Palo Alto Prisma Access: Cloud Managed Integration Guide

| 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 integration method | 6 |
| Method 1B. Override action Integration method | 10 |
| Configuration for both Block and Override modes | 13 |
| Method 2. Transparent redirection with Prisma Access Traffic Steering | 16 |
| Common Steps for all integration methods | 25 |
| Menlo Security Configuration | 29 |
| Troubleshooting | 30 |
## 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 later 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

The configuration details are covered below.
Method 1A. Block action integration method

Step 1: Set the desired URL Filtering Category to Block

Log into the Prisma Access Cloud Management portal, and navigate to Manage > Configuration > URL Access Management > select “Mobile Users” context > Access Control tab > under URL Access Management Profiles, click Add Profile

Add a new URL Access Management Profile or edit an existing one (a similar Profile can be defined for the Remote Networks).

For the URL Categories that need to be redirected to Menlo Security for Web Isolation, set the Site Access to “Block”; the same access can be set for Custom URL Categories if needed:
Step 2: Upload a custom Block Response Page

The custom Block Response Page has the role of prepending “safe.menlosecurity.com” in front of the original URL requested by the user, once that URL matches the URL Category we want to send through isolation.
Under URL Access Management > Settings, upload the custom Block Response page under the “URL Access Management Block Page”

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

Please continue with Step 3 as the configuration is similar for both methods from that point on.
<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>
</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></p>
</div>
</body>
</html>
Method 1B. Override action Integration method

Step 1: Set the desired URL Filtering Category to Override

Log into the Prisma Access Cloud Management portal, and navigate to:
Manage > Configuration > URL Access Management

Under the Mobile Users context, add a new URL Access Management Profile or edit an existing one (a similar Profile can be defined for the Remote Networks)

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

Click Save to accept changes.
Step 2: Set the destination address to be used for the Override action

Under the same URL Access management tab, navigate to Settings > URL Admin Overrides and click “Add URL Admin Overrides”
In the URL Admin Override pane, click Add. In the URL Admin Override window, fill in the form fields with the following values:

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

Continue with Step 3 as the configuration is similar for both methods from that point on.
Configuration for both Block and Override modes

Step 3: Update the policy handling the Internet-bound traffic with the previously created URL Access Management profile

Navigate to Configuration > Profile Groups > select the Mobile Users context
Add or edit an existing Profile Group using the previously configured URL Access Management Profile.
Navigate to Security Policy > under Mobile Users > Rulebase tab, and add or edit the existing policy; if the intent is to enforce the web isolation for a particular set of users, add the proper users under the Source tab.

Under the Service Entities set the services as “Any Service” (don’t use the “application-default” as the redirection may involve non-standard ports)
Under the Action and Advanced Inspection section, select the Allow option. Under the Profile Group, select the Profile Group defined in the previous step.

Click Save to accept changes. Then, click Push Config button and Push to apply changes.

Continue with the Common Step 4 and Step 5 further in the document.
Method 2. Transparent redirection with Prisma Access Traffic Steering

Step 1: Configure an IPSEC Tunnel connecting to the Menlo Security cloud

Contact Menlo Security and request the provisioning of an IPSEC tunnel pair. Obtain the below information from Menlo Security for each tunnel to setup the IPSEC tunnels on the Prisma Access side:

- Gateway IP address
- Pre-Shared Key
- Peer Identifiers
- Tunnel IP Address

Note - Ensure that the IP address of the Service Connection (available in Step 3) is specified on the tunnel setup on Menlo Security, so that it can accept the connection

Navigate to Manage > Service Setup > Service Connections and create a new Service Connection that will link the Prisma Access instance to the Menlo Security Isolation cloud.

Select a Prisma Access Region and Location as close as possible to the majority of the users that will be redirected to Menlo Security. If the users are geographically dispersed, multiple Service Connections would be recommended for a better user experience.
Step 2: Select the proper IKE crypto and IPSEC crypto settings
Under the Primary Tunnel Setup menu, use the settings captured below as an example:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Name</td>
<td>Menlo_W_Primary</td>
</tr>
<tr>
<td>Branch Device Type</td>
<td>Other Devices</td>
</tr>
<tr>
<td>Authentication</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>............................</td>
</tr>
<tr>
<td>Confirm Pre-Shared Key</td>
<td>............................</td>
</tr>
<tr>
<td>IKE Local Identification</td>
<td>FQDN (hostname)</td>
</tr>
<tr>
<td>IKE Peer Identification</td>
<td>FQDN (hostname)</td>
</tr>
<tr>
<td>Branch Device IP Address</td>
<td>Static IP</td>
</tr>
<tr>
<td>Static IP</td>
<td>54.</td>
</tr>
<tr>
<td>IKE Passive Mode</td>
<td></td>
</tr>
<tr>
<td>Turn on Tunnel Monitoring</td>
<td></td>
</tr>
<tr>
<td>Destination IP</td>
<td>169.254.10.10</td>
</tr>
</tbody>
</table>
Under the IKE Advanced Options select the following combinations:

**IKE Advanced Options**

<table>
<thead>
<tr>
<th>Selection Menu</th>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE Protocol Version</td>
<td></td>
<td>IKEv2 only mode</td>
</tr>
<tr>
<td>IKEv2 Crypto Profile</td>
<td></td>
<td>Menlo_Security_IKE</td>
</tr>
<tr>
<td>Edit Menlo_Security_IKE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td>Menlo_Security_IKE</td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td>aes-128-cbc</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>sha256</td>
</tr>
<tr>
<td>DH Group</td>
<td></td>
<td>group19</td>
</tr>
<tr>
<td>Lifetime</td>
<td></td>
<td>8 Hours</td>
</tr>
<tr>
<td>IKEv2 Authentication Multiple</td>
<td></td>
<td>0 &lt;= 50</td>
</tr>
</tbody>
</table>

© 2022 / Menlo Security, Inc. All rights reserved. | Confidential/Internal
Under the IPSEC advanced setting, select the following combination:

**IPSec Advanced Options**

- IPSec Crypto Profile
  - Menlo_Security_IPSec
  - Create New
  - Manage

- Anti Replay

- Copy ToS

- Enable GRE Encapsulation

[Back]

[Cancel] [Save]
Push the new configuration to accept changes.

Once the Service Connection is created, a dedicated Public IP will get assigned; this will be the IPSEC tunnel endpoint on the Prisma Access side; this IP can be seen under the Service IP column and will be required to be shared with Menlo Security.
NOTE: The IP in the picture below is only one random example.

Once the IPSEC tunnel is provisioned by Menlo Security as well, validate that the Tunnel status turns into the Green/OK state (please see the picture above)

**Repeat the tunnel creation process for the Secondary Tunnel**

For high availability, fault tolerance, and seamless service upgrades, please configure the Prisma Secondary Tunnel in the service connection. The secondary tunnel will use new addresses, peer identifiers, and pre-shared keys, which are supplied by Menlo Security Support. But, the secondary tunnel will use the same Prisma Service Connection IP Address.
Step 3: Configure the Traffic Steering rules to select what traffic is required for Isolation

Under the same Service Connections menu, select the Advanced Settings tab:

Under the Traffic Steering menu, create a new Traffic Forwarding rule:
Select the matching criteria for the traffic that needs to be transparently redirected through Isolation; typically the criteria are a combination of selected users and/or URL Categories.

Edit Menlo RBI

Name
Menlo RBI

Source
User Entities
Match Any User

Source Address Entities
any

Destination
Destination Address Entities
any

URL Category

URL Category
Menlo Service Domains  social-networking  Isolated Domains  unknown

Service
Service

Services
service-http  service-https

Action
○ Forward to the target  ○ Forward to the Internet

Target Service Connection Group
Menlo RBI

Create New  Manage  Save
Custom URL Categories

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Menlo Service Domains</td>
<td></td>
</tr>
</tbody>
</table>

**Custom URL Category**

- **Type**: URL List
- **Matches any of the following URLs, domains or host names.**

Enter one entry per row. Each entry may be of the form `www.example.com` or it could have wildcards like `www.*.com`.

Please note that one of the redirected URL Categories is a custom URL Category that we named “Menlo Service Domains” and contains a wildcard for any URLs under the menlosecurity.com domain.

Push the new configuration to accept changes.
Common Steps for all integration methods

Step 4: Enable SSL decryption for enhancing the URL Categorization rate

Navigate to Configuration > Security Services > Decryption under the Mobile Users context. Create a policy decrypting all the traffic for the required users.
Add the Address object that was created earlier.

Push the new configuration to accept changes.
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.

NOTE: In the case of the Transparent Redirection method, the original URL that is being accessed by the user remains unchanged (no prepend). This makes the user experience in this case totally transparent for the URLs accessed through Isolation.
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 BBC is investigating allegations
Menlo Security Configuration

The first two integration methods are using the “prepend” mode in the Menlo Security solution (prepend safe.menlosecurity.com in front of the original URL). This mode will automatically trigger an Isolate action on the Menlo Security so there is no specific configuration required on the Menlo Security side.

The transparent redirection integration methods leave the original URL that the user is accessing unchanged. For this integration method, ensure that all URL categories and Threat types have the “Isolate” or “Isolate Read-Only” action selected in Menlo Security > Web Policy > Categories / Threats. This policy ensures that any traffic selected by the Prisma forwarding policy will be isolated by the Menlo Security platform.
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 Logs > Firewall/URL logs:

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