

Palo Alto Prisma Access: Panorama Managed Integration Guide

Applies to: Menlo Cloud
Version Information: 2.86
Date Updated: October 2022

Revision History	2
Use Cases for Integration with Palo Alto Prisma Access Simplify User Policy Enforcement	3
Challenge	3
Solution	3
Protecting High Risk Users and Applications	3
Challenge	3
Solution	3
Integration Benefits	4
Integration Diagram	4
Before You Begin	5
Palo Alto Networks Configuration	5
Method 1a. Block action with custom Block Page response	5
Method 1b. Override action for redirection to isolation	12
Configuration For both Block and Override modes	19
Method 2. Transparent Proxy with Prisma Access	26
Menlo Security Product Configuration	46
Troubleshooting	47
Technical Details	47

Revision History

Release	Date	Change
2.86	October 2022	Initial Release

Use Cases for Integration with Palo Alto Prisma Access Simplify User Policy Enforcement

Challenge

The internet contains more than 4 billion websites, with millions more launched every month. Many are new and, therefore, uncategorized, while others are inaccessible because of “false positive” classification. This leaves organizations with the difficult choice to either allow or deny user access. Allowing access supports user productivity but increases cyber risk, whereas denying access limits productivity and dramatically increases help desk tickets requesting website categorizations and recategorizations.

Solution

Together, Prisma Access and the Menlo Security Isolation Platform allow organizations to leverage the URL policy capabilities of Prisma Access and selectively steer specific websites — such as uncategorized websites or those that register a false positive — to the Menlo Security Isolation Platform. This allows users to access such websites safely without risking the organization’s security posture. Users will experience 100% native web browsing, and their web browsers will receive 100% safe visual components for local rendering

Protecting High Risk Users and Applications

Challenge

Many organizations have a group of users that may require elevated security while accessing websites. These users may be privileged administrators, or they may have access to highly secure systems (e.g., payment systems, SWIFT interbank transfer systems) from their devices. The extra level of security may also be mandated by industry or government regulations.

Solution

All web traffic for specific users or groups of users may be directed through the Menlo Security Isolation Platform via integration with Prisma Access. This ensures that any website the specified user or group accesses is executed within the cloud-based Menlo Security Isolation Platform, returning only safe and malware-free visual components to the user’s device for local rendering in a web browser.

Prisma Access can integrate with Menlo Security to provide web isolation for users in two ways. The first method is via URL prepend, wherein URLs associated with a user's web traffic are prepended with safe[.]menlosecurity[.]com. The second method utilizes traffic steering policies in Prisma Access, wherein web traffic is redirected across an IPsec tunnel to the Menlo Security Isolation Platform and is completely transparent to end users for a more seamless experience. End users will see no change and can browse web pages with a native experience.

Integration Benefits

Palo Alto Prisma Access and the Menlo Security Isolation Platform work together to deliver the most proactive prevention posture available, while allowing enterprise users to be productive on the web and in email. The integrated solution:

- Stops malware from unknown/uncategorized websites.
 - Ends malware from weaponized documents and files.
 - Complies with regulations for air-gapping high-value users.
 - Improves user productivity, unhindered by excessive website blocks.
 - Reduces help desk tickets from users whose access to websites has been blocked.
- Combines the benefits of Palo Alto Prisma Access policy and Isolation

Integration Diagram

As covered in the use-cases description above, specific Internet and SaaS traffic defined by the use-case criteria (certain users, certain URLs or any combination of both) is redirected to the Menlo Security solution; this to introduce the air-gap offered by the web-isolation:

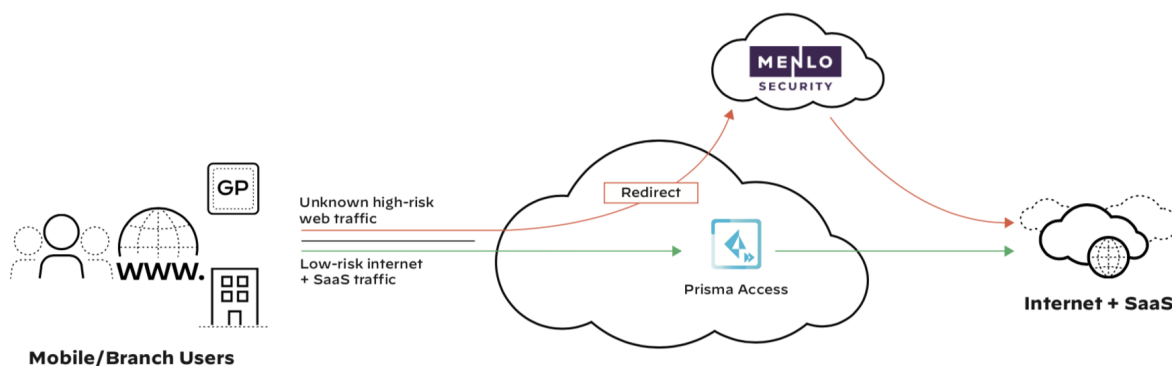


Figure 1: Forwarding of specific traffic to Menlo Security for browser isolation

Before You Begin

To ensure a smooth configuration process, please ensure the following prerequisites are met:

- Access to the Prisma Access instance and the Panorama instance managing it (similar steps as below could be followed in case the Prisma Access is managed via the Cloud Management platform)
- Access to a Menlo Security instance and the Admin Portal (admin.menlosecurity.com)

Palo Alto Networks Configuration

The redirection of the specific traffic that is traversing Prisma Access towards the Menlo Security solution can be achieved in two ways:

1. Using categorization to redirect web requests to “prepend” isolation mode. This can be done two ways
 - a. by a “block” action set to the desired URL Category and a custom Block Response Page.
 - b. by an “override” action set to the desired URL Category, that can then be applied to a Security Policy for a specific set of users; this integration method is not supported for the Explicit Proxy Mobile Users.
2. Transparent forwarding using Traffic Steering policies in Prisma Access and IPSEC tunnels between the two cloud security solutions

Method 1a. Block action with custom Block Page response

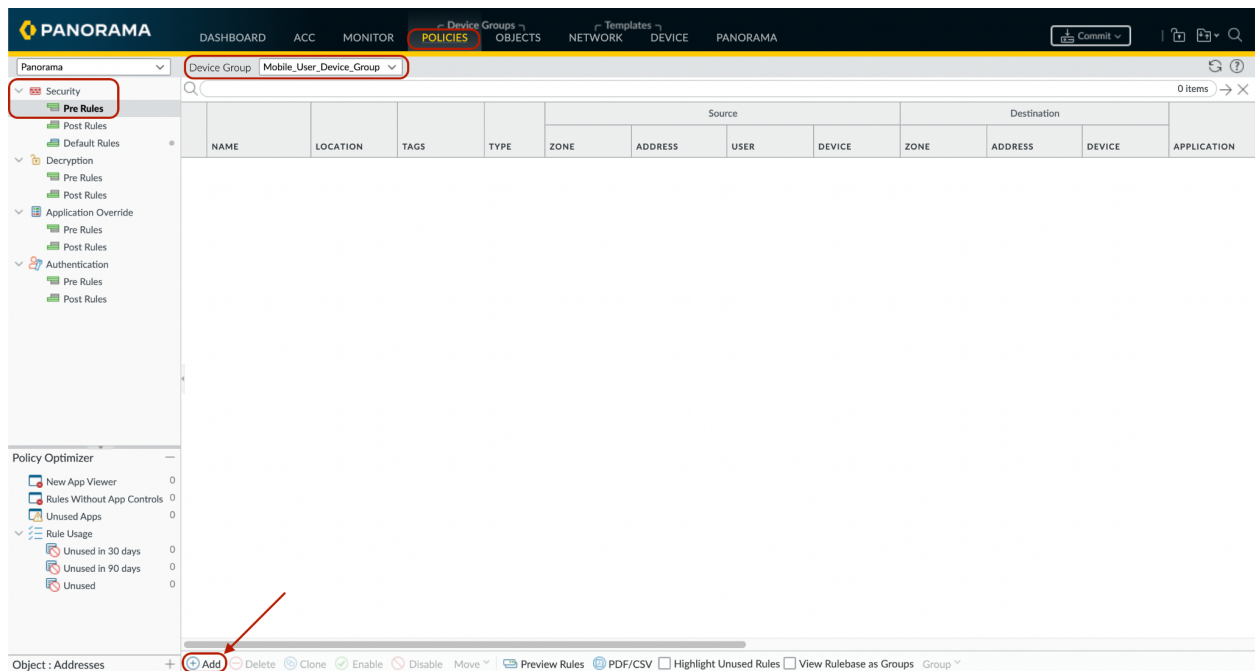
Step 1: Create or update the policy handling internet bound traffic

Log in to Panorama to view managing the Prisma Access instance. Under the Mobile Users Device Group, add a new policy or edit an existing one (a similar policy can be defined for the Remote Networks Device Group)

Under the Actions tab, select the Allow option and under the Profiles, select the URL Filtering Profile defined in the first step above

Navigate to:

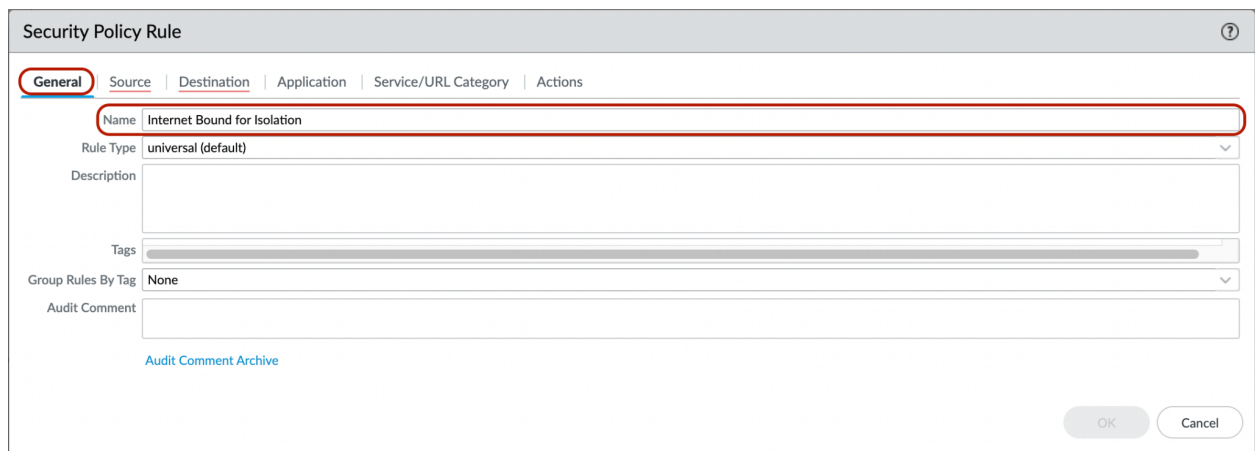
Policies > Security (Pre-Rules) > select Device Group: Mobile_User_Device_Group > select Add



Object: Addresses + Add Delete Clone Enable Disable Move Preview Rules PDF/CSV Highlight Unused Rules View Rulebase as Groups Group

In the Security Policy Rule pop up window:

Provide a name under the General tab



Security Policy Rule

General Source Destination Application Service/URL Category Actions

Name: Internet Bound for Isolation

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

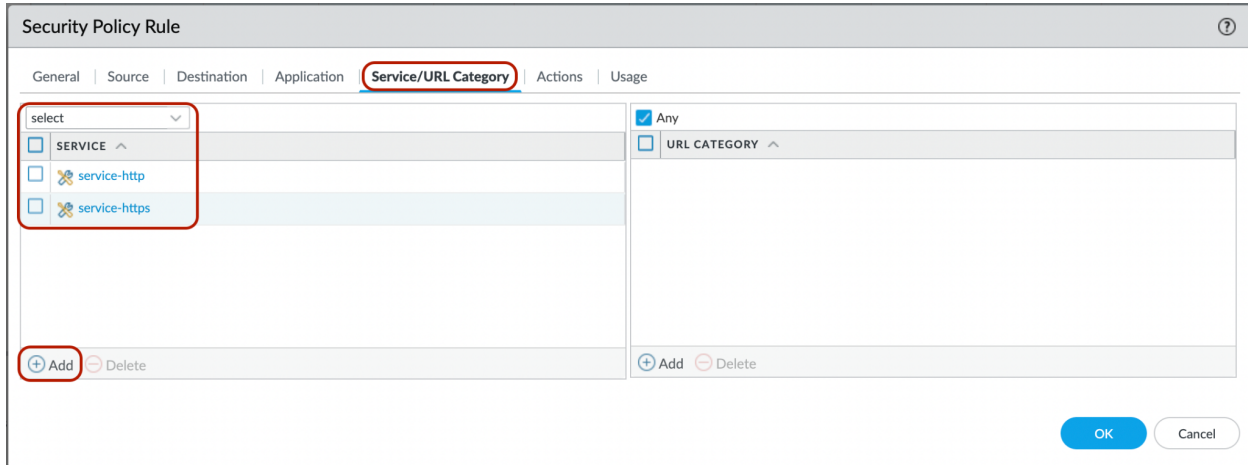
[Audit Comment Archive](#)

OK Cancel

Provide Source Zones and Source Addresses under the Source tab. To enforce the web isolation for a particular set of users, add the proper users under the Source tab:

Provide Destination Zones and Destination Addresses under the Destination tab

© 2022 / Menlo Security, Inc. All rights reserved. | Confidential/Internal 7



Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions | Usage

select

☐ SERVICE ^

☐ service-http

☐ service-https

☒ Any

☐ URL CATEGORY ^

☒ Add ☐ Delete

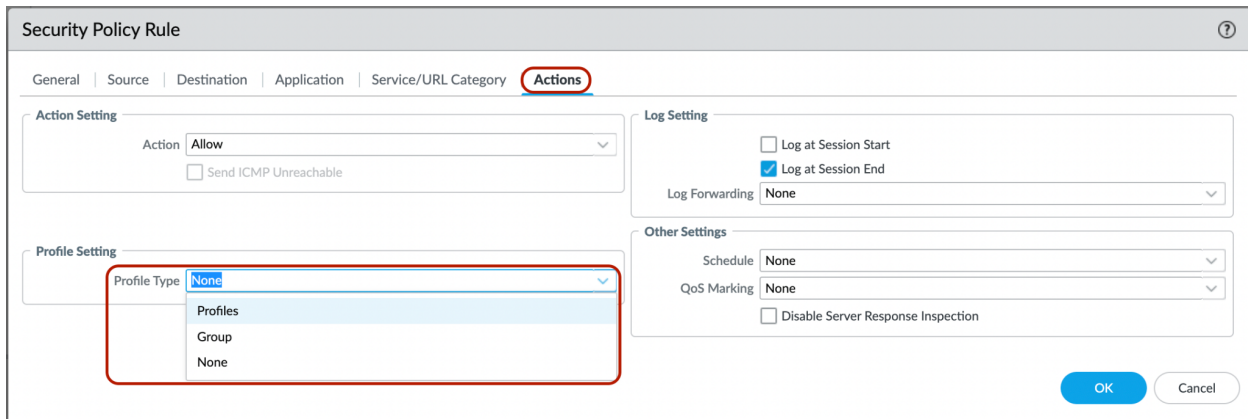
☒ Add ☐ Delete

OK Cancel

Create new URL Filtering profile under Actions tab

Navigate to:

Actions tab > Profile Type > select Profiles



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions**

Action Setting

Action: Allow

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

Profile Setting

Profile Type: None

Profiles

Group

None

OK Cancel

URL Filtering > click the drop down field > select New URL Filtering

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions**

Action Setting

Action: **Allow**

☐ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None


Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: **None**

File Blocking: None

Data Filtering: default

WildFire Analysis: New  URL Filtering

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

OK Cancel

Step 2: Create URL filtering profile to block

URL Filtering Profile

Name: Menlo-Sec

Description: Categories to be redirected to Menlo Security for Web Isolation

☐ Shared

☐ Disable override

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

75 items → ×

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
<input type="checkbox"/> extremism	allow	allow
<input type="checkbox"/> financial-services	allow	allow
<input checked="" type="checkbox"/> gambling	block	block
<input type="checkbox"/> games	allow	allow
<input type="checkbox"/> government	allow	allow
<input type="checkbox"/> grayware	allow	allow
<input type="checkbox"/> hacking	allow	allow
<input type="checkbox"/> health-and-medicine	allow	allow

* indicates a custom URL category, + indicates external dynamic list

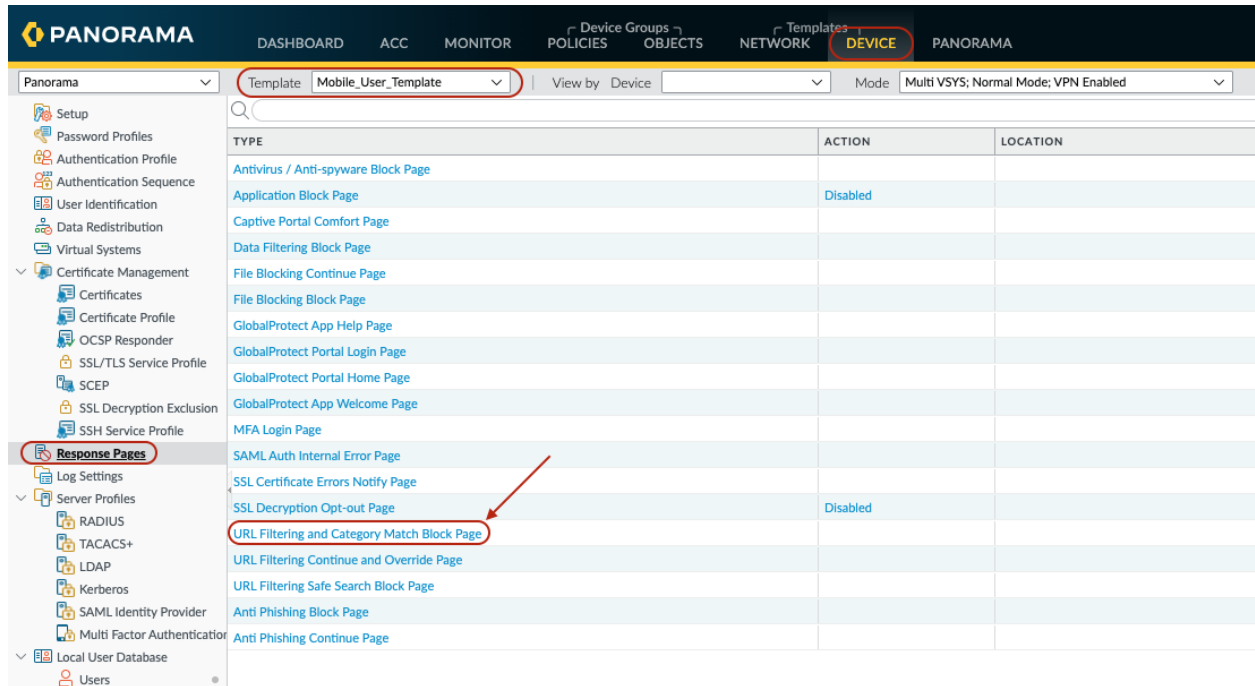
[Check URL Category](#)

OK Cancel

Step 3: Upload custom block page

Navigate to:

Device > Response Pages > under Template: Mobile_User_Template > select “URL Filtering and Category Match Block Page”



The screenshot shows the PANORAMA interface with the 'DEVICE' tab selected. The left sidebar shows the 'Response Pages' section under 'Certificate Management'. The main table lists various block pages, with 'URL Filtering and Category Match Block Page' highlighted by a red circle and an arrow.

TYPE	ACTION	LOCATION
Antivirus / Anti-spyware Block Page		
Application Block Page	Disabled	
Captive Portal Comfort Page		
Data Filtering Block Page		
File Blocking Continue Page		
File Blocking Block Page		
GlobalProtect App Help Page		
GlobalProtect Portal Login Page		
GlobalProtect Portal Home Page		
GlobalProtect App Welcome Page		
MFA Login Page		
SAML Auth Internal Error Page		
SSL Certificate Errors Notify Page		
SSL Decryption Opt-out Page	Disabled	
URL Filtering and Category Match Block Page		
URL Filtering Continue and Override Page		
URL Filtering Safe Search Block Page		
Anti Phishing Block Page		
Anti Phishing Continue Page		

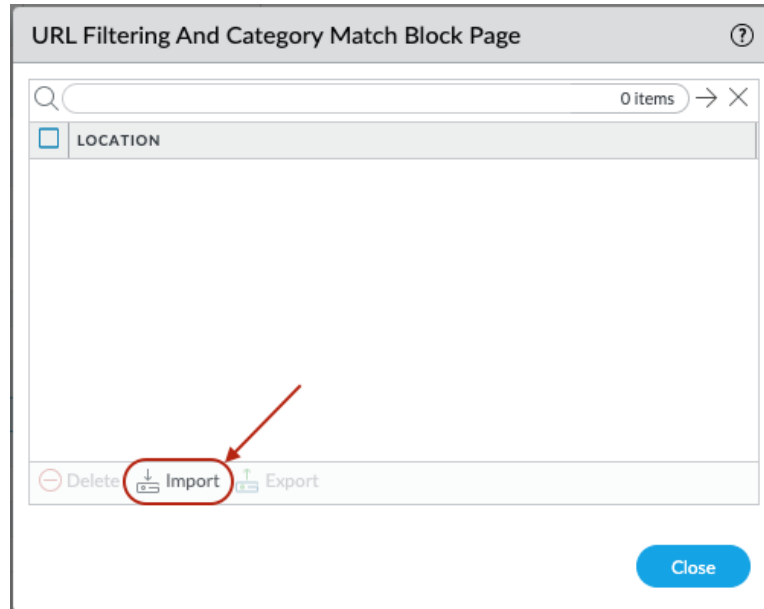
In the “URL Filtering And Category Match Block Page” pop-up window, click “Import”

An example of a Block Response age is provided below and can be changed and adapted for more specific use-cases.

```
<html>
<head>
<title>Web Page Blocked</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE">
<meta name="viewport" content="initial-scale=1.0">
<style>
  #content {
    border:3px solid#aaa;
    background-color:#fff;
    margin:1.5em;
    padding:1.5em;
    font-family:Tahoma,Helvetica,Arial,sans-serif;
    font-size:1em;
  }
  h1 {
    font-size:1.3em;
    font-weight:bold;
    color:#196390;
  }
  b {
    font-weight:normal;
    color:#196390;
  }
</style>
<script>
  var dest = "<url/>";
  var category = "<category/>";
  switch (category) {
    case 'questionable':
    case 'dynamic-dns':
    case 'unknown':
    case 'parked':
      var prepended = "https://safe.menlosecurity.com/";
      window.location.replace(prepend);
  }

  // window.location.replace('https://safe.menlosecurity.com')
</script>

</head>
<body bgcolor="#e7e8e9">
<div id="content">
<h1>Web Page Blocked</h1>
<p>Access to the web page you were trying to visit has been
blocked in
accordance with company policy. Please contact your system administrator
if you believe this is in error.</p>
<p><b>User:</b> <user/> </p>
<p><b>URL:</b> <url/> </p>
<p><b>Category:</b> <category/> </p>
<p>To view the page in <b>Isolation</b>
</div>
</body>
</html>
```



Continue to step 4 in **Configuration for both Block and Override modes** section.

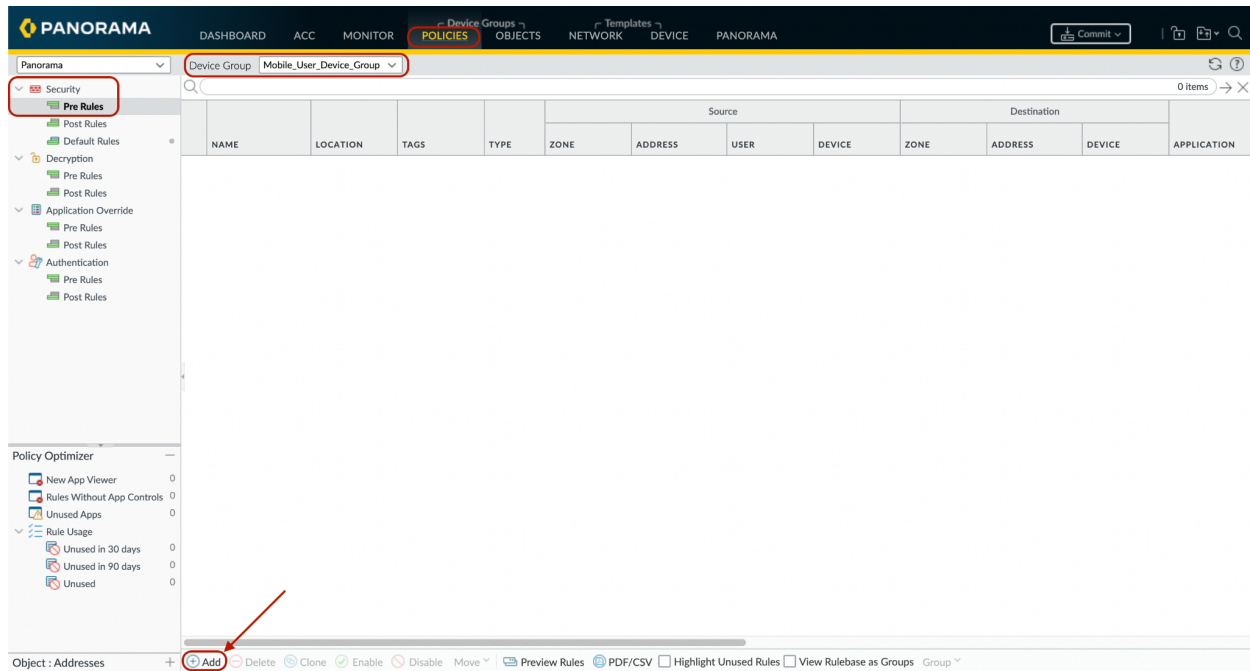
Method 1b. Override action for redirection to isolation

Step 1: Create or update the policy handling internet bound traffic

Log in to Panorama to view managing the Prisma Access instance. Under the Mobile Users Device Group, add a new policy or edit an existing one (a similar policy can be defined for the Remote Networks Device Group)

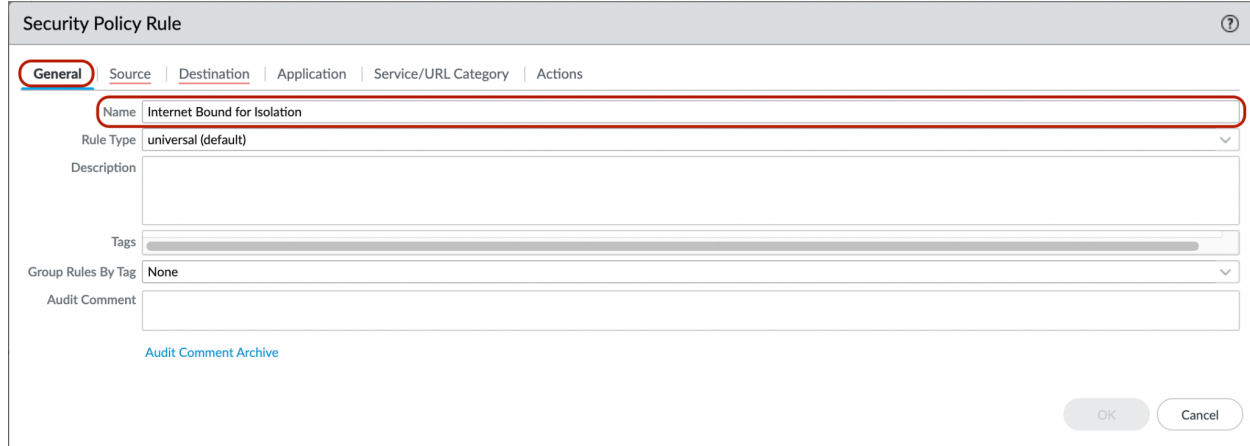
Step 2: Create URL filtering profile for isolation

Policies > Security (Pre-Rules) > select Device Group: Mobile_User_Device_Group > select Add



In the Security Policy Rule pop up window:

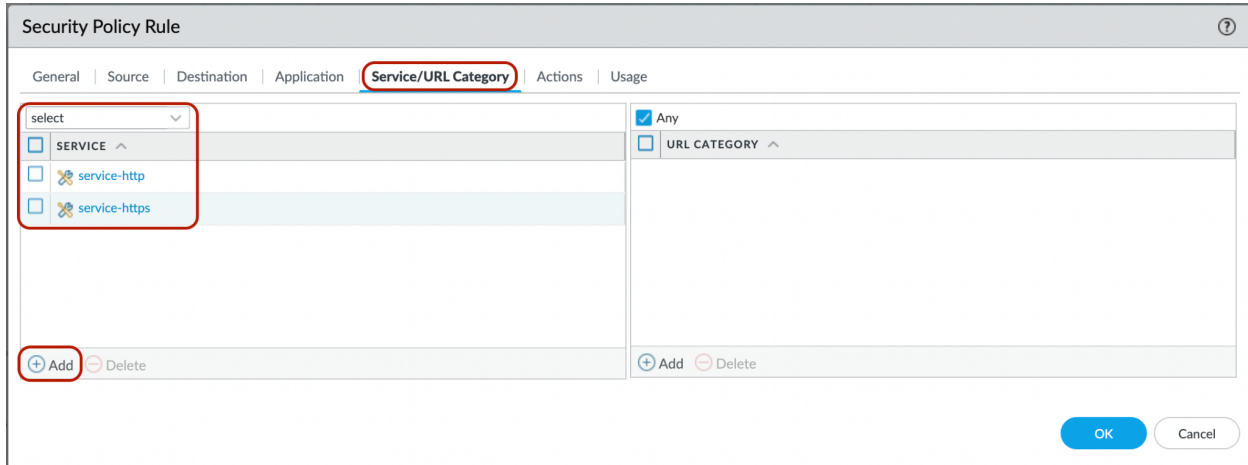
Provide a name under the General tab



Provide Source Zones and Source Addresses under the Source tab. To enforce the web isolation for a particular set of users, add the proper users under the Source tab:

Provide Destination Zones and Destination Addresses under the Destination tab

© 2022 / Menlo Security, Inc. All rights reserved. | Confidential/Internal 14



Security Policy Rule

General | Source | Destination | Application | **Service/URL Category** | Actions | Usage

select

☐ SERVICE ^

☐ service-http

☐ service-https

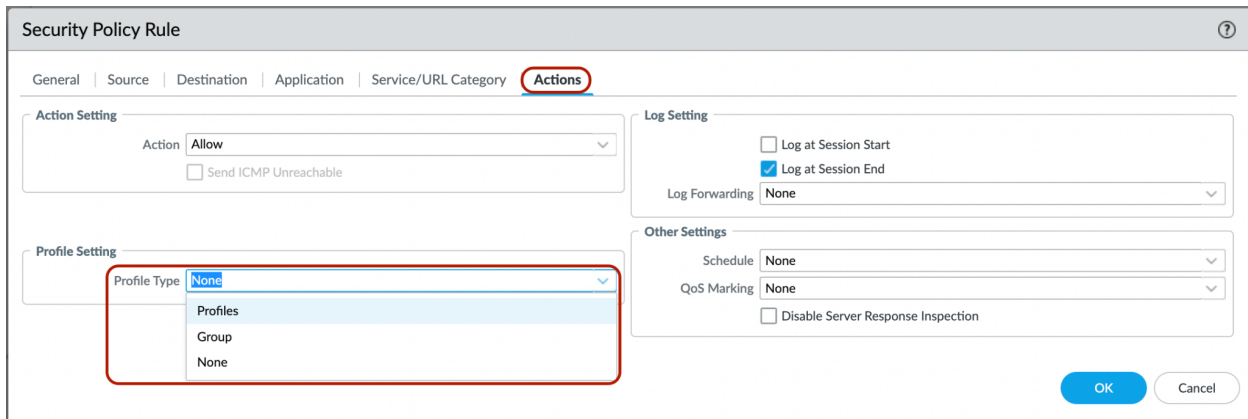
☐ Any

☐ URL CATEGORY ^

Create new URL Filtering profile under Actions tab

Navigate to:

Actions tab > Profile Type > select Profiles



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | **Actions**

Action Setting

Action:

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding:

Other Settings

Schedule:

QoS Marking:

☐ Disable Server Response Inspection

Profile Setting

Profile Type:

Profiles

Group

None

URL Filtering > click the drop down field > select New URL Filtering

Security Policy Rule

General
Source
Destination
Application
Service/URL Category
Actions

Action Setting

Action
Allow
Send ICMP Unreachable

Profile Setting

Profile Type
Profiles
Antivirus
None
Vulnerability Protection
None
Anti-Spyware
None
URL Filtering
None
File Blocking
None
Data Filtering
default
WildFire Analysis
New URL Filtering

Log Setting

Log at Session Start
Log at Session End
Log Forwarding
None

Other Settings

Schedule
None
QoS Marking
None
Disable Server Response Inspection

OK
Cancel

For the URL Categories that need to be redirected to Menlo Security for Web Isolation, select the Categories and set the Site Access to “override”; the same access can be set for Custom URL Categories if needed.

URL Filtering Profile

Name
Menlo-Sec

Description
Categories to be redirected to Menlo Security for Web Isolation

☐ Shared

☐ Disable override

Categories
URL Filtering Settings
User Credential Detection
HTTP Header Insertion
Inline ML

75 items

<input type="checkbox"/> CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
<input type="checkbox"/> motor-vehicles	allow	allow
<input type="checkbox"/> music	allow	allow
<input type="checkbox"/> newly-registered-domain	allow	allow
<input checked="" type="checkbox"/> news	override	allow
<input type="checkbox"/> not-resolved	allow	allow
<input type="checkbox"/> nudity	allow	allow
<input type="checkbox"/> online-storage-and-backup	allow	allow
<input type="checkbox"/> parked	allow	allow

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

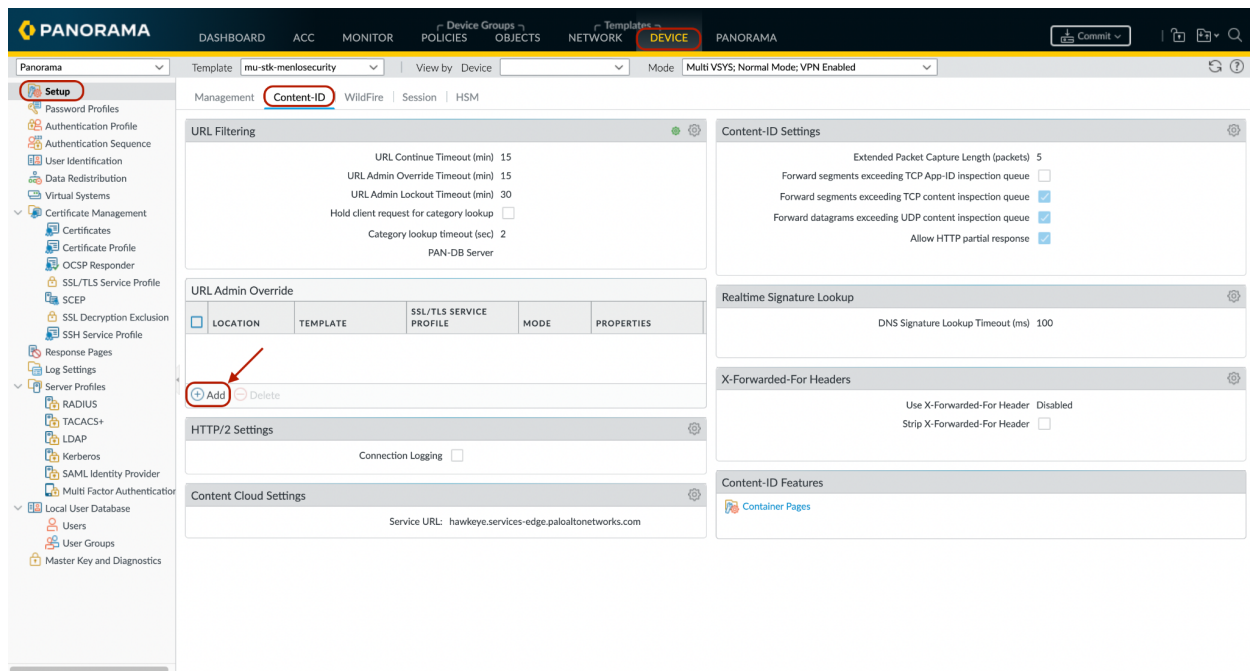
OK

Cancel

Step 3: Set the destination address to be used for the Override action

Navigate to:

Device > Setup > Content-ID > click Add under URL Admin Override



In the URL Admin Override pop-up window, fill in the form fields with the following values:

- Password and Confirm Password: Any password: this is the password that you may share with your users who are allowed the override privilege. This is not used in the Menlo Security integration.
- Server Certificate: None
- Mode: Redirect
- Address: redirector.menlosecurity.com

URL Admin Override

Location

vsys1

Password

.....

Confirm Password

.....

SSL/TLS Service Profile

None

Mode

Transparent

Redirect

Address

redirector.menlosecurity.com

OK

Cancel

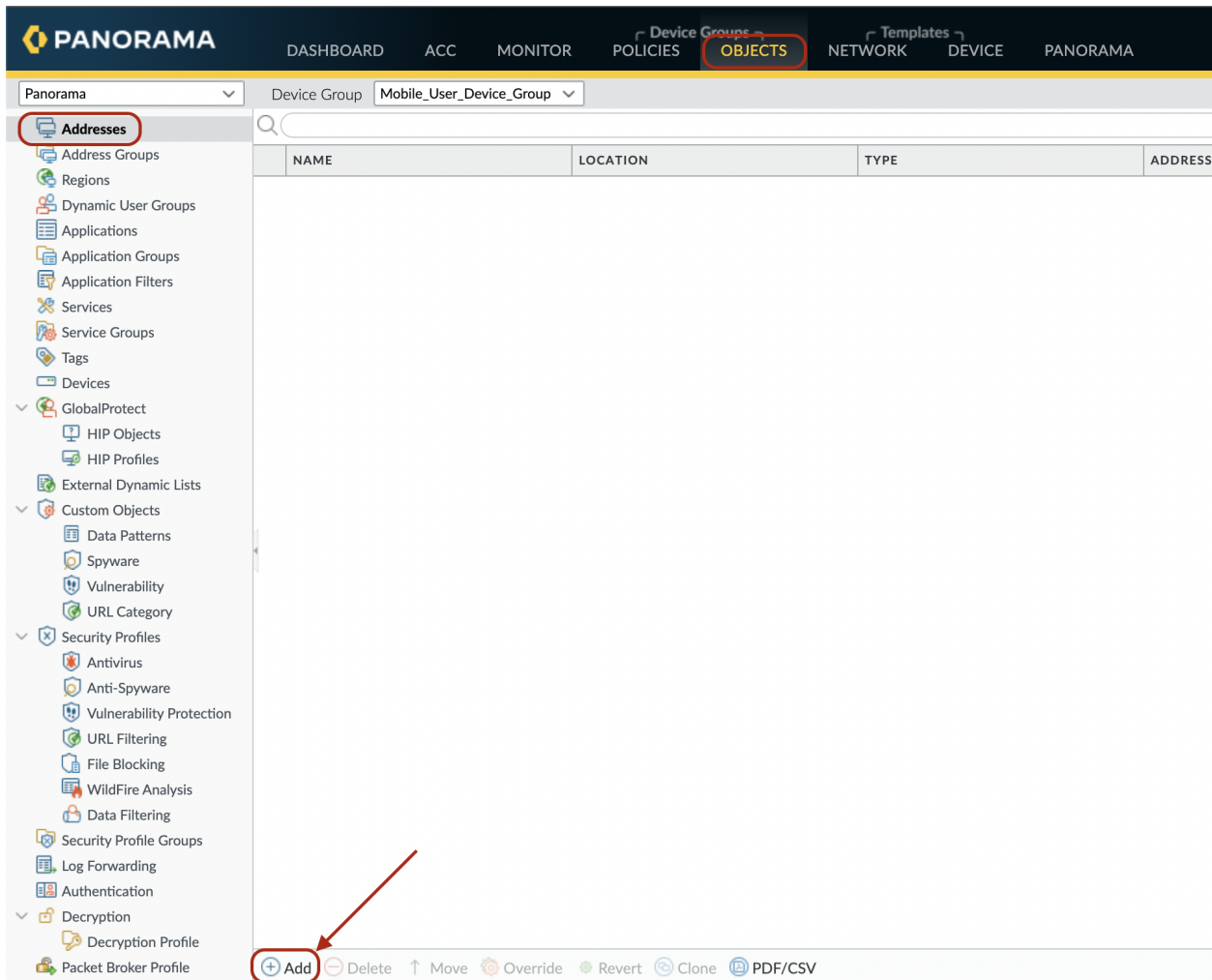
Commit and Push all the configurations.

Configuration For both Block and Override modes

Step 4: Avoid Double Decryption

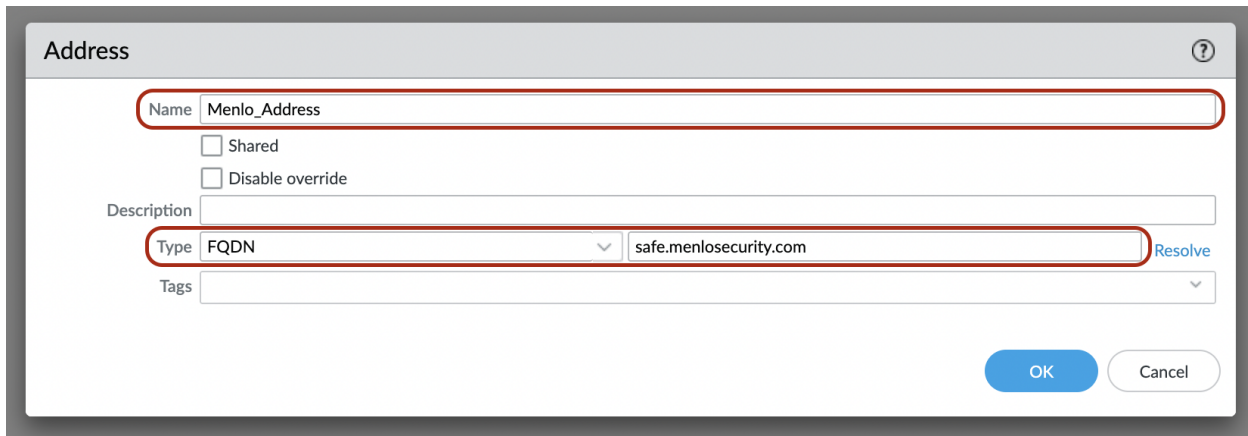
Enable SSL decryption for enhancing the URL Categorization rate, but disable the SSL decryption for traffic redirected towards Menlo Security.

Navigate to Objects > Addresses under the Mobile Users Device Group > Add



The screenshot shows the PANORAMA interface with the 'OBJECTS' tab selected. The left sidebar lists various object types, including 'Addresses'. The main panel displays a table with columns: NAME, LOCATION, TYPE, and ADDRESS. At the bottom of the panel, there is a '+ Add' button, which is highlighted with a red circle and an arrow.

Provide a name and add a new type FQDN object with the address safe.menlosecurity.com

A screenshot of a web-based configuration dialog titled "Address". The dialog has a light gray header bar with the title and a help icon. The main content area is white. It contains several fields: a "Name" field with the value "Menlo_Address", two checkboxes labeled "Shared" and "Disable override" (both unchecked), a "Description" field, a "Type" dropdown menu set to "FQDN", and a text field containing "safe.menlosecurity.com" with a "Resolve" link to its right. Below these is a "Tags" field with a dropdown arrow. At the bottom right are "OK" and "Cancel" buttons.

Address

Name

☐ Shared

☐ Disable override

Description

Type [Resolve](#)

Tags

Navigate to Policies > Decryption under the Mobile Users Device group

Create a policy decrypting all the traffic for the required users.

Create a policy to not decrypt the traffic redirected to Menlo Security, by using the Menlo Address object previously created as criteria for the Destination field. This step ensures the traffic is not decrypted twice (once by Prisma Access and the second time by Menlo Security):

PANORAMA DASHBOARD ACC MONITOR **POLICIES** Device Groups OBJECTS NETWORK Templates DEVICE PANORAMA

Panorama Device Group Mobile_User_Device_Group

Security

- Pre Rules
- Post Rules
- Default Rules
- Decryption**
 - Pre Rules**
 - Post Rules
- Application Override
 - Pre Rules
 - Post Rules
- Authentication
 - Pre Rules
 - Post Rules

Policy Optimizer

- Rule Usage
 - Unused in 30 days 0
 - Unused in 90 days 0
 - Unused 0

	NAME	LOCATION	TAGS	ZONE	ADDRESS	USER	DEVICE	ZO
1	No_Decrypt_Menlo	Mobile_User_Device_Group		any	any	any	any	an

Object : Addresses + **Add** Delete Clone Enable Disable Move Preview Rules PDF/CSV Highlight Unused Rules View Rulebas

Decryption Policy Rule

General
Source
Destination
Service/URL Category
Options

Name
No_Decrypt_Menlo

Description

Tags

Group Rules By Tag
None

Audit Comment

[Audit Comment Archive](#)

OK
Cancel

Decryption Policy Rule

General
Source
Destination
Service/URL Category
Options

☒ Any

☐ SOURCE_ZONE ^

☒ Any

☐ SOURCE_ADDRESS ^

any

☐ SOURCE_USER ^

any

☐ SOURCE_DEVICE ^

+ Add - Delete

+ Add - Delete

+ Add - Delete

+ Add - Delete

☐ Negate

OK
Cancel

Decryption Policy Rule ⓘ

General | Source | **Destination** | Service/URL Category | Options

<input checked="" type="checkbox"/> Any	<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> DESTINATION_ZONE ^	<input type="checkbox"/> DESTINATION_ADDRESS ^	<input type="checkbox"/> DESTINATION_DEVICE ^
	<input checked="" type="checkbox"/> Menlo_Address	
<input type="checkbox"/> + Add <input type="checkbox"/> - Delete	<input type="checkbox"/> + Add <input type="checkbox"/> - Delete	<input type="checkbox"/> + Add <input type="checkbox"/> - Delete

☐ Negate

OK Cancel

Decryption Policy Rule ⓘ

General | Source | Destination | Service/URL Category | **Options**

Action No Decrypt

Type SSL Forward Proxy

Decryption Profile None

Log Settings

☐ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log Forwarding None

Packet Broker Profile None

To decrypt and forward TLS traffic on PAN-OS (Seattle version or later), use Network packet Broker Policy. Decryption Broker configurations work only on PAN-OS 10.0 and earlier.

OK Cancel

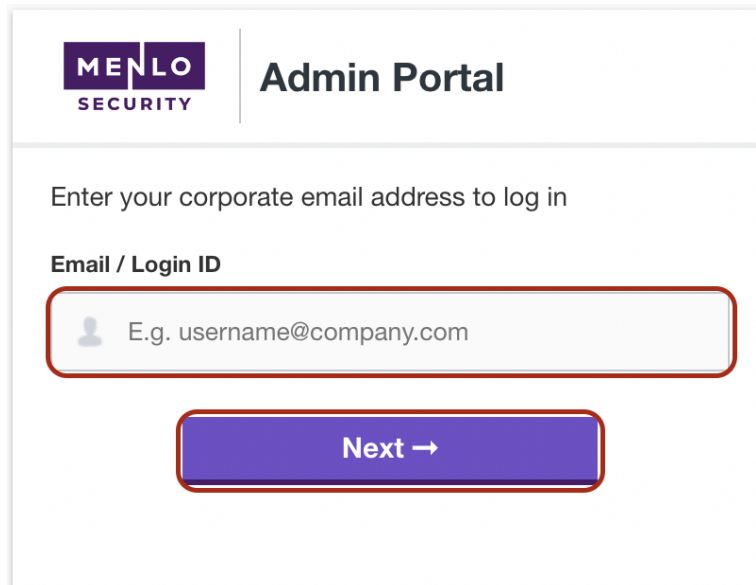
Commit and Push all the configurations.

Step 5: Verify the redirection works as expected

Connect a Mobile User to the Prisma Access instance via the GlobalProtect client.

Try to access any URL under the categories selected for redirection, in our example under the “news” category.

The user should be prompted to authenticate against the Menlo Security solution; after the user is passing the authentication once, other further redirections to Menlo Security will not require the authentication step anymore.


A screenshot of the Menlo Security Admin Portal login interface. At the top left is the Menlo Security logo. To its right is the title "Admin Portal". Below the logo and title, the text "Enter your corporate email address to log in" is displayed. Underneath this is the label "Email / Login ID". A text input field contains the placeholder text "E.g. username@company.com" preceded by a small user icon. Below the input field is a blue button with the text "Next →".

MENLO
SECURITY

Admin Portal

Enter your corporate email address to log in

Email / Login ID

 E.g. username@company.com

Next →

Welcome to BBC.com



News



'No safety concerns' with Pfizer vaccine

Promising new data on the potential



Trump campaign seeks partial recount in Wisconsin



BBC vows to 'get to truth' about Diana interview

The BBC is investigating allegations

Method 2. Transparent Proxy with Prisma Access

This configuration uses policy-based forwarding with IPsec tunnels to allow the steering of selected traffic to Menlo Security isolation.

Prerequisites needed to perform configuration:

- Palo Alto Prisma account and administrative access
- Determine the egress IP address used by the Prisma deployment for IPsec

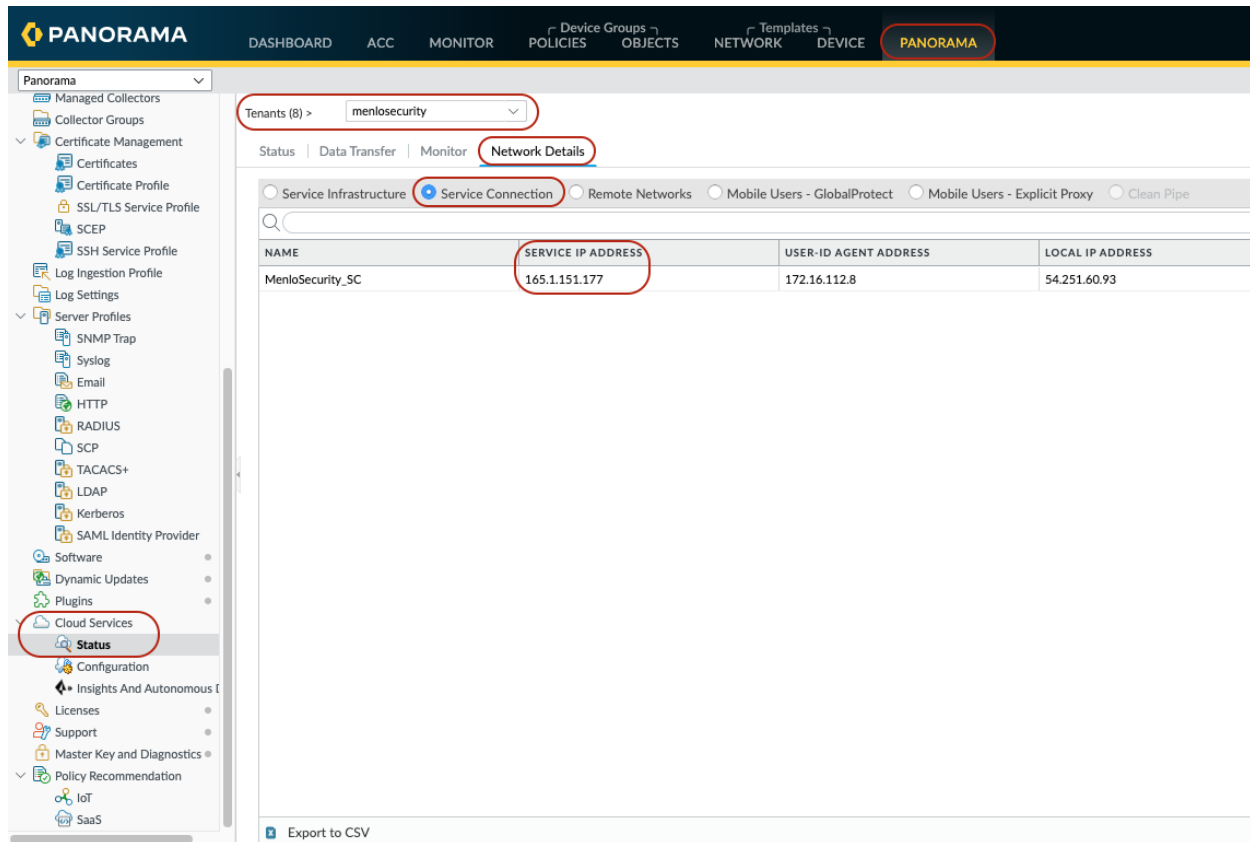
Step 1: Determine the Prisma IPsec gateway address

Prisma uses a “service address” for IPsec communications which differs from the Prisma firewall egress address. This service address needs to be known to authorize the IPsec connections.

In the Panorama administrative UI, navigate to:

Panorama tab > Cloud Services > Status

Ensure that the correct tenant is selected. In the right-hand pane, select Network Details then Service Connection. This view should show details about the service connections for the Prisma instances. Copy the IP address as shown in the “Service IP Address” column.



The screenshot shows the PANORAMA web interface. The left sidebar contains a navigation menu with categories like Managed Collectors, Certificate Management, Server Profiles, Cloud Services, and Policy Recommendation. The 'Status' option under 'Cloud Services' is highlighted. The main content area shows the 'Network Details' tab for the 'menlosecurity' tenant. The 'Service Connection' tab is selected, displaying a table with the following data:

NAME	SERVICE IP ADDRESS	USER-ID AGENT ADDRESS	LOCAL IP ADDRESS
MenloSecurity_SC	165.1.151.177	172.16.112.8	54.251.60.93

At the bottom of the interface, there is an 'Export to CSV' button.

Provide the service IP address to Menlo Security support
(<https://csportal.menlosecurity.com/hc/en-us>) to allow configuration of the IPsec settings.

Step 2: Configure an IPSEC Tunnel connecting to the Menlo Security cloud

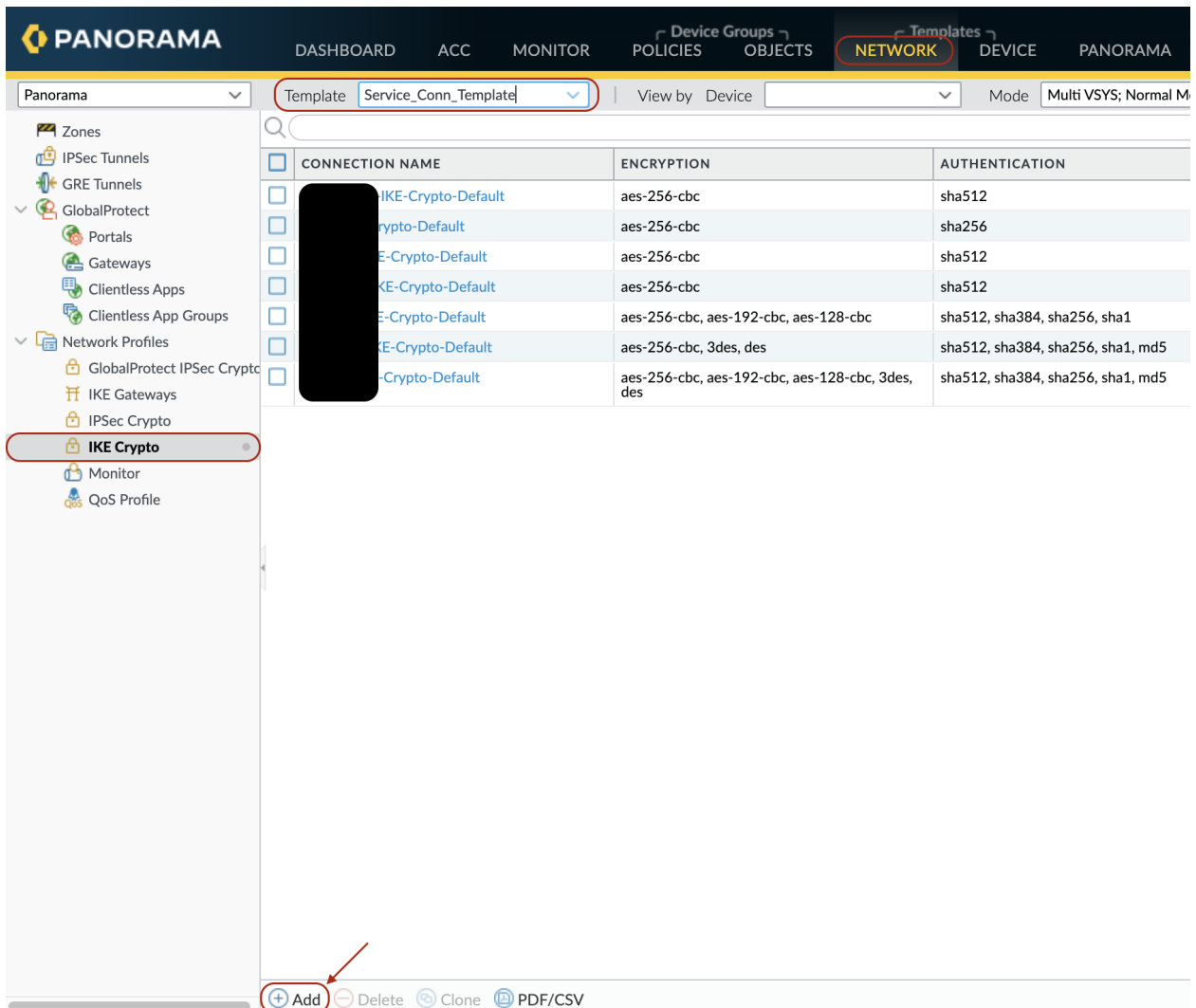
After the service IP address has been provided, Menlo Security support will provide the parameters below which will be used to configure Prisma.

Two instances of the following parameters will be provided, to configure a primary and a standby IPsec tunnel: Menlo Security Gateway IP address

- Pre-Shared Key
- Local Identifier (Prisma IPsec GW)
- Remote Identifier (Menlo IPsec GW)

Navigate to

Network > Network Profiles > IKE Crypto> under Template: Service_Conn_Template > click Add



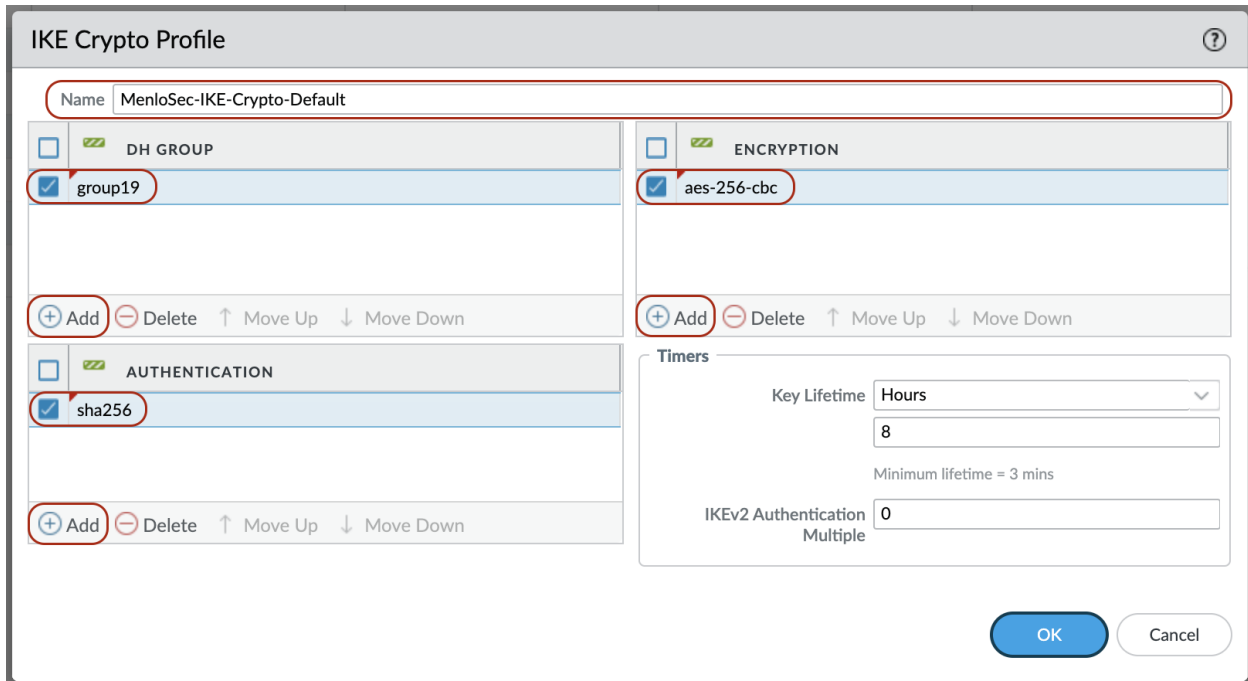
The screenshot shows the Palo Alto Networks Panorama interface. The left sidebar contains a navigation tree with the following items: Zones, IPSec Tunnels, GRE Tunnels, GlobalProtect, Portals, Gateways, Clientless Apps, Clientless App Groups, Network Profiles, GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, **IKE Crypto** (highlighted), Monitor, and QoS Profile. The main content area displays a table of IKE Crypto connections. The table has three columns: CONNECTION NAME, ENCRYPTION, and AUTHENTICATION. The table contains six rows of data. The 'Template' dropdown is set to 'Service_Conn_Template'. The 'Add' button at the bottom is highlighted with a red circle and an arrow.

CONNECTION NAME	ENCRYPTION	AUTHENTICATION
IKE-Crypto-Default	aes-256-cbc	sha512
IKE-Crypto-Default	aes-256-cbc	sha256
IKE-Crypto-Default	aes-256-cbc	sha512
IKE-Crypto-Default	aes-256-cbc	sha512
IKE-Crypto-Default	aes-256-cbc, aes-192-cbc, aes-128-cbc	sha512, sha384, sha256, sha1
IKE-Crypto-Default	aes-256-cbc, 3des, des	sha512, sha384, sha256, sha1, md5

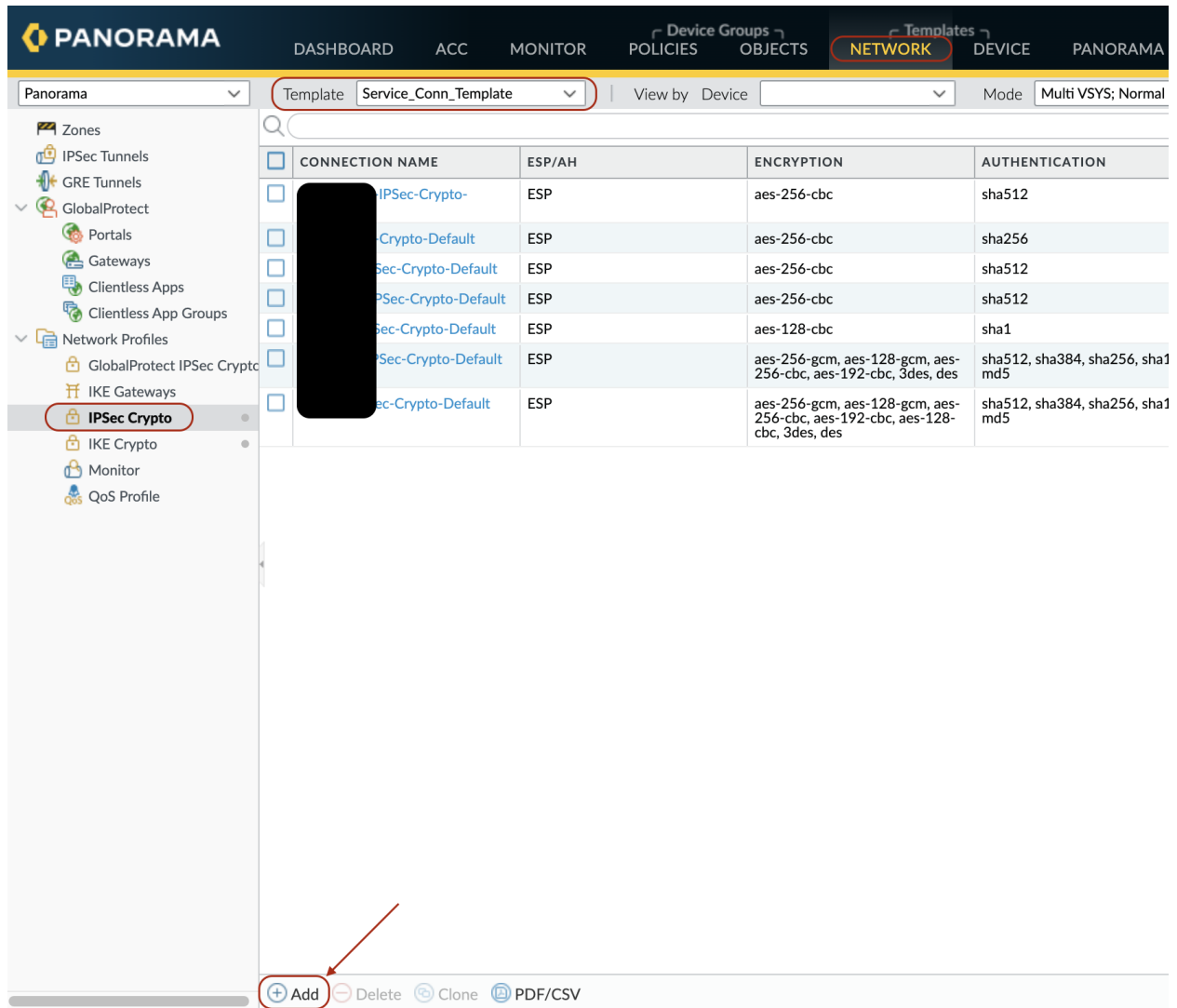
At the bottom of the interface, there is a row of buttons: **Add** (highlighted with a red circle and arrow), Delete, Clone, and PDF/CSV.

Configure an IKE Crypto profile using the settings defined below which match the Menlo Security IPSec Profile:

- AES-256-CBC Encryption
- SHA256 Authentication
- DH Group19 (256 bit Elliptic Curve)



Next, configure an IPSEC Crypto profile. Navigate to:
Network > Network Profiles > IPsec Crypto > under Template: Service_Conn_Template > click Add



PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS **Network** DEVICES PANORAMA

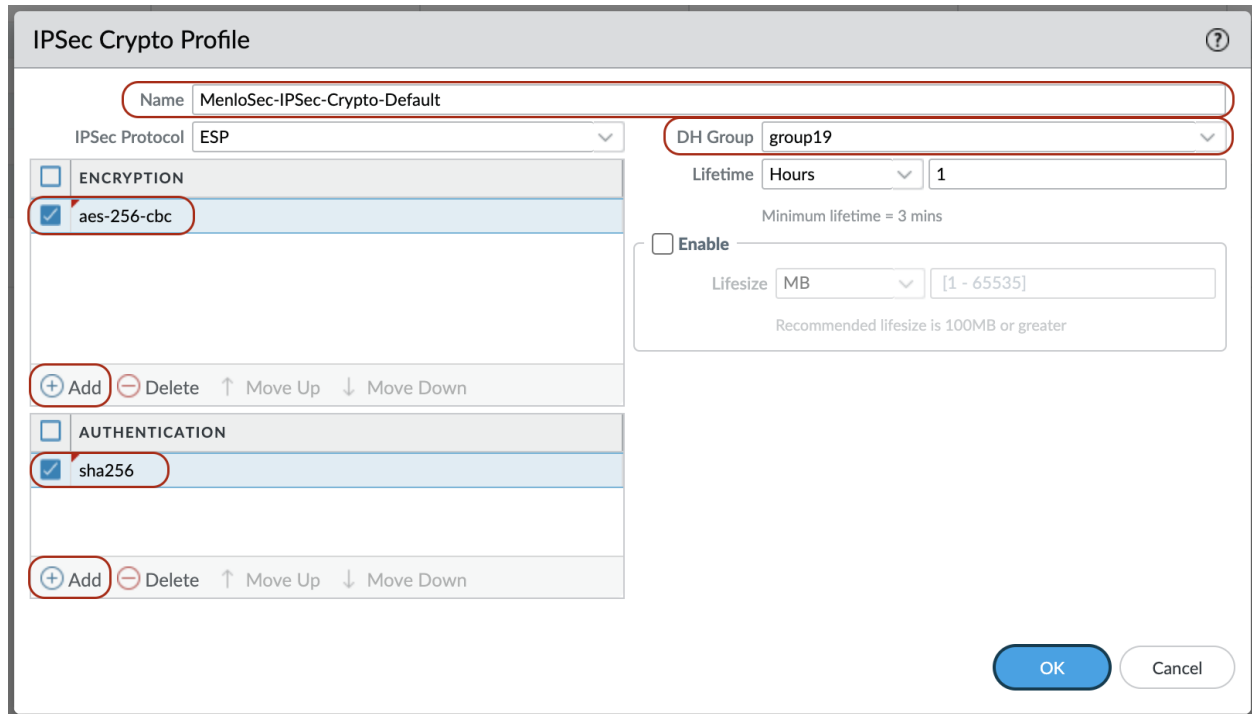
Template: Service_Conn_Template | View by: Device | Mode: Multi VSYS; Normal

CONNECTION NAME	ESP/AH	ENCRYPTION	AUTHENTICATION
IPSec-Crypto-	ESP	aes-256-cbc	sha512
Crypto-Default	ESP	aes-256-cbc	sha256
Sec-Crypto-Default	ESP	aes-256-cbc	sha512
IPSec-Crypto-Default	ESP	aes-256-cbc	sha512
Sec-Crypto-Default	ESP	aes-128-cbc	sha1
Sec-Crypto-Default	ESP	aes-256-gcm, aes-128-gcm, aes-256-cbc, aes-192-cbc, 3des, des	sha512, sha384, sha256, sha1 md5
Sec-Crypto-Default	ESP	aes-256-gcm, aes-128-gcm, aes-256-cbc, aes-192-cbc, aes-128-cbc, 3des, des	sha512, sha384, sha256, sha1 md5

+ Add Delete Clone PDF/CSV

Refer to your organization's policy as to the strength of encryption to use. In this example, the following were configured:

- AES-256-CBC Encryption
- SHA256 Authentication
- DH Group 19 (256-bit Elliptic Curve)



Create IKE Gateways for primary and secondary tunnels; the Peer Address, the Pre-shared Key and the FQDN used in the Local identification for each tunnel will be provided by Menlo Security.

Next, configure an IKE Gateway profile. Navigate to:

Network > Network Profiles > IKE Gateway > under Template: Service_Conn_Template > click Add

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE PANORAMA

Panorama Template: Service_Conn_Template View by: Device Mode: Multi VSYS; Normal Mod

IKE Gateways

	NAME	PEER ADDRESS	Peer ID		Local ID		VERSION
			ID	TYPE	ID	TYPE	
<input type="checkbox"/>	[REDACTED]						ikev1
<input type="checkbox"/>	[REDACTED]						ikev1
<input type="checkbox"/>	[REDACTED]						ikev1
<input type="checkbox"/>	[REDACTED]						ikev1
<input type="checkbox"/>	[REDACTED]						ikev2
<input type="checkbox"/>	[REDACTED]						ikev1
<input type="checkbox"/>	[REDACTED]						ikev1

Add Delete Enable Disable PDF/CSV

In the IKE Gateway pop-up, fill-in the highlighted fields.

IKE Gateway

General

Advanced Options

Name

MenloSec-IKE-Gateway-Default

Version

IKEv2 only mode

Peer IP Address Type

☒ IP
 ☐ Dynamic

Peer Address

menlosecurity

Authentication

☒ Pre-Shared Key
 ☐ Certificate

Pre-shared Key

.....

Confirm Pre-shared Key

.....

Local Identification

FQDN (hostname)

None

Peer Identification

FQDN (hostname)

None

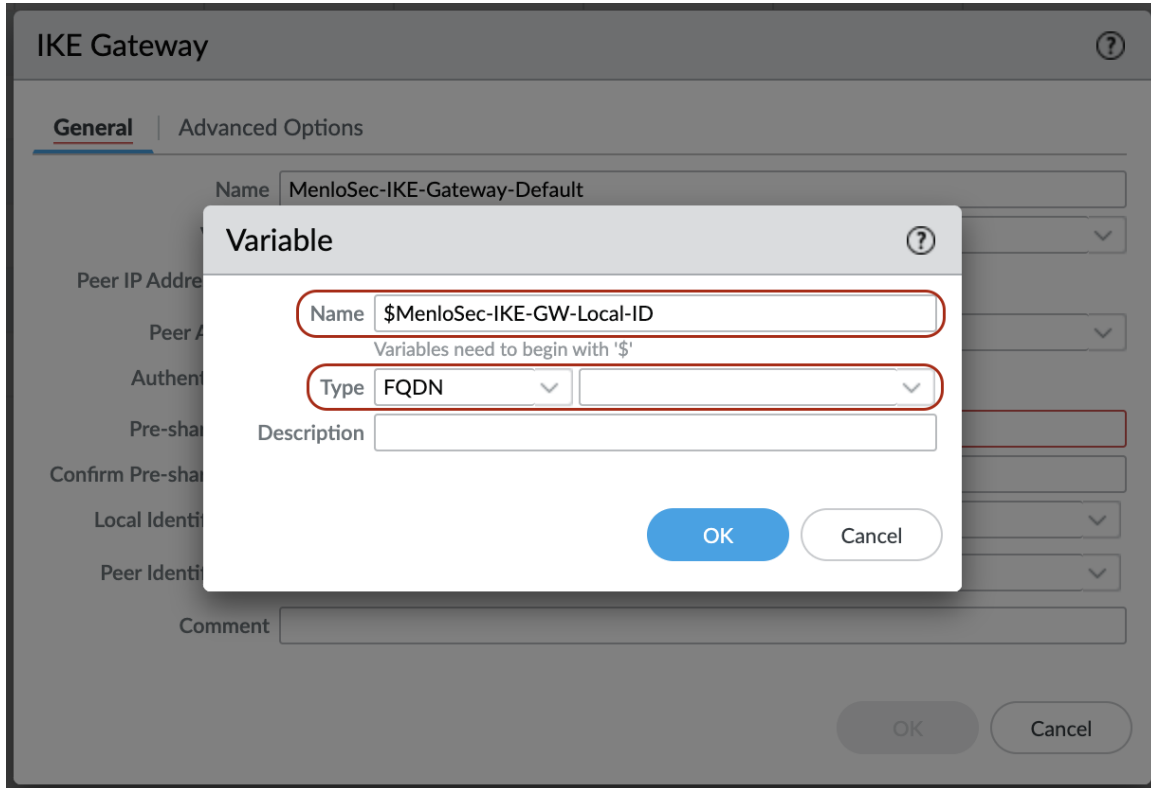
New X Variable

Comment

OK

Cancel

If they are not already created, new variables (FQDN) will need to be added for the Peer Address, Local Identification, and Peer Identification.



IKE Gateway

General | Advanced Options

Name: MenloSec-IKE-Gateway-Default

Peer IP Address: [Field]

Peer Authentication: [Field]

Pre-shared Key: [Field]

Confirm Pre-shared Key: [Field]

Local Identity: [Field]

Peer Identity: [Field]

Comment: [Field]

Variable

Name: \$MenloSec-IKE-GW-Local-ID

Type: FQDN

Description: [Field]

OK Cancel

Navigate to:
Network > IPSec Tunnels > click Add

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICES PANORAMA

Panorama Template: Service_Conn_Template View by: Device Mode: Multi VSYS; Normal Mod

IPSec Tunnels

NAME	TYPE	PEER ADDRESS
IPSec-Tunnel-Default	Auto Key	dynamic
Tunnel-Default	Auto Key	dynamic
ec-Tunnel-Default	Auto Key	dynamic
Sec-Tunnel-Default	Auto Key	dynamic
ec-Tunnel-Default	Auto Key	dynamic
Sec-Tunnel-Default	Auto Key	dynamic
ec-Tunnel-Default	Auto Key	dynamic

+ Add - Delete Enable Disable PDF/CSV

Configure two IPSEC Tunnels using the IKE Gateways previously configured. Configure a Tunnel Monitor to the address 169.254.10.1 to monitor tunnel availability.

IPSec Tunnel

General

Proxy IDs

Name

MenloSec-IPSec-Tunnel-Default

Type

Auto Key

IKE Gateway

MenloSec-IKE-Gateway-Default

IPSec Crypto Profile

MenloSec-IPSec-Crypto-Default

☐ Enable Replay Protection

Anti Replay Window

1024

☐ Copy ToS Header

☐ Add GRE Encapsulation

☒ Tunnel Monitor

Destination IP

169.254.10.1

Proxy ID

None

Comment

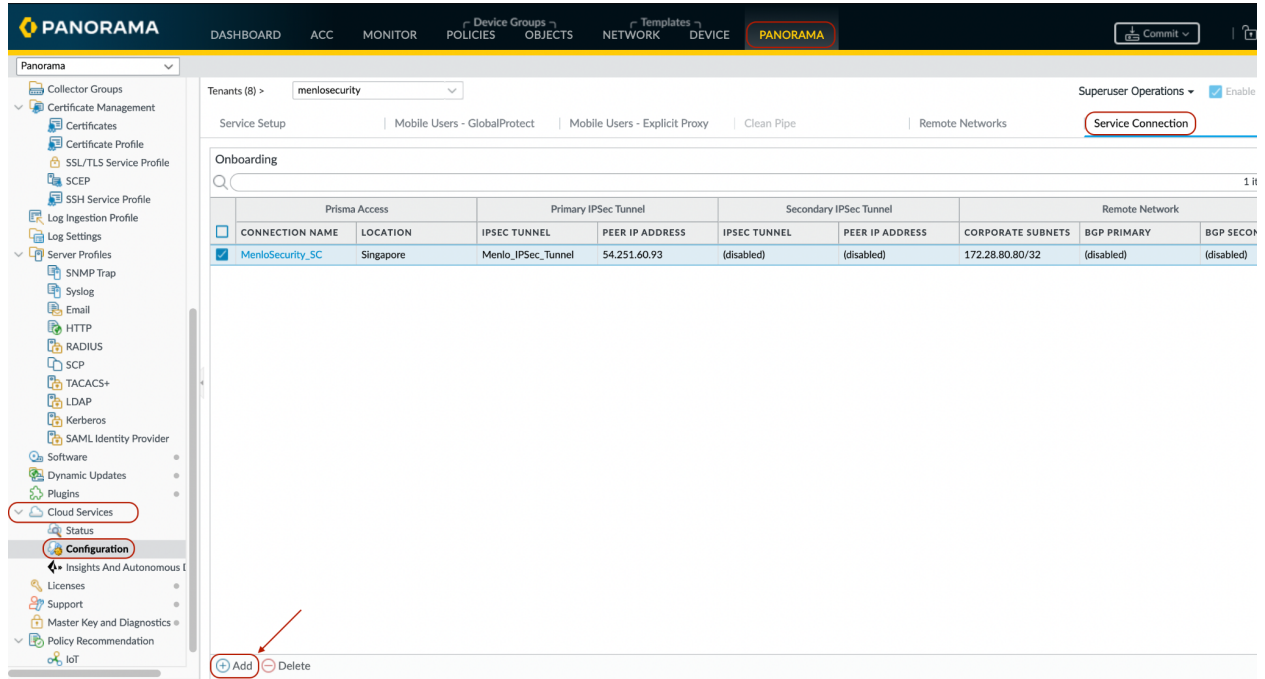
OK

Cancel

Step 2: Add a Service Connection using the previously created IPSEC Tunnel

Navigate to

Panorama > Cloud Services > Configuration > Service Connection and add a new Service Connection.



PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE **PANORAMA** Commit

Tenants (8) > **menlosecurity** Superuser Operations ☒ Enable

Service Setup | Mobile Users - GlobalProtect | Mobile Users - Explicit Proxy | Clean Pipe | Remote Networks | **Service Connection**

Onboarding

Prisma Access		Primary IPsec Tunnel		Secondary IPsec Tunnel		Remote Network		
CONNECTION NAME	LOCATION	IPSEC TUNNEL	PEER IP ADDRESS	IPSEC TUNNEL	PEER IP ADDRESS	CORPORATE SUBNETS	BGP PRIMARY	BGP SECONDARY
<input checked="" type="checkbox"/> MenloSecurity_SC	Singapore	Menlo_IPSec_Tunnel	54.251.60.93	(disabled)	(disabled)	172.28.80.80/32	(disabled)	(disabled)

+ Add - Delete

Select the Location which is closest to your geographic location. Configure both the primary and secondary Menlo Security IPsec tunnels, to provide fault-tolerant connectivity.

Onboarding

Name

MenloSecurity_US-West

Location

US West

Your subscription allows you to use up to 5 Prisma Access locations for Service Connections.

IPSec Tunnel

Menlo_IPSec_Tunnel

Backup SC

None

☒ Enable Secondary WAN

IPSec Tunnel

Menlo_IPSec_Tunnel_Secondary

Static Routes

BGP

QoS

☐ CORPORATE SUBNETS

☒ 0.0.0.0

☐ Add

☐ Delete

Enter the subnets for your corporate headquarters.

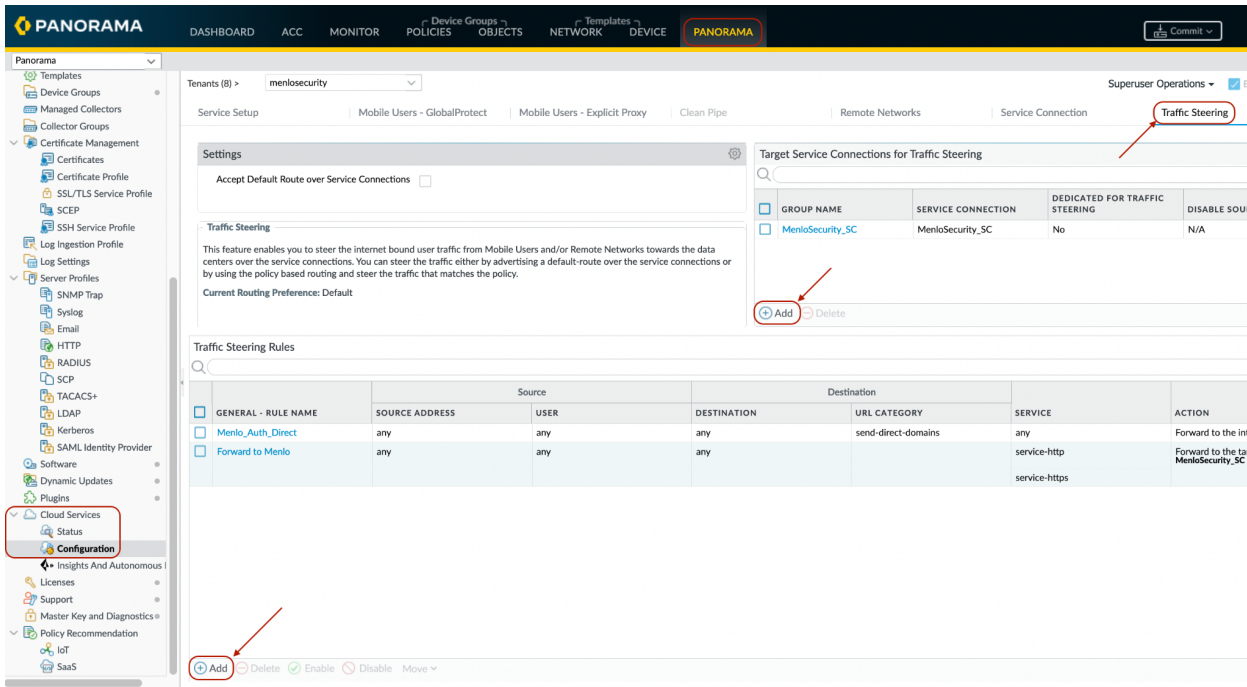
OK

Cancel

Step 3: Setup Traffic Steering Rule

Navigate to

Panorama > Cloud Services > Configuration > Traffic Steering > click Add under Traffic Steering Rules



Tenants (8) > menlosecurity

Service Setup | Mobile Users - GlobalProtect | Mobile Users - Explicit Proxy | Clean Pipe | Remote Networks | Service Connection | **Traffic Steering**

Settings

Accept Default Route over Service Connections ☐

Traffic Steering

This feature enables you to steer the internet bound user traffic from Mobile Users and/or Remote Networks towards the data centers over the service connections. You can steer the traffic either by advertising a default-route over the service connections or by using the policy based routing and steer the traffic that matches the policy.

Current Routing Preference: Default

Target Service Connections for Traffic Steering

GROUP NAME	SERVICE CONNECTION	DEDICATED FOR TRAFFIC STEERING	DISABLE SOURCE NAT
<input type="checkbox"/> MenloSecurity_SC	MenloSecurity_SC	No	N/A

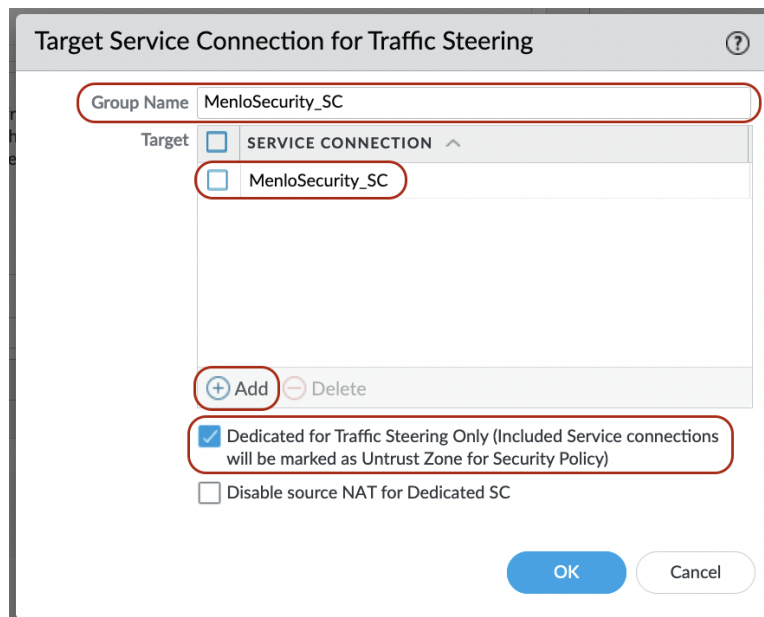
Traffic Steering Rules

GENERAL - RULE NAME	SOURCE ADDRESS	USER	DESTINATION	URL CATEGORY	SERVICE	ACTION
<input type="checkbox"/> MenloAuthDirect	any	any	any	send-direct-domains	any	Forward to the internet
<input type="checkbox"/> Forward to Menlo	any	any	any		service-http	Forward to the target MenloSecurity_SC

Configuration

Add **Delete** **Enable** **Disable** **Move**

Define the Target Service Connection for Traffic Forwarding and reference it in the Traffic Forwarding Rules.



Target Service Connection for Traffic Steering

Group Name: MenloSecurity_SC

Target: ☐ SERVICE CONNECTION ☒ MenloSecurity_SC

Add **Delete**

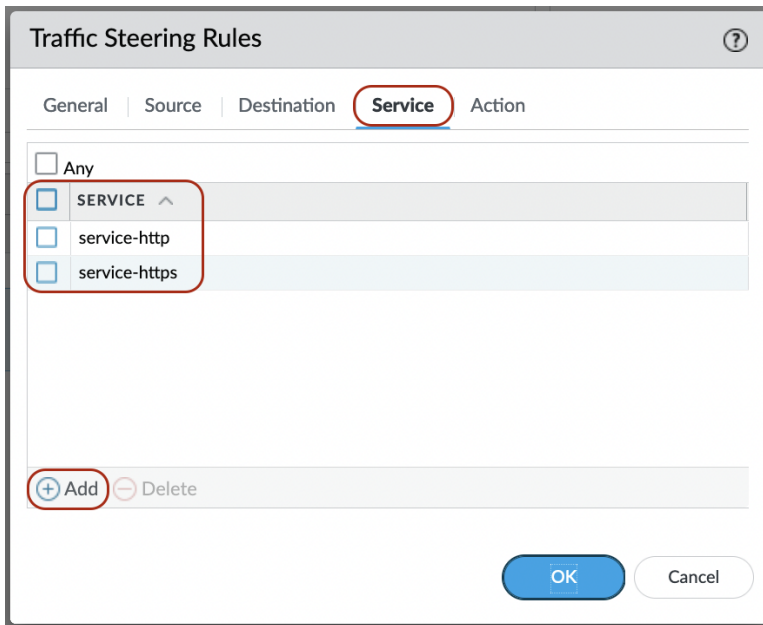
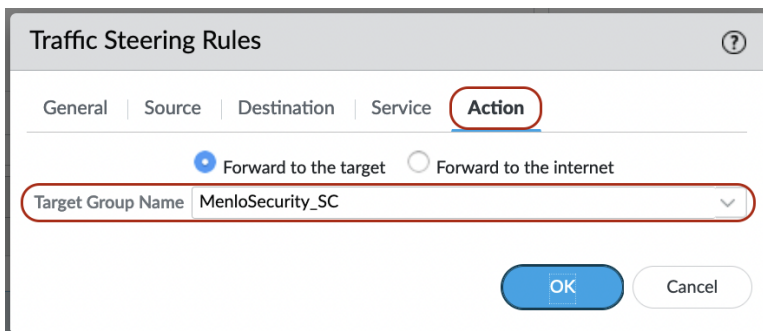
☒ Dedicated for Traffic Steering Only (Included Service connections will be marked as Untrust Zone for Security Policy)

☐ Disable source NAT for Dedicated SC

OK **Cancel**

Set Destination URL to any and Service to service-http and service-https to redirect all web traffic to Menlo Security.

If there are Internet destinations which should not be sent to isolation, such as trusted corporate applications or SAML authentication endpoints, PBF rules may be added to bypass the IPSec tunnel. Add the required destinations to a rule and select “Forward to the Internet” as the action.

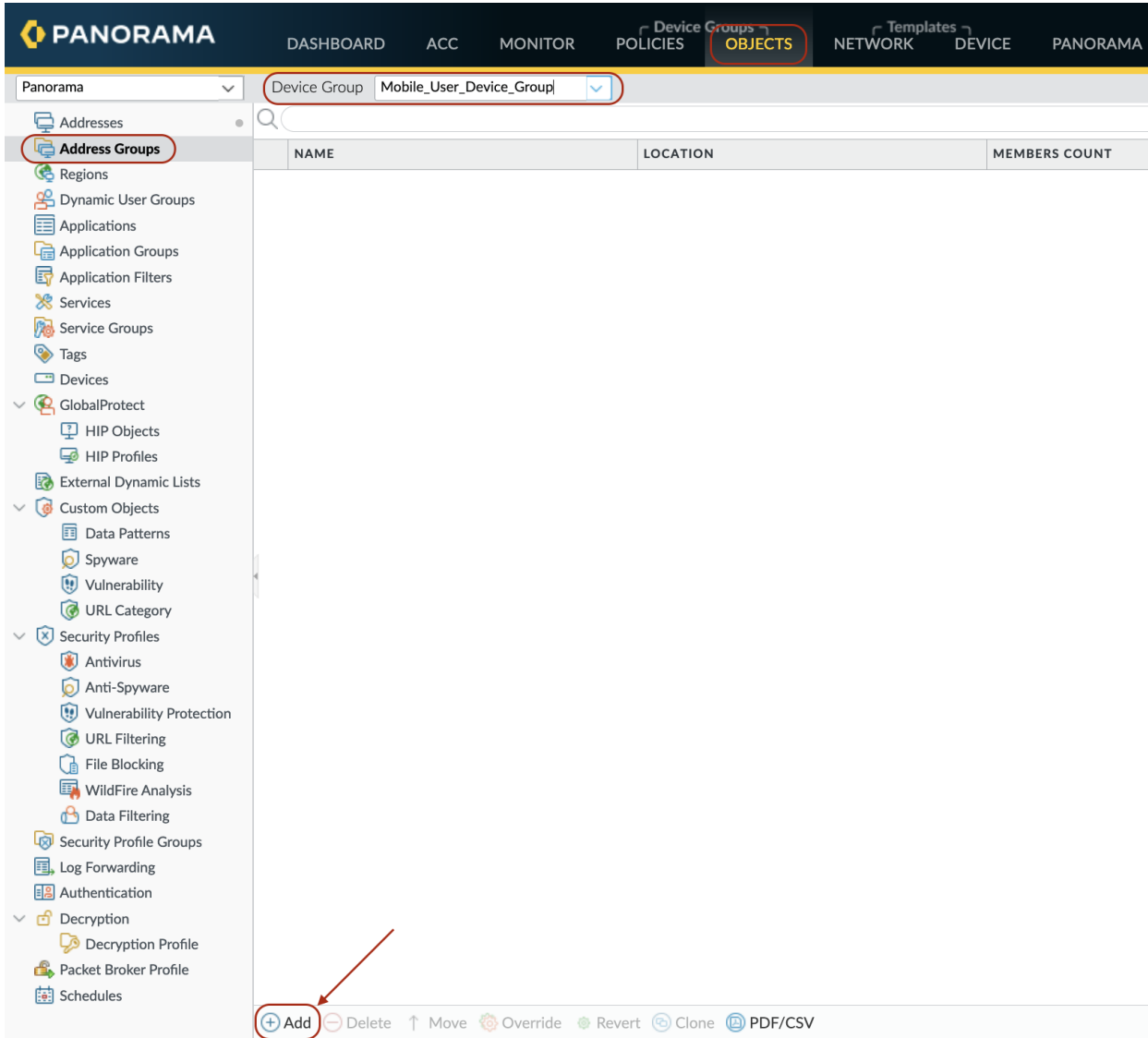



Save / Commit / Push the policy in Prisma to bring up the IPSec tunnel.

Step 4: Setup Policies on Panorama

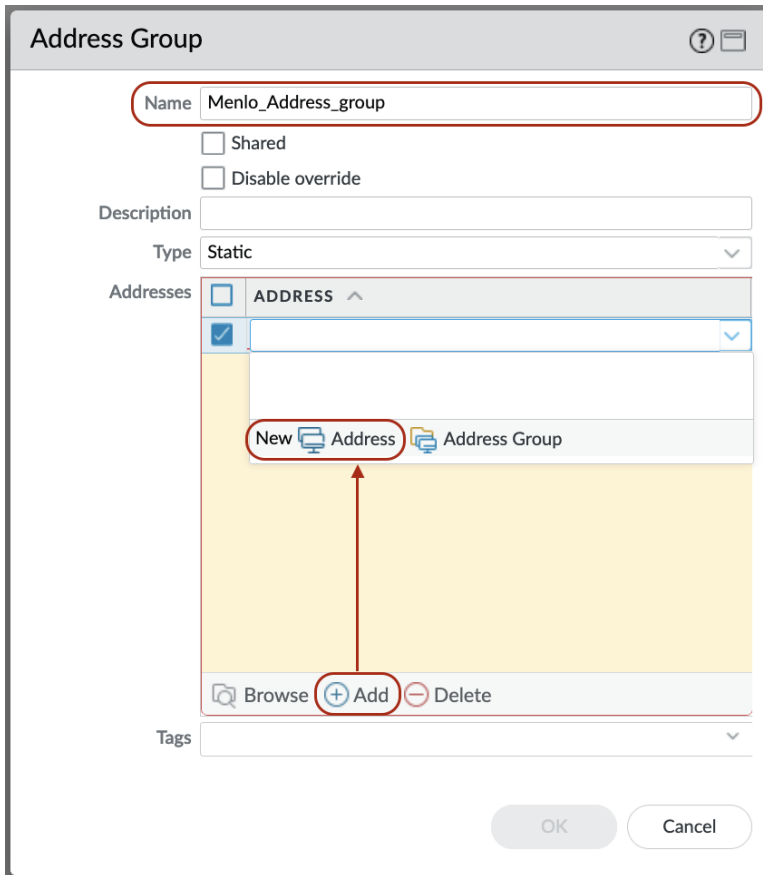
Navigate to:

Objects > Address Groups > under Device Group: Mobile_User_Device_Group > click Add



The screenshot shows the PANORAMA interface with the 'OBJECTS' tab selected. The left sidebar lists various categories, with 'Address Groups' highlighted. The main area displays a table with columns 'NAME', 'LOCATION', and 'MEMBERS COUNT'. At the bottom, a toolbar contains buttons for '+ Add', '- Delete', '↑ Move', '⚙ Override', '↺ Revert', '🔄 Clone', and '📄 PDF/CSV'. A red circle and arrow point to the '+ Add' button.

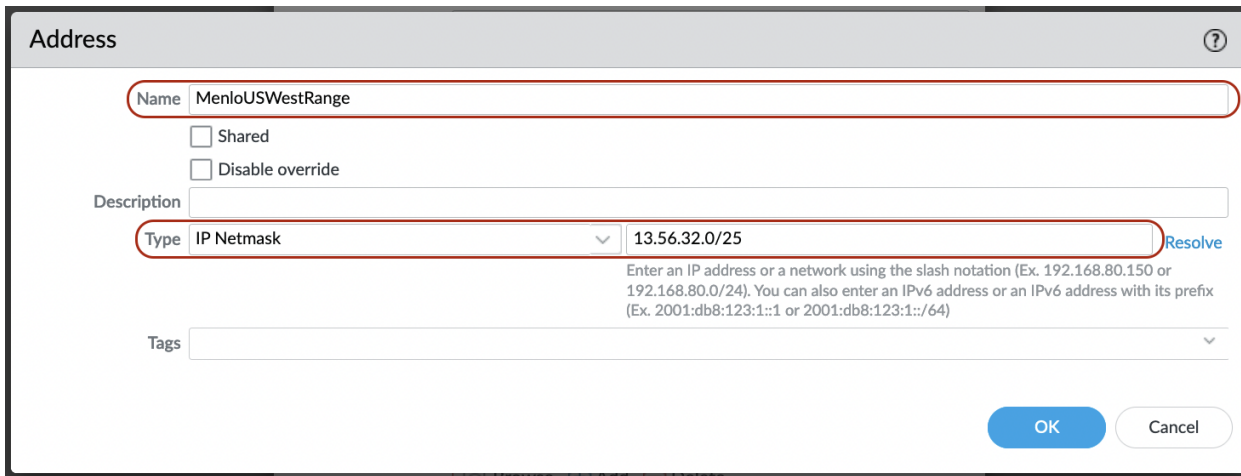
Add an address group Menlo_Address_Group



Add the following Address Ranges to the Group with type IP Netmask:

MenloUSWestRange ip-netmask 13.56.32.0/25
 MenloUSEastRange ip-netmask 34.202.62.128/25
 MenloEUWest1Range ip-netmask 52.215.251.0/25
 MenloEUWest2Range ip-netmask 35.177.154.0/25
 MenloEUCentralRange ip-netmask 52.59.184.0/25
 MenloAPNorthEast1Range ip-netmask 13.115.242.0/25
 MenloAPNorthEast2Range ip-netmask 13.124.145.128/25
 MenloAPSouthEast1Range ip-netmask 13.229.252.0/25
 MenloAPSouthEast2Range ip-netmask 13.210.1.128/25
 MenloAPSouth1Range ip-netmask 13.127.70.0/25
 MenloOhioRange ip-netmask 3.140.202.0/25
 MenloOregonRange ip-netmask 44.242.183.0/25
 MenloCanadaRange ip-netmask 3.97.43.128/25
 MenloBahrainRange ip-netmask 15.184.20.128/25
 MenloSeoulRange ip-netmask 13.124.145.128/25
 MenloHongKongRange ip-netmask 18.162.163.128/2

MenloParisRange ip-netmask 15.188.102.128/25
MenloSaoPauloRange ip-netmask 18.229.37.128/25

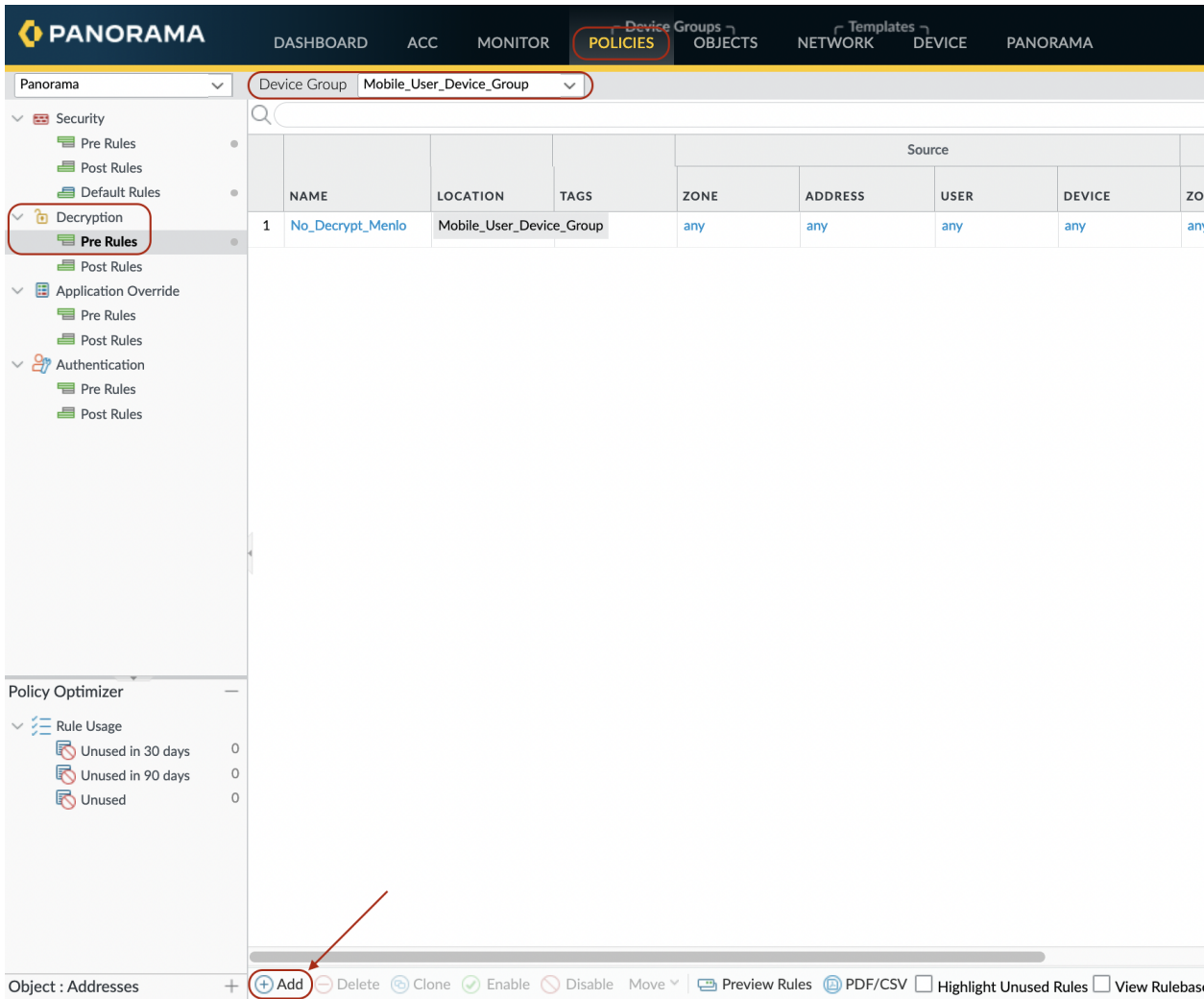


The ranges can be added via GUI or CLI. We recommend adding all regions to account for access from any Prisma location. However, if only exempting local service regions it is recommended to exempt all geographically local regions to account for failover scenarios.

Step 5: Avoid Double Decryption

The Prisma decryption policy can be optionally tuned to reduce unnecessary overhead. To configure a Decryption Policy, Navigate to:

Policies > Decryption > Pre Rules > click Add



PANORAMA

DASHBOARD ACC MONITOR **POLICIES** OBJECTS NETWORK DEVICE PANORAMA

Device Group: Mobile_User_Device_Group

Security

- Pre Rules
- Post Rules
- Default Rules
- Decryption**
 - Pre Rules**
 - Post Rules
- Application Override
 - Pre Rules
 - Post Rules
- Authentication
 - Pre Rules
 - Post Rules

Policy Optimizer

- Rule Usage
 - Unused in 30 days: 0
 - Unused in 90 days: 0
 - Unused: 0

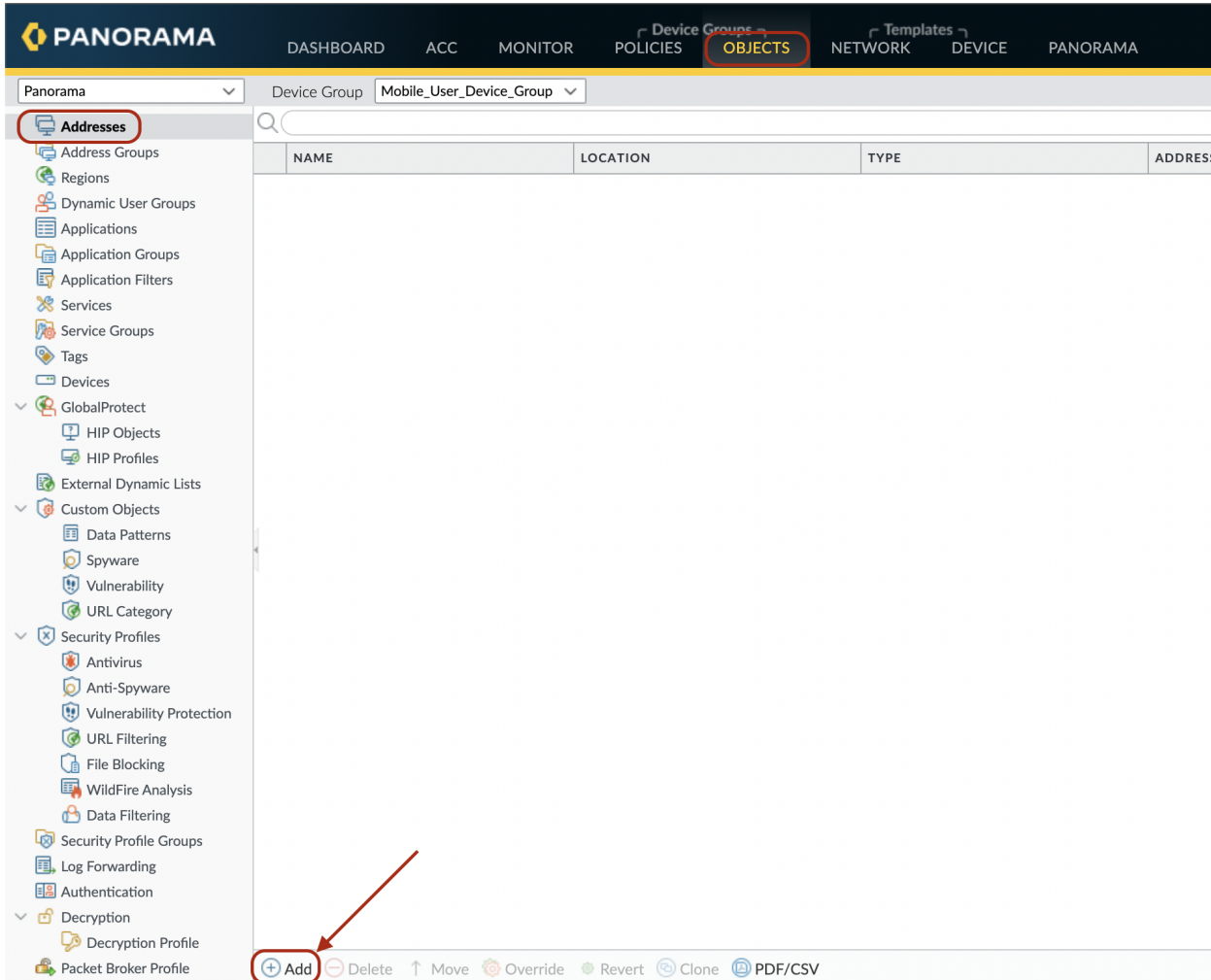
	NAME	LOCATION	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE
1	No_Decrypt_Menlo	Mobile_User_Device_Group		any	any	any	any	any

Object : Addresses + Add Delete Clone Enable Disable Move Preview Rules PDF/CSV Highlight Unused Rules View Rulebase

To disable decryption of traffic destined to Menlo Security isolation service addresses using the Address Group Menlo_Address. These addresses are used exclusively for isolated site rendering, which is the Menlo Security “ACR” protocol containing visual display information, mouse moves, scroll events, etc.

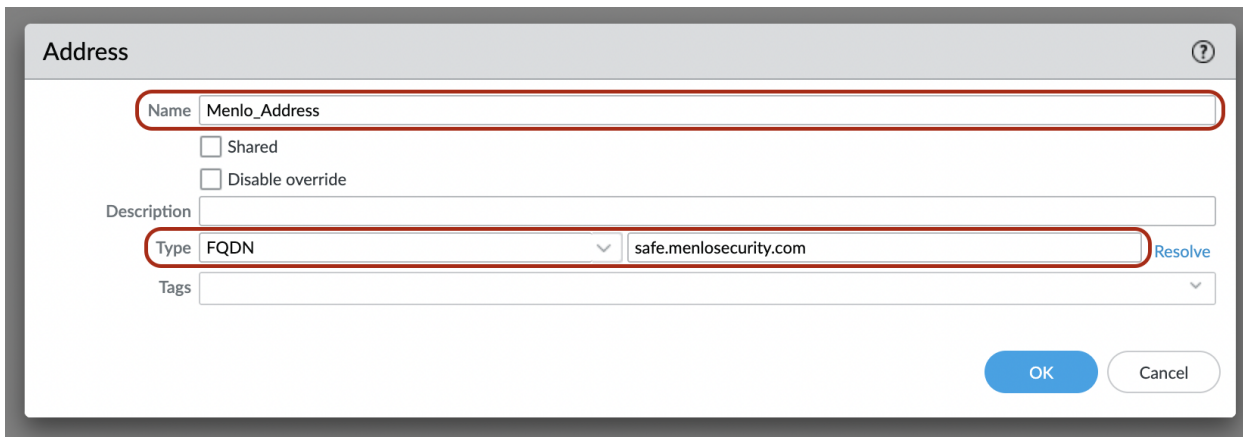
Note that “inspectable” events, such as file uploads or downloads via isolated sites, use different IP ranges which are not included in the exempted service ranges. The result of this configuration is that decryption is not performed on the majority of requests since they don’t contain data relevant to inspection, but file transfers remain visible to Prisma policy enforcement.

Navigate to Objects > Addresses under the Mobile Users Device Group > Add



The screenshot shows the PANORAMA interface with the 'OBJECTS' tab selected. The left sidebar lists various configuration categories, including 'Addresses'. The main area displays a table with columns: NAME, LOCATION, TYPE, and ADDRESS. At the bottom of the main area, there is a toolbar with buttons: '+ Add', '- Delete', '↑ Move', '⚙ Override', '↺ Revert', '🔄 Clone', and '📄 PDF/CSV'. A red circle highlights the '+ Add' button, with a red arrow pointing to it.

Provide a name and add a new type FQDN object with address safe.menlosecurity.com



The 'Address' configuration dialog box is shown. It has a title bar with a question mark icon. The 'Name' field is set to 'Menlo_Address'. There are checkboxes for 'Shared' and 'Disable override'. The 'Description' field is empty. The 'Type' dropdown is set to 'FQDN'. The address field contains 'safe.menlosecurity.com' with a 'Resolve' link next to it. The 'Tags' field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

Commit and Push all the configurations.

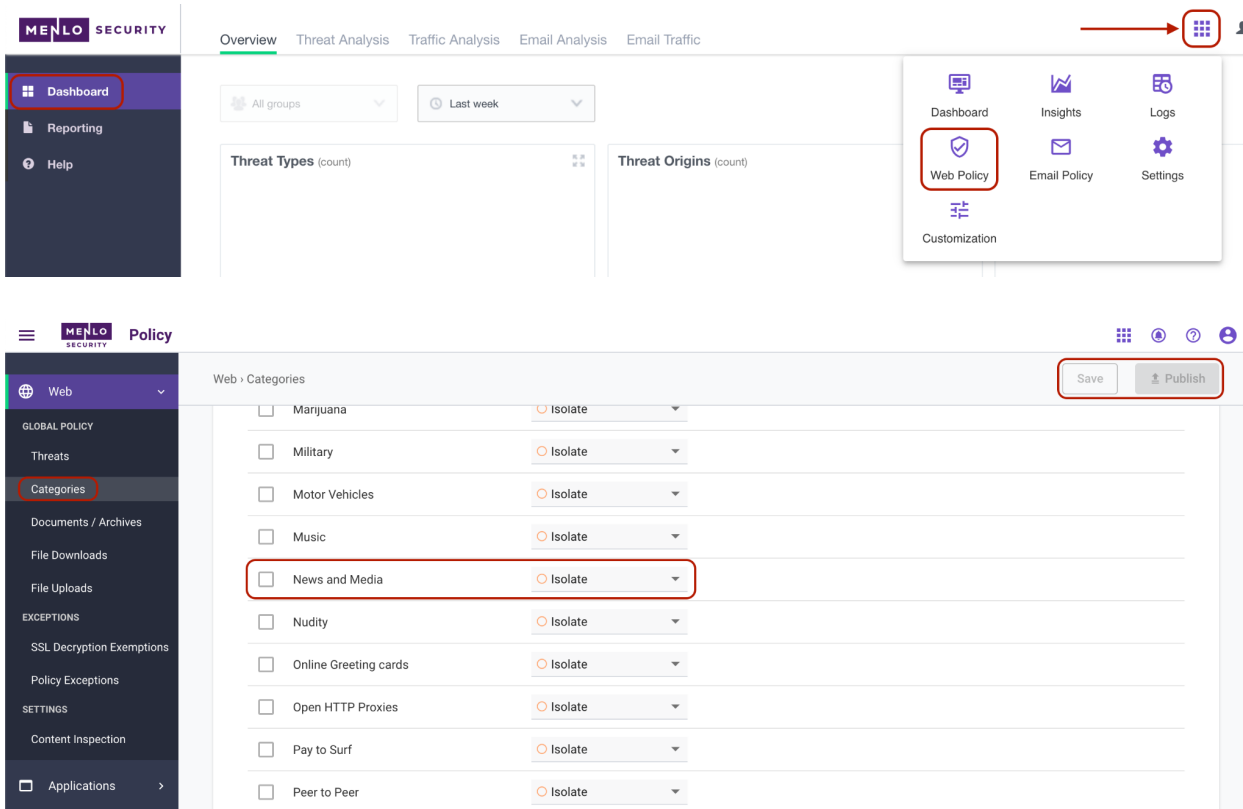
Menlo Security Product Configuration

Step 1: Configure the “Isolate” action for the desired URL Categories in the Menlo Security portal

Ensure that the categories are set to “Isolate” on Menlo Security.

Login into the Menlo Security portal (admin.menlosecurity.com) with the account credentials.

Navigate to Web Policy > Categories > change the action for the selected Category to “Isolate”



The first screenshot shows the Menlo Security portal dashboard. The 'Web Policy' menu item is highlighted in the left sidebar. The top navigation bar includes 'Overview', 'Threat Analysis', 'Traffic Analysis', 'Email Analysis', and 'Email Traffic'. The 'Web Policy' dropdown menu is open, showing options like 'Dashboard', 'Insights', 'Logs', 'Web Policy', 'Email Policy', 'Settings', and 'Customization'. The 'Web Policy' option is highlighted.

The second screenshot shows the 'Web Policy' configuration page. The 'Categories' tab is selected in the left sidebar. The 'Web Policy' page shows a list of categories with their corresponding actions. The 'News and Media' category is highlighted, and its action is set to 'Isolate'. The 'Save' and 'Publish' buttons are visible at the top right of the configuration area.

For the policy to apply, ensure that the web policy is saved and published

Step 2 : Load the Menlo certificate used for SSL decryption on the end-hosts

In order to avoid the end-user receiving certificate warnings in the browser, the Menlo Security CA certificate should be install on all the hosts. The Menlo Security certificate can be downloaded from here:

<https://csportal.menlosecurity.com/hc/en-us> (direct link to article)

The certificate can be installed on the end-hosts by the standard desired methods (eg: via Active Directory)

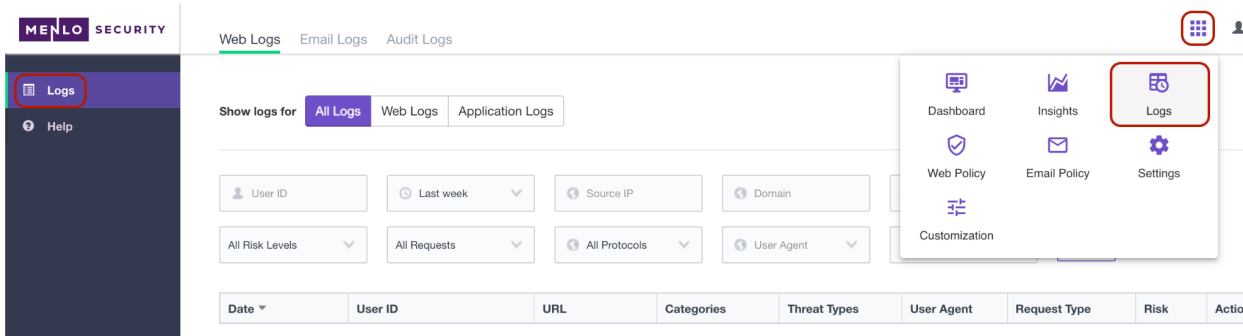
Troubleshooting

In case of issues, the traffic should be tracked step by step, first by checking if Prisma Access is applying the expected action to the desired traffic. We can verify this by looking into the URL Filtering logs under the Monitor tab in Panorama:



GENERATE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION	HEADERS INSERTED
01/08 13:57:38	menlo_cars	menlo_cars,motor-vehicles,low-risk	www.fat.com/	trust	untrust	192.168.10.4	user1		23.201.218.48			web-browsing	block-overide	

The next place to check would be in the Menlo Security platform logs to confirm that the traffic is Isolated as expected:



The screenshot shows the Menlo Security interface with the 'Logs' tab selected. The 'Web Logs' section is active, and the 'Show logs for' dropdown is set to 'All Logs'. The interface includes filters for User ID, Last week, Source IP, Domain, All Risk Levels, All Requests, All Protocols, and User Agent. A sidebar menu on the left shows 'Logs' and 'Help' options. A top navigation bar includes 'Web Logs', 'Email Logs', and 'Audit Logs'. A right-hand menu contains icons for Dashboard, Insights, Logs, Web Policy, Email Policy, Settings, and Customization. The main log table has columns: Date, User ID, URL, Categories, Threat Types, User Agent, Request Type, Risk, and Action.

Technical Details

- If applicable, list the names of API calls that are being leveraged.
- If this is a syslog integration, list out the types of log(s) being used (traffic, threat, HIP Match, config, system, endpoint agent logs, etc.).
- List out any additional technical details on how the two technologies integrate.