paloalto TECHDOCS

Netskope Integration Guide

1.0.0

Table of Contents

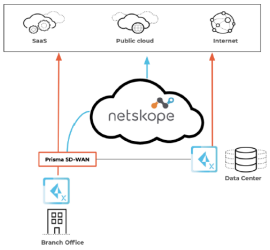
Prisma SD-WAN Netskope Integration

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.

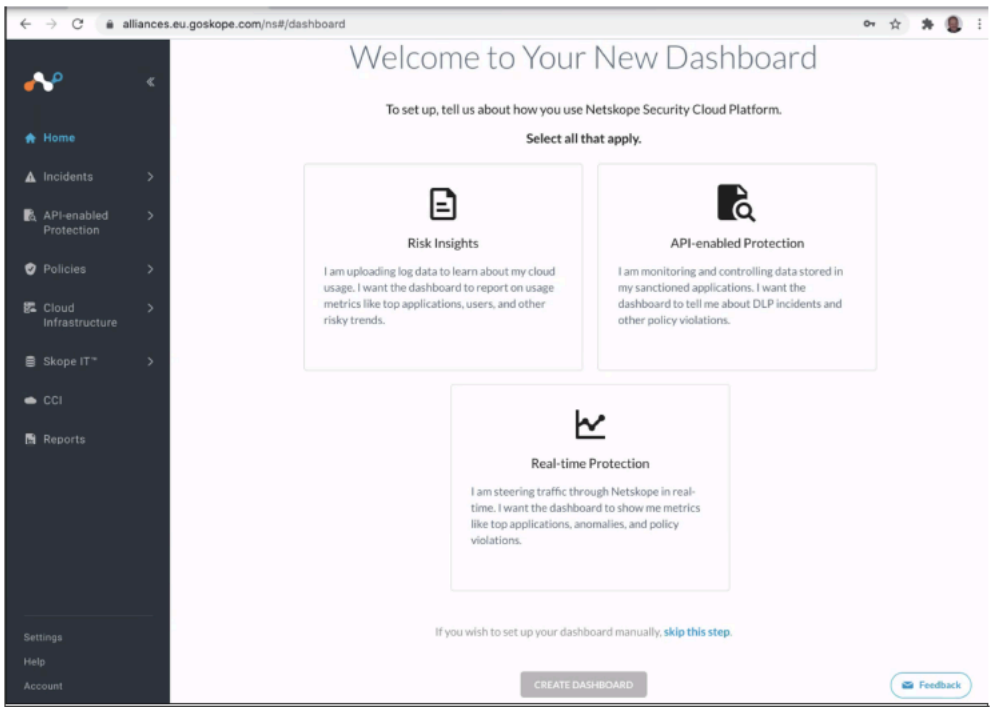
Set up the Netskope Security Cloud

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

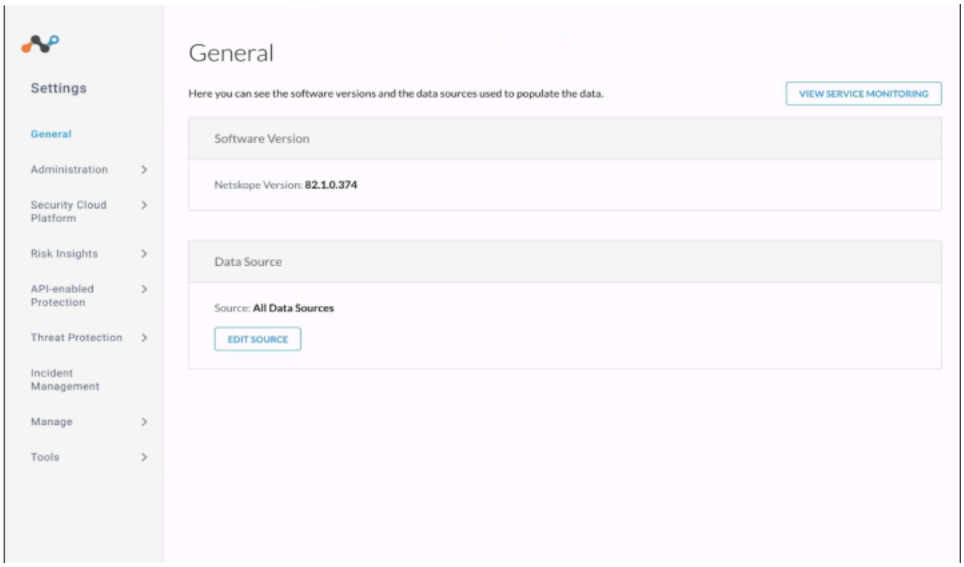


Set up the Netskope security cloud.

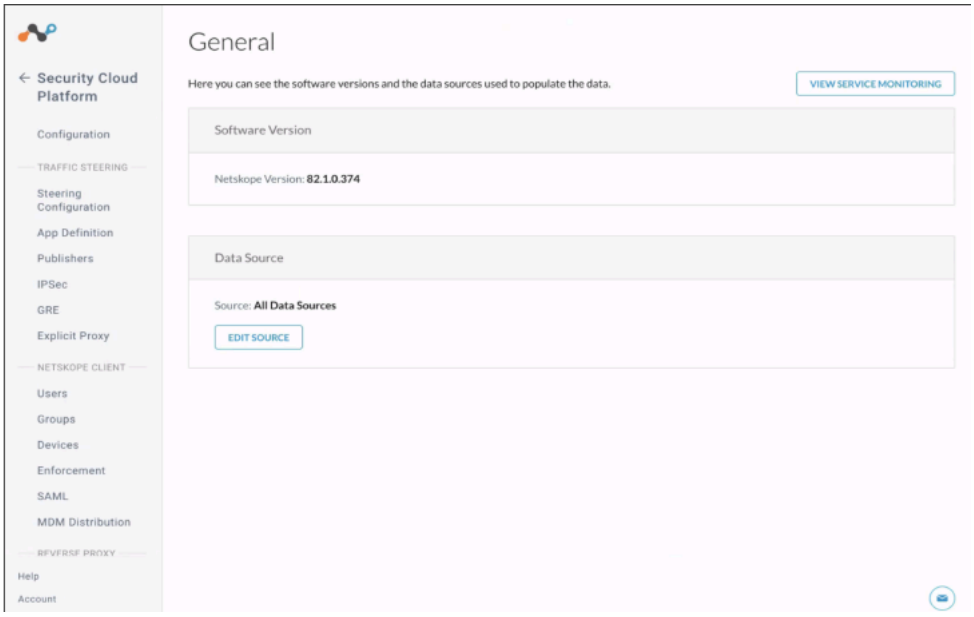
STEP 1 | Log in to **Netskope**.



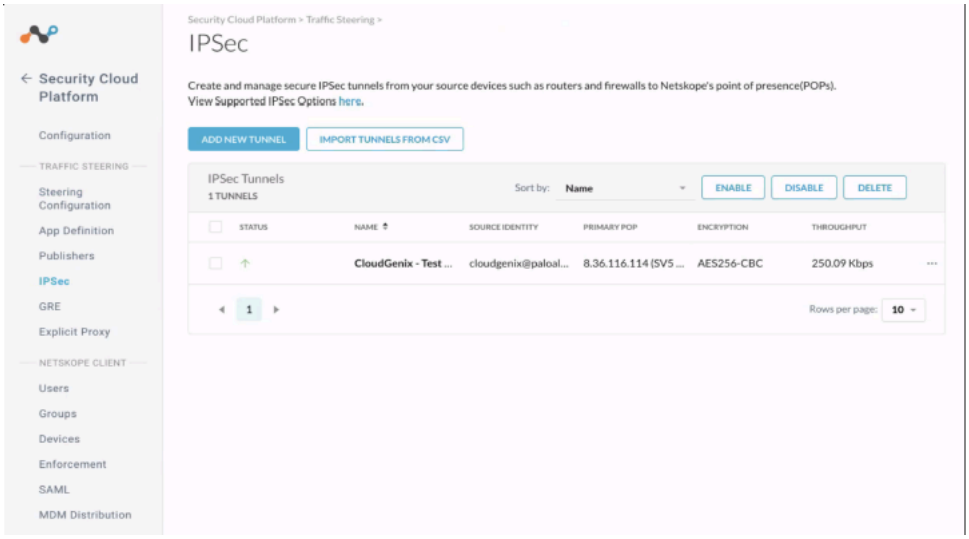
STEP 2 | Navigate to **Settings**.



STEP 3 | Select **Security Cloud Platform**.

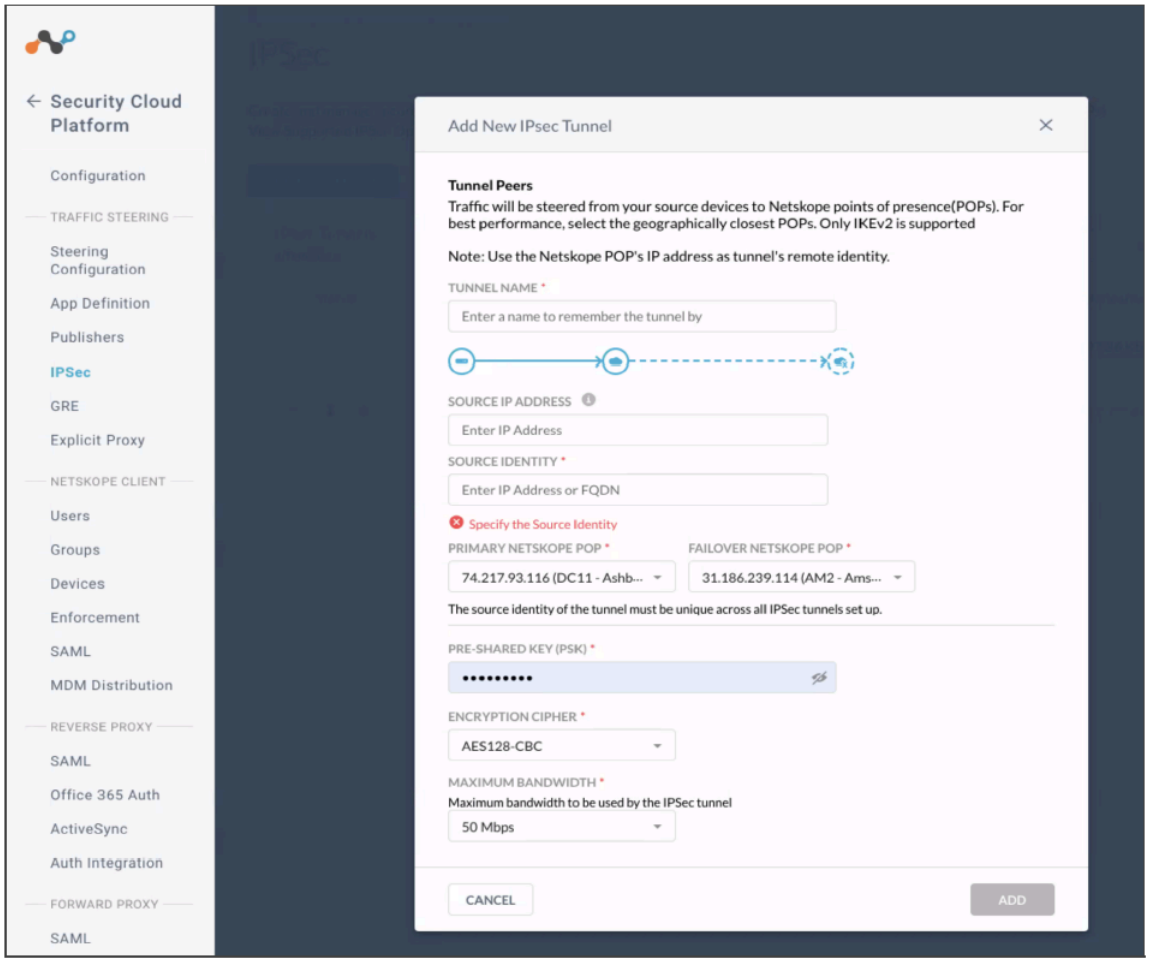


STEP 4 | Select **IPSec**.



STEP 5 | Add a new IPsec tunnel.

1. Click **Add New Tunnel**.

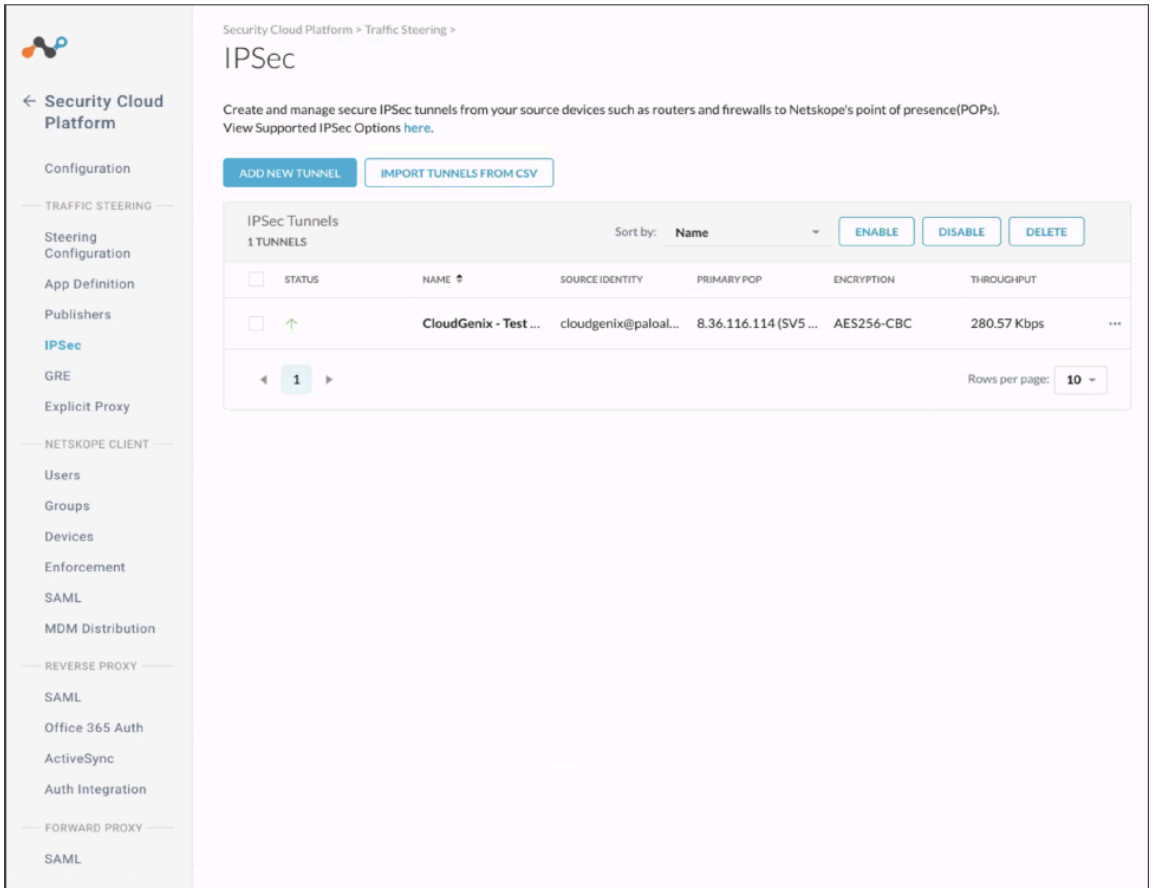


2. Enter a name for the tunnel.
3. Enter the IP address or the unique FQDN of the Prisma SD-WAN tunnel endpoint.
4. Choose the geographically closest Netskope POP as the Primary and choose a failover Netskope POP.
5. Enter a Pre-Shared key.
6. Configure an encryption cipher.
7. Configure the Maximum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

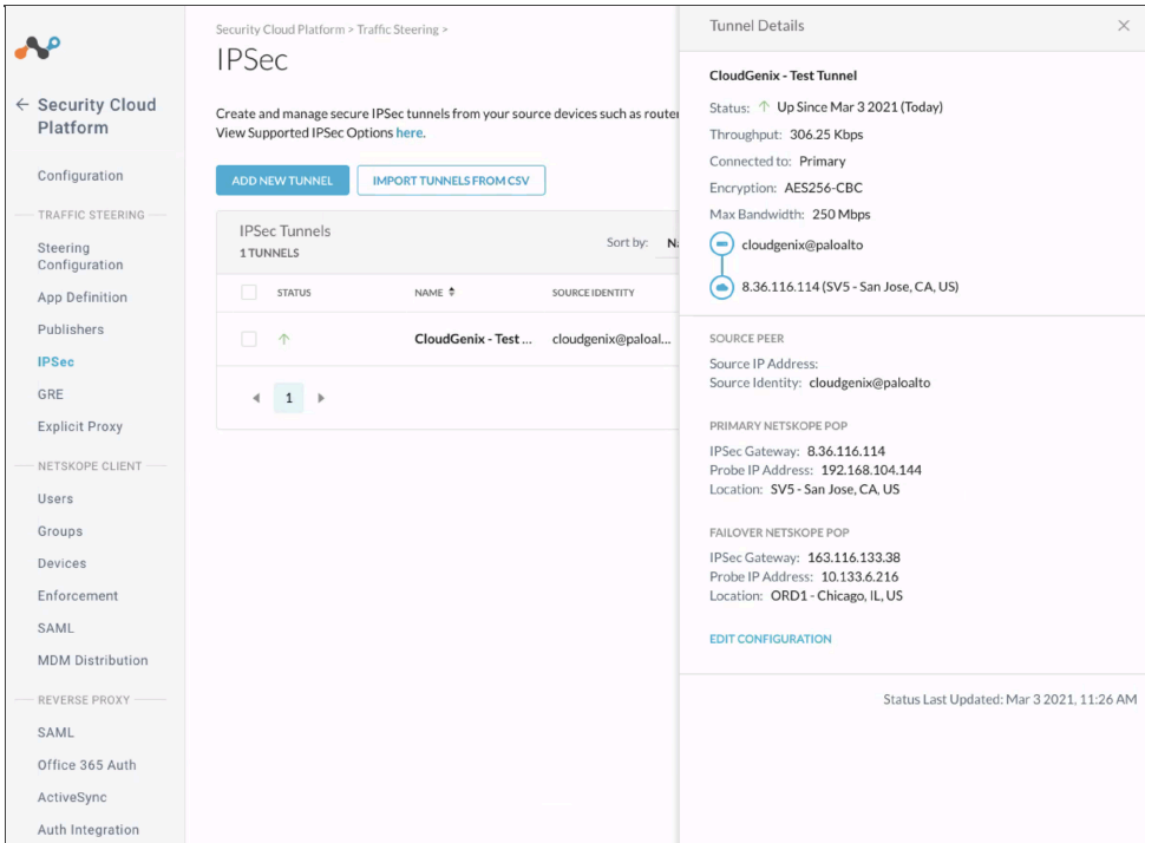
   No rate limiting happens based on the configured bandwidth.
8. Click **Add**.

   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**.



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



- 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.

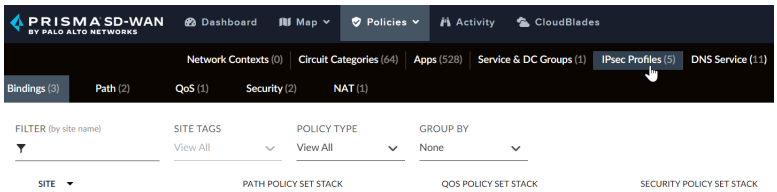
STEP 4 | Create a path policy.

STEP 5 | Verify the configuration.

Create an IPsec Profile

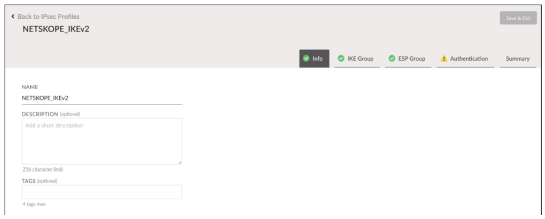
Create an IPsec profile on the Prisma SD-WAN web interface.

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

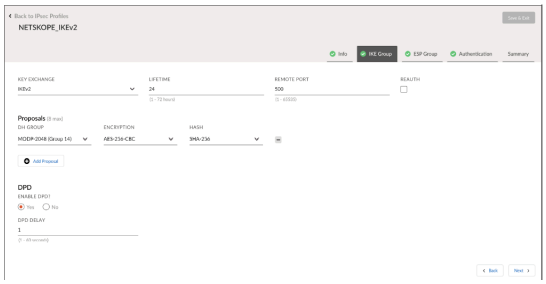


STEP 2 | Click **Add IPsec Profile**.

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



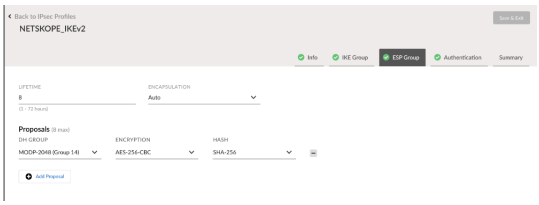
STEP 4 | Configure IKE settings.



- 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.



- 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.

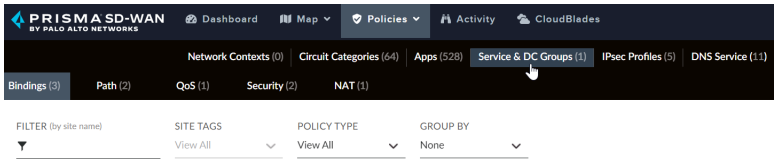
STEP 9 | Click **Next**, review the settings of the profile and then click **Save & Exit**.

Create a Service Group

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

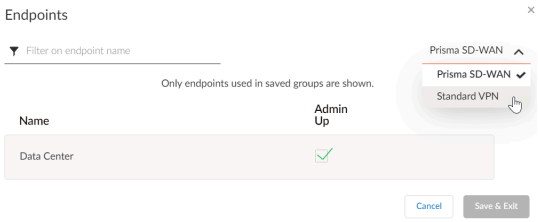
STEP 1 | Navigate to **Policies** > **Stacked Policies**.

STEP 2 | Select **Service & DC Groups**.

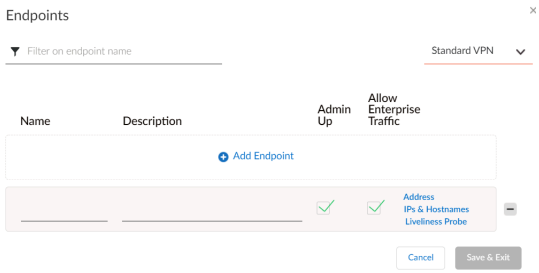


STEP 3 | Click **Endpoints**.

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



STEP 5 | Click **Add Endpoint**.

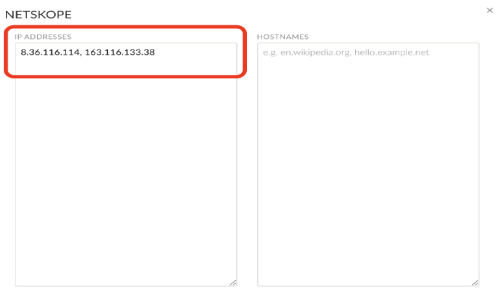


STEP 6 | Give the endpoint a name and check the **Admin UP** box.

STEP 7 | Click **IPs & Hostnames**.

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

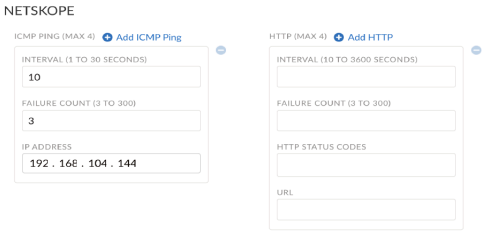
Prisma SD-WAN will check RTT for each of these IP addresses and will automatically choose the destination with the lowest latency as the IPsec tunnel endpoint.



STEP 9 | Click **Liveliness Probe**.

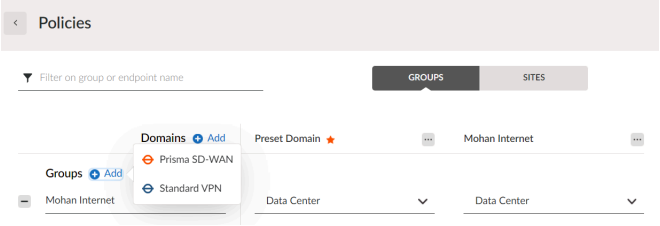
STEP 10 | Configure the Probe IP Address from Netskope Tunnel configuration along with ICMP ping interval and failure count and click **Done**.

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.



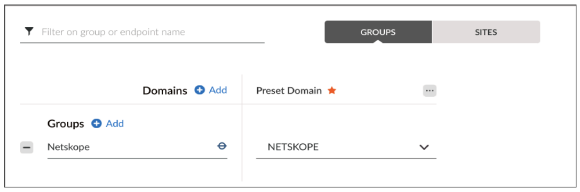
STEP 11 | Click **Save & Exit**.

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



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.



STEP 15 | Click **Save**.

Create an IPsec Tunnel

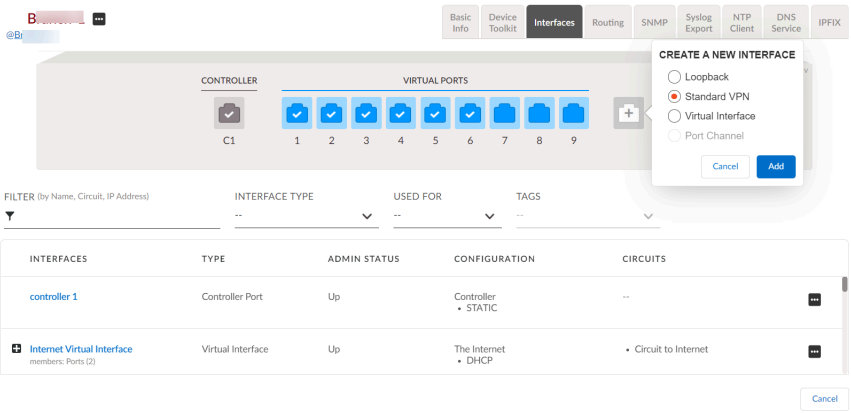
STEP 1 | Navigate to **Map** > **Claimed Devices**.

STEP 2 | Click the ellipsis menu for the device to be configured with the IPsec tunnel and select **Configure the device**.

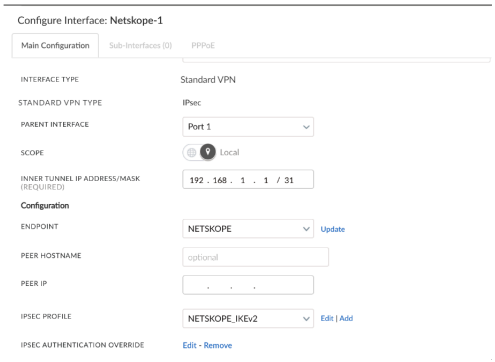
STEP 3 | Select **Interfaces**.

STEP 4 | Click the **+** sign on the Interface panel.

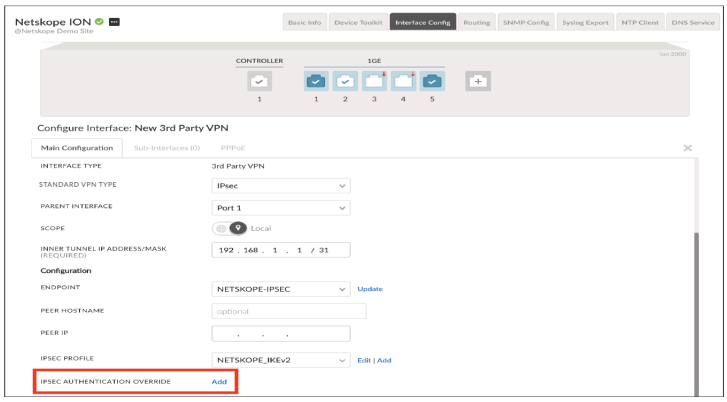
STEP 5 | Select **Standard VPN** and click **Add**.

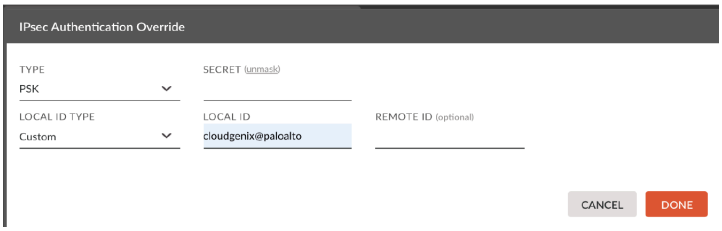


STEP 6 | On the tunnel configuration page, configure the following:



- 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.





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

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

STEP 7 | Click **Create Standard VPN**.

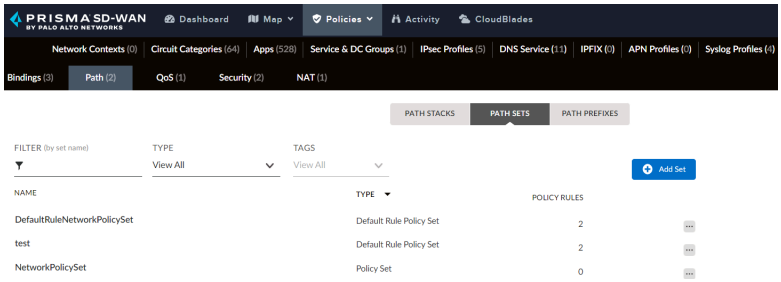
Create a Path Policy

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

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

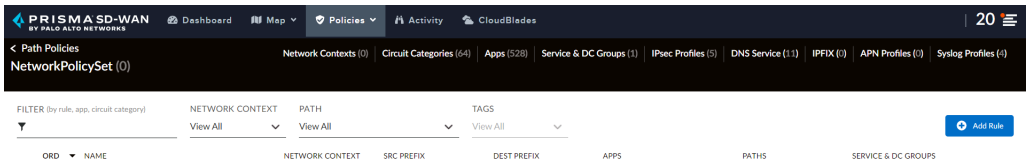
STEP 2 | Select **Path** and then **Path Sets**.

STEP 3 | Click **Add Set**.

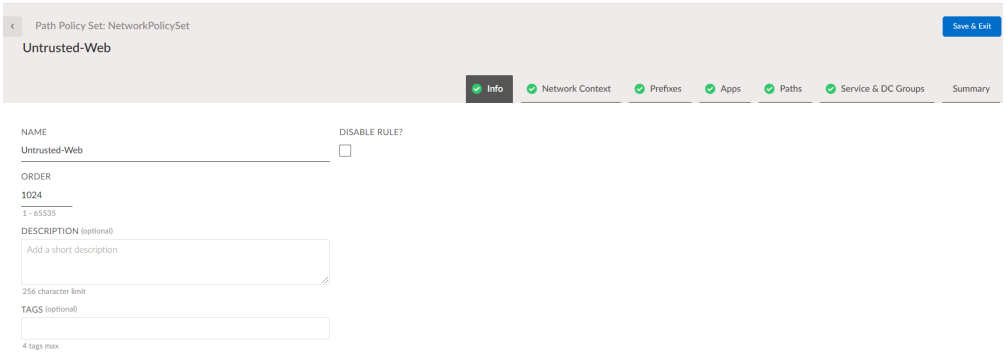


STEP 4 | Give the path policy set a name and click **Save**.

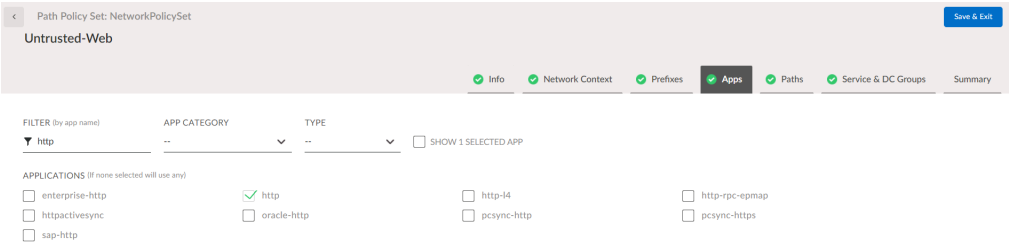
STEP 5 | Click the policy set and click **Add Rule**.



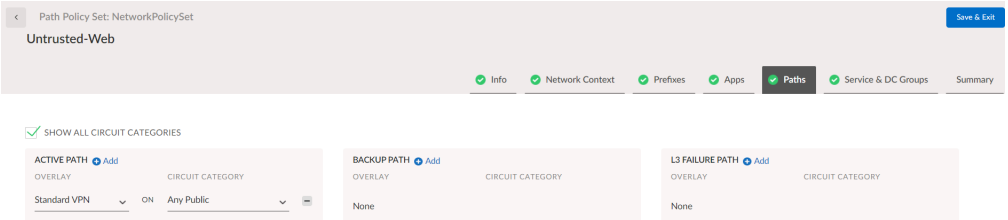
STEP 6 | Give the policy rule a name.



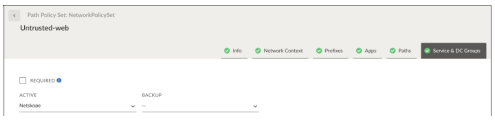
STEP 7 | Navigate to the **Apps** tab next and choose the applications that you want to forward to the Netskope Security Cloud over the Standard VPN.



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



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



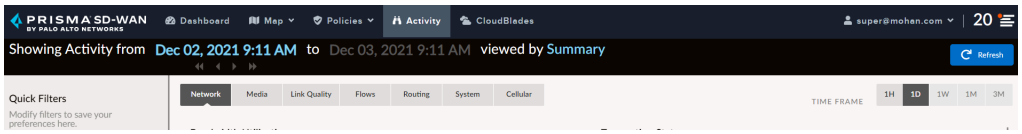
STEP 10 | Under **Active**, choose the Group configured in the previous steps from the drop-down list.

STEP 11 | Verify the configuration summary and click **Save & Exit**.

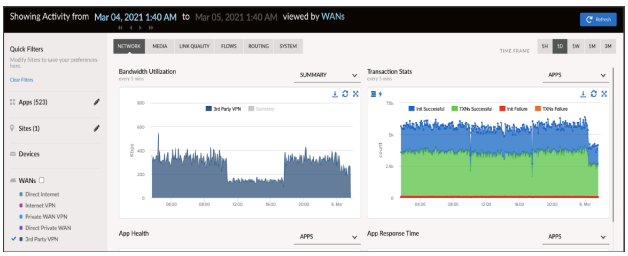
Verify the Configuration

STEP 1 | Send traffic from the LAN side of the Prisma SD-WAN ION device.

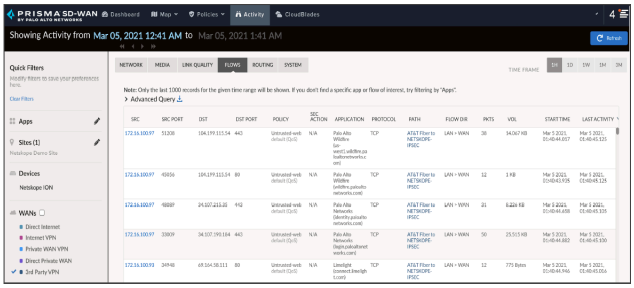
STEP 2 | On the Prisma SD-WAN web interface, navigate to the **Activity** tab.



STEP 3 | Verify analytics on the WAN path Standard VPN.



STEP 4 | Verify flows on the WAN path Standard VPN.



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/sha256DPD 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

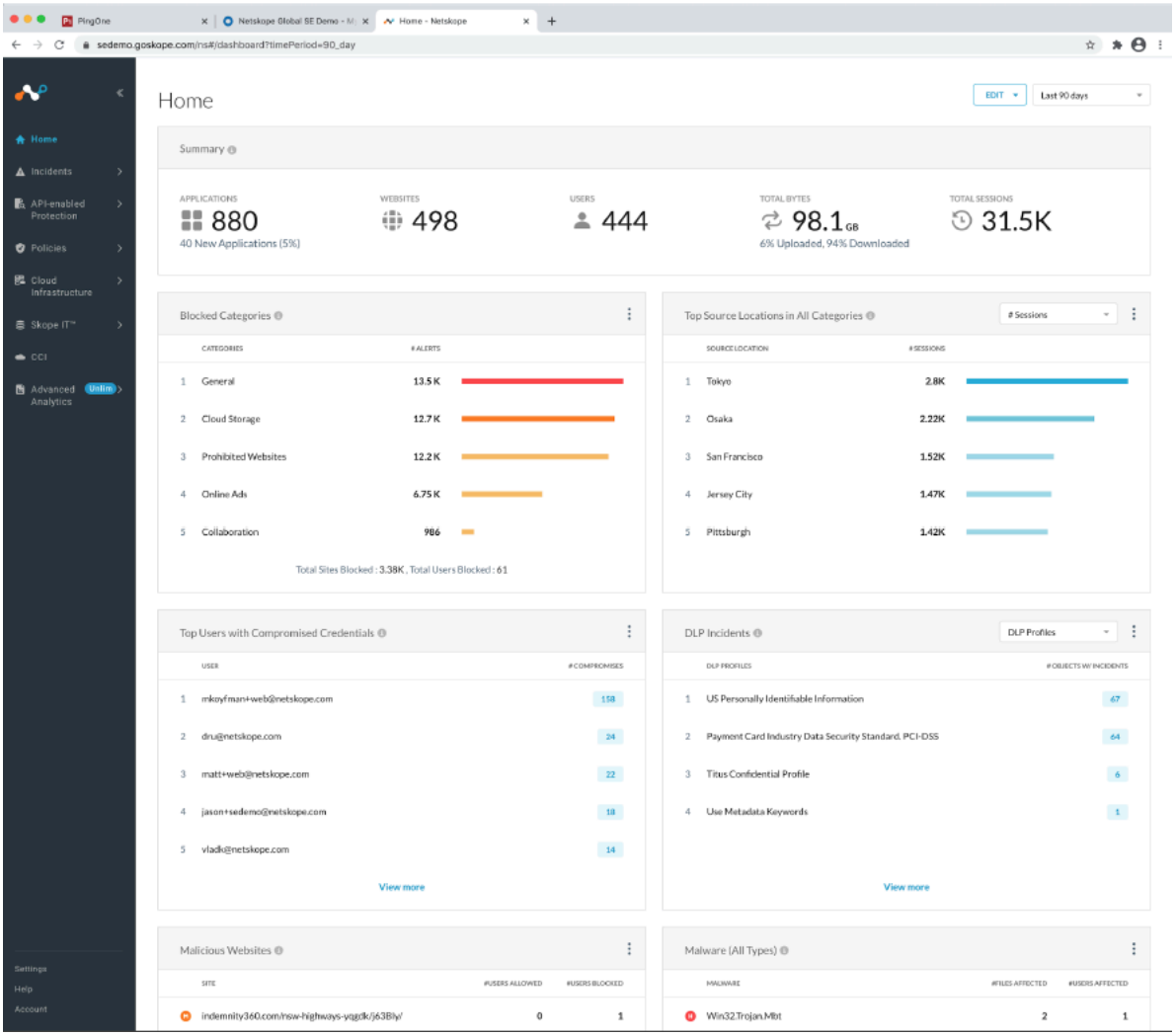
Extended State : tunnel_up

IPSec Algo : AES_CBC_256_HMAC_SHA2_256_128Ike Algo : AES_CBC_256HMAC_SHA2_256_128Remote IP : 8.36.116.114Local IP : 10.8.51.40IkeNextRekey : 2021-03-06 01:31:07.399431042 +0000 UTCIPsecLastRekeyed: 2021-03-05 09:01:02.793785216 +0000 UTCIPsecNextRekey : 2021-03-05 16:32:13.793786856 +0000 UTCPeer configured on service endpointService endpoint name: NETSKOPE-IPSECOrder of connection Try:----------
IP Address | Hostname | Reachable | Latency | Last LivelinessFailed | Hold Time |

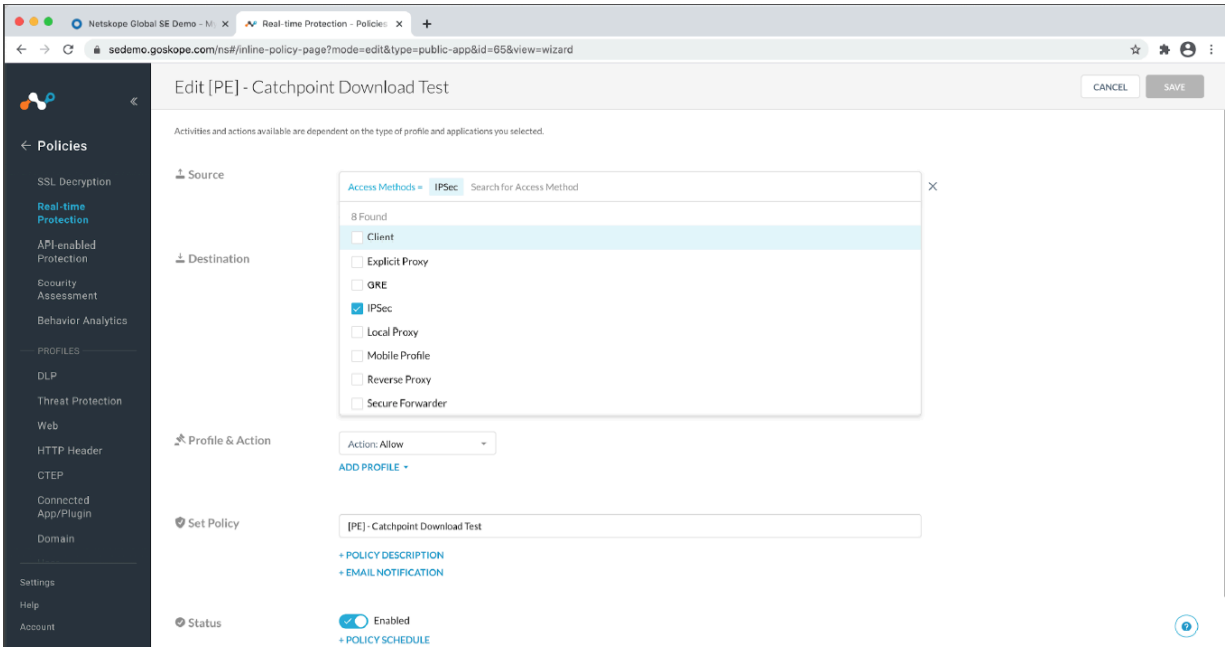
8.36.116.114 | | Yes | 5 | | || 163.116.133.38 | | Yes | 53
|----------
Liveliness probe status----------Type : icmpIpv4 : 192.168.104.144Status : trueLatency : 4Last updated : 2021-03-05T01:49:27

Monitor Cybersecurity Events on the Netskope Portal

STEP 1 | Login to the Security Admin portal.

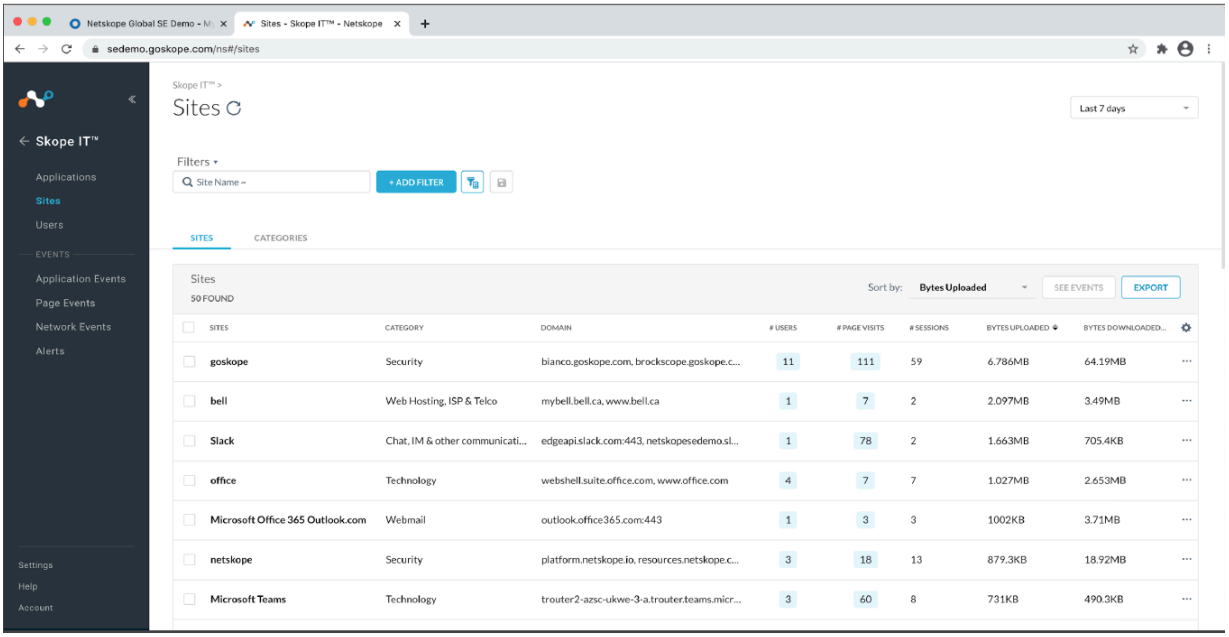


STEP 2 | Configure security policies on the **Policies** tab.

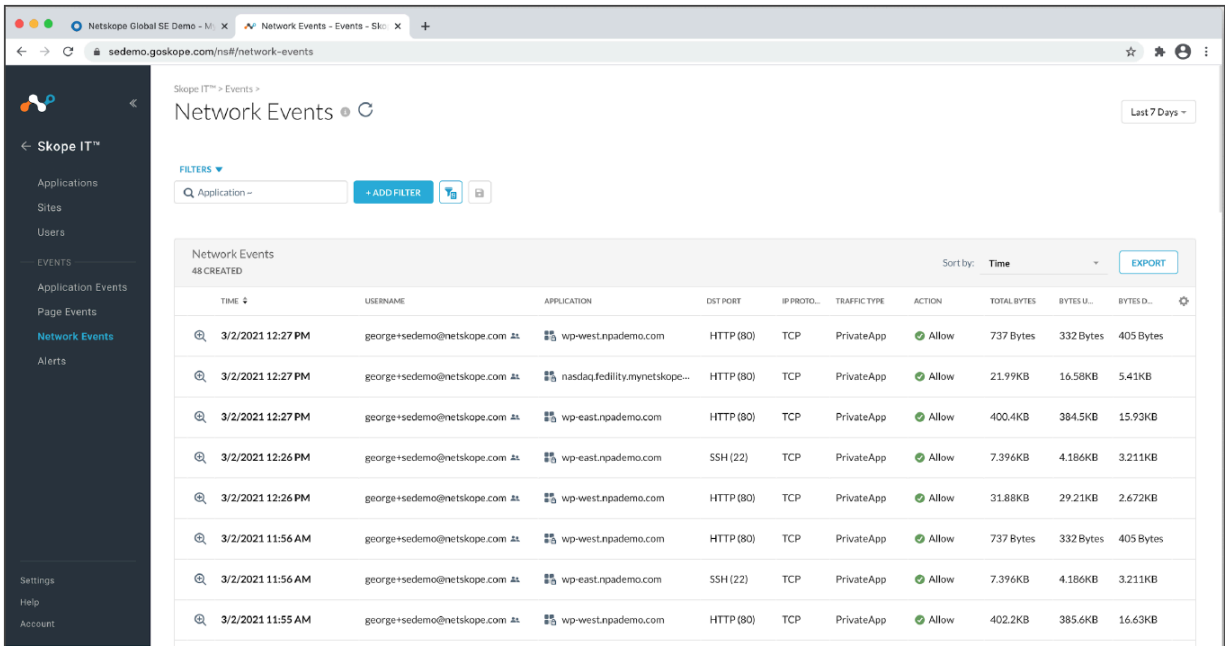


STEP 3 | Go to the main dashboard and select **Skope IT** for granular security data.

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.



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.