v1.3 | October 2022 | TN-2128

TECH NOTE

Palo Alto VM: GlobalProtect Gateway on Nutanix Cloud

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Contents

1. Executive Summary

Nutanix Cloud Services offers a native extension to Nutanix, delivering an integrated public cloud environment that customers can instantly provision and automatically configure. The first service available in Nutanix Cloud Services, Nutanix DRaaS, provides disaster recovery as a service. Nutanix DRaaS rapidly and intelligently protects the applications and data in your Nutanix environment without requiring you to purchase and maintain a separate infrastructure stack.

Palo Alto Networks GlobalProtect is a virtual private network (VPN) server that uses its advanced firewall to bring greater security, consistency, and visibility to remote-access users.

In this document, we demonstrate how to enable GlobalProtect in the Nutanix Cloud Palo Alto firewall so that remote users can connect to their Nutanix Cloud.

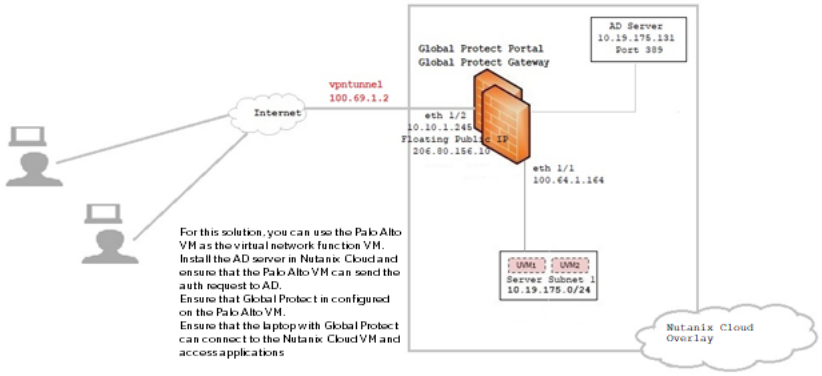

Figure 1: Diagram of Remote Access to Nutanix Cloud

Document Version History

Version Number	Published	Notes
1.0	October 2019	Original publication.
1.1	January 2021	Updated Nutanix overview.

Version Number	Published	Notes
1.2	January 2022	Refreshed content.
1.3	October 2022	Updated product names.

2. Set Up the Nutanix Cloud Virtual Private Cloud (VPC)

Sign in to the Nutanix Cloud portal and upload the VM-Series kernel-based virtual machine (KVM) image:

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

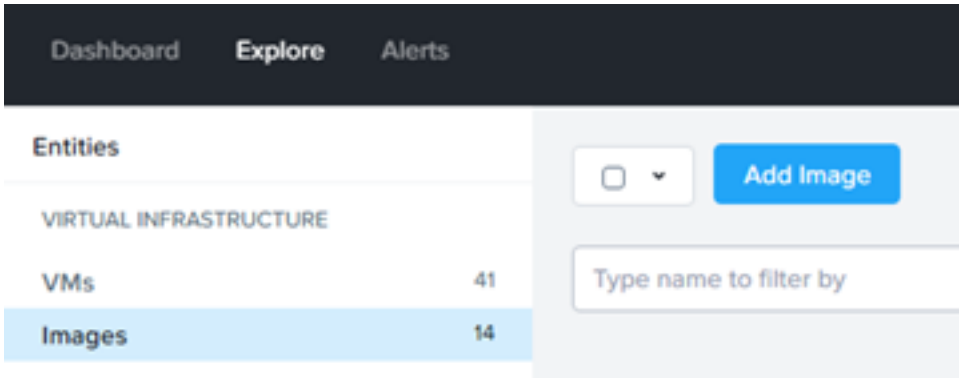

Figure 2: Nutanix Cloud Dashboard Images Pane

- 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.

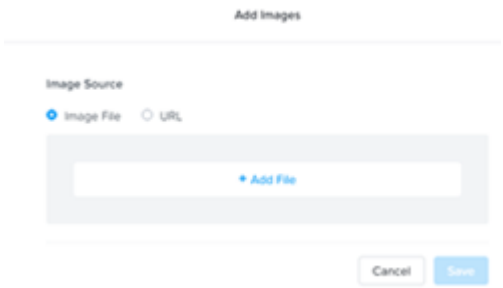

Figure 3: Nutanix Cloud Dashboard Add Images Pane

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

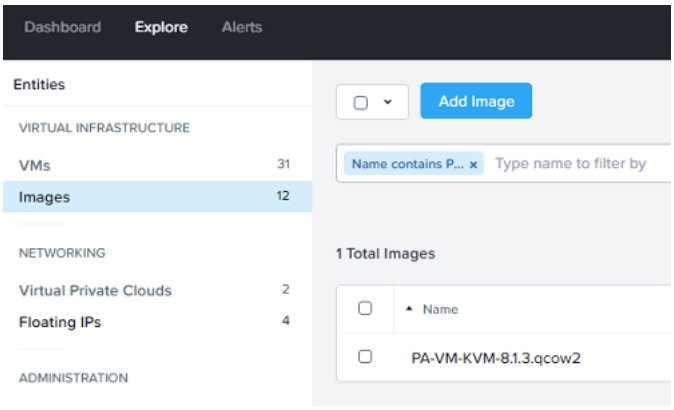

Figure 4: Use the Search Bar to Find Specific Images

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

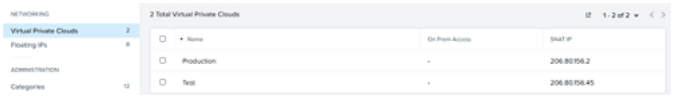

Figure 5: Nutanix Cloud Dashboard Virtual Private Clouds

Create three subnets in the Production VPC: Nutanix-vpn-internal, Prod Nutanix Cloud, and merger. Use the Nutanix-vpn-internal subnet for all routing devices, network function VMs, and data interface on the VM-Series, which is associated with a floating IP address and used as a management interface. Use Prod Nutanix Cloud for user VMs running on Nutanix Cloud and use merger (also associated with a floating IP address) to connect to the GlobalProtect portal and gateway.

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

Navigate to the Explore tab in your Nutanix Cloud 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, but you should fill in the information for your subnets as appropriate for your environment.

Figure 6: Create Nutanix-vpn-internal Subnet

Repeat this process to create the Prod Nutanix Cloud and merger subnets.

In the Production VPC, you should see three available subnets.

Note: You can access floating IP addresses from the internet and 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 IP addresses based on your needs.

3. Deploy and Configure VM-Series on Nutanix Cloud

Sign in to the Nutanix Cloud management portal and create a VM-Series VM with three networks. Use the three subnets you created in the Production VPC to create these VM networks. Assign Prod Nutanix Cloud as the VM's management interface. Assign Nutanix-vpn-internal to the VM's ethernet1/1 interface (associated with a floating IP address) to externally manage the Nutanix Cloud VM-Series and handle data traffic. Assign merger to the VM's ethernet1/2 interface (associated with a floating IP address) to connect to the GlobalProtect portal and gateway.

- To create a VM, click VMs in the Explore tab in the Nutanix Cloud dashboard.

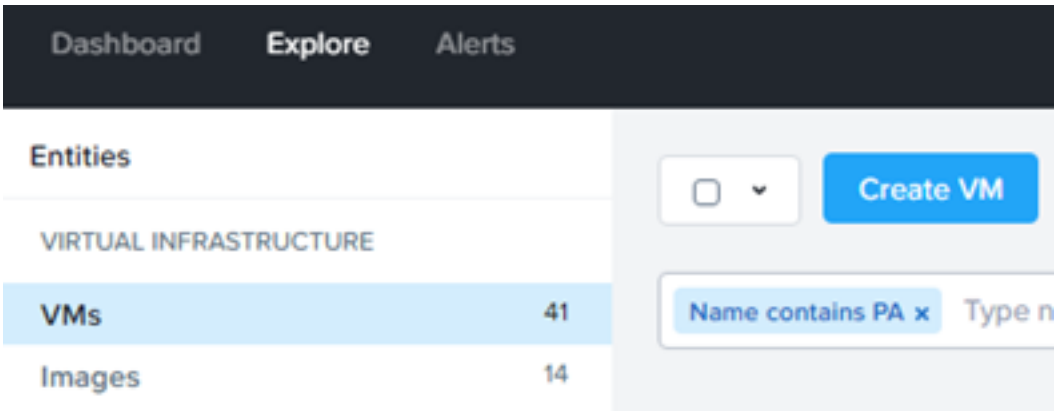

Figure 7: VMs Pane in Nutanix Cloud Dashboard

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

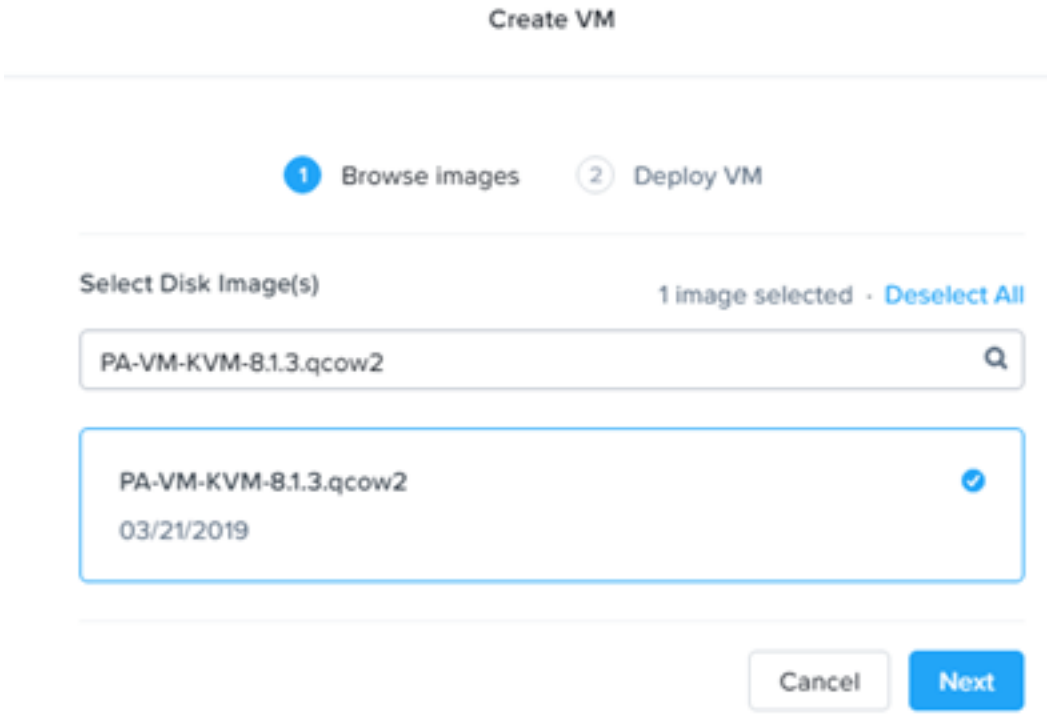

Figure 8: Create VM Pane in Nutanix Cloud Dashboard

- In the General Settings pane, enter the specifications for your environment.
  - Name: NutanixCloudPA4
  - Time zone: Select the correct time zone.
  - Disks: Ensure there is a disk called scsi.0 with the type DISK and 60 GB.
  - Network: Select Production, then Nutanix-vpn-internal, then Associate Floating IP and choose the floating IP address from the dropdown menu. Select the Prod Nutanix Cloud option. Select merger, then Associate Floating IP and choose the floating IP address from the dropdown menu.
  - Configuration: Under CPU, type 2 (VCPU). Under Memory, type 8 (GB).

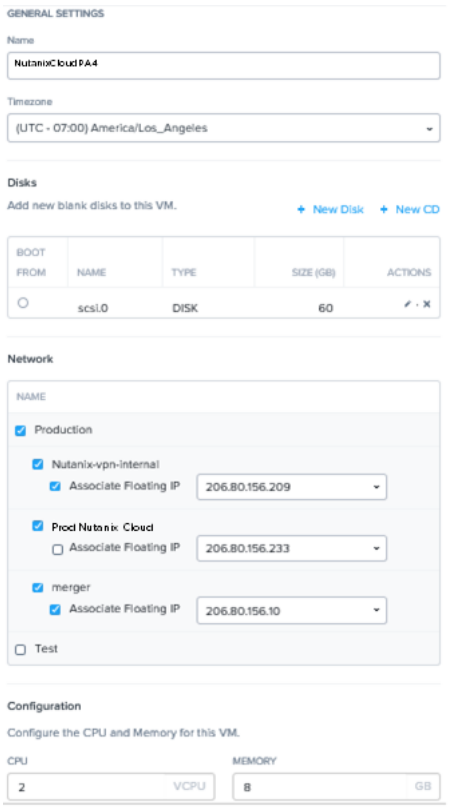

Figure 9: General Settings for VM-Series VM

You can also associate a floating IP address with Prod Nutanix Cloud and assign it to the management vNIC, then use the management vNIC to manage the Nutanix Cloud VM-Series.

> Note: The floating IP address is a public IP address, so you must change the default admin credentials on the VM-Series firewall after the configuration.

Start the VM-Series firewall and make the following configurations on ethernet1/1:

- Make sure the ethernet1/1 vNIC has a maximum transmission unit (MTU) set to less than 1,500.
- Use Secure Shell (SSH) to connect to the public IP address (associated floating IP address) with the admin 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
```

- Run the following command from the Palo Alto Networks command-line interface (CLI) to disable the Data Plane Development Kit (DPDK) on the VM:

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

Figure 10: Disable DPDK on the VM-Series

- Commit to save the changes.

With this configuration, you should be able to access the Nutanix Cloud web portal firewall using the floating IP address, which means you can start to configure the VM-Series.

4. Create Interfaces and Zones for GlobalProtect

Refer to Palo Alto Networks Configure Interfaces guide for more information.

> Note: Palo Alto Networks VM-Series refers to vNICs as "interfaces."

We provide the steps to set up a VPN connection that allows you to connect two Local Area Networks (LANs), one in the Nutanix 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 destination IP address.

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

Configure Ethernet Interface

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 Networks VM WebGUI and complete the following steps.

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

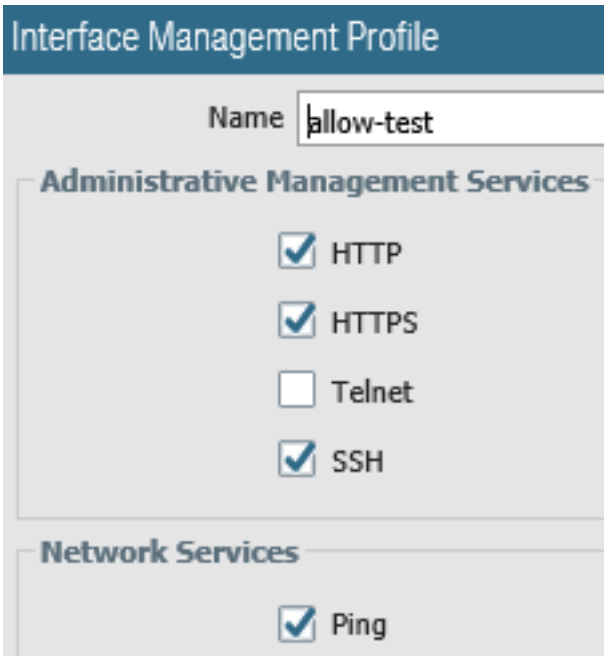

Figure 11: Add Interface Management Profile

Now you're ready to configure the ethernet interface:

- In the Palo Alto Networks VM WebGUI, navigate to the Network tab, then to Interfaces, then to Ethernet. Click ethernet1/1 to open the Ethernet Interface window.
- Leave the interface name as ethernet1/1, select Layer3 as the interface type, and use None as the netflow profile.
- In the Config tab, set Virtual Router to default and Security Zone to test.

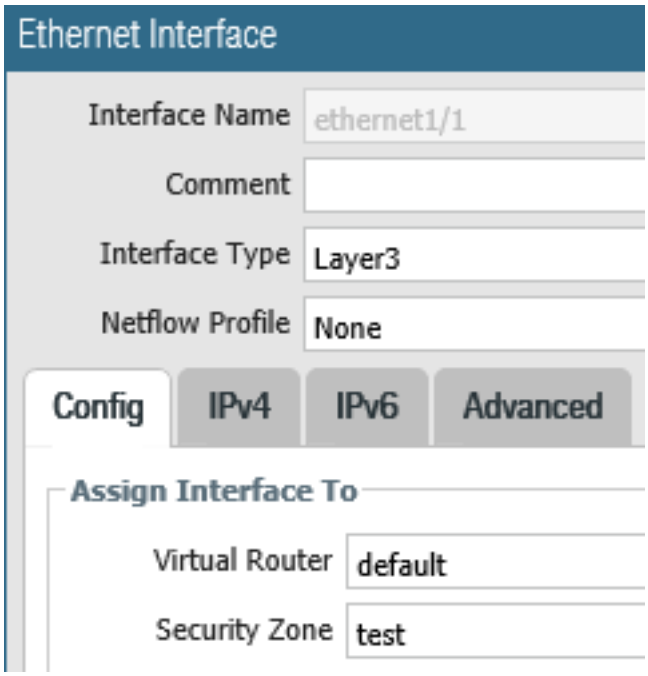

Figure 12: Ethernet Interface Configuration

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

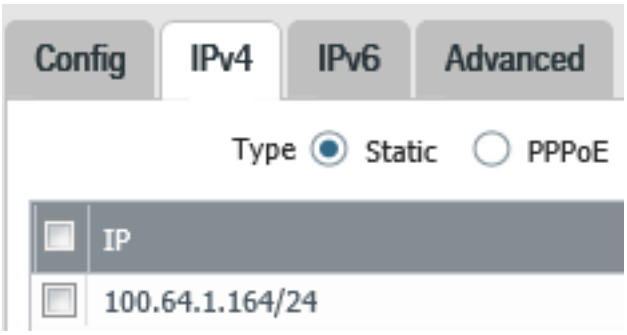

Figure 13: Ethernet Interface IPv4 Settings

- In the Advanced settings tab, leave the Link Speed set to auto and type allow-test in the Management Profile box.

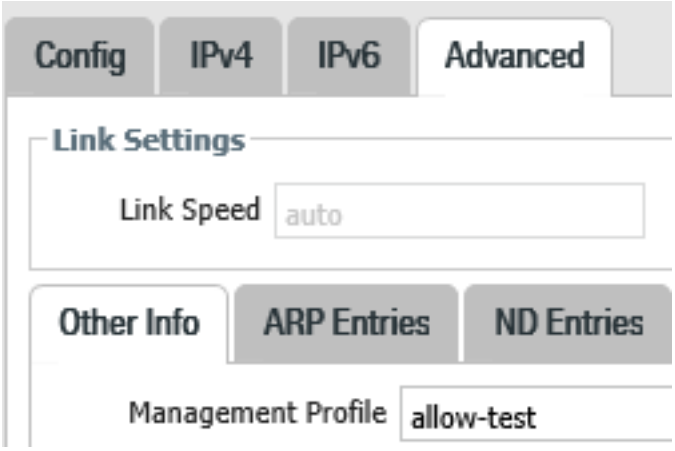

Figure 14: Ethernet Interface Advanced Settings

- Repeat these steps to configure ethernet1/2 but choose a different IP address.

In the Ethernet tab, you should see the two ethernet interfaces you just configured.

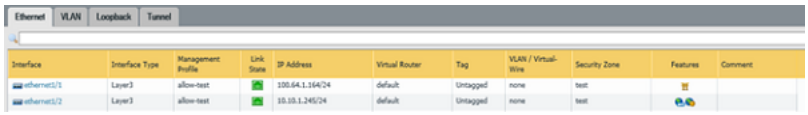

Figure 15: Ethernet Interface List

Add the interfaces ethernet1/1 and ethernet1/2 to the security zone and the virtual router:

- In the Virtual Router tab, click default to open the Virtual Router default pane. Navigate to the Static Route tab and click Add to add a static route using 100.64.1.1 to reach the user VMs at 10.19.175.0/24. The static route you added should look like the following image.

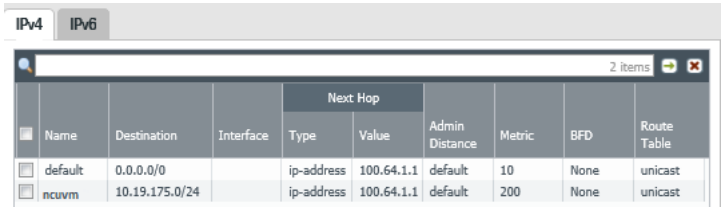

Figure 16: Add the Interfaces to the Virtual Router

Create Tunnel Interface

Before you create the tunnel interface, you need to create an IP address named vpntunnel:

- In the Palo Alto Networks VM WebGUI, navigate to Objects, then to Addresses, and click Add.
- In the Address window that appears, configure vpntunnel as shown in the following image and click OK.

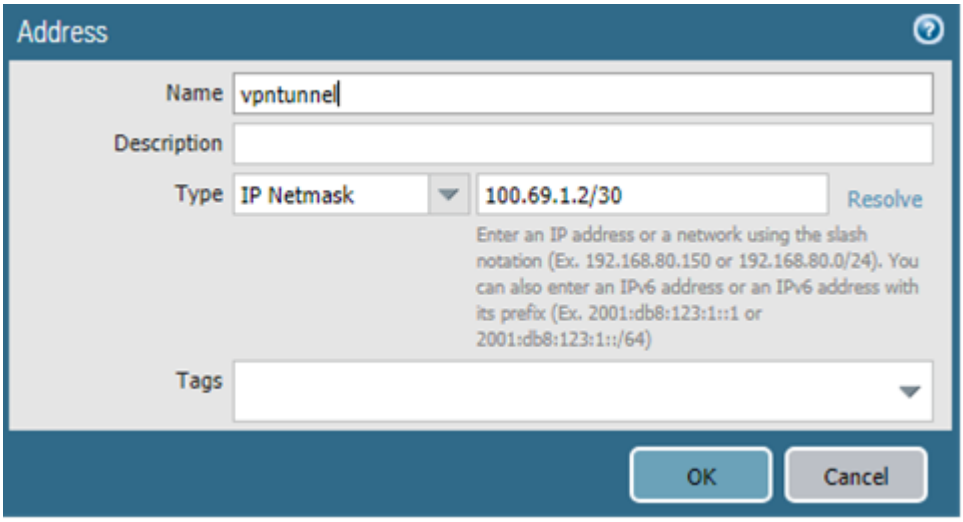

Figure 17: Create vpntunnel IP Address

- You should see the vpntunnel IP address in the list under Addresses.

Now you're ready to create the tunnel interface:

- In the Palo Alto Networks VM WebGUI, navigate to the Network tab, then click Interfaces, then Tunnel and click Add.
- Leave Interface Name as tunnel.3 and leave Netflow Profile as None.
- Under the Config tab, set Virtual Router to default and Security Zone to test.

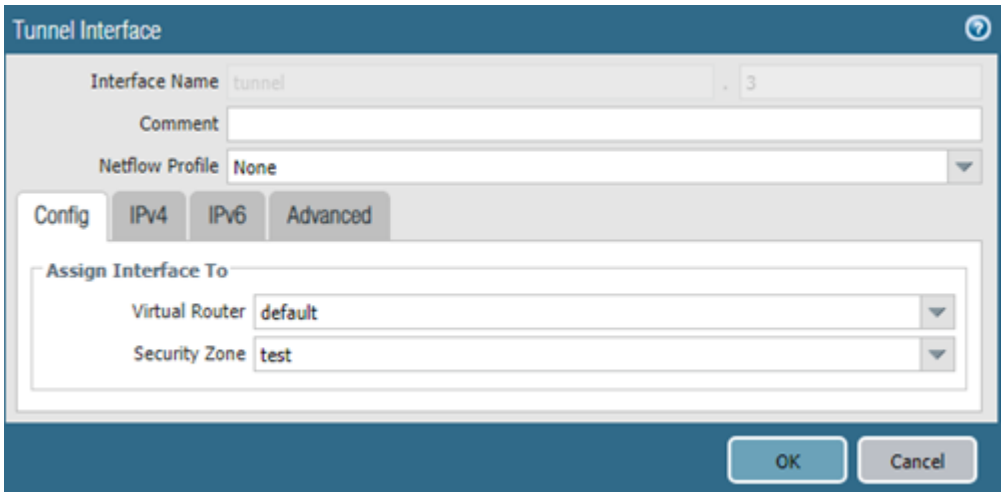

Figure 18: Tunnel Interface Configuration

- In the IPv4 tab, select vpntunnel.

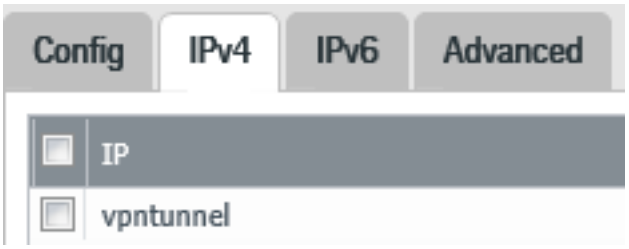

Figure 19: Tunnel Interface IPv4 Settings

Create Zone

- In the Palo Alto Networks VM 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, select all three interfaces you created (ethernet1/1, ethernet1/2, and tunnel.3).
  - In the User Identification ACL section, select Enable User Identification.

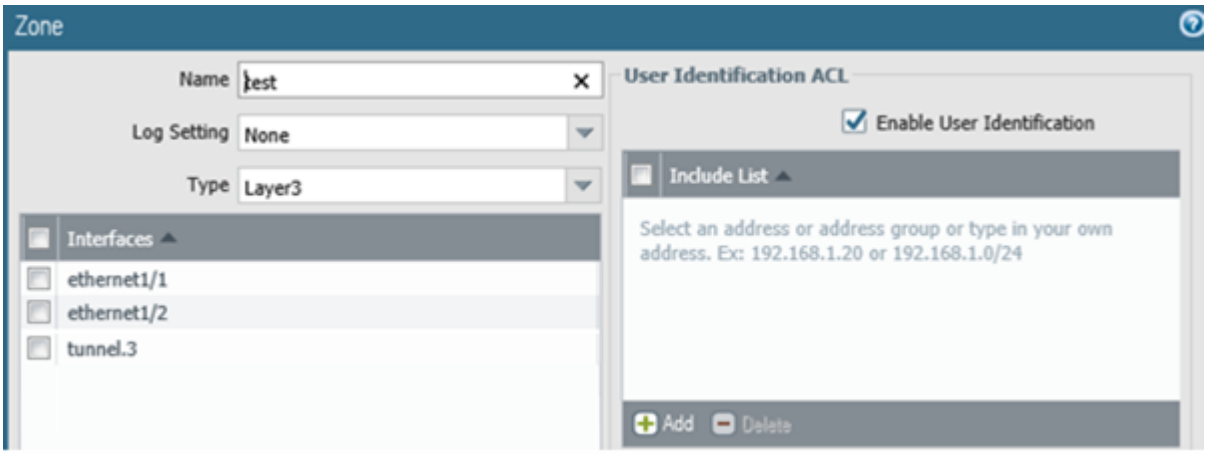

Figure 20: Zone Configuration

- The final list should look like the following image.

Figure 21: Test Zone

Configure Virtual Router

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

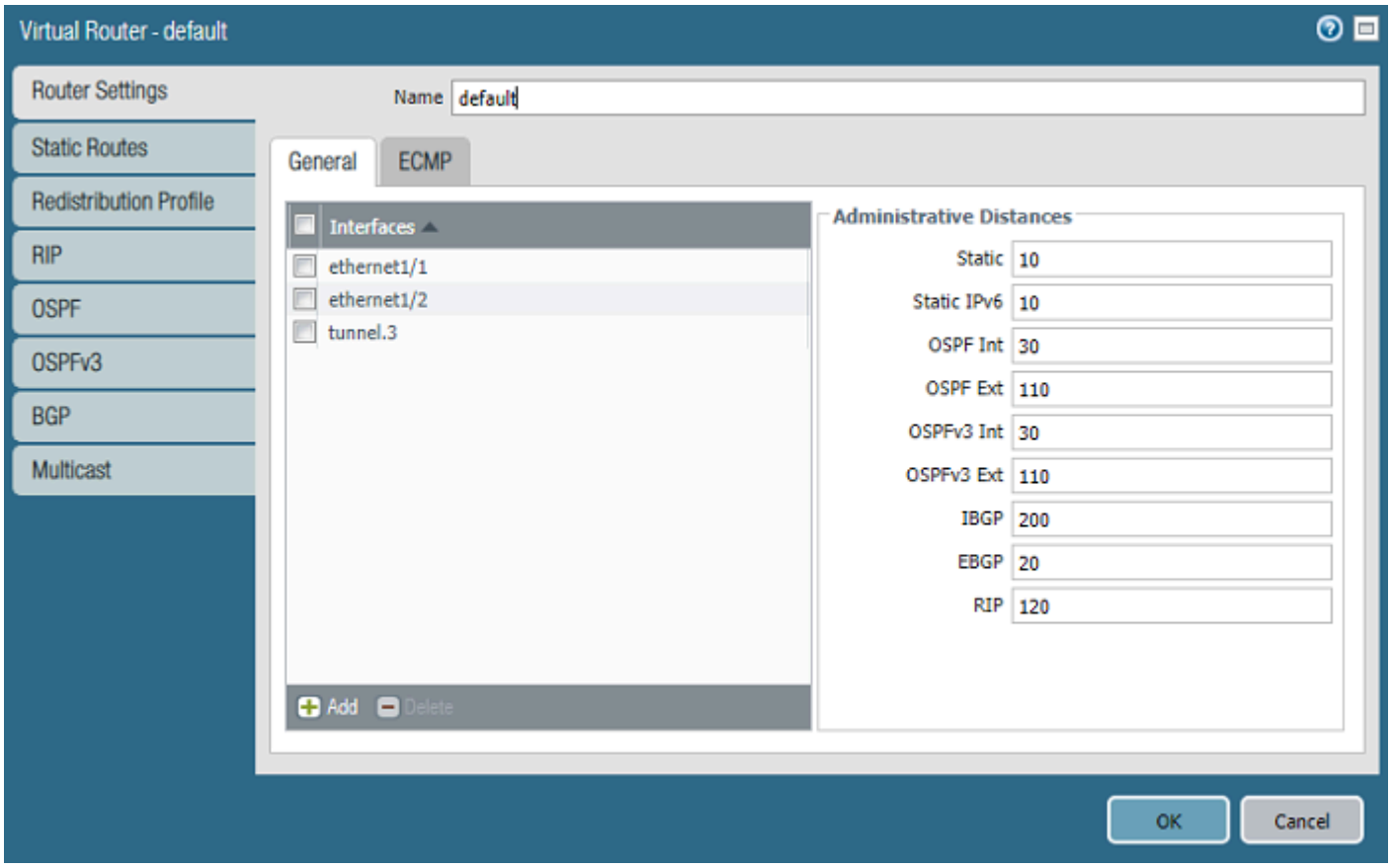

Figure 22: Virtual Router General Settings

5. Nutanix Cloud VM-Series GlobalProtect Configuration

In the Network tab, click GlobalProtect and add a portal and gateways.

GlobalProtect Portal

Use the information in this Palo Alto Networks article to create the RootCert, IntermediateCert, and ServerCert certificates.

Before you create the GlobalProtect portal, you need to create the LDAP_Auth authentication profile:

- In the Palo Alto Networks VM WebGUI, click Device, then Authentication Profile, and create the authentication profile as shown in the following figure. For more details, see the Palo Alto Networks GlobalProtect documentation website.

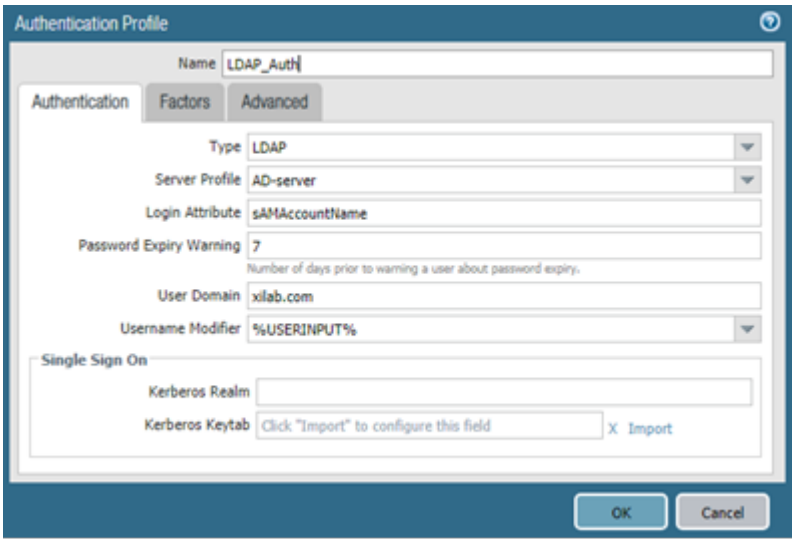

Figure 23: Create LDAP_Auth Authentication Profile

You also need to create the SSL/TLS service profile SSL-TSL-Server:

- In the Palo Alto Networks VM WebGUI, click Device, then Certificate Management, then Certificate to create the server certificate ServerCert as shown in the following image.

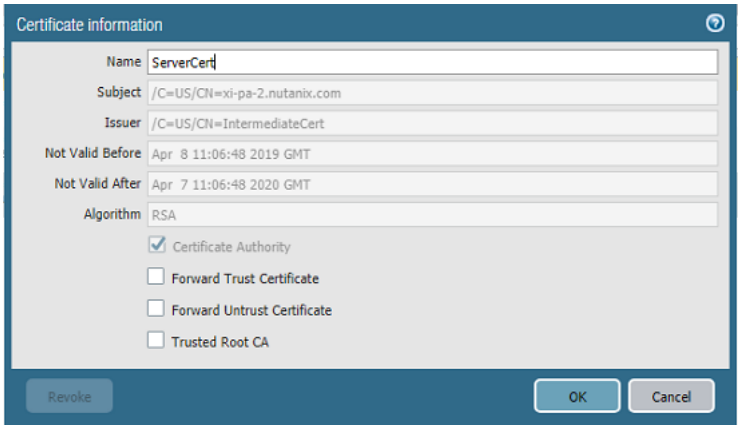

Figure 24: ServerCert Certificate Information

- In the Palo Alto Networks VM WebGUI, click Device, then Certificate Management, then SSL/TLS Service Profile to create the SSL/TLS service profile SSL-TSL-Server. Select the server certificate you created from the SSL/TLS Service Profile dropdown for the Server Authentication.

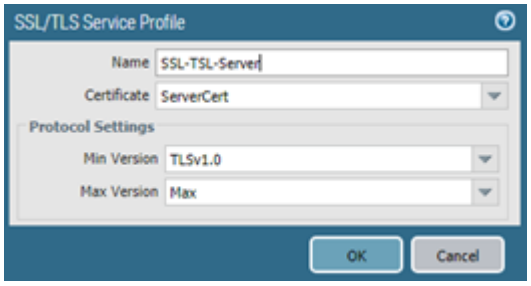

Figure 25: SSL/TLS Service Profile SSL-TSL-Server

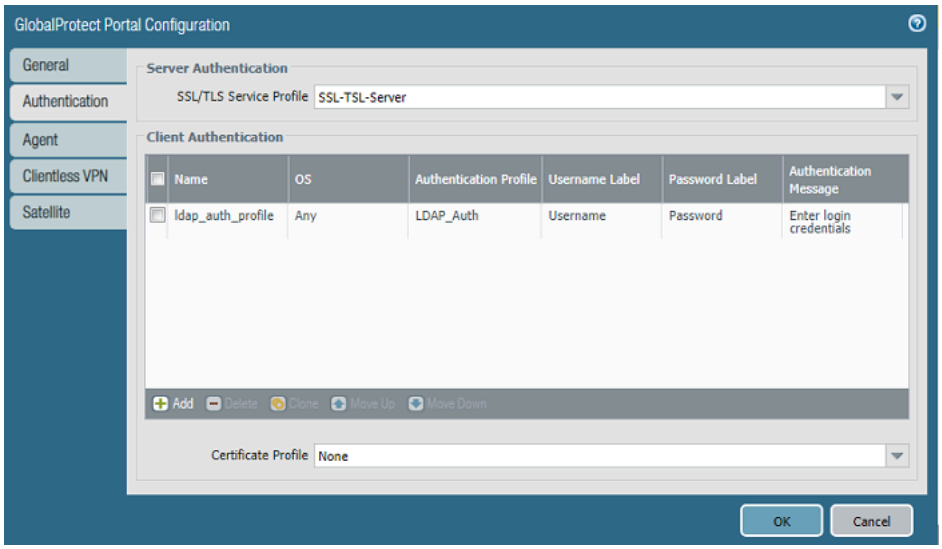

Figure 26: GlobalProtect Portal Server Authentication

Now you're ready to create the GlobalProtect portal:

- In the Palo Alto Networks VM WebGUI, open the GlobalProtect Portal Configuration window.
- In the General tab, name the portal GP-Portal and assign it the following configuration:
  - Interface: ethernet1/2
  - IP Address Type: IPv4 Only
  - IPv4 Address: 10.10.1.245/24
  - Leave Portal Login Page and Portal Landing Page as factory-default
  - App Help Page: None

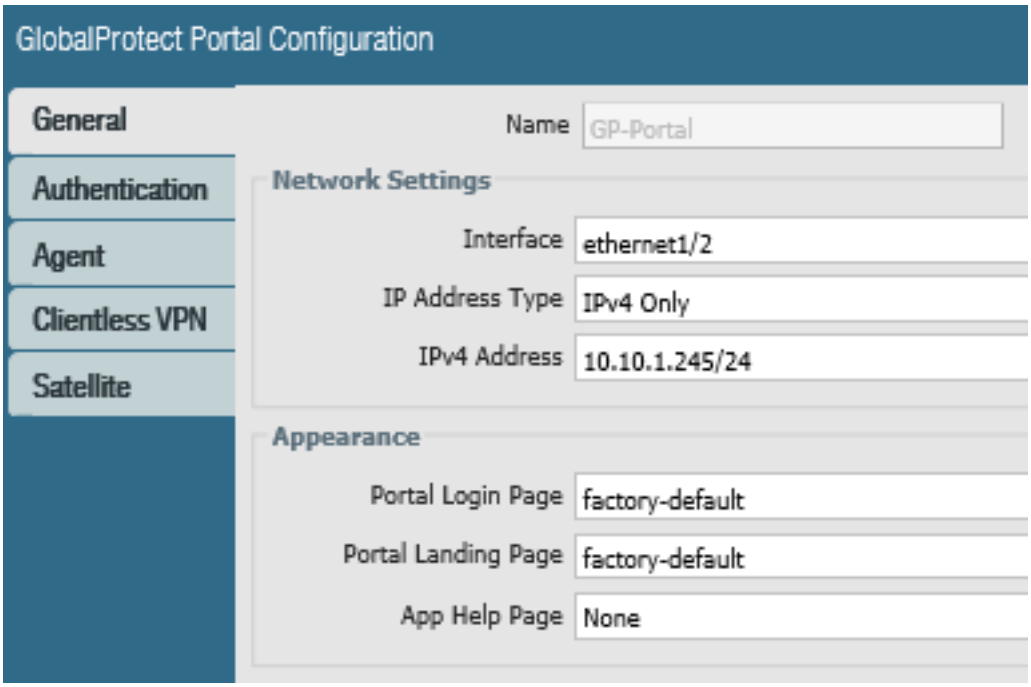

Figure 27: GlobalProtect Portal General Settings

- In the Authentication tab, click Add to open the Client Authentication window and configure client authentication with the following settings:
  - Name: ldap_auth_profile
  - OS: Any
  - Authentication Profile: LDAP_Auth
  - Enter your logon information and click OK.

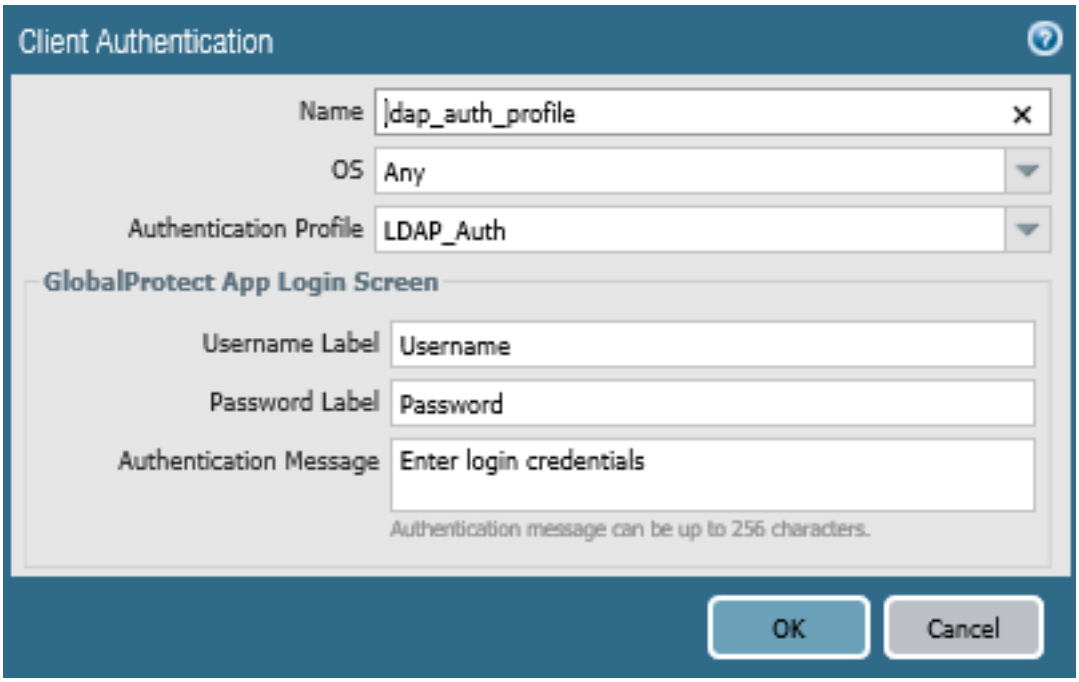

Figure 28: GlobalProtect Portal Client Authentication

- In the Agent tab, select the client configuration called GP-Client-Config-1.

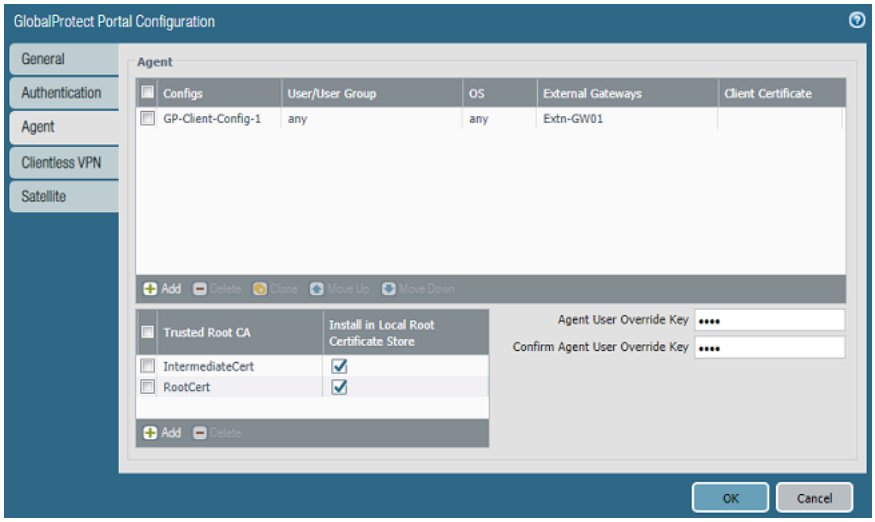

Figure 29: GlobalProtect Portal Agent

- Also in the Agent tab, in the Trusted Root CA column, select RootCert and IntermediateCert, then Install in Local Root Certificate Store for both. This

configuration installs these certificates in the client's local root certificate store after the client successfully connects to the portal for first time. Enter your agent user override credentials.

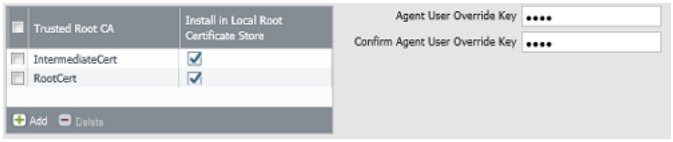

Figure 30: GlobalProtect Portal Trust Root CA Settings

- In the Configs pane, click Agent, then Add and configure as follows:
  - Name: GP-Client-Config-1
  - Client Certificate: None
  - Save User Credentials: Yes
  - Select Generate cookie for authentication override
  - Select Accept cookie for authentication override
  - Cookie Lifetime: select Hours, then type 72.
  - Certificate to Encrypt/Decrypt Cookie: RootCert
  - Don't select any options under Components that Require Dynamic Passwords (Two-Factor-Authentication).

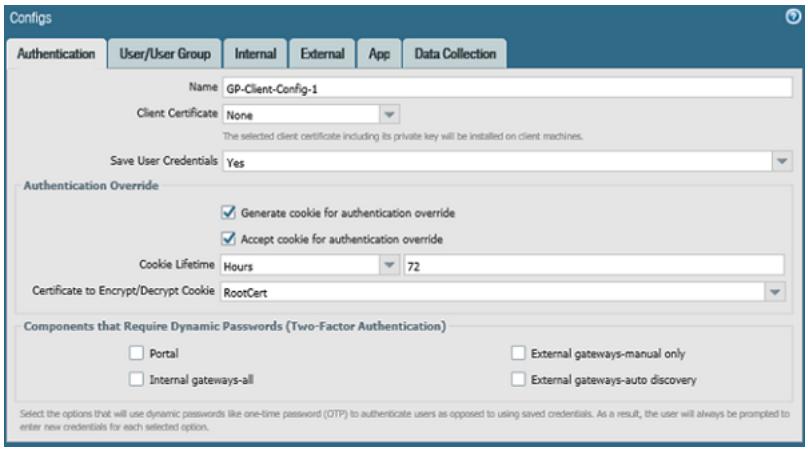

Figure 31: GlobalProtect Portal Authentication Settings

- In the User/Users Group tab, leave the OS as the default and set User Group to Any.
- In the External tab, click Add in the External Gateway tab to open the External Gateway window and create the following gateway:
  - Name: Extn-GW01
  - Select IP
  - IPv4: 206.80.156.10
  - Priority Rule: Any (Highest Priority)

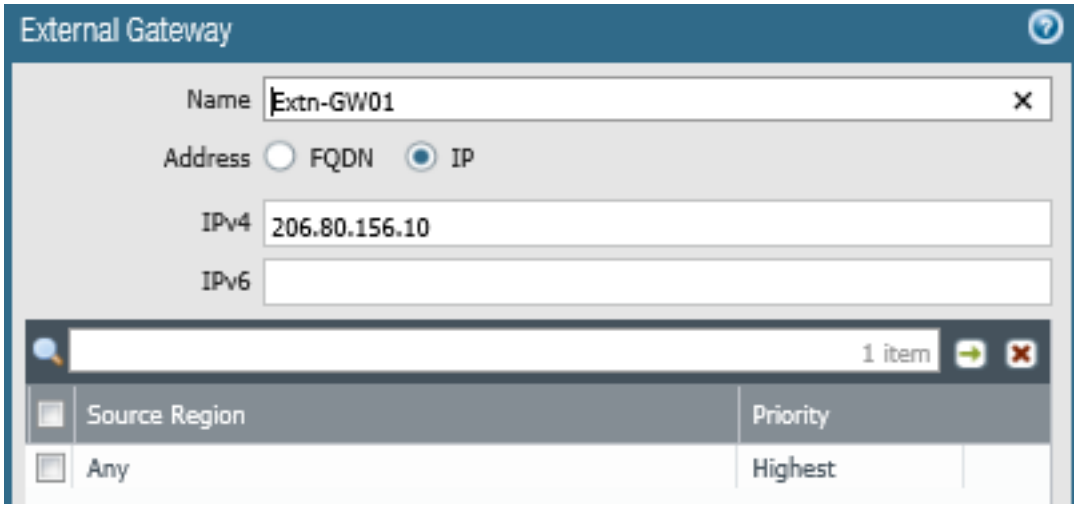

Figure 32: GlobalProtect Portal External Gateway

- Still in the External tab, enter 5 in the Cutoff Time (sec) box and select Extn-GW01 under External Gateways.

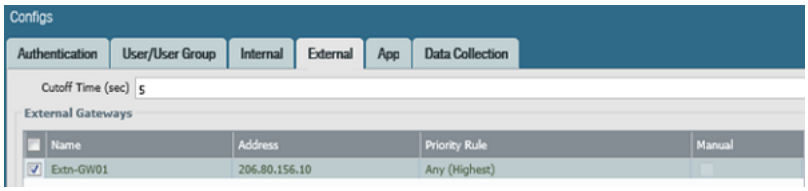

Figure 33: GlobalProtect Portal External Settings

- In the App tab, choose On-demand as the Connect Method and leave everything else with the default settings.

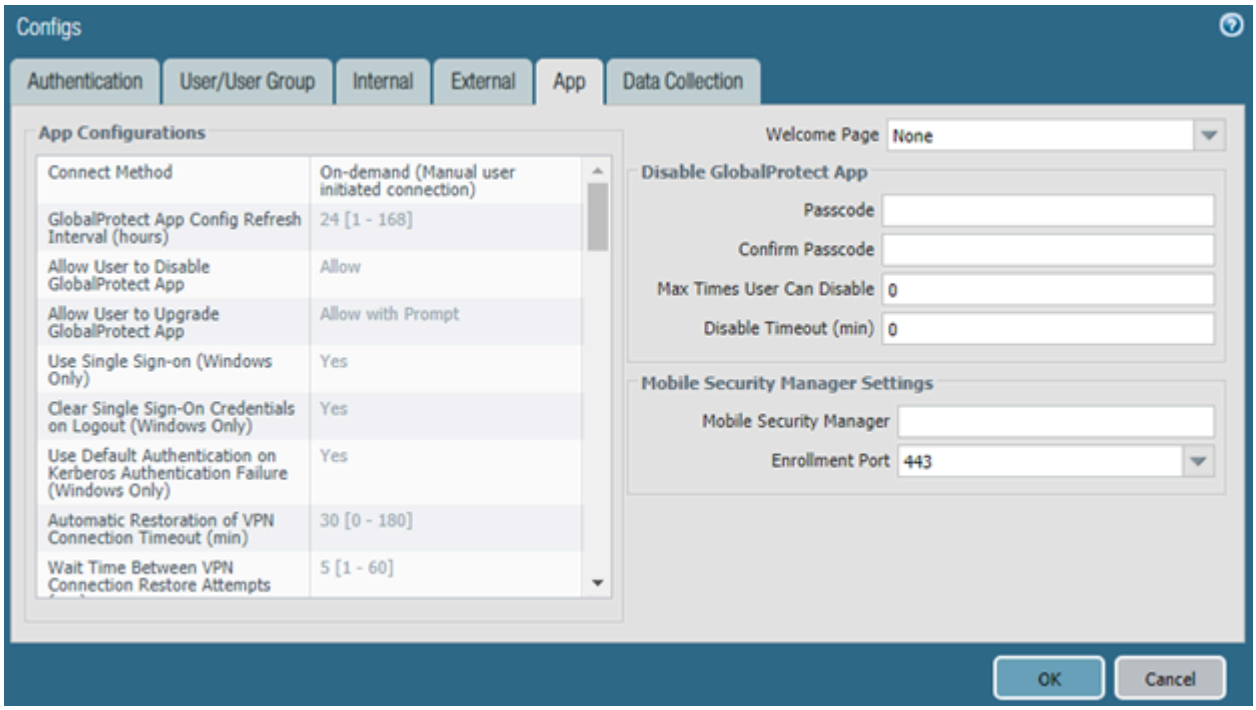

Figure 34: GlobalProtect Portal App Configurations

GlobalProtect Gateways

In the Palo Alto Networks VM WebGUI, open the GlobalProtect Gateway Configuration window and configure a gateway.

In the General tab, enter the following configuration:

- Name: GP-GW-01
- Interface: ethernet1/2 (gateway for remote users)
- IP Address Type: IPV4 Only
- IPv4 Address: 10.10.1.245/24

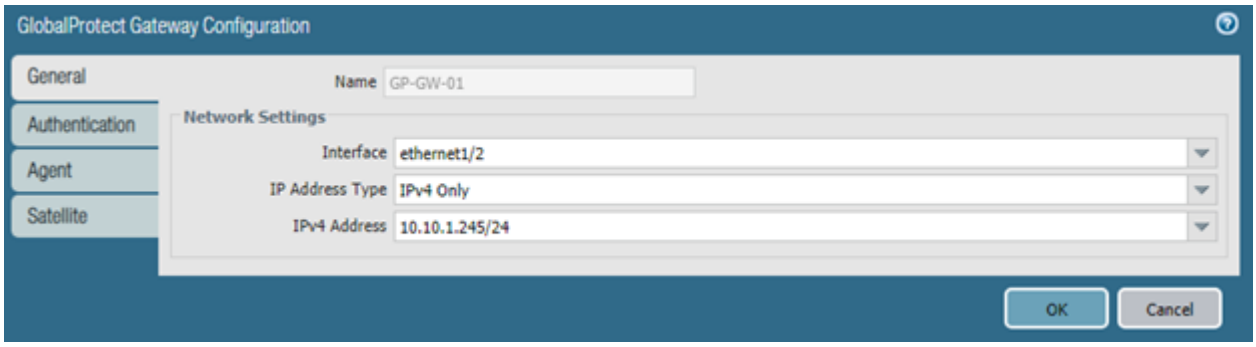

Figure 35: GlobalProtect Gateway General Settings

In the Authentication tab, click Create Client Authentication and configure as follows:

- Name: auth2
- OS: Any
- Authentication Profile: LDAP_Auth
- Enter your credentials.

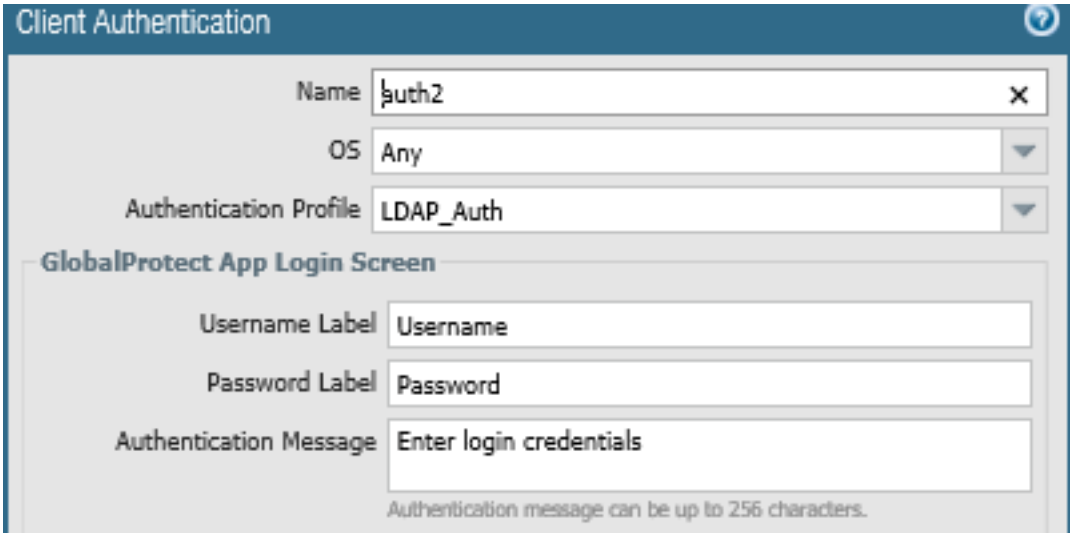

Figure 36: GlobalProtect Gateway Create Client Authentication

- Select the same SSL/TLS service profile you did for the GlobalProtect portal authentication and select the client authentication you created.

Figure 37: GlobalProtect Gateway Authentication Settings

In the Agent tab, click Tunnel Settings and configure as follows:

- Select Tunnel Mode.
- Tunnel Interface: tunnel.3
- Max User: 5
- Select Enable IPSec (With this setting enabled, GlobalProtect always tries to connect over IPSec first, then falls back to SSL if that fails.)
- GlobalProtect IPSec Crypto: default
  - To create the IPSec crypto profile, in the Palo Alto Networks VM WebGUI, navigate to Network, then Network Profiles, then GlobalProtect IPSec Crypto. Click Add to create the crypto profile default.

Figure 38: GlobalProtect IPSec Crypto Profile

- Leave Enable X-Auth Support cleared.
- Leave Group Name, Group Password, and Confirm Group Password blank and select Skip Auth on IKE Rekey.

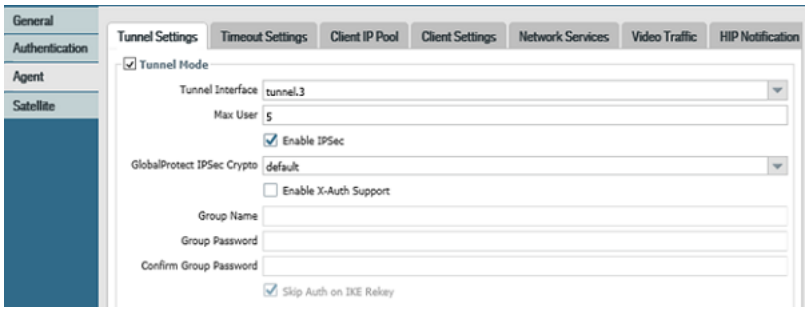

Figure 39: GlobalProtect Gateway Agent Tunnel Settings

Still in the Agent tab, click Client Settings:

- Click Add to open the Configs window. Click Authentication Override and configure as follows:
  - Name: GP-GW-Client-Config
  - Select Generate cookie for authentication override
  - Select Accept cookie for authentication override
  - Cookie Lifetime: select Hours, then type 72
  - Certificate to Encrypt/Decrypt Cookie: RootCert

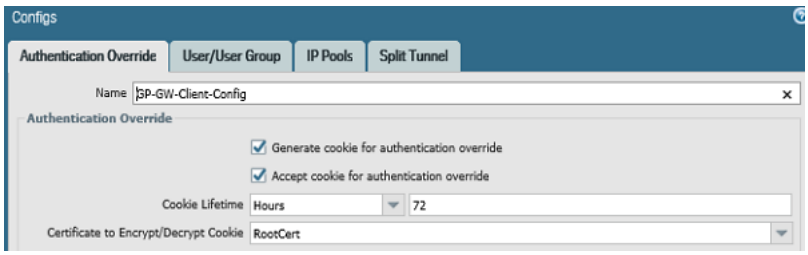

Figure 40: GlobalProtect Gateway Agent Client Settings: Authentication Override

- In the User/User Group tab, leave the OS as default and set the User Group to Any.
- In the IP Pools tab, select the IP pool you use to assign IP addresses to clients.

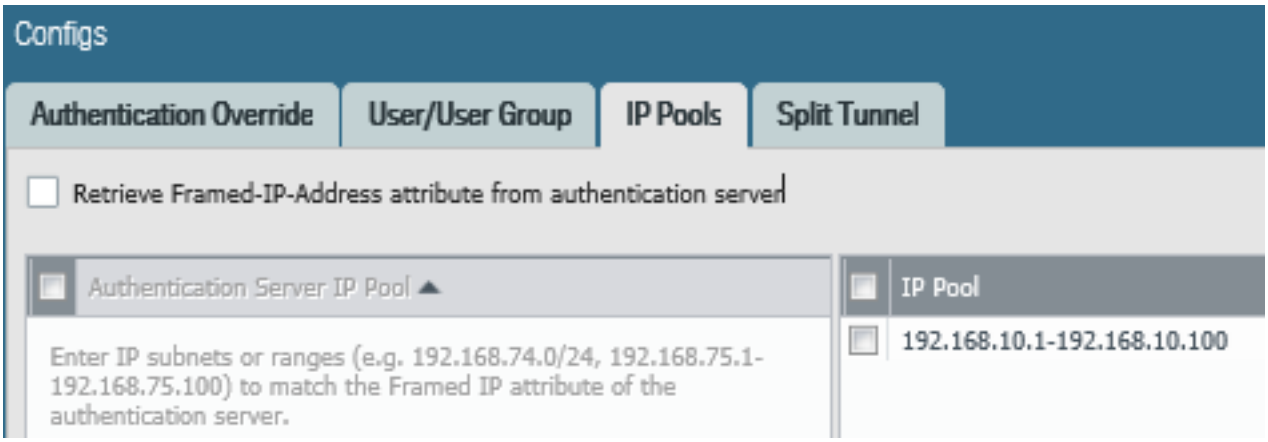

Figure 41: GlobalProtect Gateway Agent Client Settings: IP Pools

- In the Split Tunnel tab, under Access Route, don't select No Direct access to local network. Select 10.19.175.0/24.

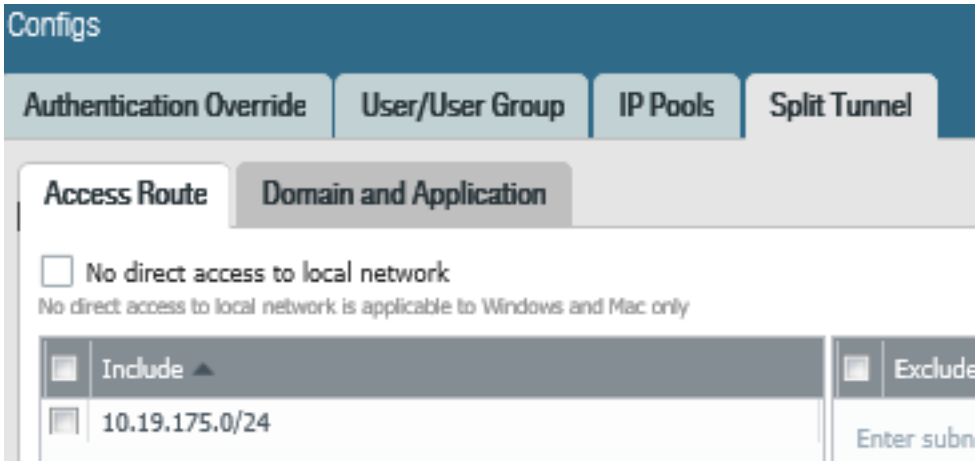

Figure 42: GlobalProtect Gateway Agent Client Settings: Split Tunnel

6. Conclusion

After you complete the entire configuration in this document, you should be able to connect to the Nutanix Cloud VPN gateway using the GlobalProtect client software on your personal laptop or Mac.

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 or follow us on Twitter @nutanix.

List of Figures