# MENLO SECURITY

# Palo Alto Prisma Access: Cloud Managed Integration Guide

November 2024

# **Table of Contents**

1. Revision History	1
2. Use Cases for Integration with Palo Alto Prisma Access	2
2.1. Simplify User Policy Enforcement	2
2.2. Protecting High-Risk Users and Applications	2
2.3. Integration Benefits	3
2.4. Before You Begin	3
3. Palo Alto Networks Configuration	4
3.1. Block action integration method	4
3.2. Override action Integration method	7
3.3. Transparent redirection with Prisma Access Traffic Steering 1	3
3.4. Common Steps for any of the selected integration methods 2	23
4. Menlo Security Configuration	26
5. Troubleshooting	27
5.1. Technical Support	27

# **1. Revision History**

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

# 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.

# 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.



# 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).

# 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**.

4	Manage Manage > URLAccess/Management Mobile Licens								Push Confi			
٠	Service Setup ~	Control	Luners' access to the credentials to	- 100	content, and how	whey interact with it (for en Also enforce safe search to	ample, to prevent phis ir search engines like G	hing, block users fro cogie and Bing.	an submitti	NE.		
•	Terrette Terretere	Access	Control Ser	tin	ps Best Prac	tices						
۰	Security Policy	-										
8	Anti-Spyware	Q	Add New Till	ber							Reset Filb	ers
	Withersdollby Protoction         URL Access Management Profiles (3)           WildFire and Artivirus         The profiles here are active only when you add them to a profile group, and add the profile group, and add the profile group is a security rule.         Q. Search         To be Conv. Management Profiles (3)								Care Mare	Anthon		
	UIL Access Management											514.7
	File Blocking HTTP Header Insertion		Name		BPA Vordict	Location	Security	Profile Gr	Allow	Aiert.	Cont	8
	Profile Groups		best-grac	ê	O Pass	predefined	6/14	best-practice	7	52		2
	SaaS Application Management		Explicit P	4	Pass	predefined	0/14	Explicit Proxy	80			
	Network Services ~		Menip-U.	8	O fail	Prisma Access	3734	Ments-sec	74			
?	Identity Services. • Objects •	Meeting Services S0.0% of your security policy rules are using a URL Access Management profile (7 of 54 rules)										
*		Cu	stom URL Ca	ater	gories (3)	on a surface to the						
		cate	gories.		a new Constant Arrite	Post of the current set.	Q. Search			Dalets Clave	Add Catego	
=									Used In			1

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.

4	Manage	Manag		langement Protie	> URLAccess	Anagement Profile - N	Aphile Users			
	Service Setup +	Carlo	Add OKE Access Management Prome							
0	Configuration  Security Services Security Policy	* Nati	e sisterunity	Unige			Description Categories to block for redirection to isolation			
8	Anti-Spyware Materiability Protection									
	WidFire and Antivirus									
	DHG Security URL Access Hanagement File Blocking HITTP Header Insertion Profile Groups	Ac	Coess Contro FOI classifier webs	d hes haved on site co	terit, Ratures, av	6 selety: fait Schemales -	User Credential Detection Detect when users attempt to submit corporate credentials to a website. User Gredential Detection Disabled v			
	SadS Application Management Decryption		Category	Site Access	User Gred	His	Advanced LIPI Julies Categorization			
	Network Services y	-	domain	land w	1 1111		You can set the action for each model			
	Mently Services +	-	nut-resolved	1000	+ .00m	-	Enable cloud inline Categorization			
?	uqua -		nudity	Allow	+ atou	-	Enable local Inline Categorization Exclude custom URL sategories or external dynamic lists from brine Machine			
			online storage	Buck	* allow		Learning actions.			
		+ Rep	and Field	Cantinue	]		Cavat Land			

#### 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.

4	Manage	Manage > URL Access Manage	mont > Settings			Push Cavity ~
	Service Setup +	Control users' access Man	agement M	Nobile Users	phishing, block users from submitting	
	Configuration -	Access Control Settings	Best Practices	a sale wardt for wardt engries i	to Google and Bing	
•	Security Services	Location	554	TLS Service Profile	Mode	Properties
-	Vulnerability Protection	Prisma Access			redirect	address safe.merihae(safty.com
1	WidFire and Antivirus DNI Security					
	UR, Access Management File Blocking HETP Header Insertion Pratile Groups Sati Application Management					
	Decryption Network Services -	Response Pages (5) Configure the web pages that a	en displayed when certa	an actions are biggered.		
	Mentity Services -	Response Page		location	Actions	
**	Objects -	Anti Phishing Block Page		predefined	Export HTM	L'Templane
?		Anti Phishing Continue Page		predefined	Export HTM	L Template
		URL Access Management Safe	Search Block Page	predefined	Export HTM	L Template
		URL Access Management Block	Page	Mobile Users Container	Revert to be Expert HTM	ented Template L'Template
=		URL Access Management Cont	inue and Override Page	predefined	Expert HTM	Template

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:lem;
  }
 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>
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.
<b>User:</b> <user/> 
<b>URL:</b> <url/> 
<b>Category:</b> <category/> 
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).

4	Manage	Manag	Manage > URL Access Management Profile > URL Access Management Profile - Mobile Users Manalon, Special risks									
	Service Setup +	( Contra	Configuration Profile Usage  * Name Description									
	Configuration +	* Nam										
۰	Security Service A	Meril	io-Security				Categories to override for redirection to isolation					
8	Anti-Spyware Vulnerability Protection	Securit Profile	y Rules Using This Groups Containing	Profile 0 This Profile 0								
	WidFire and Anthreas	office and Anthreas										
•	DNS.Security URLAccess.Management FileBlocking	cess Contro	l Res based on site co	tont, Rodures, and	f safety.	User Credential Detection Extert when users attempt to submit corporate condentials to a website.						
	HTTP Header Intertion Profile Groups		Q, Search		SetAcom -	Set Submission -	User Credential Detection Disabled ~					
	Sad Application Management		Category	Site Access	User Cred	1626						
	Decryption Network Services +		registered- domain				Advanced URL Inline Categorization					
	Identity Services +	0	news	Dverride v	• silou		Enable clouil Inline Categorization					
	Objects v		not-resolved	Part	+ allow	24	Enable local Inline Categorization					
?			nudity	Allow	+ allow		Exclude costone URL categories or external dynamic lists from Indine Machine					
			ardine storage-	Buck	* alize	-	Prevent accore.					
		+ Rep	ind Field	Continue			Canal Los					
			enter in	Override								

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**.

4	Manage	Manage > URLAccessManagement 3	Settings		Push Config +
		Control users' access to web content, and I	Nent Mobile Users	e phidzing, block users from submitting	
0	Configuration +	Access Cantral Settings Best P	ng kao estorio uni scaro for scaro-ingresi nation	our Cooger and teng.	
•	Security Policy Anti-Spymare	General Settings - Donut	۰.	Remote Browser Isolation Sett	Sing - Internation Starval
	Vulnerability Protection WildFire and Anthena	URL Continue Timeout (min) URL Admin Overvide Timeout	15-minutes 15-minutes	Remote Browser Isolation	Disabled
-	URL Access Hangement File Stecking	URL Admin Lockout Teneout (nin) Hold Client Repuest for Category	30-minutes		
	HTTP Header Insertion Profile Groups Saafi Application Hanagement	Category Lookup Timeout Append End Token to List Entries	2 seconds		
	Decryption Network Services v	PAN OB Server	Default		
	Mentily Services v	URL Admin Overrides (0)		α	Colors And URL Admin Docember
*	Objects +	Location .	551/TLS Service Profile	Mode .	Properties
?					
+				0	
			Allow certain people to acc	es blocket URL categories.	

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

URL Admin Overri	de Settings
Mode	O Transparent O Redirect
* Address	redirector.menlosecurity.com
* Password	••••••
* Confirm Password	
SSL/TLS Service Profile	None 🗸
	Create New Manage
* Required Field	Cancel Save

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.

4	Manage	Manage > Profile Groups	Mohile Lisers	5						Push Config ~
٠		Security justiles scan traffic h	or threads, and a profile group	is a collection of each	type of profile. S	0				
	Configuration •	a security rule (go to Security	Services + Securital.	ng (to this here) and	arrest die floore	" Q 5	carch			
• • •	Security Services A Security Policy Acti-Sepware Valuerability Protection WildFire and Archivus DMS-Security UELAccess Management File Booking HITTP Header Insection Profile Groups Sad: Apple atten Hanagement Decreption –	Profile Groups (2)	Location Anti Profile productioned best-proc. productioned best-proc.	Vulnerabilit Profile best-practice best-practice	URL Profile best prik. Explicit	File_ Profile Inst-pra_	III HIT Puble	Done Com Widfine Profile best-practice best-practice	DAS Profile best pr	Days Un
4	Manage	Add Profile Group	<ul> <li>Profile Group - Mobile Un</li> <li>OUP</li> </ul>	m						
1	Configuration +	Configuration								
•	Security Services A Security Policy Anti-Spaware	Profile Group	Constant							

Click Save to accept changes.

• Required Field

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.

4	Manage Manage > Security Policy								Push Config *
•	Service Setup 👻	Protect nets	icy r	sets from threats and disruptions. Allocate network	resour	rces to enhancing p	roductivity and effici	ency.	
	Configuration *	Rukbase	Ber	I Practices					
۰	Security Policy	-							
8	Anti-Spyware Vulnerability Protection	U	dil No	e Filter					Reset Filters
	WildFire and Antivirus	Securi	ty Pol	Icy Rules (15) Q. Search		Datata Datata	Evalle Dualle	Care Mave	Add Bull
	URL Access Management								
	File Blocking			Name		EPA Verdict	Cleanup	Zone	Address
	HTTPHeader Insertion	<ul> <li>Pris</li> </ul>	na Acc	ess - Pre Rules (8)					
	Profile Groups		1	Allow All	ŵ.	O Fail		trust	My .
	SaaS Application Management Decryption		2	Drop Traffic to Known Malicious IP Addresses	ŝ	O Pass	Zero Hit Rule Zero Hit Obie	any	any .
**	Network Services • Identity Services •		3	Drop Traffic to Potential High Risk IP Addresses	â	O Pass	Zero Hit Rule	any	iny
?	Objects +	-0	4	Drop Traffic to Bulletproof hosting providers		O Pasa	Zero Hit Rule	any	ing

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

4	Manage	Manage > Security Policy > Security Policy Rule - Mobile Users	The best for the first
•	Service Setup +	Add Security Policy Rule	12 Best Practor Checks
•	Configuration A Security Services A Security Policy Anti-Spyware Velocability Protection	Applications, Services and URLs Control applications, services (perfoct and port usage), and web access based on URL categories. APPLICATION ENTITIES  Any Application Add Applications Add Applications	
•	WildFire and Antivirus DNS Security URL Access Management File Biocking HTTP Header Insertion	Add Application Filters           SERVICE ENTITIES + Any Service v           Add Services           Add Service Croups	
?	Profile Groups SaaS Application Management Decryption Network Services v Identity Services v Objects v	URL CATEGORY ENTITIES * Any URL Category Add URL Categories Add External Dynamic Lists Add SaaS Application Endpoints TENANT RESTRICTIONS Add SaaS Applications	

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

4	Manage	Manage > Security Policy > Securit	ty Policy Rule - Mobile Users		
•	Service Setup -	Add Security Policy I	Rule		t# Best Practice Checks
0 0 1	Configuration  Security Services  Security Palicy  Anti-Spyware  Waherability Protection  WildFire and Antivirus  DNS Security  URL Access Management  File Blocking  HITTP Header Insertion  Profile Groups	Action and Advanced Set the action to take on traffic that is practice security profile settings. Action # Allow Send ICMP Unreachable Profile Group Mento Security Profile Anti-Spynare	Inspection) atches the oriteria you've sp	ecified above. By default, this traffic	is also scanned for threads based on the best
? 4 B	SaaS Application Management Decryption Network Services • Identity Services • Objects •	Vulnerability Protection URL Access Management File Blocking HTTP Header Insertion WildFire and Anthrhus	Metio-Security		Cancel Son

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.

٠	Manage Investment -	Add Service Conv	e lancionale.						
-	hill	General 	na.e		landa Manan				
	Testigonite 1	- Printery Terrori			1 a <sup>16</sup> 0 <sup>16</sup> 1 a 16	0			
		Ruling					94		
				<u>.</u>				60 <sup>10</sup>	

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.

< Back		
Tunnel Name *		
Menlo_W_Primary		
Branch Device Type		
Other Devices		Ŷ
Authentication		
• Pre-Shared Key O Certificate		
Pre-Shared Key *		
•••••		
INTER- TRANSPORT		
INE Local Identification		
FQDN (hostname)	××	Prisma_Tunnel_16_1
FQDN (hostname)	× •	Prisma_Tunnel_16_1
IKE Local Identification FQDN (hostname) IKE Peer Identification FQDN (hostname)	× •	Prisma_Tunnel_16_1 Menlo_16_Primary
IKE Local Identification FQDN (hostname) IKE Peer Identification FQDN (hostname) Branch Device IP Address	× •	Prisma_Tunnel_16_1 Menlo_16_Primary
IKE Local Identification FQDN (hostname) IKE Peer Identification FQDN (hostname) Branch Device IP Address Static IP O Dynamic	× •	Prisma_Tunnel_16_1 Menlo_16_Primary
IKE Local Identification FQDN (hostname) IKE Peer Identification FQDN (hostname) Branch Device IP Address Static IP O Dynamic	× •	Prisma_Tunnel_16_1 Menlo_16_Primary
IKE Local Identification FQDN (hostname) IKE Peer Identification FQDN (hostname) Branch Device IP Address Static IP Opynamic Static IP * 54	× •	Prisma_Tunnel_16_1 Menlo_16_Primary
IKE Local Identification         FQDN (hostname)         IKE Peer Identification         FQDN (hostname)         Branch Device IP Address         Static IP       Dynamic         Static IP *         54.         IKE Passive Mode	× •	Prisma_Tunnel_16_1 Menlo_16_Primary
IKE Local Identification FQDN (hostname) IKE Peer Identification FQDN (hostname) Branch Device IP Address Static IP Opynamic Static IP * 54. IKE Passive Mode Turn on Tunnel Monitoring	× × × •	Prisma_Tunnel_16_1 Menlo_16_Primary
IKE Local Identification FQDN (hostname) IKE Peer Identification FQDN (hostname) Branch Device IP Address Static IP Opynamic Static IP * 54. IKE Passive Mode Turn on Tunnel Monitoring Destination IP *	× •	Prisma_Tunnel_16_1 Menlo_16_Primary

Under the IKE Advanced Options select the following combinations:

IKE Advanced Options	
< Back	
IKE Protocol Version	
IKEv2 only mode	× •
IKEv2 Crypto Profile	
Menlo_Security_IKE	× •
Create New Manage	
IKE NAT Traversal	
	Cancel Save

#### 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.

Edit Menlo_Security_IKE			
Back			
Name *			
Menlo_Security_IKE			
Encryption * aes-128-cbc ···· +			
Authentication * sha256 ···· +			
DH Group * group19 ··· +			
Lifetime			
8	Hours		÷
IKEv2 Authentication Multiple			
0 [<= 50]			
* Required Field		Cancel	Save

Under the IPSec Advanced Options, select the following combination:

IPSec Advanced Options	
< Back	
IPSec Crypto Profile	
Menlo_Security_IPSec	× •
Create New Manage	
🛃 Anti Replay	
Copy ToS	
Enable GRE Encapsulation	
	Cancel Save

Edit Menlo_Security_IPSec		
< Back		
Name *		
Menio_Security_IPSec		
IPSec Protocol		
ESP		*
Encryption *		
aes-128-cbc … 🕂		
Authentication *		
sha256 ··· +		
DH Group		
group19		× ~
Lifetime 🔹		
1	Hours	v
Lifesize		
[1 - 65535]	MB	Ÿ
* Required Field		Cancel Save

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.

۰	Hanage										
:	Series Series	Service Canne	COONS SHUP	-	and the second						-
	The second secon										
-	Galacture	Service Lorence	ine III						Being daring the	e • e	the set (second test
			50		Rote		through hereit				144
	Second second	0.989	mouth .	Tatas	Contra Co	100884	Tervice IP	(BUTMAN)	807.04	8972-0	Plac Same
-		C Heart		8-04	diam'r.	Vel Germal	URDERSON AND	1051403014	deater	<b>Enables</b>	Secondary for the second

**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.

General					
Name	Prod_GW				
	Region		Location		
Prives Access Location	North America	*	US West	¥	
Primary Tunnel					@ <b>E</b> Ø
IPves Tarres	Marky, W. Primary O				
Branch Device IP Addres	54.				
Authenticatio	n Pro Shared Key				
Tannel Manitaring II	P 169.254.10.1				
Secondary Tunnel					© 10
Page Turn	d Menio_Secondary				
Branch Device IP Addres	a 52.				
Authenticatio	n Pre-Shared Key				
Turned Munituring I	P 169.254.11.1				

#### 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.

٠	Harage	Amage 2 Stretc Control	-								Part and pr
:	Bervic Inter -	Service Connec	tions Setup						Party Roomer		-
	CodePress Substitutes		-		Traine .		Wants Street,				144
	Risks States	-	salvati.	ficial	1949	10080	Solut.	1007-0102	307.012	aur eus	and the second
		0 1462		6×	Q have	- III General	DEDEDATE	PERMIT	Outer	Dubi	Log be

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

u Pic Pa	overling fulls	nu .					Color	the line of the l
			histin		Deditoritore			
	Harre	Use Betties	Address British	Destination	URL Calegory	Antes	larvior.	Taype Group
	I Diverte SIN		-	-	Pitela Grocier Damaiourrespon-	Personal to the Larget	service https://www.ior.it/ips	Marcia (60)

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 *		
Menio RBI		
Source		
User Entitles		
Match Any User 😒		
Source Address Entities *		
anv		~
Destination		
Destination Address Entities		
any		~
URL Category		
v		
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		
• Formation of the same to the internet		
Target Service Connection Group *		
Menie RBI		~
Create New Manage		
	Cancel	Save

Name	Description				
Menio Service Compins					
Custom URL Category * Type					
URL Lite Matches any of the following URLs, domains or host names.	V Items (1) Q Sea Caleta Add Fapor Import				
	Enter one entry per row. Each entry may be of the form www.example.com it could have wildcards like www.".com.				

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.



Add the Address object that was created earlier.

4	Manage	Manage > Decryption > Decryption Policy-Mubile Users	
	Service Setup 👻	Add Decryption Policy	22 Best Practice Checks
8 • • •	Configuration  Security Services  Security Policy Anti-Spyware Valuesability Protection WildPire and Antivirus DNS Security URL Access Management File Blocking HTTPHeader Insertion	Source Extense traffic based on its origin. ZONES = Custom = Zones trust × • ADDRESSES = Custom = @ Match   Declude (Hegated Addresses Mento Address × •	
<b>*</b> ? ▲ ₽	Public Groups See3 Application Management Decryption Network Services v Identity Services v Objects v	Add Address Groups Add External Dynamic Lins Add External Dynamic Lins Add Extern USERS # Any Uner ~ Add Uner Groups Add Uners	Canool Sum

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.

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.

# 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.

= MESIC Policy				
O WH -	Web - Catoporles			
A DEAL POICT	L Manyuana	C. BOB'S	*	
Twish	L Minay	O isolata		
Categories	Motor Vehicles	C isolate		
baoureens / Archeves	Heale	O Isolata		
File lip-tech	News and Media	O Isolatic	-	
04071005	<ul> <li>Nolly</li> </ul>	O Isolate		
SSE Decryption Dosmptions Patho Exceptions	Online Depicting cards	O hostera		
10710401	Open HTTP Proces	O teolaror	*	
Carted Inpedia	Pag to Surf	O teolarte	*	
Applications •	Peer ta Reer	C toolars	-	

# 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*.

ACCESS	Logs Your help and automatical hop-monthal events who	e generalest and pro re Prima Access act	nde at audit toal het system, surdigurale soe jeur retowert traffis.	or, and retrievely morely. Notice th				
🕈 Isigits 🔹 P							_	
to Hanage	Presd SPE +	Q, Phase and C	la pune					
Me logo	Time Generates		- 194	UR: Domain	WE Company	UR: Catagory Lin:	Severity	Steen Zone
B Reports	C 6487,0001 6	10.27 964 897	independing resultations?	andpaint.hgran.rt.	Nam-Sal	computer and internet C.	-	Full

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