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

Menlo Security / Palo Alto Networks Next-Generation Firewall Configuration Guide
Overview / Purpose of Feature 3
Prerequisites 3
Palo Alto Networks Next-Generation Firewall Configuration 4
Add VPN Zone for Next-Generation Firewall Policy 4
Add Tunnel Interfaces 4
Configure IPSec / IKE Parameters 5
Network > IKE Crypto 5
Network > IPSec Crypto 5
Network > IKE Gateways 6
Network > IPSec Tunnels 8
Next-Generation Firewall Policy 9
Policy-Based Forwarding (PBF) 10
High Availability and PBF Monitoring 10
Load Distribution (Optional) 11
Menlo Security Address Objects 12

Backend Configuration (Menlo Internal Only) 13
IPSec Config in Service Portal 13
Create Gateway Group 14
IKE Settings 15
IPSec Settings 17
## Revision History

<table>
<thead>
<tr>
<th>Release</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>January 25, 2023</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>
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.

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.
Configure IPSec / IKE Parameters

Network > IKE Crypto

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

Network > IPSec Crypto

Supported values:
- **Encryption**: aes-128-cbc, aes-256-cbc
- **Authentication**: sha1, sha256
- **DH Group**: group19
- **Lifetime**: 1 Hour
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>
IKE Gateway

**General**

- **Name**: MenloSecurity
- **Version**: IKEv2 only mode
- **Address Type**: IPv4
- **Interface**: ethernet1/1
- **Local IP Address**: None
- **Peer IP Address Type**: IP
- **Peer Address**: <From Configuration Data>
- **Authentication**: Pre-Shared Key
- **Pre-shared Key**: ••••••
- **Confirm Pre-shared Key**: ••••••
- **Local Identification**: FQDN (hostname)
- **Peer Identification**: FQDN (hostname)

**Advanced Options**

- **OK**
- **Cancel**
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.
**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
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

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

### 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.
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.
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

<table>
<thead>
<tr>
<th>GROUP NAME</th>
<th>TUNNEL TYPE</th>
<th>TENANT GATEWAY IP(S)</th>
<th>MENLO GATEWAY IP(S)</th>
<th>REGION</th>
<th>NUMBER OF TUNNELS</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSEC-PAN-uw1</td>
<td>IPSEC</td>
<td>12.219.129.130</td>
<td>50.18.117.162</td>
<td>us-west-1</td>
<td>1</td>
</tr>
</tbody>
</table>
Create Gateway Group

### Gateway Group Details

**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.

<table>
<thead>
<tr>
<th>Tenant Remote IP(s)</th>
<th>+ Add</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify up to 2 tenant remote IPs</td>
<td></td>
</tr>
<tr>
<td>Add remote IP</td>
<td>+ Add</td>
</tr>
<tr>
<td>REMOTE IP</td>
<td></td>
</tr>
<tr>
<td>35.8.2.41</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regions</th>
<th>+ Add</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select up to 2 regions</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>REGIONS</td>
<td></td>
</tr>
<tr>
<td>us-west-1</td>
<td></td>
</tr>
<tr>
<td>us-west-1</td>
<td></td>
</tr>
</tbody>
</table>
VPN > Gateway Groups > Tunnel

Tunnel Details

Select Remote IP and Gateway to create tunnel between

<table>
<thead>
<tr>
<th>Name</th>
<th>Gateway*</th>
</tr>
</thead>
<tbody>
<tr>
<td>PANW</td>
<td>50.18.117.162 - 50.18.117.162</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mtu</th>
</tr>
</thead>
<tbody>
<tr>
<td>1400</td>
</tr>
</tbody>
</table>

Remote IP*:
12.219.129.130

local_link_ping
- True
- False
- Inherit

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 Settings

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

<table>
<thead>
<tr>
<th>Proposal</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>aes256-sha1-modp1024</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>aes128-sha1-modp1024</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>aes256-sha256-modp1024</td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>aes128-sha256-modp1024</td>
<td>✗</td>
<td></td>
</tr>
</tbody>
</table>

- **rekey_time**: 5400
- **rekey_bytes**: 500000000
- **rekey_packets**: 1000000
- **life_time**: 20

---

© 2022 / Menlo Security, Inc. All rights reserved. | Confidential/Internal