

Netskope Integration Guide

1.0.0

docs.paloaltonetworks.com

Table of Contents

Prisma SD-WAN Netskope Integration	4
Set up the Netskope Security Cloud	5
Configure Prisma SD-WAN Tunnels to Netskope Security Cloud	11
Create an IPsec Profile	11
Create a Service Group	12
Create an IPsec Tunnel	14
Create a Path Policy	17
Verify the Configuration	18
Monitor Cybersecurity Events on the Netskope Portal	20



Prisma SD-WAN Netskope 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 cumbersome policies for direct-to-internet versus policy enforcement per-application. Router-based approaches are packet-based versus application-session based and fail to meet application session-symmetry requirements, causing network and security outages.

You can integrate Prisma SD-WAN with Netskope Security Cloud to have a remote office hardware, while still having a full suite of application-specific security policies.

Set up the Netskope Security Cloud

Integrate prisma SD-WAN with Netskope to have a lightweight remote office hardware footprint along with a full suite of application-specific security policies.



Set up the Netskope security cloud.

STEP 1 | Log in to **Netskope**.

← → C 🔒 alliances.eu.goskope.com/ns#/da	shboard		아☆ 🛪 😫 🗄								
⊷ ° <	Welcome to Your New Dashboard To set up, tell us about how you use Netskope Security Cloud Platform.										
A Home	Select all that apply.										
▲ Incidents >	D										
🖹 API-enabled > Protection	Risk Insights	API-enabled Protection									
🔮 Policies 🔷 🗲	I am uploading log data to learn about my cloud usage. I want the dashboard to report on usage	I am monitoring and controlling data stored in my sanctioned applications. I want the									
E Cloud > Infrastructure	metrics like top applications, users, and other risky trends.	dashboard to tell me about DLP incidents and other policy violations.									
₿ Skope IT* >											
👄 CCI	h	,									
ពីថា Reports	Real-time I am steering traffic thro time. I want the dashboa like top applications, and violations.	Protection ugh Netskope in real- rd to show me metrics mmalles, and policy									
Settings	If you wish to set up your dashb	oard manually, skip this step .									
Help Account	CREATE DAS	HBOARD	Feedback								

STEP 2 | Navigate to **Settings**.

~	General	
Settings	Here you can see the software versions and the data sources used to populate the data.	IONITORING
General	Software Version	
Administration	> Netskope Version: 82.10.374	
Security Cloud Platform		
Risk Insights	Data Source	
API-enabled Protection	> Source: All Data Sources	
Threat Protection	EDITSOURCE	
Incident Management		
Manage	>	
Tools		

STEP 3 | Select Security Cloud Platform.

*	General	
← Security Cloud Platform	Here you can see the software versions and the data sources used to populate the data.	VIEW SERVICE MONITORING
Configuration	Software Version	
TRAFFIC STEERING	Netskope Version: 82.1.0.374	
App Definition		
Publishers	Data Source	
IPSec	Source: All Data Sources	
Explicit Proxy	EDIT SOURCE	
NETSKOPE CLIENT		
Users		
Groups		
Devices		
Enforcement		
SAML		
MDM Distribution		
REVERSE PROXY		
Help		
Account		۲

STEP 4 | Select **IPSec**.

≁	Security Cloud Platform > Traffic Steering > IPSec
← Security Cloud Platform	Create and manage secure IPSec tunnels from your source devices such as routers and firewalls to Netskope's point of presence(POPs). View Supported IPSec Options here.
Configuration	ADD NEW TUNNEL IMPORT TUNNELS FROM CSV
TRAFFIC STEERING	IPSec Tunnels 1 TUNNELS Sort by: Name ~ ENABLE DISABLE DELETE
App Definition	STATUS NAME C SOURCE IDENTITY PRIMARY POP ENCRYPTION THROUGHPUT
Publishers	↑ CloudGenix - Test cloudgenix@paloal 8.36.116.114 (SV5 AES256-CBC 250.09 Kbps ···
GRE Evolucit Provv	 ⊀ 1 ▶ Rows per page: 10 -
- NETSKOPE CLIENT	
Users	
Groups	
Devices	
Enforcement	
SAML	
MDM Distribution	

STEP 5 | Add a new IPsec tunnel.

1. Click Add New Tunnel.

≁	IPSec							
← Security Cloud Platform	Grafe mittin vir 102 Voldergeyna Ken fly	Add New IPsec Tunnel		×				
Configuration		Tunnel Peers Traffic will be steered from your sou best performance, select the geogra	rce devices to Netskope points of presence(PO phically closest POPs. Only IKEv2 is supported	Ps). For				
Steering Configuration		Note: Use the Netskope POP's IP address as tunnel's remote identity.						
App Definition Publishers		Enter a name to remember the tunnel by						
IPSec			X@)					
GRE Explicit Proxy	- 3 A	SOURCE IP ADDRESS						
NETSKOPE CLIENT		SOURCE IDENTITY * Enter IP Address or FQDN						
Users Groups		Specify the Source Identity PRIMARY NETSKOPE POP *	FAILOVER NETSKOPE POP *					
Devices		74.217.93.116 (DC11 - Ashb	31.186.239.114 (AM2 - Ams *					
Enforcement SAML		PRE-SHARED KEY (PSK) *	unique across an in sec tunnels set up.					
MDM Distribution			4 <u>6</u>					
SAML		AES128-CBC -						
Office 365 Auth		MAXIMUM BANDWIDTH * Maximum bandwidth to be used by the IPS	Sec tunnel					
ActiveSync Auth Integration		50 Mbps 👻						
FORWARD PROXY		CANCEL		ADD				
SAML								

- 2. Enter a name for the tunnel.
- 3. Enter the IP address or the unique FQDN of the Prisma SD-WAN tunnel endpoint.
- 4. Choose the geographically closest Netskope POP as the Primary and choose a failover Netskope POP.
- 5. Enter a Pre-Shared key.
- 6. Configure an encryption cipher.
- 7. Configure the Maximum BW to be used by the IPsec tunnel.

No rate limiting happens based on the configured bandwidth.

8. Click Add.

When you click **Add**, the IPsec tunnel entry can be seen.

9. Verify the status of the tunnel.

An upward arrow indicates the tunnel is **UP**.

^₽	Security Cloud Platform > IPSec	Traffic Steering >				
← Security Cloud Platform	Create and manage secur View Supported IPSec Op	re IPSec tunnels from your source otions here.	e devices such as route	rs and firewalls to Netsk	ope's point of pres	ence(POPs).
Configuration	ADD NEW TUNNEL	IMPORT TUNNELS FROM CSV]			
TRAFFIC STEERING						
Steering Configuration	1 TUNNELS		Sort by: N	ame ~	ENABLE	DISABLE
App Definition	STATUS	NAME 🕈	SOURCE IDENTITY	PRIMARY POP	ENCRYPTION	THROUGHPUT
Publishers	□ ↑	CloudGenix - Test	cloudgenix@paloal	8.36.116.114 (SV5	AES256-CBC	280.57 Kbps
GRE	< 1 →					Rows per page: 10 -
Explicit Proxy						
NETSKOPE CLIENT						
Users						
Groups						
Devices						
Enforcement						
SAML						
MDM Distribution						
REVERSE PROXY						
SAML						
Office 365 Auth						
ActiveSync						
Auth Integration						
FORWARD PROXY						
SAML						

10. (Optional) Click the ellipsis next to the tunnel entry to see additional options to edit and view tunnel configuration parameters.

*	Security Cloud Platform > Traffic Steering >	Tunnel Details ×
 ← Security Cloud Platform 	IPSEC Create and manage secure IPSec tunnels from your source devices such as route View Supported IPSec Options here.	CloudGenix - Test Tunnel Status: ① Up Since Mar 3 2021 (Today) Throughput: 306.25 Kbps Connected th: Primary
Configuration	ADD NEW TUNNEL IMPORT TUNNELS FROM CSV	Encryption: AES256-CBC
	IPSec Tunnels Sort by: N 1 TUNNELS	Max Bandwidth: 250 Mbps cloudgenix@paloalto
App Definition	STATUS NAME C SOURCE IDENTITY	6.30.110.114 (5V5 - San Juse, CA, US)
Publishers	↑ CloudGenix - Test cloudgenix@paloal	SOURCE PEER
IPSec		Source IP Address:
GRE	4 1 ▶	boli ce rachtery. clougening publice
Explicit Proxy		PRIMARY NETSKOPE POP
NETSKOPE CLIENT		Probe IP Address: 192.168.104.144
Users		Location: SV5 - San Jose, CA, US
Groups		FAILOVER NETSKOPE POP
Devices		IPSec Gateway: 163.116.133.38 Probe IP Address: 10.133.6.216
Enforcement		Location: ORD1 - Chicago, IL, US
SAML		EDIT CONFIGURATION
MDM Distribution		
REVERSE PROXY		Status Last Updated: Mar 3 2021, 11:26 AM
SAML		
Office 365 Auth		
ActiveSync		
Auth Integration		

- The throughput capacity refers to the actual traffic going through the tunnel.
- Save the probe IP address to be used later in the Prisma SD-WAN endpoint configuration for liveliness checks.

Configure Prisma SD-WAN Tunnels to Netskope Security Cloud

Use the following steps to configure Prisma SD-WAN tunnels to the Netskope security cloud.

- **STEP 1** | Create an IPsec profile.
- **STEP 2** | Create a service group.
- **STEP 3** | Create an IPsec tunnel.
- **STEP 4** | Create a path policy.
- **STEP 5** | Verify the configuration.

Create an IPsec Profile

Create an IPsec profile on the Prisma SD-WAN web interface.

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

	MA SD-WAN	🙆 Dashba	oard 🛝	IMap Ƴ	Policies	Y Act	tivity 🛸 CloudBlad	es	
		Network C	ontexts (0)	Circuit Ca	ategories (64)	Apps (528)	Service & DC Groups (1)	IPsec Profiles (5)	DNS Service (11)
Bindings (3)	Path (2)	QoS (1)	Security (2) 🕨	IAT (1)				
FILTER (by site	name)	SITE TAGS		POLICY T	YPE	GROUP BY			
Ŧ		View All	\sim	View All	~	None	~		
SITE 🔻			PATH POLIC	CY SET STACE	к	QOS PO	DLICY SET STACK	SECURITY	POLICY SET STACK

STEP 2 | Click Add IPsec Profile.

STEP 3 On the **Info** tab, enter a name and an optional description.



STEP 4 Configure IKE settings.

						🗢 Info 🔗 INE (Croup 0 ESP Group	Authentication	Sammary
EY DICHANGE		LIFETIME			REMOTE PORT		REAUTH		
@v2	~	24 (1 - 72 hours)			500 (5 - 45533)				
Proposals (1 mm) IN GROUP	ENCRYPTION		HASH						
10DP-2048 (Group 14) V	A85-256-CBC	~	3HA-230	~					
A Att Brown									
•									
OPD									
NARLE DPD1									
IPD DELAY									

- Netskope Security Cloud supports IKEv2 configuration only.
- Netskope supports the following encryption ciphers: AES128-CBC, AES192-CBC, AES256-CBC.
- Netskope supports the following hash algorithms: SHA256, SHA384, SHA512.
- Netskope supports the following DH Groups: 14, 15, 16, 18.
- DPD must be enabled.

STEP 5 Click **Next**.

STEP 6 Configure **ESP Group** settings.

Back to IPsec Profiles NETSKOPE_IKEv2									Sour & Dat
					O Info	😒 IKE Group	🔮 ESP Group	Authentication	Summary
UPETIME	ENCAP	SULATION							
0 (1 - 72 hours)									
Proposals (8 mix) DH GROUP	ENCRYPTION		HASH						
MODP-2048 (Group 14) V	AES-256-CBC	~	SHA-256	~	=				
Add Propesal					-				

- Netskope supports the following encryption ciphers: AES128-CBC, AES256-CBC, AES128-GCM, AES192-GCM, AES256-GCM, Null.
- Netskope supports the following hash algorithms: SHA256, SHA384, SHA512.
- Netskope supports the following DH Groups:14, 15, 16, 18.

STEP 7 Click Next.

STEP 8 On the **Authentication** tab, select **None** for **Type**.

This is because authentication settings will be configured locally on the device using an IPsecauthentication override.

STEP 9 Click **Next**, review the settings of the profile and then click **Save & Exit**.

Create a Service Group

A service group is a set of labels that associate the Prisma SD-WAN ION with a NetskopeEndpoint.

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

STEP 2 Select Service & DC Groups.

	MA SD-WAN	🙆 Dashbo	ard 🍂	I Map Ƴ	🛛 Policie	• ¥ 4	Activit	y 🛳 CloudBlad	9 5	
		Network Co	ontexts (0)	Circuit C	ategories (64)	Apps (528) Se	rvice & DC Groups (1)	IPsec Profiles (5)	DNS Service (11)
Bindings (3)	Path (2)	QoS (1)	Security (2)	NAT (1)			v		
FILTER (by site	name)	SITE TAGS		POLICY 1	TYPE	GROU	JP BY			
T		View All	\sim	View All	~	None		~		

STEP 3 Click **Endpoints**.

< Policies			Dit .
Tiller or group or endpoint name	arcurs	3112	Engenites
Domains 0 444 #	huset Domain 🔹 🔤		
Groups O Add			

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

						Prism	na SD-W
Name	Only endpoint	used in saved gro	Admin Up	wn.		Stand	lard VPN
Data Center			\checkmark				
					Car	ncel	Save
ndpoints							
ndpoints Filter on endp	oint name				-	Standa	ard VPN
Indpoints Filter on endp Name	oint name		Admin Up	Allow Enterp Traffic	rise	Standa	ard VPN
ndpoints ▼ Filter on endp Name	oint name Description	Add Endpoint	Admin Up	Allow Enterp Traffic	rise	Standa	ard VPN

- **STEP 6** Give the endpoint a name and check the **Admin UP** box.
- **STEP 7** | Click **IPs & Hostnames**.

STEP 5 | Click Add Endpoint.

STEP 8 | Enter a comma separated list of the Netskope Primary and Failover POP IP addresses and click **Done**.

Prisma SD-WAN will check RTT for each of these IP addresses and will automatically choose the destination with the lowest latency as the IPsec tunnel endpoint.

IETSKOPE	
IP ADDRESSES	HOSTNAMES
8.36.116.114, 163.116.133.38	e.g. en.wikipedia.org, hello.example.net

STEP 9 Click Liveliness Probe.

NETSKOPE	Description	\checkmark	Address IPs & Hostnames
			Liveliness Probe

STEP 10 | Configure the Probe IP Address from Netskope Tunnel configuration along with ICMP ping interval and failure count and click **Done**.

The probe IP address in the Netskope Security Cloud will be pinged to check liveliness of the tunnel. In the example below, an ICMP packet will be sent once every 10 seconds. When 3 consecutive pings fail, the tunnel will be declared Down.

PING (MAX 4) G Add ICMP Ping	HTTP (MAX 4) O Add HTTP
NTERVAL (1 TO 30 SECONDS)	INTERVAL (10 TO 3600 SECONDS)
10	
AILURE COUNT (3 TO 300)	FAILURE COUNT (3 TO 300)
3	
PADDRESS	HTTP STATUS CODES
192.168.104.144	

STEP 11 | Click Save & Exit.

STEP 12 At the **Groups** tab, under the **Domains** column, against the **Groups** row, click **Add** to add a new group.

Policies					
Filter on group or end	dpoint name		GROUPS	SITES	
	Domains 🚯 Add	Preset Domain ★		Mohan Internet	

STEP 13 | Select Standard VPN.

STEP 14 | Give the group a name and in the **Endpoints** drop-down, choose the endpoint that was just configured.

Filter on group or endpoint name	GRC	DUPS	SITES
Domains 🔮 Add	Preset Domain ★	-	
Groups 🚭 Add			
	NETSKOPE	~	

STEP 15 | Click Save.

Create an IPsec Tunnel

- **STEP 1** | Navigate to **Map** > **Claimed Devices**.
- **STEP 2** | Click the ellipsis menu for the device to be configured with the IPsec tunnel and select **Configure the device**.

- **STEP 3** | Select Interfaces.
- **STEP 4** | Click the + sign on the Interface panel.
- **STEP 5** Select **Standard VPN** and click **Add**.

B							Basic Info	Device Toolkit	Interf	aces	Routing	SNMP	Syslog Export	NTP Client	DNS Service	IPF
												CR	REATE A N	EW INTE	RFACE	
	CONTROLLER				VIE	TUAL PO	ORTS					() Loopba	ck ul VDN		
											÷	k d	Virtual I	nterface		
	C1	1	2	3	4	5	6	7	8	9			Port Ch	annel		
													c	ancel	Add	
TER (by Name, Circuit, IP Address)	INTERFA	CE TYPE			USE	O FOR		1	TAGS							
				~				~				\sim				
INTERFACES	TYPE		ADM	1IN STA	TUS		CONFI	GURATI	ION		CI	RCUITS				
controller 1	Controller Port		Up				Control • STA	ler FIC								
Internet Virtual Interface	Virtual Interface		Up				The Inte	emet				Circuit to	Internet			•••
members: Ports (z)							• DHC	.P								

STEP 6 On the tunnel configuration page, configure the following:

Main Configuration	Sub-Interfaces (0)	PPPoE		
INTERFACE TYPE		Standard VPN		
TANDARD VPN TYP	E	IPsec		
PARENT INTERFACE		Port 1	\sim	
SCOPE		() 🕑 Local		
INNER TUNNEL IP ADD REQUIRED)	RESS/MASK	192.168.1.1/31		
Configuration				
ENDPOINT		NETSKOPE	~ L	Ipdate
PEER HOSTNAME		optional		
PEER IP				
PSEC PROFILE		NETSKOPE IKEv2	V E	dit I Add

- Give the tunnel a name.
- Configure the **Standard VPN** type as **IPsec**.
- Parent interface should be set to the outboundinterface.
- Inner Tunnel IP / Address Mask should be set to an internal IP behind your device that you should allocate for the tunnel.
- Set the **endpoint** configured from the previous step.
- **Peer IP** can be used to configure the Netskope endpoint's IP. This configuration is skipped in this example, since the endpoint configuration in the previous step has the Netskope POP's IP addresses configured already.
- Select the IPSEC Profile that was created for Netskope.
- Add an **IPSEC Authentication Override** to configure IPsec authentication settings local to the site.

		CONTROLLER 1		10E 3 4 5			
Configure Interface	: New 3rd Party	/ VPN					
Main Configuration	Sub-Interfaces (0)	PPPoE					
INTERFACE TYPE		3rd Party VPN					
STANDARD VPN TYPE		IPsec	~				
PARENT INTERFACE		Port 1	~				
SCOPE		(Cocal					
INNER TUNNEL IP ADDR (REQUIRED)	ESS/MASK	192.168.1.	1 / 31				
Configuration							
ENDPOINT		NETSKOPE-IPSEC	~ u	Ipdate			
PEER HOSTNAME		optional					
PEER IP							
IPSEC PROFILE		NETSKOPE_IKEv2	~ E	dit Add			
	N OVERRIDE	Add					
IPSEC AUTHENTICATION							
IPSEC AUTHENTICATION							
IPSEC AUTHENTICATION							
IPSEC AUTHENTICATION					_	_	-
ec Authenticatio	n Override						
ec Authenticatio	n Override						
ec Authenticatio	n Override	SECRET (unmask)					
ec Authenticatio	n Override	SECRET (<u>unmask</u>)					
ec Authenticatio	n Override	SECRET (unmask)		REMOTE ID (opt	ional)		
ec Authenticatio	n Override	SECRET (urmask) LOCAL ID cloudgenix@paloa	to	REMOTE ID (opt	ional)		
ec Authentication	n Override	SECRET (unmask) LOCAL ID cloudgenix@paloa	to	REMOTE ID (opt	ional)		
IPPEC AUTHENTICATION	n Override	SECRET (unmask) LOCAL ID cloudgenix@paloa	'to	REMOTE ID (opt	ional)		

- **Type** should be Pre-Shared Key.
- Configure the same Pre-shared key at both the Prisma SD-WAN and Netskope endpoints.

- Local ID can be set to Interface IP Address or FQDN.
- To configure a local FQDN, choose **Local ID Type** as **Custom** and configure a FQDN under Local ID.

STEP 7 | Click Create Standard VPN.

Create a Path Policy

Configure a path policy to allow traffic to flow through the IPsec VPN to Netskope Security Cloud.

- **STEP 1** Navigate to **Policies** > **Stacked Policies**.
- **STEP 2** Select **Path** and then **Path Sets**.
- STEP 3 | Click Add Set.

PRISMA SD-WAN	🙆 Dashb	oard 🖡	🔰 Map 🚿	🥏 Po	olicies 🗸	Activity	🛳 CloudBlades			
Network Contexts (0)	Circuit Catego	ries (64)	Apps (528	3) Service	e & DC Group	s (1) IPsec Pro	ofiles (5) DNS Ser	vice (11) IPFIX (0)	APN Profiles (0)	Syslog Profiles (4
Bindings (3) Path (2)	QoS (1)	Security	(2)	NAT (1)						
						PATH STACKS	PATH SETS	PATH PREFIXES		
FILTER (by set name)	TYPE			TAGS						
T	View All		~	View All	\sim				🕂 Add Set	
NAME					туре 🔻			POLICY RULES		
DefaultRuleNetworkPolicySet					Default R	tule Policy Set		2		
test					Default R	tule Policy Set		2		
NetworkPolicySet					Policy Se	t		0		

- **STEP 4** Give the path policy set a name and click **Save**.
- **STEP 5** Click the policy set and click **Add Rule**.

	🙆 Dashboard	ili Map Y	🕏 Policies 🛩	/1 Activit	y t	CloudBlades							20 들
< Path Policies NetworkPolicySet (0)		Net	work Contexts (0)	Circuit Catego	ries (64	4) Apps (528)	Service	& DC Groups (1)	IPsec Profiles (5)	DNS Service (11)	IPFIX (0)	APN Profiles (0)	Syslog Profiles (4)
FILTER (by rule, app, circuit category)	View All	ONTEXT	PATH View All		~	TAGS View All	~						Add Rule
ORD - NAME		NET	WORK CONTEXT	SRC PREFIX		DEST PREFI	<	APPS		PATHS		SERVICE & DC GROUP	5

STEP 6 Give the policy rule a name.

Path Policy Set: NetworkPolicySet Untrusted-Web								Sav
		🤗 Info	Network Context	Prefixes	Apps	🕑 Paths	Service & DC Groups	Su
NAME	DISABLE RULE?							
Untrusted-Web								
ORDER								
1024								
1 - 65535								
DESCRIPTION (optional)								
Add a short description								
256 character limit	11							
TAGS (optional)								
4 tags max								

STEP 7 | Navigate to the **Apps** tab next and choose the applications that you want to forward to the Netskope Security Cloud over the Standard VPN.

 Path Policy Set: NetworkF Untrusted-Web 	PolicySet							Save & Exit
			🥑 Info	Network Context	Prefixes	pps 🥑 Paths	Service & DC Groups	Summary
FILTER (by app name) http	APP CATEGORY	туре	SHOW 1 SELECTED	1.PP				
APPLICATIONS (If none selected wi	II use any)		http-l4	ł	http-ri	ic-eomap		
httpactivesync sap-http	oracle-	http	pcsyne	-http	_ pcsyne	-https		

STEP 8 | Navigate to the **Paths** tab and choose the overlay path **Standard VPN** on circuit category **Any Public**.

Path Policy Set: NetworkPolicySet Untrusted-Web				Save & Exit
		 Info Network Context 	Prefixes Apps Paths Service & DC Groups	Summary
SHOW ALL CIRCUIT CATEGORIES				
ACTIVE PATH O Add OVERLAY CIRCUIT CATEGORY	BACKUP PATH O Add	CIRCUIT CATEGORY	L3 FAILURE PATH Add OVERLAY CIRCUIT CATEGORY	
Standard VPN 🗸 ON Any Public 🗸 😑	None		None	

STEP 9 Navigate to the **Service & DC Groups** tab.

Path Policy Set: NetworkPolicySet Untrusted-web								
			🔿 kifo	 Network Context 	O Prefixes	Apps	O Paths	🥏 Service & DC Groups
REQUIRED 0								
ACTIVE MURPHONE		DACKUP						
Netskole	Ť							

- **STEP 10** Under **Active**, choose the Group configured in the previous steps from the drop-down list.
- **STEP 11** | Verify the configuration summary and click **Save & Exit**.

Verify the Configuration

- **STEP 1** Send traffic from the LAN side of the Prisma SD-WAN ION device.
- **STEP 2** On the Prisma SD-WAN web interface, navigate to the **Activity** tab.

PRISMASD-WAN	🙆 Dashboard	AU Map Y	🕏 Policies 🗸	A Activity	🛳 CloudBl	ades	🚊 suj	er@mohan.com ❤	20 皆	
Showing Activity from	Dec 02, 2021	9:11 AM	to Dec 03.	2021 9:11	AM view	ed by Summary			C Datase	
									C Refresh	
Quick Filters	Network	Media Lin	k Quality Flows	Routing	System C	ellular	TIME FRAME	1H 1D 1W	1M 3M	
Modify filters to save your preferences here.						_				

STEP 3 Verify analytics on the WAN path Standard VPN.

Quick Filters	NETWORK	MEDIA	LINK QUALITY	FLOWS	ROUTING	SYSTEM					1	ME FRAME	SH ID	sw s	м :
inne. Dere Filters	Bandwis every 5 mil	kh Utilizatio	n			SUNMA	ir v	Transaction every 5 miles	Stats				APPS		v
1 Apps (523)	/		-	and Party VPN	Summery		¥ 0 X	∎∮ 15.	ht Succe	utul 🔳 1396 :	Soccentral 📕	int Failure	TXNs Falure	± i	c x
Sites (1)									where they	ind in	the house	the last	made	ndi)	
Devices	Kitas	· • •	lly hybrid	uly.		lan fan	dial Agence	5 5K	and the	-	inima in	أدرسالهم	quéndo	lines	1
Devices	Klas	- Pul	llydydydyd	lihy 	a jutas	lunal ini	and land	50 256	and the second	waying the	(nimeri)	Angereration	quinte	enil ⁱ	
	N N N N N N N N N N N N N N N N N N N			1. Hellow 1200	n jul m		ate () the	5K 103 2.5k 0	Delto	0120	nimmi 200	26.03 26(1997)	976 - 18 10 2020		

STEP 4 Verify flows on the WAN path Standard VPN.

						-									
howing Activity from	i Mari	05, 2021 12:	41 AM to												C is
wick Filters		NETWORK N	IEDIA UNI		NS ROUT	NG SYSTEM							TINE FRAME	14 10	1W 1H
e dify filters to save your prefere ine. ser Filters	nces	Note: Only the > Advanced	last 1000 reco Query 🛓	ods for the given	tine range will	be shown. If yes	don't find	a specific app or	flow of intere	st, try filtering by	"Apps".				
Apps	1	SRC	SRC PORT	DST	DST PORT	POLICY	SEC ACTION	APPLICATION	PROTOCOL	RATH	FLOW DIR.	PKTS	VOL	STARTTIME	LAST ACTIVITY
Sites (1) takopa Darro Sita	1	172.55.100.97	51208	104.192.115.54	443	Untracted-web default (QcG)	NW	Palo Alto Wildline (an- west), wildline.pa loaltoretivoris.c om)	TOP	ATAT For to NETSHOPS- IPSIC	LAN > WAN	38	54.017 NB	Mar 5 2021, 01:40:44.017	Har 5 2021; 01:40:45:125
Devices Netskope ION		172.15.100.97	45856	184,199,115,54	80	Writestel web default (QcS)	NW	Palo Alto Wildhre (elidhre.palouho metworks.com)	TCP	AT&T Fber ta NETSKOPE- IPSEC	UN > WIN	12	188	Mar 5 2021. 004043.925	Mar 5 2021. 01:40:45:125
WANs		172.16.100.97	48037	34.107.215.35	442	Untrasted web default (QcR)	NN	Pala Alta Networks (identity palaalto networks.com)	TOP	ATAT Flair ta NETSKOPE- IPSCC	MN > MM	21	8.221 KB	Mar 5 2021, 00-10-44.458	Mar & 2021, 01:40:45:325
Direct Internet Internet VPN Private WAN VPN		172.35.100.97	33809	34.107.199.164	443	Untrasted web default (QcR)	NA	Palo Alto Networks Orgin.poloaltonet werks.com/	TCP	AT&T Fber to NETSKOPE- IPSEC	UAN > WAN	50	25.515 NB	Mar 5 2021. 85:40:44.882	Mar 5 2021, 01:40:45:100
 Direct Private WAN 3rd Party VPN 		172.15.100.93	34548	67.104.58.111	80	Untrusted web detault (QcS)	NA	Linelight (connect.lineligh	TOP	ATAT Floer to NETSHOPE-	LAN - WAN	12	775 Dytes	Mar 5 2021, 00-40-44.946	Mar 5 2021, 05:40:45:056

STEP 5 | Verify the status of the Servicelink using Device Toolkit.

Netskope ION# dump servicelink status sldev=sl1ServiceLink : sl1Interface : Netskope-1Description :ID : 15748768634780249Type : service_link (ipsec)Admin State : upAlarms : enabledNetworkContextID :Scope : localDirected Broadcast : falseMTU : 1400

IP : staticAddress : 192.168.1.1/31Parent Interface : 1Parent Device : eth5Service Endpoint : NETSKOPE-IPSECIPSec Profile : NETSKOPE_IKEv2Authentication Type : pskLocal ID Type : local_ipKey Exchange : ikev2IKE Reauth : noIKE Lifetime : 24 hoursIKE Remote Port : 500IKE DH Group/Encryption/Hash : modp2048/aes256/sha256ESP Lifetime : 8 hoursESP Encapsulation : AutoESP DH Group/Encryption/Hash : modp2048/aes256/sha256ESP Lifetime : 8 hoursESP Enabled : yesDPD Delay : 1DPD Timeout : 5Authentication OverrideAuthentication Type : pskLocal ID Type : customLocal ID : cloudgenix@paloaltoDevice : sl1State : upLast Change : 2021-03-05 01:49:28.414 (8h10m28s ago)Address : 192.168.1.1/31Route : 0.0.0.0/0 via 192.168.1.1 metric 0

Extended State : tunnel_up

Liveliness probe status-----Type : icmplpv4 :

192.168.104.144Status : trueLatency : 4Last updated : 2021-03-05T01:49:27

Monitor Cybersecurity Events on the Netskope Portal

STEP 1 | Login to the Security Admin portal.

🗢 😑 🗧 PingOne	🗙 📔 🗿 Netskope Global SE Demo - Mij 🗙 🔷	Home - Netskope × +			
$\leftarrow \rightarrow$ C \oplus sedemo.gos	kope.com/ns#/dashboard?timePeriod=90_day				x * 🖰 E
≁ ° <	Home				EDIT v Last 90 days v
A Home	Summary				
▲ Incidents > ♣ API-enabled > Protection ♥ Policies >	APPLICATIONS WE 8880 40 New Applications (5%)	asires 498	users ▲ 444	TOTAL BYTES TOTAL TOTAL BYTES TOTAL 98.1 G8 6% Uploaded, 94% Downloaded	31.5K
Cloud → Infrastructure					
⊜ Skope IT** >	Blocked Categories ()		:	Top Source Locations in All Categories ①	# Sessions *
🗢 CCI	CATEGORIES	#ALERTS		SOURCELOCATION #SESSIONS	
Advanced (Unlim)> Analytics	1 General	13.5K		1 10890 2.08	
	2 Cloud Storage	12.7K		2 Osaka 2.22K	
	3 Prohibited Websites	12.2 K		3 San Francisco 1.52K	
	4 Online Ads	6.75 K		4 Jersey City 1.47K	
	5 Collaboration	986 💻		5 Pittsburgh 1.42K	
	Total Sites Blocked : 3.3	8K, Total Users Blocked : 61			
	Top Users with Compromised Credentials ()		:	DLP Incidents (1)	DLP Profiles *
	USER		#COMPROMISES	DLP PROFILES	# OBJECTS W/ INCIDENTS
	1 mkøyfman+web@netskope.com		158	1 US Personally Identifiable Information	67
	2 dru@netskope.com		24	2 Payment Card Industry Data Security Standard. PCI-DSS	64
	3 matt+web@netskope.com		22	3 Titus Confidential Profile	6
	4 jason+sedemo@netskope.com		18	4 Use Metadata Keywords	1
	5 vladki≊netskope.com		14		
	Vie	w more		View more	
Settings	Malicious Websites (1)		÷	Malware (All Types) 🔘	:
Help	SITE	PUSERS ALLOWED	RUSERS BLOCKED	MALINARE	#FILES AFFECTED #USERS AFFECTED
Account	indemnity360.com/nsw-highways-yqgdk/j63Bl	w' 0	1	Win32.Trojan.Mbt	2 1

STEP 2 | Configure security policies on the **Policies** tab.

🔴 🕘 🌒 🔘 Netskope Glob	al SE Demo - My 🗙 💉 Real-time Pro	ataction - Policies × +	
\leftrightarrow \rightarrow C \triangleq sedemo.	goskope.com/ns#/inline-policy-page	ge?mode=edit&type=public-app&id=65&view=wizard	* * 🖰 ÷
≁ «	Edit [PE] - Catchpo	int Download Test	CANCEL
← Policies	Activities and actions available are de	pendent on the type of profile and applications you selected.	
SSL Decryption	<u>↑</u> Source	Access Methods = IPSec Search for Access Method	x
Real-time Protection		8 Found	
API-enabled		Client	
Protection	Destination	Explicit Proxy	
Scourity Assessment		GRE	
Behavior Analytics		V IPSec	
PROFILES		Local Proxy	
		Mobile Profile	
Threat Protection		Reverse Proxy	
Inteac Protection		Secure Forwarder	
VIED	Action 🖈 Profile & Action	Action: Allow ~	
orro		ADD PROFILE -	
CIEP			
App/Plugin	Set Policy		
Domain	w Set Policy	[PE] - Catchpoint Download Test	
U		+ POLICY DESCRIPTION	
Settings		T EMPRETATION	
Help	Charles and Charles	Enabled	
Account	🐨 Status	+ POLICY SCHEDULE	(0)
	-		

STEP 3 Go to the main dashboard and select **Skope IT** for granular security data.

The **Sites** tab shows URL analytics.



STEP 4 | Click the **Network Events** tab to show user information, application accessed, action taken on this session and bytes transferred.

🔴 😑 🌑 🔘 Netskope Global	SE Demo - M) 🗙 💊 Network Events - Ev	vents - Skor × +									
\leftarrow \rightarrow C \cong sedemo.g	oskope.com/ns#/network-events									☆ *	e :
≁ «	skope IT™> Events > Network Events	S 0								Last 7 Da	ays -
← Skope IT™											
Applications Sites Users	FILTERS ▼ Q Application ~										
EVENTS	Network Events 48 CREATED						Sort by:	Time	¥	EXPORT	
Application Events	TIME \$	USERNAME	APPLICATION	DST PORT	IP PROTO	TRAFFIC TYPE	ACTION	TOTAL BYTES	BYTES U	BYTES D	0
Network Events	④ 3/2/2021 12:27 PM	george+sedemo@netskope.com 🛤	wp-west.npademo.com	HTTP (80)	TCP	PrivateApp	🛛 Allow	737 Bytes	332 Bytes	405 Bytes	
Alerts	④ 3/2/2021 12:27 PM	george+sedemo@netskope.com 👪	📸 nasdaq.fedility.mynetskope	HTTP (80)	TCP	PrivateApp	Allow	21.99KB	16.58KB	5.41KB	
	④ 3/2/2021 12:27 PM	george+sedemo@netskope.com 🏜	Wp-east.npademo.com	HTTP (80)	TCP	PrivateApp	Ø Allow	400.4KB	384.5KB	15.93KB	
	④ 3/2/2021 12:26 PM	george+sedemo@netskape.com ≛	Wp-east.npademo.com	SSH (22)	TCP	PrivateApp	Allow	7.396KB	4.186KB	3.211KB	
	⊕ 3/2/2021 12:26 PM	george+sedemo@netskope.com 🏜	wp-west.npademo.com	HTTP (80)	TCP	PrivateApp	Ø Allow	31.88KB	29.21KB	2.672KB	
	④ 3/2/2021 11:56 AM	george+sedemo@netskope.com 👪	wp-west.npademo.com	HTTP (80)	TCP	PrivateApp	Ø Allow	737 Bytes	332 Bytes	405 Bytes	
Settings	④ 3/2/2021 11:56 AM	george+sedemo@netskope.com 👪	* wp-east.npademo.com	SSH (22)	TCP	PrivateApp	Ø Allow	7.396KB	4.186KB	3.211KB	
Heip Account	⊕ 3/2/2021 11:55 AM	george+sedemo@netskope.com 🛤	wp-west.npademo.com	HTTP (80)	TCP	PrivateApp	🛛 Allow	402.2KB	385.6KB	16.63KB	

STEP 5 Click on **Alerts** to see what policy was applied to a flow and what action was taken on it and if there were malicious objects detected in this flow.

🗧 🗧 🌑 💽 Netskope Global S	E Demo - M) 🗙 📣 Alerts - Events - Sko	ppe IT™ - N × +							
\leftarrow \rightarrow \mathcal{C} \triangleq sedemo.gos	skope.com/ns#/alerts?query=(acked%	20eq%20'false')						☆ *	0 :
	Skope IT™ > Events > Alerts C							Last 7 Days	•
← Ѕкоре П	FILTERS V								
Applications Sites	Q Application ~	Acknowledged: No × + ADD	FILTER T						
Users — Events — — — — — — — — — — — — — — — — — — —	Alerts					Sort by: Time	* ACKN	IOWLEDGE + EXPORT]
Application Events	TIME \$	NAME	TYPE	ACTION	ACTIVITY	POLICY NAME	SITE OBJE	ст	0
Page Events Network Events	① ④ 3/5/2021 3:03 PM	[RProxy Box] Block Downloads	policy	block	Download	[RProxy Box] Block Downloads to	Box 5M	3.mp3	
Alerts	④ 3/5/2021 2:29 PM	[RProxy Box] Block Downloads	policy	block	Download	[RProxy Box] Block Downloads to	Box 5M	3.mp3	
	● 3/5/2021 1:54 PM	[RProxy Box] Block Downloads	policy	block	Download	[RProxy Box] Block Downloads to	Box 5M	3.mp3	
	④ 3/5/2021 1:29 PM	[FINRA Compliance] - Alert use	policy	useralert	Post	[FINRA Compliance] - Alert users	Slack		
	④ 3/5/2021 1:29 PM ⑤	[FINRA Compliance] - Alert use	DLP	useralert	Post	[FINRA Compliance] - Alert users	Slack		
	① ④ 3/5/2021 1:29 PM ③	[FINRA Compliance] - Alert use	DLP	useralert	Post	[FINRA Compliance] - Alert users	Slack		
Settings		[FINRA Compliance] - Alert use	policy	useralert	Post	[FINRA Compliance] - Alert users	Slack		
Help	@ 3/5/2021 1:29 PM	[FINRA Compliance] - Alert use	policy	useralert	Post	[FINRA Compliance] - Alert users	Slack		
Recourt	⊕ 3/5/2021 1:29 PM	[FINRA Compliance] - Alert use	DI P	useralert	Post	FINRA Compliancel - Alert users	Slack		