Securing work.

Menlo Security / Palo Alto Networks Next-Generation Firewall Configuration Guide

Applies to:
Menlo Cloud Security Platform Version: 2.87
Palo Alto Networks NGFW PAN-OS 10.2.3
Date Updated: January 25, 2023

Revision History

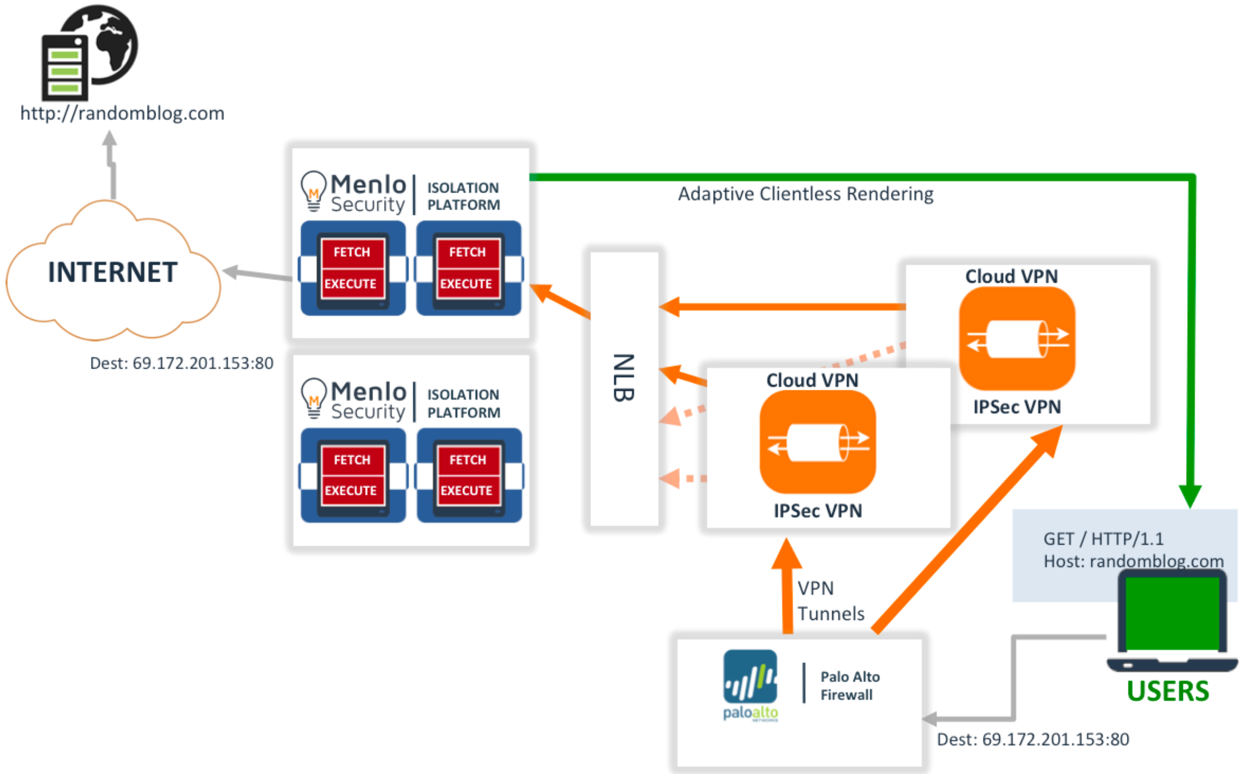
Release	Date	Change
1.0	January 25, 2023	Initial Release

Menlo Security / Palo Alto Networks Next-Generation Firewall Configuration Guide

Note: Please contact your Menlo Security account team to request support for this feature.

Overview / Purpose of Feature

Menlo Security continuously adds new cloud data centers, or Menlo Cloud Security Platform regions, to various global locations. This document describes the IPSec VPN and policy-based forwarding configuration required to transparently steer traffic for isolation when using Palo Alto Networks Next-Generation Firewall with the Menlo Security Isolation Platform.



Integration Architecture Diagram

Prerequisites

- Palo Alto Networks Next-Generation Firewall running a PAN-OS version currently supported by Palo Alto Networks Networks
- Provide Palo Alto Networks Next-Generation Firewall external IP address to Menlo Security Support for IPSec configuration

- Receive IPSec parameters from Menlo Security Support for Primary and Secondary tunnels:
  - Menlo Security VPN Gateway IP Addresses
  - Menlo Security VPN Pre-shared Key Strings
  - IPSec Peer Identifiers

Palo Alto Networks Next-Generation Firewall Configuration

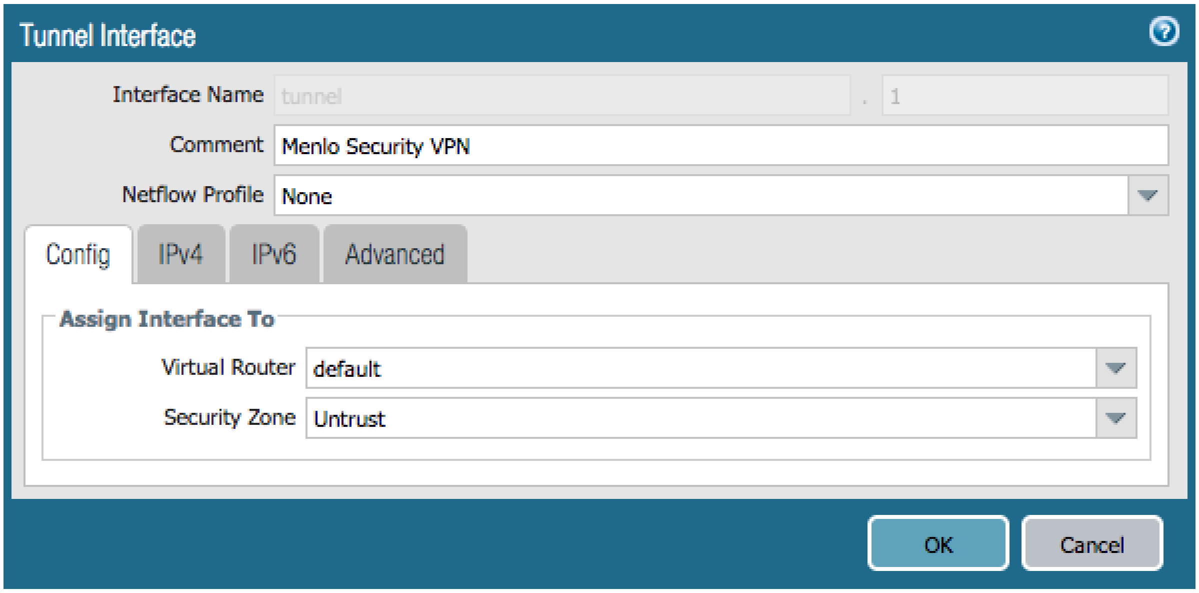
Add VPN Zone for Next-Generation Firewall Policy

Optionally, a new VPN zone can be defined for use in Next-Generation Firewall policy if a distinct policy will be used for the VPN zone. Zones can be managed in Network > Zones and should be created as a Layer 3 Zone. Otherwise a standard Untrust zone can be used.

Add Tunnel Interfaces

Network > Interfaces: Tunnel Interface

Configure tunnel interfaces to be used for the VPN, on the preferred VR and zone.
Add two interfaces: one for each Menlo VPN tunnel. The Palo Alto Networks Next-Generation Firewall requires an IP address to be assigned to the tunnel interface to enable routing. The address can be configured in the IPv4 tab. Any IP available address can be used, and it is not dependent on the IPSec parameters.


Tunnel Interface

Interface Name: tunnel . 1

Comment: Menlo Security VPN

Netflow Profile: None

Assign Interface To

Virtual Router: default

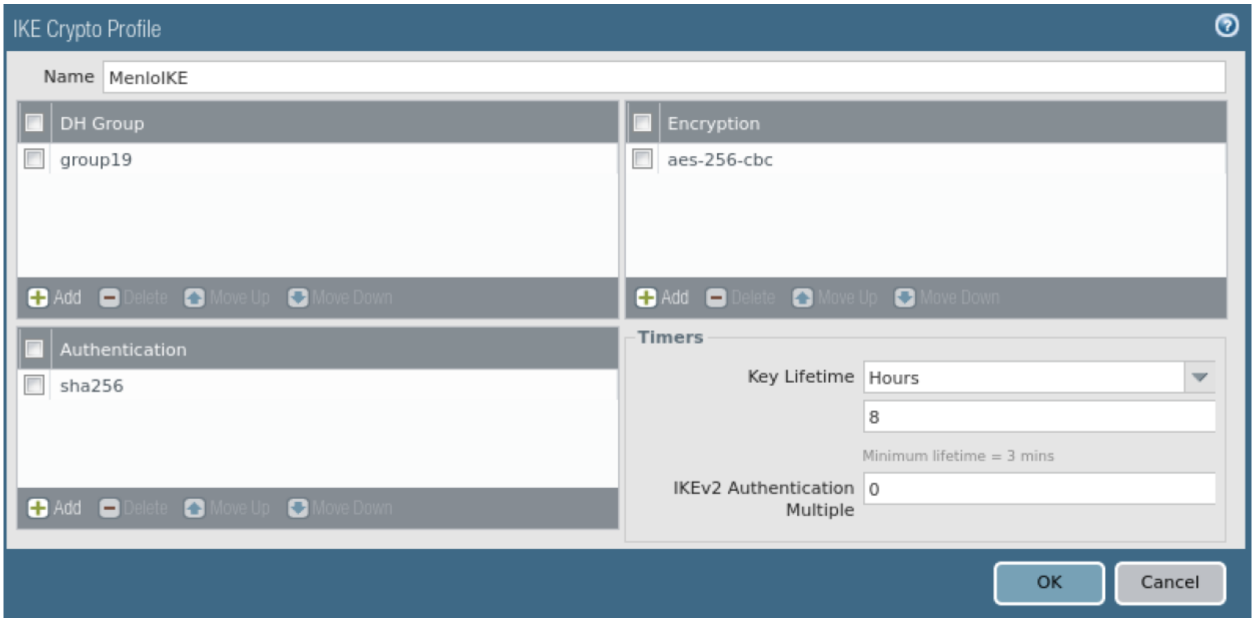
Security Zone: Untrust

Configure IPSec / IKE Parameters

Network > IKE Crypto

Supported values:

- **DH Group**: group19
- **Authentication**: sha1, sha256
- **Encryption**: aes-128-cbc, aes-256-cbc



IKE Crypto Profile

Name MenloIKE

DH Group: group19

Encryption: aes-256-cbc

Authentication: sha256

Timers

Key Lifetime Hours

8

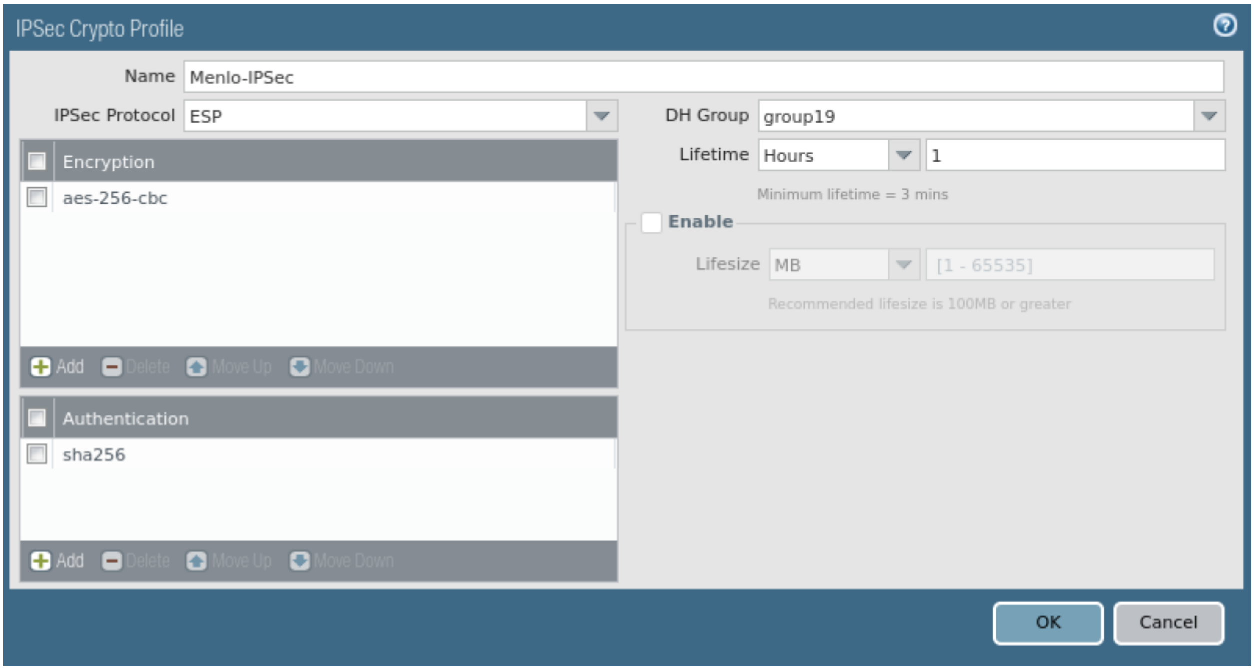
Minimum lifetime = 3 mins

IKEv2 Authentication Multiple 0

Network > IPSec Crypto

Supported values:

- **Encryption**: aes-128-cbc, aes-256-cbc
- **Authentication**: sha1, sha256
- **DH Group**: group19
- **Lifetime**: 1 Hour



IPSec Crypto Profile

Name: Menlo-IPSec

IPSec Protocol: ESP

DH Group: group19

Lifetime: Hours 1

Minimum lifetime = 3 mins

□ Enable

Lifesize: MB [1 - 65535]

Recommended lifesize is 100MB or greater

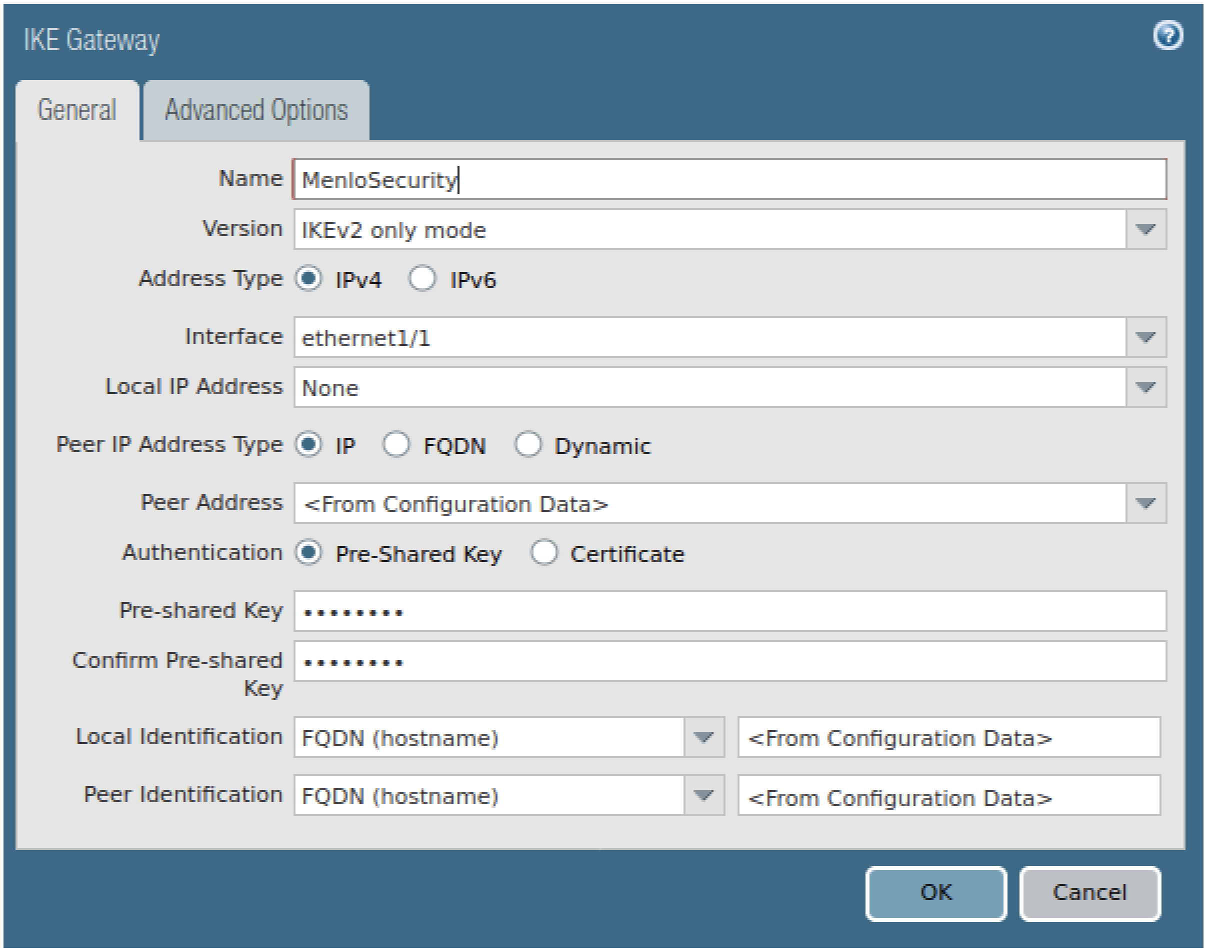
□ Encryption
□ aes-256-cbc

□ Authentication
□ sha256

Network > IKE Gateways

Details of the Menlo Security VPN:

- IKEv2 only mode
- **Peer IP Address Type**: IP
- **Peer IP Address**: <See Menlo Security Configuration Data>
- **Authentication**: Pre-Shared Key
- **Pre-shared Key value**: <See Menlo Security Configuration Data>
- **Local Identifier: FQDN**: Customer identifier FQDN: <See Menlo Security Configuration Data>
- **Peer Identifier: FQDN**: <See Menlo Security Configuration Data>



Name: MenloSecurity

Version: IKEv2 only mode

Address Type: ● IPv4 ○ IPv6

Interface: ethernet1/1

Local IP Address: None

Peer IP Address Type: ● IP ○ FQDN ○ Dynamic

Peer Address: <From Configuration Data>

Authentication: ● Pre-Shared Key ○ Certificate

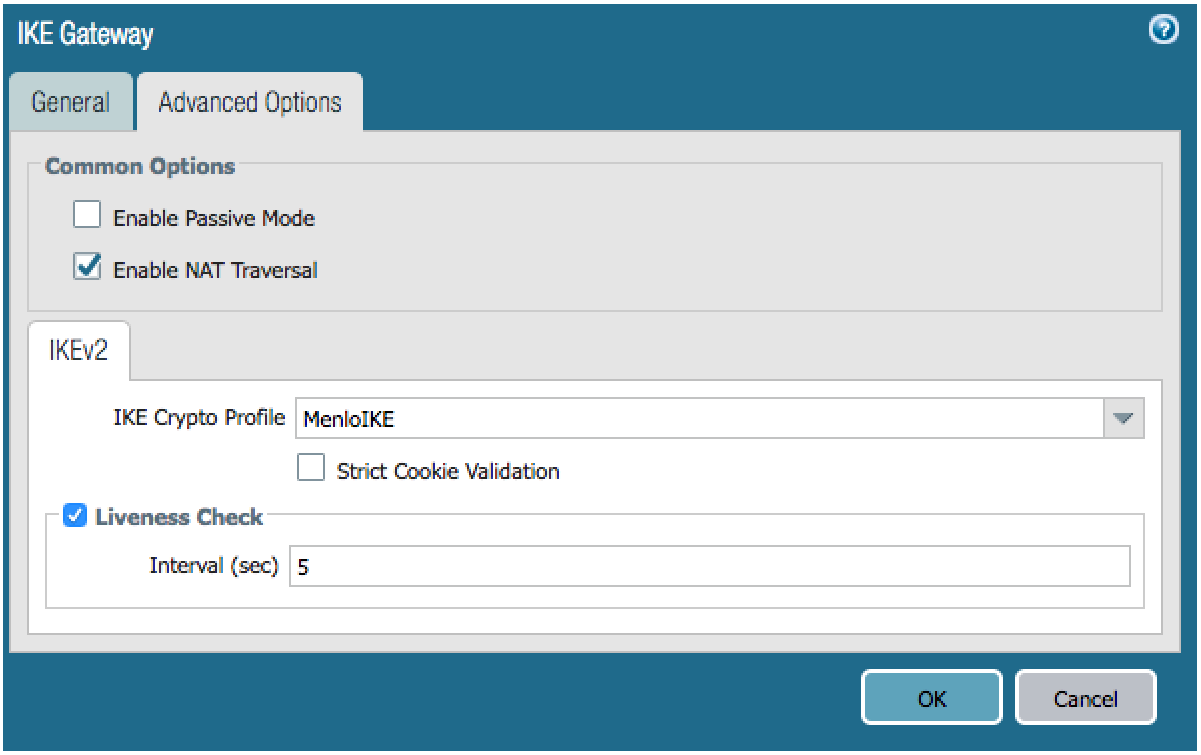
Pre-shared Key: ••••••••

Confirm Pre-shared Key: ••••••••

Local Identification: FQDN (hostname) <From Configuration Data>

Peer Identification: FQDN (hostname) <From Configuration Data>

Advanced Options:



IKE Gateway

General | Advanced Options

Common Options

□ Enable Passive Mode

☑ Enable NAT Traversal

IKEv2

IKE Crypto Profile: MenloIKE

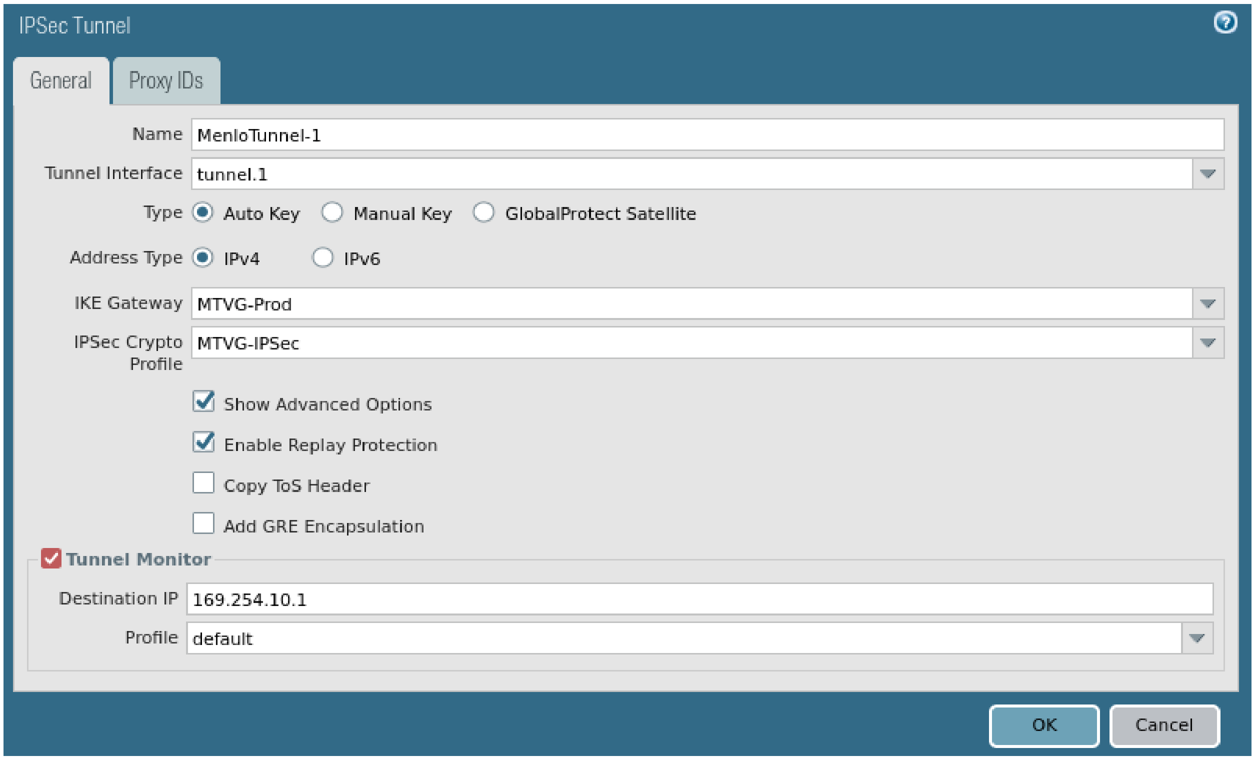
□ Strict Cookie Validation

☑ Liveness Check

Interval (sec): 5

Network > IPSec Tunnels

The tunnel configuration combines the previously defined objects into the VPN tunnel configurations. Configure two tunnels: one for each Menlo Security VPN node.



IPSec Tunnel

Name	MenloTunnel-1
Tunnel Interface	tunnel.1
Type	● Auto Key ○ Manual Key ○ GlobalProtect Satellite
Address Type	● IPv4 ○ IPv6
IKE Gateway	MTVG-Prod
IPSec Crypto Profile	MTVG-IPSec

☑ Show Advanced Options

☑ Enable Replay Protection

□ Copy ToS Header

□ Add GRE Encapsulation

☑ Tunnel Monitor

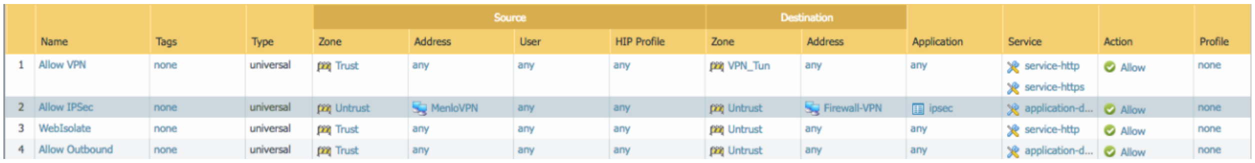
Destination IP	169.254.10.1
Profile	default

- **Tunnel Monitoring**: Tunnel monitoring passes ICMP requests through the tunnel to verify the tunnel is operational and brings the tunnel up once it is fully configured, allowing simple validation of tunnel status.
- **Tunnel Monitor Destination IP**: 169.254.10.1
  (**Note that any address in the 169.254.0.0/16 range can be used for tunnel monitoring.**)

Next-Generation Firewall Policy

The existing Next-Generation Firewall policy must be updated to allow IPSec setup and HTTP/HTTPS connections to the VPN

- Policy to allow Web access to VPN Zone
- Policy to allow Encapsulated IPSec and IKE requests
  - **Ipsec-esp-udp**: UDP/4500
  - **Ike**: UDP/500



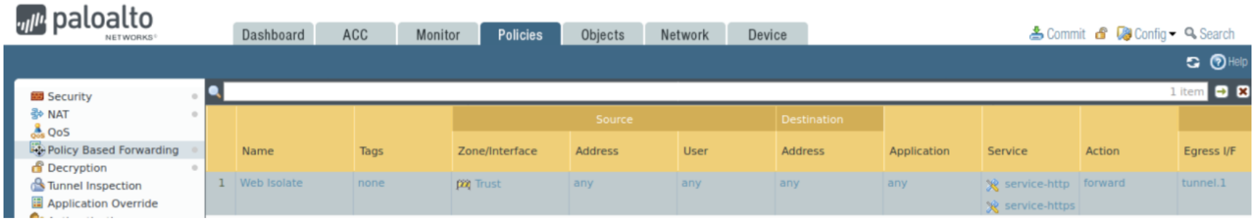
				Source				Destination					
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	Allow VPN	none	universal	Trust	any	any	any	VPN_Tun	any	any	service-http service-https	Allow	none
2	Allow IPSec	none	universal	Untrust	MenloVPN	any	any	Untrust	Firewall-VPN	ipsec	application-d...	Allow	none
3	WebIsolate	none	universal	Trust	any	any	any	Untrust	any	any	service-http	Allow	none
4	Allow Outbound	none	universal	Trust	any	any	any	Untrust	any	any	application-d...	Allow	none

Policy-Based Forwarding (PBF)

PBF allows us to choose which traffic is forwarded to Menlo Security. The session routing decision is made when the initial packet of this session is seen. Routing decisions can be made on any IP header (source IP, Dest IP, Service) or user-name (if available).

When initially configuring the integration, it is recommended to define a single source IP to be routed to the VPN tunnel for validation. Once validated, expand the matched source IP addresses to expand the group of isolated users.

- **Source**: User Names or IP Address range of users to be isolated
- **Services**: HTTP + HTTPS
- **Egress I/F**: VPN Tunnel



			Source			Destination				
	Name	Tags	Zone/Interface	Address	User	Address	Application	Service	Action	Egress I/F
1	Web Isolate	none	Trust	any	any	any	any	service-http service-https	forward	tunnel.1

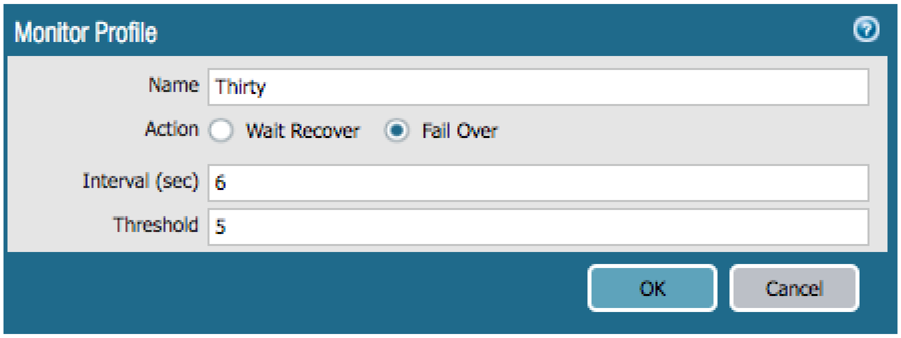
Note: Previous integrations required routing Menlo Security requests outside the VPN tunnel. This is no longer required and it is recommended to route menlosecurity.com requests via the tunnel to better manage service upgrades.

Note: If using SAML authentication, the SAML destinations should either be configured to bypass the IPSec tunnel, or be added as an SSL Exemption in the Menlo policy. This prevents an ‘authentication loop’ where authentication is required to connect to the authentication server.

High Availability and PBF Monitoring

For fault tolerance and availability during service upgrades, the configuration includes two IPSec tunnels and a PBF monitor configuration to disable the PBF rule when the tunnel is unavailable. In this case, the connections will use the second PBF rule and route traffic to the standby tunnel.

In Network > Monitor, add a **Monitor Profile** to control the polling configuration used in PBF monitoring.



Monitor Profile

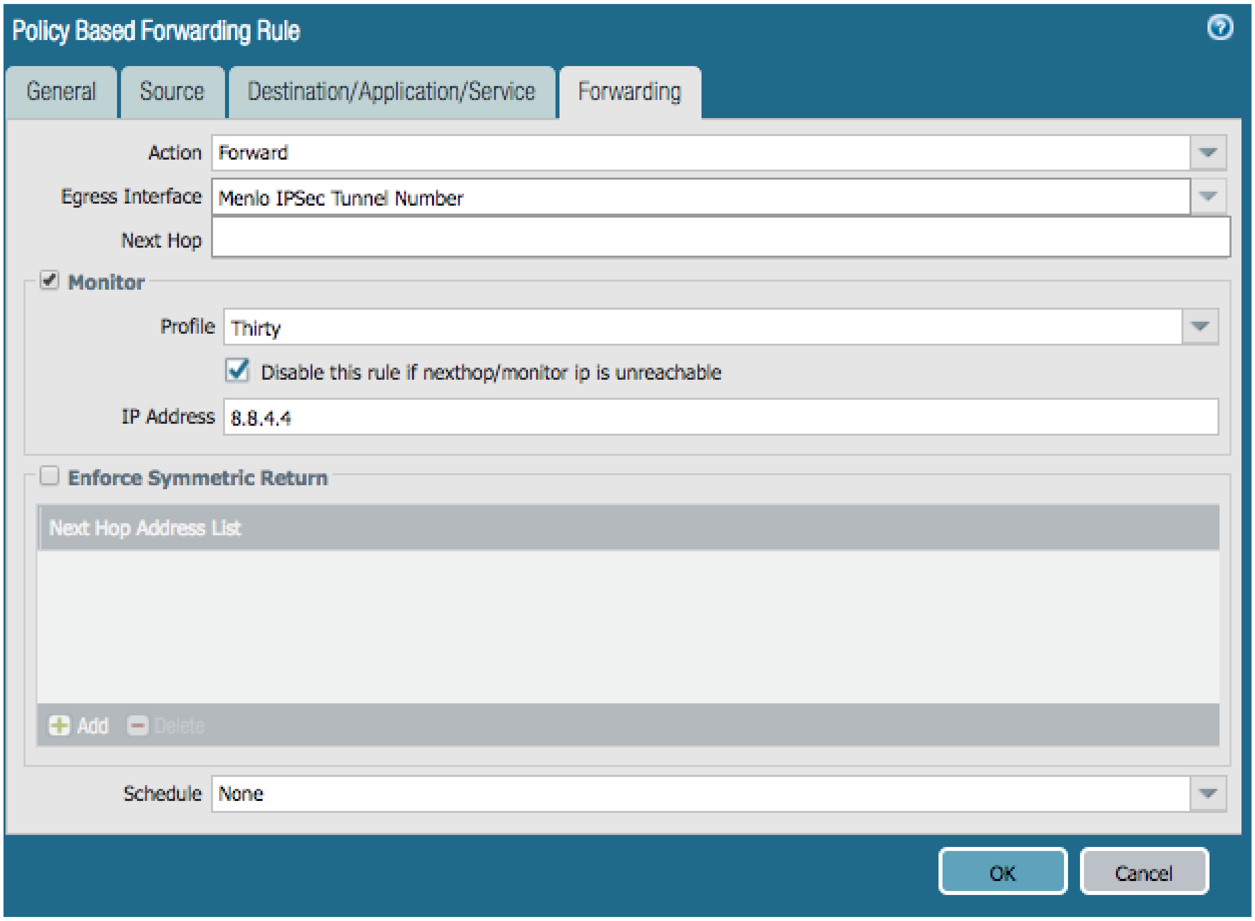
Name: Thirty

Action: ○ Wait Recover ● Fail Over

Interval (sec): 6

Threshold: 5

In the Policy Based Forwarding rule, enable the **Monitor** and select the profile defined above.



Policy Based Forwarding Rule

Action: Forward

Egress Interface: Menlo IPSec Tunnel Number

Next Hop:

☑ Monitor

Profile: Thirty

☑ Disable this rule if nexthop/monitor ip is unreachable

IP Address: 8.8.4.4

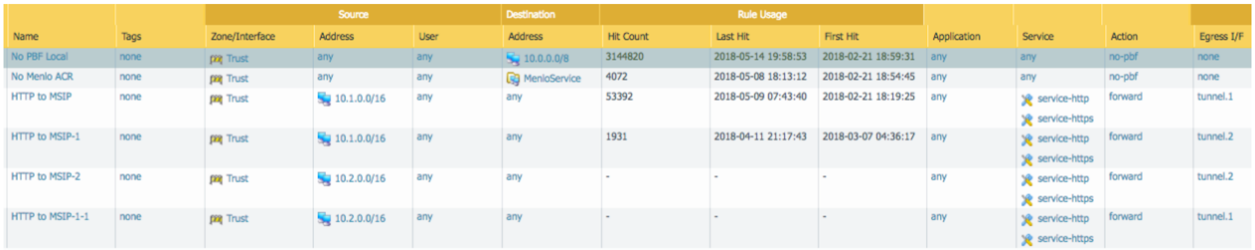
□ Enforce Symmetric Return

Next Hop Address List

Schedule: None

Load Distribution (Optional)

To distribute sessions across both Menlo Security VPN nodes, the policy based forwarding rules can be structured to send a subset of traffic to each VPN tunnel. If a load balancing configuration is used, the monitoring configuration must also be structured to use the secondary tunnel if the primary is unavailable.



		Source			Destination	Rule Usage						
Name	Tags	Zone/Interface	Address	User	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Egress I/F
No PBF Local	none	Trust	any	any	10.0.0.0/8	3144820	2018-05-14 19:58:53	2018-02-21 18:59:31	any	any	no-pbf	none
No Menlo ACR	none	Trust	any	any	MenloService	4072	2018-05-08 18:13:12	2018-02-21 18:54:45	any	any	no-pbf	none
HTTP to MSIP	none	Trust	10.1.0.0/16	any	any	53392	2018-05-09 07:43:40	2018-02-21 18:19:25	any	service-http service-https	forward	tunnel.1
HTTP to MSIP-1	none	Trust	10.1.0.0/16	any	any	1931	2018-04-11 21:17:43	2018-03-07 04:36:17	any	service-http service-https	forward	tunnel.2
HTTP to MSIP-2	none	Trust	10.2.0.0/16	any	any	-	-	-	any	service-http service-https	forward	tunnel.2
HTTP to MSIP-1-1	none	Trust	10.2.0.0/16	any	any	-	-	-	any	service-http service-https	forward	tunnel.1

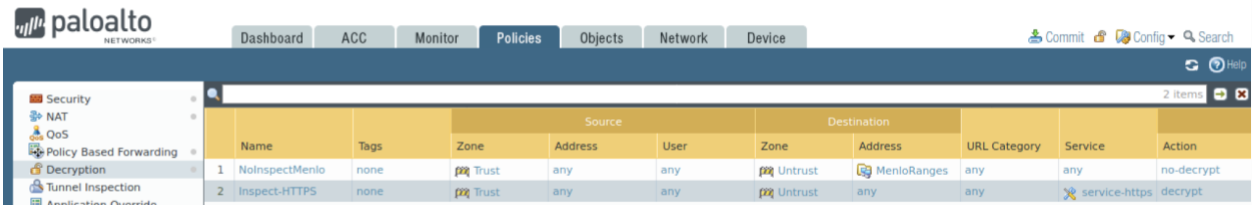
In the illustration above, two user subnets are forwarded separately, each using a different tunnel as its primary.

Menlo Security Address Objects

To minimize TLS decryption overhead, the Menlo ACR isolation HTTPS traffic can be configured to bypass decryption using the Menlo Security service addresses. The addresses are available in this knowledge base entry in CLI syntax which can be pasted into the device configuration CLI to simplify object and group definition. The current list of Menlo Security address ranges is also available in the 'installation prerequisites' section of the product documentation.

The address group is used in the policy based forwarding rules as 'no-decrypt' so it is not decrypted.

Please Note: This policy bypasses decryption of only the Menlo ACR rendering operations, which do not contain any data which an inspection device can understand. Any 'inspectable' events, such as file uploads or downloads, are processed via different IP ranges and are not bypassed from decryption.



			Source			Destination				
	Name	Tags	Zone	Address	User	Zone	Address	URL Category	Service	Action
1	NoInspectMenlo	none	Trust	any	any	Untrust	MenloRanges	any	any	no-decrypt
2	Inspect-HTTPS	none	Trust	any	any	Untrust	any	any	service-https	decrypt

Backend Configuration (Menlo Internal Only)

IPSec Config in Service Portal

In the legacy VPN nodes, the IPSec configuration was hard coded as part of the node type and tenant parameters were passed via AMI Config metadata.

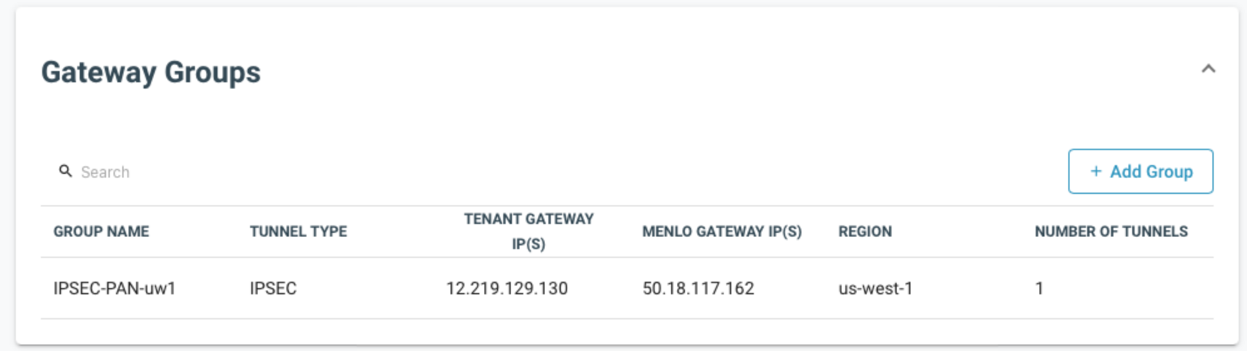
In the new ‘Multi-Tenant VPN Gateway’, this configuration is done within the service portal.

The settings described here have been captured as a “Palo Alto Networks Next-Generation Firewall” configuration profile, so most of the settings will not require manual configuration. This page documents those underlying settings.

In a production environment, we always allocate two VPN tunnels per customer peer GW for HA purposes. Both gateways must be added when the Gateway Group is created to support distribution of gateways across availability zones.

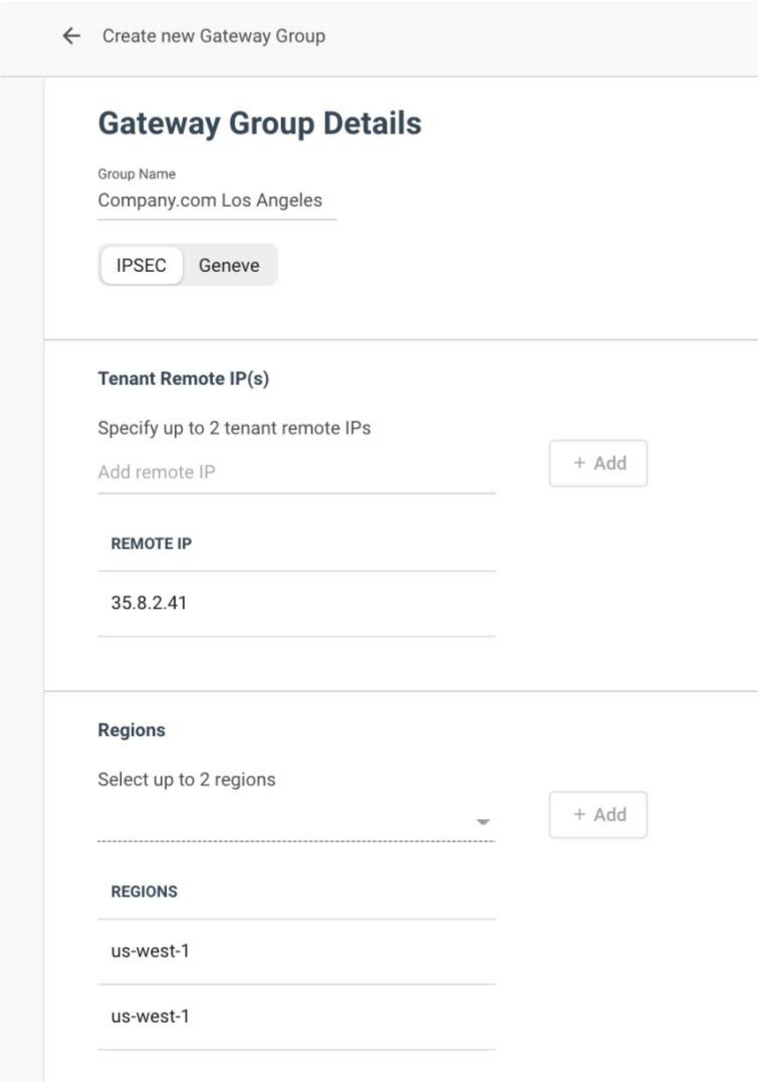
In Service Portal tenant settings:

VPN > Add Gateway Group



GROUP NAME	TUNNEL TYPE	TENANT GATEWAY IP(S)	MENLO GATEWAY IP(S)	REGION	NUMBER OF TUNNELS
IPSEC-PAN-uw1	IPSEC	12.219.129.130	50.18.117.162	us-west-1	1

Create Gateway Group



Create new Gateway Group

Gateway Group Details

Group Name: Company.com Los Angeles

IPSEC Geneve

Tenant Remote IP(s)

Specify up to 2 tenant remote IPs

Add remote IP

+ Add

REMOTE IP
35.8.2.41

Regions

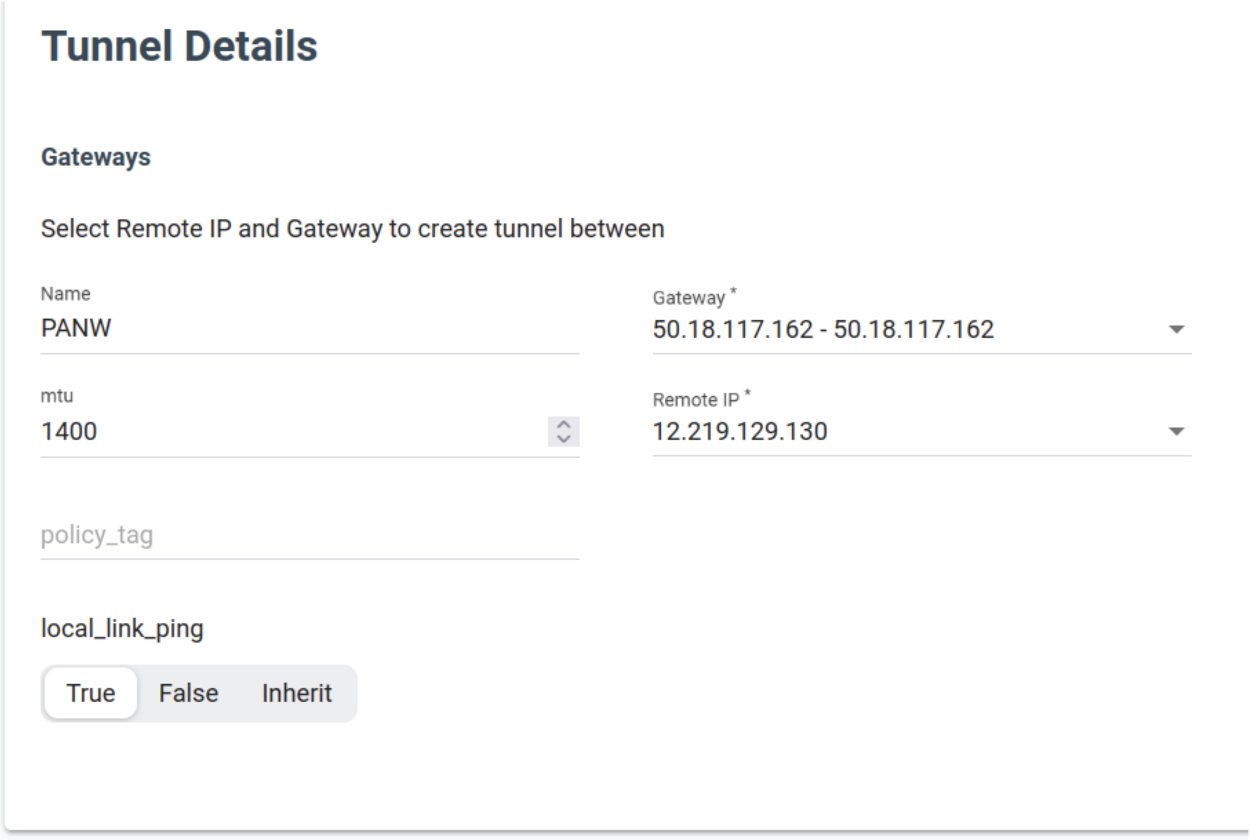
Select up to 2 regions

+ Add

REGIONS
us-west-1
us-west-1

- **Group Name**: This is a string name and should capture customer location or use case for future reference.
- **Tenant Remote IP**: This is the IP Address we see as the customer IPSec gateway. Note that this is currently mandatory. We need the customer IP prior to configuring a gateway and tunnel. In the future, this will be optional and editable.
- **Region** = AWS region to use for tunnel provisioning. The gateway will be assigned from available resources in that region and will be available in the tunnel configuration. **When creating a Gateway Group, add two gateways in the required region.** This will assign gateways within each availability zone, which is needed for fault tolerance and management of the Menlo gateway upgrade process.

VPN > Gateway Groups > Tunnel



Tunnel Details

Gateways

Select Remote IP and Gateway to create tunnel between

Name: PANW

Gateway *: 50.18.117.162 - 50.18.117.162

mtu: 1400

Remote IP *: 12.219.129.130

policy_tag

local_link_ping

[✓ True] False Inherit

Select the gateway from the list of gateways in the service portal.

- **Remote IP**: Customer's external IP address. Input this in the Gateway Group's configuration.
- **local_link_ping**: Enable 'local_link_ping', which allows the VPN gateway to respond to pings to 169.254.* addresses.
- **mtu**: Set MTU to 1400.

IKE Settings

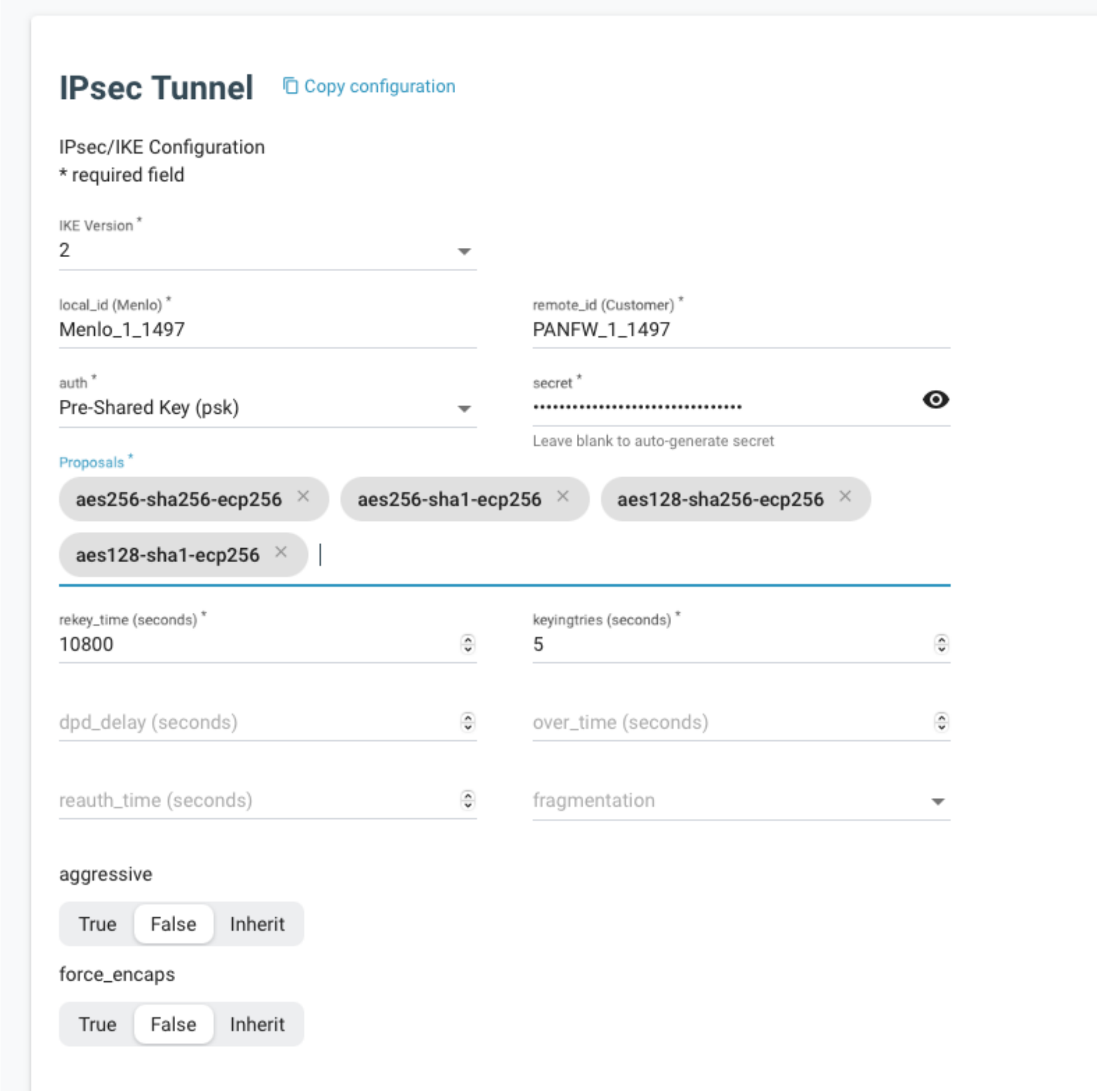
The following settings are to be provided to the customer.

# = gateway number (1 or 2 for the redundant VPN tunnels)
tid = tenant id

- **Menlo Gateway IP Address**
- **local_id** (Menlo Side): String Value: Menlo_#_tid
- **remote_id** (Customer Side): String Value: PANFW_#_tid
- **Pre-Shared-Key:** Service Portal will automatically generate when the tunnel is saved.

Note that the local and remote Peer IDs should be defined as FQDN String values, not the IP addresses of the endpoints. Using unique string names allow multiple tunnels to be provisioned behind a single peer IP address.

Proposals: The default set correlates with PANFW config, allowing AES128 or AES 256 and SHA1 or SHA256 and Diffie Hellman Group 19 (256 bit elliptic curve).



IPsec Tunnel

Copy configuration

IPsec/IKE Configuration
* required field

IKE Version * 2

local_id (Menlo) * Menlo_1_1497

remote_id (Customer) * PANFW_1_1497

auth * Pre-Shared Key (psk)

secret * ••••••••••••••••••••••••••••••••

Leave blank to auto-generate secret

Proposals * aes256-sha256-ecp256 ×, aes256-sha1-ecp256 ×, aes128-sha256-ecp256 ×, aes128-sha1-ecp256 ×

rekey_time (seconds) * 10800

keyingtries (seconds) * 5

dpd_delay (seconds)

over_time (seconds)

reauth_time (seconds)

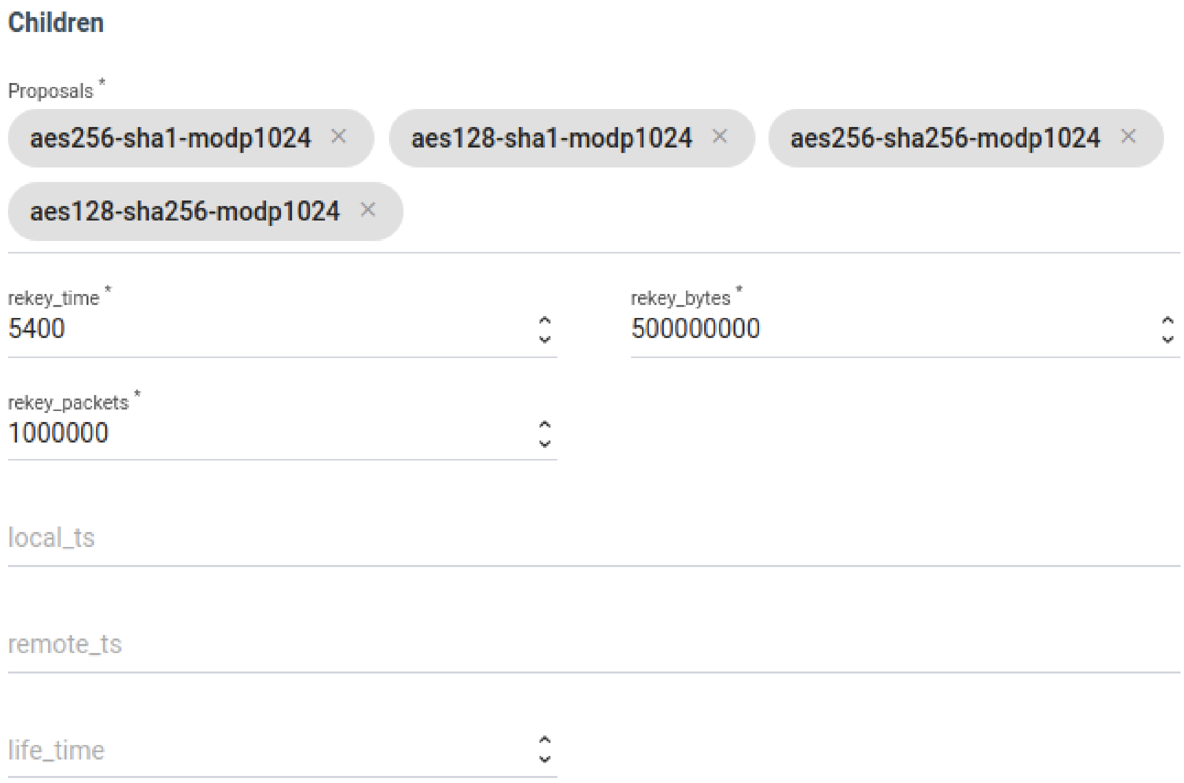
fragmentation

aggressive: True [✓ False] Inherit

force_encaps: True [✓ False] Inherit

IPSec Settings

The following defaults also support AES 128/256, SHA1/256, and DH Group 19.



Children

Proposals *

aes256-sha1-modp1024 ×

aes128-sha1-modp1024 ×

aes256-sha256-modp1024 ×

aes128-sha256-modp1024 ×

rekey_time *
5400

rekey_bytes *
500000000

rekey_packets *
1000000

local_ts

remote_ts

life_time