Palo Alto Prisma Access: Cloud Managed Integration Guide

November 2024

 © 2024 / Menlo Security, Inc. All rights reserved.

Table of Contents

© 2024 / Menlo Security, Inc. All rights reserved.

1. Revision History

Release	Date	Change
November 2024 (2.90.0.16)	November 2024	Added a note to recommend enabling tunnel monitoring when configuring an IPsec tunnel.
2.86	October 2022	Initial release

 © 2024 / Menlo Security, Inc. All rights reserved.

2. Use Cases for Integration with Palo Alto Prisma Access

2.1. Simplify User Policy Enforcement

Challenge

The internet contains more than four 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 Secure Cloud Browser 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 Secure Cloud Browser. 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.

2.2. 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 Secure Cloud Browser via integration with Prisma Access. This ensures any website the specified user or group accesses is executed within the Menlo Secure Cloud Browser, 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 Secure Cloud Browser 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.

 © 2024 / Menlo Security, Inc. All rights reserved.

2.3. Integration Benefits

Palo Alto Prisma Access and the Menlo Secure Cloud Browser 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.
- Combines the benefits of Palo Alto Prisma Access policy and Isolation.
- Reduces help desk tickets from users whose access to websites has been blocked.

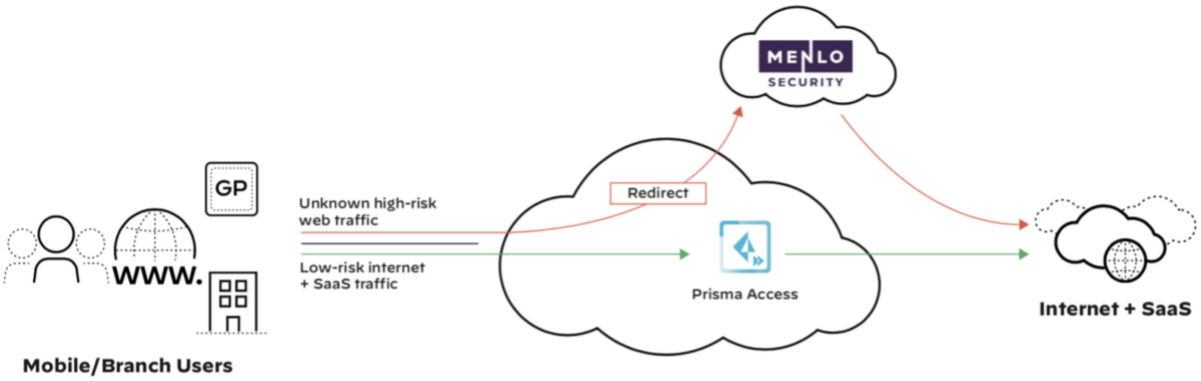


Figure 1: Forwarding of specific traffic to Menlo Security for browser isolation

2.4. Before You Begin

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

- Access to the Prisma Access instance and the Cloud Management portal 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).

 © 2024 / Menlo Security, Inc. All rights reserved.

3. Palo Alto Networks Configuration

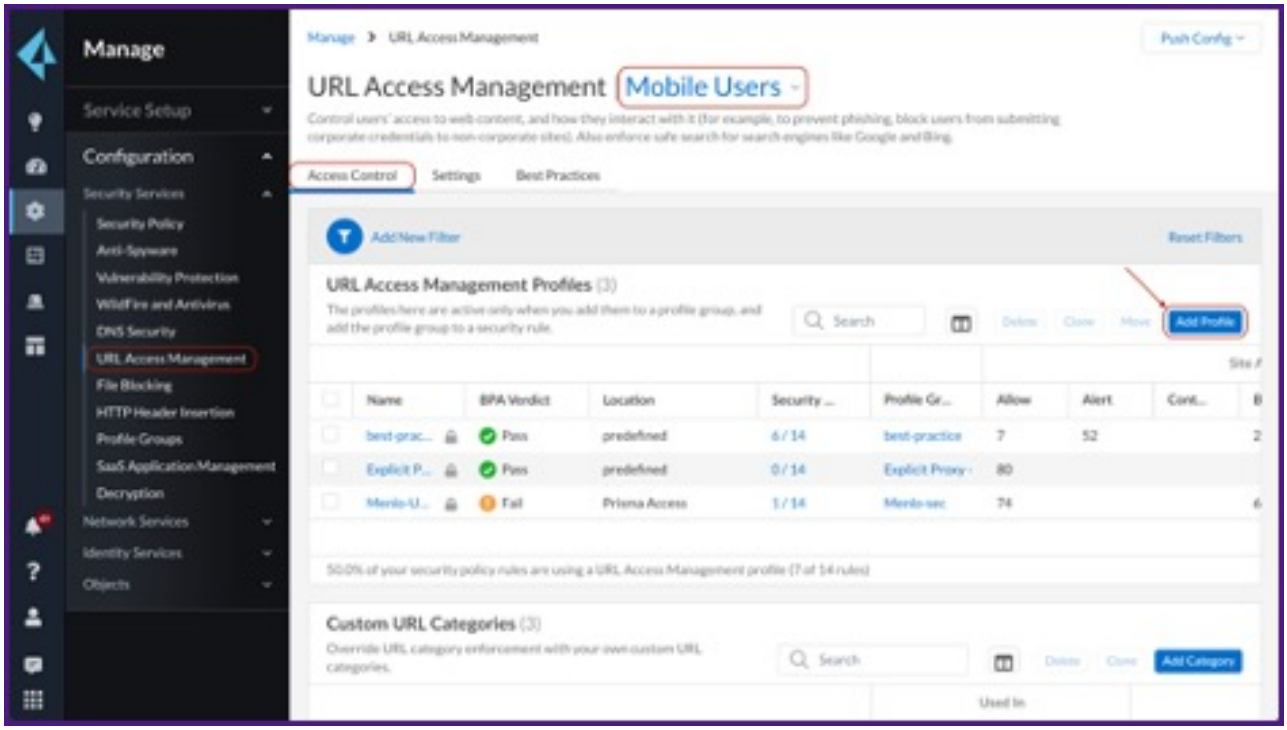
The redirection of the specific traffic that is traversing Prisma Access towards the Menlo Secure Cloud Browser can be achieved in two ways:

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.

3.1. Block action integration method

Step 1: Set the desired URL Filtering Category to Block

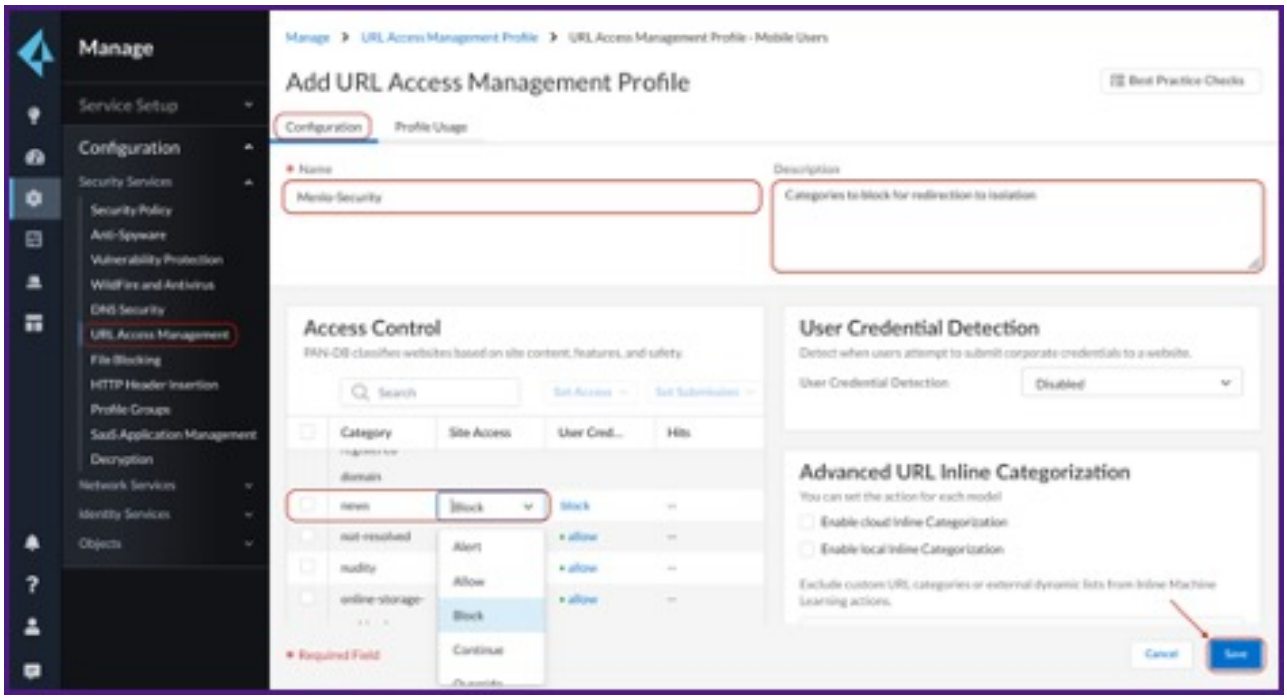
Log into the Prisma Access Cloud Management portal and navigate to *Manage* > *Configuration* > *URL Access Management* > select **Mobile Users** context > *Access Control* tab > under **URL Access Management Profiles**, click **Add Profile**.



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

 © 2024 / Menlo Security, Inc. All rights reserved.

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.

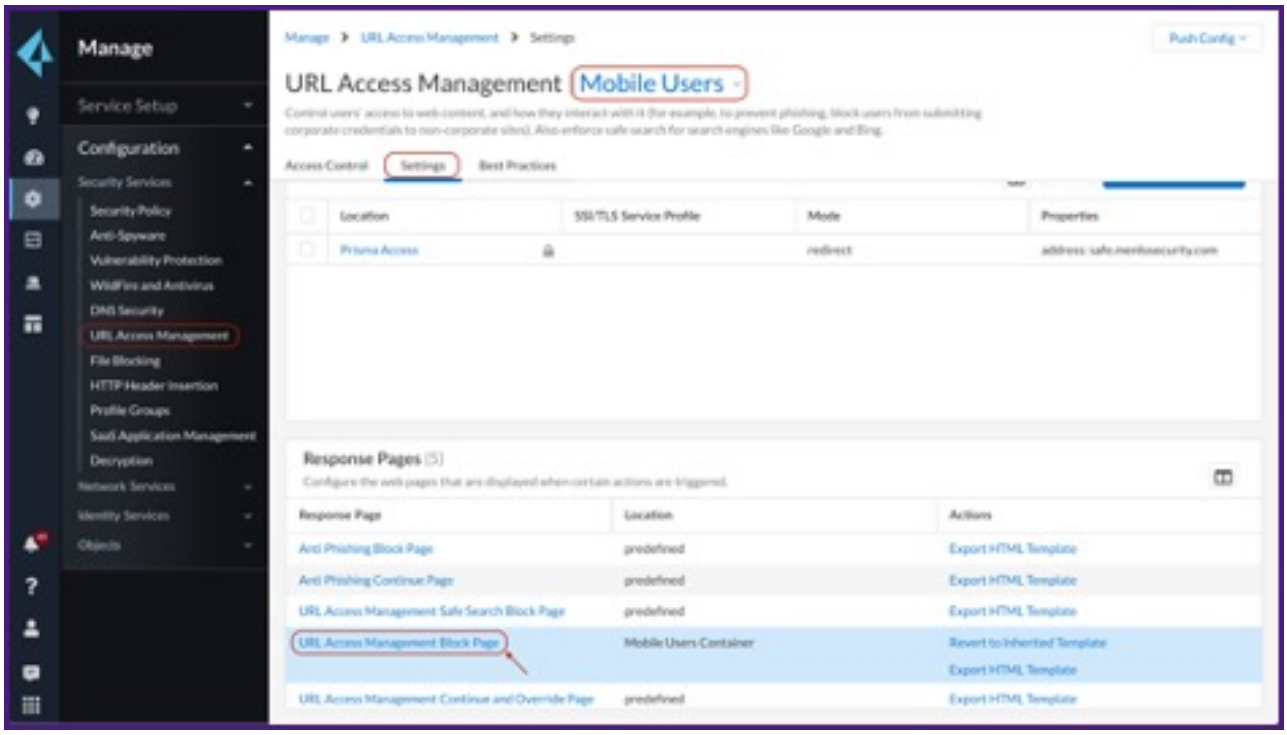


Step 2: Upload a custom Block Response Page

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**.

 © 2024 / Menlo Security, Inc. All rights reserved.



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

Custom Block Response page example:

```
<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;
```

 © 2024 / Menlo Security, Inc. All rights reserved.

```
    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>
</div>
</body>
</html>
```

Please continue with Step 3 as the configuration is similar for both methods from that point on.

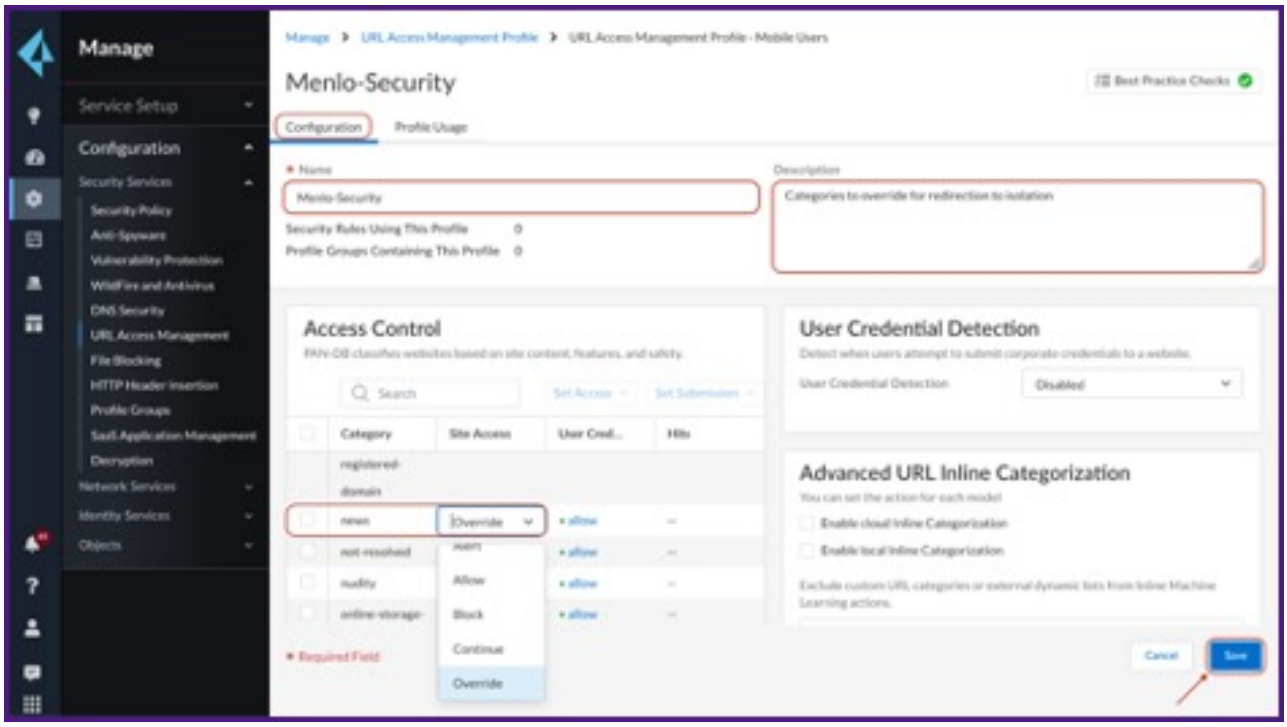
3.2. Override action Integration method

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).

 © 2024 / Menlo Security, Inc. All rights reserved.



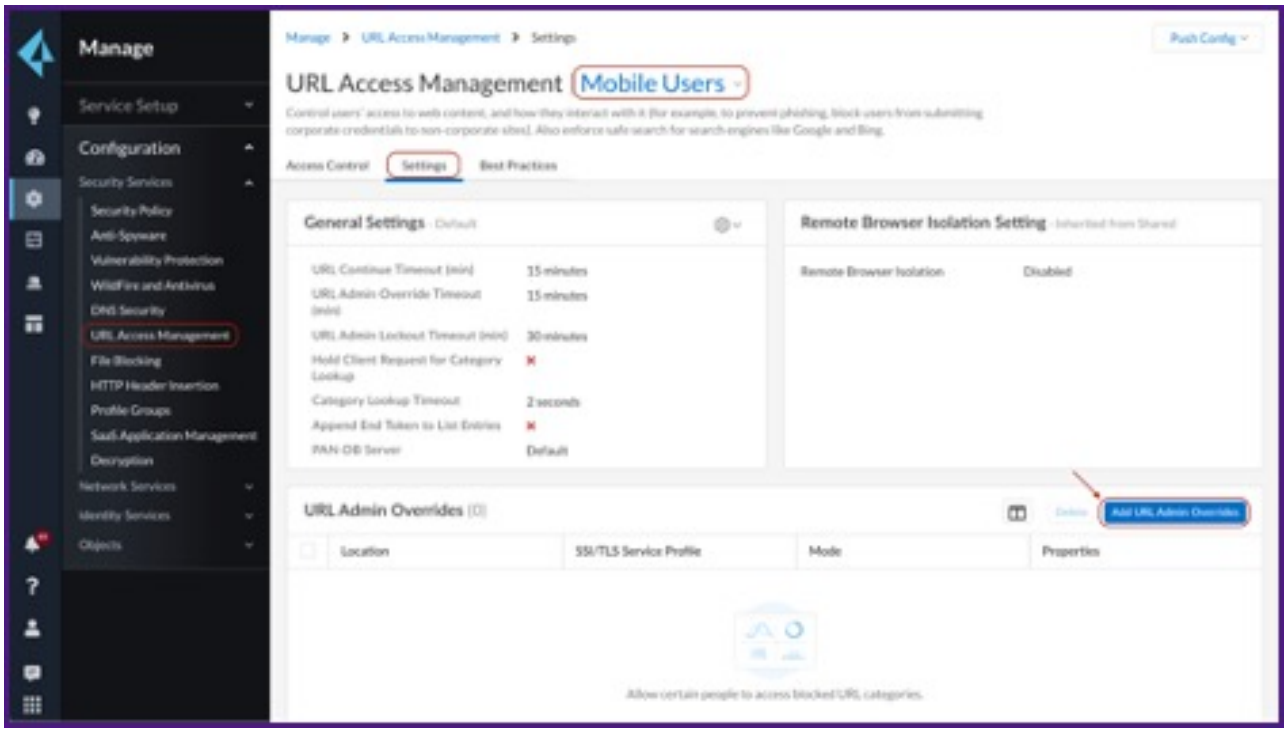
For the URL Categories that need to be redirected to Menlo Security for Web Isolation, set the Site Access to override; the same access can be set for Custom URL Categories if needed.

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**.

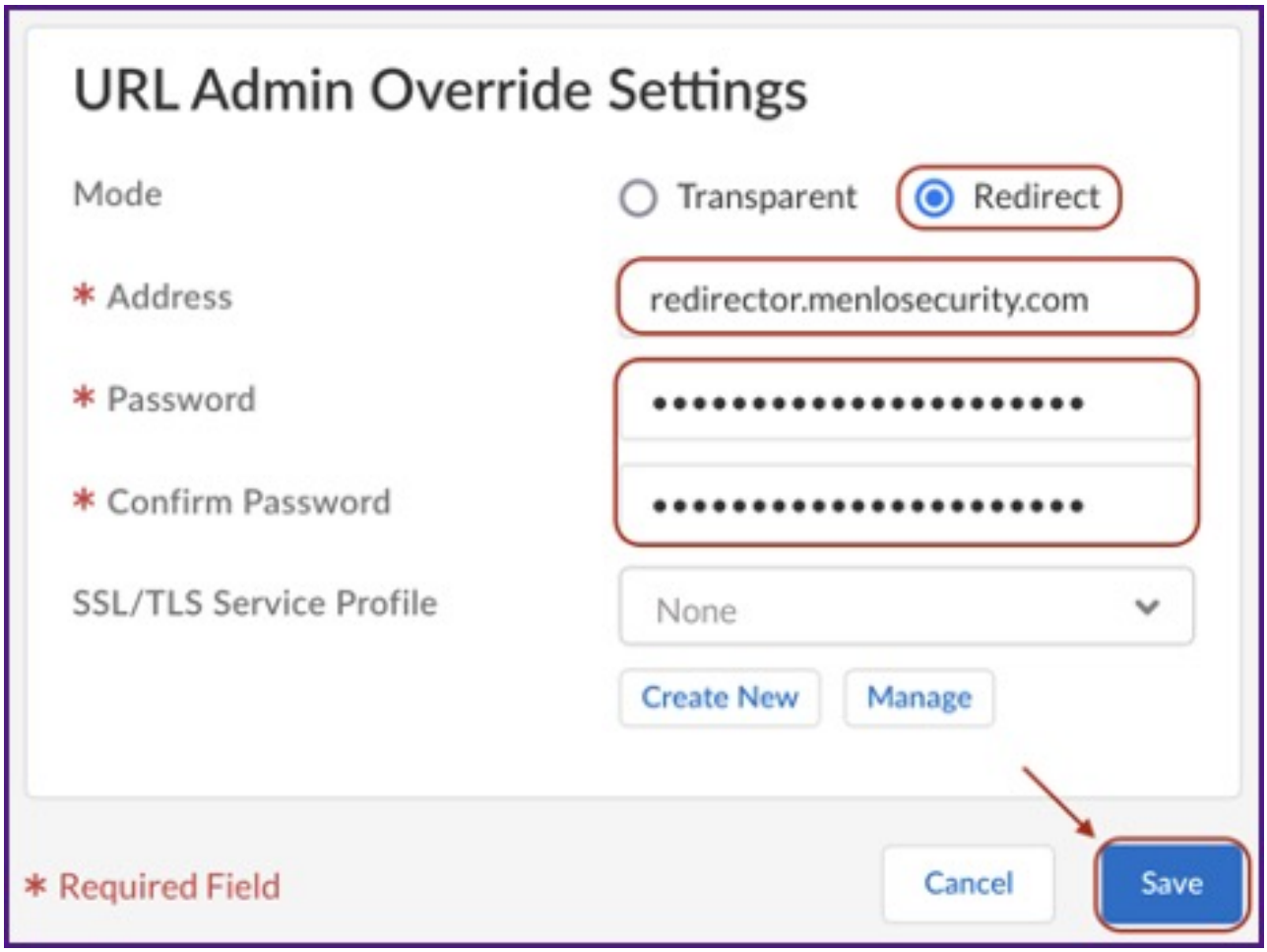
 © 2024 / Menlo Security, Inc. All rights reserved.



In the *URL Admin Override* pane, fill in the form fields with the following values:

- **Mode**: Redirect
- **Address**: redirector.menlosecurity.com
- **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

 © 2024 / Menlo Security, Inc. All rights reserved.



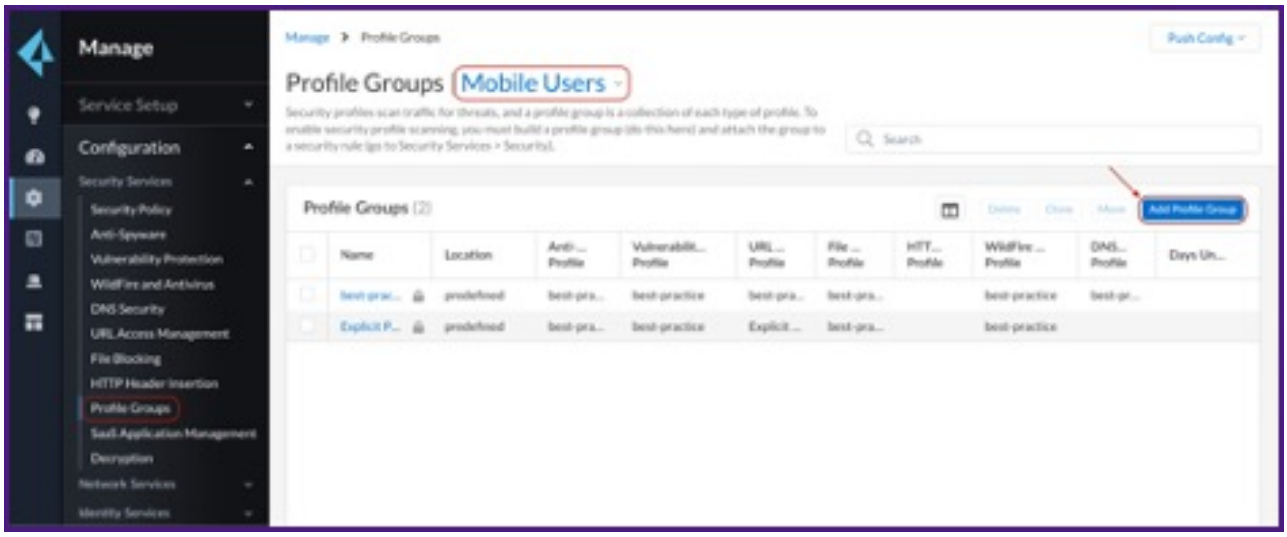
Continue with Step 3 as the configuration is similar for both methods from that point on.

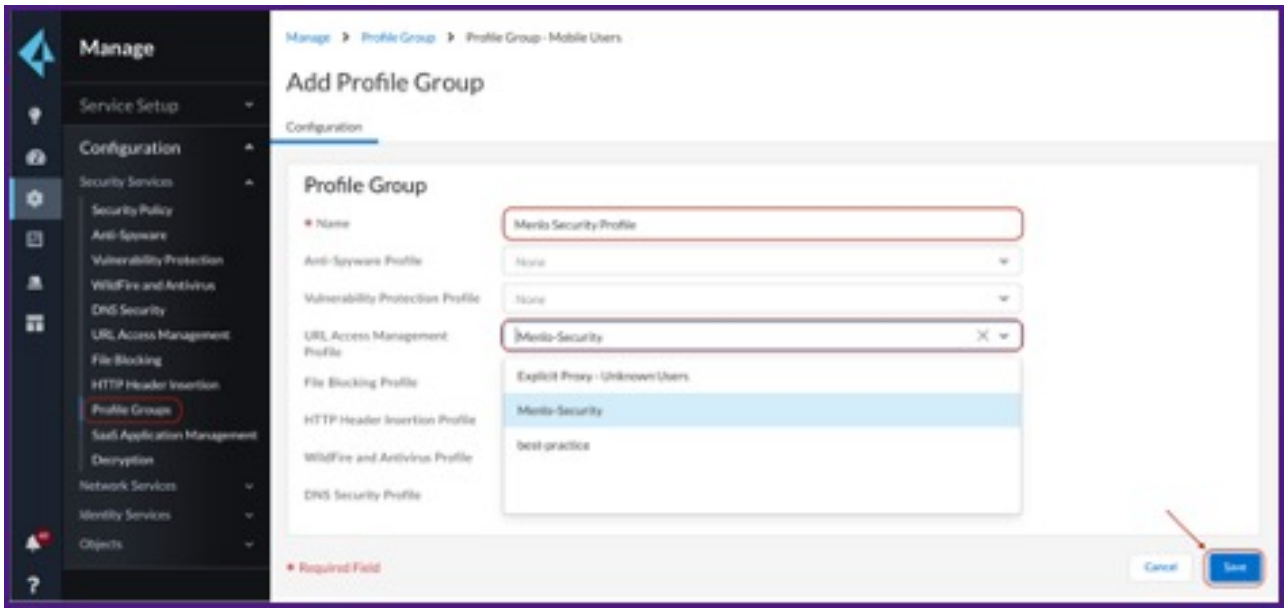
Step 3: Update the policy handling the Internet bound traffic with the previously created URL Access Management profile

Navigate to *Configuration* > *Profile Groups* > select the *Mobile Users* context > click **Add Profile Group**

Add or edit an existing Profile Group using the previously configured URL Access Management Profile.

 © 2024 / Menlo Security, Inc. All rights reserved.

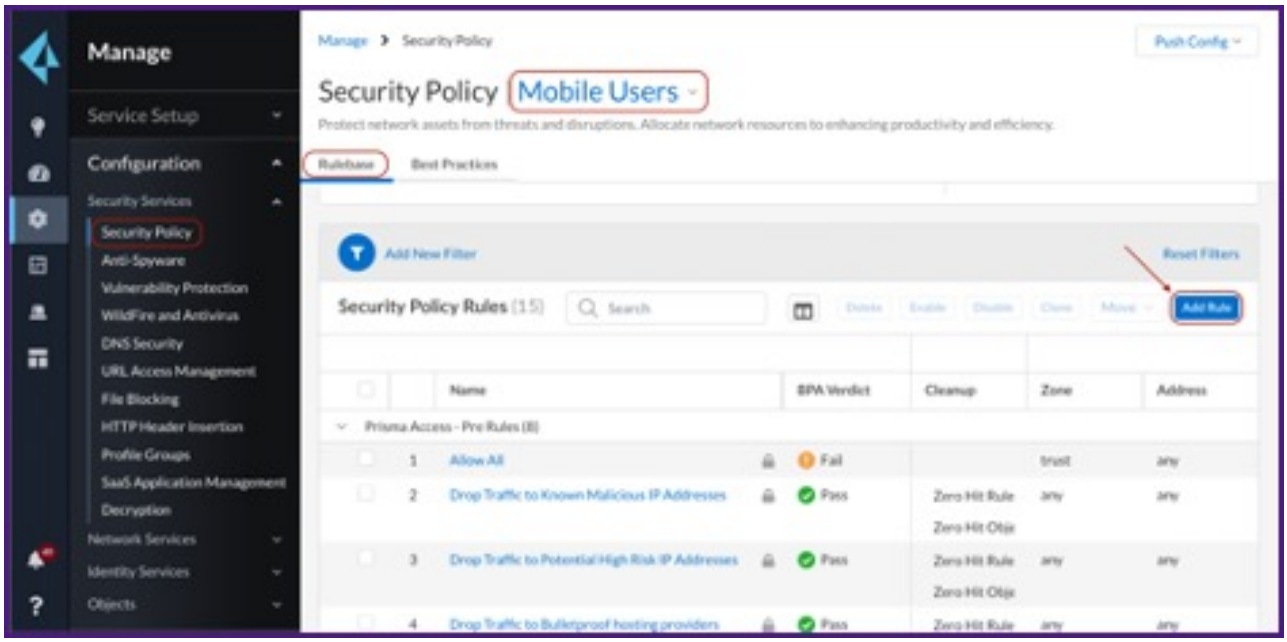




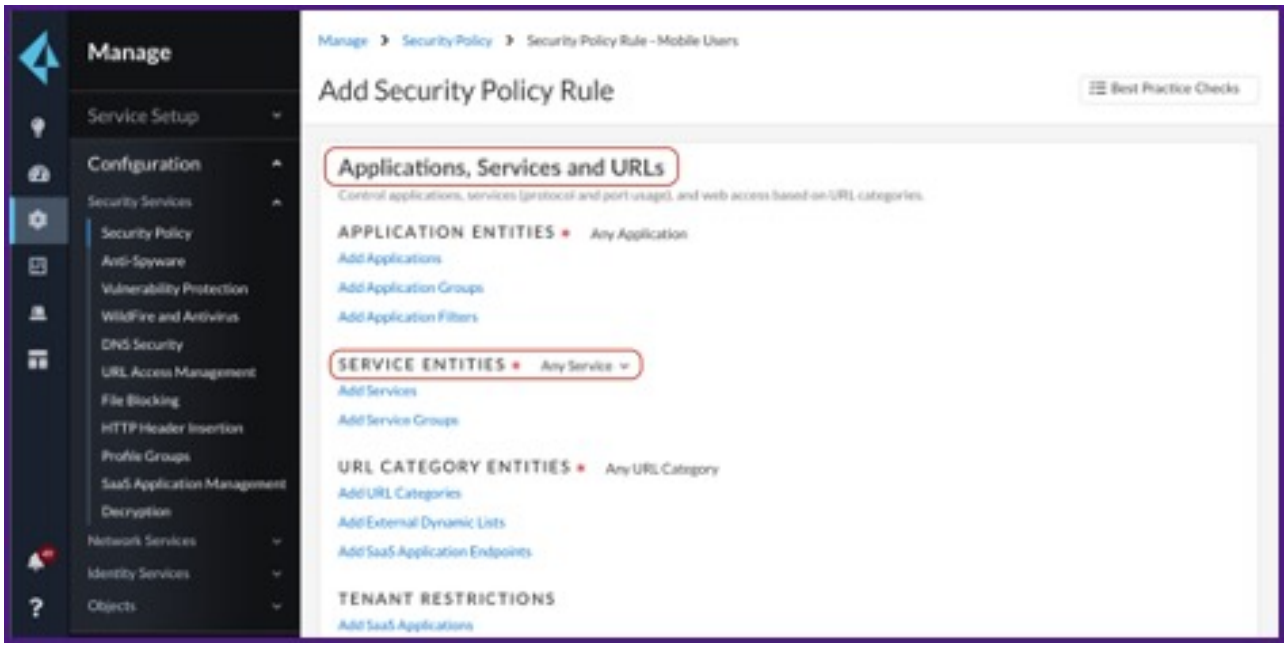
Click **Save** to accept changes.

Navigate to *Security Policy* > under the *Mobile Users* > *Rulebase* tab, 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.

 © 2024 / Menlo Security, Inc. All rights reserved.

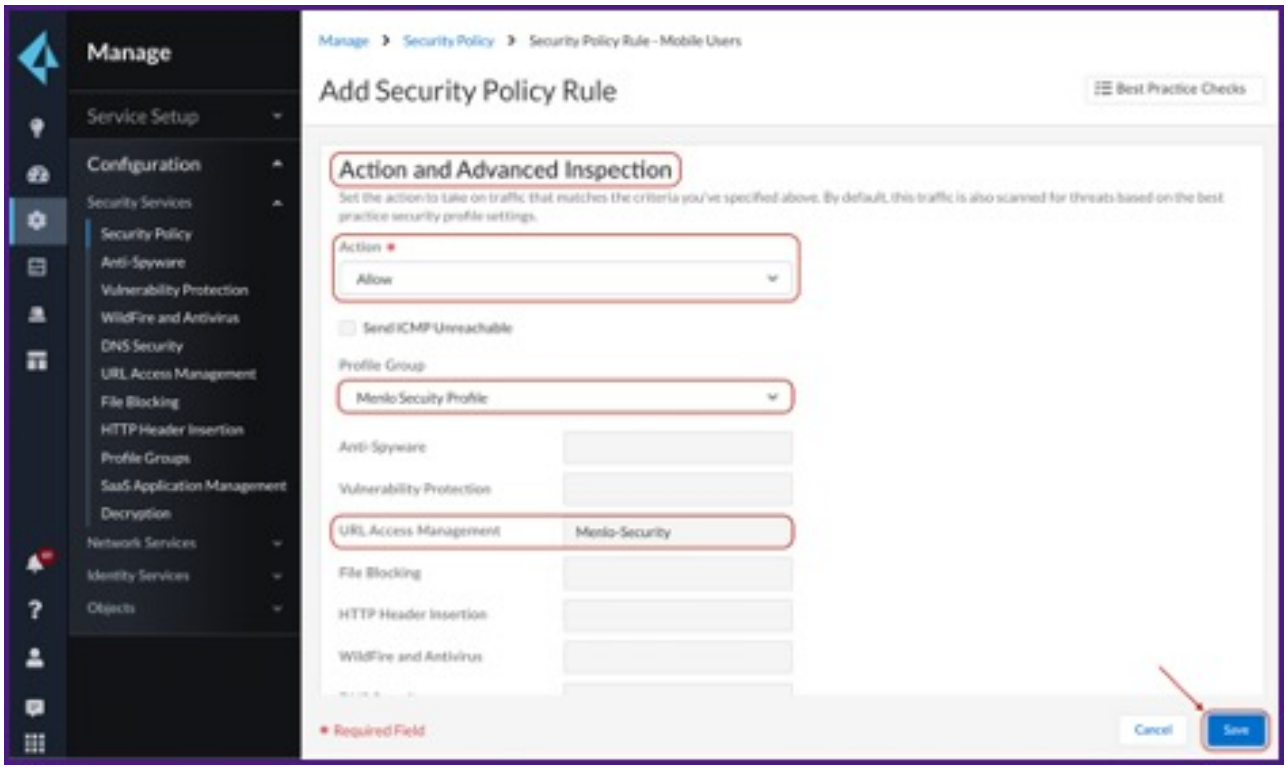


Under the *Service Entities,* set the services as **Any Service** (don't use the **application-default** as the redirection might involve non-standard ports).



Under the *Action and Advanced Inspection* section, select the **Allow** option. Under the Profile Group, select the Profile Group defined in the previous step.

 © 2024 / Menlo Security, Inc. All rights reserved.



Click **Save** to confirm changes. Then click **Push Config** and **Push** to apply the changes.

Continue with the common Step 4 and Step 5 further in this document.

3.3. 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.

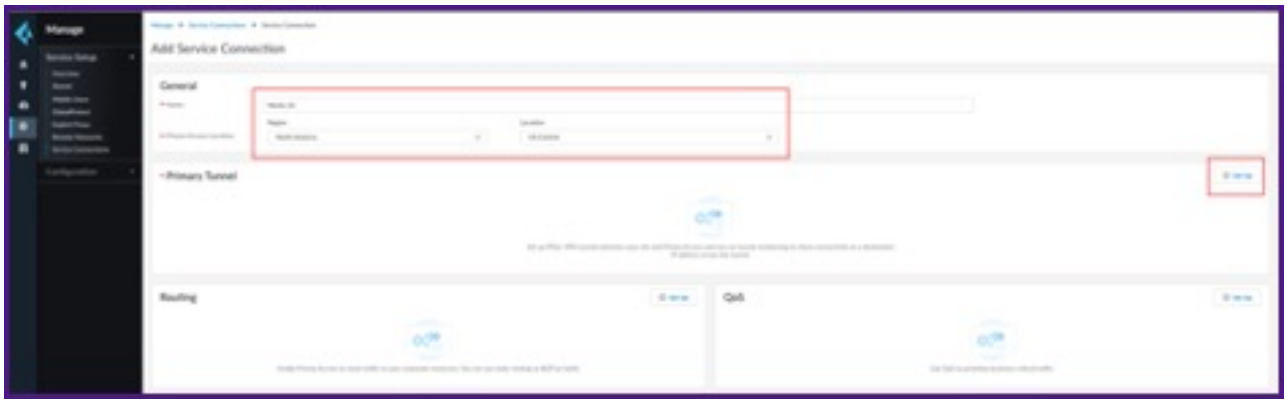
> **Important**
> You need to provide Menlo Security Customer Success with your service IP address so the IPsec tunnel pair can be created.

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

Navigate to *Manage* > *Service Setup* > *Service Connections* and create a new Service Connection that will link the Prisma Access instance to the Menlo Secure Cloud Browser.

 © 2024 / Menlo Security, Inc. All rights reserved.



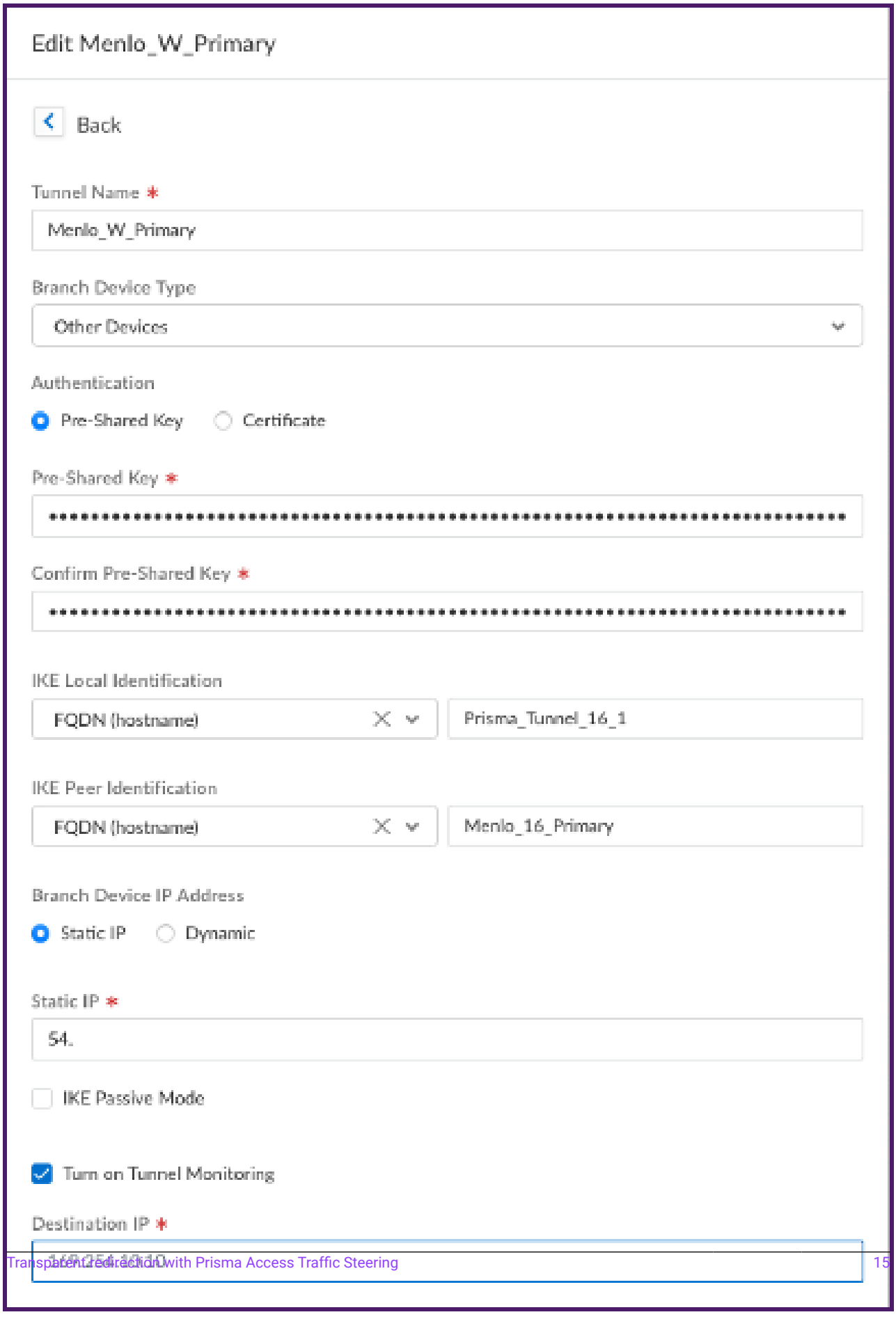
Select a **Prisma Access Region** and **Location** as close as possible from the majority of the users that will be redirected to Menlo Security. If the users are geographically dispersed, multiple Service Connections would be recommended for a better user experience.

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:

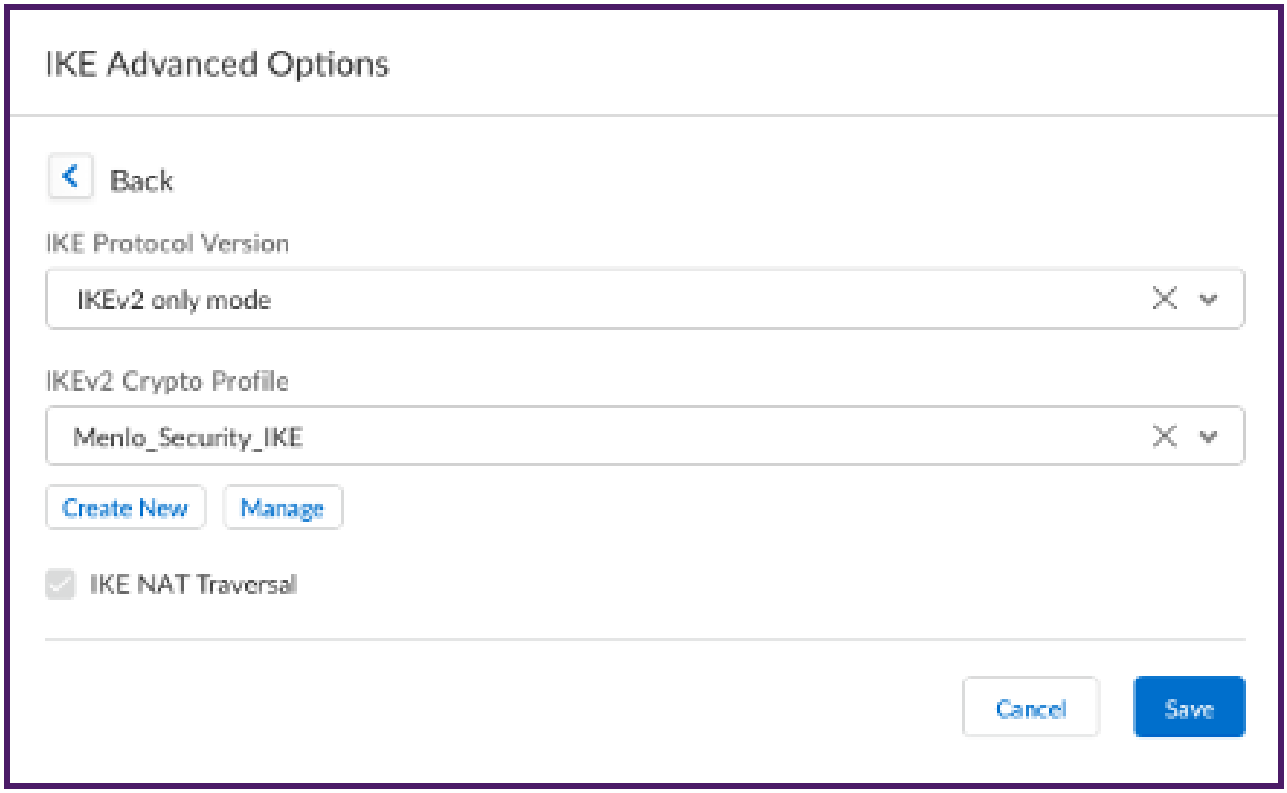
> **Note**
> Enabling **Tunnel Monitoring** is recommended to monitor the status of the IPsec tunnels by passing ICMP packets through the tunnel to verify it's operational. The IP address in the range 169.254.0.0/16 is used as the destination address for tunnel monitoring. The destination address can be same if they are established with different IKE peers, otherwise it has to be unique.

© 2024 / Menlo Security, Inc. All rights reserved.



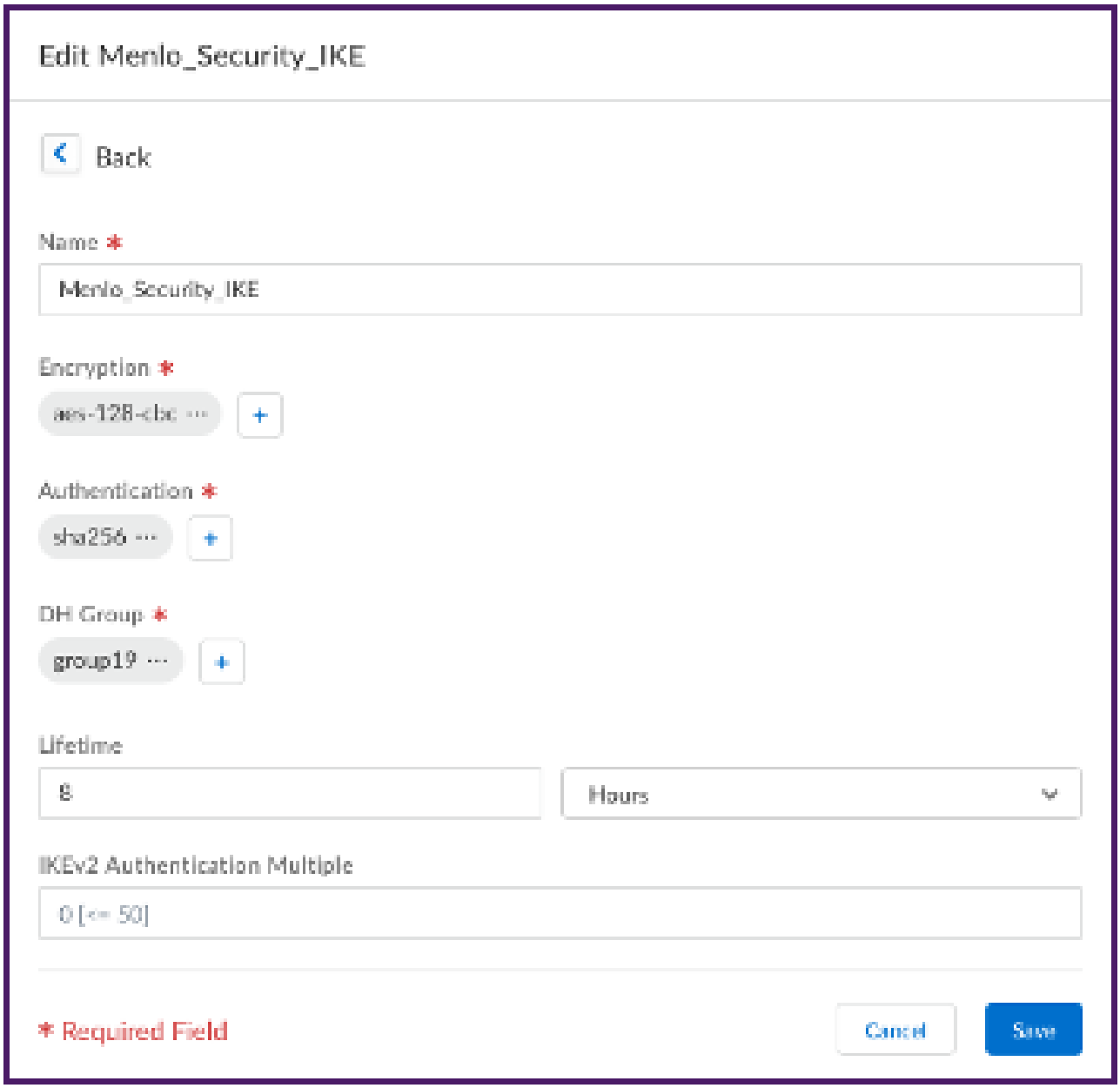
 © 2024 / Menlo Security, Inc. All rights reserved.

Under the *IKE Advanced Options* select the following combinations:



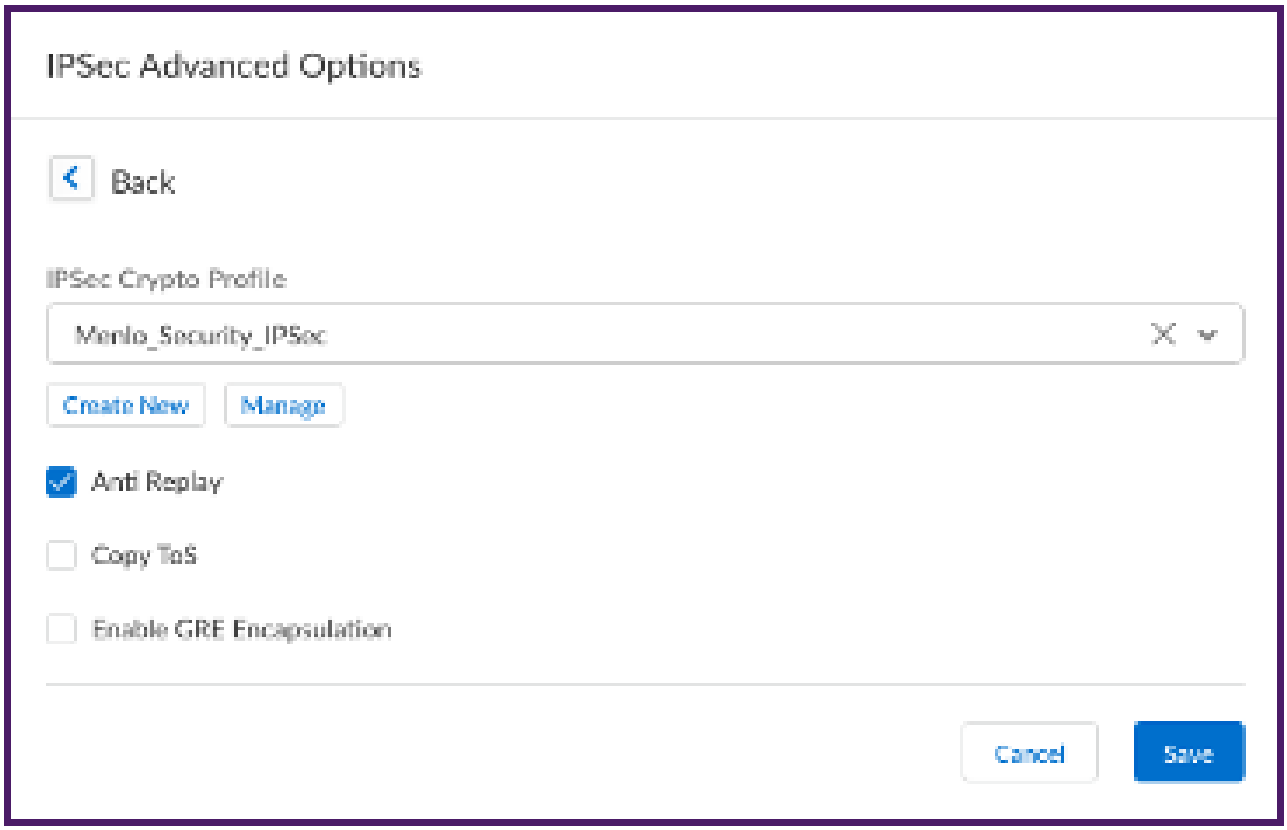
Note
The **Lifetime** value entered should match the Lifetime value provided by Menlo Security Customer Success for both IKE crypto and IPsec crypto settings when the IPsec tunnel is configured.

 © 2024 / Menlo Security, Inc. All rights reserved.

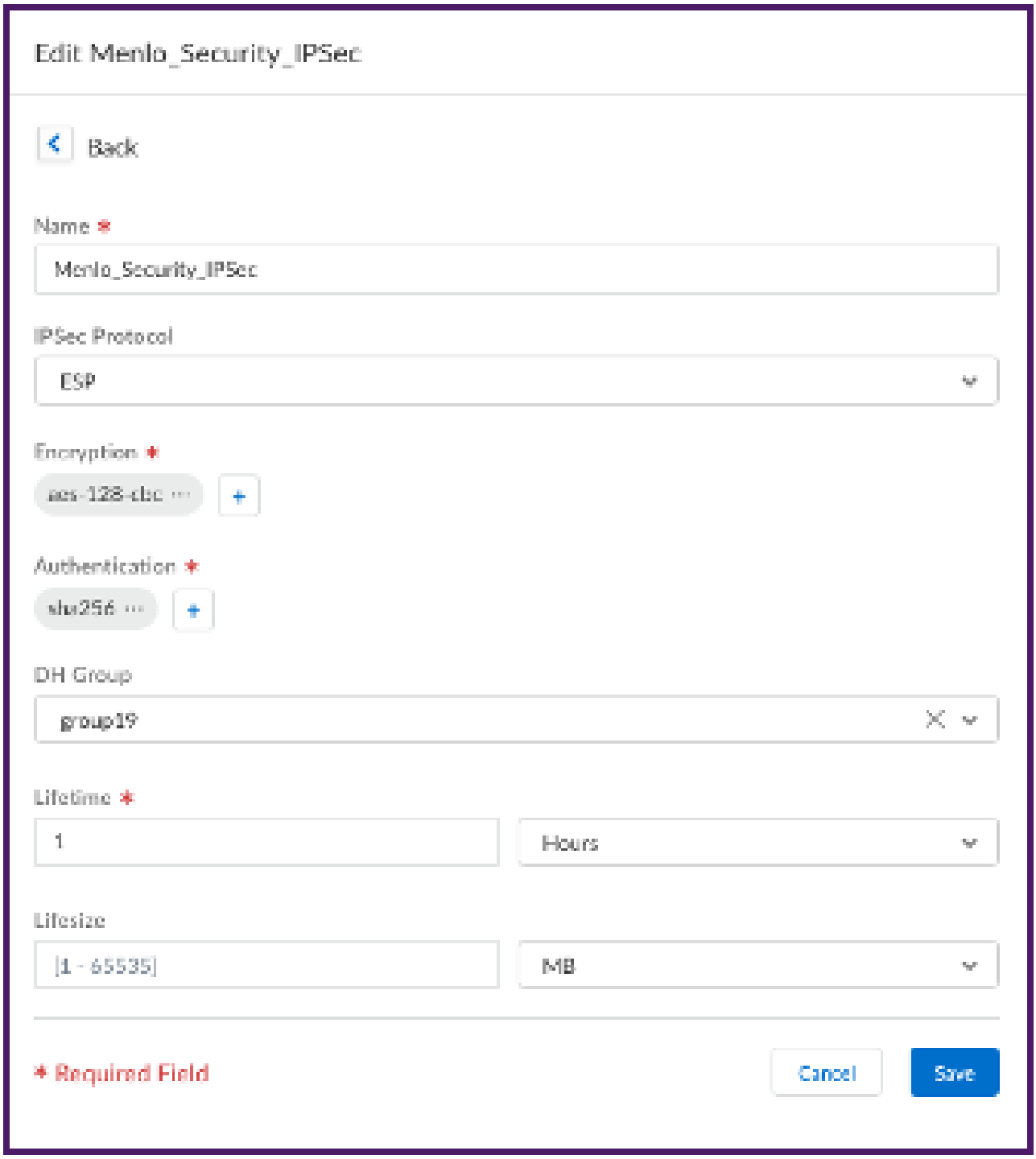


Under the *IPSec Advanced Options*, select the following combination:

© 2024 / Menlo Security, Inc. All rights reserved.



 © 2024 / Menlo Security, Inc. All rights reserved.



Push the new configuration.

Once the Service Connection is created, a dedicated Public IP will get assigned; this will be the IPsec tunnel end point 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.

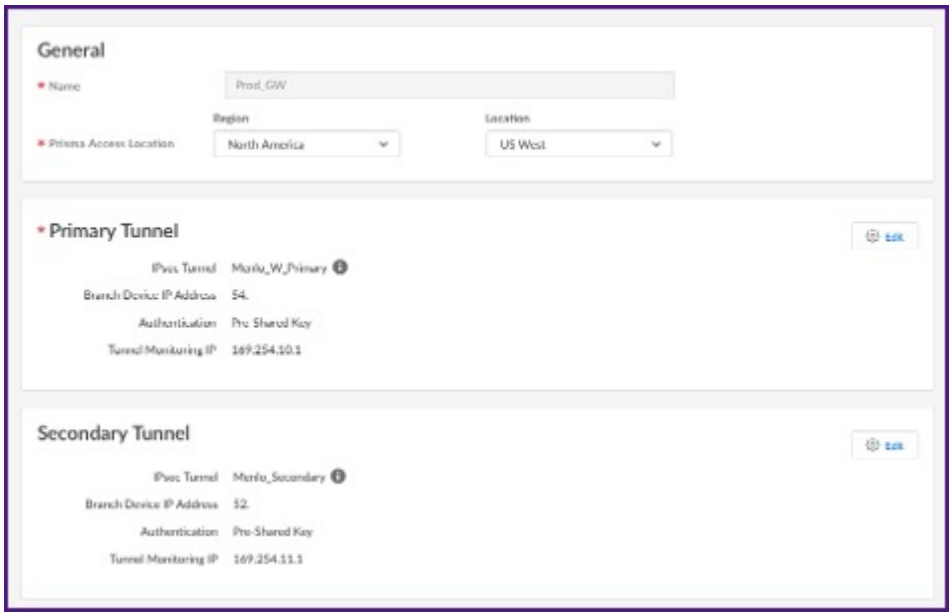
 © 2024 / Menlo Security, Inc. All rights reserved.

Note
The IP in the image above is only one random example.

Once the IPSec tunnel is provisioned by Menlo Security as well, validate the Tunnel status turns into the Green/OK state.

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.

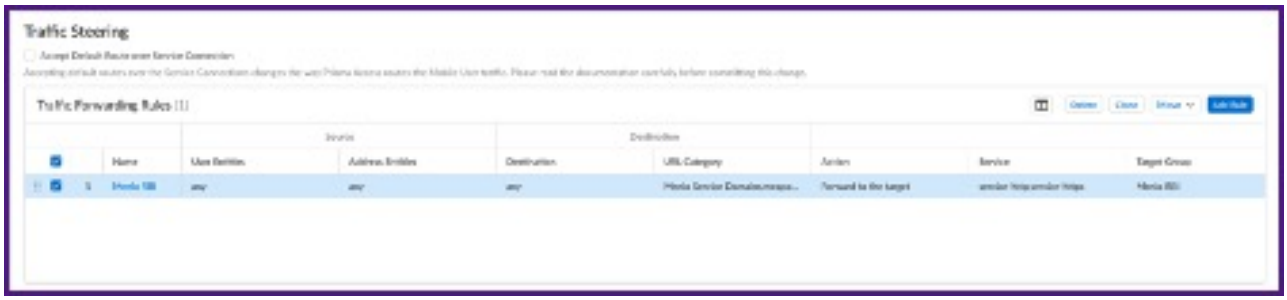


Step 3: Configure the Traffic Steering rules to select what traffic is required for Isolation

Under the same *Service Connections* menu, select the *Advanced Settings* tab.

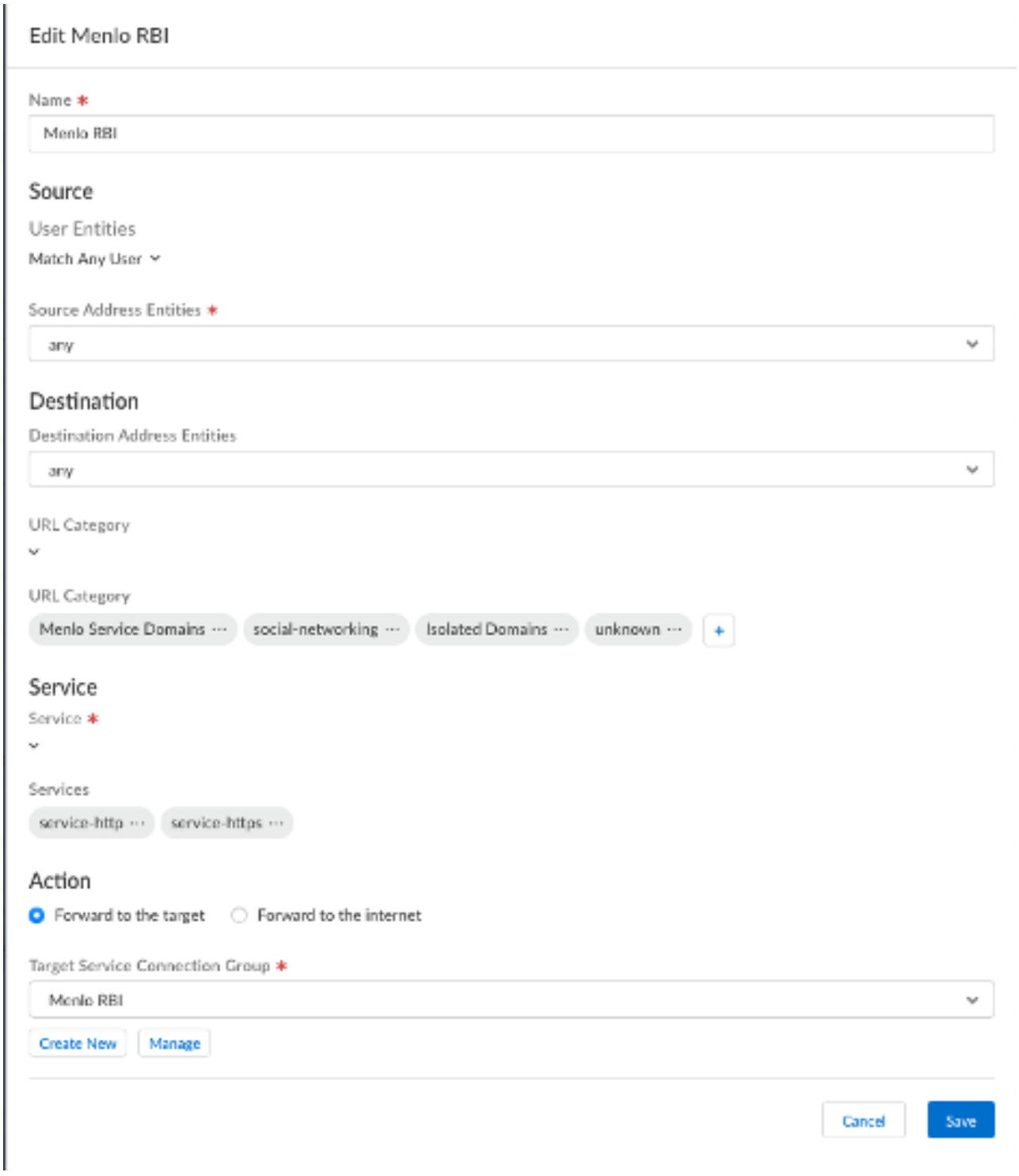
Under the *Traffic Steering* menu, create a new Traffic Forwarding rule.

 © 2024 / Menlo Security, Inc. All rights reserved.

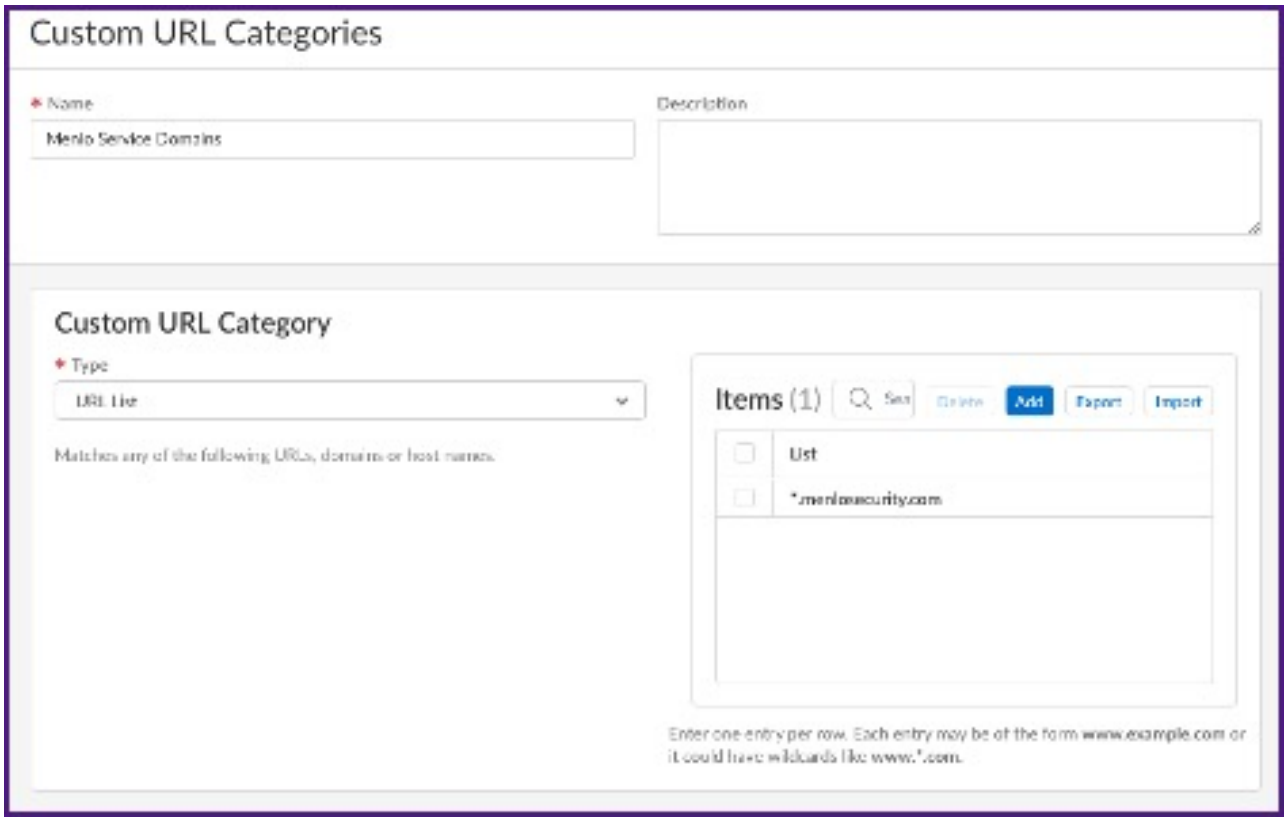


Select the matching criteria for the traffic that needs to be transparently redirected through Isolation; typically the criteria are a combination of selected users and/or URL Categories.

 © 2024 / Menlo Security, Inc. All rights reserved.



 © 2024 / Menlo Security, Inc. All rights reserved.



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.

Make sure that all the above configurations are being pushed.

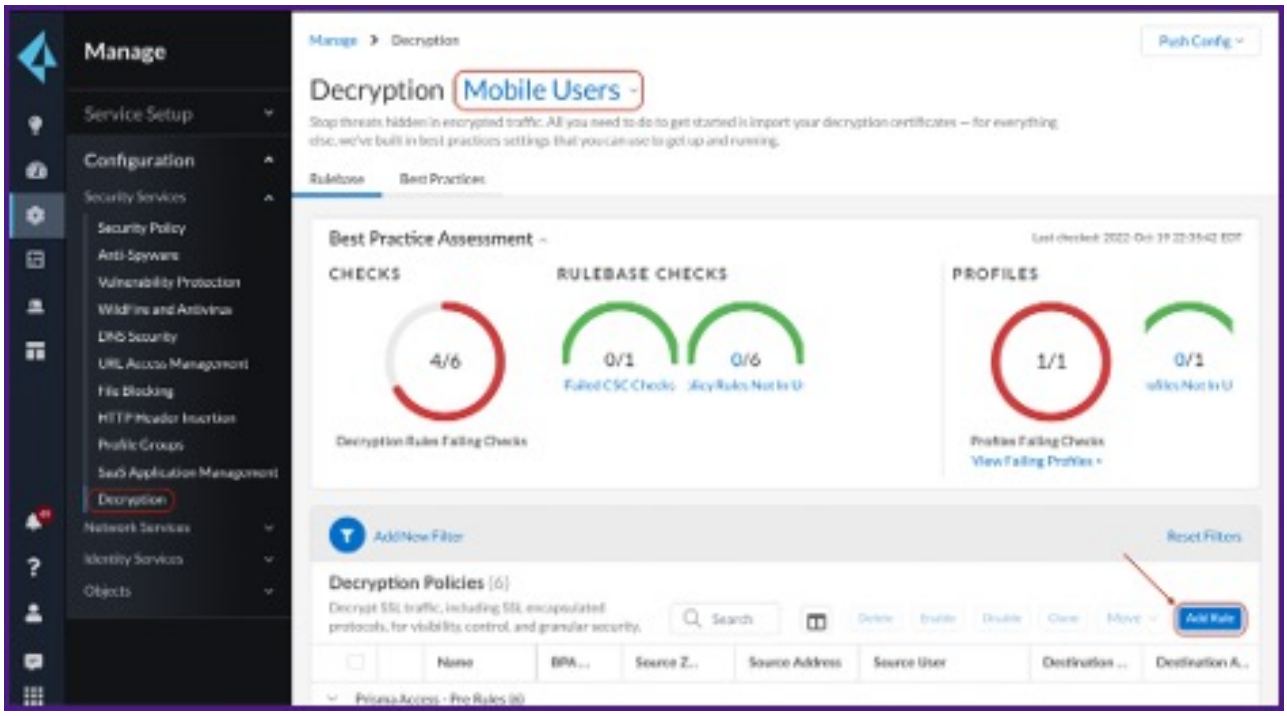
3.4. Common Steps for any of the selected integration methods

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

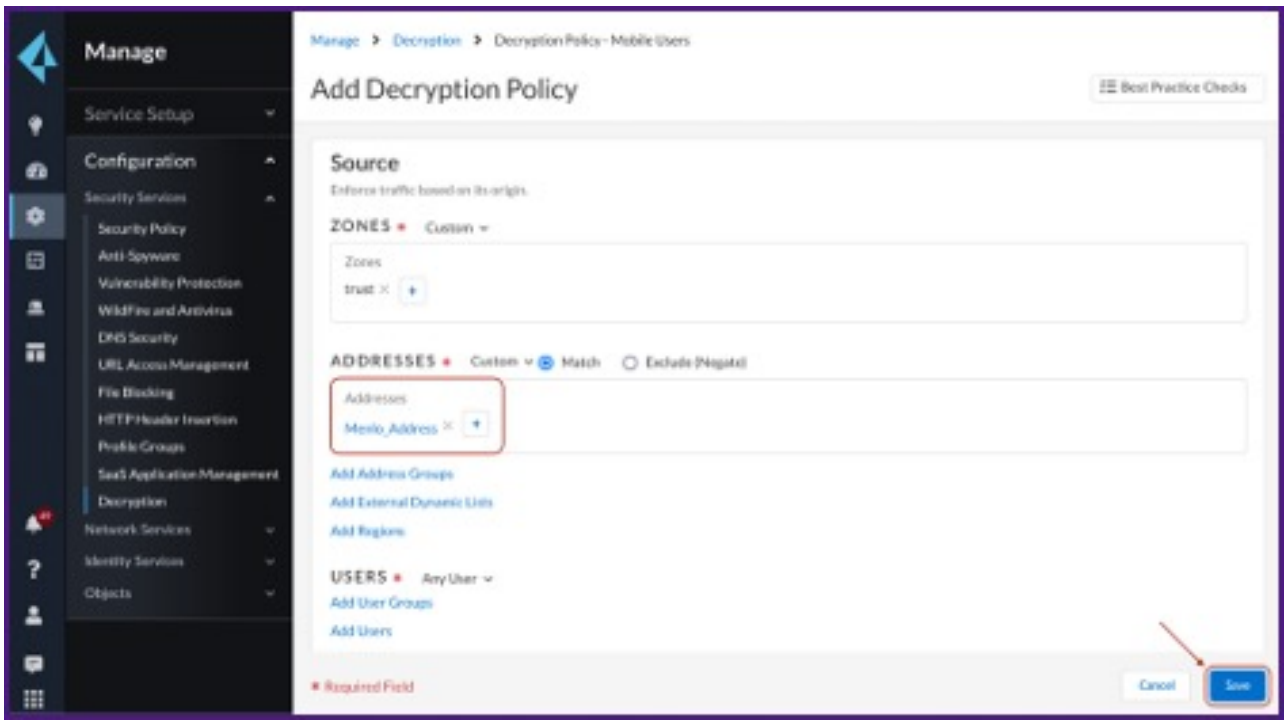
Navigate to *Configuration* > *Security Services* > *Decryption* under the *Mobile Users* context.

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

 © 2024 / Menlo Security, Inc. All rights reserved.



Add the Address object that was created earlier.



Click the Push Config button and Push.

Step 5: Verify the redirection works as expected

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

 © 2024 / Menlo Security, Inc. All rights reserved.

Try to access any URL under the categories selected for redirection.

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.

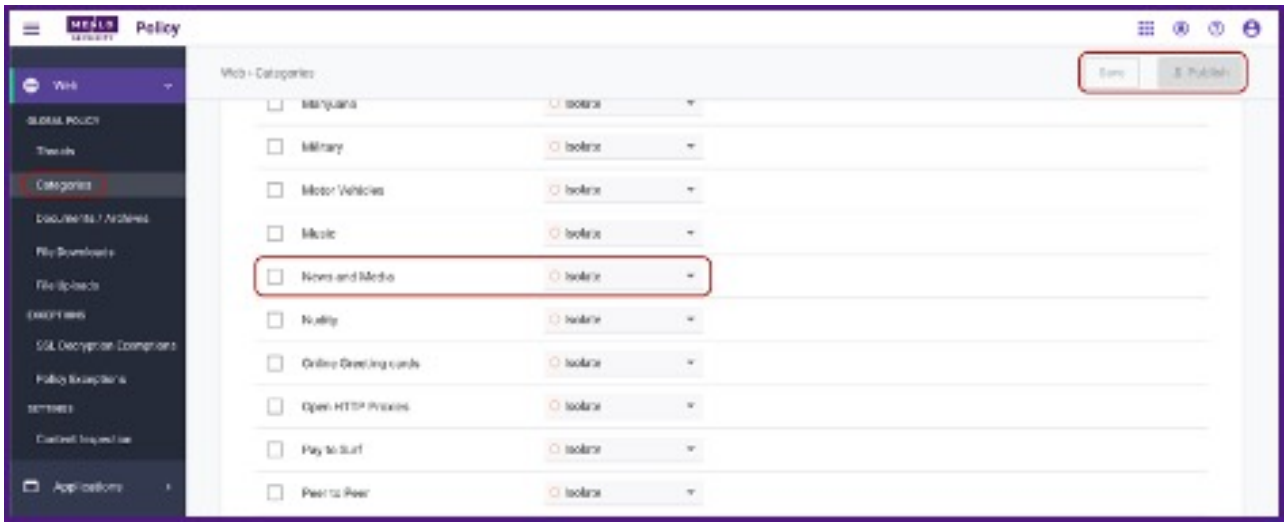
> **Note**
> In the case of the Transparent Redirection method, the original URL that is being accessed by the user remains unchanged (no prepend). This makes the user experience in this case totally transparent for the URLs accessed through Isolation.

 © 2024 / Menlo Security, Inc. All rights reserved.

4. Menlo Security Configuration

The first two integration methods are using the 'prepend' mode in the Menlo Security solution (prepending 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 *Web Policy* > *Categories / Threats*. This policy ensures that any traffic selected by the Prisma forwarding policy will be isolated by the Menlo Security platform.



 © 2024 / Menlo Security, Inc. All rights reserved.

5. 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 is in the Menlo Security platform logs to confirm that the traffic is Isolated as expected.

5.1. Technical Support

- Contact information for Palo Alto technical support: https://support.paloaltonetworks.com
- Contact information for Menlo Security technical support: https://csportal.menlosecurity.com