

Check Point Integration Guide

1.0.0

docs.paloaltonetworks.com

Table of Contents

Prisma SD-WAN Check Point Network Security-as-a-Service	
Integration	4
Sign in to the Check Point Infinity Portal	6
Create a Site	8
Configure your Router or SD-WAN Device	12
Support for Multiple External IP Addresses	13
Set up Prisma SD-WAN Overview	14
Create an IPsec Profile	15
Create a Service Group	20
Assign IPsec Tunnels to your Site	23
Test the Configuration	
Monitor Cybersecurity Events at the Check Point Infinity Portal	

TECH**DOCS**

Prisma SD-WAN Check Point Network Security-as-a-Service Integration

As enterprises rely on SaaS or Cloud-based delivery models for business-critical applications, there is a compelling need for per-application policy enforcement without increasing remote office infrastructure. Traditional hardware-router based approaches are limited by heavy-handed 'all or nothing' policies for direct-to-internet versus policy enforcement per-application. Additionally, because router-based approaches are packet-based versus application-session based, they fail to meet application session-symmetry requirements, causing network and security outages.



This guide explains how to set up IPsec tunnels and service chain traffic from a Prisma SD-WAN ION device to Check Point's Network Security-as-a-Service through the Prisma SD-WAN portal and Check Point's Network Security-as-a-Service web-based management.

It is intended for network and security administrators who are responsible for cybersecurity for branch office users. These instructions are applicable to Prisma SD-WAN ION devices running version 4.7.1 and above.

This guide describes how to create a site at Check Point's Infinity Portal, how to set up Prisma SD-WAN, and finally, how to monitor Cybersecurity events at Check Point's portal.

The images in this document mather have references to **CloudGenix** and the term **3rd Party/3rd Party VPN**. The CloudGenix instances now display as **Prisma SD-WAN**, and the new term for 3rd Party/3rd Party VPN is **Standard VPN** on the Prisma SD-WAN web interface. In this guide, branch offices will be protected by creating two IPsec tunnels to Check Point's Network Security as a Service. This involves signing in to the **Check Point Infinity Portal**, creating a site, configuring a router or SD-WAN device, and supporting more than one external IP address.

Read on to know more about how to sign into Check Point's Infinity portal, create a site, configure your router, and support multiple external IP addresses.

- > Sign in to the Check Point Infinity Portal
- > Create a Site
- > Configure your Router or SD-WAN Device
- > Support for Multiple External IP Addresses

Sign in to the Check Point Infinity Portal

STEP 1 | Sign in to the **Check Point Infinity Portal** at https://portal.checkpoint.com.



If you don't have an account yet, you can register for one at https://portal.checkpoint.com/ register/cloudguardnsaas.

Upon registration, make sure that the "Network" sign is colored in Pink and that the text says **Create your Infinity account to access Network Security as a Service**, otherwise you might end up subscribing to a different security product.

Network Security as a Service is dependent on a purchased software license. For more about licensing, contact your Check Point Sales representative, or check for updates at Check Point's User Community.



STEP 2 Once you are logged into the Check Point Infinity Portal, make sure that you are currently looking at the Network Security as a Service application.



If the title says a name of a different application, click the application switcher icon at the topleft corner () and select Network Security as a Service.



Create a Site

To create a site:

STEP 1 Navigate to **Sites**.

The Sites screen will display.



STEP 2 | Select the + button to create a new site.

A site represents your Prisma SD-WAN edge device. The **CREATE NEW SITE** screen will display.

- **STEP 3** In the **Site Name** field, enter a name for the site.
- **STEP 4** In the **Location of the cloud service** field, select a location that suits your site.

Check Point's Network Security as a Service inspects traffic from your branch office to the Internet with a cloud service that resides in one of these locations. So typically you would want to select the location of the cloud service with an option that is closest to the location of your site, in order to achieve the best performance. For some countries, most notably South America or the Middle East, the best choice for Location of the cloud service might be presence of a strong cross-country Internet link.

- Check Point Infinity Portal
 C Check Point Infinity Portal
 A C I https://portal.check.point.com/Dashboard/Network/SecurityAsaService/Cloudia#/sites
 NETWORK SECURITY AS A SERVICE
 NETWORK SECURITY AS A SERVICE
 C REATE NEW SITE
 STE
 C REATE NEW SITE
 I SITE DETAILS
 I SITE DETAILS
 I Name
 Marketing Office
 I Location of the cloud service I
 US: South-East
 I INTERNAL SUBNETS
 I CONFIRM SITE
 C COMMENTS
 Branch office in Northern California where Marketing department resides
 ETTNOS
 C CANCEL
 Next
- **STEP 5** In the **Comments** field, enter an optional description of the site.

- STEP 6 | Click Next.
- **STEP 7** Choose **IPsec Pre-Shared Key** as **Tunnel Type**.
- **STEP 8** In the **External IP** field, define the IP address of your branch office site.

Note that this IP must be static and accessible from the Internet. You can track Check Point's updates regarding support of other topologies at this User Community thread. Supporting more than 1 external IP address per site will be explained later on.

CREATE NEW SITE		×
SITE DETAILS	 Tunnel Type ● IPsec - Pre-Shared Key 	
2 ROUTER DETAILS	* External IP @ 209.87.209.100	
3 INTERNAL SUBNETS	* Shared Secret	Auto-Generate
(4) CONFIRM SITE CREATION		
	ВАСК	Next

STEP 9 Click **Next**.

STEP 10 | In the **Internal Subnets** page, enter the IP address of your internal networks in the branch office site.

Check Point's Network Security as a Service applies its cybersecurity features on any traffic coming from these network addresses.

Check Point	t Infinity Portal × +		- • ×
$\leftrightarrow \rightarrow \mathbf{G}$	https://portal.checkpoint.co	m/Dashboard/NetworkSecurityAsaService/Cloudia#/site	s 🕶 🖈 🚺 👼 🗄
		JRITY AS A SERVICE	CHECK POINT
SITES	CREATE NEW SITE		×Ţ
POLICY	SITE DETAILS	Enter site subnets that will be routed to the	cloud gateway
Logs	ROUTER DETAILS	(eg. 192.168.37.0/24) 192.168.1.0/24	+ 28
		192.168.2.0/24	2
	INTERNAL SUBNETS		_
© SETTINGS	CONFIRM SITE CREATION		
		BAC	K Next

STEP 11 | Click Next.



STEP 12 | Select **Finish and Create Site**. Check Point might take a few minutes to create the site.



Configure your Router or SD-WAN Device

Configure your router or SD-WAN device to route traffic through Check Point Network Securityas-a-Service as follows:

- **STEP 1** | Select the card that represents your site.
- **STEP 2** | Select Menu > View Instructions.



STEP 3 Get the IPsec configuration properties, pre-shared key, tunnel addresses, and the traffic routes by viewing the instructions.



Support for Multiple External IP Addresses

A common use case is a branch office with more than one Internet link. In case your branch office site has more than one Internet link, repeat the steps above in order to create another site.

• At the Router Details page, the External IP should represent the other IP address of your branch office site.



This IP must be static and accessible from the Internet. You can track Check Point's updates regarding support of other topologies at this User Community thread.

- At the **Site Details** page, the **Location of the cloud service** should be a different location than the one defined at the original site object. This is because of a technical limitation at the Check Point side. In this case, typically you would want to select the location of the cloud service with an option that is the second-closest to the location of your site, in order to achieve the best performance.
- After your other **Site** is ready, get the **IPsec configuration properties**, **pre-shared key**, **tunnel addresses**, and the **traffic routes** by viewing the instructions.

Technically, that would mean that one of the Internet links will have 2 redundant IPsec tunnels served in a location closest to the branch, while the other Internet link will have 2 tunnels at the second-closest location to the branch.

Check Point can modify the internal configuration so that each Internet link would get one tunnel at the closest location and one tunnel at the second-closest location, therefore having good performance on both outbound interfaces.

In order to have that enabled, please open a support ticket at Check Point.

- Subject of the ticket should be Please change the internal configuration of my IPsec tunnels.
- **Product** should be set to **Network Security as a Service**.
- **Description** should include:
 - Your account name at Check Point Infinity Portal.
 - The names of the 2 or more sites that represent the same branch office.

This practice can be repeated for more than two external IP addresses per branch office site.

For the remainder of this guide, we will assume one external IP address, as this process can easily be repeated for each additional tunnel.



Set up Prisma SD-WAN Overview

To set up Prisma SD-WAN, log in to the Prisma SD-WAN portal, followed by creating an IPsec Profile, creating a service group, assigning IPsec tunnels to your site, and finally, testing the overall configuration.

- > Create an IPsec Profile
- > Create a Service Group
- > Assign IPsec Tunnels to your Site
- > Test the Configuration
- > Monitor Cybersecurity Events at the Check Point Infinity Portal

Create an IPsec Profile

To create an IPsec Profile:

STEP 1 | Navigate to **Policies** > **Stacked Policies**.



STEP 2 | Click **IPsec Profiles**.

X Software-D	efined Enterprise V	VAI × +								-	- 0	×
$\leftrightarrow \ \Rightarrow \ G$	https://pc	ortal.elcapita	in.cloudgenix.co	m/#policies/bindings				07	☆	0 😐	•	
CLOUD	GENIX	мар		ACTIVITY								E
				Network Contexts (0)	Circuit C	ategories (64)	Apps (518)	Service & DC	Groups	(2) IPs	ec Profile	s (5)
Bindings (1)	Path (3)	QoS	(3)									
		SITE TA	AGS	PATH STACK		QOS STACK		POLICY TYPE		GROUP	BY	
▼ Filter on	site name	View	All	View All	~	View All	\sim	View All	~	None		~

STEP 3 Click Add IPsec Profile.

X Software-Defined Enterprise WAL ×	+						-		×
\leftrightarrow \rightarrow C $$ https://portal.elcapi	tan.cloudgenix.com/#	policies/binding	gs/ipsecprofiles		☆	0	8		: 0
CLOUDGENIX MAP	POLICIES	ACTIVITY							≣
< Bindings IPsec Profiles (5)									
FILTER (by iPsec profile name, description)	FILTER (by tags)	~	Showing 5/5 Items	Γ		🗘 AD	D IPSE	C PROF	R.E.
NAME -	IKE GROUP		ESP GROUP	AUTHENTICATION		UPD	C		-

A wizard for adding an IPsec profile will display.

STEP 4 Define a **name** and **description**, and click **Next**.



STEP 5 | Edit the **IKE settings** of the IPsec profile.

→ C http:	s://port	al.elcapita	n.cloudgenix.com/#p	policies/bindings/ip	secprofile	is 🛣 🕐	2	•	J
undefined Policie	es								
CHECKPOINT ike v	T_IF 2 ipsec	CEV2							
		Info	🥑 IKE Group	SESP Group	0	Authentication	1	Sur	nma
KEY EXCHANGE		LIFET	IME	REMOTE PORT		REAUTH			
IKEv2	V	24		500					
	-	(1 - 72	hours)	(1 - 65535)					
Proposals (8 max	X)								
DH GROUP			ENCRYPTION		HASH				
MODP-1024		V	AES-256	~	SHA-1			V	
Add Proposal									
DPD									
ENABLE DPD?									
• Yes No									
DPD DELAY									
10									
10 T									

BACK

- Key Exchange should be set to IKEv2. IKEv1 is also supported.
- DH Group should be set to MODP-1024.
- Encryption should be set to AES-256.
- Hash should be set to SHA-1.
- **DPD** should be **enabled**.

STEP 6 Click Next.

STEP 7 | Edit the **ESP Group** settings.

	portaneicopia	incloudgenix.com/ap	oncres/ bindings/ ip	seepromes д 🗸	
undefined Policies					
CHECKPOINT CHECKPOINT ike v2 in	_IKEV2				
	🕑 Info	IKE Group	SP Group	Authentication	Summary
LIFETIME	ENC/	PSULATION			
8	Force	UDP V			
(1 - 72 hours)	_				
Proposals (8 max)					
		ENCRYPTION		HASH	
DH GROUP					

	_
BACK	NEXT

- Encapsulation should be set to Force UDP
- At the **Proposals** section, there should be 1 proposal with the following settings:
 - DH Group should be set to None
 - Encryption should be set to AES-256
 - Hash should be set to SHA-1

STEP 8 Click Next.

STEP 9 | Edit the **Authentication** settings.

X Software-Defined B	Enterprise W/	+ × ×				- 🗆 ×
← → C ●	https://por	tal.elcapitar	.cloudgenix.com/#p	olicies/bindings/ipse	cprotiles 🛠 Օ	😐 🖻 i 🕕 i
< undefined Po	olicies					SAVE & EXIT
CHECKPO		KEV2				
CHECKPOINT	ike vz ipsed	c prome				
			V IKE Group	esp Group	Authentication	Summary
TANE		SECRE	(unmask)			
PSK	~					
LOCAL ID TYPE		REMO	I E ID (optional)			
Interface IP Add	dress 🗸					

BACK	NEXT
------	------

- Type should be set to PSK.
- Secret should be set to the pre-shared key of the Check Point Site that you copied at the previous steps.
- Local ID type should be set to Interface IP Address

STEP 10 | Click Next, review the settings of the profile, then click Save & Exit.



Create a Service Group

A Service Group is a set of tags and labels representing the integration with Check Point. This lets the user get an overview of the association between Prisma SD-WAN devices and third-party integrations.

To create a Service Group:

STEP 1 Navigate to **Policies** > **Stacked Policies**.

STEP 2 Click Service & DC Groups.

← → C 	X Software-Defined Enterprise WAL X	+							-		×
CLOUDGENIX MAP POLICIES ACTIVITY	← → C ≜ https://portal.eld	capitan.cloudgenix.com//	policies/path/sets				0v 🕁	0		0	1
Network Contexts (1) Grout Categories (2) Apps (10) Service & DC Groups (2) Place Profiles (2)	CLOUDGENIX MAI	POLICIES	ACTIVITY								≣
	Bindings (1) Path (3)	QoS (3)		Network Contexts (0)	Circuit Categories (64)	Apps (518) Serv	rice & DC Groups (2)	IPse	c Profil	les (5)	

STEP 3 Click **Endpoints**.

X Software-Defined Enterprise WAL X +		-		×
← → C ≜ https://portal.elcapitan.cloudgenix.com/#policies/path/sets	o+ ☆	0 🖬 🛛		
< Policies		E	XIT	
Filter on group or endpoint name stres				

STEP 4 Change the view from **Prisma SD-WAN** to **Standard VPN**.



Software-Defined Enterp	rise WAI × +					-	
ightarrow $ ightarrow$ $ ightarrow$ $ ightarrow$ https	//portal.elcapitan.cloudgenix.com/#p	policies/path/sets	07	☆ C		•	G
< Policies						EXI	ŕ
Endpoints							×
▼ Filter on endp	point name			3rd Par	ty		~
Name	Description	Admin Up	Allow Enterprise Traffic				
	Add 🕄	d Endpoint					

STEP 5 Click **Add Endpoint** in order to create a tag for the first tunnel.

STEP 6 | **Name** should be an alias for this tunnel.

In this case, we will name it to **Check Point Tunnel 1**.

- **STEP 7** | Admin Up should be checked.
- **STEP 8** Click **Add Endpoint** in order to create a tag for the second tunnel.
- **STEP 9** | **Name** should be an alias for this tunnel.

In this case, we will name it to **Check Point Tunnel 2**.

- **STEP 10 | Admin Up** should be **checked**.
- **STEP 11** Click Save & Exit.

STEP 12 | At the Groups tab, next to the Domains column, click Add to add a new Domain.



- STEP 13 | Name should be an alias for the Site. In this case, we will name it to Check Point.
- **STEP 14** | Select the **Domain** column that you find that fits this site the most. In these instructions will use **Preset Domain**. Then, select the two **Endpoints** that we defined in the previous step.
- STEP 15 | Click Sites.

STEP 16 | Identify your Prisma SD-WAN device and select the Domain where you associated the Check Point endpoint labels at the previous step. In our case, we will select **Preset Domain**.

X Software-Defined Enterprise WAL ×	÷							- 0		×
← → C @ https://portal.elcapit	an.cloudgenix.com	/#policies/path/sets				아 ☆	0		0	:
< Policies								EXIT		
Filter on site or domain name	TYPE View All	~	GROUPS	SITES						
Site	Туре	Domain		🖌 Edit All						
CheckPoint Demo Lab	Brench	US West Asia EU Preset Domain US East US West	1	~						

STEP 17 | Click Save.

X Softwa	are-Defined Enterprise WAL	+								- 1		×
$\leftarrow \ \rightarrow$	C A https://portal.elcap	pitan.cloudgenix.com/#p	olicies/path/sets				04	¢	0		0	:
< F	Policies									Đ	л	
Y F	Filter on group or endpoint ner	ne		GROUPS	SITES	1	ENDPOINTS			5AN	VE	

Assign IPsec Tunnels to your Site

To assign IPsec tunnels to your site:

STEP 1 Click the **MAP** tab.



STEP 2 | Locate your device on the map, and then click it.

X Software-Defined Enterprise WAL X +			- 🗆 ×
← → C 🕯 https://portal.elcapitan.	cloudgenix.com/#map/site/1555959649851	0059	ov 🛧 🚺 🖬 🗉 🗊 🗄
CLOUDGENIX MAP	POLICIES ACTIVITY		· E
© Search site name or address	ALARM STATUS View All	View All View All	Clessic Mep
× 8+	Demo Lab 2665 N 1st St, Suite 110, San Jose, CA 95	X ISI, United States	+
8	CONNECTIVITY Physical: 2 of 2 Secure Fabric: 0 of 0 2rd Patrix: 4 of 4	ALAIMS Critical: 0 Minor: 0	
2	INTERNET CIRCUITS	PRIVATE WAN CIRCUITS There are no private WAN circuits Add Circuits	
	DEVICES	IP PREPORES There are no IP prefixes Add IP Prefixes n 2000)	
	OPTIONS Lest Updated Fri Apr 26, 2019, 2:35:52 pm	SITE DETAILS	
Last Undered Eri Avr 25, 2019, 2,35,42 nm			Feedbark Oldenby ChreeStreethan

- **STEP 3** | Click the device to edit its settings.
- **STEP 4** Navigate to **Interface Config**.
- **STEP 5** Add the first IPsec tunnel.

STEP 6 Click the + icon near the ports, select **Standard VPN**, and click **Add**. The **Tunnel Configuration** page will open.



- **STEP 7** Name should be an alias for this tunnel. In this case, we will name it to **Check Point Tunnel 1**.
- **STEP 8** | Admin Up should be a.
- **STEP 9** | **Parent Interface** should be set to the **outbound interface**.
- **STEP 10 | Inner Tunnel IP / Address Mask** should be set to an **internal IP** behind your device that you should allocate for the tunnel.
- **STEP 11 | Endpoint** should be set to the Endpoint that represented a tunnel defined in the previous step. In our case, this should be set to .
- **STEP 12 | Peer Hostname** should be set to the destination of the **first Check Point tunnel** that you copied from the previous steps.
- **STEP 13 | Peer IP** should remain empty.
- STEP 14 | IPSec Profile should be set to the IPsec Profile that we defined at the first step.
- **STEP 15** | Click **Create Standard VPN**. An indication at the top-right corner should appear in case the tunnel was created successfully or not.
- **STEP 16** | Click **Cancel** to go back to the interface configuration.
- **STEP 17** | Repeat this process for the **second** IPsec tunnel.

After creating the second IPsec tunnel, once again, an indication at the top-right corner should appear in case the tunnel was created successfully or not.

STEP 18 | Click **Cancel** to go back to the interface configuration.

Test the Configuration

To test the overall configuration:

- **STEP 1** Send traffic from behind your **Site** to the **Internet**.
- **STEP 2** | Navigate to **Activity**.
- **STEP 3** Check that the traffic is displayed.



Monitor Cybersecurity Events at the Check Point Infinity Portal

In the previous step we confirmed that end-to-end connectivity is working as expected. In this step, we will observe which attacks were prevented by Check Point's various cybersecurity engines.

STEP 1 | Sign in to the Check Point Infinity Portal at https://portal.checkpoint.com.



STEP 2 Once you are logged into the Check Point Infinity Portal, make sure that you are currently looking at the **Network Security as a Service** application.



STEP 3 | If the title says a name of a different application, click the application switcher icon at the top-left corner () and select **Network Security as a Service**.







- **STEP 5** Click the **Cyber Attack View** tab to observe attacks that were prevented by Check Point.
- **STEP 6** | Click the **Access Control** tab to observe malicious applications that were prevented by CheckPoint, as well as total consumed traffic and visibility at the applications that were access the most by your end-users.
- **STEP 7** | Click the **Application and URL Filtering** tab to generate a real-time report of your branch office cybersecurity posture. You can export this report to PDF by clicking the **Menu** at the top-right.

STEP 8 | Navigate to **Policy** to view and change your security policy for access control, threat prevention, and HTTPS inspection.



Changes to security policies are not applied until clicking **Install Policy**.

