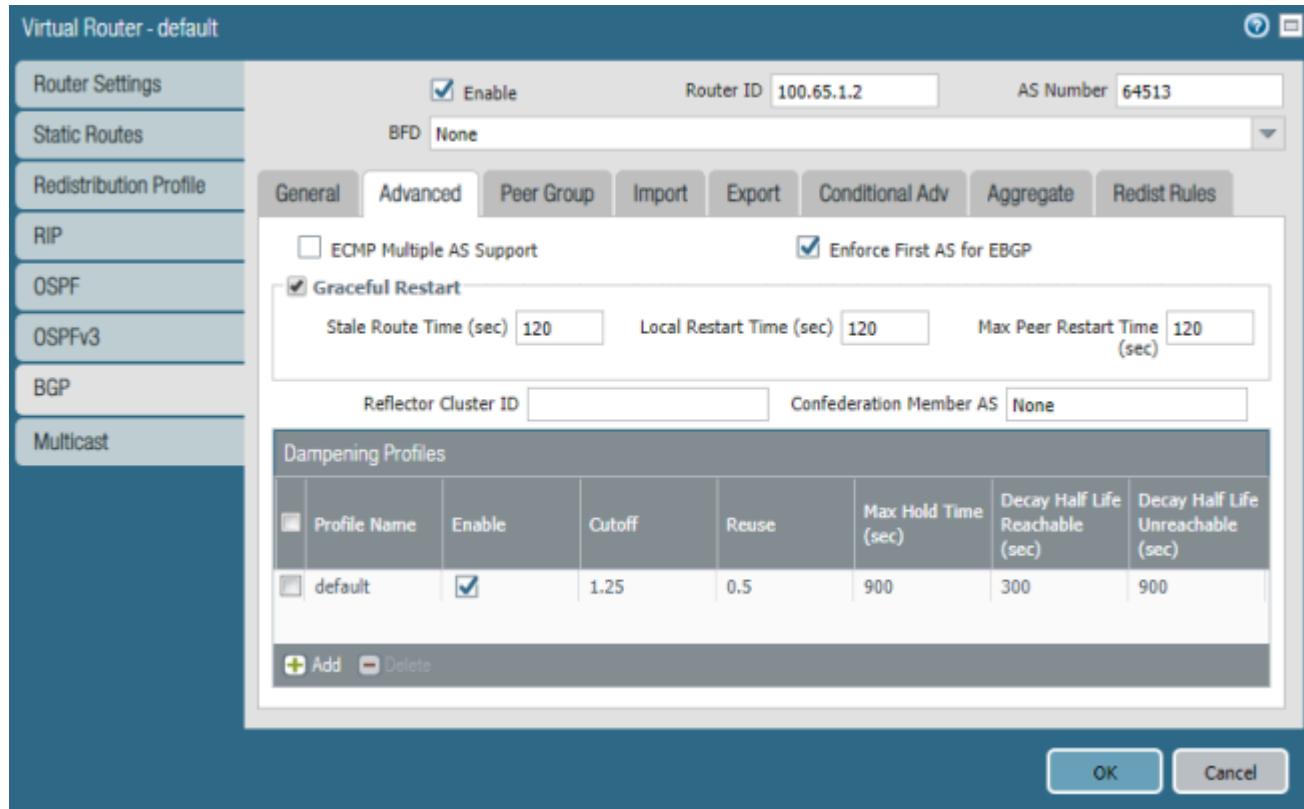


Figure 28: BGP Advanced Settings

In the Peer Group tab:

- Click Add to open the Peer Group/Peer window and create the following peer group:
  - › Name: peergroup1
  - › Select the Enable checkbox.
  - › Type: EBGP
  - › Select the checkboxes for Aggregated Confed AS Path (default) and Soft Reset With Stored Info.
  - › Select Original for Import Next Hop.
  - › Select Use Self for Export Next Hop.

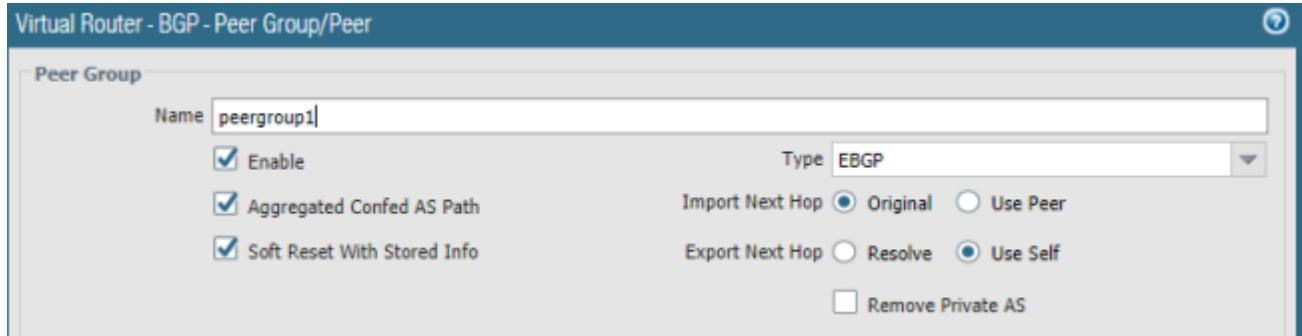


Figure 29: BGP Peer Group Settings

- Still in the Peer Group/Peer window, click Add and create the following peer:
  - › Name: onprem-pa
  - › Select the Enable checkbox.
  - › Peer AS: 64512
  - › In the Addressing tab, Address Family Type is IPv4 (default) and Subsequent Address Family is Unicast (default). In the Local Address section, select tunnel.1, which is connected to the peer, as the interface, and select 100.65.1.2 as the tunnel.1 IP. In the Peer Address section, enter 100.65.1.1.
  - › In the Connection Options tab, use the default settings for all options.
  - › In the Advanced tab, select Inherit Protocol's Global BFD Profile for BFD and use the default settings for the other options.

Virtual Router - BGP - Peer Group - Peer

Name	onprem-pa
<input checked="" type="checkbox"/> Enable	
Peer AS	64512
<b>Addressing</b> <b>Connection Options</b> <b>Advanced</b>	
<input type="checkbox"/> Enable MP-BGP Extensions	
Address Family Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
Subsequent Address Family	<input checked="" type="checkbox"/> Unicast <input type="checkbox"/> Multicast
<b>Local Address</b>	
Interface	tunnel.1
IP	100.65.1.2/30
<b>Peer Address</b>	
IP	100.65.1.1
<b>OK</b> <b>Cancel</b>	

Figure 30: Peer Addressing Options

Virtual Router - BGP - Peer Group - Peer

Name

Enable

Peer AS

Addressing    Connection Options    Advanced

Auth Profile

Keep Alive Interval (sec)

Multi Hop

Open Delay Time (sec)

Hold Time (sec)

Idle Hold Time (sec)

Min Route Advertisement Interval (sec)

Incoming Connections    Outgoing Connections

Remote Port   
 Allow

Local Port   
 Allow

OK    Cancel

Figure 31: Peer Connection Options

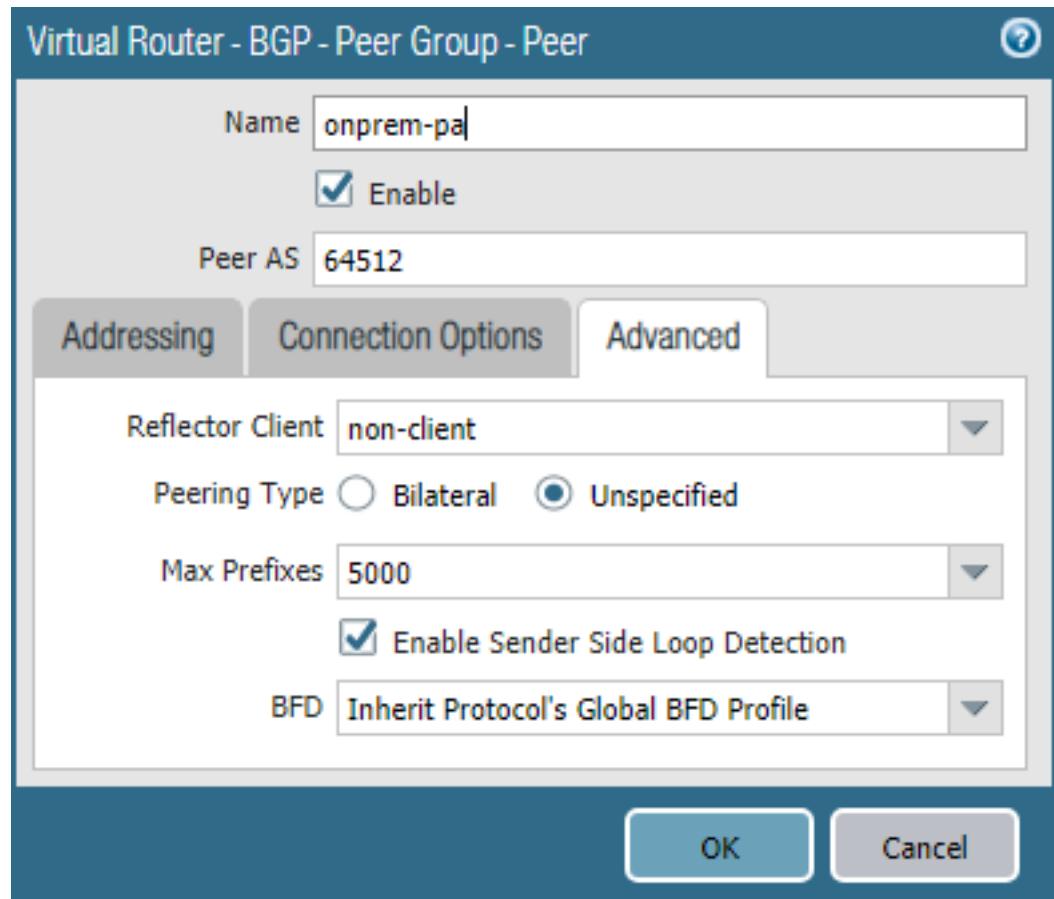


Figure 32: Peer Advanced Options

You have now configured peergroup1 and its peer.

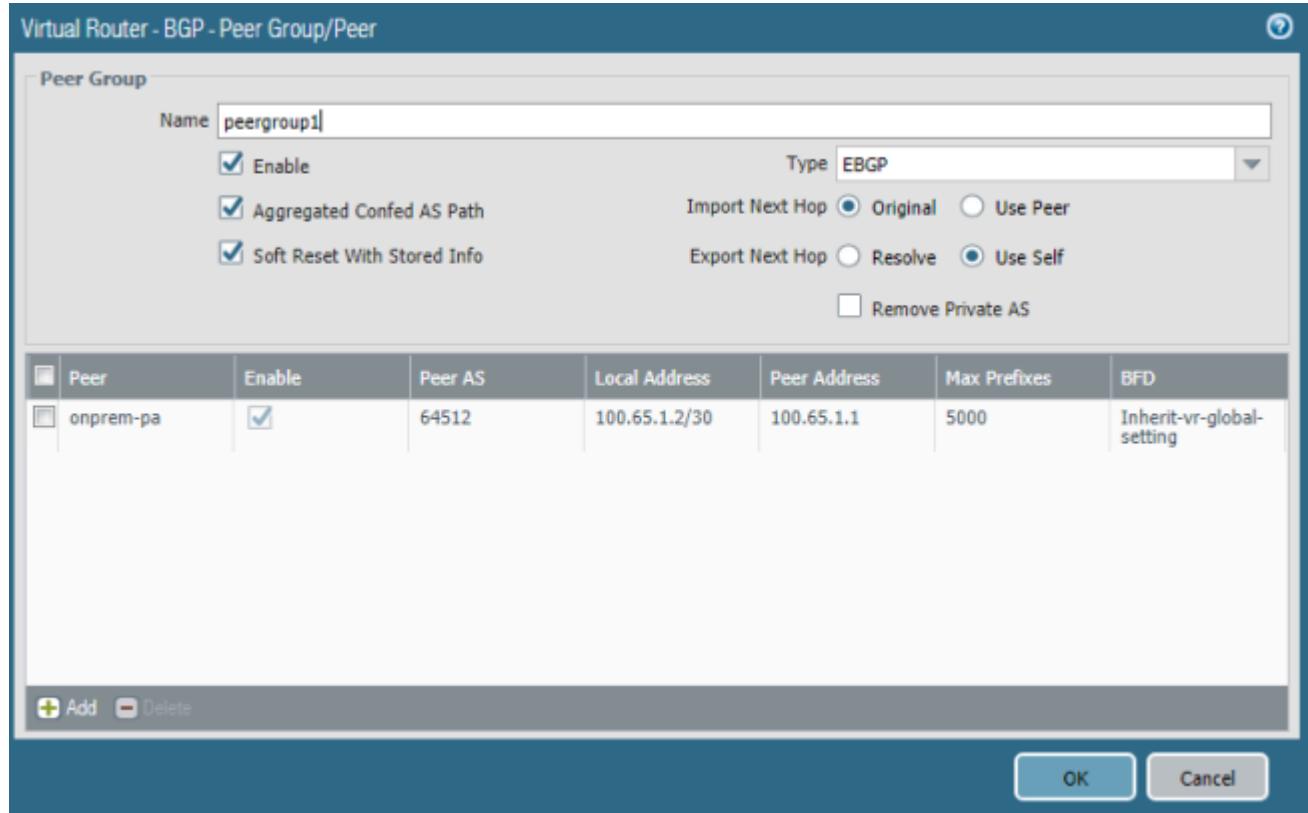


Figure 33: peergroup1 with onprem-pa Peer

- Back in the Peer Group tab, click Add to create another peer group and repeat the peer group creation steps to create a second peer group, named op-peer2.
- Still in the Peer Group/Peer window, click the Add button and repeat the peer creation steps to create a second peer, named op2. Set its local address interface to tunnel.2 and the IP to 100.66.1.2/30. Set the peer IP address to 100.66.1.1.

You have now configured the BGP peer groups.

The screenshot shows the 'Virtual Router - default' configuration page. On the left, a sidebar lists options: Router Settings, Static Routes, Redistribution Profile, RIP, OSPF, and OSPFv3. The 'Router Settings' tab is active, displaying the following configuration:

- Enable:** Checked
- Router ID:** 100.65.1.2
- AS Number:** 64513
- BFD:** None

Below these settings, there are tabs for General, Advanced, Peer Group, Import, Export, Conditional Adv, Aggregate, and Redist Rules. The 'Peer Group' tab is selected, showing a table of peers:

Name	Enable	Type	Peers		
			Name	Peer Address	Local Address
peergroup1	<input checked="" type="checkbox"/>	ebgp	onprem-pa	100.65.1.1	100.65.1.2/30
op-peer2	<input checked="" type="checkbox"/>	ebgp	op2	100.66.1.1	100.66.1.2/30

Figure 34: BGP Peer Groups

In the Import tab:

- Click Add Import Rule. In the Import Rule window that opens, name the rule `onprem_policy` and enable it.
- Under Used By, click Add to add the peer groups. Select the checkboxes beside `op-peer2` and `peergroup1`.

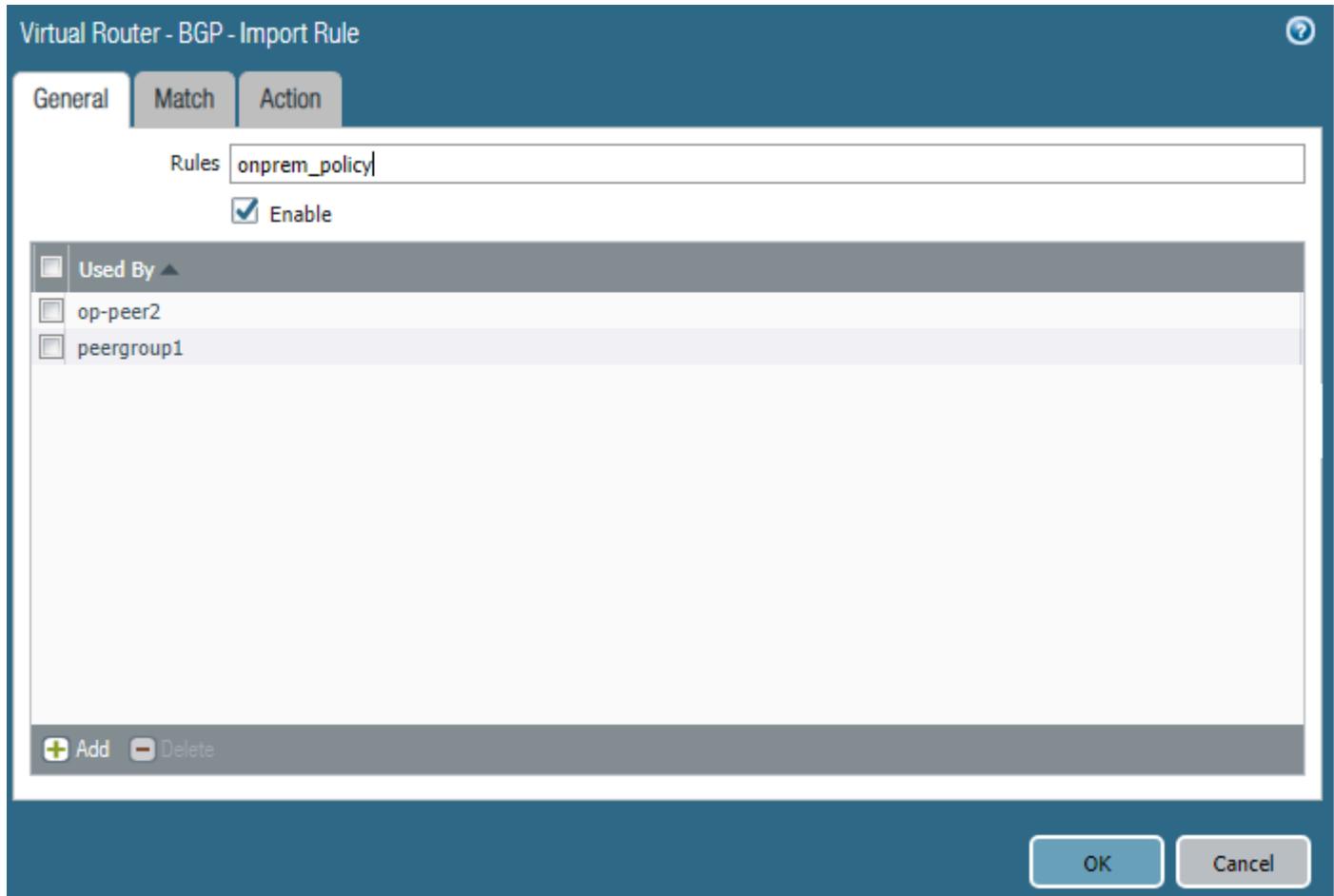


Figure 35: BGP Import Rule General Settings

- In the Action tab of the Import Rule window, keep the default configuration but set the local preference to 200. BGP gives preference to prefixes it receives that have higher local preference and inserts them into the routing table.

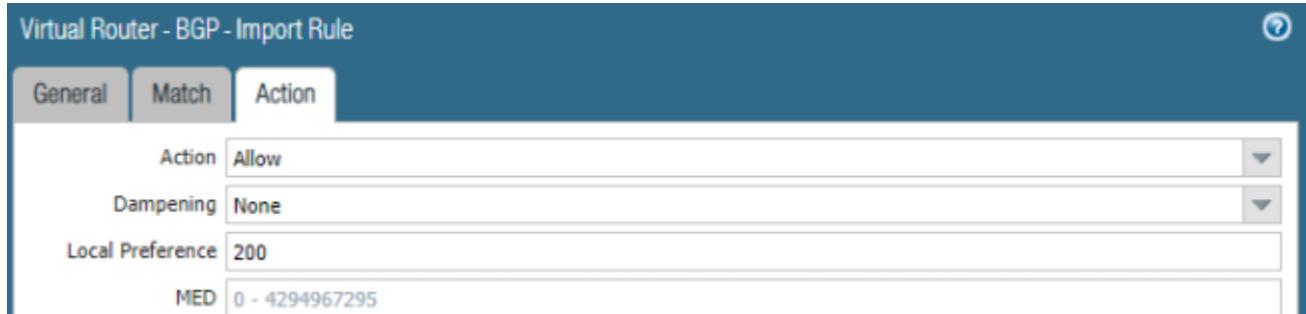


Figure 36: BGP Import Rule Action Settings

Return to the Import tab, and repeat this process with the following changes:

- Name the import rule `import1` and enable it.
- Under Used by, select the checkbox for `Xi-Xi-ibgp`.
- In the Action tab of the Import Rule window, set the local preference to 50.

You've now configured all the import rules for BGP.

General		Advanced		Peer Group		Import		Export		Conditional Adv		Aggregate		Redist Rules	
Name		Enable		Used By		Match								Action	
<input type="checkbox"/>	<code>import1</code>	<input checked="" type="checkbox"/>		<code>Xi-Xi-ibgp</code>											<code>allow</code>
<input type="checkbox"/>	<code>onprem_policy</code>	<input checked="" type="checkbox"/>		<code>op-peer2</code>											<code>allow</code>
<code>peergroup1</code>															

Figure 37: BGP Import Rules

In the Export tab:

- Click Add in the Export Rule pane. In the Export Rule window that appears, name the rule `export1` and enable it.
- Under Used By, click Add to add the peer groups, then select the checkboxes for `peergroup1`, `op-peer2`, and `Xi-Xi-ibgp`.

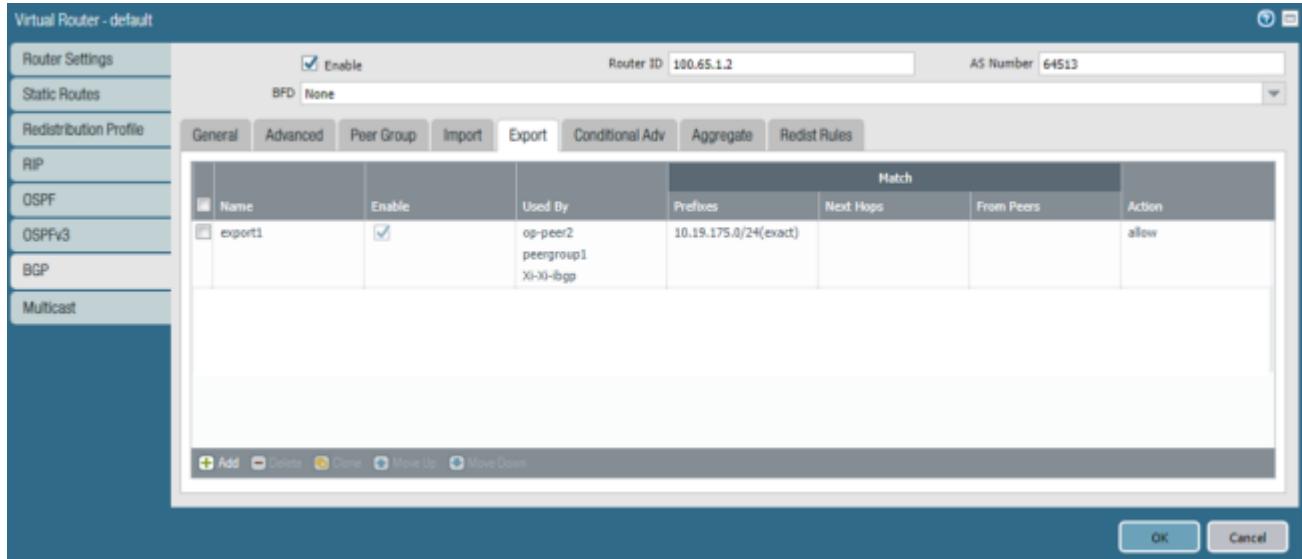


Figure 38: BGP Export Rule General Settings

- In the Match tab of the Export Rule window, add the address prefix 10.19.175.0/24 and select the checkbox for Exact.

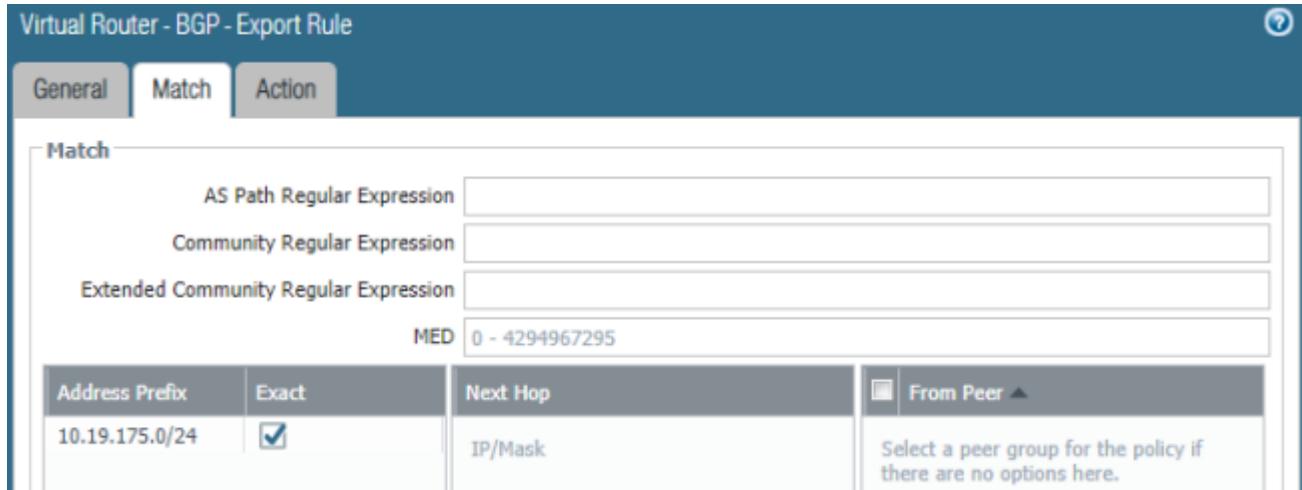


Figure 39: BGP Export Rule Match Settings

You have now configured the BGP export rule.

Match							
	Name	Enable	Used By	Prefixes	Next Hops	From Peers	Action
<input type="checkbox"/>	export1	<input checked="" type="checkbox"/>	op-peer2 peergroup1 Xi-Xi-ibgp	10.19.175.0/...			allow

Figure 40: BGP Export Rule

In the Redist Rules tab:

- Enable Allow Redistribute Default Route.

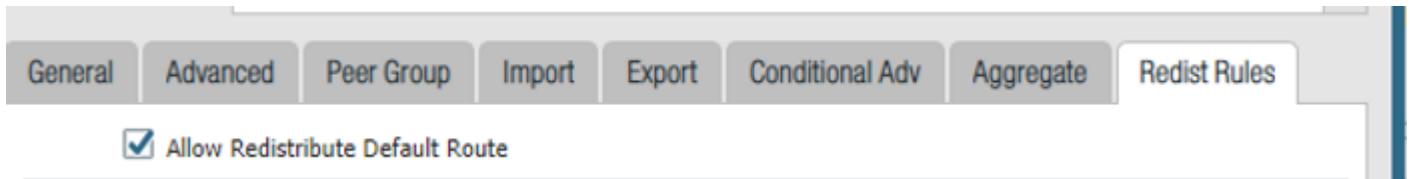


Figure 41: BGP Redist Rules Allow Redistribute Default Route

- Click Add in the Rule pane. In the Redistribute Rules window that appears, name the rule redis3 and enable it. Keep the default values for everything else.

Virtual Router - BGP - Redistribute Rules - Rule

Address Family Type  IPv4  IPv6

Name **redis3**  
Enter a IPv4 subnet or create a IPv4 redistribution profile first

Enable

Metric **[1 - 65535]**

Set Origin **incomplete**

Set MED **0 - 4294967295**

Set Local Preference **0 - 4294967295**

Set AS Path Limit **1 - 255**

Figure 42: BGP Redistribute Rule redis3

You have now configured the BGP redistribute rule.

General	Advanced	Peer Group	Import	Export	Conditional Adv	Aggregate	Redist Rules		
<input checked="" type="checkbox"/> Allow Redistribute Default Route									
Name	Type	Enable	Set Origin	Metric	Set MED	Set Local Prefere...	Set AS Path Limit	Set Commu...	Set Extended Commu...
redis3	ipv4	<input checked="" type="checkbox"/>	incompl...						

Figure 43: BGP Redistribute Rule

## Create VPC Policy to Reroute Traffic Through Xi

In priority-based routing, the policy's priority determines when it is used. In the Production VPC, create two priority policies to reroute traffic:

1. One with a priority of 299 that reroutes traffic going from 10.19.175.0/24 to 10.16.80.0/24 to go to 100.64.1.180 instead.
2. One with a priority of 300 that reroutes traffic going from 10.19.175.0/24 to 10.16.40.0/24 to go to 100.64.1.180 instead.

In the Xi web portal, go to the Explore tab, click Production, then click Policies. In the Policies tab, click the More dropdown menu and select Create Policy:

- Set Priority as 299, set Source Subnet IP as 10.19.175.0/24, set Destination Subnet IP as 10.16.80.0/24, and set Reroute IP as 100.64.1.180. Keep the default values for everything else.

PRIORITY	UNDERSTAND PRIORITIES
299	
SOURCE	
Custom	
SOURCE SUBNET IP	
10.19.175.0/24	
DESTINATION	
Custom	
DESTINATION SUBNET IP	
10.16.80.0/24	
PROTOCOL	
Any	
ACTION	
Reroute	
REROUTE IP	
100.64.1.180	

Figure 44: Production VPC Priority Policy

Repeat this process to create the second policy, changing the following specifications:

- Set Priority as 300, set Source Subnet IP as 10.19.175.0/24, set Destination Subnet IP as 10.16.40.0/24, and set Reroute IP as 100.64.1.180. Keep the default values for everything else.

You have now created the two required VPC policies.

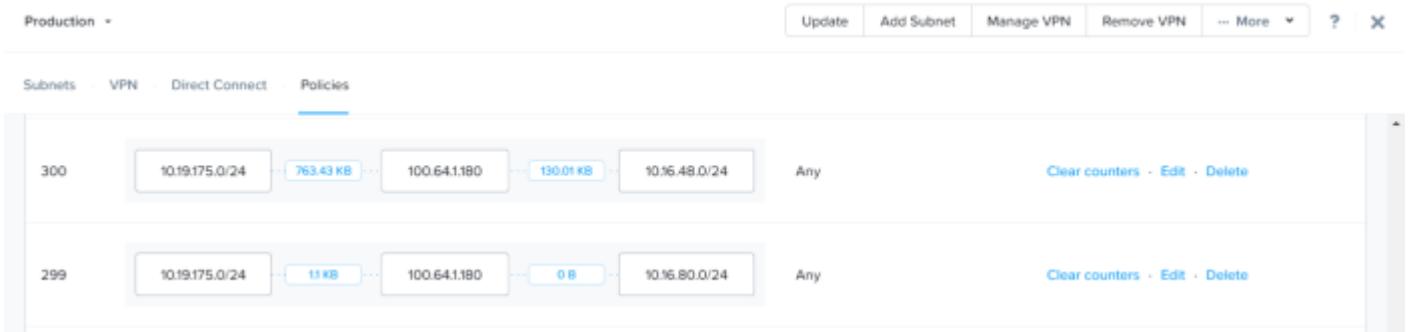


Figure 45: Two Required VPC Policies

## Use Case 1: Deploy and Configure VM-Series on On-Prem 1

Sign in to your AHV cluster and upload the VM-Series KVM image:

- Navigate to Home, then Settings, then Image Configuration. Click Upload Image.
- Select Upload a file as the Image Source and upload the VM-Series KVM image.

Create Image

Name  
PA-VM-KVM-8.1.3.qcow2

Annotation

Image Type  
DISK

Storage Container  
default-container-78880

Image Source  
 From URL  
 Upload a file [?](#) Choose File PA-VM-KVM-8.1.3.qcow2

[Back](#) [Cancel](#) [Save](#)

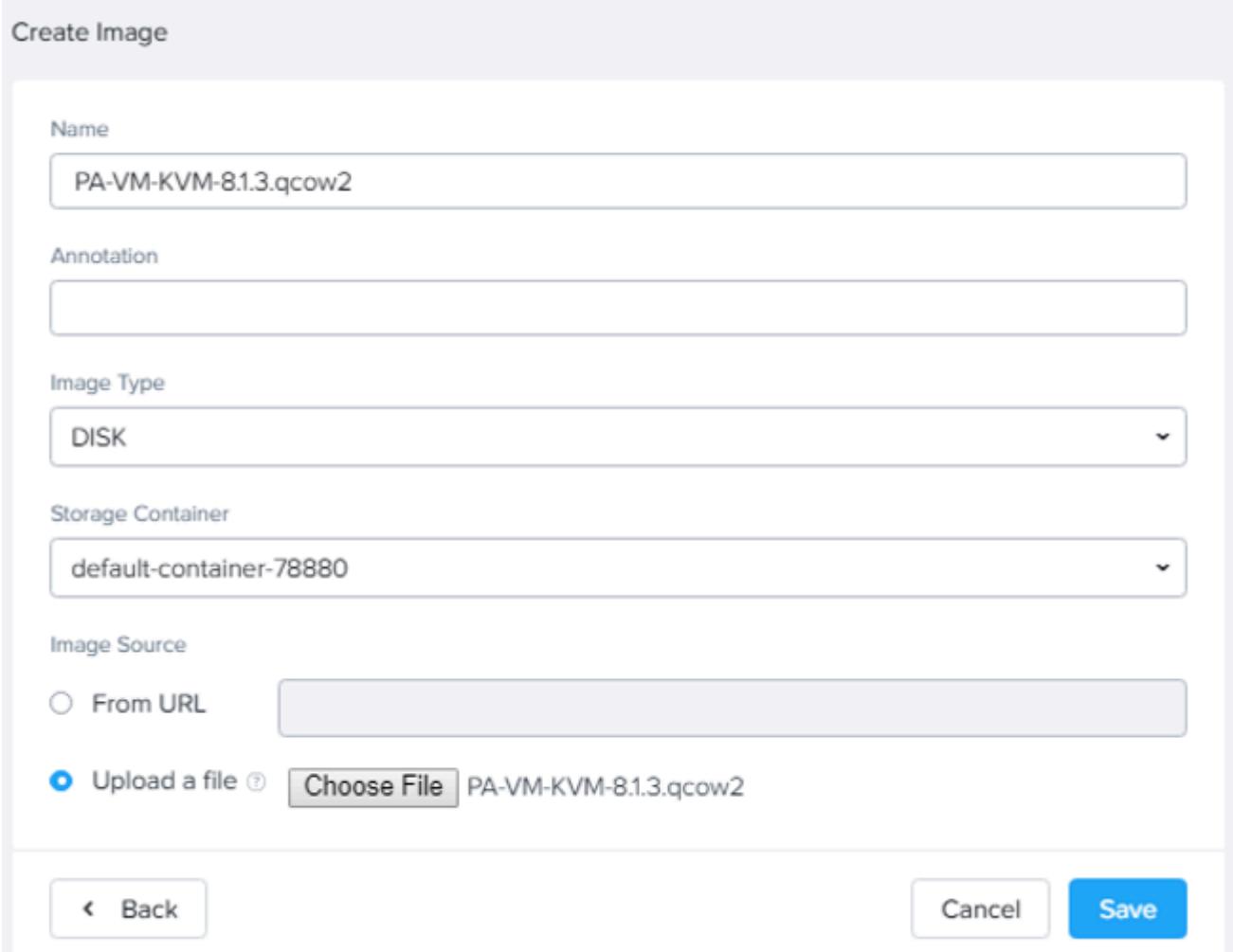


Figure 46: Create Image on On-Prem 1

## Network Configuration on On-Prem 1

AHV clusters are by default configured with two virtual networks you can use to host VMs:

1. NR\_PRT\_DHCP: management interface of the VM.
2. NR\_PRT\_STATIC: data interface of the VM.

To create additional virtual networks, click VM in your AHV GUI. Select Network Config, then Virtual Networks, then Create Network. Configure as necessary for your environment.

Name

NR\_PRT\_DHCP

UUID

f504b9d4-ebab-4615-94a8-89e7d9f2dec0

VLAN ID [?](#)

3132

Enable IP address management

This gives AHV control of IP address assignments within the network.

Cancel

Save

Figure 47: Create Additional Virtual Network

The following image shows an example network configuration.

Network Configuration		?	X
Virtual Networks		Internal Interfaces	
<a href="#">+ Create Network</a>			
NAME	VLAN ID		
NR_INT_DHCP	vlan.3164		
NR_INT_STATIC	vlan.3180		
NR_PROD_DHCP	vlan.0		
NR_PRT_DHCP	vlan.3132		
NR_PRT_STATIC	vlan.3148		

Figure 48: Example Network Configurations

### Create VM on On-Prem 1

You need to create a VM for your first on-premises environment. However, before you can do that, you need to create a new network interface connection (NIC). The process is shown in the following figure.

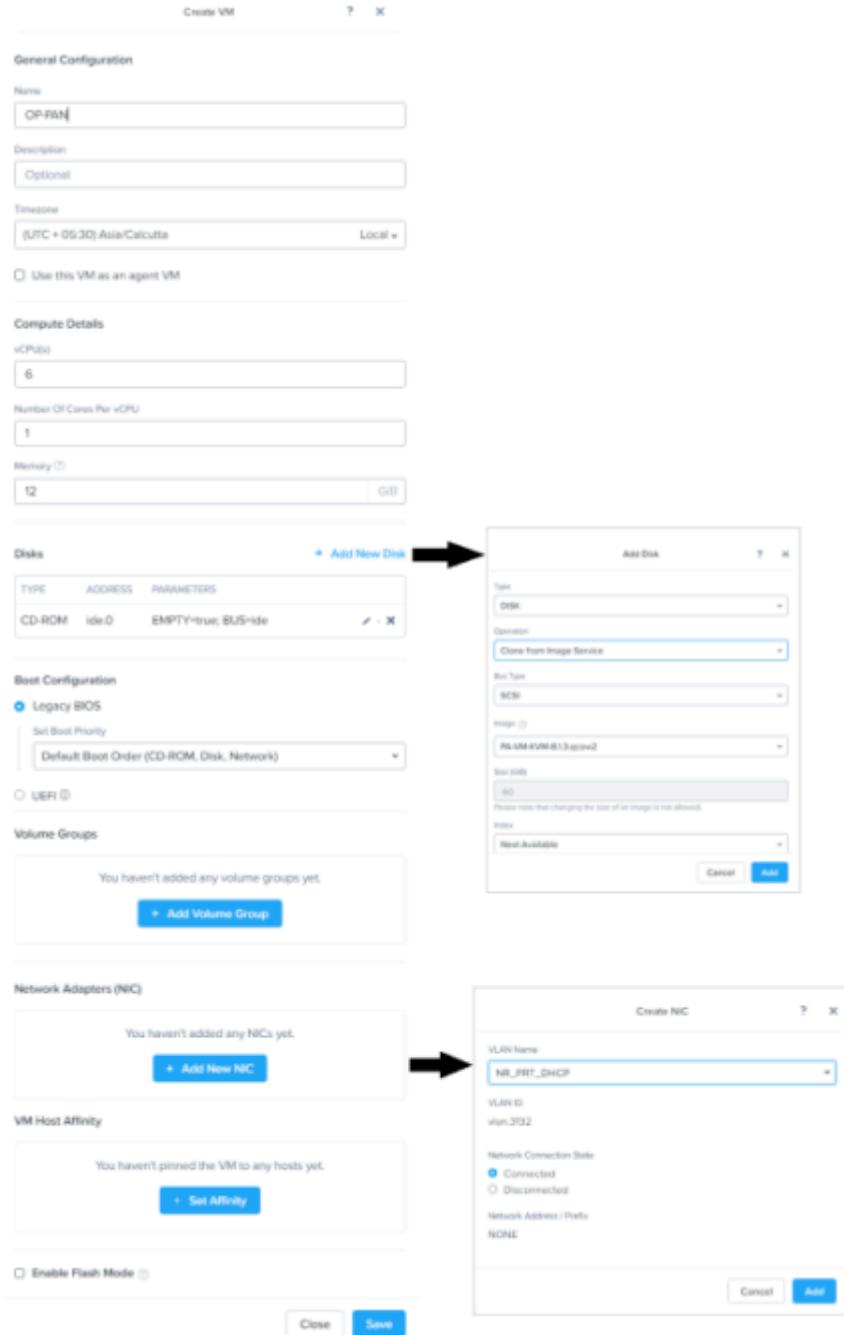


Figure 49: Create New Network Interface Connection (NIC)

Power on the VM-Series firewall and sign in.

## Create Interfaces and Zones on On-Prem 1

The following steps outline how to set up a VPN connection that allows you to connect LANs in on-prem 1 to your Nutanix Xi Cloud LAN. This configuration is a route-based VPN tunnel to connect Palo Alto Networks firewalls located at two sites. The firewall makes a routing decision based on the destination IP address.

Before you configure a VPN tunnel, you must configure the Ethernet interface, tunnel interface, zone, and virtual router.

### Configure Zone on On-Prem 1

- In the Palo Alto WebGUI, navigate to Network, then to Zones, then click Add Zone.
  - › Name the zone untrust.
  - › For Log Setting, select None.
  - › For Type, select Layer3.
  - › In the Interfaces section, click Add to add the ethernet1/1 and tunnel1 interfaces. (We describe the process for creating these interfaces in the Configure Tunnel Interfaces on On-Prem 1 section.)

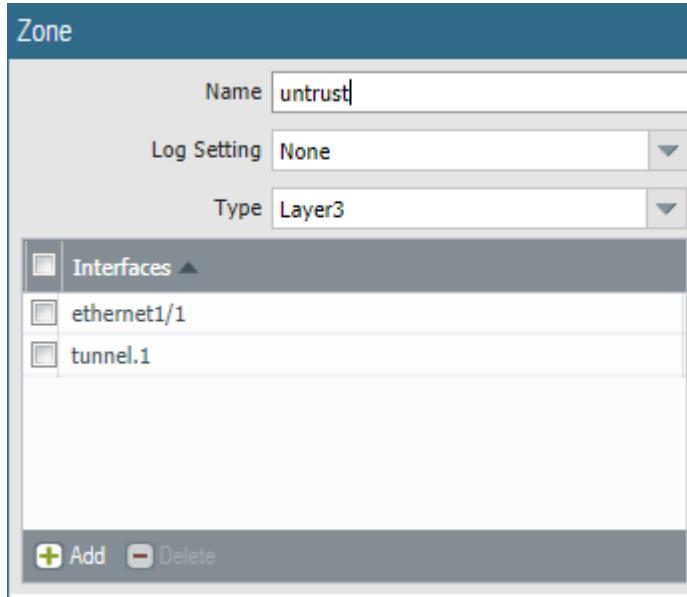


Figure 50: Zone Configuration on On-Prem 1

### Configure Ethernet Interface on On-Prem 1

Before you configure the Ethernet interface, create a management profile that can ping to test connectivity. Open the Palo Alto WebGUI and complete the following steps.

- In Palo Alto WebGUI, navigate to Network, then Network Profiles, then click Interface Management.
- Click Add to open the Interface Management Profile window. Name the profile allow\_all and configure it as shown in the following image.

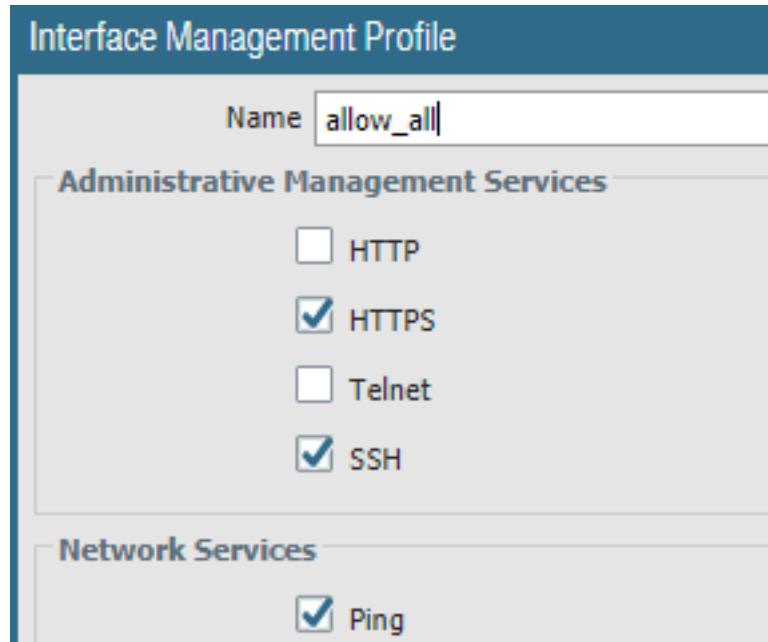


Figure 51: allow\_all Interface Management Profile for On-Prem 1 VM

Now you're ready to create the Ethernet interface.

- In the Palo Alto WebGUI, navigate to Network, then Interfaces, then Ethernet. Click ethernet1/1, which opens the Ethernet Interface window.
- Keep ethernet1/1 as the interface name, select Layer3 as the interface type, and use None as the Netflow Profile.
- In the Config tab, use the default virtual router and create the new zone untrust. (We describe this process in the Configure Zone on On-Prem 1 section.)

**Ethernet Interface**

Interface Name	ethernet1/1
Comment	
Interface Type	Layer3
Netflow Profile	None
<b>Config    IPv4    IPv6    Advanced</b>	
<b>Assign Interface To</b>	
Virtual Router	default
Security Zone	untrust

Figure 52: Ethernet Interface Configuration for On-Prem 1 VM

- In the IPv4 tab, assign a static IP address from the NR\_PRT\_STATIC subnet. We used 10.64.48.80/20.

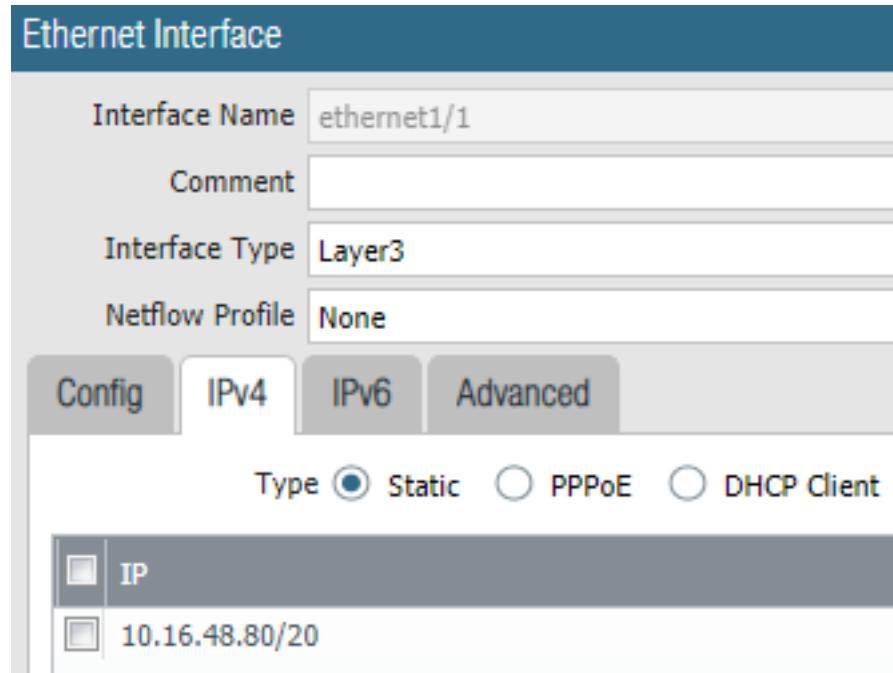


Figure 53: Ethernet Interface IP Configuration for On-Prem 1 VM

- In the Advanced tab, enter allow\_all for the management profile.

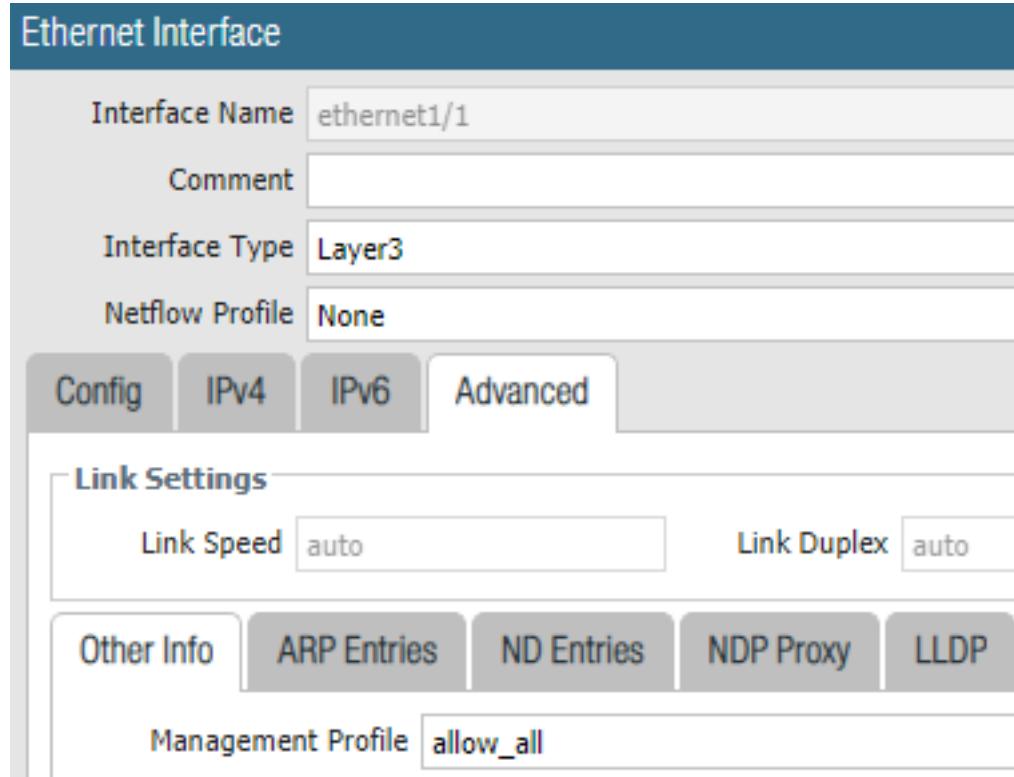


Figure 54: Ethernet Interface Advanced Configuration for On-Prem 1 VM

### Configure Tunnel Interface on On-Prem 1

Before you create the tunnel interface, you need to create an IP address for it, because you're going to use a dynamic routing protocol (BGP) to redirect traffic to the IPSec tunnel.

- In the Palo Alto WebGUI, navigate to Objects, then to Addresses. Click Add.
- In the Address window that appears, create a /30 IP address and click OK.

Now you're ready to create the tunnel interface.

- In the Palo Alto WebGUI, navigate to Network, then Interfaces, then Tunnel. Click Add.
- Leave tunnel as the Interface Name and keep Netflow Profile set to None.
- Under the Config tab, set the Virtual Router to default and the Security Zone to untrust.

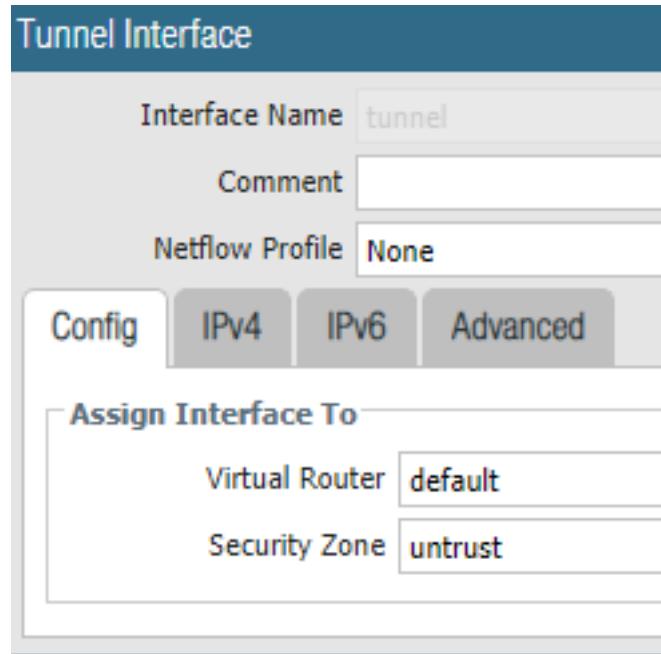


Figure 55: Tunnel Interface Configuration on On-Prem 1

- In the IPv4 tab, click Add and add IP address 100.65.1.1/30.

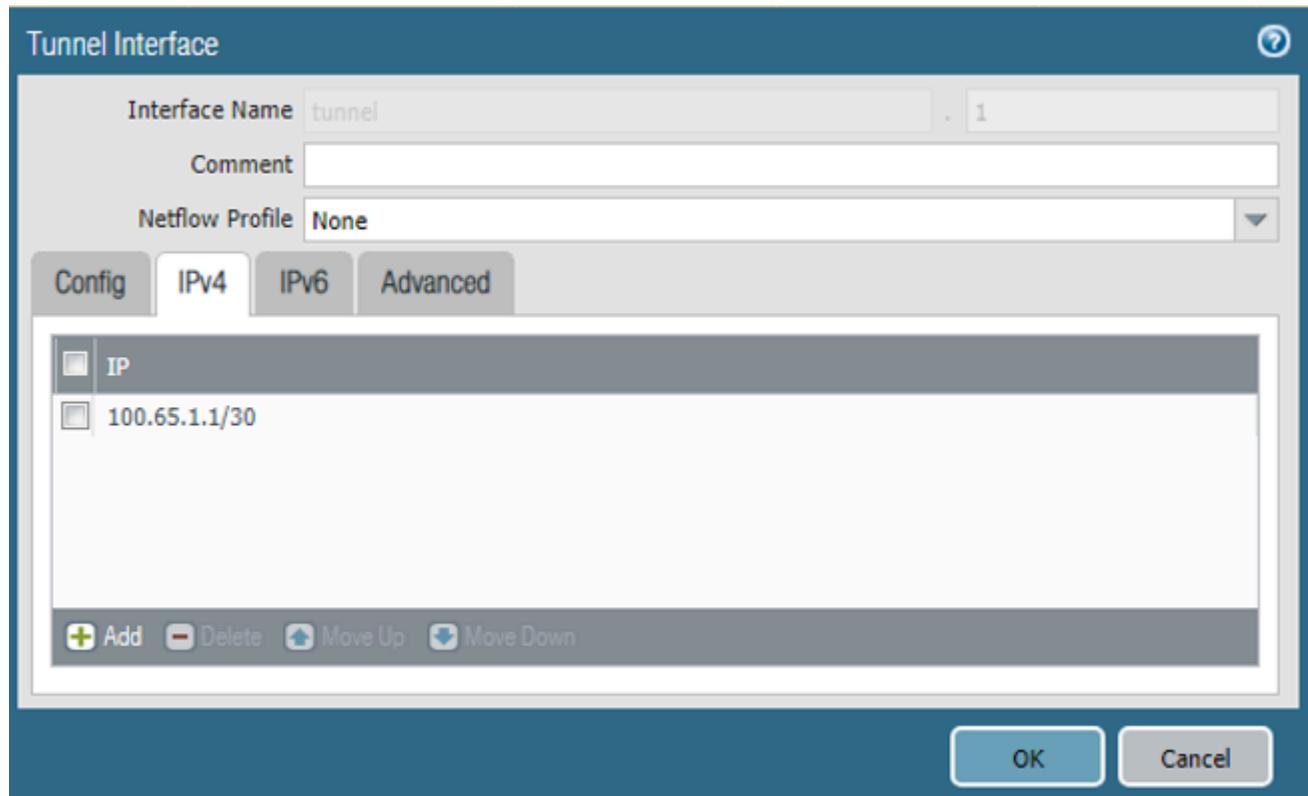


Figure 56: Tunnel Interface IPv4 Settings on On-Prem 1

#### Configure Virtual Router on On-Prem 1

In the Palo Alto WebGUI, use the default router (or create a new one) and add the Ethernet and tunnel interfaces to it.

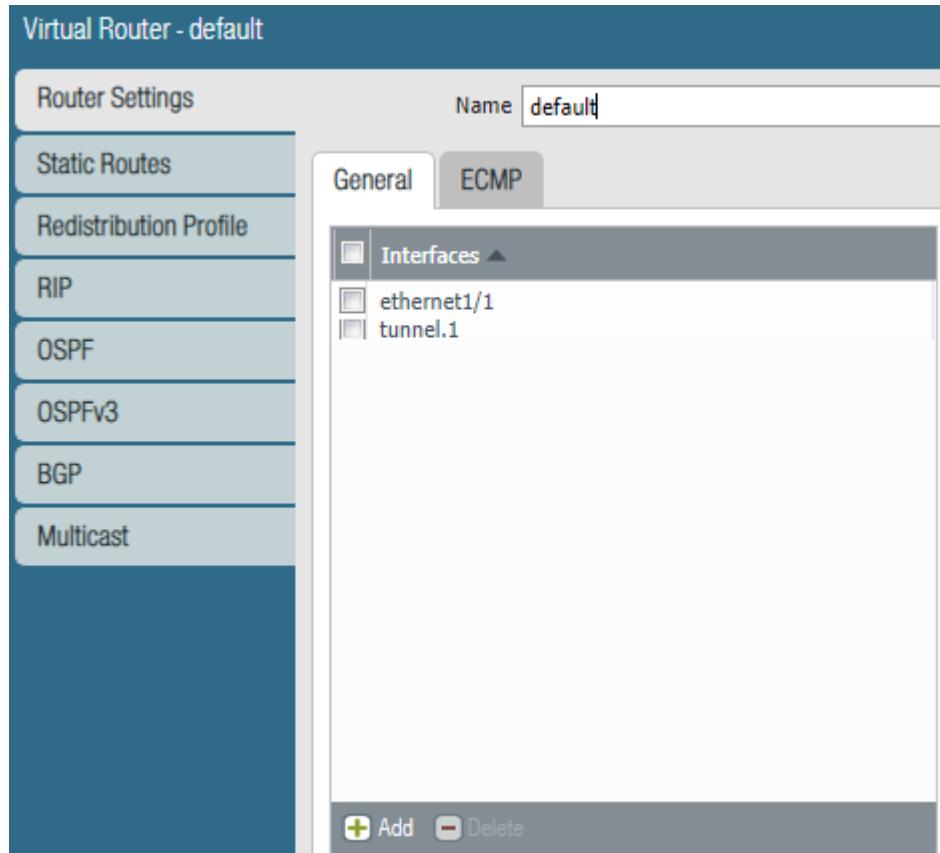


Figure 57: Virtual Router General Settings on On-Prem 1

## Configure VPN on On-Prem 1

Refer to [the Palo Alto VPN Deployments document](#) for additional information on how to configure VPNs.

### Create IKE Crypto Profile on On-Prem 1

In the Palo Alto WebGUI, navigate to Network, then Network Profiles, then IKE Crypto. Click Add to open the IKE Crypto Profile window and create a new IKE crypto profile with the following specifications:

- Name: Suite-B-GCM-256
- DH Group: group20
- Encryption: aes-256-cbc

- Authentication: sha384
- Under Timers, select Hours for Key Lifetime and type 8. Type 0 for IKEv2 Authentication Multiple.

### [Create IKE Gateway on On-Prem 1](#)

In the Palo Alto WebGUI, navigate to Network, then Network Profiles, then IKE Gateways. Click Add to open the IKE Gateway window and configure a new IKE gateway.

- In the General tab, enter the following configuration:
  - › Name: xi\_IKE
  - › Version: IKEv2 only mode
  - › Address Type: IPv4
  - › Interface: ethernet1/1
  - › Local IP Address: IP address of ethernet1/1
  - › Peer IP Address Type: IP
  - › Peer Address: public IP of the remote or branch site
  - › Authentication: Pre-Shared Key
  - › Local Identification: Select FQDN (hostname) and onprem-pa.nutanix.com
  - › Peer Identification: Select FQDN (hostname) and xi-pa.nutanix.com

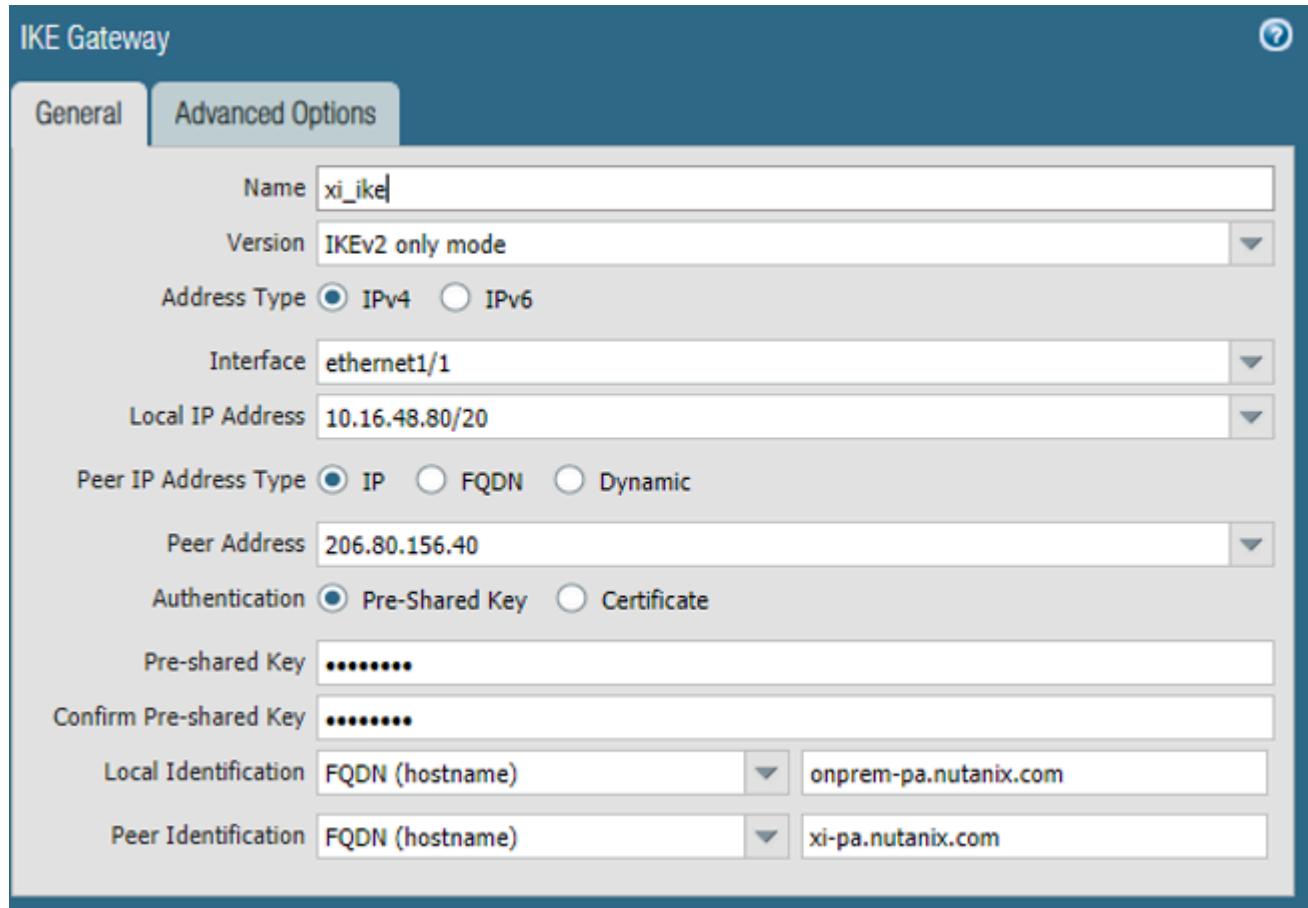


Figure 58: IKE Gateway General Configuration on On-Prem 1

- In the Advanced Options tab, select the checkbox for Enable NAT Traversal. Choose Suite-B-GCM-256 for the IKE crypto profile, select the checkbox for Liveness Check, and type 5 as the Interval (sec).

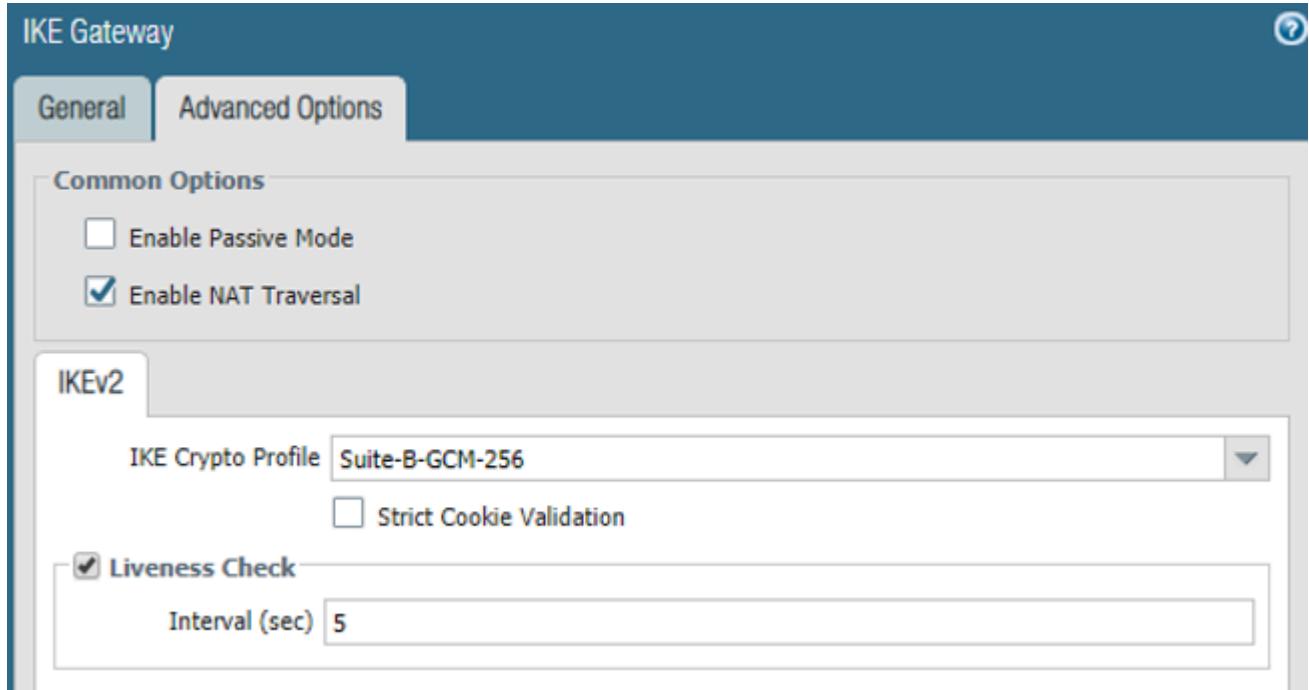


Figure 59: IKE Gateway Advanced Options on On-Prem 1

Repeat this process to create xi\_ike\_2, using the public IP of the remote or branch site as the peer address and xi-pa-2.nutanix.com as the peer ID.

### Configure Routing on On-Prem 1

Refer to the [Palo Alto Border Gateway Protocol \(BGP\) document](#) for more information on configuring BGPs.

In the Palo Alto WebGUI, navigate to Network, then Virtual Router. Click default to open the default Virtual Router window. At the top of the BGP tab, enter the following configuration:

- Select the checkbox for Enable.
- Use the IPv4 address for Router ID to ensure the router ID is unique.
- Assign an AS Number between 1 and 4,294,967,295.

Then configure the settings in the General BGP tab:

- Select Reject Default Route to ignore any default routes advertised by BGP peers.
- Select Install Route to update the global routing table with BGP routes.
- Select Aggregate MED to enable route aggregation even when routes have different multiexit discriminator (MED) values.
- Specify a Default Local Preference (used to determine preferences among different paths).
- Select the AS Format that supports interoperability for your deployment.
- Leave the Always Compare MED checkbox cleared.
- Select Deterministic MED comparison. (With this setting enabled, the system compares MED values to choose between routes advertised by iBGP peers.)

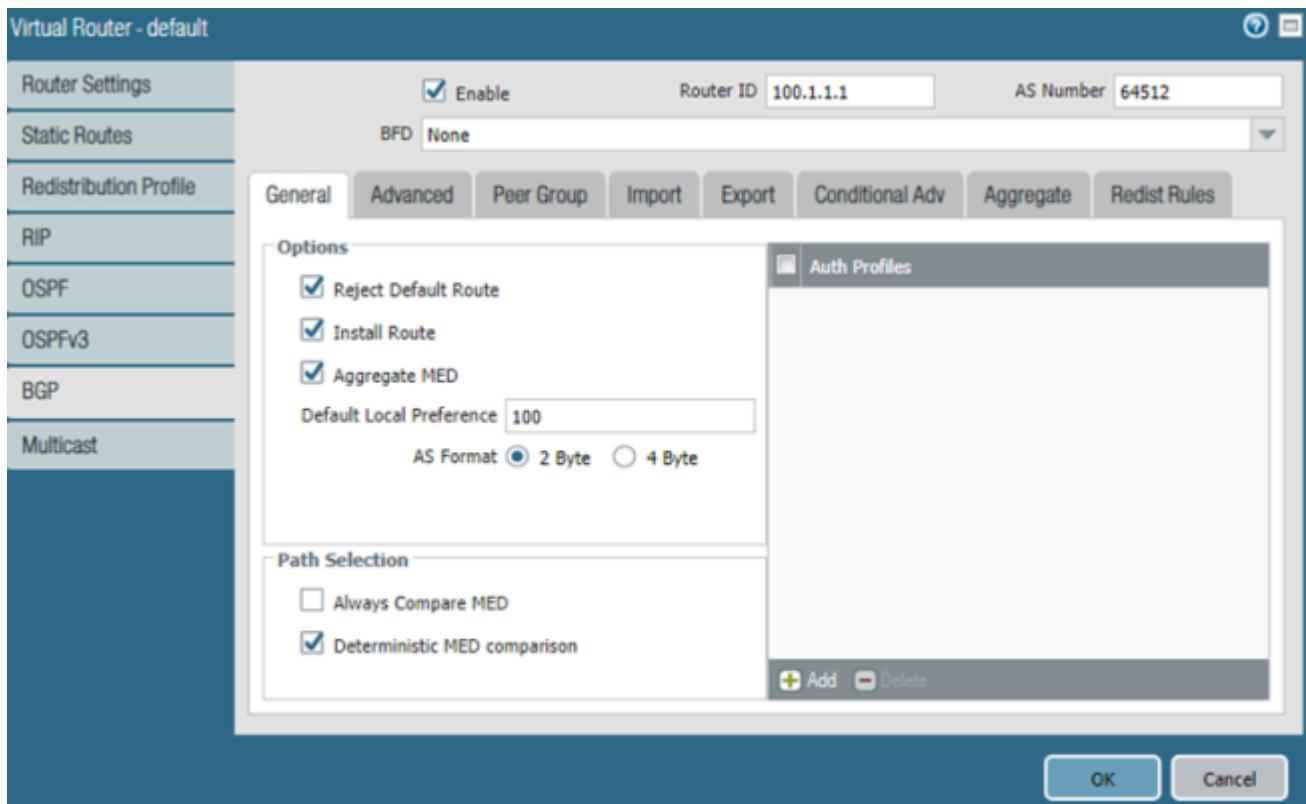


Figure 60: BGP General Settings for On-Prem 1

In the Advanced tab:

- First AS for EBGP is enabled by default; keep this default setting.
- Enable Graceful Restart and enter 120 for Stale Route Time (sec), Local Restart Time (sec), and Max Peer Restart Time (sec).
- Under Dampening Profiles, click the Add button to open the Dampening Profile window and create the profile default as shown in the following image.

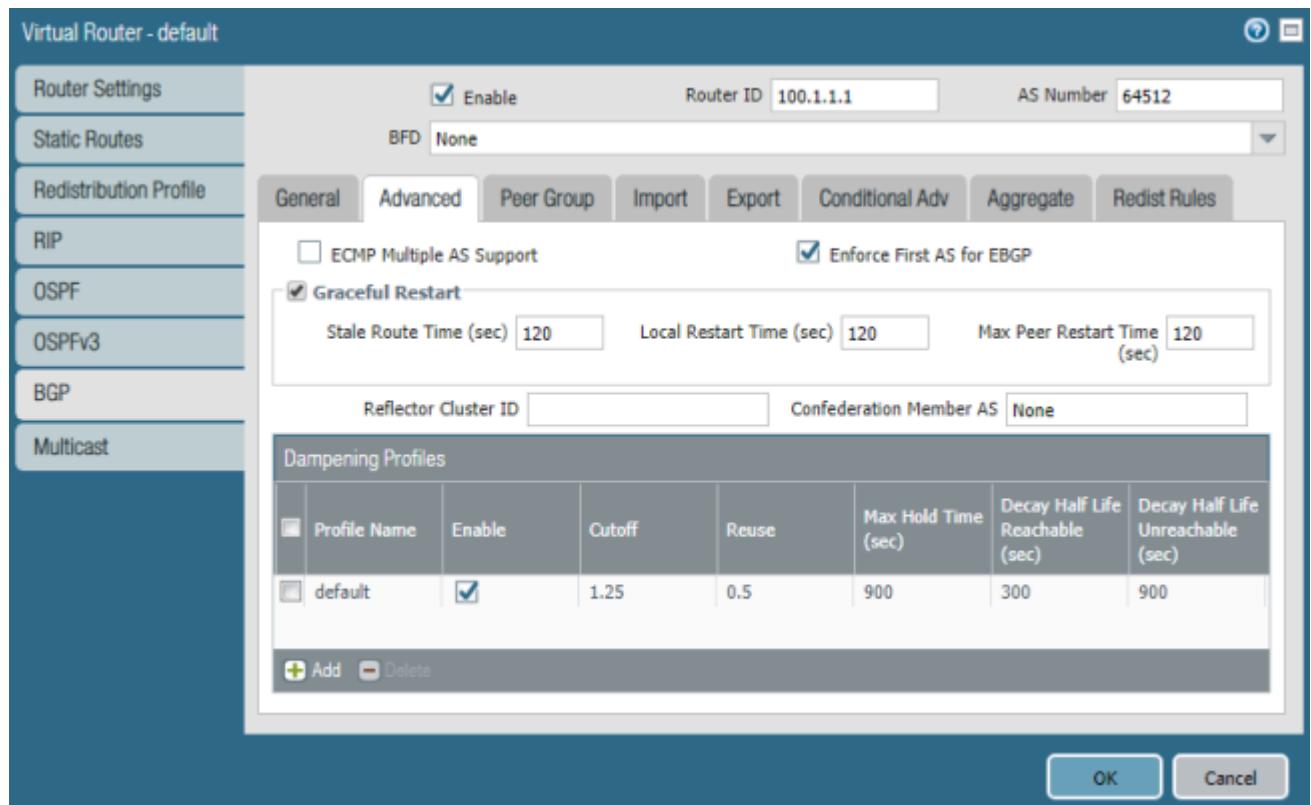


Figure 61: Create Virtual Router default Profile

In the Peer Group tab:

- Click Add and create the following peer group in the Peer Group/Peer window that appears:
  - › Name: peergroup1
  - › Select the Enable checkbox.
  - › Type: EBGP
  - › Select the checkboxes for Aggregated Confed AS Path (default) and Soft Reset With Stored Info.
  - › Select Original for Import Next Hop.
  - › Select Use Self for Export Next Hop.
- Still in the Peer Group/Peer window, click Add and create the following peer:
  - › Name the peer xi\_pa and select the Enable checkbox.
  - › Peer AS: 64513
  - › In the Addressing tab, Address Family Type is IPv4 (default) and Subsequent Address Family is Unicast (default). In the Local Address section, select tunnel.1, which is connected to the peer, as the interface, and select 100.65.1.1/30 as the tunnel.1 IP. In the Peer Address section, enter the IP address of the tunnel interface for Xi (in this case, 100.65.1.2).
  - › In the Connection Options tab, use the default settings for all options.
  - › In the Advanced tab, select Inherit Protocol's Global BFD Profile for BFD and use the default settings for the other options.

**Virtual Router - BGP - Peer Group/Peer**

**Peer Group**

Name	peergroup1	Type	EBGP
<input checked="" type="checkbox"/> Enable		Import Next Hop	<input checked="" type="radio"/> Original <input type="radio"/> Use Peer
<input checked="" type="checkbox"/> Aggregated Confed AS Path		Export Next Hop	<input type="radio"/> Resolve <input checked="" type="radio"/> Use Self
<input type="checkbox"/> Soft Reset With Stored Info		<input type="checkbox"/> Remove Private AS	

Peer	Enable	Peer AS	Local Address	Peer Address	Max Prefixes	BFD
xi_pa	<input checked="" type="checkbox"/>	64513	100.65.1.1/30	100.65.1.2	5000	Inherit-vr-global-setting

Figure 62: peergroup1 with xi\_pa Peer

You have now configured peergroup1 and its peer.

In the Import tab:

- Click Add Import Rule. In the Import Rule window that opens, name the rule import1 and enable it.
- Under Used By, select the checkbox for peergroup1.

**Virtual Router - BGP - Import Rule**

**General** **Match** **Action**

Rules	import1
<input checked="" type="checkbox"/> Enable	

**Used By**

- peergroup1

Figure 63: BGP Import Rule General Settings for On-Prem 1

You've now configured the import rule for BGP.

The screenshot shows a table with the following columns: Name, Enable, Used By, Prefixes, Next Hops, From Peers, and Action. The row for 'import1' has 'Enable' checked, 'Used By' set to 'peergroup1', and 'Action' set to 'allow'.

Match						
Name	Enable	Used By	Prefixes	Next Hops	From Peers	Action
import1	<input checked="" type="checkbox"/>	peergroup1				allow

Figure 64: BGP Import Rule for On-Prem 1

In the Export tab:

- Click Add Export Rule. In the Export Rule window that opens, name the rule export1 and enable it.
- Under Used By, select the checkbox for peergroup1.



Figure 65: BGP Export Rule for On-Prem 1

In the Redist Rules tab:

- Click Add to open the Rule window. Name the rule redis2 and enable it. Leave everything else with the default settings.

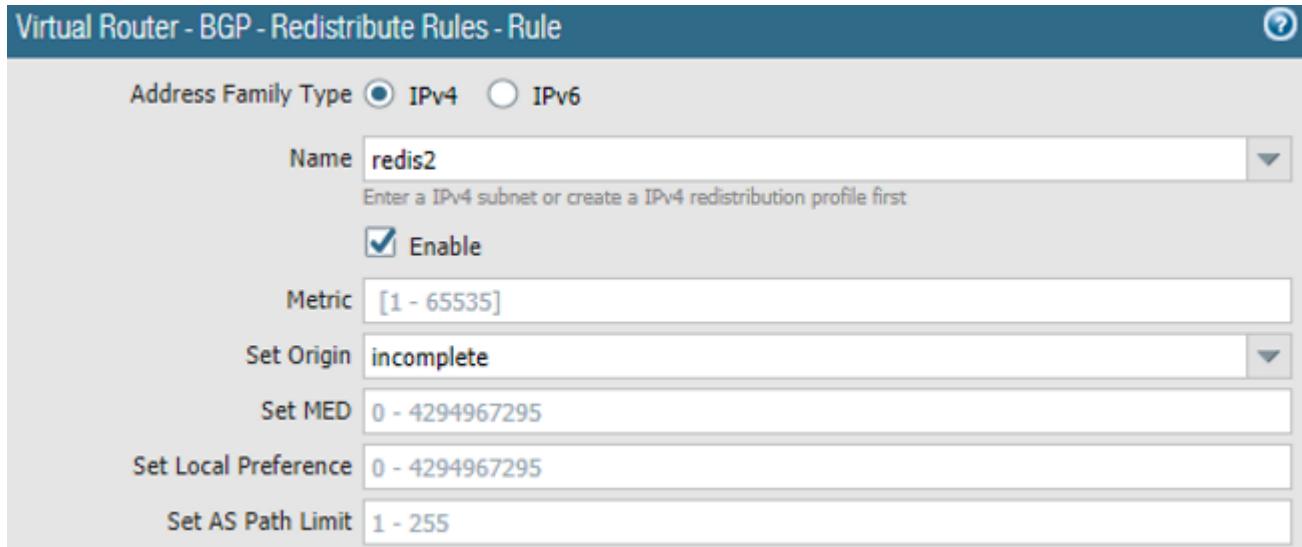


Figure 66: BGP Redistribute Rule redis2 for On-Prem 1

## Use Case 1: Deploy and Configure VM-Series on On-Prem 2

Refer to the section Deploy and Configure VM-Series on On-Prem 1 for instructions on deploying the VM-Series firewall. When you configure the network, use the NR\_PRT\_STATIC virtual network as the data interface.

### Create Interfaces and Zones on On-Prem 2

The following steps outline how to set up a VPN connection that allows you to connect LANs in on-prem 2 to your Nutanix Xi Cloud LAN. This configuration is a route-based VPN tunnel to connect Palo Alto Networks firewalls located at two sites. The firewall makes a routing decision based on the destination IP address.

Before you configure a VPN tunnel, you must configure the Ethernet interface, tunnel interface, zone, and virtual router.

#### Configure Ethernet Interface on On-Prem 2

Before you configure the Ethernet interface, you need to create a management profile that can ping to test connectivity. Open the Palo Alto WebGUI and complete the following steps.

- In the Palo Alto WebGUI, navigate to the Network tab, then click Network Profiles, then Interface Management.
- Click Add to open the Interface Management Profile window, name the profile allow\_mgmt\_ping, and select the checkboxes for HTTPS and Ping.

Now you're ready to create the Ethernet interface.

- In the Palo Alto WebGUI, navigate to Network, then Interfaces, then Ethernet. Click ethernet1/1 to open the Ethernet Interface window.
- Leave ethernet1/1 as the interface name, select Layer3 as the interface type, and use None as the Netflow Profile.
- In the Config tab, use the default virtual router and create the new Security Zone WAN as shown in the following image.

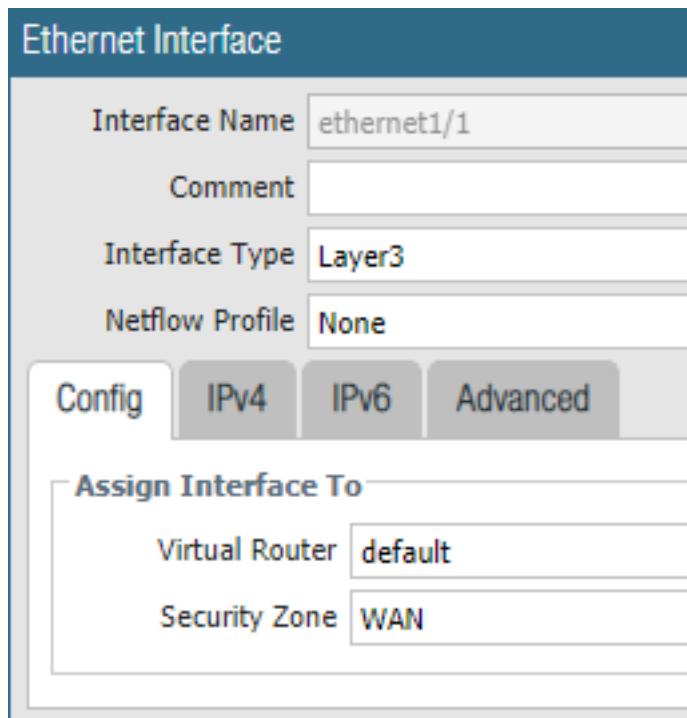


Figure 67: Ethernet Interface Configuration for On-Prem 2

- In the IPv4 tab, assign a static IP address. We used 10.16.80.80/20.

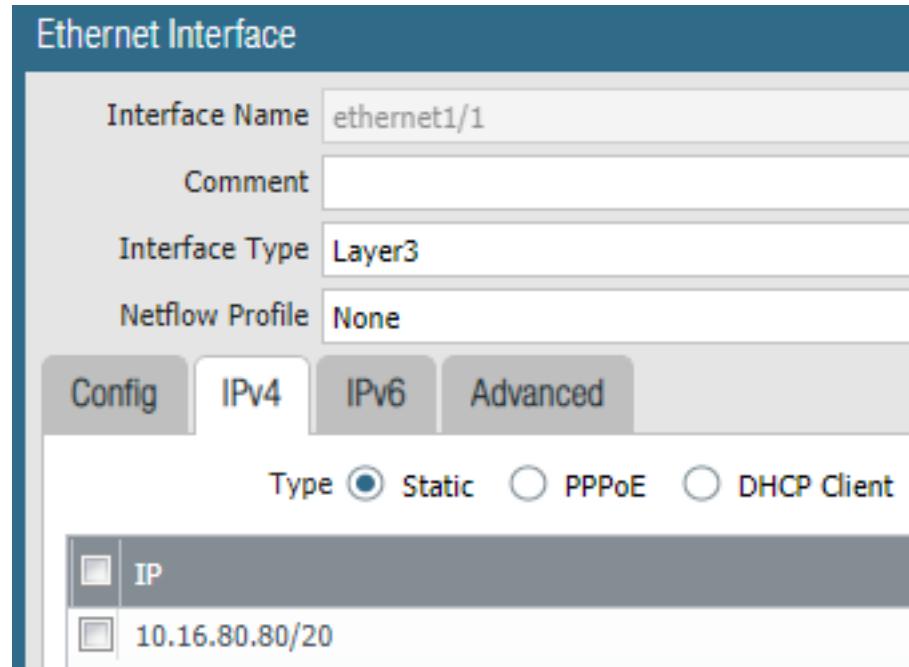


Figure 68: Ethernet Interface IP Configuration for On-Prem 2

- In the Advanced tab, enter allow\_mgmt\_ping for the management profile.

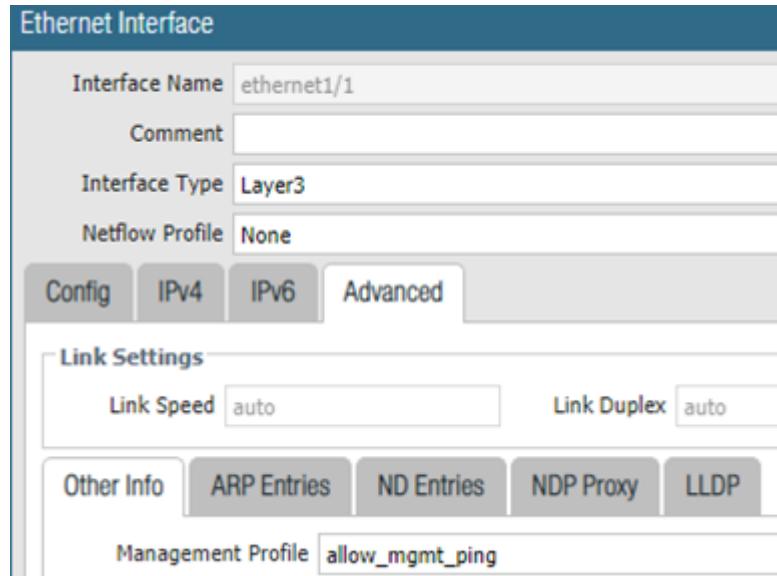


Figure 69: Ethernet Interface Advanced Configuration for On-Prem 2

### Configure Tunnel Interface on On-Prem 2

- In the Palo Alto WebGUI, navigate to Network, then Interfaces, then Tunnel. Click Add.
- Keep tunnel as the Interface Name and leave Netflow Profile set to None.
- Under the Config tab, set the Virtual Router to default and the Security Zone to WAN.

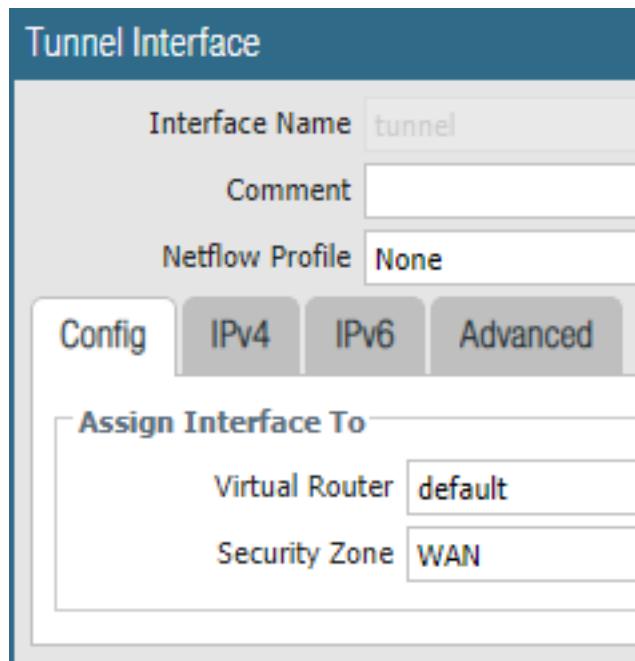


Figure 70: Tunnel Interface Configuration on On-Prem 2

- In the IPv4 tab, click Add and add IP 100.65.1.1/30.

## Configure Zone on On-Prem 2

- In the Palo Alto WebGUI, navigate to Network, then to Zones, then click Add Zone.
  - › Name the zone WAN.
  - › For Log Setting, select None.
  - › For Type, select Layer3.
  - › In the Interfaces section, select the checkboxes for the ethernet1/1 and tunnel.1 interfaces.

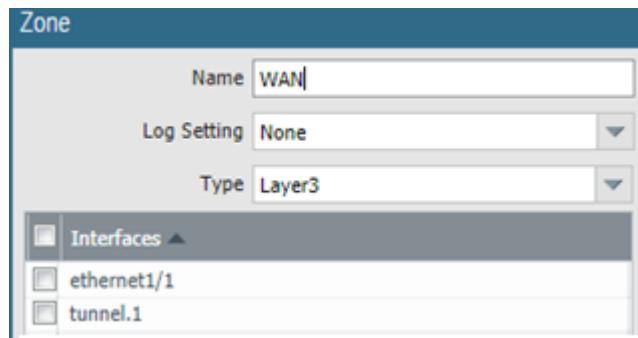


Figure 71: Zone Configuration on On-Prem 2

## Configure Virtual Router on On-Prem 1

In the Palo Alto WebGUI, use the default router (or create a new one) and add the Ethernet and tunnel interfaces to it.

## Configure VPN on On-Prem 2

Refer to [the Palo Alto VPN Deployments document](#) for additional information on how to configure VPNs.

### Create IKE Crypto Profile on On-Prem 1

In the Palo Alto WebGUI, navigate to Network, then Network Profiles, then IKE Crypto. Click Add to open the IKE Crypto Profile window and create a new IKE crypto profile with the following specifications:

- Name: Suite-B-GCM-256
- DH Group: group20

- Encryption: aes-256-cbc
- Authentication: sha384
- Under Timers, select Hours for Key Lifetime and type 8. Type 0 for IKEv2 Authentication Multiple.

### [Create IKE Gateway on On-Prem 2](#)

In the Palo Alto WebGUI, navigate to Network, then Network Profiles, then IKE Gateways. Click Add to open the IKE Gateway window and configure a new IKE gateway.

- In the General tab, enter the following configuration:
  - › Name: xi-OP2-IKE
  - › Version: IKEv2 only mode
  - › Address Type: IPv4
  - › Interface: ethernet1/1
  - › Local IP Address: IP address of ethernet1/1
  - › Peer IP Address Type: IP
  - › Peer Address: public IP of the remote or branch site
  - › Authentication: Pre-Shared Key
  - › Local Identification: Select FQDN (hostname) and onprem2-pa.nutanix.com
  - › Peer Identification: Select FQDN (hostname) and xi-pa.nutanix.com

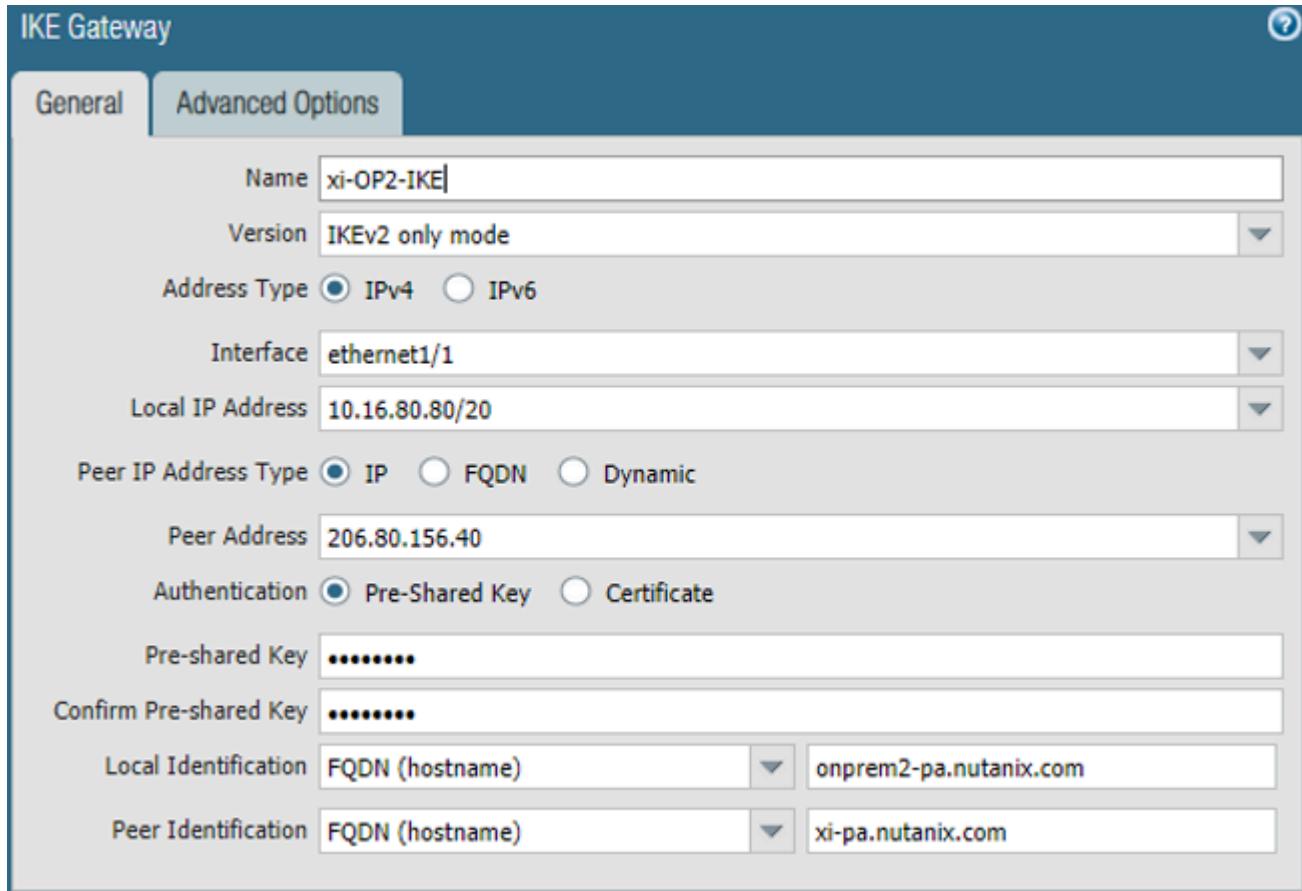


Figure 72: IKE Gateway General Configuration on On-Prem 2

- In the Advanced Options tab, select the checkbox for Enable NAT Traversal. Choose Suite-B-GCM-256 for the IKE crypto profile, select the checkbox for Liveness Check, and type 5 as the Interval (sec).

Repeat this process to create xi-OP2-IKE-2, using the public IP of the remote or branch site as the peer address and xi-pa-2.nutanix.com as the peer ID.

## Configure Routing on On-Prem 2

Refer to the [Palo Alto Border Gateway Protocol \(BGP\) document](#) for more information on configuring BGPs. Follow the steps in the Configure Routing on On-Prem 1 section until you get to the Peer Group tab. In the Peer Group tab:

- Click Add to open the Peer Group/Peer window that appears and create the following peer group:
  - › Name: xi-side
  - › Select the Enable checkbox.
  - › Type: EBGP
  - › Select the checkbox for Aggregated Confed AS Path (default).
  - › Select Original for Import Next Hop.
  - › Select Use Self for Export Next Hop.
- Still in the Peer Group/Peer window, click Add and create the following peer:
  - › Name the peer to-xi and select the Enable checkbox.
  - › Peer AS: 64513
  - › In the Addressing tab, Address Family Type is IPv4 (default) and Subsequent Address Family is Unicast (default). In the Local Address section, select tunnel.1, which is connected to the peer, as the interface, and select 100.66.1.1/30 as the tunnel.1 IP. In the Peer Address section, enter the IP address of the tunnel interface for Xi (in this case, 100.66.1.2).
  - › In the Connection Options tab, use the default settings for all options.
  - › In the Advanced tab, select Inherit Protocol's Global BFD Profile for BFD and use the default settings for the other options.

The screenshot shows the 'Virtual Router - BGP - Peer Group/Peer' configuration page. The 'Peer Group' tab is selected. The 'Name' field is set to 'xi-side'. The 'Type' dropdown is set to 'EBGP'. Under 'Import Next Hop', the 'Original' radio button is selected. Under 'Export Next Hop', the 'Use Self' radio button is selected. There is also a checked checkbox for 'Remove Private AS'. The 'Peer' table lists one peer named 'to-xi' with the following details:

Peer	Enable	Peer AS	Local Address	Peer Address	Max Prefixes	BFD
to-xi	<input checked="" type="checkbox"/>	64513	100.66.1.1/30	100.66.1.2	5000	Inherit-vr-global-setting

Figure 73: Peer Group xi-side with to-xi Peer

You've now configured the peer group xi-side and its peer.

In the Import tab:

- Click Add Import Rule. In the Import Rule window that opens, name the rule 1 and enable it.
- Under Used By, select the checkbox for xi-side.

In the Export tab:

- Click Add Export Rule. In the Export Rule window that appears, name the rule 1 and enable it.
- Under Used By, select the checkbox for xi-side.

In the Redist Rules tab:

- Click Add to open the Rule window. Name the rule redis-static and enable it. Keep the default settings for everything else.

Virtual Router - BGP - Redistribute Rules - Rule

Address Family Type  IPv4  IPv6

Name **redis-static**  
Enter a IPv4 subnet or create a IPv4 redistribution profile first

Enable

Metric **[1 - 65535]**

Set Origin **incomplete**

Set MED **0 - 4294967295**

Set Local Preference **0 - 4294967295**

Set AS Path Limit **1 - 255**

Figure 74: BGP Redistribute Rule redis-static for On-Prem 2

### 3. Use Case 2: Full-Mesh VPN Between Xi and On-Premises Firewall

If you have datacenters in multiple on-premises sites that require multiple connections to the Xi Cloud to ensure link and node redundancy, a full-mesh VPN may be the solution.

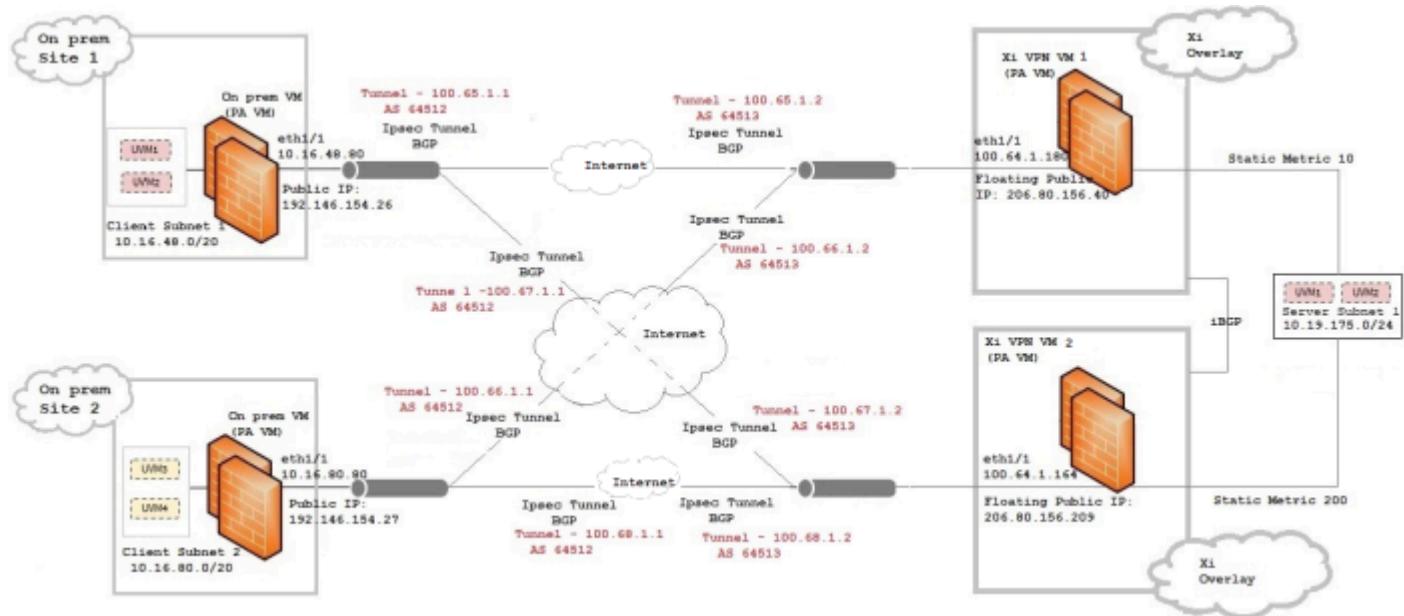


Figure 75: Full-Mesh VPN Between Xi and On-Premises Firewall Deployment

In this use case, a full mesh of eBGP sessions runs over IPSec tunnels, and an iBGP session is established between the two Xi devices. Xi-VPN-VM1 should be the primary gateway for incoming and outgoing traffic. Configure the static route on the Xi devices for the Xi VM network and use Xi-VPN-VM2 as the secondary gateway, as it has a static route with a higher metric to the Xi VM network.

In a steady state, traffic flows in the following order:

1. On-prem VM to On-prem-1 to Xi-VPN-VM1 to Xi VM (forward)

2. Xi VM to Xi-VPN-VM1 to On-prem-1 to On-prem VM (return)

In case of a tunnel failure between on-prem 1 and Xi-VPN-VM1, traffic flows in this order:

1. On-prem uvm to On-prem-1 to Xi-VPN-VM2 to Xi-VPN-VM1 to Xi VM (forward)
2. Xi VM to Xi-VPN-VM1 to Xi-VPN-VM2 to On-prem-1 to On-prem VM (return)

If Xi-VPN-VM1 fails, traffic flows in this order:

1. On-prem VM to On-prem-1 to Xi-VPN-VM2 to Xi VM (forward)
  2. Xi VM to Xi-VPN-VM2 to On-prem-1 to On-prem VM (return)
- 

## Use Case 2: Set Up the Nutanix Xi VPC

Refer to the Use Case 1: Set Up the Nutanix Xi VPC section to upload the VM-Series KVM image and create the same two subnets from that section: Nutanix-vpn-internal (contains all routing devices and NFVMs) and Prod Xi (contains all user VMs).

---

## Use Case 2: Deploy and Configure VM-Series on Xi-VPN-VM1 and VM2

Refer to the Deploy and Configure VM-Series on Xi section and follow the same steps to create two VM-Series VMs. For the floating IP mapping:

- Xi-VPN-VM1: 100.64.1.180 mapped to FIP 206.80.156.40.
- Xi-VPN-VM2: 100.64.1.164 mapped to FIP 206.80.156.209.

## Create Interfaces and Zones on Xi-VPN-VM1 and VM2

### Ethernet Interface Configuration on Xi-VPN-VM1 and VM2

Refer to the Configure Ethernet Interface on Xi section and configure the interfaces for the two Xi VM-Series to create a full-mesh VPN setup. The eth1/1 IP addresses for each VM are as follows:

- VM1: 100.64.1.180
- VM2: 100.64.1.164

## Tunnel Interface Configuration on Xi-VPN-VM1 and VM2

Refer to the Configure Tunnel Interface on Xi section and configure the tunnel interfaces as follows:

- VM1 Tunnel 1: 100.65.1.2 to 100.65.1.1 (on-prem 1 VM).
- VM1 Tunnel 2: 100.66.1.2 to 100.66.1.1 (on-prem 1 VM).
- VM2 Tunnel 1: 100.67.1.2 to 100.67.1.1 (on-prem 1 VM).
- VM2 Tunnel 2: 100.68.1.2 to 100.68.1.1 (on-prem 1 VM).

## Create Zone and Virtual Router on Xi-VPN-VM1 and VM2

Refer to the Create Zone on Xi and Configure Virtual Router on Xi section and create a layer 3 zone (named test, for example). Add ethernet1/1 and the tunnel interfaces you created.

## Configure VPN on Xi-VPN-VM1 and VM2

Refer to the Configure VPN on Xi section to set up the IKE gateway.

- Xi VPN VM 1: local IP address is 100.64.1.180, peer IP address is 192.146.154.26.
- Xi VPN VM 1: local IP address is 100.64.1.180, peer IP address is 192.146.154.27.
- Xi VPN VM 2: local IP address is 100.64.1.164, peer IP address is 192.146.154.26.
- Xi VPN VM 2: local IP address is 100.64.1.164, peer IP address is 192.146.154.27.

## Configure Routing on Xi-VPN-VM1 and VM2

Refer to the Configure Routing on Xi section to enable eBGP between your Xi VM-Series and your on-premises VM Series. Configure the eBGP for Xi-VPN-VM1 as follows:

- Router ID: 100.65.1.2
- AS: 64513
- peergroup1: Peer: onprem-pa; Local IP: 100.65.1.2; Peer IP: 100.65.1.1
- op-peer2: Peer: op2; Local IP: 100.66.1.2; Peer IP: 100.66.1.1

Configure the eBGP for Xi-VPN-VM2 as follows:

- Router ID: 100.64.1.164
- AS: 64513
- op-peer1: Peer: op\_peer\_1; Local IP: 100.67.1.2; Peer IP: 100.67.1.1
- op-peer2: Peer: op\_peer\_2; Local IP: 100.68.1.2; Peer IP: 100.68.1.1

Enable the iBGP between Xi-VPN-VM1 and Xi-VPN-VM2:

- In VM1, create the peer group Xi-Xi-ibgp with the peer xi-peer, interface eth1/1, local IP 100.64.1.180, and peer IP 100.64.1.164.

Peers						
	Name	Enable	Type	Name	Peer Address	Local Address
<input type="checkbox"/>	peergroup1	<input checked="" type="checkbox"/>	ebgp	onprem-pa	100.65.1.1	100.65.1.2/30
<input type="checkbox"/>	op-peer2	<input checked="" type="checkbox"/>	ebgp	op2	100.66.1.1	100.66.1.2/30
<input type="checkbox"/>	Xi-Xi-ibgp	<input checked="" type="checkbox"/>	ibgp	xi-peer	100.64.1.164	100.64.1.180/24

Figure 76: iBGP Peer Group in Xi-VPN-VM1

- In VM2, create the peer group Xi-ibgp with the peer xi-peer, interface eth1/1, local IP 100.64.1.164, and peer IP 100.64.1.180.

Peers						
	Name	Enable	Type	Name	Peer Address	Local Address
<input type="checkbox"/>	Xi-ibgp	<input checked="" type="checkbox"/>	ibgp	xi-peer	100.64.1.180	100.64.1.164/24
<input type="checkbox"/>	op-peer1	<input checked="" type="checkbox"/>	ebgp	op_peer_1	100.67.1.1	100.67.1.2/30
<input type="checkbox"/>	op-peer2	<input checked="" type="checkbox"/>	ebgp	op_peer_2	100.68.1.1	100.68.1.2/30

Figure 77: iBGP Peer Group in Xi-VPN-VM2

Add static routes in VM1 and VM2 as shown in the following figures, so that traffic to 10.19.175.0/24 uses VM1, which has the lowest metric (10).

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
default	0.0.0.0/0	ethernet1/1	ip-address	100.64.1.1	default	10	None	unicast
xi kvm	10.19.175.0/24	ethernet1/1	ip-address	100.64.1.1	default	10	None	unicast

Figure 78: Xi-VPN-VM1 Static Route

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
default	0.0.0.0/0	ethernet1/1	ip-address	100.64.1.1	default	10	None	unicast
xi kvm	10.19.175.0/24	ethernet1/1	ip-address	100.64.1.1	default	200	None	unicast

Figure 79: Xi-VPN-VM2 Static Route

For the BGP Import, Export, and Redis rules, refer to the Configure Routing on Xi section and add the peer groups you created to the Import and Export rules.

## Create VPC Policy on Xi-VPN-VM1 and VM2

Refer to the Create VPC Policy to Reroute Traffic Through Xi section and create policies with priority to reroute traffic. The priority of the access control list (ACL) determines which ACL is picked first. Create the two priorities listed in the earlier section (299 and 300), then create two more:

1. One with a priority of 291 that reroutes traffic going from 10.19.175.0/24 to 10.16.48.0/20 to go to 100.64.1.164 instead.
2. One with a priority of 311 that reroutes traffic going from 10.19.175.0/24 to 192.168.0.0/16 to go to 100.64.1.164 instead.

299	10.19.175.0/24	1116R	100.64.1.180	on R	10.16.80.0/24	Any	<a href="#">Clear counters</a> · <a href="#">Edit</a> · <a href="#">Delete</a>
300	10.19.175.0/24	206.4.9.1CR	100.64.1.180	on on R	10.16.48.0/24	Any	<a href="#">Clear counters</a> · <a href="#">Edit</a> · <a href="#">Delete</a>
311	10.19.175.0/24	on R	100.64.1.164	on R	192.168.0.0/16	Any	<a href="#">Clear counters</a> · <a href="#">Edit</a> · <a href="#">Delete</a>
291	10.19.175.0/24	on R	100.64.1.164	on R	10.16.48.0/24	Any	<a href="#">Clear counters</a> · <a href="#">Edit</a> · <a href="#">Delete</a>

Figure 80: VPC Policies on Xi-VPN-VM1 and VM2

## Use Case 2: Deploy and Configure VM-Series on On-Prem 1

This VM-Series configuration is almost the same as the one described in the section Use Case 1: Deploy and Configure VM-Series on On-Prem 1. You need to configure an additional tunnel interface to connect to Xi-VPN-VM2. The configuration of the tunnel interface, virtual router, and zones should look like the following image.

Ethernet	VLAN	Loopback	Tunnel				
Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment	
tunnel		none	none	none			
tunnel.1	allow_all	100.65.1.1/30	default	untrust			
tunnel.2	allow_all	100.67.1.1/30	default	untrust			

Figure 81: Use Case 2 On-Premises 1 Tunnel Interfaces

Refer to the Configure VPN on Xi section to set up two IKE gateways with the following IP addresses:

1. Local IP address: 10.16.48.80; peer IP address: 206.80.156.80
2. Local IP address: 10.16.48.80; peer IP address: 206.80.156.209

Refer to the Configure Routing on On-Prem 1 section to configure routing here. Add another peer group (named peergroup2) to establish the eBGP connection with Xi-VPN-VM2:

- Peer: xi\_peer\_2
- Peer Address: 100.67.1.2
- Local Address: 100.67.1.1/30

Peers					
Name	Enable	Type	Name	Peer Address	Local Address
peergroup1	<input checked="" type="checkbox"/>	ebgp	xi_pa	100.65.1.2	100.65.1.1/30
peergroup2	<input checked="" type="checkbox"/>	ebgp	xi_peer_2	100.67.1.2	100.67.1.1/30

Figure 82: Use Case 2 On-Prem 1 Peer Group Configuration

For the BGP Import, Export, and Redis rules, refer to the Configure Routing on Xi section and add the two peers you created to the Import and Export rules.

## Use Case 2: Deploy and Configure VM-Series on On-Prem 2

This VM-Series configuration is almost the same as the one described in the section Use Case 1: Deploy and Configure VM-Series on On-Prem 2. You need to configure an additional tunnel interface to connect to Xi-VPN-VM2. The configuration of the tunnel interfaces, virtual routers, and zones should look like the following image.

Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel		none	none	none		
tunnel.1	allow_mgmt_ping	100.66.1.1/30	default	WAN		
tunnel.2	allow_mgmt_ping	100.68.1.1/30	default	WAN		

Figure 83: Use Case 2 On-Prem 2 Tunnel Configuration

Refer to the Configure VPN on On-Prem 2 section to set up two IKE gateways with the following IP addresses:

- Local IP address: 10.16.80.80; peer IP address: 206.80.156.80
- Local IP address: 10.16.80.80; peer IP address: 206.80.156.209

Refer to the Configure Routing on On-Prem 1 section to configure routing here. Add another peer group (named xi-peer-2) to establish the eBGP connection with Xi-VPN-VM2:

- Peer: xi\_peer\_2
- Peer Address: 100.68.1.2
- Local Address: 100.68.1.1/30

Peers						
	Name	Enable	Type	Name	Peer Address	Local Address
<input type="checkbox"/>	xi-side	<input checked="" type="checkbox"/>	ebgp	to-xi	100.66.1.2	100.68.1.1/30
<input type="checkbox"/>	xi-peer-2	<input checked="" type="checkbox"/>	ebgp	xi_peer_2	100.68.1.2	100.68.1.1/30

Figure 84: Use Case 2 On-Prem 2 Peer Group Configuration

Add the peers you just created to the Import and Export rules.

## About Nutanix

Nutanix is a global leader in cloud software and a pioneer in hyperconverged infrastructure solutions, making clouds invisible and freeing customers to focus on their business outcomes. Organizations around the world use Nutanix software to leverage a single platform to manage any app at any location for their hybrid multicloud environments. Learn more at [www.nutanix.com](http://www.nutanix.com) or follow us on Twitter [@nutanix](https://twitter.com/nutanix).

## List of Figures

Figure 1: VPN Between Xi and On-Premises Firewall Deployment.....	5
Figure 2: Xi Dashboard Images Pane.....	6
Figure 3: Xi Dashboard Add Images Pane.....	6
Figure 4: Use the Search Bar to Find Specific Images.....	7
Figure 5: Xi Dashboard Virtual Private Clouds.....	7
Figure 6: Create Nutanix-vpn-internal Subnet.....	9
Figure 7: Available Production VPC Subnets.....	10
Figure 8: VMs Pane in Xi Dashboard.....	11
Figure 9: Create VM Pane in Xi Dashboard.....	11
Figure 10: General Settings for VM-Series VM.....	13
Figure 11: Set MTU to 1,310.....	14
Figure 12: Disable DPDK on VM-Series with Version Earlier Than 9.1.....	14
Figure 13: Add Interface Management Profile.....	16
Figure 14: Internet ethernet1/1 Configuration.....	17
Figure 15: Ethernet Interface IPv4 Settings.....	18
Figure 16: Ethernet Interface Advanced Settings.....	19
Figure 17: Tunnel Interface Configuration.....	20
Figure 18: Tunnel Interface IPv4 Settings.....	20
Figure 19: Zone Configuration.....	22
Figure 20: Virtual Router General Settings.....	23
Figure 21: IKE Crypto Profile Configuration.....	24
Figure 22: IKE Gateway General Configuration.....	26
Figure 23: IKE Gateway Advanced Options.....	27

Figure 24: IPSec Crypto Profile Configuration.....	28
Figure 25: IPSec Tunnel on-prem-ipsec.....	29
Figure 26: IPSec Tunnel on-prem2-ipsec.....	29
Figure 27: BGP General Settings.....	31
Figure 28: BGP Advanced Settings.....	32
Figure 29: BGP Peer Group Settings.....	33
Figure 30: Peer Addressing Options.....	34
Figure 31: Peer Connection Options.....	35
Figure 32: Peer Advanced Options.....	36
Figure 33: peergroup1 with onprem-pa Peer.....	37
Figure 34: BGP Peer Groups.....	38
Figure 35: BGP Import Rule General Settings.....	39
Figure 36: BGP Import Rule Action Settings.....	40
Figure 37: BGP Import Rules.....	40
Figure 38: BGP Export Rule General Settings.....	41
Figure 39: BGP Export Rule Match Settings.....	41
Figure 40: BGP Export Rule.....	42
Figure 41: BGP Redist Rules Allow Redistribute Default Route.....	42
Figure 42: BGP Redistribute Rule redis3.....	43
Figure 43: BGP Redistribute Rule.....	43
Figure 44: Production VPC Priority Policy.....	44
Figure 45: Two Required VPC Policies.....	45
Figure 46: Create Image on On-Prem 1.....	46
Figure 47: Create Additional Virtual Network.....	47
Figure 48: Example Network Configurations.....	48
Figure 49: Create New Network Interface Connection (NIC).....	49

Figure 50: Zone Configuration on On-Prem 1.....	51
Figure 51: allow_all Interface Management Profile for On-Prem 1 VM.....	52
Figure 52: Ethernet Interface Configuration for On-Prem 1 VM.....	53
Figure 53: Ethernet Interface IP Configuration for On-Prem 1 VM.....	54
Figure 54: Ethernet Interface Advanced Configuration for On-Prem 1 VM.....	55
Figure 55: Tunnel Interface Configuration on On-Prem 1.....	56
Figure 56: Tunnel Interface IPv4 Settings on On-Prem 1.....	57
Figure 57: Virtual Router General Settings on On-Prem 1.....	58
Figure 58: IKE Gateway General Configuration on On-Prem 1.....	60
Figure 59: IKE Gateway Advanced Options on On-Prem 1.....	61
Figure 60: BGP General Settings for On-Prem 1.....	62
Figure 61: Create Virtual Router default Profile.....	63
Figure 62: peergroup1 with xi_pa Peer.....	65
Figure 63: BGP Import Rule General Settings for On-Prem 1.....	65
Figure 64: BGP Import Rule for On-Prem 1.....	66
Figure 65: BGP Export Rule for On-Prem 1.....	66
Figure 66: BGP Redistribute Rule redis2 for On-Prem 1.....	67
Figure 67: Ethernet Interface Configuration for On-Prem 2.....	68
Figure 68: Ethernet Interface IP Configuration for On-Prem 2.....	69
Figure 69: Ethernet Interface Advanced Configuration for On-Prem 2.....	69
Figure 70: Tunnel Interface Configuration on On-Prem 2.....	70
Figure 71: Zone Configuration on On-Prem 2.....	71
Figure 72: IKE Gateway General Configuration on On-Prem 2.....	73
Figure 73: Peer Group xi-side with to-xi Peer.....	75
Figure 74: BGP Redistribute Rule redis-static for On-Prem 2.....	76
Figure 75: Full-Mesh VPN Between Xi and On-Premises Firewall Deployment.....	77

Figure 76: iBGP Peer Group in Xi-VPN-VM1.....	80
Figure 77: iBGP Peer Group in Xi-VPN-VM2.....	80
Figure 78: Xi-VPN-VM1 Static Route.....	81
Figure 79: Xi-VPN-VM2 Static Route.....	81
Figure 80: VPC Policies on Xi-VPN-VM1 and VM2.....	82
Figure 81: Use Case 2 On-Premises 1 Tunnel Interfaces.....	82
Figure 82: Use Case 2 On-Prem 1 Peer Group Configuration.....	83
Figure 83: Use Case 2 On-Prem 2 Tunnel Configuration.....	83
Figure 84: Use Case 2 On-Prem 2 Peer Group Configuration.....	84