



PaloAlto

VM-Series on OCB FE

Configuration Guide

1st February 2020
Version 2.0

document control

date	version no.	author	change/addition
12 - September 2018	1.00	Ahmad Samak	Creation
1 st February 2020	2.00	Ahmad Samak	Update

table of contents

1	References	4
2	Introduction	5
3	Deployment Method	6
3.1	Hybrid and VPC to VPC	6
3.2	On Cloud /On Cloud	7
4	Solution Configuration	8
4.1	Hybrid and VPC to VPC Model	8
4.1.1	On Premises ESXI PaloAlto VM-Series configuration	8
4.2	Configure PaloAlto VM-Series firewall on OCB FE	11
4.2.1	configure Interfaces and zones	11
4.2.2	Add static routes	11
4.2.3	Add policy security rules	11
4.2.4	Add Nat Policy Rules	11
4.3	Site-to-Site VPN-IPSEC Tunnel Configuration	12
4.3.1	Configuring the Palo Alto Networks Firewalls	12
4.4	GlobalProtect User Authentication	17
4.4.1	Create interfaces and zones	17
4.4.2	Establish Trust	20
4.4.3	Authenticate the User	21
4.4.4	Configure the Gateway	22
4.4.5	Configure Portal	23
4.4.6	Deploy GlobalProtect Agent	25
4.4.7	Service Route Configuration	26

1 References

Reference	Description	Link to document
1	VM-Series Deployment Guide	https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization
2	PaloAlto troubleshooting	https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/troubleshooting

2 Introduction

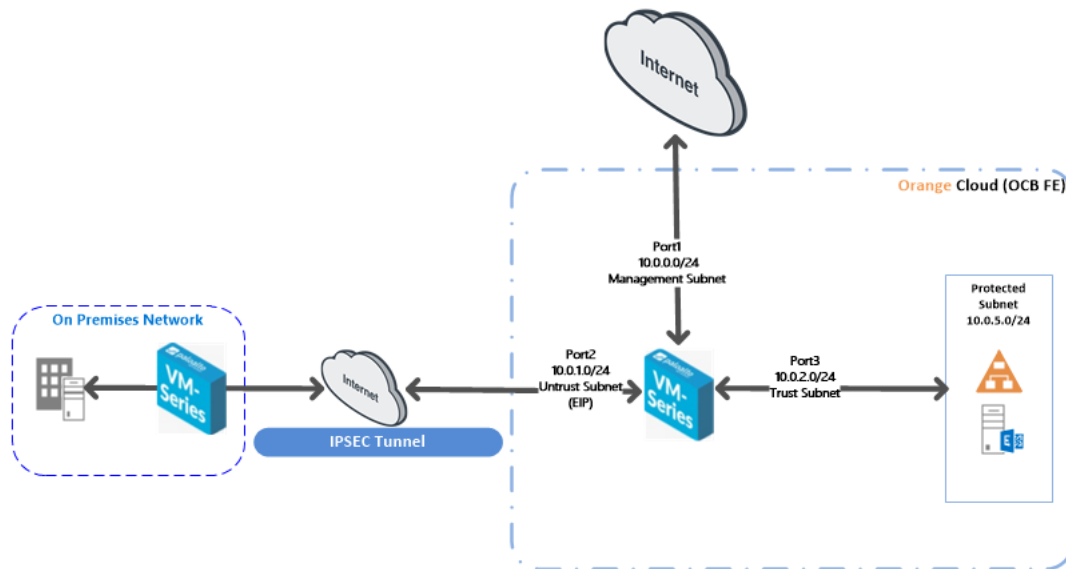
Paloalto VM-Series is a network security appliance that can apply a number of features to network traffic, providing a consolidated security solution to match the needs of any network, big or small. This document mainly shows how to prepare and configure a Site-to-Site VPN connection between and on Premises PaloAlto VM-Series on ESXI and vm-series firewall on OCB FE on a VPC as well as a connection between vm-series firewall and vpn gateways.

3 Deployment Method

Use the VM-Series firewall on Azure to secure your network users in the following scenarios:

3.1 Hybrid and VPC to VPC

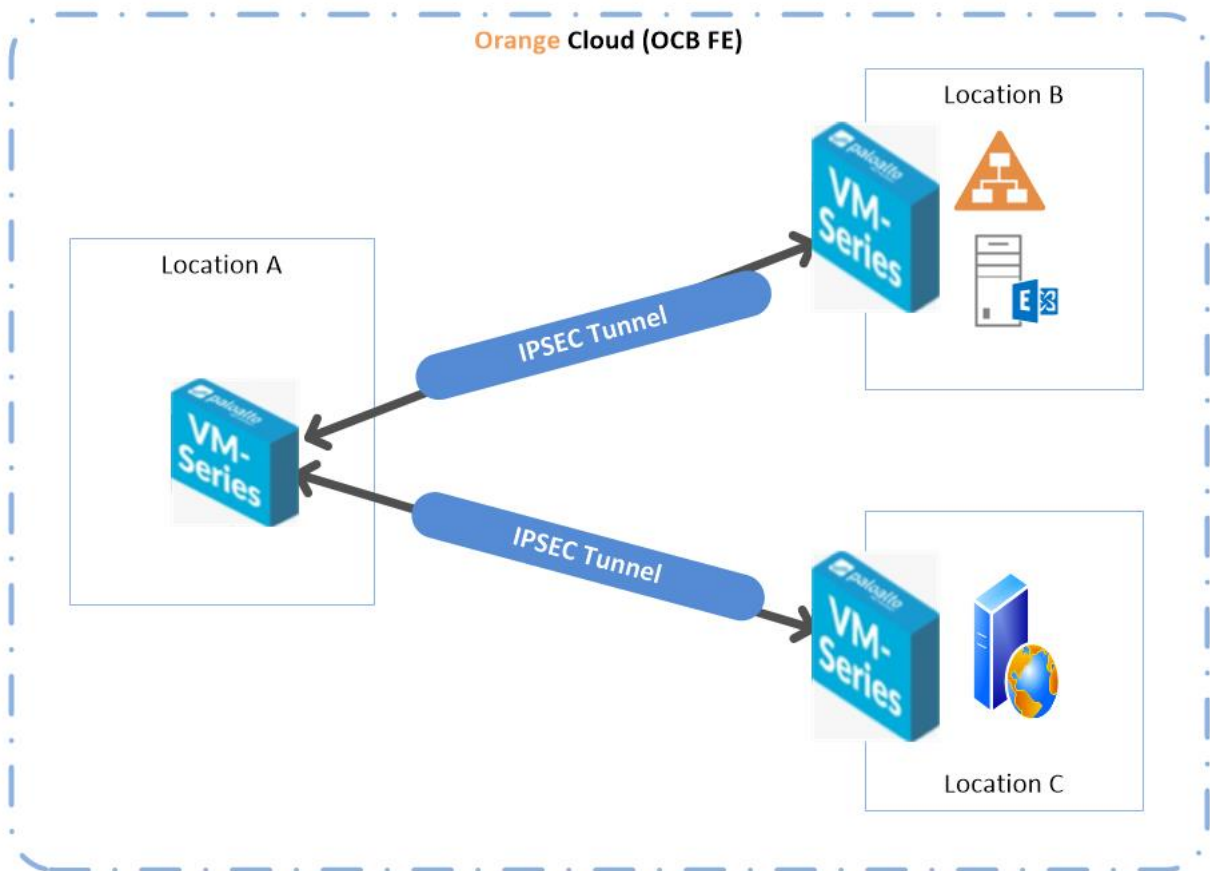
The VM-Series firewall on OCB FE allows you to securely extend your physical data center/private cloud into OCB FE using IPsec tunneling. To improve your data center security, if you have segmented your network and deployed your workloads in separate VPC's, you can secure traffic flowing between VPC's with an IPsec tunnel and application whitelisting policies.



- **Inter-Subnet**—The VM-Series firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.
- **Gateway**—The VM-Series firewall serves as the VPC gateway to protect Internet-facing deployments in the OCB FE (VPC). The VM-Series firewall secures traffic destined to the servers in the VPC and it also protects against lateral threats for inter-subnet traffic between applications in a multitier architecture.
- **GlobalProtect**—Use the Azure infrastructure to quickly and easily deploy the VM-Series firewall as GlobalProtect™ and extend your gateway security policy to remote users and devices, regardless of location.

3.2 On Cloud /On Cloud

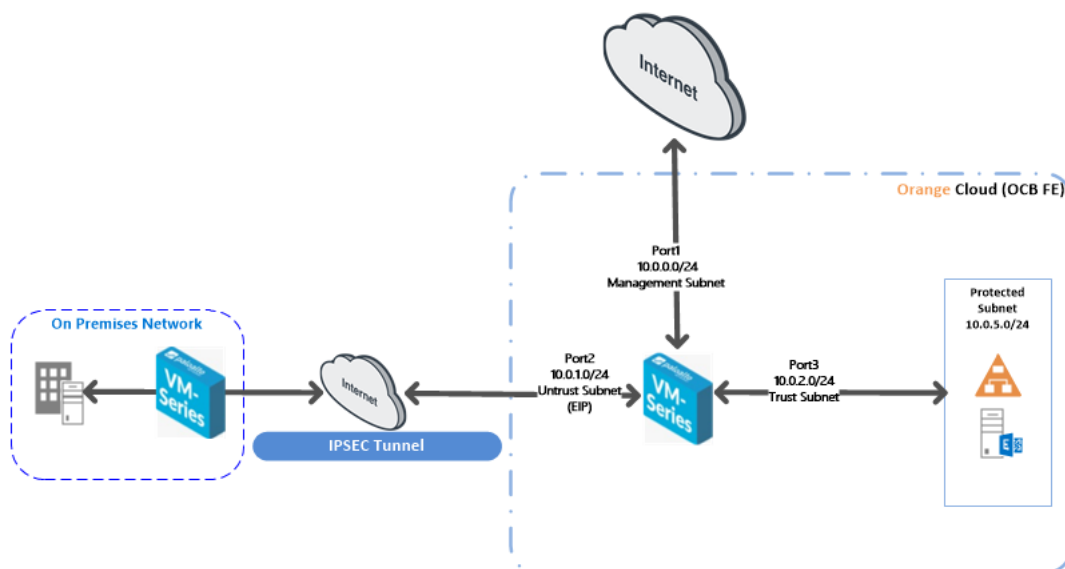
The VM-Series firewall on OCB FE allows you to securely extend your multiple location cloud VPC's into OCB FE using IPsec tunneling.



- **Inter-Subnet** The VM-Series firewall can front your servers in a VPC and protects against lateral threats for inter-subnet traffic between applications in a multi-tier architecture.
- **VPN Gateway** A Virtual Private Network (VPN) provides an encrypted communication channel that enables users to remotely access VPCs. In this Scenario. Palo Alto VM's are the VPN gateways in each region
- **Multiple location VPC's** with one subnet in each VPC.

4 Solution Configuration

4.1 Hybrid and VPC to VPC Model



In this model we will configure the following:

1. On Premises ESXI PaloAlto VM-Series configuration
2. IPSEC tunnel configuration between on premises vm-series ESXI firewall and OCB FE vm-series firewall.
3. GlobalProtect Remote VPN configuration

4.1.1 On Premises ESXI PaloAlto VM-Series configuration

4.1.1.1 Creating a policy to allow traffic from the internal network to the Internet

	Name	Tags	Type	Source				Destination		Application
				Zone	Address	User	HIP Profile	Zone	Address	
1	Trust-To-Internet	none	universal	Trust_Zone	any	any	any	Internet_Zone	any	any
2	Internet-To-Trust	none	universal	Internet_Zone	any	any	any	Trust_Zone	any	any
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any
4	interzone-default	none	interzone	any	any	any	any	any	any	any

4.1.1.2 Add NAT Policy Rule

			Original Packet							
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	
1	Internet	none	Trust_Zone	Internet_Zone	any	any	any	any	dynamic-ip-and-port ethernet1/1 192.168.1.106/24	

NAT Policy Rule ?

General Original Packet Translated Packet

☐ Any

Source Zone Trust_Zone

Destination Zone Internet_Zone

Destination Interface any

Service any

☒ Any

Source Address

☒ Any

Destination Address

+ Add - Delete

OK Cancel

NAT Policy Rule ?

General Original Packet Translated Packet

Source Address Translation

Translation Type Dynamic IP And Port

Address Type Interface Address

Interface ethernet1/1

IP Address 192.168.1.106/24

☐ **Destination Address Translation**

Translated Address

Translated Port [1 - 65535]

OK Cancel

4.1.1.3 Create a Static Route for the internet and the onpremis trust zone

Network > Virtual Router > Default > Static Routes > Add

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 IPv6

5 items

	Name	Destination	Interface	Next Hop		Admin Distance	Metric	BFD	Route Table
				Type	Value				
<input type="checkbox"/>	Internet-Route	0.0.0.0/0	ethernet...	ip-address	192.16...	default	10	None	unicast
<input type="checkbox"/>	Route-Inside	192.168.4.0/24	ethernet...	ip-address	192.16...	default	10	None	unicast
<input type="checkbox"/>	to-web-vpc	10.0.0.0/16	tunnel.3			default	10	None	unicast
<input type="checkbox"/>	to-business...	10.1.0.0/16	tunnel.3			default	10	None	unicast
<input type="checkbox"/>	to-tunnel	172.16.4.0/24	tunnel.3			default	10	None	unicast

+ Add - Delete Clone

OK Cancel

Virtual Router - Static Route - IPv4

Name Internet-Route

Destination 0.0.0.0/0

Interface ethernet1/1

Next Hop IP Address

192.168.1.250

Admin Distance 10 - 240

Metric 10

Route Table Unicast

BFD Profile Disable BFD

☐ Path Monitoring

Failure Condition ☒ Any ☐ All Preemptive Hold Time (min) 2

	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count
<p>+ Add - Delete</p>						

OK Cancel

4.2 Configure PaloAlto VM-Series firewall on OCB FE

4.2.1 configure Interfaces and zones

configure 2 interfaces

- Untrust interface
- Trust Interface

ethernet1/2	Layer3	Allow All Management		172.16.4.4/24	default	Untagged	none	VPN-Zone
ethernet1/3	Layer3	Allow All Management		10.0.0.231/24	default	Untagged	none	Web-Zone
ethernet1/4	Layer3	Allow All Management		10.1.0.72/24	default	Untagged	none	Business_Zone

4.2.2 Add static routes

Static Routes	IPv4
Redistribution Profile	
RIP	
OSPF	
OSPFv3	

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
to-lab	192.168.0.0/16	tunnel.1			default	10	None	unicast
to-Internet	0.0.0.0/0	ethernet1/2	ip-address	172.16.4.1	default	10	None	unicast

Important Notice:

By default, the vm-series firewall can access the internet only through the management interface so we must add a static route for the internet access of the Untrust interface and the next hop should be the gateway of the untrust Subnet as shown below. The next hop is 172.16.4.1 (gateway of the untrust Subnet)

to-Internet	0.0.0.0/0	ethernet1/2	ip-address	172.16.4.1	default	10	None	unicast
-------------	-----------	-------------	------------	------------	---------	----	------	---------

4.2.3 Add policy security rules

Policies > Security > Add

1	vpn-to-Web	none	universal	VPN-Zone	any	any	any	Web-Zone	any	any
2	Web-to-vpn	none	universal	Web-Zone	any	any	any	VPN-Zone	any	any
3	VPN-Business	none	universal	VPN-Zone	any	any	any	Business_Zone	any	any
4	Business-VPN	none	universal	Business_Zone	any	any	any	VPN-Zone	any	any

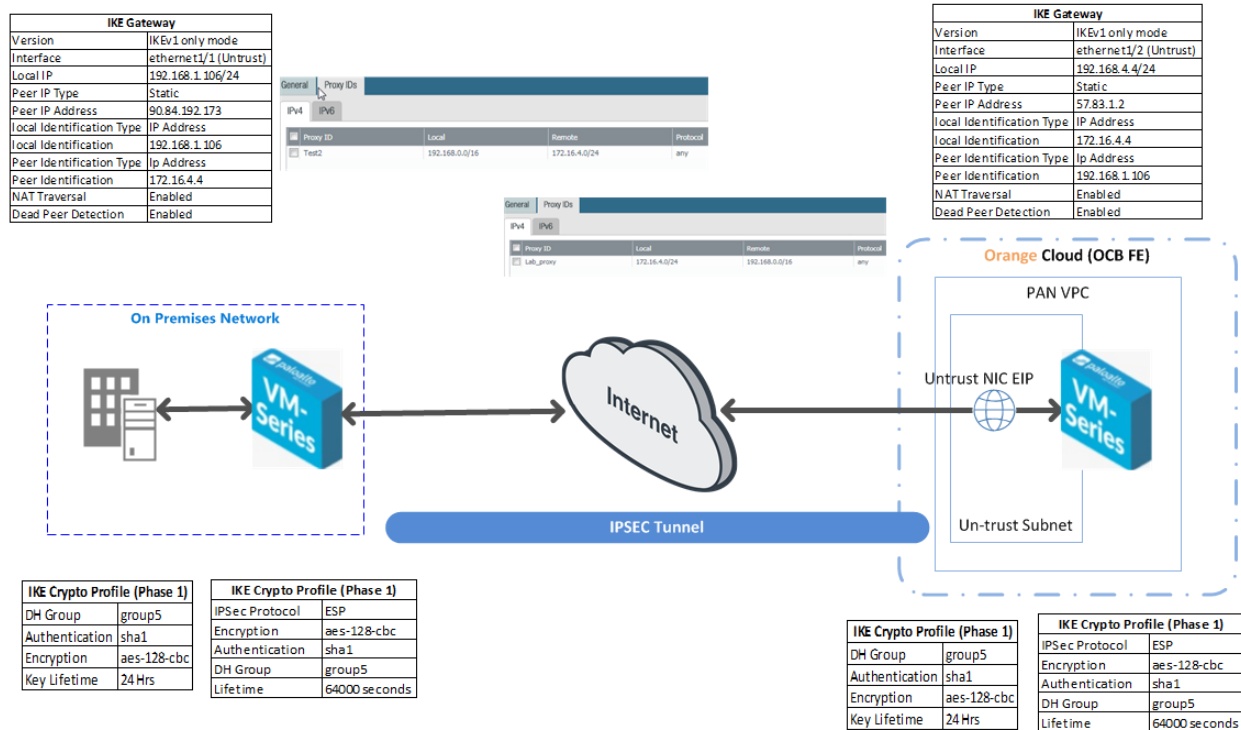
4.2.4 Add Nat Policy Rules

Policies > Nat > Add

1	VPN-to-Web	none	VPN-Zone	Web-Zone	any	any	any	any	dynamic-ip-and-port	ethernet1/3	10.0.0.231/24
2	Web-to-VPN	none	Web-Zone	VPN-Zone	any	any	any	any	dynamic-ip-and-port	ethernet1/2	172.16.4.4/24
3	VPN-to-Biz	none	Business_Zone	Business_Zone	any	10.1.0.4	172.16.4.4	any	none		
4	Biz-to-VPN	none	VPN-Zone	Business_Zone	any	any	any	any	dynamic-ip-and-port	ethernet1/4	10.1.0.72/24

4.3 Site-to-Site VPN-IPSEC Tunnel Configuration

4.3.1 Configuring the Palo Alto Networks Firewalls



IPSec Tunnel configuration will be performed on Both the firewalls as per the diagram above,

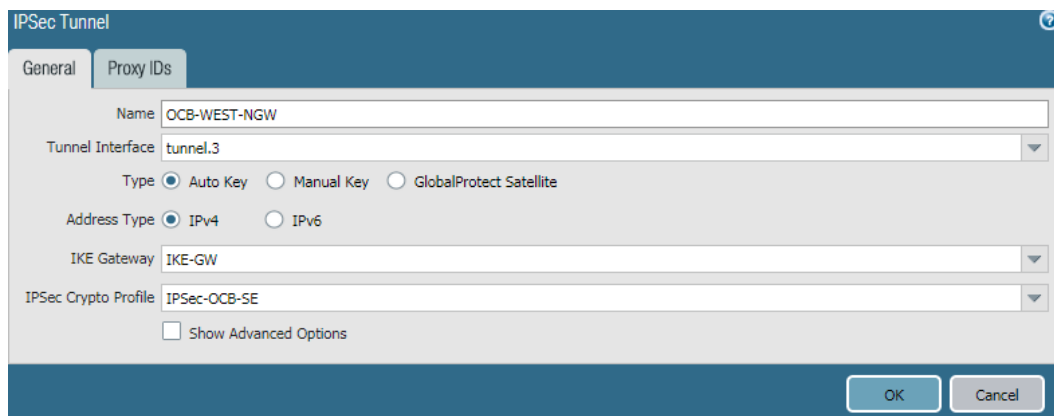
Set Up an IPSec Tunnel

The IPSec tunnel configuration allows you to authenticate and/or encrypt the data (IP packet) as it traverses across the tunnel.

If you are setting up the Palo Alto Networks firewall to work with a peer that supports policy-based VPN, you must define Proxy IDs. Devices that support policy-based VPN use specific security rules/policies or access-lists (source addresses, destination addresses and ports) for permitting interesting traffic through an IPSec tunnel. These rules are referenced during quick mode/IKE phase 2 negotiation, and are exchanged as Proxy-IDs in the first or the second message of the process. So, if you are configuring the Palo Alto Networks firewall to work with a policy-based VPN peer, for a successful phase 2 negotiation you must define the Proxy-ID so that the setting on both peers is identical. If the Proxy-ID is not configured, because the Palo Alto Networks firewall supports route-based VPN, the default values used as Proxy-ID are source ip: 0.0.0.0/0, destination ip: 0.0.0.0/0 and application: any; and when these values are exchanged with the peer, it results in a failure to set up the VPN connection.

Steps

1. Select Network>IPSec Tunnels and then Add a new tunnel configuration.
2. On the General tab, enter a Name for the new tunnel.
3. Select the Tunnel interface that will be used to set up the IPSec tunnel.



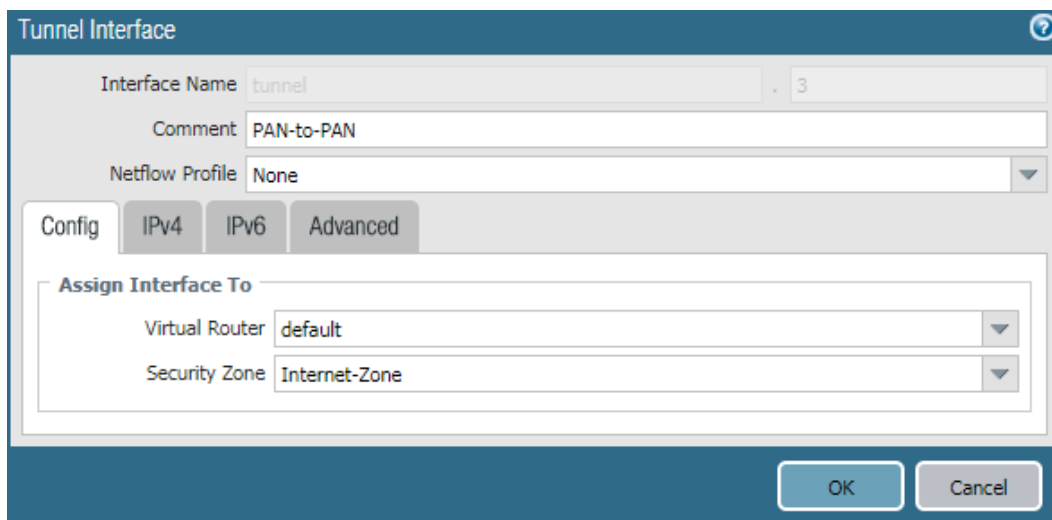
The IPSec Tunnel configuration window shows the following settings:

- Name:** OCB-WEST-NGW
- Tunnel Interface:** tunnel.3
- Type:** Auto Key (selected), Manual Key, GlobalProtect Satellite
- Address Type:** IPv4 (selected), IPv6
- IKE Gateway:** IKE-GW
- IPSec Crypto Profile:** IPSec-OCB-SE
- Show Advanced Options:** (unchecked)

Buttons: OK, Cancel

To create a new tunnel interface:

- Select Tunnel Interface>New Tunnel Interface. (You can also select NetworkInterfaces>Tunnel and click Add.)
- In the Interface Name field, specify a numeric suffix, such as .2.



The Tunnel Interface configuration window shows the following settings:

- Interface Name:** tunnel.3
- Comment:** PAN-to-PAN
- Netflow Profile:** None
- Config tab:** Selected
- Assign Interface To:**
 - Virtual Router:** default
 - Security Zone:** Internet-Zone

Buttons: OK, Cancel

- On the Config tab, select the Security Zone drop-down to define the zone as follows:

Use your trust zone as the termination point for the tunnel—Select the zone from the drop-down. Associating the tunnel interface with the same zone (and virtual router) as the external-facing interface on which the packets enter the firewall mitigates the need to create inter-zone routing.

Or:

Create a separate zone for VPN tunnel termination (Recommended)—Select New Zone, define a Name for the new zone (for example vpn-corp), and click OK.

- In the Virtual Router drop-down, select default.
- (Optional) If you want to assign an IPv4 address to the tunnel interface, select the IPv4 tab, and Add the IP address and network mask, for example 10.31.32.1/32.
- Click OK.

4. Define the IKE Gateway .

- Select NetworkProfilesIKE Gateways, click Add, and on the General tab, enter the Name of the gateway.
- For Version, select IKEv1 only mode, IKEv2 only mode, or IKEv2 preferred mode. The IKE gateway begins its negotiation with its peer in the mode specified here. If you select IKEv2 preferred mode, the two peers will use IKEv2 if the remote peer supports it; otherwise they will use IKEv1. The Version selection also determines which options are available on the Advanced Options tab.

The screenshot shows the 'IKE Gateway' configuration window with the 'General' tab selected. The configuration details are as follows:

Field	Value
Name	IKE-GW
Version	IKEv1 only mode
Address Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Interface	ethernet1/1
Local IP Address	192.168.1.106/24
Peer IP Type	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
Peer IP Address	90.84.192.137
Authentication	<input checked="" type="radio"/> Pre-Shared Key <input type="radio"/> Certificate
Pre-shared Key
Confirm Pre-shared Key
Local Identification	IP address 192.168.1.106
Peer Identification	IP address 172.16.4.4

At the bottom right, there are 'OK' and 'Cancel' buttons.

The screenshot shows the 'IKE Gateway' configuration window with the 'Advanced Options' tab selected. Under 'Common Options', 'Enable NAT Traversal' is checked. The 'IKEv1' section shows 'Exchange Mode' set to 'auto', 'IKE Crypto Profile' set to 'IKE-OCB-SE', and 'Enable Fragmentation' is unchecked. 'Dead Peer Detection' is checked with an interval of 5 and a retry of 5. 'OK' and 'Cancel' buttons are at the bottom right.

5- Define IKE Crypto Profile

In this phase, the firewalls use the parameters defined in the IKE Gateway configuration and the IKE Crypto profile to authenticate each other and set up a secure control channel. IKE Phase supports the use of preshared keys or digital certificates (which use public key infrastructure, PKI) for mutual authentication of the VPN peers. Preshared keys are a simple solution for securing smaller networks because they do not require the support of a PKI infrastructure. Digital certificates can be more convenient for larger networks or implementations that require stronger authentication security.

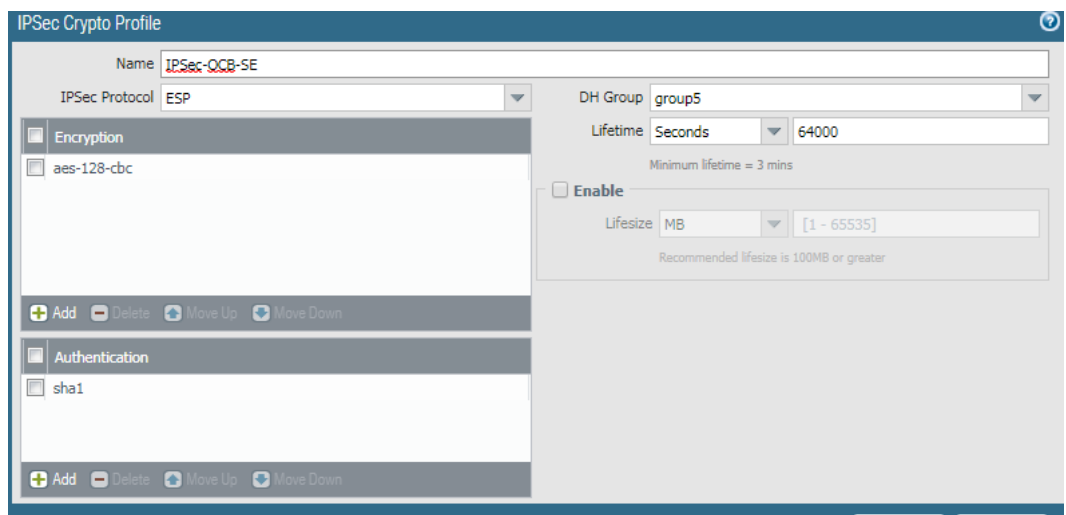
When using certificates, make sure that the CA issuing the certificate is trusted by both gateway peers and that the maximum length of certificates in the certificate chain is 5 or less. With IKE fragmentation enabled, the firewall can reassemble IKE messages with up to 5 certificates in the certificate chain and successfully establish a VPN tunnel.

The screenshot shows the 'IKE Crypto Profile' configuration window. The 'Name' field is 'IKE-OCB-SE'. Under 'DH Group', 'group5' is selected. Under 'Encryption', 'aes-128-cbc' is selected. Under 'Authentication', 'sha1' is selected. The 'Timers' section shows 'Key Lifetime' set to 'Hours' with a value of '24' and a note 'Minimum lifetime = 3 mins'. 'IKEv2 Authentication' is set to 'Multiple'. 'OK' and 'Cancel' buttons are at the bottom right.

6. Define IPSEC Crypto

Create a new IPSEC profile.

- Select Network>Network Profiles>IPSec Crypto and select Add.
- Enter a Name for the new profile.
- Select the IPsec Protocol—ESP or AH—that you want to apply to secure the data as it traverses across the tunnel.
- Click Add and select the Authentication and Encryption algorithms for ESP, and Authentication algorithms for AH, so that the IKE peers can negotiate the keys for the secure transfer of data across the tunnel.
- Commit your IPsec profile.
- Click OK and click Commit.
- Attach the IPsec Profile to an IPsec tunnel configuration.



7. Setup Tunnel Monitoring (Optional)

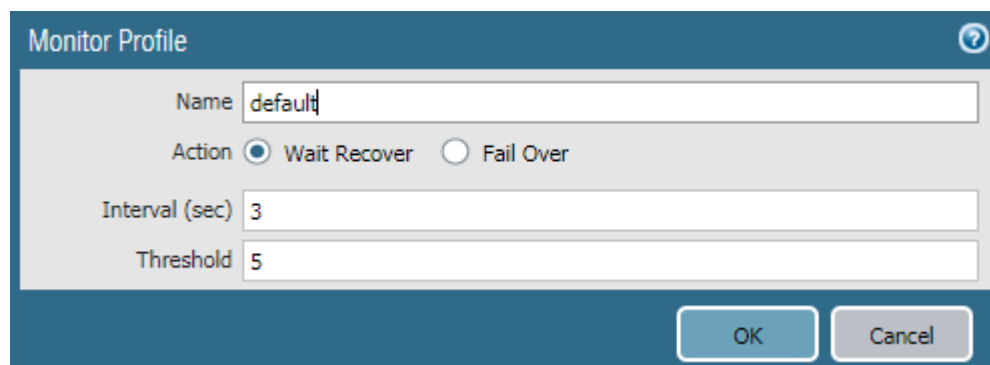
To provide uninterrupted VPN service, you can use the Dead Peer Detection capability along with the tunnel monitoring capability on the firewall. You can also monitor the status of the tunnel. These monitoring tasks are described in the following sections:

- Define a Tunnel Monitoring Profile

A tunnel monitoring profile allows you to verify connectivity between the VPN peers; you can configure the tunnel interface to ping a destination IP address at a specified interval and specify the action if the communication across the tunnel is broken.

- a. Select Network>Network Profiles>Monitor. A default tunnel monitoring profile is available for use.
- b. Click Add, and enter a Name for the profile.
- c. Select the Action to take if the destination IP address is unreachable.
 - Wait Recover—the firewall waits for the tunnel to recover. It continues to use the tunnel interface in routing decisions as if the tunnel were still active.
 - Fail Over—forces traffic to a back-up path if one is available. The firewall disables the tunnel interface, and thereby disables any routes in the routing table that use the interface.

In either case, the firewall attempts to accelerate the recovery by negotiating new IPsec keys.



The image shows a 'Monitor Profile' configuration window. It has a title bar with a question mark icon. Inside, there are four fields: 'Name' with the value 'default', 'Action' with radio buttons for 'Wait Recover' (selected) and 'Fail Over', 'Interval (sec)' with the value '3', and 'Threshold' with the value '5'. At the bottom right are 'OK' and 'Cancel' buttons.

Receive Time	Type	Severity	Event	Object	Description
05/27 16:06:02	vpn	informational	ike-nego-p1-fail-common	23.99.84.154[50...	IKE phase-1 negotiation is failed. Couldn't find configuration for IKE phase-1 request for peer IP 23.99.84.154[500].
05/27 16:05:10	vpn	informational	ikev2-nego-ike-succ	Azure-IKE2	IKEv2 IKE SA negotiation is succeeded as responder, non-rekey. Established SA: 209.37.97.9[500]-23.99.86.11[500] SPI:00dfebf80aac70f:a83615fe96f47e33 lifetime 28800 Sec.
05/27 16:05:10	vpn	informational	ikev2-nego-child-succ	Azure-IKE2	IKEv2 child SA negotiation is succeeded as responder, non-rekey. Established SA: 209.37.97.9[500]-23.99.86.11[500] message id:0x00000001, SPI:0x99713E05/0xA9F939AE.
05/27 16:05:10	vpn	informational	ipsec-key-install	Azure-IKE2	IPSec key installed. Installed SA: 209.37.97.9[500]-23.99.86.11[500] SPI:0x99713E05/0xA9F939AE lifetime 3600 Sec lifetize 106954752 KB.
05/27 16:05:10	vpn	informational	ikev2-nego-child-start	Azure-IKE2	IKEv2 child SA negotiation is started as responder, non-rekey. Initiated SA: 209.37.97.9[500]-23.99.86.11[500] message id:0x00000001

4.4 GlobalProtect User Authentication

The first time a GlobalProtect client connects to the portal, the user is prompted to authenticate to the portal. If authentication succeeds, the GlobalProtect portal sends the GlobalProtect configuration, which includes the list of gateways to which the agent can connect, and optionally a client certificate for connecting to the gateways. After successfully downloading and caching the configuration, the client attempts to connect to one of the gateways specified in the configuration. Because these components provide access to your network resources and settings, they also require the end user to authenticate.

The appropriate level of security required on the portal and gateways varies with the sensitivity of the resources that the gateway protects. GlobalProtect provides a flexible authentication framework that allows you to choose the authentication profile and certificate profile that are appropriate to each component.

4.4.1 Create interfaces and zones

1. Create tunnel Interface

Tunnel Interface

Interface Name: tunnel.2

Comment: Remote-VPN

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: RemoteVPN-Zone

OK Cancel

2. Create and new security zone and assign to the new tunnel interface. Make sure that user identification is enabled.

Zone

Name: RemoteVPN-Zone

Log Setting: None

Type: Layer3

Interfaces

- tunnel.2

+ Add - Delete

Zone Protection

Zone Protection Profile: None

☐ Enable Packet Buffer Protection

User Identification ACL

☒ Enable User Identification

Include List

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

+ Add - Delete

Users from these addresses/subnets will be identified.

Exclude List

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

+ Add - Delete

Users from these addresses/subnets will not be identified.

OK Cancel

3. Add security policy rule for known users.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

☐ Any

☐ Source Zone ▲

☐ RemoteVPN-Zone

☒ Any

☐ Source Address ▲

+ Add - Delete

+ Add - Delete

☐ Negate

OK Cancel

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

select ▼

☐ Destination Zone ▲

☐ Business_Zone

☒ Any

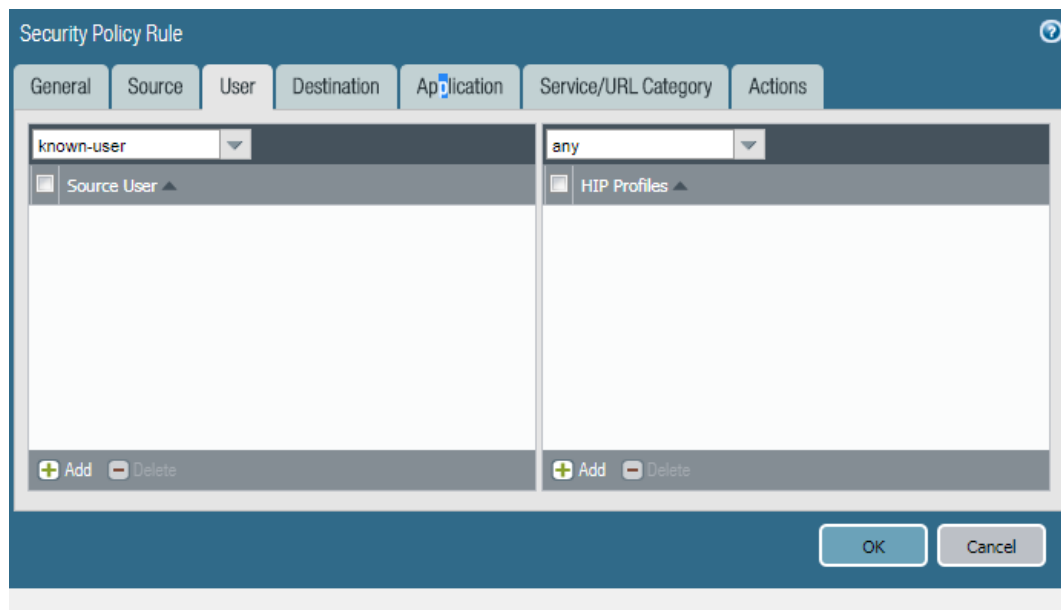
☐ Destination Address ▲

+ Add - Delete

+ Add - Delete

☐ Negate

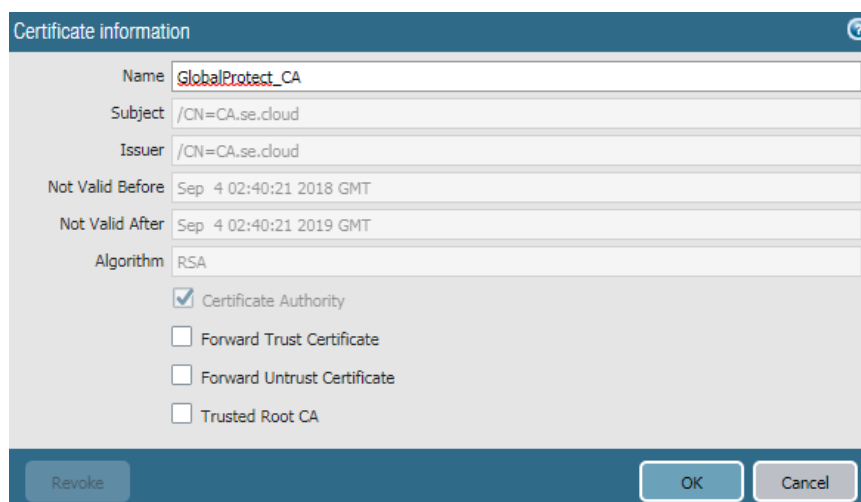
OK Cancel



The image shows the 'Security Policy Rule' configuration window. It has a tabbed interface with 'General', 'Source', 'User', 'Destination', 'Application', 'Service/URL Category', and 'Actions'. The 'Source' tab is selected. It contains two columns: 'Source User' and 'HIP Profiles'. The 'Source User' column has a dropdown menu set to 'known-user' and a list area below it. The 'HIP Profiles' column has a dropdown menu set to 'any' and a list area below it. Both list areas have '+ Add' and '- Delete' buttons at the bottom. The window also has 'OK' and 'Cancel' buttons at the bottom right.

4.4.2 Establish Trust

1. Create GlobalProtect certificate



The image shows the 'Certificate information' configuration window. It has a 'Name' field with the value 'GlobalProtect_CA'. Below it are fields for 'Subject' (value: /CN=CA.se.cloud), 'Issuer' (value: /CN=CA.se.cloud), 'Not Valid Before' (value: Sep 4 02:40:21 2018 GMT), and 'Not Valid After' (value: Sep 4 02:40:21 2019 GMT). The 'Algorithm' is set to 'RSA'. There are four checkboxes: 'Certificate Authority' (checked), 'Forward Trust Certificate' (unchecked), 'Forward Untrust Certificate' (unchecked), and 'Trusted Root CA' (unchecked). At the bottom, there are 'Revoke', 'OK', and 'Cancel' buttons.

2. Created gateway Certificate

Certificate information

Name: Gateway_Cert

Subject: /CN=172.16.1.4

Issuer: /CN=CA.se.cloud

Not Valid Before: Sep 4 02:40:52 2018 GMT

Not Valid After: Sep 4 02:40:52 2019 GMT

Algorithm: RSA

☐ Certificate Authority

☐ Forward Trust Certificate

☐ Forward Untrust Certificate

☐ Trusted Root CA

☐ Certificate for Secure Syslog

4.4.3 Authenticate the User

1. Create LDAP server Profile

LDAP Server Profile

Profile Name: AD-Server

☐ Administrator Use Only

Name	LDAP Server	Port
ad-business.se.cloud	10.1.0.4	389

[Add](#) [Delete](#)

Enter the IP address or FQDN of the LDAP server

Server Settings

Type: active-directory

Base DN: DC=se,DC=cloud

Bind DN: administrator@se.cloud

Password:

Confirm Password:

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

☐ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

[OK](#) [Cancel](#)

2. Create Authentication Profile

Authentication Profile

Name: AD-Users

Authentication **Factors** **Advanced**

Type: LDAP

Server Profile: AD-Server

Login Attribute:

Password Expiry Warning: 7

Number of days prior to warning a user about password expiry.

User Domain:

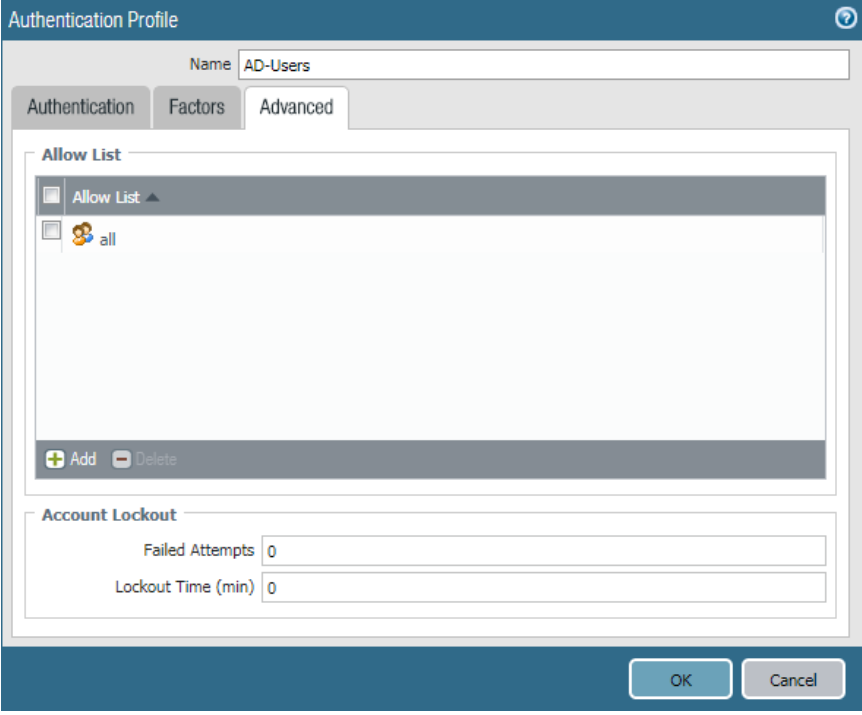
Username Modifier: %USERDOMAIN%\%USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field [X](#) [Import](#)

[OK](#) [Cancel](#)



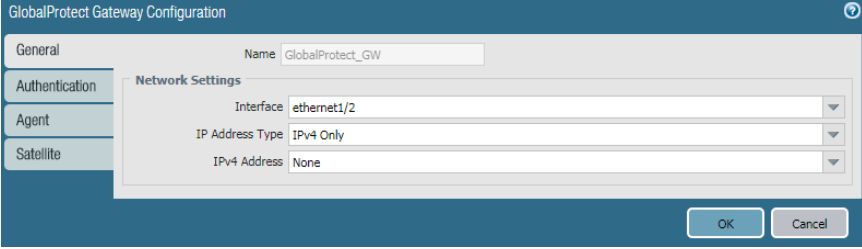
The **Authentication Profile** window for **AD-Users** is shown. It has three tabs: **Authentication**, **Factors**, and **Advanced**. The **Authentication** tab is active. It contains an **Allow List** section with a list box showing **all** and buttons for **Add** and **Delete**. Below this is an **Account Lockout** section with fields for **Failed Attempts** (0) and **Lockout Time (min)** (0). **OK** and **Cancel** buttons are at the bottom right.

3. Commit the configuration.

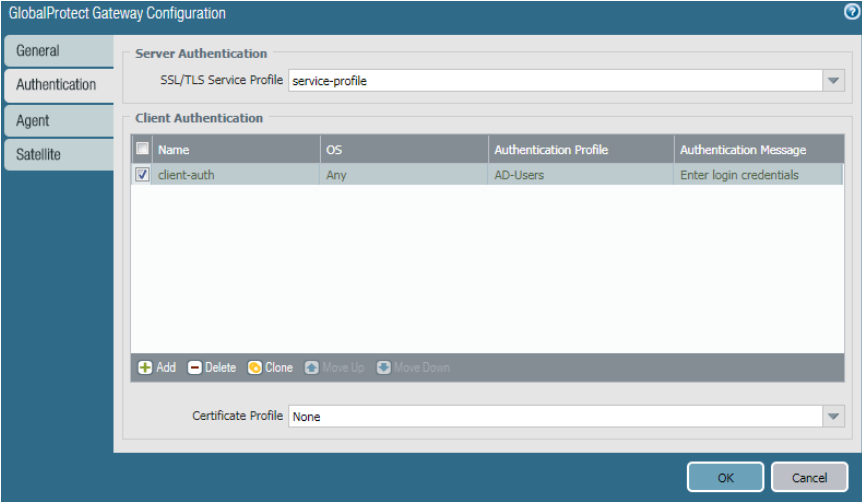
4.4.4 Configure the Gateway

1. GlobalProtect Gateway.

Network > GlobalProtect > Gateway and press add

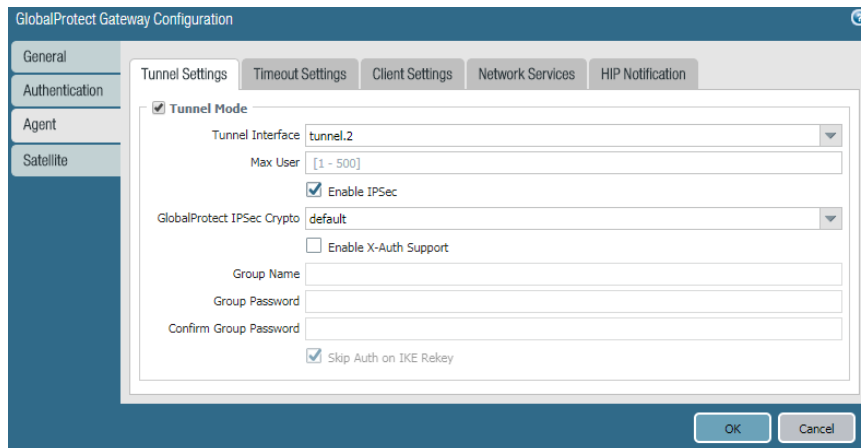


The **GlobalProtect Gateway Configuration** window, **General** tab, is shown. The **Name** is **GlobalProtect_GW**. The **Network Settings** section includes **Interface** (ethernet1/2), **IP Address Type** (IPv4 Only), and **IPv4 Address** (None). **OK** and **Cancel** buttons are at the bottom right.



The **GlobalProtect Gateway Configuration** window, **Authentication** tab, is shown. The **SSL/TLS Service Profile** is **service-profile**. The **Client Authentication** section contains a table with one entry: **client-auth** (checked), **Any** OS, **AD-Users** Authentication Profile, and **Enter login credentials** Authentication Message. Below the table are buttons for **Add**, **Delete**, **Clone**, **Move Up**, and **Move Down**. The **Certificate Profile** is **None**. **OK** and **Cancel** buttons are at the bottom right.

Name	OS	Authentication Profile	Authentication Message
<input checked="" type="checkbox"/> client-auth	Any	AD-Users	Enter login credentials



GlobalProtect Gateway Configuration

General
Authentication
Agent
Satellite

Tunnel Settings Timeout Settings Client Settings Network Services HIP Notification

☒ Tunnel Mode

Tunnel Interface: tunnel.2

Max User: [1 - 500]

☒ Enable IPSec

GlobalProtect IPSec Crypto: default

☐ Enable X-Auth Support

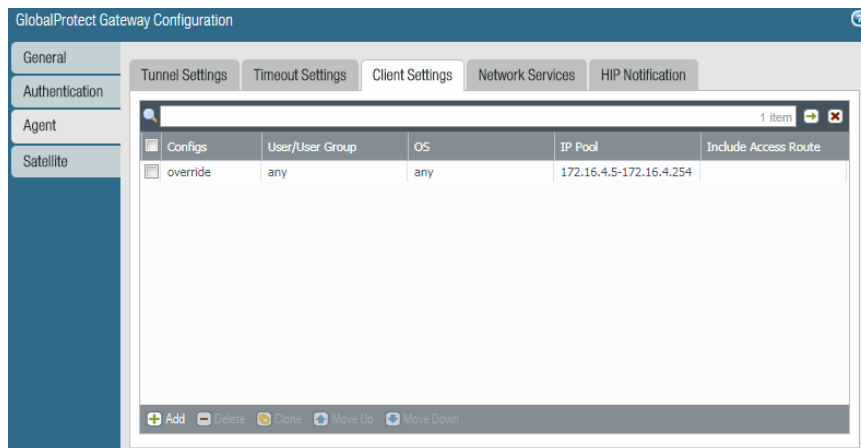
Group Name:

Group Password:

Confirm Group Password:

☒ Skip Auth on IKE Rekey

OK Cancel



GlobalProtect Gateway Configuration

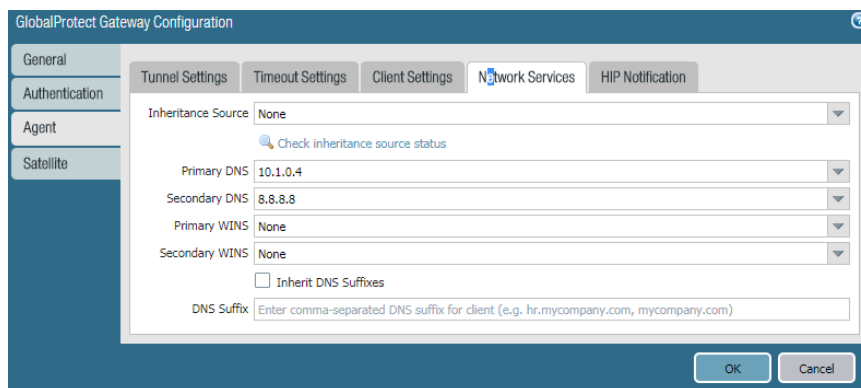
General
Authentication
Agent
Satellite

Tunnel Settings Timeout Settings Client Settings Network Services HIP Notification

1 item

Configs	User/User Group	OS	IP Pool	Include Access Route
<input checked="" type="checkbox"/> override	any	any	172.16.4.5-172.16.4.254	

+ Add - Delete Clone Move Up Move Down



GlobalProtect Gateway Configuration

General
Authentication
Agent
Satellite

Tunnel Settings Timeout Settings Client Settings Network Services HIP Notification

Inheritance Source: None

[Check inheritance source status](#)

Primary DNS: 10.1.0.4

Secondary DNS: 8.8.8.8

Primary WINS: None

Secondary WINS: None

☐ Inherit DNS Suffixes

DNS Suffix:

OK Cancel

4.4.5 Configure Portal

Network > GlobalProtect > Portal then press add

GlobalProtect Portal Configuration

General Name: AD-Portal

Authentication

Agent

Clientless VPN

Satellite

Network Settings

Interface: ethernet1/2

IP Address Type: IPv4 Only

IPv4 Address: 172.16.4.4/24

Appearance

Portal Login Page: None

Portal Landing Page: None

App Help Page: None

OK Cancel

GlobalProtect Portal Configuration

General

Authentication

Agent

Clientless VPN

Satellite

Server Authentication

SSL/TLS Service Profile: service-profile

Client Authentication

<input type="checkbox"/>	Name	OS	Authentication Profile	Authentication Message
<input type="checkbox"/>	user-auth	Any	AD-Users	Enter login credentials

+ Add - Delete Clone Move Up Move Down

Certificate Profile: None

OK Cancel

GlobalProtect Portal Configuration

General

Authentication

Agent

Clientless VPN

Satellite

Agent

<input type="checkbox"/>	Configs	User/User Group	OS	External Gateways	Client Certificate
<input checked="" type="checkbox"/>	AD-access	any	any	Gateway_Cert	

+ Add - Delete Clone Move Up Move Down

Trusted Root CA

	Install in Local Root Certificate Store
<input type="checkbox"/> GlobalProtect_CA	<input checked="" type="checkbox"/>

+ Add - Delete

Agent User Override Key: ****

Confirm Agent User Override Key: ****

OK Cancel

The screenshot shows the 'Configs' window with the 'Authentication' tab selected. The 'Name' field is set to 'AD-access'. The 'Client Certificate' dropdown is set to 'None'. Below it, a note states: 'The selected client certificate including its private key will be installed on client machines.' The 'Save User Credentials' dropdown is set to 'Yes'. The 'Authentication Override' section contains two unchecked checkboxes: 'Generate cookie for authentication override' and 'Accept cookie for authentication override'. Below these, the 'Cookie Lifetime' is set to 'Hours' with a value of '24'. The 'Certificate to Encrypt/Decrypt Cookie' dropdown is set to 'None'. The 'Components that Require Dynamic Passwords (Two-Factor Authentication)' section has four unchecked checkboxes: 'Portal', 'Internal gateways-all', 'External gateways-manual only', and 'External gateways-auto discovery'. A note at the bottom states: 'Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.' The 'OK' and 'Cancel' buttons are at the bottom right.

The screenshot shows the 'External Gateway' configuration window. The 'Name' field is set to 'Gateway_Cert'. The 'Address' section has 'FQDN' and 'IP' radio buttons, with 'IP' selected. The 'IPv4' field is set to '172.16.4.4' and the 'IPv6' field is empty. Below this is a table with the following data:

Source Region	Priority
Any	Highest

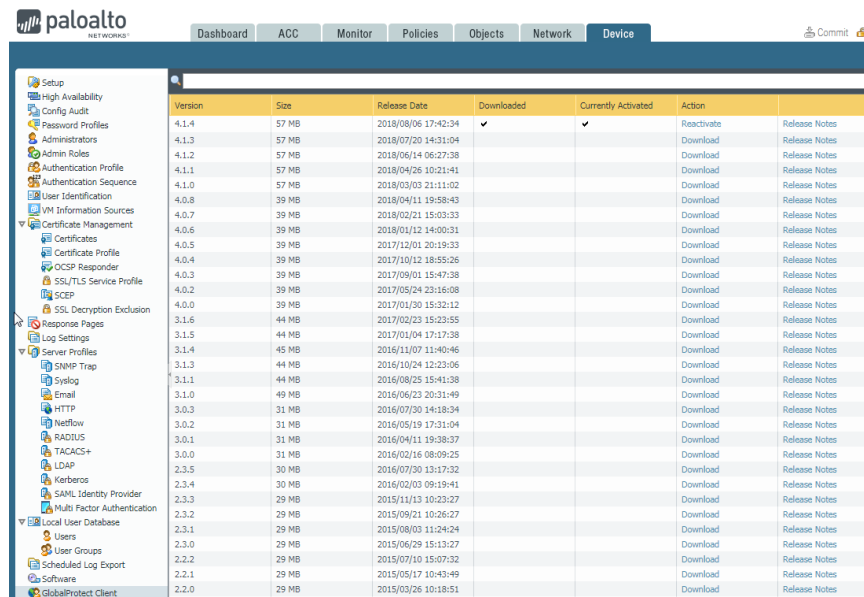
At the bottom, there is an 'Add' button, a 'Delete' button, and a checkbox labeled 'Manual (The user can manually select this gateway)'. The 'OK' and 'Cancel' buttons are at the bottom right.

Commit the configuration

4.4.6 Deploy GlobalProtect Agent

Device > GlobalProtect Client

Download the client then Activate

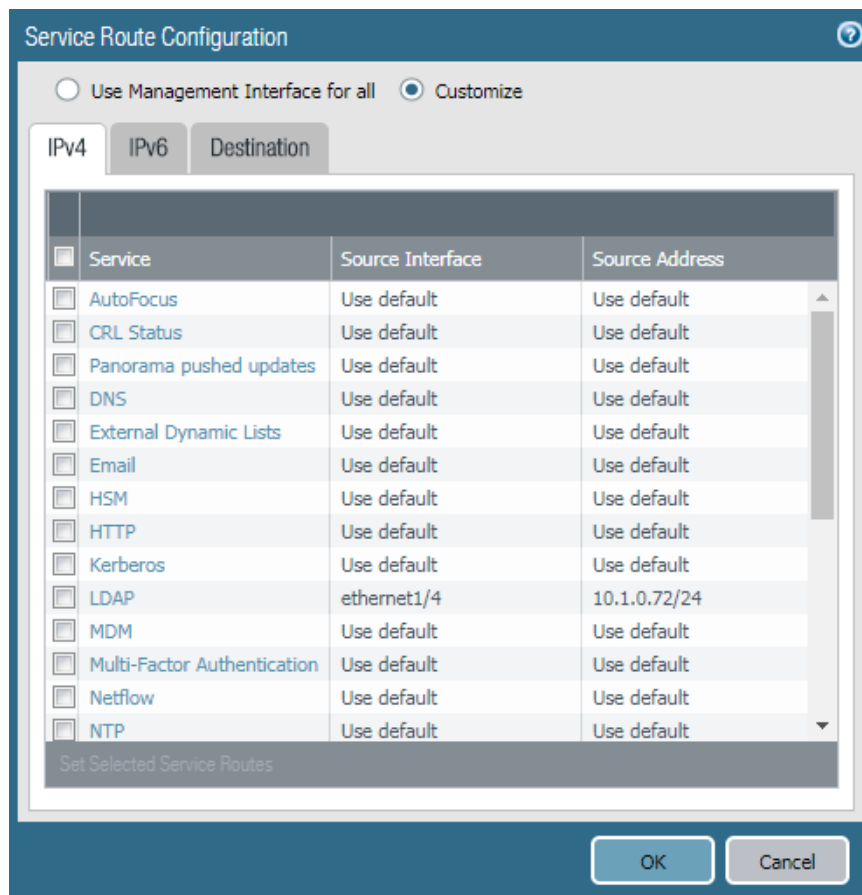


Version	Size	Release Date	Downloaded	Currently Activated	Action
4.1.4	57 MB	2018/08/06 17:42:34	✓	✓	Reactivate Release Notes
4.1.3	57 MB	2018/07/20 14:31:04			Download Release Notes
4.1.2	57 MB	2018/06/14 06:27:38			Download Release Notes
4.1.1	57 MB	2018/04/26 10:21:41			Download Release Notes
4.1.0	57 MB	2018/03/03 21:11:02			Download Release Notes
4.0.8	39 MB	2018/04/11 19:58:43			Download Release Notes
4.0.7	39 MB	2018/02/21 15:03:33			Download Release Notes
4.0.6	39 MB	2018/01/12 14:00:31			Download Release Notes
4.0.5	39 MB	2017/12/01 20:19:33			Download Release Notes
4.0.4	39 MB	2017/10/12 18:55:26			Download Release Notes
4.0.3	39 MB	2017/09/01 15:47:38			Download Release Notes
4.0.2	39 MB	2017/05/24 23:16:08			Download Release Notes
4.0.0	39 MB	2017/01/30 15:32:12			Download Release Notes
3.1.6	44 MB	2017/02/23 15:23:55			Download Release Notes
3.1.5	44 MB	2017/01/04 17:17:38			Download Release Notes
3.1.4	45 MB	2016/11/07 11:40:46			Download Release Notes
3.1.3	44 MB	2016/10/24 12:23:06			Download Release Notes
3.1.1	44 MB	2016/08/25 15:41:38			Download Release Notes
3.1.0	49 MB	2016/04/23 20:31:49			Download Release Notes
3.0.3	31 MB	2016/07/30 14:18:34			Download Release Notes
3.0.2	31 MB	2016/05/19 17:31:04			Download Release Notes
3.0.1	31 MB	2016/04/11 19:38:37			Download Release Notes
3.0.0	31 MB	2016/02/16 08:09:25			Download Release Notes
2.3.5	30 MB	2016/07/30 13:17:32			Download Release Notes
2.3.4	30 MB	2016/02/03 09:19:41			Download Release Notes
2.3.3	29 MB	2015/11/13 10:23:27			Download Release Notes
2.3.2	29 MB	2015/09/21 10:26:27			Download Release Notes
2.3.1	29 MB	2015/08/03 11:24:24			Download Release Notes
2.3.0	29 MB	2015/06/29 15:13:27			Download Release Notes
2.2.2	29 MB	2015/07/10 15:07:32			Download Release Notes
2.2.1	29 MB	2015/05/17 10:43:49			Download Release Notes
2.2.0	29 MB	2015/03/26 10:18:51			Download Release Notes

4.4.7 Service Route Configuration

Change the service route configuration for LDAP service and make the source address the Untrust Interface IP

Device > Setup > Service Route Configuration



Service Route Configuration

☐ Use Management Interface for all
 ☒ Customize

☒ IPv4
 ☐ IPv6
 ☐ Destination

Service	Source Interface	Source Address
<input type="checkbox"/> AutoFocus	Use default	Use default
<input type="checkbox"/> CRL Status	Use default	Use default
<input type="checkbox"/> Panorama pushed updates	Use default	Use default
<input type="checkbox"/> DNS	Use default	Use default
<input type="checkbox"/> External Dynamic Lists	Use default	Use default
<input type="checkbox"/> Email	Use default	Use default
<input type="checkbox"/> HSM	Use default	Use default
<input type="checkbox"/> HTTP	Use default	Use default
<input type="checkbox"/> Kerberos	Use default	Use default
<input type="checkbox"/> LDAP	ethernet1/4	10.1.0.72/24
<input type="checkbox"/> MDM	Use default	Use default
<input type="checkbox"/> Multi-Factor Authentication	Use default	Use default
<input type="checkbox"/> Netflow	Use default	Use default
<input type="checkbox"/> NTP	Use default	Use default

Set Selected Service Routes

OK Cancel