# Palo Alto Prisma Access: Panorama Managed Integration Guide

## Revision History

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to: Menlo Cloud</td>
<td>2</td>
</tr>
<tr>
<td>Version Information: 2.86</td>
<td>2</td>
</tr>
<tr>
<td>Date Updated: October 2022</td>
<td>2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Challenge</td>
<td>3</td>
</tr>
<tr>
<td>Solution</td>
<td>3</td>
</tr>
<tr>
<td>Protecting High Risk Users and Applications</td>
<td>3</td>
</tr>
<tr>
<td>Challenge</td>
<td>3</td>
</tr>
<tr>
<td>Solution</td>
<td>3</td>
</tr>
</tbody>
</table>

## Integration Benefits

<table>
<thead>
<tr>
<th>Integration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Benefits</td>
<td>4</td>
</tr>
</tbody>
</table>

## Integration Diagram

<table>
<thead>
<tr>
<th>Diagram</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Diagram</td>
<td>4</td>
</tr>
</tbody>
</table>

## Before You Begin

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palo Alto Networks Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Method 1a. Block action with custom Block Page response</td>
<td>5</td>
</tr>
<tr>
<td>Method 1b. Override action for redirection to isolation</td>
<td>12</td>
</tr>
<tr>
<td>Configuration For both Block and Override modes</td>
<td>19</td>
</tr>
<tr>
<td>Method 2. Transparent Proxy with Prisma Access</td>
<td>26</td>
</tr>
</tbody>
</table>

## Menlo Security Product Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menlo Security Product Configuration</td>
<td>46</td>
</tr>
</tbody>
</table>

## Troubleshooting

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting</td>
<td>47</td>
</tr>
</tbody>
</table>

## Technical Details

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Details</td>
<td>47</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Release</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.86</td>
<td>October 2022</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>
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
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
Create new URL Filtering profile under Actions tab

Navigate to:

Actions tab > Profile Type > select Profiles

URL Filtering > click the drop down field > select New URL Filtering
Step 2: Create URL filtering profile to block

1. Create a new URL filtering profile.
2. Name the profile as "Menlo-Sec".
3. Description: Categories to be redirected to Menlo Security for Web Isolation.
4. Select the "gambling" category and set the action to "block".
5. Save the URL filtering profile.
Step 3: Upload custom block page

Navigate to:
Device > Response Pages > under Template: Mobile_User_Template > select “URL Filtering and Category Match Block 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(prepended);
    
// window.location.replace('https://safe.menlosecurity.com')
</script>

<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>
</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
Create new URL Filtering profile under Actions tab

Navigate to:

Actions tab > Profile Type > select Profiles

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

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

Provide a name and add a new type FQDN object with the address safe.menlosecurity.com
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):
### Decryption Policy Rule

**General**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service/URL Category</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>No_Decrypt_Menlo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tags</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Rules By Tag</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Comment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source**

<table>
<thead>
<tr>
<th>Any</th>
<th>SOURCE ZONE</th>
<th>SOURCE ADDRESS</th>
<th>SOURCE USER</th>
<th>SOURCE DEVICE</th>
</tr>
</thead>
</table>

**Options**

<table>
<thead>
<tr>
<th>Add</th>
<th>Delete</th>
<th>Add</th>
<th>Delete</th>
<th>Add</th>
<th>Delete</th>
<th>Add</th>
<th>Delete</th>
<th>Add</th>
<th>Delete</th>
</tr>
</thead>
</table>

Negate

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.
Welcome to BBC.com

Pfizer vaccine is '94% effective in over-65s'
The jab works equally well in people of all ages and ethnicities, further data suggests.

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 RBC 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.
Provide the service IP address to Menlo Security support (https://cspatial.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

<table>
<thead>
<tr>
<th>CONNECTION NAME</th>
<th>ENCRYPTION</th>
<th>AUTHENTICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE-Crypto-Default</td>
<td>aes-256-cbc</td>
<td>sha512</td>
</tr>
<tr>
<td>Crypto-Default</td>
<td>aes-256-cbc</td>
<td>sha256</td>
</tr>
<tr>
<td>E-Crypto-Default</td>
<td>aes-256-cbc</td>
<td>sha512</td>
</tr>
<tr>
<td>E-Crypto-Default</td>
<td>aes-256-cbc, aes-192-cbc, aes-128-cbc</td>
<td>sha512, sha384, sha256, sha1</td>
</tr>
<tr>
<td>Crypto-Default</td>
<td>aes-256-cbc, 3des, des</td>
<td>sha512, sha384, sha256, sha1, md5</td>
</tr>
</tbody>
</table>
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
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
In the IKE Gateway pop-up, fill-in the highlighted fields.
If they are not already created, new variables (FQDN) will need to be added for the Peer Address, Local Identification, and Peer Identification.
Navigate to:
Network > IPSec Tunnels > click Add
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.
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.
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.
Step 3: Setup Traffic Steering Rule
Navigate to Panorama > Cloud Services > Configuration > Traffic Steering > click Add under Traffic Steering Rules
Define the Target Service Connection for Traffic Forwarding and reference it in the Traffic Forwarding Rules.

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.

```
Traffic Steering Rules

<table>
<thead>
<tr>
<th>General</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Any</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SERVICE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>service-http</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>service-https</td>
<td></td>
</tr>
</tbody>
</table>
```

Add or delete as required. Select OK. 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
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
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
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
Provide a name and add a new type FQDN object with address safe.menlosecurity.com

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”

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:

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

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.