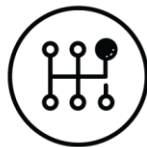


ULTIMATE TEST DRIVE

Secure Access Service Edge (SASE)

Workshop Guide



ULTIMATE
TEST DRIVE

Table of Contents

How to Use This Guide	4
Activity 0 – Initiate the UTD Workshop	5
Task 1 – Log In to Your Ultimate Test Drive Class Environment	5
Task 2 - Understand the UTD Environment Setup	6
Activity 1 – Configure Branch Office Network	8
Task 1 – Retrieve assigned Student-ID	8
Task 2 – Configure NGFW-Branch	9
Task 3 – Configure win-subnet1	14
Task 4 – Configure win-subnet2	17
Activity 2 – Secure Mobile Users with Prisma Access	20
Task 1 – Log in to GlobalProtect Application	21
Task 2 – Access Panorama for Prisma Access Management	24
Task 3 – Access Internet from win-mobile VM	27
Activity 3 – Next Generation Secure Remote Access	29
Task 1 – Control Access with User-ID	29
Activity 4 – Use Remote Networks to Secure Branches (1 WAN Link)	32
Task 1 – Review Prisma Access Remote Networks from Panorama	33
Task 2 – Configure IPSec Tunnel on NGFW	36
Task 3 – Verify Secured Remote Network	41
Activity 5 – Secure Branch Sites with 2 WAN Links (Active/Passive)	44
Task 1 – Review Remote Network Secondary WAN Configuration	45
Task 2 – Configure Secondary/Passive IPSec Tunnel on NGFW	46
Task 3 – Verify IPSec Tunnel Failover	50
Activity 6 – Secure Branch Sites with 2 WAN Links (Active/Active)	53
Task 1 – Review Prisma Access Remote Networks from Panorama	54
Task 2 – Configure Secondary/Active IPSec Tunnel on NGFW	55
Task 3 – Verify Two Active IPSec Tunnels	59
Activity 7 – Enterprise DLP with Prisma Access	61
Task 1 – Review Enterprise DLP on Panorama	61
Task 2 – Attempt Upload of Sensitive Content from Mobile User	64
Task 3 – Review Logs in Panorama	67
Task 4 – [Optional] Attempt Upload of Sensitive Content from Remote Network	68
Activity 8 – Prisma SD-WAN: Actionable Analytics - Identify & Measure	69
Task 1 – Log in to CloudGenix Portal	69
Task 2 – Network Analytics	71

Task 3 – Media Analytics	78
Task 4 – Link Quality	81
Task 5 – Flow Browser	83
Activity 9 – Prisma SD-WAN: Application Policy	87
Task 1 – Application Definitions	88
Task 2 – Path Policies	91
Task 3 – QoS Policies	94
Activity 10 – Prisma SD-WAN: Application Defined	98
Task 1 – Topology	98
Task 2 – Site Review	100
Task 3 – Physical Connectivity	101
Task 4 – Secure Fabric	103
Task 5 – Devices	105
Activity 11 - Feedback on Ultimate Test Drive	107
Task 1 – Take the online survey	107
Appendix-1: Network Diagram	108

How to Use This Guide

The activities outlined in this Ultimate Test Drive Workshop Guide are meant to contain all the information necessary to navigate the workshop interface, complete the workshop activities, and troubleshoot any potential issues with the UTD environment. This guide is meant to be used in conjunction with the information and guidance provided by your facilitator.

Notes:

This workshop covers only basic topics and is not a substitute for training classes conducted by Palo Alto Networks Authorized Training Centers. Please contact your partner or regional sales manager for more information on available training and how to register for one near you.

Unless specified, the Google® Chrome™ web browser will be used to perform any tasks outlined in the following activities (Chrome is pre-installed on the student desktop of the workshop PC).

Terminology:

Tab refers to the seven tabs along the top of each screen in the GUI.

Node refers to the options associated with each tab, found in the left-hand column of each screen.

Activity 0 – Initiate the UTD Workshop

In this activity, you will:

- Log in to the Ultimate Test Drive Workshop from your laptop.
- Learn the layout of the environment and its various components.

Task 1 – Log In to Your Ultimate Test Drive Class Environment

Step 1: Verify that your laptop is equipped with a modern browser that supports HTML 5.0. We recommend using the latest version of Firefox®, Chrome, or Internet Explorer®/Edge®.

Step 2: Open a browser window and navigate to the class URL. If you have an invitation email, you will find the class URL and passphrase there. Otherwise, your instructor will provide them.



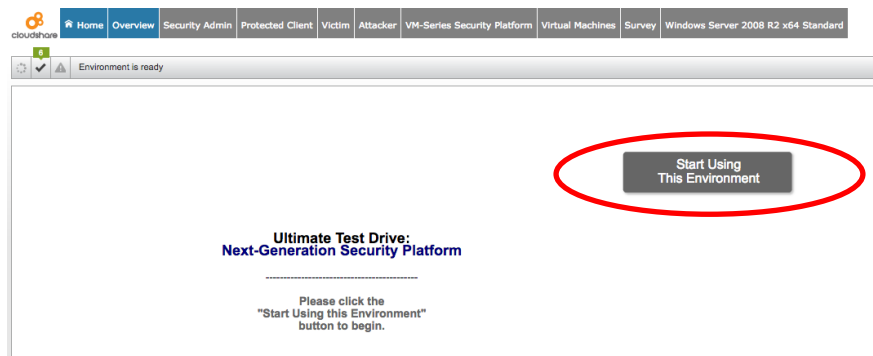
The screenshot shows the Palo Alto Networks login interface. At the top left is the Palo Alto Networks logo. Below it, the text reads: "Access your class environment. Enter the credentials supplied by your instructor to start working with your environment." There are two input fields: "Email: *" and "Class Passphrase: *". A "Login" button is located at the bottom right. A note "* Indicates required field" is positioned to the right of the input fields.

Enter your email address and the class passphrase.

Step 3: Complete the registration form and click **Login** at the bottom.

Step 4: Once you have logged in, the system will create a unique UTD environment for you. Please note that this process may take a while, as indicated by the green progress bar at the top of the screen.

Once the environment has been created, the system will display a welcome page. Click **Start Using This Environment** to begin.



This will display a list of all virtual systems that constitute the UTD environment.

Take note of the shortcut menu at the top of your browser window. You will use this menu throughout the workshop to switch between the available desktops.

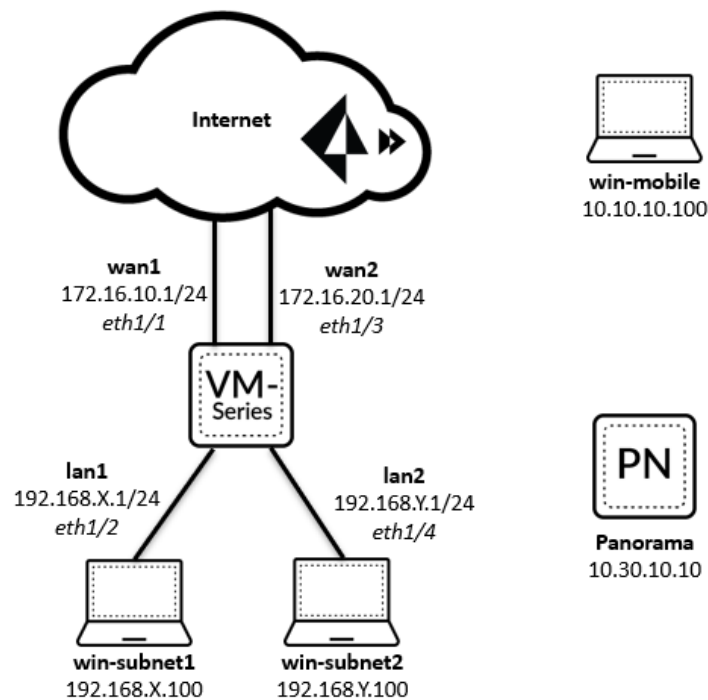
Task 2 - Understand the UTD Environment Setup

This UTD environment consists of the following components:

- A. **Panorama-UI:** Panorama is used for management of Prisma Access.
- B. **NGFW-Branch-UI:** Used to establish IPSec tunnel only. No security policy enforcement is done from this VM.
- C. **Win-subnet1:** Windows VM in subnet1. Each student will have their own unique subnet.
- D. **Win-subnet2:** Windows VM in subnet2. Each student will have their own unique subnet.
- E. **Win-mobile:** Windows VM running GlobalProtect agent for remote user. Each student will be logged in with their own unique login.

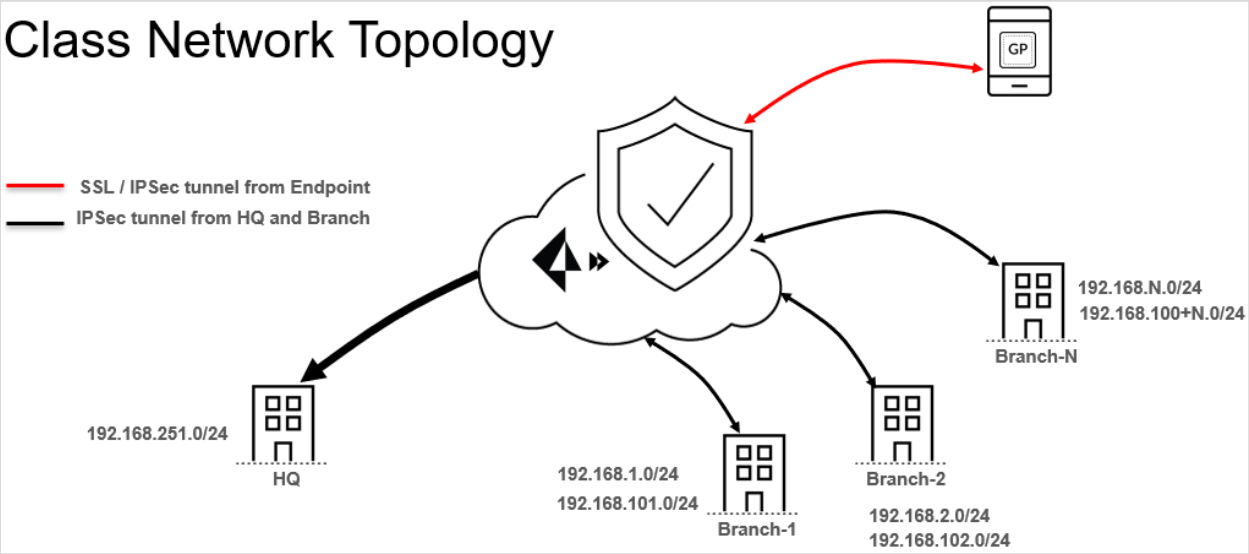
Review the diagram below to better understand the UTD environment setup.

Student Network Topology



Each student will be assigned a unique Student-ID which will be used for the configuration of your Branch Office.

Class Network Topology



Each student will represent one Branch Office. Each Branch Office will have two WAN links and two LAN links.

End of Activity 0

Activity 1 – Configure Branch Office Network

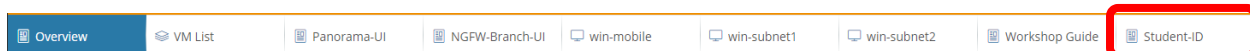
In this activity, you will:

- Retrieve your assigned Student-ID
- Access the NGFW-Branch, win-subnet1, and win-subnet2 VMs
- Configure your own environment to a unique IP subnet

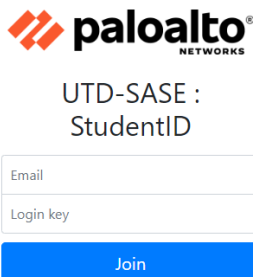
Task 1 – Retrieve assigned Student-ID

These are pre-requisite steps necessary to get your environment ready for the workshop. These are specific to your personal workshop environment and not related to Prisma Access.

Step 1: Click the **Student-ID** tab. Click the **Student-ID**  icon to launch the browser. The **UTD-SASE: Student-ID** page should load.

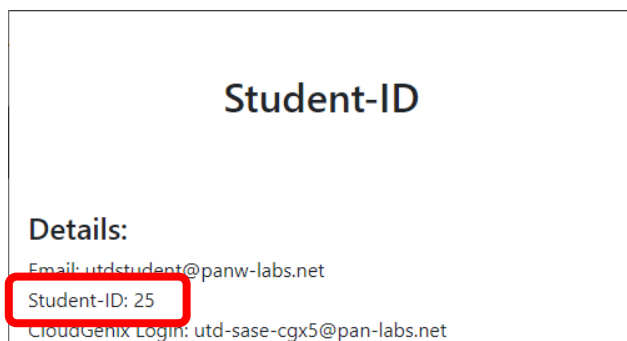


Step 2: Enter your **email** and for the **Login key:** use **utd1234**.

A screenshot of the Palo Alto Networks UTD-SASE Student ID login page. The page features the Palo Alto Networks logo at the top, followed by the text 'UTD-SASE : StudentID'. Below this is a form with two input fields: 'Email' and 'Login key'. A blue 'Join' button is positioned at the bottom of the form.

Click **Join**.

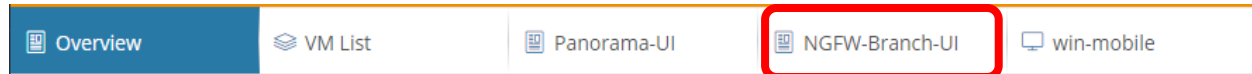
Step 3: Get **Student-ID**. Your **Student-ID** will be used throughout this workshop. It is important to use your assigned value as to not interfere with others who are doing this workshop.

A screenshot of the 'Student-ID' details page. The page has a large 'Student-ID' heading. Below it, under the heading 'Details:', there are three lines of text: 'Email: utdstudent@panw-labs.net', 'Student-ID: 25', and 'CloudGenix Login: utd-sase-cgx5@pan-labs.net'. The 'Student-ID: 25' line is highlighted with a red rectangular box.

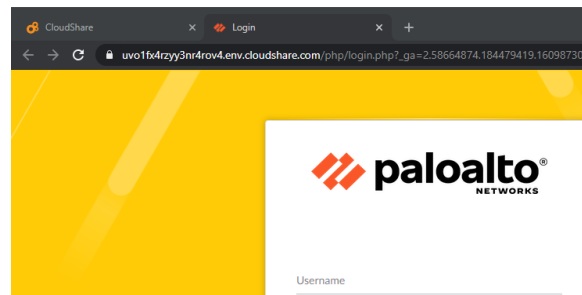
Task 2 – Configure NGFW-Branch

These are pre-requisite steps necessary to get your environment ready for the workshop. These are specific to your personal workshop environment and not related to Prisma Access.

Step 1: Click the **NGFW-Branch-UI** tab.



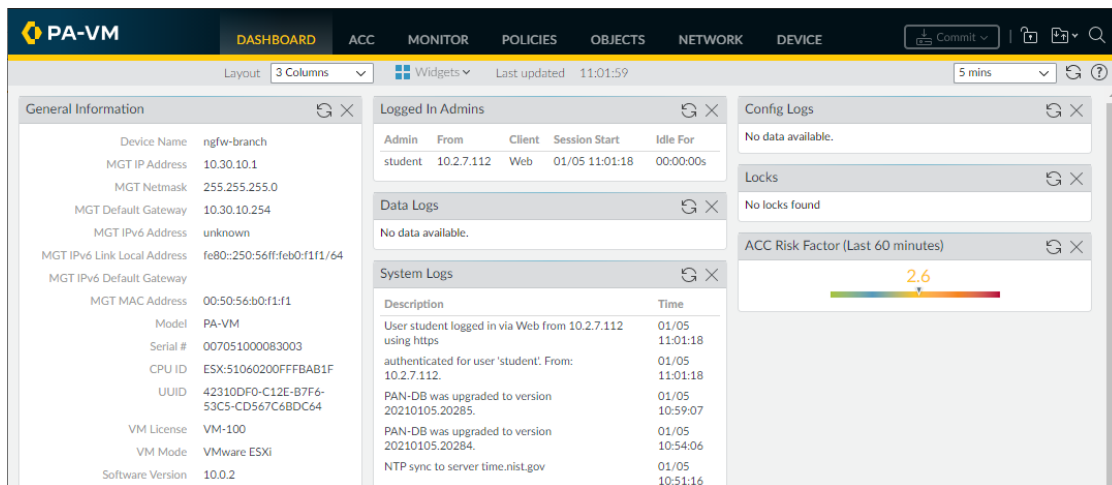
This will open a new tab in your browser with the login page for the **NGFW-Branch VM**.



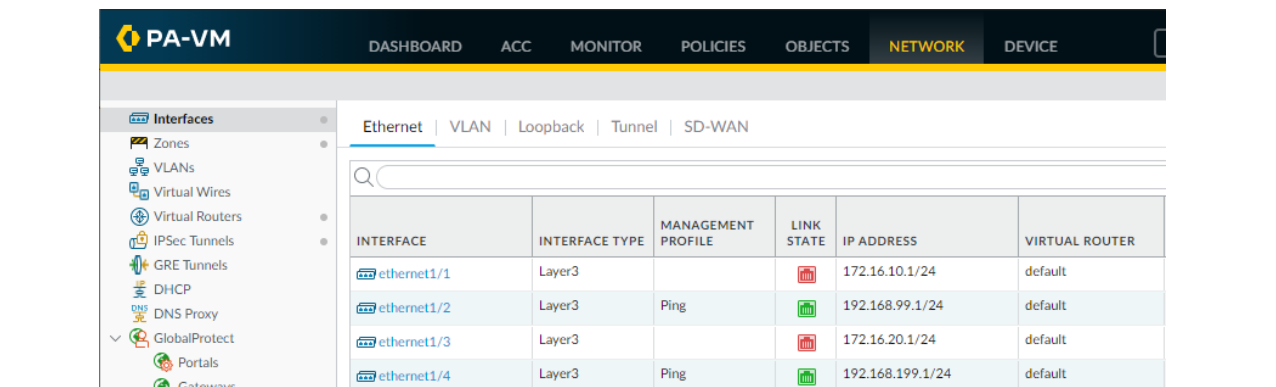
Step 2: Log in with the following credentials:

Name: *student*

Password: *utd1234*



Step 3: Go to **Network > Interfaces**.



Step 4: Click **ethernet1/2**. This brings up the **Ethernet Interface** window.

Ethernet Interface

Interface Name ethernet1/2

Comment

Interface Type Layer3

Netflow Profile None

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router default

Security Zone lan

OK Cancel

Step 5: Click the **IPv4** tab.

Config | IPv4 | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type Static PPPoE DHCP Client

<input type="checkbox"/>	IP
<input type="checkbox"/>	192.168.99.1/24

Click **192.168.99.1/24** and change the IP to **192.168.X.1/24**, where **X** is your assigned **Student-ID**.

If your **Student-ID** is **25**, this would be **192.168.25.1/24**. It is important to use your assigned value as to not conflict with other students.

Config | IPv4 | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type Static PPPoE DHCP Client

<input type="checkbox"/>	IP
<input checked="" type="checkbox"/>	192.168.25.1/24

Click **OK**.

Step 6: Click **ethernet1/4** to bring up the **Ethernet Interface** window for this interface.

Step 7: Click the **IPv4** tab.

Config | IPv4 | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type Static PPPoE DHCP Client

<input type="checkbox"/>	IP
<input type="checkbox"/>	192.168.199.1/24

Click **192.168.199.1/24** and change the IP to **192.168.Y.1/24**, where **Y** is your assigned **Student-ID+100**.

If your **Student-ID** is **25**, this would be **192.168.125.1/24**. It is important to use your assigned value as to

not conflict with other students.

Config | **IPv4** | IPv6 | SD-WAN | Advanced

Enable SD-WAN

Type Static PPPoE DHCP Client

IP
<input checked="" type="checkbox"/> 192.168.125.1/24

Click **OK**.

For **Student-ID 25**, the results will be:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
ethernet1/1	Layer3			172.16.10.1/24
ethernet1/2	Layer3	Ping		192.168.25.1/24
ethernet1/3	Layer3			172.16.20.1/24
ethernet1/4	Layer3	Ping		192.168.125.1/24

Step 8: Click **ethernet1/1** to bring up the **Ethernet Interface** window for this interface.

Step 9: Click the **Advanced** tab.

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

Link Settings

Link Speed: auto Link Duplex: auto Link State: down

Change the **Link State** from **down** to **up**.

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

Link Settings

Link Speed: auto Link Duplex: auto Link State: up

Click **OK**.

Step 10: Click **ethernet1/3** to bring up the **Ethernet Interface** window for this interface.

Step 11: Click the **Advanced** tab.

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

Link Settings

Link Speed: auto Link Duplex: auto Link State: down

Change the **Link State** from **down** to **up**.

Config | IPv4 | IPv6 | SD-WAN | **Advanced**

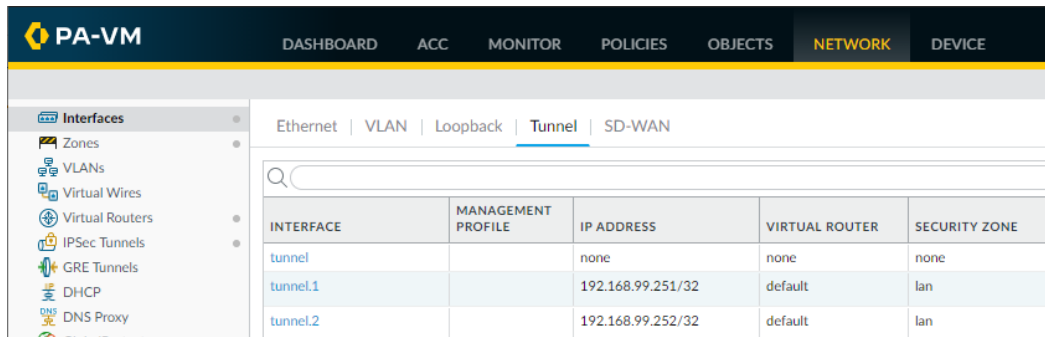
Link Settings

Link Speed: auto Link Duplex: auto Link State: up

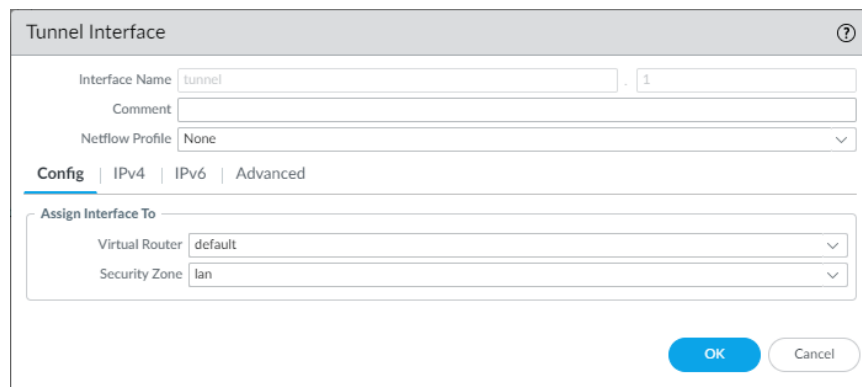
Click **OK**.

Note: The red **Link State** icons will not change at this point as you have not committed the configuration.

Step 12: From **Network > Interfaces**, select the **Tunnel** tab.



Step 13: Click **tunnel.1** to bring up the **Tunnel Interface** window.

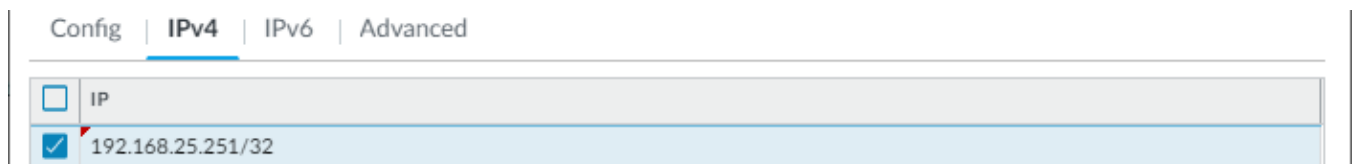


Step 14: Click the **IPv4** tab.



Click **192.168.99.251/32** and change the IP to **192.168.X.251/32**, where **X** is your assigned **Student-ID**.

If your **Student-ID** is **25**, this would be **192.168.25.251/32**. It is important to use your assigned value as to not conflict with other students.



Click **OK**.

Step 15: Click **tunnel.2** to bring up the **Tunnel Interface** window for that interface.

Step 16: Click the **IPv4** tab.

Click **192.168.99.252/32** and change the IP to **192.168.X.252/32**, where **X** is your assigned **Student-ID**.

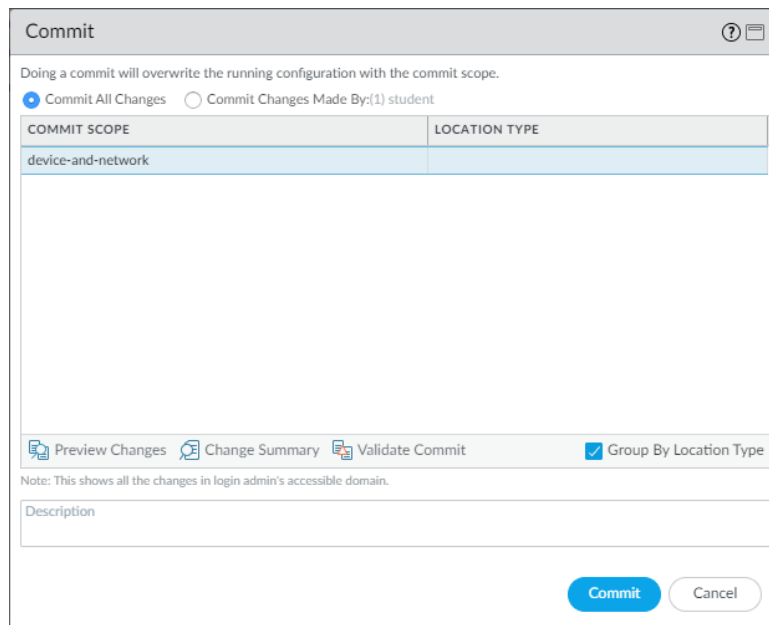
If your **Student-ID** is **25**, this would be **192.168.25.252/32**. It is important to use your assigned value as to not conflict with other students.

Click **OK**.

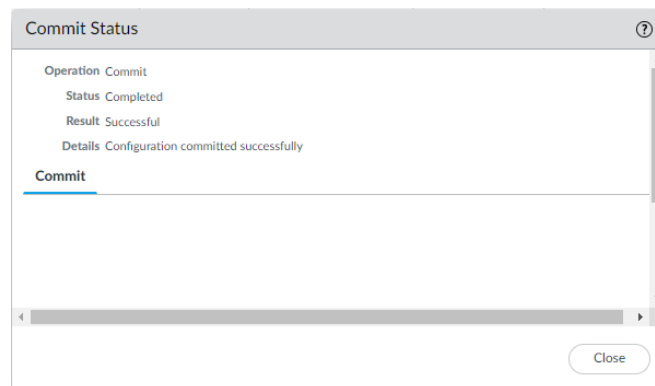
For **Student-ID 25**, the results will be:

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER
tunnel		none	none
tunnel.1		192.168.25.251/32	default
tunnel.2		192.168.25.252/32	default

Step 17: From the upper right-hand corner, click **Commit**. This brings up the **Commit** window.











Step 18: Click the **Commit** button.



Once the commit has completed, click **Close**.

Step 19: Navigate to **Network > Interfaces > Ethernet** and verify all interfaces are up.

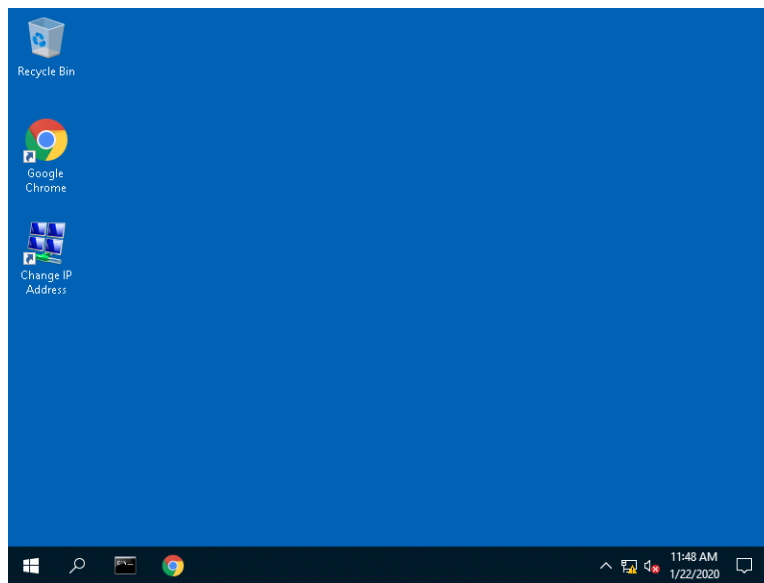
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS
 ethernet1/1	Layer3			172.16.10.1/24
 ethernet1/2	Layer3	Ping		192.168.25.1/24
 ethernet1/3	Layer3			172.16.20.1/24
 ethernet1/4	Layer3	Ping		192.168.125.1/24

Task 3 – Configure win-subnet1

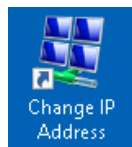
Step 1: Click the **win-subnet1** tab to access that desktop in your browser.



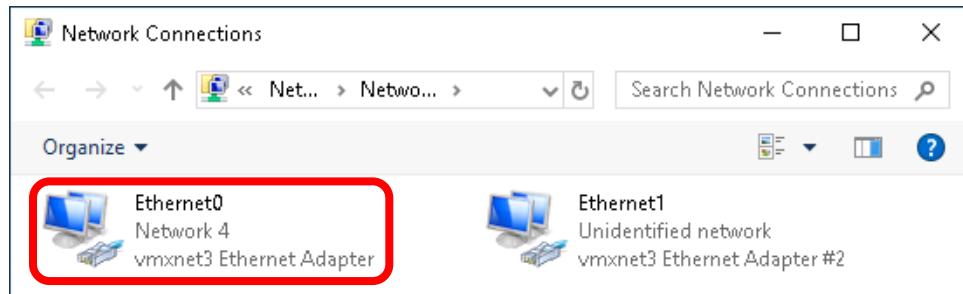
Step 2: You will be connected to the **win-subnet1** desktop through your browser.



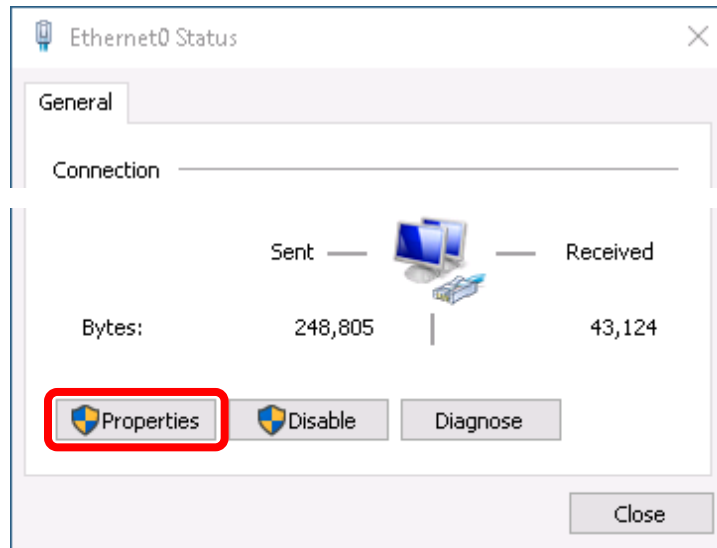
Step 3: Double-click the **Change IP Address** icon on the Desktop to bring up the **Network Connections** window.



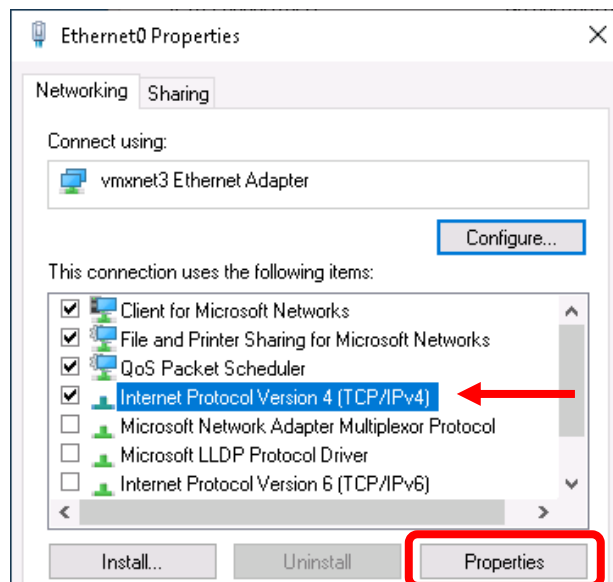
Step 4: Double-click on **Ethernet0**. **Note:** Do not change the IP address on **Ethernet1**).



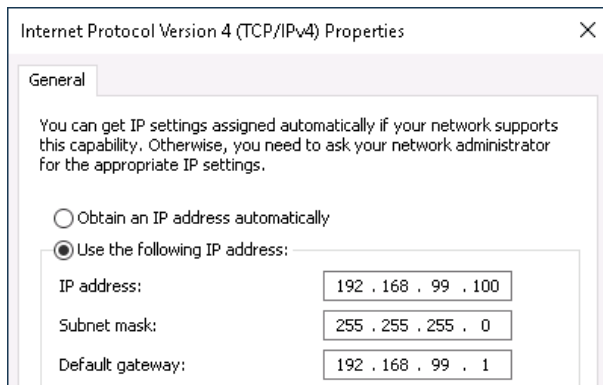
Step 5: From the **Ethernet0 Status** window, click **Properties**.



Step 6: From the **Ethernet0 Properties** window, click to select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



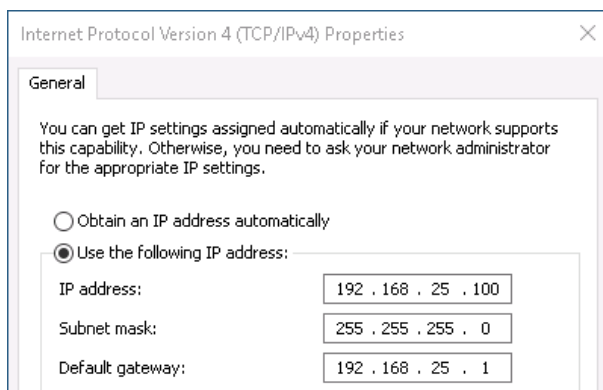
Step 7: On the **Internet Protocol Version 4 (TCP/IPv4) Properties** window,



Change **IP address**: **192.168.99.100** to **192.168.X.100**, where **X** is your assigned **Student-ID**.

Change **Default gateway**: **192.168.99.1** to **192.168.X.1**, where **X** is your assigned **Student-ID**.

If your **Student-ID** is **25**, this would be **192.168.25.100** and **192.168.25.1** respectively. It is important to use your assigned value to establish connectivity to the **NGFW-Branch VM**.



Click **OK**.

From the **Ethernet0 Properties** window, click **Close**.

From the **Ethernet0 Status** window, click **Close**. If prompted from a **Networks** window, click **No**.

On the **Network Connections** window, click the **X** to close the window.

Step 8: From the Windows taskbar, click the **Command Prompt**  icon to launch the **Command Prompt**.

Type **ping 192.168.X.1**, where **X** is your assigned **Student-ID**.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\root>ping 192.168.25.1

Pinging 192.168.25.1 with 32 bytes of data:
Reply from 192.168.25.1: bytes=32 time=16ms TTL=64
Reply from 192.168.25.1: bytes=32 time=20ms TTL=64
Reply from 192.168.25.1: bytes=32 time=14ms TTL=64
Reply from 192.168.25.1: bytes=32 time=8ms TTL=64

Ping statistics for 192.168.25.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 20ms, Average = 14ms

C:\Users\root>
```

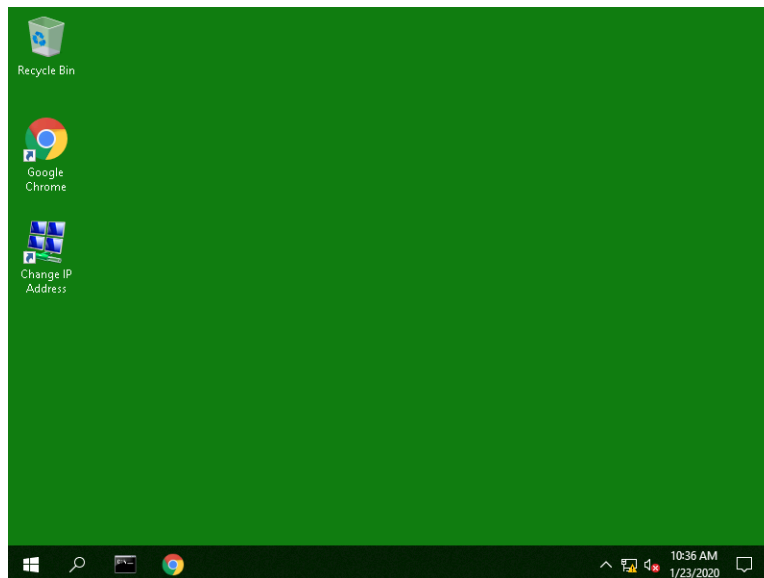
Close the **Command Prompt** window.

Task 4 – Configure win-subnet2

Step 1: Click the **win-subnet2** tab to access that desktop in your browser.



Step 2: You will be connected to the **win-subnet2** desktop through your browser.



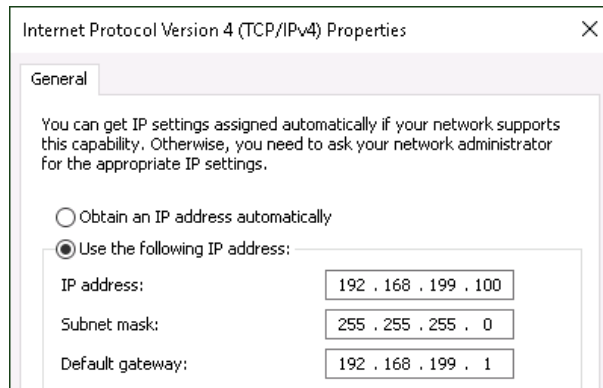
Step 3: Double-click the **Change IP Address** icon on the Desktop to bring up the **Network Connections** window.

Step 4: Double-click on **Ethernet0**. **Note:** Do not change the IP address on **Ethernet1**).

Step 5: From the **Ethernet0 Status** window, click **Properties**.

Step 6: From the **Ethernet0 Properties** window, click to select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

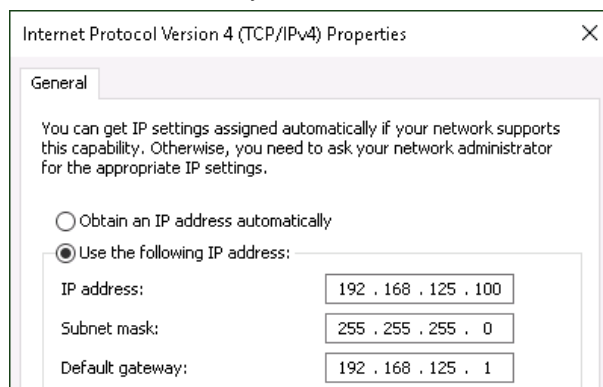
Step 7: On the **Internet Protocol Version 4 (TCP/IPv4) Properties** window,



Change **IP address:** **192.168.199.100** to **192.168.Y.100**, where **Y** is your assigned **Student-ID+100**.

Change **Default gateway:** **192.168.199.1** to **192.168.Y.1**, where **Y** is your assigned **Student-ID+100**.

If your **Student-ID** is **25**, this would be **192.168.125.100** and **192.168.125.1** respectively. It is important to use your assigned value to establish connectivity to the **NGFW-Branch VM**.



Click **OK**.

From the **Ethernet0 Properties** window, click **Close**.

From the **Ethernet0 Status** window, click **Close**. If prompted from a **Networks** window, click **No**.

On the **Network Connections** window, click the **X** to close the window.

Step 8: From the Windows taskbar, click the **Command Prompt**  icon to launch the **Command Prompt**.

Type **ping 192.168.Y.1**, where **Y** is your assigned **Student-ID+100**.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\root>ping 192.168.125.1

Pinging 192.168.125.1 with 32 bytes of data:
Reply from 192.168.125.1: bytes=32 time=26ms TTL=64
Reply from 192.168.125.1: bytes=32 time=2ms TTL=64
Reply from 192.168.125.1: bytes=32 time=6ms TTL=64
Reply from 192.168.125.1: bytes=32 time=20ms TTL=64

Ping statistics for 192.168.125.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 26ms, Average = 13ms

C:\Users\root>
```

Close the **Command Prompt** window.

End of Activity 1

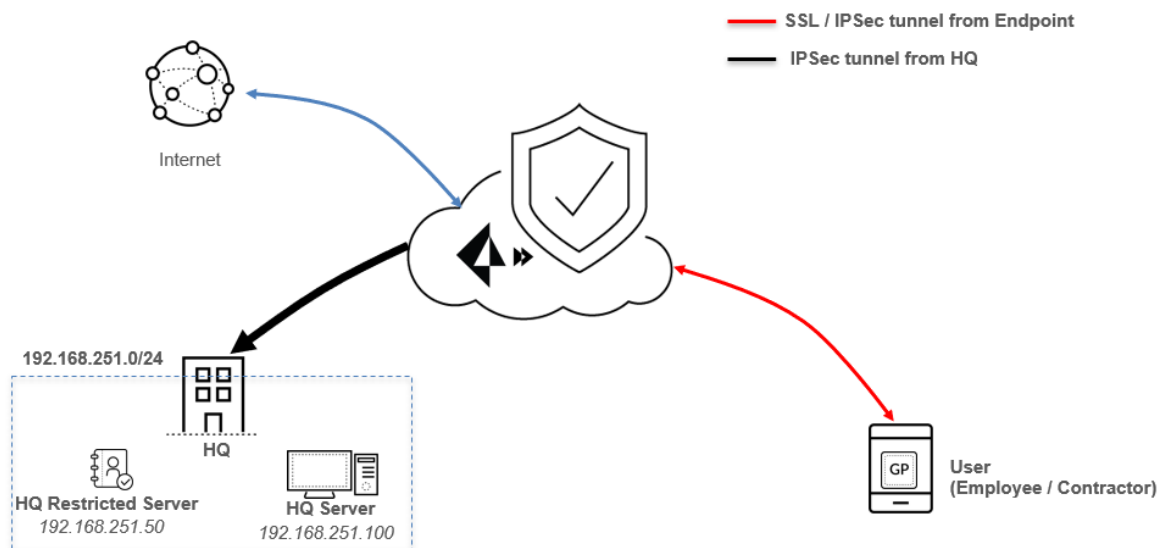
Activity 2 – Secure Mobile Users with Prisma Access

In this activity, you will:

- Access win-mobile VM
- Access Panorama and review Prisma Access configuration for Mobile Users
- Demonstrate how mobile user traffic is secured

Prisma Access is a Secure Access Service Edge delivered from multiple regions in the cloud. The GlobalProtect agent on user endpoints automatically determines the best Gateway for the user and tunnels traffic to this location. This allows for consistent security and access to the internet, cloud applications and private data center apps with better user experience. The 100+ points of presence allows security inspection closer to the user with better localization, instead of back-hauling all traffic to the Data Center.

Secure Mobile Users

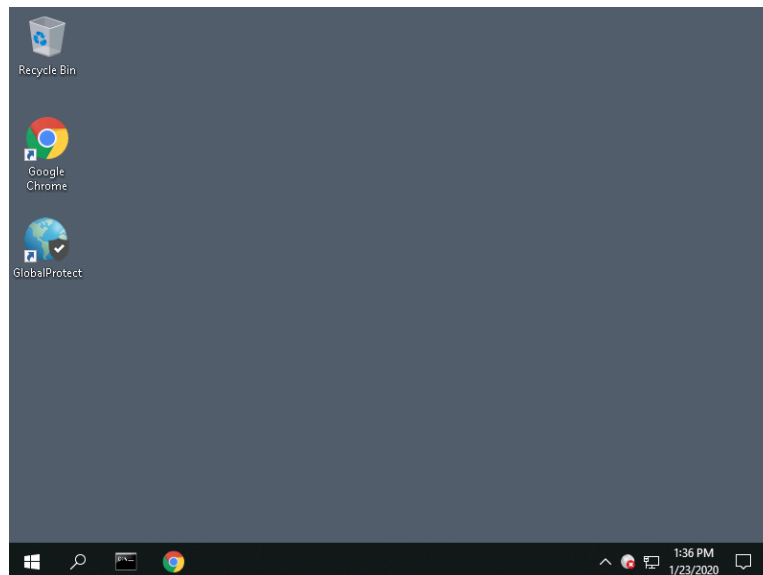



Task 1 – Log in to GlobalProtect Application

Step 1: Click the **win-mobile** tab to access that desktop in your browser.

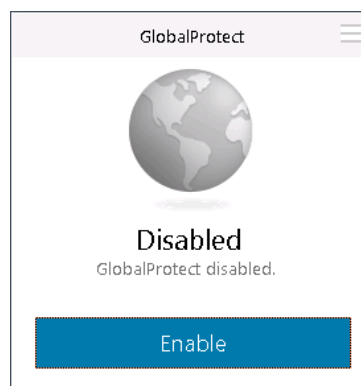


Step 2: You will be connected to the **win-mobile** desktop.



Step 3: From the system tray, click the **GlobalProtect**  icon.

Step 4: Click the **Enable** button.



Step 5: Sign in to the **GlobalProtect** application with the following credentials:

Username: *contractor[X]* where *[X]* is your **Student-ID** (e.g. contractor25)

Password: *utd1234*

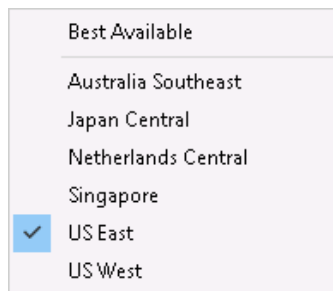
Click **Sign In**.

This will establish a secure tunnel from the **win-mobile** VM to nearest available **Prisma Access** gateway.



Depending on which CloudShare regional data center your workshop is originating from, you are likely to see the **Gateway** as **US-East**, **Netherlands Central**, or **Singapore**.

Step 6: Click the **Gateway** drop-down to see the available gateways that are user selectable for this Prisma Access tenant.

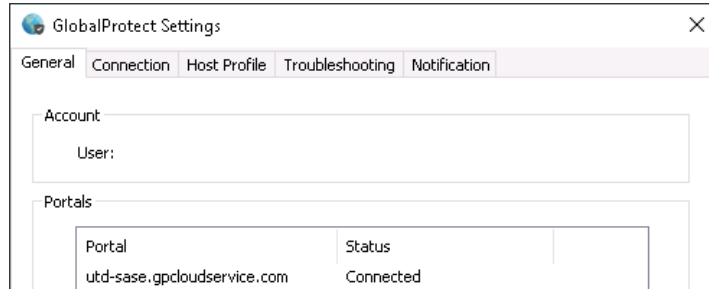


Click into the **GlobalProtect** window to dismiss the drop-down list.

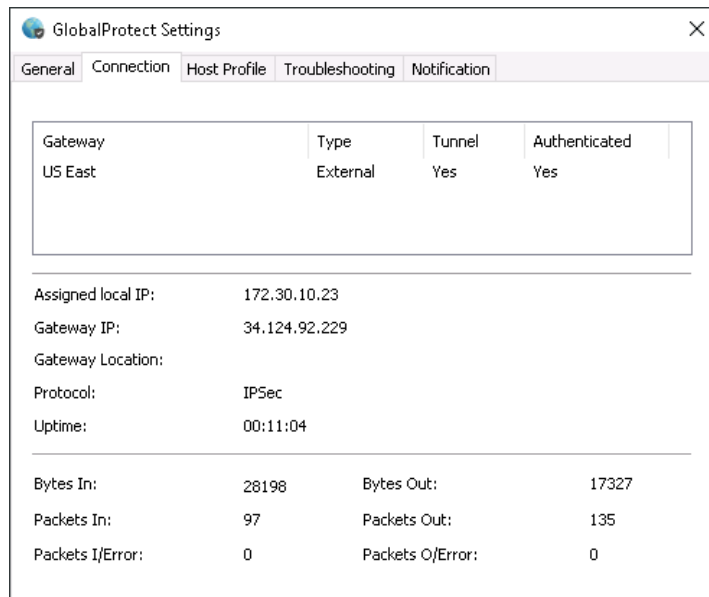
Note: This list is a small subset of the locations available. See <https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/list-of-prisma-access-locations.html> for the current list. In addition, the selectable list, as seen in this Prisma Access tenant, is also configurable as a subset off all your available gateway locations.

Note: You may get a notification regarding a new version of the GlobalProtect agent being available. You may choose to update or not, it should not affect your lab.

Step 7: Click the hamburger  icon then select **Settings** to bring up the **GlobalProtect Settings** window.

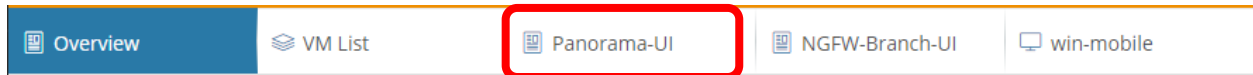


Step 8: Click the **Connection** tab to see the details on this connection to the Prisma Access gateway.

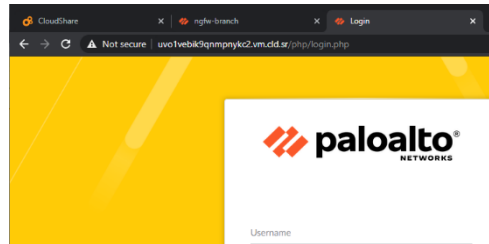


Task 2 – Access Panorama for Prisma Access Management

Step 1: Click the **Panorama-UI** tab.



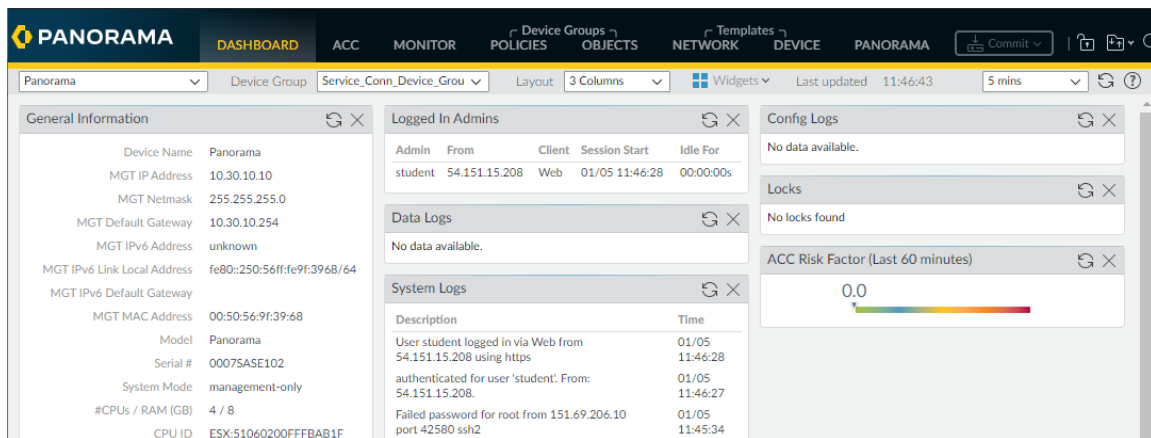
This will open a new tab in your browser with the login page for the **Panorama VM**.



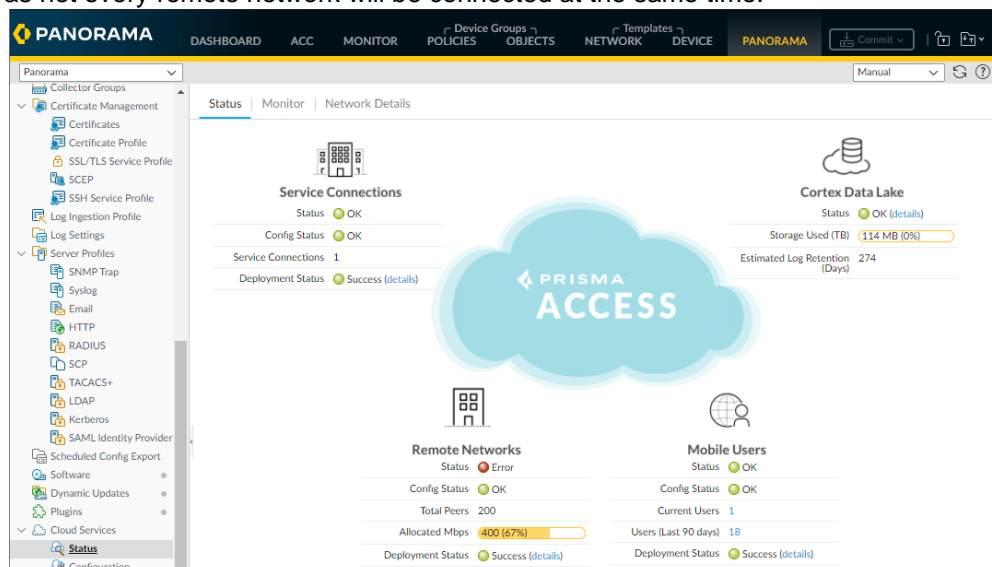
Step 2: Log in with the following credentials:

Name: *student*

Password: *utd1234*

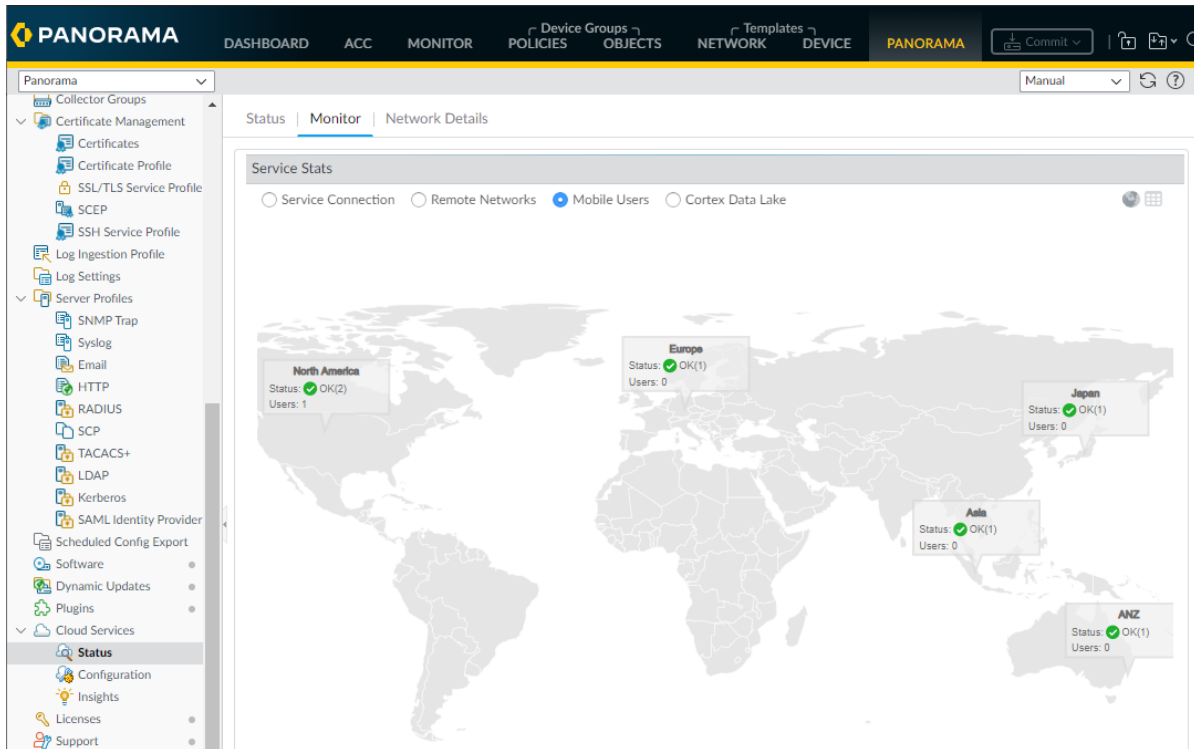


Step 3: Navigate to **Panorama > Cloud Services > Status > Status**. This will show the overall status of the Prisma Access tenant. **Note:** The **Remote Networks** status will be in **Error**. This is expected in this workshop as not every remote network will be connected at the same time.

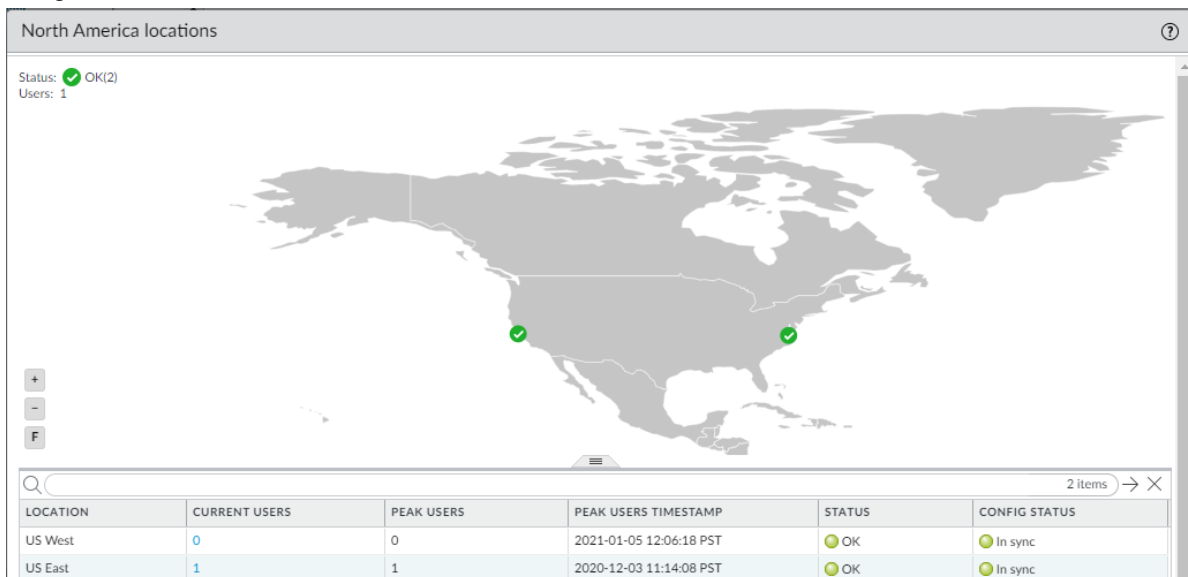


Step 4: Navigate to **Panorama > Cloud Services > Status > Monitor > Mobile Users.**

This will show a summary of each region indicating status, number of gateways and how many mobile users are currently connected. As you can see here, this Prisma Access tenant has two gateways enabled in **North America**, and one each in **Europe, Asia, Japan, and ANZ**. This is a small subset of what is available. See the URL in the previous activity for the entire list.

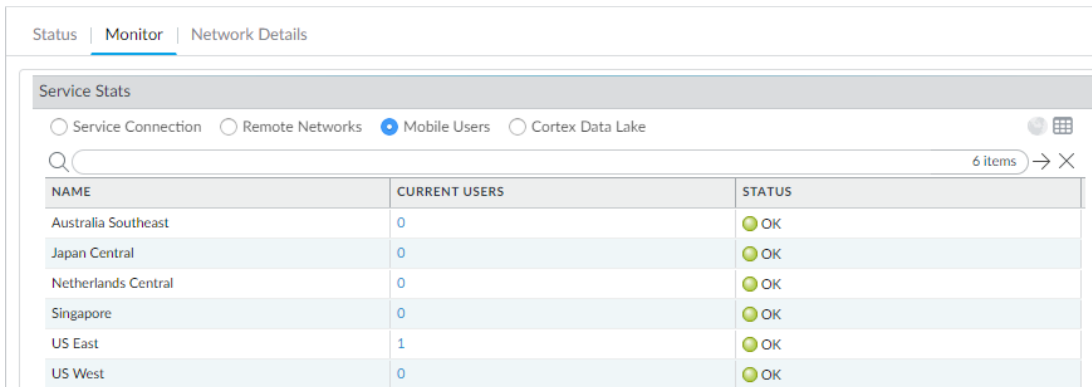


Step 5: Click on the **North America** status to bring up the **North America locations** window. This will show the gateway locations for that region as well as how many users are connected to each gateway in that region.



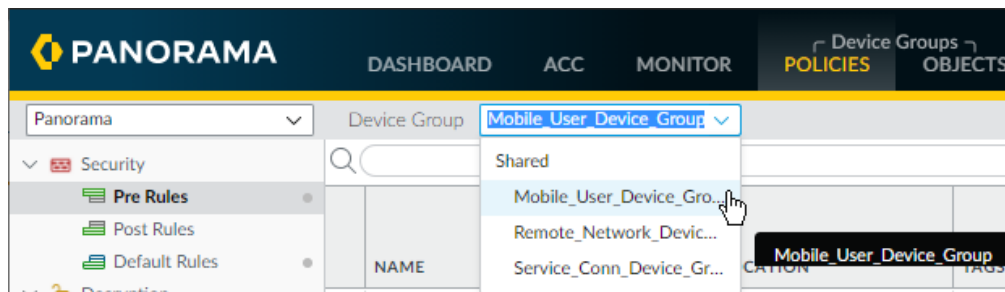
Click **Close**.

Step 6: In the upper right-hand corner, click the table  icon to see a different view.



NAME	CURRENT USERS	STATUS
Australia Southeast	0	OK
Japan Central	0	OK
Netherlands Central	0	OK
Singapore	0	OK
US East	1	OK
US West	0	OK

Step 7: Navigate to **Policies > Security > Pre Rules**. Make sure the **Device Group** is set to **Mobile_User_Device_Group**.



Step 8: Review the **Security Policies**.

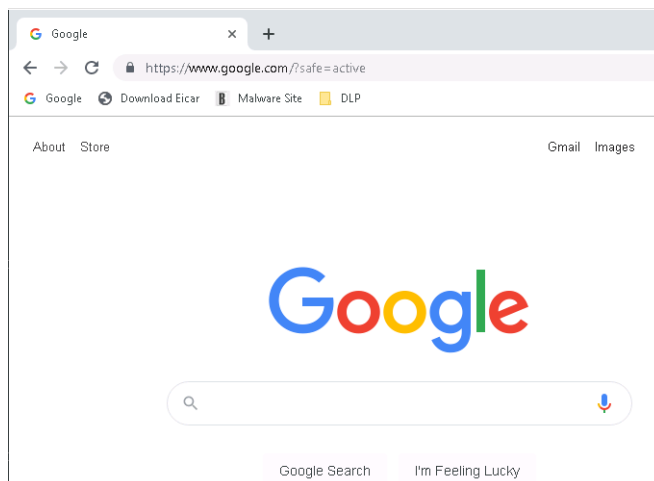
What access does the user (employee/contractor) have to HQ servers?

What security features are enabled in the **Secure-Internet-Traffic** policy?

NAME	LOCATION	TAGS	TYPE	Source				Destination	
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1 Deny QUIC	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any	any	Internet	any
2 Deny QUIC-UDP	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any	any	Internet	any
3 Secure-Internet-Traffic	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any	any	Internet	any
4 Secure-Access-to-HQ-Restricted-Server	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	employee	any	HQ	Restricted-Server
5 Deny-Access-to-HQ-Restricted-Server	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	contractor	any	HQ	Restricted-Server
6 Secure-Access-to-HQ-and-Branch-Office	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	contractor employee	any	Branch-Office HQ	any

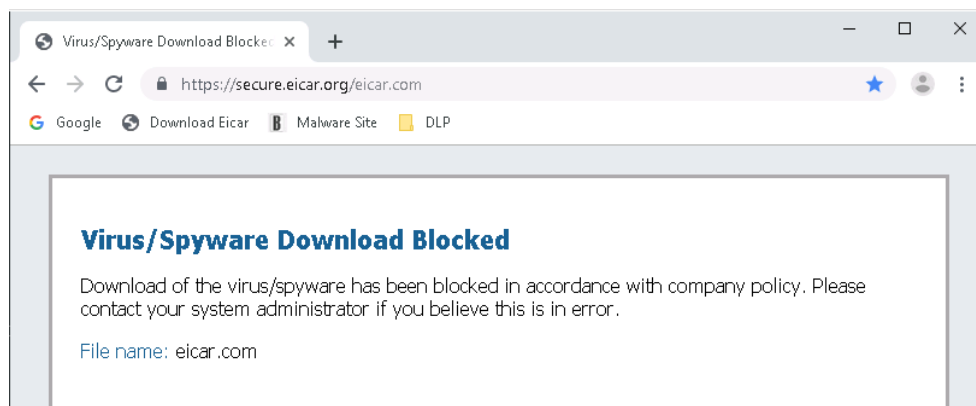
Task 3 – Access Internet from win-mobile VM

Step 1: From the **win-mobile** VM, launch the **Chrome** browser. Use the **Google** bookmark to browse to **https://www.google.com**. This should be successful.

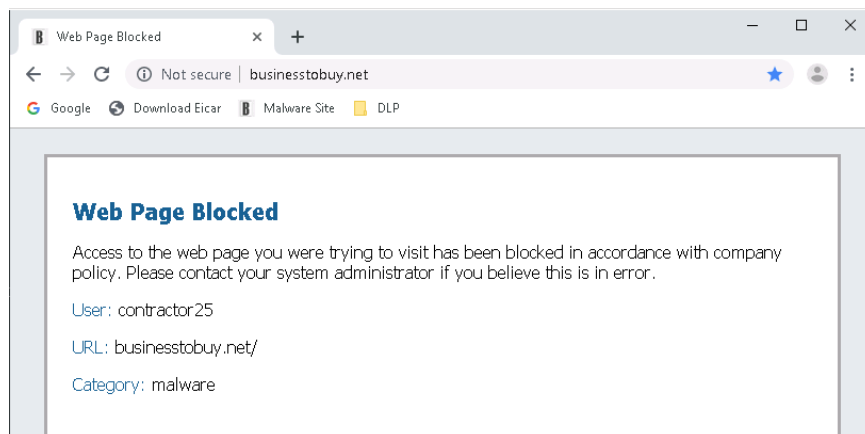


Step 2: Use the **Download Eicar** bookmark to go to **https://secure.eicar.org/eicar.com**. This should be blocked as a security threat by the anti-virus signatures.

Note: Prisma Access is capable of performing decryption. You can't defend against what you can't see.



Step 3: Use the **Malware Site** bookmark to go to **http://businesstobuy.net**. This should be blocked as a malware site by **URL Filtering**.



Summary:

- ✓ Security is delivered from the cloud and closer to where the users are.
- ✓ Security capabilities such as URL Filtering, Threat Prevention and WildFire are included.
- ✓ Removes the need to back-haul users' traffic to the HQs or the data center.

End of Activity 2

Activity 3 – Next Generation Secure Remote Access

In this activity, you will:

- **Demonstrate how User-ID can control access**

Remote users who are connected to Prisma Access can securely access enterprise applications in their HQ or in their branch sites. The HQs and the branch sites are on-boarded to the Cloud Service as well.

Prisma Access allows administrators to control access to enterprise applications based on User / User-Groups, device compliance state and / or the specific application being accessed.

- **Authenticate First** – GlobalProtect agent requires users to successfully authenticate to set up the tunnel. Various authentication methods such as Multi-Factor authentication (MFA), SAML, RADIUS, Active Directory, Certificates are supported
- **Authorize Access** – Successfully setting up a tunnel does not provide access to all application and resources in the HQs / branch office. Only authorized users from authorized devices can access those specific applications that are available for them.
 - **User-ID** – based on user and the user group the user belongs to
 - **Host Information Profile (HIP)** – based on the compliance state of the device from where the application is accessed.
 - **App-ID** – based on application the user is accessing
 - **Services** - based on the service / ports on which the application is accessed.

Task 1 – Control Access with User-ID

Step 1: Recall that the security policies for the **Mobile_User_Device_Group (Panorama-UI: Policies > Security > Pre Rules)** are:

ID	NAME	LOCATION	TAGS	TYPE	Source				Destination	
					ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	Deny QUIC	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any	any	Internet	any
2	Deny QUIC-UDP	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any	any	Internet	any
3	Secure-Internet-Traffic	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any	any	Internet	any
4	Secure-Access-to-HQ-Restricted-Server	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	employee	any	HQ	Restricted-Server
5	Deny-Access-to-HQ-Restricted-Server	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	contractor	any	HQ	Restricted-Server
6	Secure-Access-to-HQ-and-Branch-Office	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	contractor employee	any	Branch-Office HQ	any

The **HQ-Restricted-Server** (IP: 192.168.251.50) is only allowed access by the **employee** user group (**Secure-Access-to-HQ-Restricted-Server**). The **contractor** user group is denied (**Deny-Access-to-HQ-Restricted-Server**).

Step 2: From the **win-mobile** VM, launch the **Command Prompt** from the Windows taskbar.

Type **ping 192.168.251.100**

```
Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\root>ping 192.168.251.100

Pinging 192.168.251.100 with 32 bytes of data:
Reply from 192.168.251.100: bytes=32 time=115ms TTL=61
Reply from 192.168.251.100: bytes=32 time=112ms TTL=61
Reply from 192.168.251.100: bytes=32 time=113ms TTL=61
Reply from 192.168.251.100: bytes=32 time=119ms TTL=61

Ping statistics for 192.168.251.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 112ms, Maximum = 119ms, Average = 114ms

C:\Users\root>
```

As you are still logged into a **contractor[X]** account and are part of the **contractor** user group, you have access to the 192.168.251.100 server. The security policy **Secure-Access-to-HQ-and-Branch-Office** applies to this host.

Step 3: Now try to ping the **HQ-Restricted-Server**.

Type **ping 192.168.251.50**

```
Command Prompt

C:\Users\root>ping 192.168.251.50

Pinging 192.168.251.50 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

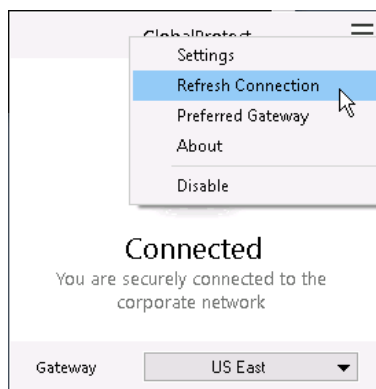
Ping statistics for 192.168.251.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\root>
```

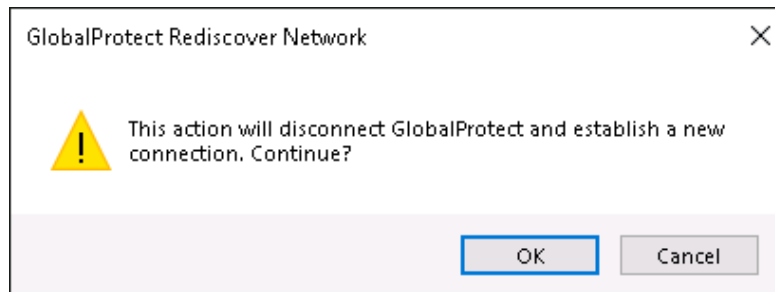
The ping fails as expected due to the **Deny-Access-to-HQ-Restricted-Server** security policy.

Step 4: Bring up the **GlobalProtect** application by clicking the  icon in the system tray.

Step 5: Click on **Settings** (hamburger  icon) > **Refresh Connection**



Step 6: Click **OK** on the **GlobalProtect Rediscover Network** window.



Step 7: In the **GlobalProtect Sign In** window, log in with the following credentials:

Username: *employee[X]* where *[X]* is your **Student-ID** (e.g. employee25)

Password: *utd1234*

Click **Sign In**.

This will establish a new secure tunnel logged into an **employee[X]** account and part of the **employee** user group.

Step 8: As an **employee**, try to ping the **HQ-Restricted-Server**.

Type ***ping 192.168.251.50***

```
Command Prompt
C:\Users\root>ping 192.168.251.50

Pinging 192.168.251.50 with 32 bytes of data:
Reply from 192.168.251.50: bytes=32 time=123ms TTL=61
Reply from 192.168.251.50: bytes=32 time=140ms TTL=61
Reply from 192.168.251.50: bytes=32 time=119ms TTL=61
Reply from 192.168.251.50: bytes=32 time=126ms TTL=61

Ping statistics for 192.168.251.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 119ms, Maximum = 140ms, Average = 127ms

C:\Users\root>
```

The ping is successful as the **Secure-Access-to-HQ-Restricted-Server** is applied here.

You may also ***ping 192.168.251.100*** confirm you still have access to the other HQ server.

Summary:

- ✓ Next Gen Secure remote access to internal applications.
- ✓ Successful tunnel set up and authentication does not automatically provide access to internal applications.
- ✓ Authenticate first and authorize only based on who the user is, what group the user belongs to, the state of the device from where the user is requesting access, the application being accessed, and the ports and services being used

End of Activity 3

Activity 4 – Use Remote Networks to Secure Branches (1 WAN Link)

In this activity, you will:

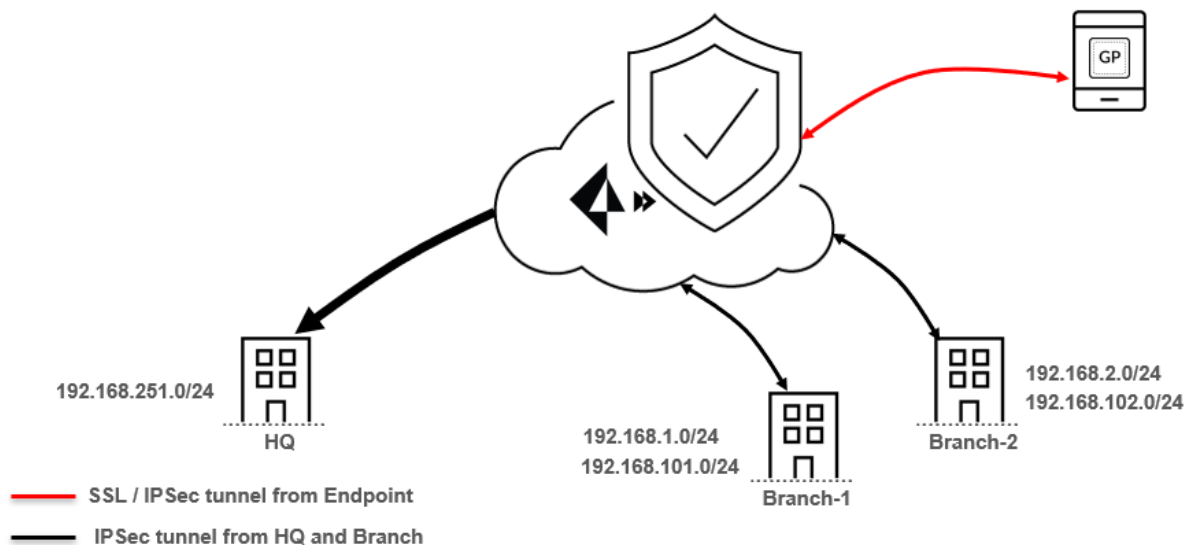
- Access Panorama and review configuration for remote network
- Configure branch/remote network to establish IPsec tunnel to Prisma Access
- Demonstrate that branch/remote network is secure

Prisma Access provides consistent security for all your branch offices without deploying expensive hardware or back-hauling traffic to your data center. All the branch sites have the same set of security policies and controls, centrally managed from Panorama. You can on-board your branch sites to any of the 100+ points of presence available in Prisma Access.

To on-board you need to set up a site-to-site IPsec tunnel from your branch to Prisma Access. You can use any IPsec VPN capable device, including SD-WAN devices to set up this tunnel.

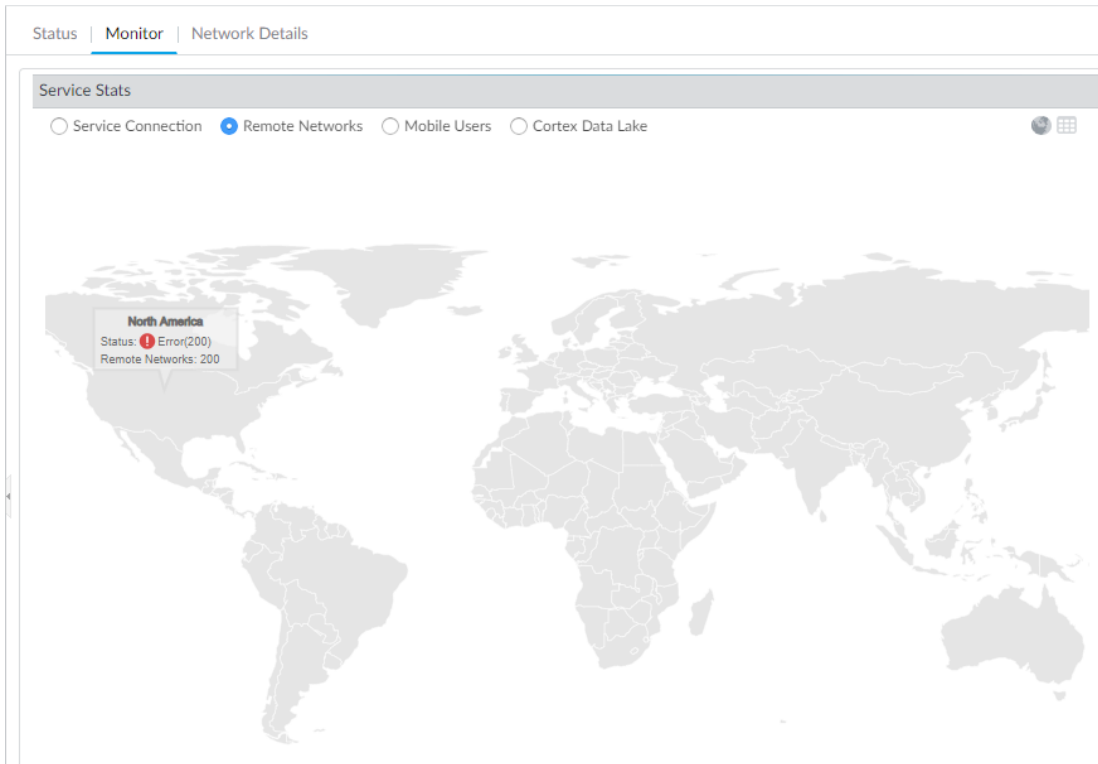
In this workshop you will use a VM-Series firewall as the on-premise device.

Secure Branch Sites (1 WAN Link)



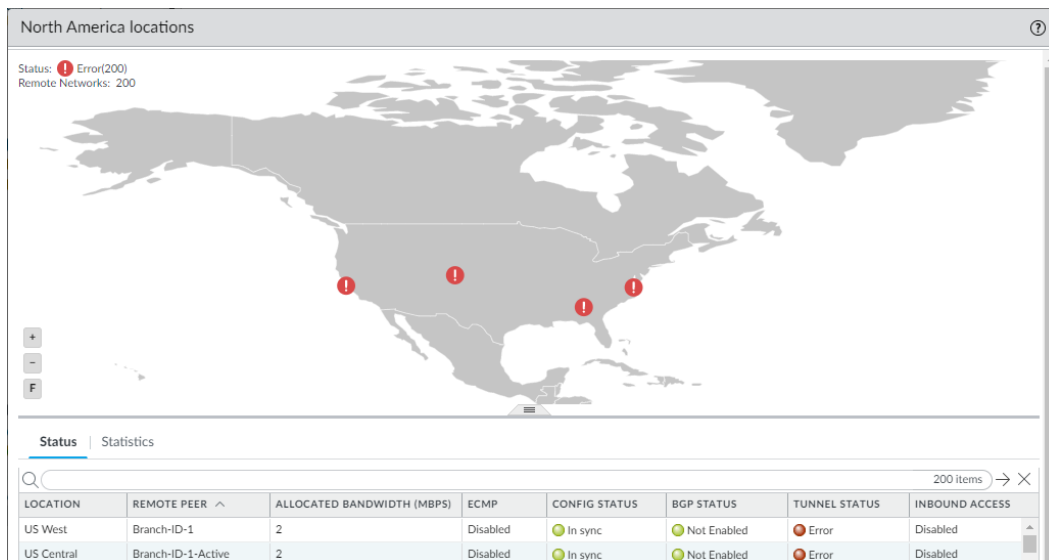
Task 1 – Review Prisma Access Remote Networks from Panorama

Step 1: From the **Panorama-UI** browser tab, navigate to **Panorama > Cloud Services > Status > Monitor > Remote Networks**



As was mentioned in activity 2, task 2, it is expected to see **Error** as not every Remote Network will be connected in our lab.


Step 2: Click on **North America** to bring up the **North America locations** window.

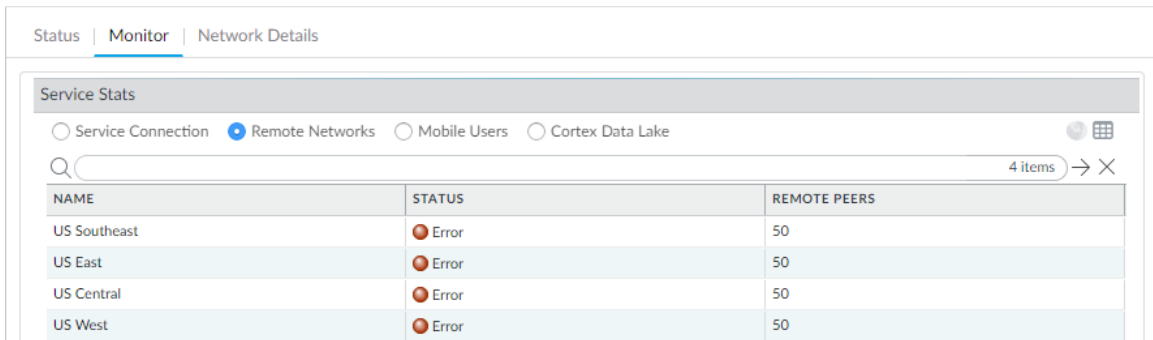


LOCATION	REMOTE PEER	ALLOCATED BANDWIDTH (MBPS)	ECMP	CONFIG STATUS	BGP STATUS	TUNNEL STATUS	INBOUND ACCESS
US West	Branch-ID-1	2	Disabled	In sync	Not Enabled	Error	Disabled
US Central	Branch-ID-1-Active	2	Disabled	In sync	Not Enabled	Error	Disabled

You may review the details of each Remote Network here.

Click **Close**.

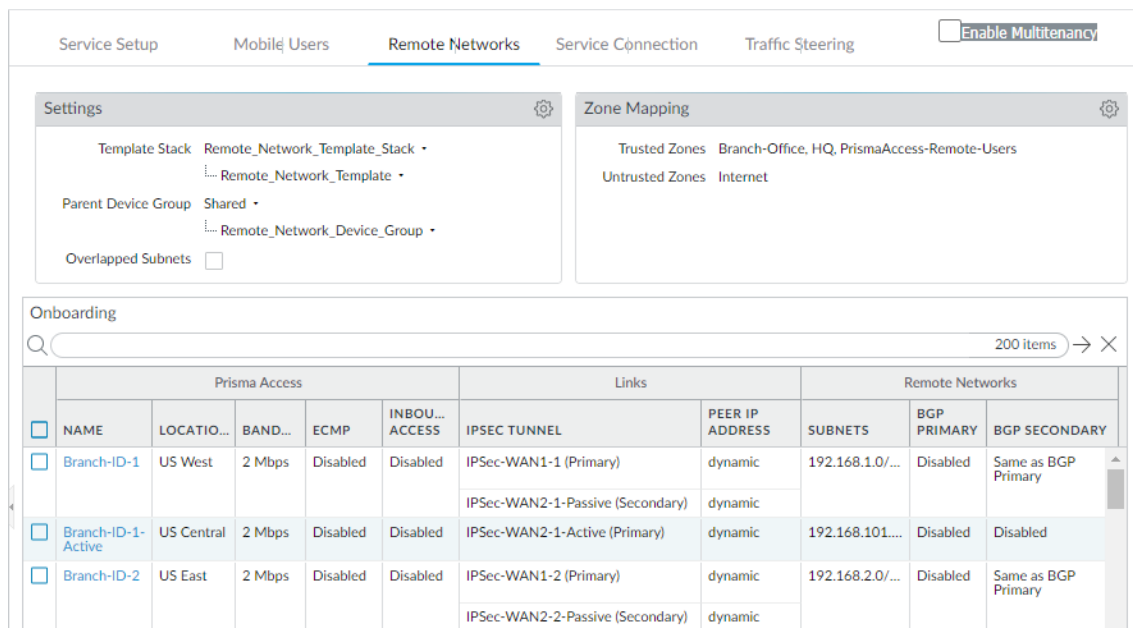
Step 3: In the upper right-hand corner, click the table  icon.




NAME	STATUS	REMOTE PEERS
US Southeast	Error	50
US East	Error	50
US Central	Error	50
US West	Error	50

This will show the number of Remote Networks per region.

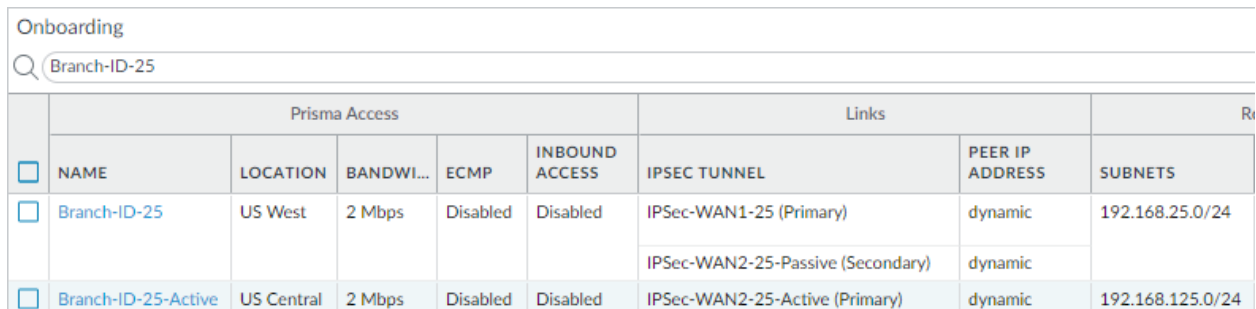
Step 4: Navigate to **Panorama > Cloud Services > Configuration > Remote Networks**



	Prisma Access					Links		Remote Networks		
	NAME	LOCATIO...	BANDW...	ECMP	INBOU... ACCESS	IPSEC TUNNEL	PEER IP ADDRESS	SUBNETS	BGP PRIMARY	BGP SECONDARY
<input type="checkbox"/>	Branch-ID-1	US West	2 Mbps	Disabled	Disabled	IPSec-WAN1-1 (Primary)	dynamic	192.168.10/...	Disabled	Same as BGP Primary
						IPSec-WAN2-1-Passive (Secondary)	dynamic			
<input type="checkbox"/>	Branch-ID-1-Active	US Central	2 Mbps	Disabled	Disabled	IPSec-WAN2-1-Active (Primary)	dynamic	192.168.101...	Disabled	Disabled
<input type="checkbox"/>	Branch-ID-2	US East	2 Mbps	Disabled	Disabled	IPSec-WAN1-2 (Primary)	dynamic	192.168.20/...	Disabled	Same as BGP Primary
						IPSec-WAN2-2-Passive (Secondary)	dynamic			

Step 5: Under **Onboarding**, in the search  box, type **Branch-ID-X**, where **X** is your assigned **Student-ID**.

If your **Student-ID** is **25**, this would look like:



	Prisma Access					Links		SUBNETS
	NAME	LOCATION	BANDWI...	ECMP	INBOUND ACCESS	IPSEC TUNNEL	PEER IP ADDRESS	
<input type="checkbox"/>	Branch-ID-25	US West	2 Mbps	Disabled	Disabled	IPSec-WAN1-25 (Primary)	dynamic	192.168.25.0/24
						IPSec-WAN2-25-Passive (Secondary)	dynamic	
<input type="checkbox"/>	Branch-ID-25-Active	US Central	2 Mbps	Disabled	Disabled	IPSec-WAN2-25-Active (Primary)	dynamic	192.168.125.0/24

Step 6: Click **Branch-ID-X** to review the configuration for that remote network.

What is the assigned **Bandwidth**?

What regional cloud **Location** will your remote network connect to?

What **IPsec Tunnel** profile which be applied?

Which of your **Branch IP Subnets** can be reached via this tunnel?

Is a **Secondary WAN** link available?

Click **Cancel**.

Step 7: Navigate to **Panorama > Cloud Services > Status > Network Details > Remote Networks**

NAME ^	SERVICE IP ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET	Secure Inbound Apps		EBGP ROUTER	BRANCH AS AND ROUTER
				APP NAME / PUBLIC ADDRESS / PRIVATE ADDRESS:PORT			
Branch-ID-1	208.127.86.164	dynamic	192.168.1.0/24			172.31.1.16	
Branch-ID-1-Active	208.127.191.116	dynamic	192.168.101.0/24			172.31.1.15	

Step 8: From the search box, type **Branch-ID-X**, where **X** is your assigned **Student-ID**.

If your **Student-ID** is **25**, this would look like:

NAME ^	SERVICE IP ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET	Secure Inbound Apps		EBGP ROUTER	BRANCH AS AND ROUTER
				APP NAME / PUBLIC ADDRESS / PRIVATE ADDRESS:PORT			
Branch-ID-25	208.127.86.164	dynamic	192.168.25.0/24			172.31.1.16	
Branch-ID-25-Active	208.127.191.116	dynamic	192.168.125.0/24			172.31.1.15	

Record the **Service IP Address** for your **Branch-ID-X**. This will be used in the next task. **Note:** Do not use the IP for Branch-ID-X-Active for this activity- it will be used later.

Task 2 – Configure IPsec Tunnel on NGFW

Step 1: From the **NGFW-Branch-UI (student / utd1234)** tab, navigate to **Network > Network Profiles > IKE Gateways**.

NAME	PEER ADDRESS	Local Address		Peer ID		Local ID		VERSION
		INTERFACE	IP	ID	TYPE	ID	TYPE	
<input type="checkbox"/> WAN-1-IKE-GW	10.10.10.10	ethernet1/1	172.16.10.1/24	cloud1-99@utd-sase.local	User FQDN (email address)	wan1-99@utd-sase.local	User FQDN (email address)	ikev1
<input type="checkbox"/> WAN-2-IKE-GW	10.10.10.10	ethernet1/3	172.16.20.1/24	cloud2-99@utd-sase.local	User FQDN (email address)	wan2-99@utd-sase.local	User FQDN (email address)	ikev1

Step 2: Click **WAN-1-IKE-GW** to open the **IKE Gateway** window.

IKE Gateway ⓘ

General | Advanced Options

Name: WAN-1-IKE-GW

Version: IKEv1 only mode

Address Type: IPv4 IPv6

Interface: ethernet1/1

Local IP Address: 172.16.10.1/24

Peer IP Address Type: IP FQDN Dynamic

Peer Address: 10.10.10.10

Authentication: Pre-Shared Key Certificate

Pre-shared Key: ●●●●●●

Confirm Pre-shared Key: ●●●●●●

Local Identification: User FQDN (email address) wan1-99@utd-sase.local

Peer Identification: User FQDN (email address) cloud1-99@utd-sase.local

Comment:

OK Cancel

Step 3: Update the **Peer Address (10.10.10.10)** with the **Service IP Address** you recorded in the previous task in Panorama.

Also, change the **Local Identification** and **Peer Identification** values of **wan1-99@utd-sase.local** and **cloud1-99@utd-sase.local**, replacing the **99** with your **Student-ID**.

If your **Student-ID** is **25**, this would be **wan1-25@utd-sase.local** and **cloud1-25@utd-sase.local**.

Click **OK**.

Step 4: Select **WAN1-IKE-GW** and click **Enable** **Enable** at the bottom of the page.

Click **Yes**.

	NAME	PEER ADDRESS	Local Address	
			INTERFACE	IP
<input type="checkbox"/>	WAN-1-IKE-GW	208.127.86.164	ethernet1/1	172.16.10.1/24
<input type="checkbox"/>	WAN-2-IKE-GW	10.10.10.10	ethernet1/3	172.16.20.1/24

The text should change from grey to black.

Step 5: Navigate to **Network > IPsec Tunnels**.

The screenshot shows the Palo Alto VM Network configuration page. The left sidebar contains a navigation menu with items: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels (selected), GRE Tunnels, DHCP, and DNS Proxy. The main content area displays a table of IPsec Tunnels under the heading 'IKE Gateway/Satellite'.

	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS
<input type="checkbox"/>	WAN-1-IPsec	● Tunnel Info	Auto Key	ethernet1/1	172.16.10.1/24	208.127.86.164	● IKE Info
<input type="checkbox"/>	WAN-2-IPsec	● Tunnel Info	Auto Key	ethernet1/3	172.16.20.1/24	10.10.10.10	● IKE Info

Step 6: Select **WAN-1-IPsec** and click **Enable** **Enable**.

The dialog box is titled 'IPsec Tunnel' and contains the question: 'Do you really want to enable 1 IPsec Tunnel(s)?'. Below the question are two buttons: 'Yes' and 'No'.

Click **Yes**.

Step 7: Navigate to **Network > Virtual Routers**.

The screenshot shows the Palo Alto VM Network configuration page with 'Virtual Routers' selected in the sidebar. The main content area displays a table of Virtual Routers.

	NAME	INTERFACES	CONFIGURATION	RIP	OSPF
<input type="checkbox"/>	default	ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4 tunnel.1 tunnel.2	Static Routes: 6 ECMP status: Disabled		

Step 8: Click **default** to open the **Virtual Router – default** window.

Select the **Static Routes** node.

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

6 items

	NAME	DESTINATION	INTERFACE	Next Hop		ADMIN DISTAN...	ME...	BFD	ROUTE TABLE
				TYPE	VALUE				
<input type="checkbox"/>	default-route	0.0.0.0/0	tunnel.1			default	10	None	unicast
<input type="checkbox"/>	Alt-default-route	0.0.0.0/0	tunnel.2			default	100	None	unicast
<input type="checkbox"/>	Route-WAN-1-Tunnel-Setup	10.10.10.10/32	ethernet1/1	ip-address	172.16.10.254	default	10	None	unicast
<input type="checkbox"/>	Alt-Route-WAN-1-Tunnel-Setup	10.10.10.10/32	ethernet1/3	ip-address	172.16.20.254	default	100	None	unicast
<input type="checkbox"/>	Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/3	ip-address	172.16.20.254	default	10	None	unicast
<input type="checkbox"/>	Alt-Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/1	ip-address	172.16.10.254	default	100	None	unicast

+ Add - Delete Clone

OK Cancel

Step 9: Click **Route-WAN-1-Tunnel-Setup**.

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

	NAME	DESTINATION	INTERFACE	Next Hop	
				TYPE	VALUE
<input type="checkbox"/>	default-route	0.0.0.0/0	tunnel.1		
<input type="checkbox"/>	Alt-default-route	0.0.0.0/0	tunnel.2		
<input type="checkbox"/>	Route-WAN-1-Tunnel-Setup	10.10.10.10/32	ethernet1/1	ip-address	172.16.10.254
<input type="checkbox"/>	Alt-Route-WAN-1-Tunnel-Setup	10.10.10.10/32	ethernet1/3	ip-address	172.16.20.254
<input type="checkbox"/>	Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/3	ip-address	172.16.20.254

Step 10: Update the **Destination** of **10.10.10.10/32** with the **Service IP Address** previously recorded.
Note: Make sure to append **/32** to the IP. This allows the IPsec tunnel to be set up with Prisma Access over ethernet1/1.

Virtual Router - Static Route - IPv4

Name: Route-WAN-1-Tunnel-Setup

Destination: 208.127.86.164/32

Interface: ethernet1/1

Next Hop: IP Address

172.16.10.254

Admin Distance: 10 - 240

Metric: 10

Route Table: Unicast

BFD Profile: Disable BFD

Path Monitoring

Click **OK** to close the **Virtual Router – Static Route – IPv4** window.
 Click **OK** to close the **Virtual Router – default** window.

Step 11: **Commit** your changes.

Step 12: Navigate to **Network > IPsec Tunnels** to confirm that **WAN-1-IPsec** is up.

	NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface				
				INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERF...	VIRTUAL ROUTER	VIRT... SYST...	S... Z...	ST...
<input type="checkbox"/>	WAN-1-IPsec	● Tunnel Info	Auto Key	ethernet1/1	172.16.10.1/24	208.127.86.164	● IKE Info	tunnel.1	default (Show Routes)	vsys1	lan	
<input type="checkbox"/>	WAN-2-IPsec	● Tunnel Info	Auto Key	ethernet1/3	172.16.20.1/24	10.10.10.10	● IKE Info	tunnel.2	default (Show Routes)	vsys1	lan	

Troubleshooting: If the tunnel does not come up, verify the following:

- Confirm **IKE Gateway** is using correct **Peer Address**, and **Local** and **Peer Identification** settings.
- Confirm the **IKE Gateway** and **IPsec Tunnel** are enabled.
- Confirm **Virtual Router** settings are correct for **Static Route**.
- Confirm **Student-ID** values in **Interfaces** and **Tunnel**.
- Review logs at **Monitor > System** to confirm if IKE phase-1 and IKE phase-2 are up. It may help to search (*subtype eq vpn*) to help filter messages. If you see: **IKE phase-1 negotiation is failed as initiator, aggressive mode. Failed SA... Due to timeout.** Proceed to the next list item.
- If all of the above are correct, reboot the NGFW via **Device > Setup > Operations > Device Operations > Reboot Device**. If this step is necessary, it is due to the lab environment. Please let your instructor know you needed to perform this operation.

Task 3 – Verify Secured Remote Network

Step 1: From the **win-mobile** VM and connected as a remote user (**employeeX**) to Prisma Access, access resources in your branch/remote network.

Type **ping 192.168.X.100**, where **X** is your assigned **Student-ID**.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\root>ping 192.168.25.100

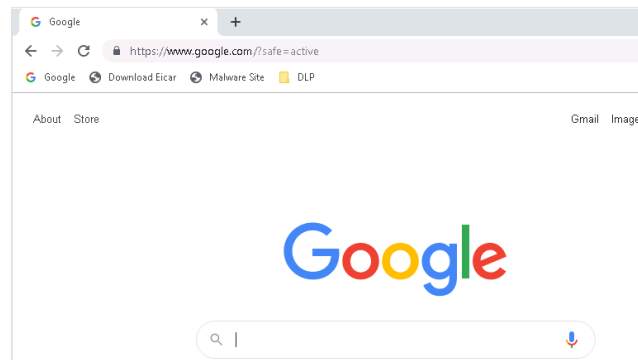
Pinging 192.168.25.100 with 32 bytes of data:
Reply from 192.168.25.100: bytes=32 time=164ms TTL=124
Reply from 192.168.25.100: bytes=32 time=151ms TTL=124
Reply from 192.168.25.100: bytes=32 time=146ms TTL=124
Reply from 192.168.25.100: bytes=32 time=158ms TTL=124

Ping statistics for 192.168.25.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 146ms, Maximum = 164ms, Average = 154ms

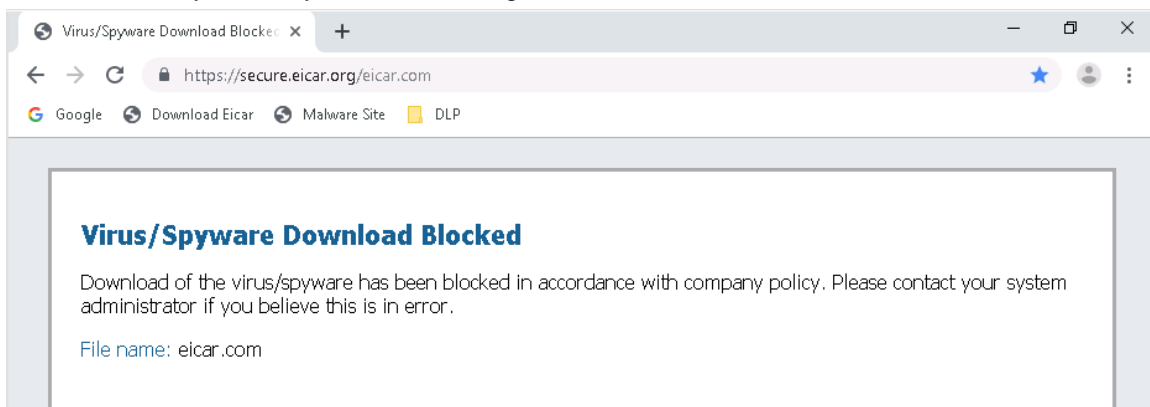
C:\Users\root>
```

Note: You should also be able to access other branch/remote networks if they are connected. If Student-ID 10 is connected, you should be able to ping 192.168.10.100 as well.

Step 2: From the **win-subnet1** VM, launch **Chrome**. Use the **Google** bookmark to browse to www.google.com. This should be successful.

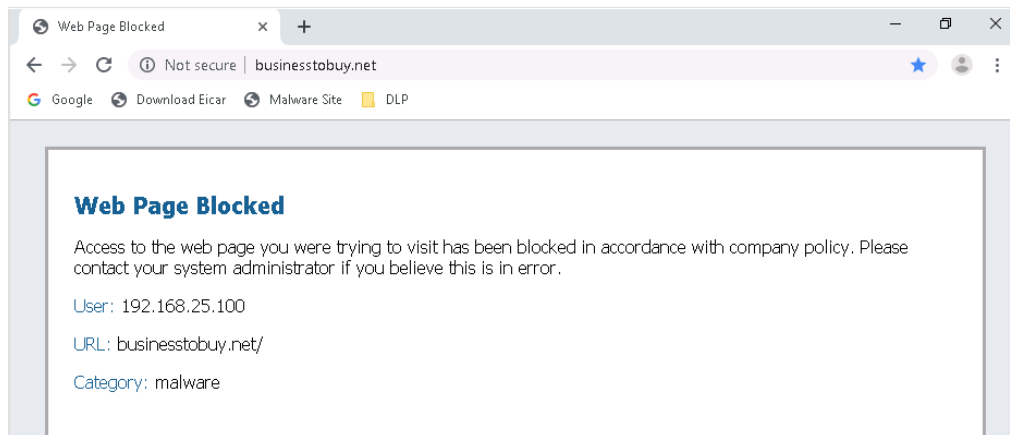


Step 3: Use the **Download Eicar** bookmark to go to <https://secure.eicar.org/eicar.com>. This should be blocked as a security threat by the anti-virus signatures.



Note: As before, Prisma Access is able to decrypt your SSL/TLS based traffic. Branch office and remote users have the same protections.

Step 4: Use the **Malware Site** bookmark to go to ***http://businessstobuy.net***. This should be blocked as a malware site by **URL Filtering**.



Step 5: From the **Command Prompt**, type ***ping 192.168.251.50***

```
ca Command Prompt
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\root>ping 192.168.251.50

Pinging 192.168.251.50 with 32 bytes of data:
Reply from 192.168.251.50: bytes=32 time=108ms TTL=60
Reply from 192.168.251.50: bytes=32 time=106ms TTL=60
Reply from 192.168.251.50: bytes=32 time=111ms TTL=60
Reply from 192.168.251.50: bytes=32 time=105ms TTL=60

Ping statistics for 192.168.251.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 105ms, Maximum = 111ms, Average = 107ms

C:\Users\root>
```

As a user within the Remote Network, you should have access to the **HQ-Restricted-Server**.

Step 6: From the **Panorama-UI** tab, navigate to **Policies > Security > Pre Rules**. Change the **Device Group** to **Remote_Network_Device_Group**.

	NAME	LOCATION	TAGS	TYPE	Source				Des
					ZONE	ADDRESS	USER	DEVICE	
1	Deny QUIC	Remote_Network_Device_Group	none	universal	Branch-Office	any	any	any	Internet
2	Deny QUIC-UDP	Remote_Network_Device_Group	none	universal	Branch-Office	any	any	any	Internet
3	Secure-Internet-Traffic	Remote_Network_Device_Group	none	universal	Branch-Office	any	any	any	Internet
4	Secure-Access-to-HQ	Remote_Network_Device_Group	none	universal	Branch-Office	any	any	any	HQ
5	Secure-Access-to-Branch	Remote_Network_Device_Group	none	universal	Branch-Office HQ PrismaAccess-Remote-Users	any	any	any	Branch-Office

Review the security policies that are applied to the branch/remote networks.

Summary:

- ✓ Branch offices secured by Prisma Access
- ✓ Secured consistently and operationally efficiently
- ✓ Enables secure communication between
 - Remote mobile users and the branch
 - Remote branch offices
 - Remote branch offices and HQ

End of Activity 4

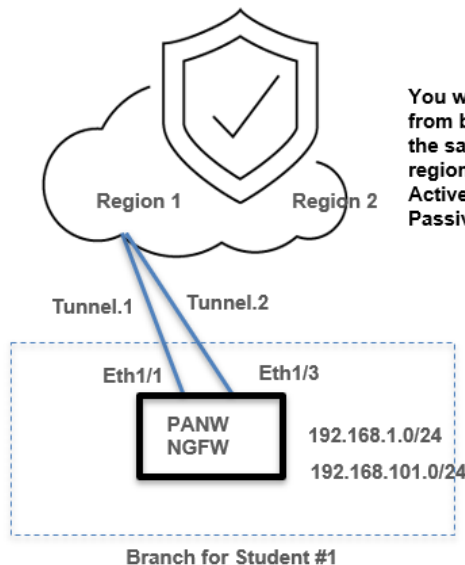
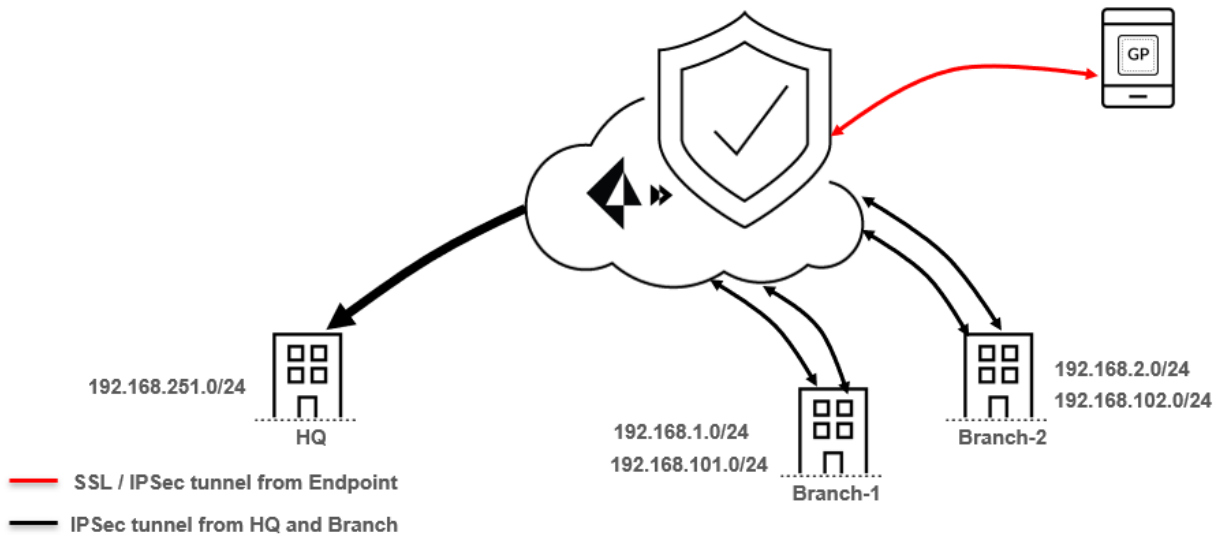
Activity 5 – Secure Branch Sites with 2 WAN Links (Active/Passive)

In this activity, you will:

- Configure branch/remote network to establish active/passive IPSec tunnels to Prisma Access
- Demonstrate IPSec tunnel failover

You can on-board your remote network or branch office using more than 1 WAN link. In this activity, you will on-board using 2 WAN links and use the 2nd WAN link as a Secondary or Passive. The Secondary Tunnel will become active in case the tunnel through Primary WAN link is identified as down.

Secure Branch Sites (2 WAN Links)



Task 1 – Review Remote Network Secondary WAN Configuration

Step 1: From the **Panorama-UI** browser tab, navigate to **Panorama > Cloud Services > Configuration > Remote Networks**.

Click **Branch-ID-X**, where **X** is your assigned **Student-ID**.

	Prisma Access					Links		Remote Networks		
<input type="checkbox"/>	CONNECTION NAME	LOCATION	BANDWI...	ECMP	INBOUND ACCESS	IPSEC TUNNEL	PEER IP ADDRESS	SUBNETS	BGP PRIMARY	BGP SECONDARY
<input type="checkbox"/>	Branch-ID-25	US West	2 Mbps	Disabled	Disabled	IPSec-WAN1-25 (Primary)	dynamic	192.168.25.0/24	Disabled	Same as BGP Primary
						IPSec-WAN2-25-Passive (Secondary)	dynamic			
<input type="checkbox"/>	Branch-ID-25-Active	US Central	2 Mbps	Disabled	Disabled	IPSec-WAN2-25-Active (Primary)	dynamic	192.168.125.0/24	Disabled	Disabled

Step 2: Confirm that **Enable Secondary WAN** is checked and note which **IPSec Tunnel** it will use.

Onboarding ⓘ

Name: Branch-ID-25

ECMP Load Balancing: None

Location: US West

Bandwidth: 2 Mbps

IPSec Tunnel: IPSec-WAN1-25

Enable Secondary WAN

IPSec Tunnel: IPSec-WAN2-25-Passive

Static Routes | BGP | QoS | Inbound Access

<input type="checkbox"/>	BRANCH IP SUBNETS
<input type="checkbox"/>	192.168.25.0/24

Click **Cancel**.

Step 3: Navigate to **Panorama > Cloud Services > Status > Network Details > Remote Networks**.

NAME ^	SERVICE IP ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET
Branch-ID-25	208.127.86.164	dynamic	192.168.25.0/24
Branch-ID-25-Active	208.127.191.116	dynamic	192.168.125.0/24

You will be using the same **Service IP Address** as the previous activity as the secondary/passive link will be used in the event of a failure with the primary/active connection.

Task 2 – Configure Secondary/Passive IPSec Tunnel on NGFW

Step 1: From the **NGFW-Branch-UI** tab, navigate to **Network > Network Profiles > IKE Gateways**.

NAME	PEER ADDRESS	Local Address		Peer ID		Local ID		VERSION
		INTERFACE	IP	ID	TYPE	ID	TYPE	
WAN-1-IKE-GW	208.127.86.164	ethernet1/1	172.16.10.1/24	cloud1-25@utd-sase.local	User FQDN (email address)	wan1-25@utd-sase.local	User FQDN (email address)	ikev1
WAN-2-IKE-GW	10.10.10.10	ethernet1/3	172.16.20.1/24	cloud2-99@utd-sase.local	User FQDN (email address)	wan2-99@utd-sase.local	User FQDN (email address)	ikev1

Step 2: Click **WAN-2-IKE-GW** to open the **IKE Gateway** window.

IKE Gateway

General | Advanced Options

Name: WAN-2-IKE-GW

Version: IKEv1 only mode

Address Type: IPv4 IPv6

Interface: ethernet1/3

Local IP Address: 172.16.20.1/24

Peer IP Address Type: IP FQDN Dynamic

Peer Address: 10.10.10.10

Authentication: Pre-Shared Key Certificate

Pre-shared Key:

Confirm Pre-shared Key:

Local Identification: User FQDN (email address) wan2-99@utd-sase.local

Peer Identification: User FQDN (email address) cloud2-99@utd-sase.local

Comment:

OK Cancel

Step 3: Update the **Peer Address (10.10.10.10)** with the **Service IP Address** you recorded in the previous task in Panorama.

Also, change the **Local Identification** and **Peer Identification** values of **wan2-99@utd-sase.local** and **cloud2-99@utd-sase.local**, replacing the **99** with your **Student-ID**.

If your **Student-ID** is **25**, this would be **wan2-25@utd-sase.local** and **cloud2-25@utd-sase.local**.

Click **OK**.

Step 4: Select **WAN2-IKE-GW** and click **Enable** **Enable** at the bottom of the window.

Click **Yes**.

	NAME	PEER ADDRESS	Local Address	
			INTERFACE	IP
<input type="checkbox"/>	WAN-1-IKE-GW	208.127.86.164	ethernet1/1	172.16.10.1/24
<input type="checkbox"/>	WAN-2-IKE-GW	208.127.86.164	ethernet1/3	172.16.20.1/24

The text should change from grey to black.

Step 5: Navigate to **Network > IPsec Tunnels**.

IKE Gateway/Satellite							
	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS
<input type="checkbox"/>	WAN-1-IPSec	● Tunnel Info	Auto Key	ethernet1/1	172.16.10.1/24	208.127.86.164	● IKE Info
<input type="checkbox"/>	WAN-2-IPSec	● Tunnel Info	Auto Key	ethernet1/3	172.16.20.1/24	208.127.86.164	● IKE Info

Step 6: Select **WAN-2-IPSec** and click **Enable** **Enable**.

IPsec Tunnel

Do you really want to enable 1 IPsec Tunnel(s)?

Click **Yes**.

Step 7: Navigate to **Network > Virtual Routers**.

	NAME	INTERFACES	CONFIGURATION	RIP	OSPF
<input type="checkbox"/>	default	ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4 tunnel.1 tunnel.2	Static Routes: 6 ECMP status: Disabled		

Step 8: Click **default** to open the **Virtual Router – default** window.

Select the **Static Routes** node.

Virtual Router - default ?

Router Settings

Static Routes | IPv4 | IPv6

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

	NAME	DESTINATION	INTERFACE	Next Hop		ADMIN DISTAN...	ME...	BFD	ROUTE TABLE
				TYPE	VALUE				
<input type="checkbox"/>	default-route	0.0.0.0/0	tunnel.1			default	10	None	unicast
<input type="checkbox"/>	Alt-default-route	0.0.0.0/0	tunnel.2			default	100	None	unicast
<input type="checkbox"/>	Route-WAN-1-Tunnel-Setup	208.127.86.164...	ethernet1/1	ip-address	172.16.10.254	default	10	None	unicast
<input type="checkbox"/>	Alt-Route-WAN-1-Tunnel-Setup	10.10.10.10/32	ethernet1/3	ip-address	172.16.20.254	default	100	None	unicast
<input type="checkbox"/>	Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/3	ip-address	172.16.20.254	default	10	None	unicast
<input type="checkbox"/>	Alt-Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/1	ip-address	172.16.10.254	default	100	None	unicast

Step 9: Click **Alt-Route-WAN-1-Tunnel-Setup**.

Virtual Router - default						
Router Settings						
Static Routes						
Redistribution Profile						
RIP						
OSPF						
OSPFv3						
BGP						
Multicast						
	NAME	DESTINATION	INTERFACE	Next Hop		
				TYPE	VALUE	
<input type="checkbox"/>	default-route	0.0.0.0/0	tunnel.1			
<input type="checkbox"/>	Alt-default-route	0.0.0.0/0	tunnel.2			
<input type="checkbox"/>	Route-WAN-1-Tunnel-Setup	208.127.86.164...	ethernet1/1	ip-address	172.16.10.254	
<input type="checkbox"/>	Alt-Route-WAN-1-Tunnel-Setup	10.10.10.10/32	ethernet1/3	ip-address	172.16.20.254	

Step 10: Update the **Destination** of **10.10.10.10/32** with the **Service IP Address** (from **Branch-ID-X**) previously recorded. **Note:** Make sure to append **/32** to the IP. This allows the IPsec tunnel to be set up with Prisma Access over ethernet1/3.

Virtual Router - Static Route - IPv4	
Name	Alt-Route-WAN-1-Tunnel-Setup
Destination	208.127.86.164/32
Interface	ethernet1/3
Next Hop	IP Address
	172.16.20.254
Admin Distance	10 - 240
Metric	100
Route Table	Unicast
BFD Profile	Disable BFD
<input type="checkbox"/> Path Monitoring	

Click **OK** to close the **Virtual Router – Static Route – IPv4** window.
 Click **OK** to close the **Virtual Router – default** window.

Step 11: Commit your changes.

Step 12: Navigate to **Network > IPSec Tunnels** to confirm that **WAN-2-IPSec** is up.

	NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface				
				INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERF...	VIRTUAL ROUTER	VIRT... SYST...	S... Z...	ST...
<input type="checkbox"/>	WAN-1-IPSec	● Tunnel Info	Auto Key	ethernet1/1	172.16.10.1/24	208.127.86.164	● IKE Info	tunnel.1	default (Show Routes)	vsys1	lan	
<input type="checkbox"/>	WAN-2-IPSec	● Tunnel Info	Auto Key	ethernet1/3	172.16.20.1/24	208.127.86.164	● IKE Info	tunnel.2	default (Show Routes)	vsys1	lan	

Task 3 – Verify IPSec Tunnel Failover

Step 1: From **win-mobile**, use the **Command Prompt** to trace the route to your remote network.

Type **tracert 192.168.X.100**, where **X** is your assigned **Student-ID**.

```
Command Prompt

C:\Users\root>tracert 192.168.25.100

Tracing route to 192.168.25.100 over a maximum of 30 hops

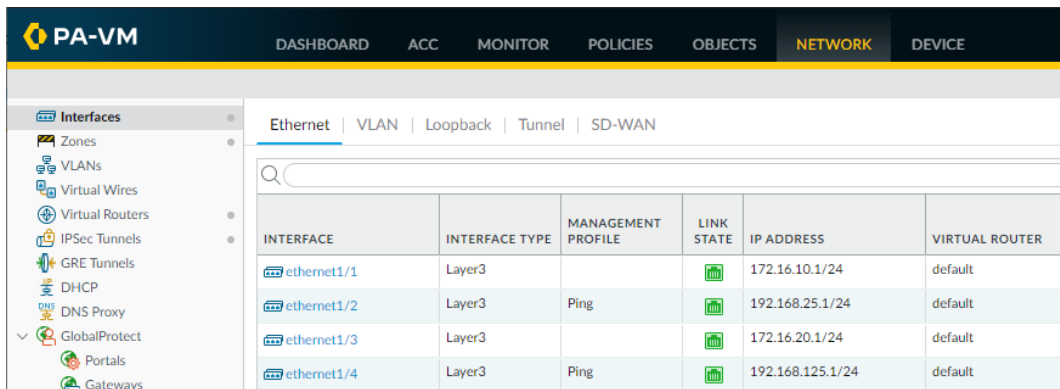
  1    57 ms    27 ms    26 ms    172.30.10.1
  2     *        *        *        Request timed out.
  3     *        *        *        Request timed out.
  4   149 ms   149 ms   144 ms   192.168.25.251
  5   160 ms   149 ms   148 ms   192.168.25.100

Trace complete.

C:\Users\root>
```

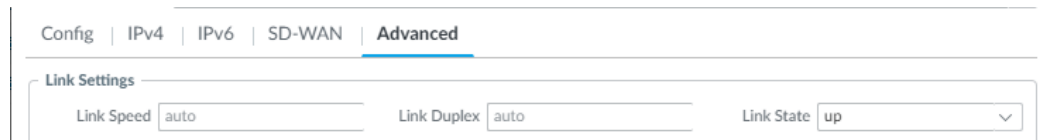
Notice that the network packets travel through **tunnel.1 (192.168.X.251)**.

Step 2: From the **NGFW-Branch-UI** tab, navigate to **Network > Interfaces > Ethernet**.

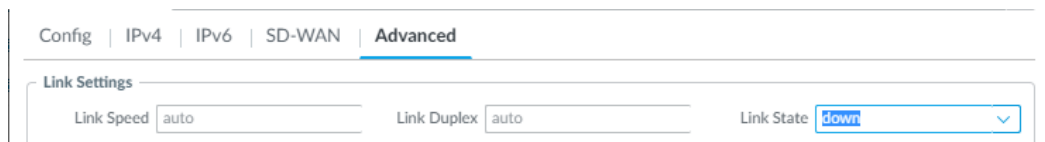


Step 3: Click **ethernet1/1** to bring down the **Ethernet Interface** window for this interface.

Step 4: Click the **Advanced** tab.



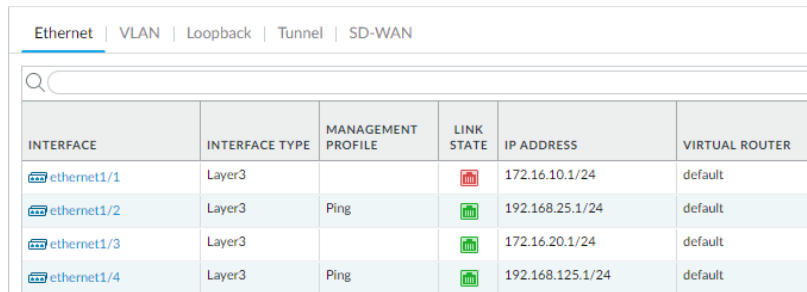
Change the **Link State** from **up** to **down**.



Click **OK**.

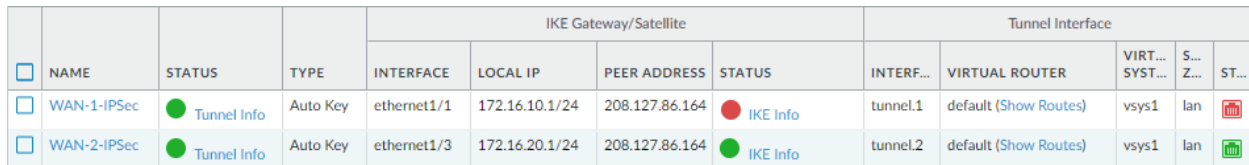
Step 5: Commit your changes.

Step 6: Verify that **ethernet1/1** is down.



INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER
ethernet1/1	Layer3			172.16.10.1/24	default
ethernet1/2	Layer3	Ping		192.168.25.1/24	default
ethernet1/3	Layer3			172.16.20.1/24	default
ethernet1/4	Layer3	Ping		192.168.125.1/24	default

Step 7: Navigate to **Network > IPSec Tunnels**. Verify that the **WAN-1-IPSec** tunnel is down.

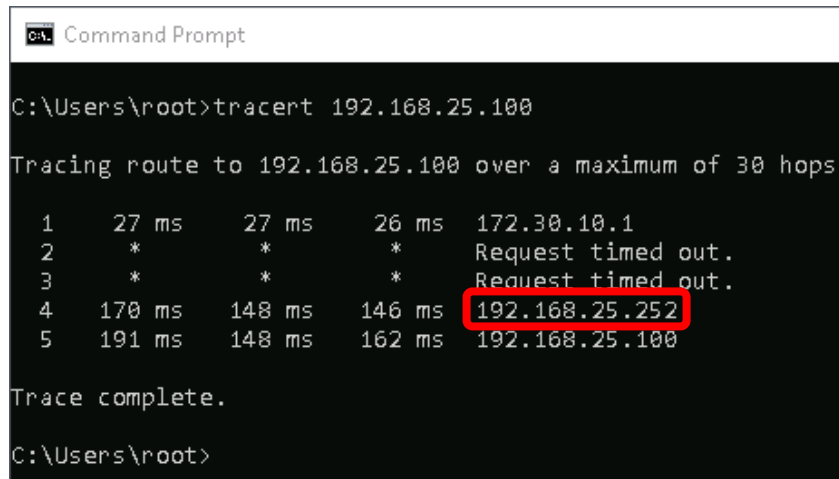


	NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface				
				INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERF...	VIRTUAL ROUTER	VIRT... SYST...	S... Z...	ST...
<input type="checkbox"/>	WAN-1-IPSec	Tunnel Info	Auto Key	ethernet1/1	172.16.10.1/24	208.127.86.164	IKE Info	tunnel.1	default (Show Routes)	vsys1	lan	
<input type="checkbox"/>	WAN-2-IPSec	Tunnel Info	Auto Key	ethernet1/3	172.16.20.1/24	208.127.86.164	IKE Info	tunnel.2	default (Show Routes)	vsys1	lan	

Note: It will take a few minutes for the GUI to reflect the IKE Gateway and IPSec tunnel to be down. If you see the red status icon, then the tunnel is likely already down. You will verify this in the next step.

Step 8: From **win-mobile**, use the **Command Prompt** to trace the route to your remote network.

Type **tracert 192.168.X.100**, where **X** is your assigned **Student-ID**.



```
C:\Users\root>tracert 192.168.25.100

Tracing route to 192.168.25.100 over a maximum of 30 hops

  1  27 ms  27 ms  26 ms  172.30.10.1
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.
  4  170 ms 148 ms 146 ms 192.168.25.252
  5  191 ms 148 ms 162 ms 192.168.25.100

Trace complete.

C:\Users\root>
```

Notice that the network packets now travel through **tunnel.2 (192.168.X.252)**.

Step 9: From the **NGFW-Branch-UI** tab, navigate to **Network > Interfaces > Ethernet**.

Bring up **ethernet1/1**.

Commit.

Step 10: You may also do the *tracert 192.168.X.100* again to confirm that traffic is going back through **tunnel.1**.

Summary:

- ✓ Branch offices can be on-boarded to Prisma Access using 2 WAN links.
- ✓ Prisma Access monitors the tunnel and automatically falls back to using the Secondary WAN link.

End of Activity 5

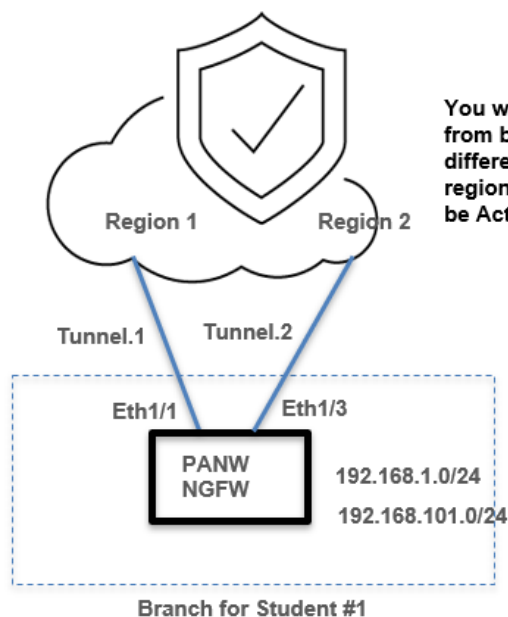
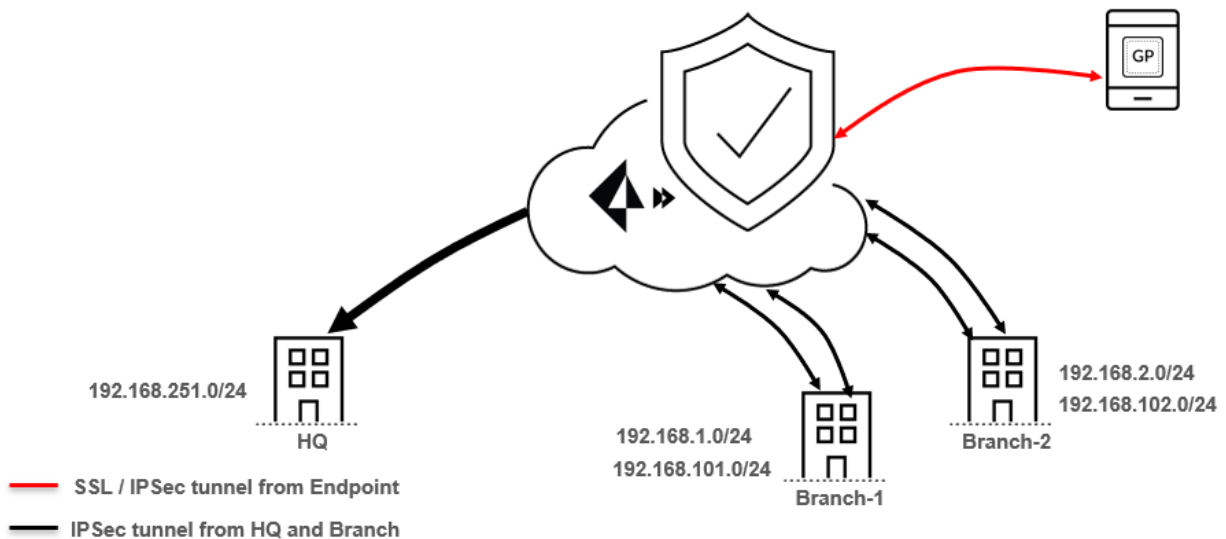
Activity 6 – Secure Branch Sites with 2 WAN Links (Active/Active)

In this activity, you will:

- Configure branch/remote network to establish active/active IPSec tunnels to Prisma Access
- Demonstrate concurrent access to subnets

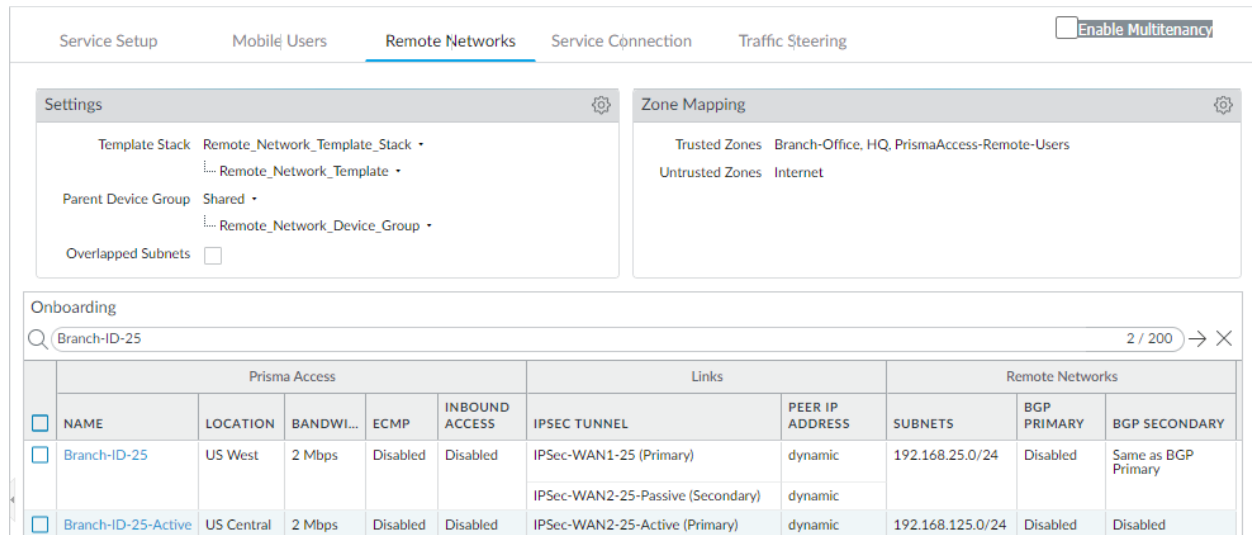
From your remote branch office, you can also have more than one actively used connection to Prisma Access. You will configure them as individual Remote Networks configuration in Panorama and specify their individual Bandwidth requirement and Region in the Cloud.

Secure Branch Sites (2 WAN Links)



Task 1 – Review Prisma Access Remote Networks from Panorama

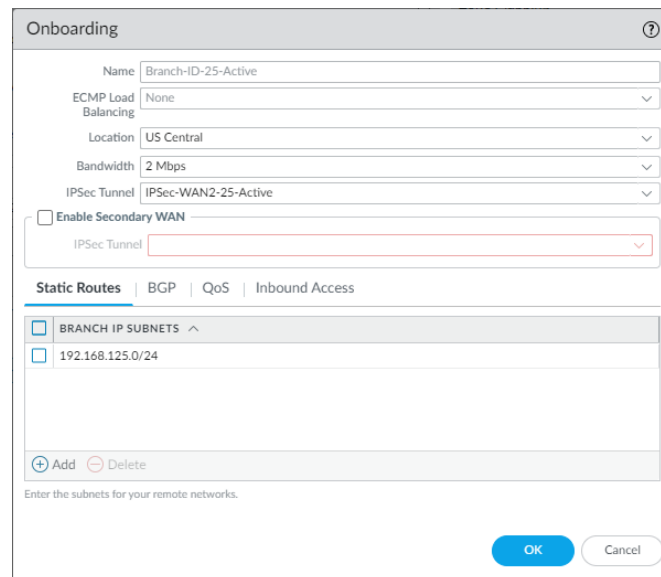
Step 1: From the **Panorama-UI** browser tab, navigate to **Panorama > Cloud Services > Configuration > Remote Networks**



The screenshot shows the Panorama UI configuration page for Remote Networks. The top navigation bar includes Service Setup, Mobile Users, Remote Networks (selected), Service Connection, and Traffic Steering. There is an 'Enable Multitenancy' toggle. The main content area is divided into two panels: Settings and Zone Mapping. The Settings panel shows Template Stack (Remote_Network_Template_Stack), Parent Device Group (Shared), and Overlapped Subnets (unchecked). The Zone Mapping panel shows Trusted Zones (Branch-Office, HQ, PrismaAccess-Remote-Users) and Untrusted Zones (Internet). Below these panels is an 'Onboarding' section with a search bar for 'Branch-ID-25' and a table of remote networks.

	Prisma Access					Links		Remote Networks		
	NAME	LOCATION	BANDWI...	ECMP	INBOUND ACCESS	IPSEC TUNNEL	PEER IP ADDRESS	SUBNETS	BGP PRIMARY	BGP SECONDARY
<input type="checkbox"/>	Branch-ID-25	US West	2 Mbps	Disabled	Disabled	IPSec-WAN1-25 (Primary)	dynamic	192.168.25.0/24	Disabled	Same as BGP Primary
						IPSec-WAN2-25-Passive (Secondary)	dynamic			
<input type="checkbox"/>	Branch-ID-25-Active	US Central	2 Mbps	Disabled	Disabled	IPSec-WAN2-25-Active (Primary)	dynamic	192.168.125.0/24	Disabled	Disabled

Step 2: Click **Branch-ID-X-Active** to review the configuration for that remote network.



The screenshot shows the 'Onboarding' configuration window for the remote network 'Branch-ID-25-Active'. The window has a search icon in the top right. The configuration fields are: Name (Branch-ID-25-Active), ECMP Load Balancing (None), Location (US Central), Bandwidth (2 Mbps), and IPsec Tunnel (IPSec-WAN2-25-Active). There is an unchecked checkbox for 'Enable Secondary WAN' with an associated IPsec Tunnel dropdown. Below these fields are tabs for 'Static Routes', 'BGP', 'QoS', and 'Inbound Access'. The 'Static Routes' tab is active, showing a list of 'BRANCH IP SUBNETS' with one entry: 192.168.125.0/24. At the bottom, there are 'Add' and 'Delete' buttons, and a note: 'Enter the subnets for your remote networks.' The window ends with 'OK' and 'Cancel' buttons.

What is the assigned **Bandwidth**?

What regional cloud **Location** will your remote network connect to?

What **IPSec Tunnel** profile will be applied?

Which of your **Branch IP Subnets** can be reached via this tunnel?

How does this differ from **Branch-ID-X**?

Click **Cancel**.

Step 3: Navigate to **Panorama > Cloud Services > Status > Network Details > Remote Networks.**

NAME ^	SERVICE IP ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET
Branch-ID-25	208.127.86.164	dynamic	192.168.25.0/24
Branch-ID-25-Active	208.127.191.116	dynamic	192.168.125.0/24

Record the **Service IP Address** for your **Branch-ID-X-Active**. This will be used to establish two active IPsec tunnels.

Task 2 – Configure Secondary/Active IPsec Tunnel on NGFW

Step 1: From the **NGFW-Branch-UI** tab, navigate to **Network > Network Profiles > IKE Gateways.**

NAME	PEER ADDRESS	Local Address		Peer ID		Local ID	
		INTERFACE	IP	ID	TYPE	ID	TYPE
<input type="checkbox"/> WAN-1-IKE-GW	208.127.86.164	ethernet1/1	172.16.10.1/24	cloud1-25@utd-sase.local	User FQDN (email address)	wan1-25@utd-sase.local	User FQDN (email address)
<input type="checkbox"/> WAN-2-IKE-GW	208.127.86.164	ethernet1/3	172.16.20.1/24	cloud2-25@utd-sase.local	User FQDN (email address)	wan2-25@utd-sase.local	User FQDN (email address)

Step 2: Click **WAN-2-IKE-GW** to open the **IKE Gateway** window.

IKE Gateway ?

General | Advanced Options

Name: WAN-2-IKE-GW

Version: IKEv1 only mode

Address Type: IPv4 IPv6

Interface: ethernet1/3

Local IP Address: 172.16.20.1/24

Peer IP Address Type: IP FQDN Dynamic

Peer Address: 208.127.86.164

Authentication: Pre-Shared Key Certificate

Pre-shared Key:

Confirm Pre-shared Key:

Local Identification: User FQDN (email address) | wan2-25@utd-sase.local

Peer Identification: User FQDN (email address) | cloud2-25@utd-sase.local

Comment:

Step 3: Update the **Peer Address** with the **Service IP Address** you recorded in the previous task in Panorama.

There is no need to change the **Local Identification** and **Peer Identification** as you did previously.

The screenshot shows the 'IKE Gateway' configuration window with the 'General' tab selected. The 'Peer Address' field is highlighted with a red box and contains the value '208.127.191.116'. Other fields include Name (WAN-2-IKE-GW), Version (IKEv1 only mode), Address Type (IPv4 selected), Interface (ethernet1/3), Local IP Address (172.16.20.1/24), Peer IP Address Type (IP selected), Authentication (Pre-Shared Key selected), Pre-shared Key, Confirm Pre-shared Key, Local Identification (wan2-25@utd-sase.local), and Peer Identification (cloud2-25@utd-sase.local).

Click **OK**.

Step 4: Navigate to **Network > Virtual Routers**.

The screenshot shows the 'PA-VM' dashboard with the 'NETWORK' tab selected. The 'Virtual Routers' section is highlighted in the left sidebar. The main content area displays a table with the following data:

NAME	INTERFACES	CONFIGURATION	RIP	OSPF
default	ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4 tunnel.1 tunnel.2	Static Routes: 6 ECMP status: Disabled		

Step 5: Click **default** to open the **Virtual Router – default** window.

Select the **Static Routes** node.

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

6 items

	NAME	DESTINATION	INTERFACE	Next Hop		ADMIN DISTAN...	ME...	BFD	ROUTE TABLE
				TYPE	VALUE				
<input type="checkbox"/>	default-route	0.0.0.0/0	tunnel.1			default	10	None	unicast
<input type="checkbox"/>	Alt-default-route	0.0.0.0/0	tunnel.2			default	100	None	unicast
<input type="checkbox"/>	Route-WAN-1-Tunnel-Setup	208.127.86.164/32	ethernet1/1	ip-address	172.16.10.254	default	10	None	unicast
<input type="checkbox"/>	Alt-Route-WAN-1-Tunnel-Setup	208.127.86.164/32	ethernet1/3	ip-address	172.16.20.254	default	100	None	unicast
<input type="checkbox"/>	Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/3	ip-address	172.16.20.254	default	10	None	unicast
<input type="checkbox"/>	Alt-Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/1	ip-address	172.16.10.254	default	100	None	unicast

Step 6: Click **Route-WAN-2-Tunnel-Setup**.

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

	NAME	DESTINATION	INTERFACE	Next Hop	
				TYPE	VALUE
<input type="checkbox"/>	default-route	0.0.0.0/0	tunnel.1		
<input type="checkbox"/>	Alt-default-route	0.0.0.0/0	tunnel.2		
<input type="checkbox"/>	Route-WAN-1-Tunnel-Setup	208.127.86.164/32	ethernet1/1	ip-address	172.16.10.254
<input type="checkbox"/>	Alt-Route-WAN-1-Tunnel-Setup	208.127.86.164/32	ethernet1/3	ip-address	172.16.20.254
<input type="checkbox"/>	Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/3	ip-address	172.16.20.254
<input type="checkbox"/>	Alt-Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/1	ip-address	172.16.10.254

Step 7: Update the **Destination** of **10.10.10.11/32** with the **Service IP Address** previously recorded.
Note: Make sure to append **/32** to the IP. This allows the IPsec tunnel to be set up with Prisma Access over ethernet1/3.

Virtual Router - Static Route - IPv4

Name: Route-WAN-2-Tunnel-Setup

Destination: **208.127.191.116/32**

Interface: ethernet1/3

Next Hop: IP Address

172.16.20.254

Admin Distance: 10 - 240

Metric: 10

Route Table: Unicast

BFD Profile: Disable BFD

Path Monitoring

Click **OK**.

Step 8: Click **Alt-Route-WAN-2-Tunnel-Setup**.

Virtual Router - default						
Router Settings						
Static Routes						
Redistribution Profile						
RIP						
OSPF						
OSPFv3						
BGP						
Multicast						
<input type="checkbox"/>	NAME	DESTINATION	INTERFACE	Next Hop		
<input type="checkbox"/>	default-route	0.0.0.0/0	tunnel.1	TYPE	VALUE	
<input type="checkbox"/>	Alt-default-route	0.0.0.0/0	tunnel.2			
<input type="checkbox"/>	Route-WAN-1-Tunnel-Setup	208.127.86.164/32	ethernet1/1	ip-address	172.16.10.254	
<input type="checkbox"/>	Alt-Route-WAN-1-Tunnel-Setup	208.127.86.164/32	ethernet1/3	ip-address	172.16.20.254	
<input type="checkbox"/>	Route-WAN-2-Tunnel-Setup	208.127.191.116/32	ethernet1/3	ip-address	172.16.20.254	
<input type="checkbox"/>	Alt-Route-WAN-2-Tunnel-Setup	10.10.10.11/32	ethernet1/1	ip-address	172.16.10.254	

Step 9: Update the **Destination** of **10.10.10.11/32** with the **Service IP Address** previously recorded.
Note: Make sure to append **/32** to the IP. This is the same IP as in step 7.

Virtual Router - Static Route - IPv4	
Name	Alt-Route-WAN-2-Tunnel-Setup
Destination	208.127.191.116/32
Interface	ethernet1/1
Next Hop	IP Address
	172.16.10.254
Admin Distance	10 - 240
Metric	100
Route Table	Unicast
BFD Profile	Disable BFD
<input type="checkbox"/> Path Monitoring	

Click **OK** to close the **Virtual Router – Static Route – IPv4** window.
 Click **OK** to close the **Virtual Router – default** window.

Step 10: Commit your changes.

Step 11: Navigate to **Network > IPSec Tunnels** to confirm that **WAN-2-IPSec** is up.

	NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface				
				INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERF...	VIRTUAL ROUTER	VIRT... SYST...	S... Z...	ST...
<input type="checkbox"/>	WAN-1-IPSec	● Tunnel Info	Auto Key	ethernet1/1	172.16.10.1/24	208.127.86.164	● IKE Info	tunnel.1	default (Show Routes)	vsys1	lan	
<input type="checkbox"/>	WAN-2-IPSec	● Tunnel Info	Auto Key	ethernet1/3	172.16.20.1/24	208.127.191.116	● IKE Info	tunnel.2	default (Show Routes)	vsys1	lan	

Note: The **Peer Address** for **WAN-1-IPSec** is different than **WAN-2-IPSec**. You have two active tunnels now.

Task 3 – Verify Two Active IPsec Tunnels

Step 1: From **win-mobile**, use the **Command Prompt** to trace the route to your remote network.

Type **ping 192.168.X.100**, where **X** is your assigned **Student-ID**.

```
CA: Command Prompt

C:\Users\root>ping 192.168.25.100

Pinging 192.168.25.100 with 32 bytes of data:
Reply from 192.168.25.100: bytes=32 time=148ms TTL=124
Reply from 192.168.25.100: bytes=32 time=183ms TTL=124
Reply from 192.168.25.100: bytes=32 time=148ms TTL=124
Reply from 192.168.25.100: bytes=32 time=146ms TTL=124

Ping statistics for 192.168.25.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 146ms, Maximum = 183ms, Average = 156ms

C:\Users\root>
```

Step 2: Type **ping 192.168.Y.100**, where **Y** is your assigned **Student-ID+100**.

```
CA: Command Prompt

C:\Users\root>ping 192.168.125.100

Pinging 192.168.125.100 with 32 bytes of data:
Reply from 192.168.125.100: bytes=32 time=160ms TTL=124
Reply from 192.168.125.100: bytes=32 time=160ms TTL=124
Reply from 192.168.125.100: bytes=32 time=158ms TTL=124
Reply from 192.168.125.100: bytes=32 time=157ms TTL=124

Ping statistics for 192.168.125.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 157ms, Maximum = 160ms, Average = 158ms

C:\Users\root>
```

Step 3: Type **tracert 192.168.X.100**, where **X** is your assigned **Student-ID**.

```
CA: Command Prompt

C:\Users\root>tracert 192.168.25.100

Tracing route to 192.168.25.100 over a maximum of 30 hops

  1    28 ms    26 ms    25 ms    172.30.10.1
  2     *        *        *        Request timed out.
  3     *        *        *        Request timed out.
  4   146 ms   144 ms   146 ms   192.168.25.251
  5   185 ms   145 ms   201 ms   192.168.25.100

Trace complete.

C:\Users\root>
```

Notice that the network packets travel through **tunnel.1 (192.168.X.251)**.

Step 4: Type *tracert 192.168.Y.100*, where *Y* is your assigned **Student-ID+100**.

```
Command Prompt
C:\Users\root>tracert 192.168.125.100
Tracing route to 192.168.125.100 over a maximum of 30 hops
  0  27 ms  26 ms  26 ms  172.30.10.1
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  279 ms 265 ms 225 ms 192.168.25.252
  4  156 ms 163 ms 164 ms 192.168.125.100
Trace complete.
C:\Users\root>
```

Notice that the network packets travel through **tunnel.2 (192.168.X.252)**.

Summary:

- ✓ Next Gen Secure remote access to internal applications.
- ✓ Successful tunnel set up does not automatically provide access to internal applications.
- ✓ Authenticate first and authorize only based on who the user is, what group the user belongs to, the state of the device from where the user is requesting access, the application being accessed, and the ports and services being used

End of Activity 6

Activity 7 – Enterprise DLP with Prisma Access

In this activity, you will:

- Review Enterprise DLP on Panorama
- Attempt to upload sensitive content

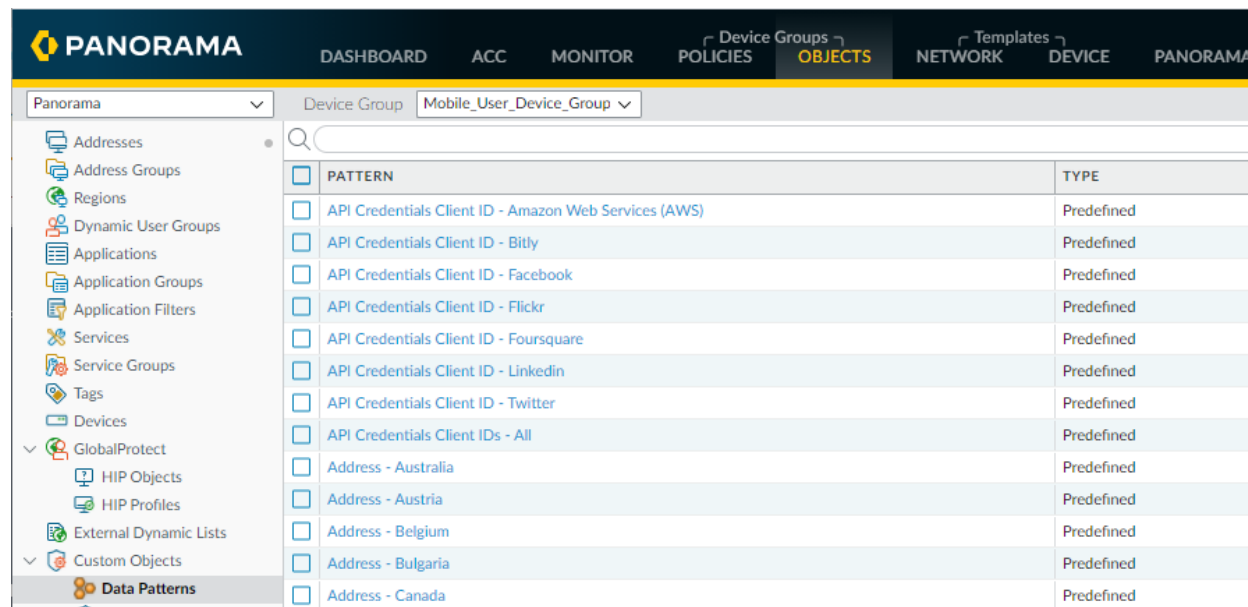
Data loss prevention (DLP) is a set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing. DLP on Prisma Access enables you to use Prisma Access to enforce your organization's data security standards and prevent the loss of sensitive data across mobile users and remote networks.

DLP on Prisma Access, also known as Enterprise DLP, is a cloud-based service that uses supervised machine learning algorithms to sort sensitive documents into Financial, Legal, Healthcare, and other categories for document classification to guard against exposures, data loss and data exfiltration. These patterns can identify the sensitive information in your cloud apps and protect them from exposure.

Enterprise DLP offers hundreds of data patterns and many predefined data filtering profiles, and it is designed to automatically make new patterns and profiles available to you for use in Data Filtering policies, as soon as they are added to the cloud service.

Task 1 – Review Enterprise DLP on Panorama

Step 1: From the Panorama-UI browser tab, navigate to **Objects > Custom Objects > Data Patterns**.



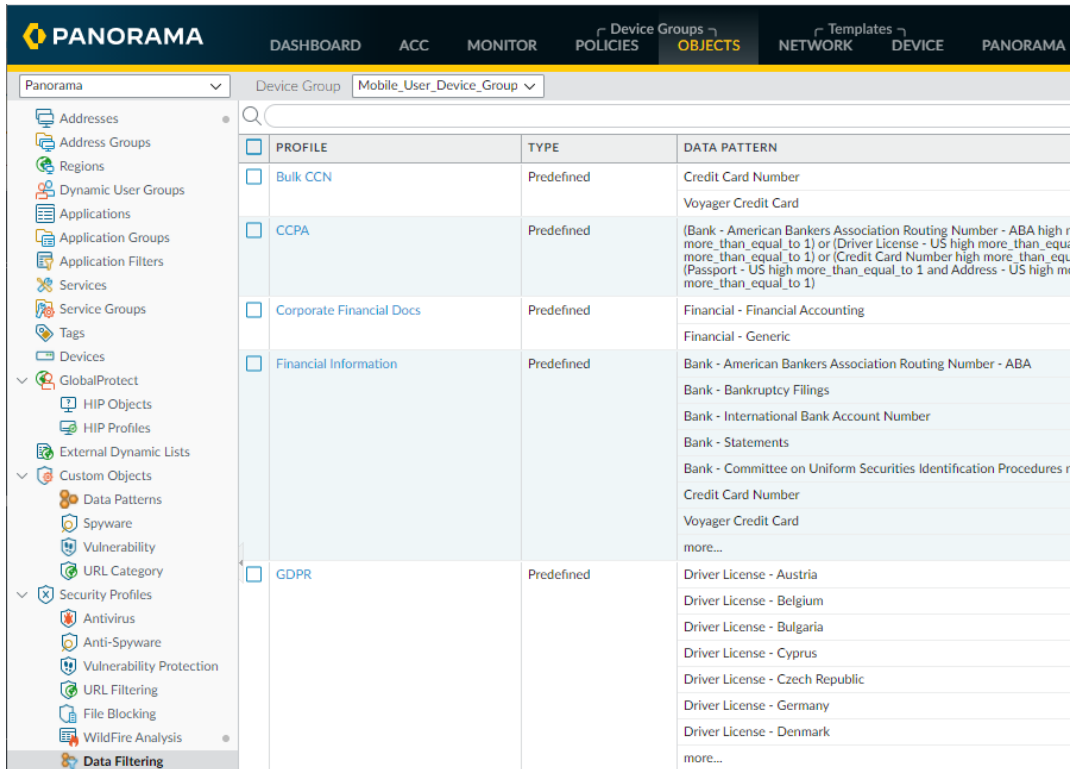
The screenshot shows the Panorama web interface. The top navigation bar includes 'PANORAMA', 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS' (selected), 'NETWORK', 'DEVICE', and 'PANORAMA'. Below the navigation bar, there is a search bar and a table of data patterns. The table has columns for 'PATTERN' and 'TYPE'. The 'PATTERN' column lists various predefined patterns, and the 'TYPE' column indicates they are all 'Predefined'.

PATTERN	TYPE
<input type="checkbox"/> API Credentials Client ID - Amazon Web Services (AWS)	Predefined
<input type="checkbox"/> API Credentials Client ID - Bitly	Predefined
<input type="checkbox"/> API Credentials Client ID - Facebook	Predefined
<input type="checkbox"/> API Credentials Client ID - Flickr	Predefined
<input type="checkbox"/> API Credentials Client ID - Foursquare	Predefined
<input type="checkbox"/> API Credentials Client ID - LinkedIn	Predefined
<input type="checkbox"/> API Credentials Client ID - Twitter	Predefined
<input type="checkbox"/> API Credentials Client IDs - All	Predefined
<input type="checkbox"/> Address - Australia	Predefined
<input type="checkbox"/> Address - Austria	Predefined
<input type="checkbox"/> Address - Belgium	Predefined
<input type="checkbox"/> Address - Bulgaria	Predefined
<input type="checkbox"/> Address - Canada	Predefined

Predefined data patterns and built-in settings make it easy for you to protect files that contain certain file properties (such as a document title or author), credit card numbers, regulated information from different countries (such as driver's license numbers), and third-party DLP labels. To improve detection rates for the sensitive data in your organization supplement the predefined data patterns, you can define custom data patterns that are specific to your content inspection and data protection requirements. In a custom data pattern, you can also define regular expressions and file properties to look for metadata or attributes

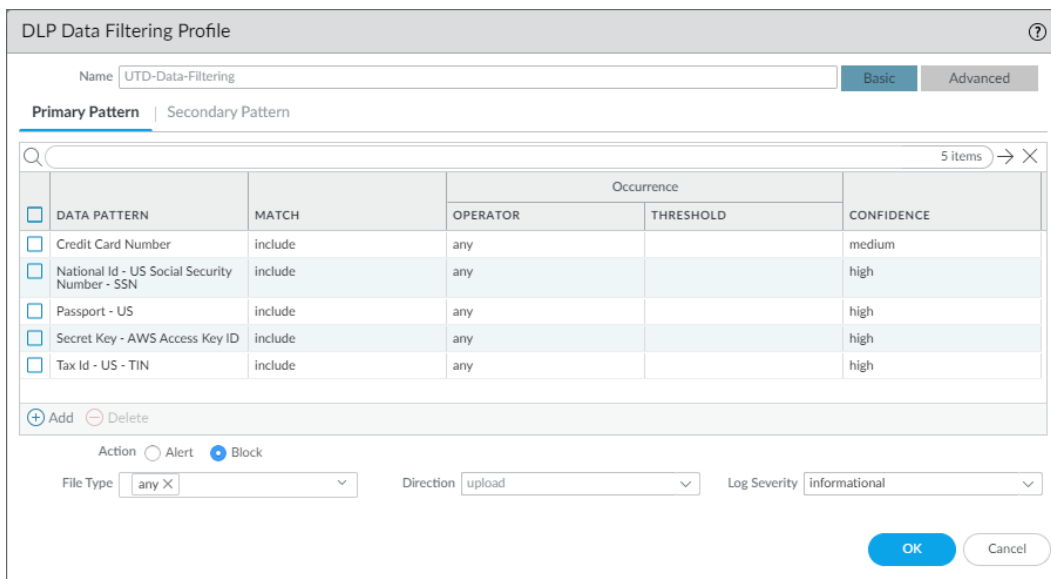
in the file's custom or extended properties and use it in a data filtering profile.

Step 2: Navigate to Objects > Security Profiles > Data Filtering.



Data filtering profiles are a collection of data patterns that are grouped together to scan for a specific object or type of content. To perform content analysis, the predefined data profiles have data patterns that include industry-standard data identifiers, keywords, and built-in logic in the form of machine learning, regular expressions, and checksums for legal and financial data patterns. When you use the data filtering profile in a Data Filtering policy rule, the firewall can inspect the content for a match and take action.

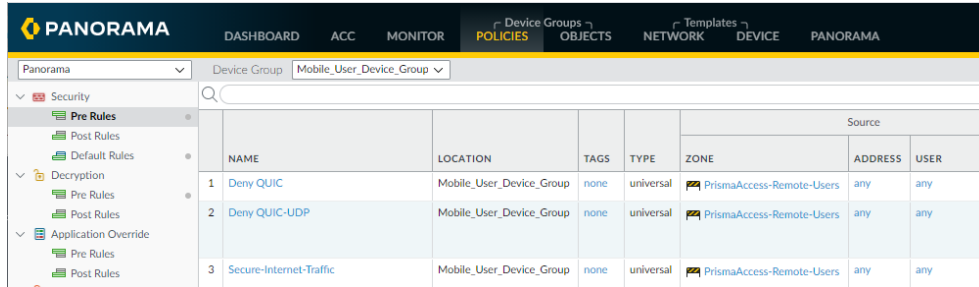
Step 3: Scroll down and click on UTD-Data-Filtering to open the profile.



Using the predefined **Data Patterns**, a custom **Data Filtering** profile has been created. Note that the **Action** is set to **Block**.

Click **Cancel**.

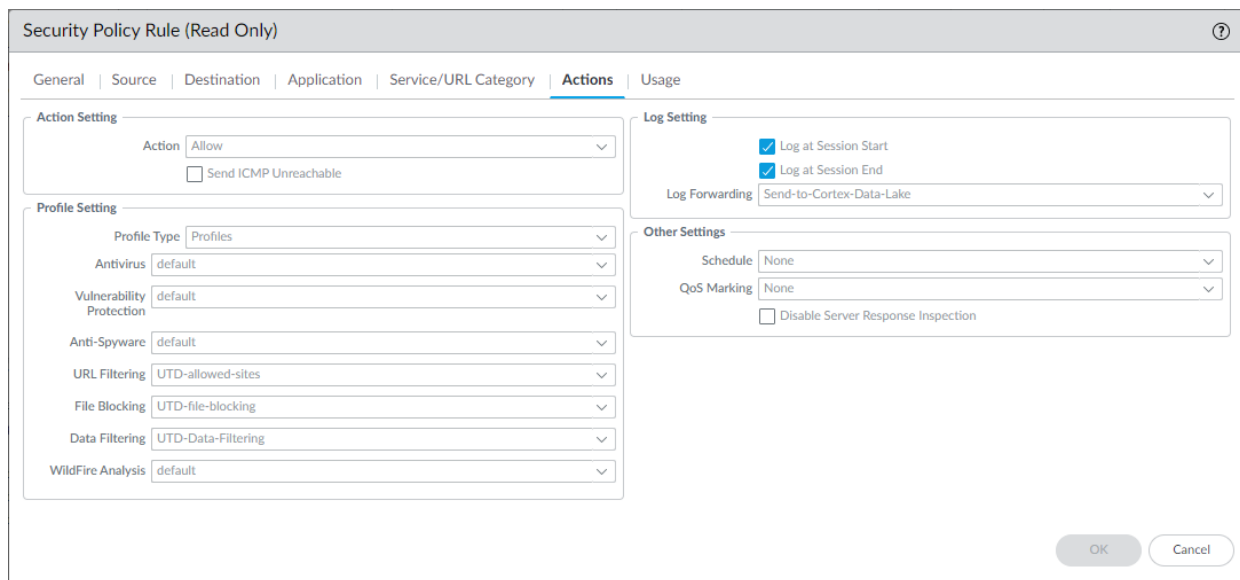
Step 4: Navigate to **Policies > Security > Pre Rules**. The **Device Group** should be set to **Mobile_User_Device_Group**.



	NAME	LOCATION	TAGS	TYPE	ZONE	ADDRESS	USER
1	Deny QUIC	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any
2	Deny QUIC-UDP	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any
3	Secure-Internet-Traffic	Mobile_User_Device_Group	none	universal	PrismaAccess-Remote-Users	any	any

Step 5: Click on **Secure-Internet-Traffic** to open the **Security Policy** profile.

Click on **Actions**.



Security Policy Rule (Read Only)

General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action: Allow

Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: default

Anti-Spyware: default

URL Filtering: UTD-allowed-sites

File Blocking: UTD-file-blocking

Data Filtering: UTD-Data-Filtering

WildFire Analysis: default

Log Setting

Log at Session Start

Log at Session End

Log Forwarding: Send-to-Cortex-Data-Lake

Other Settings

Schedule: None

QoS Marking: None

Disable Server Response Inspection

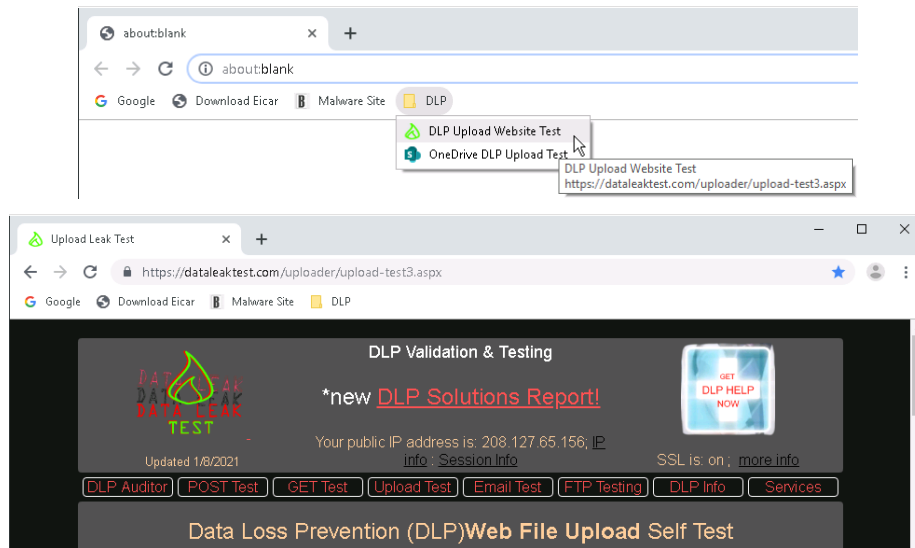
OK Cancel

Note that the **Data Filtering** profile is set to **UTD-Data-Filtering**. Also notice that a **File Blocking** profile is set. Not only can Prisma Access inspect data in motion but can also block undesired file types.

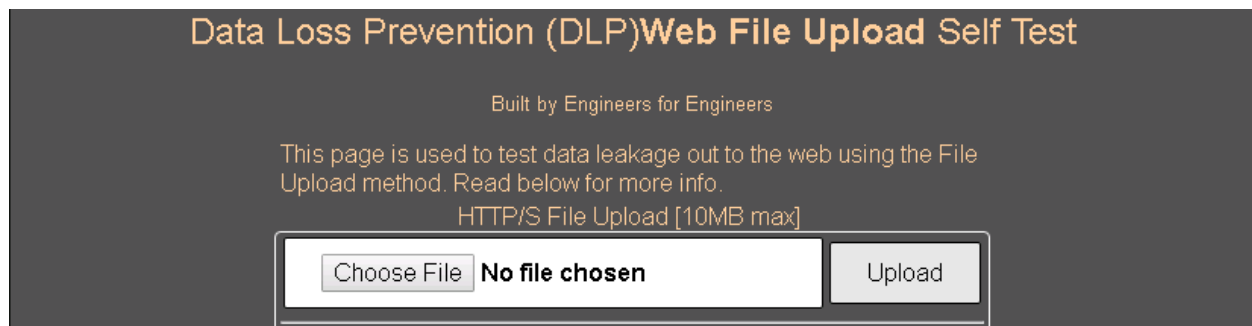
Click **Cancel**.

Task 2 – Attempt Upload of Sensitive Content from Mobile User

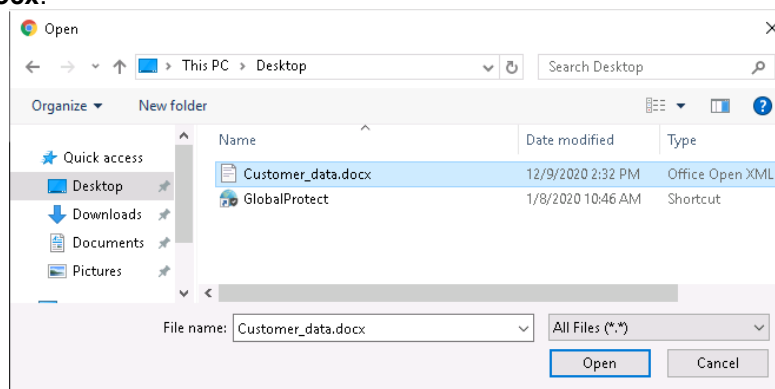
Step 1: From the win-mobile VM, use the **Chrome** browser bookmarks to go to **DLP > DLP Upload Website Test**.



Step 2: Click the **Choose File** button to review the configuration for that remote network.



Step 3: From the **File Explorer** pop-up, click **Desktop** on the left-hand column and select **Customer_data.docx**.

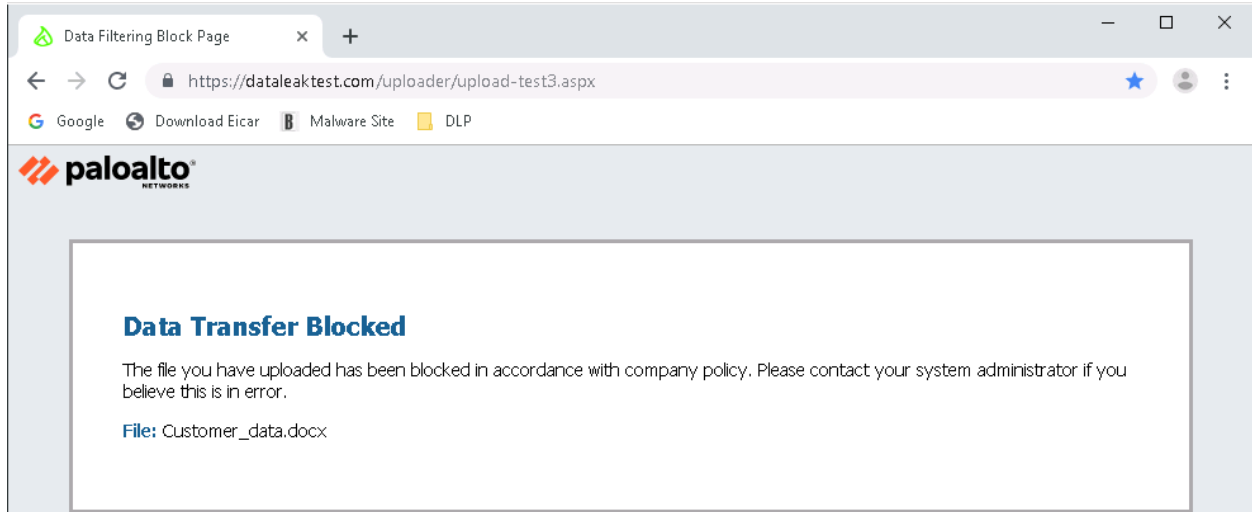


Click **Open**.

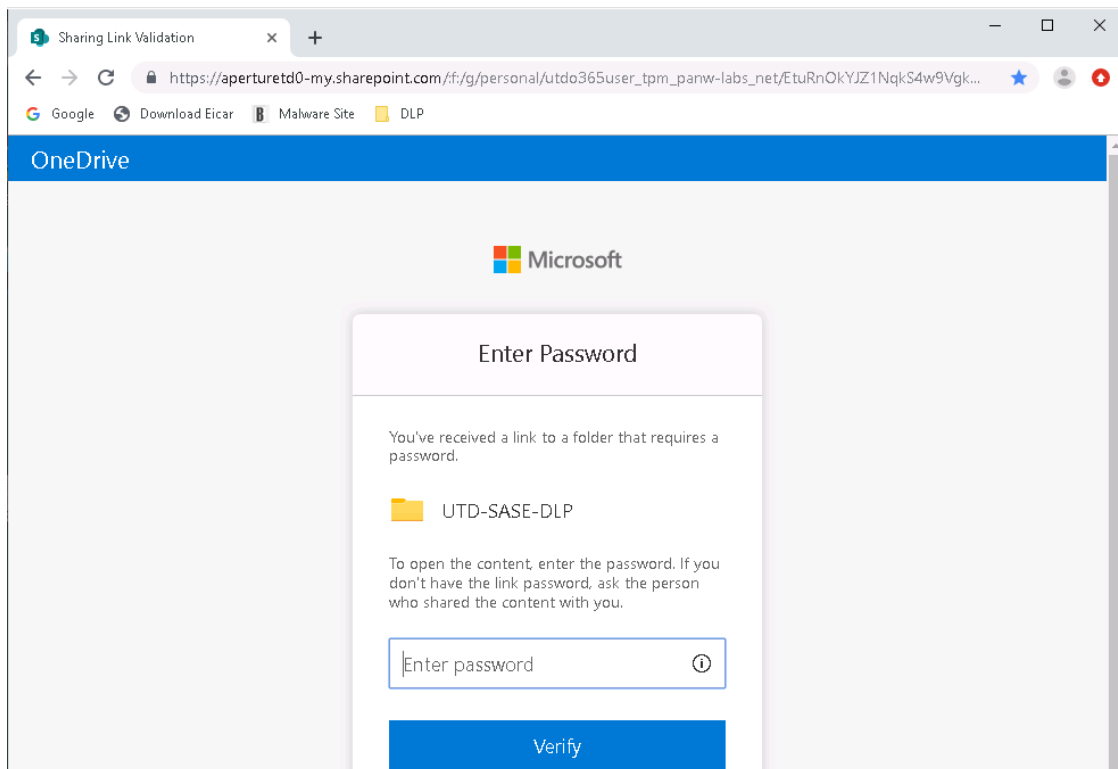
Step 4: Click the **Upload** button.



Step 5: The upload of the file containing sensitive data is blocked.

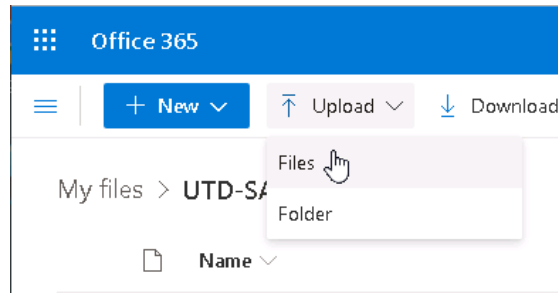


Step 6: Use the **Chrome** browser bookmark to go to **DLP > OneDrive DLP Upload Test**.

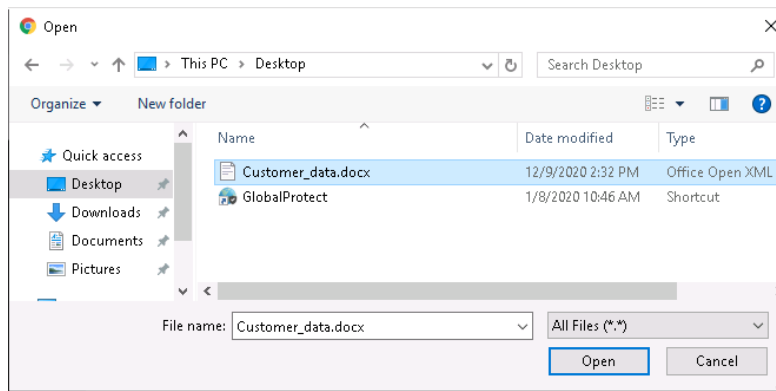


In the **Enter password** box, type **utd1234** and click **Verify**.

Step 7: Click **Upload > Files**.

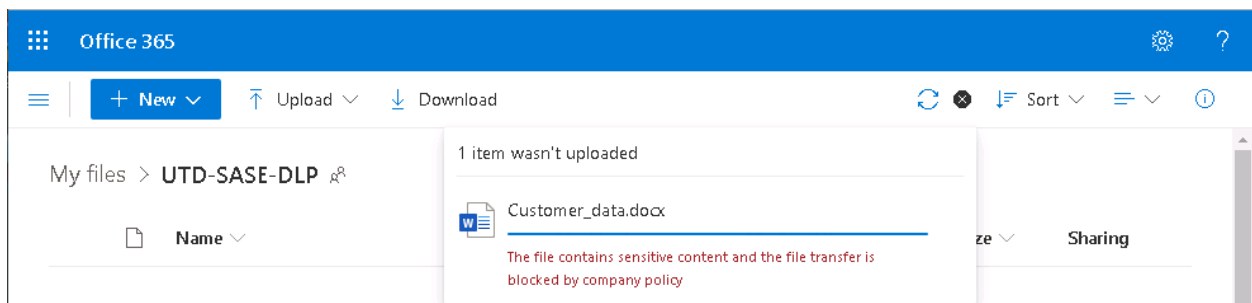


Step 8: From the **File Explorer** pop-up, click **Desktop** on the left-hand column and select **Customer_data.docx**.



Click **Open**.

Step 9: The file containing sensitive is blocked.



Task 3 – Review Logs in Panorama

Step 1: From the Panorama-UI browser tab, navigate to **Monitor > Logs > Data Filtering**.

GENERATE TIME	CATEGORY	FILE NAME	FILE URL	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	DESTINATION ADDRESS	TO PORT	APPLICATION	ACTION
01/11 15:45:19	UTD-allowed-sites	Customer_data.docx		11995024	trust	untrust	172.30.123.27	employee25	13.107.136.9	443	sharepoint-online-uploading	block
01/11 15:44:53	UTD-allowed-sites	Customer_data.docx		11995024	trust	untrust	172.30.123.27	employee25	50.62.160.34	443	web-browsing	block

As the log entries are not real-time, it may take several minutes for your file upload attempts to show up.

You may use a filter of **(user.src eq employeeX)** where **X** is your assigned Student-ID.

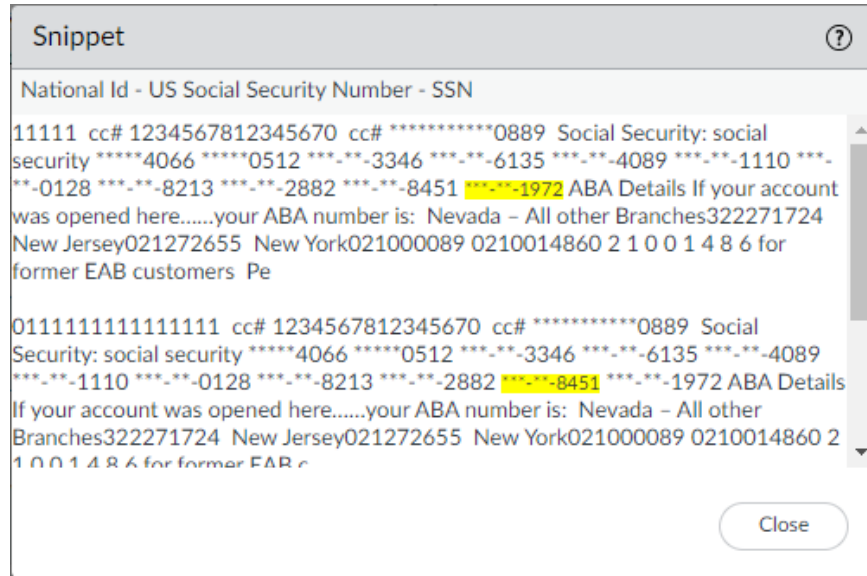
Step 2: Click on the magnifying glass to open the **Detailed Log View**.

PCAP	RECEIVE TIME	TYPE	APPLICA...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATE...	URL CATE... LIST	VERDI...	URL	FILE NAME
	2021/01/11 15:45:54	end	sharepoint-online-uploading	allow	Secure-Intern...Traffic	97181...	22...		UTD-allowed-sites				
	2021/01/11 15:45:35	start	web-browsing	allow	Secure-Intern...Traffic	97181...	7512		any				

Click the **DLP** tab.

PATTERN	CONFIDENCE	TOTAL OCCURRENCES	UNIQUE OCCURRENCES	SNIPPETS
Credit Card Number	Low	1	1	Show Snippet
National Id - US Social Security Number - SSN	Low	15	15	Show Snippet
	High	11	11	
Passport - US	Low	6	6	Show Snippet
	High	4	4	
Secret Key - AWS Access Key ID	Low	2	2	Show Snippet
	High	2	2	
Tax Id - US - TIN	Low	15	15	Show Snippet

Step 3: Click **Show Snippet** on any entry that has a **Medium** or **High Confidence**.



Prisma Access extracts a snippet of the sensitive data that caused the alert or block notification. A snippets enables forensics by allowing you to verify why an uploaded file generated an alert notification or was blocked. By default, Prisma Access uses data masking to partially mask the snippets to prevent the sensitive data from being exposed. You can configure Prisma Access to completely mask the sensitive information, unmask the snippets, or disable snippet extraction and viewing.

Click **Close**.

Task 4 – [Optional] Attempt Upload of Sensitive Content from Remote Network

Step 1: You may use **win-subnet1** and repeat the steps of **Task 2** to see consistent security no matter where you users are located.

End of Activity 7

Activity 8 – Prisma SD-WAN: Actionable Analytics - Identify & Measure

In this activity, you will:

- Observe the way the Prisma SD-WAN identifies, measures, and prioritizes application traffic

Prisma SD-WAN was formerly known as CloudGenix SD-WAN. This lab guide will have references to both names.

It is not enough for network administrators to set it and forget it. They need visibility to verify that their intended policy actually took effect, as well as be able to profile the application from the perspective of Layer 7 reachability and verify its performance.

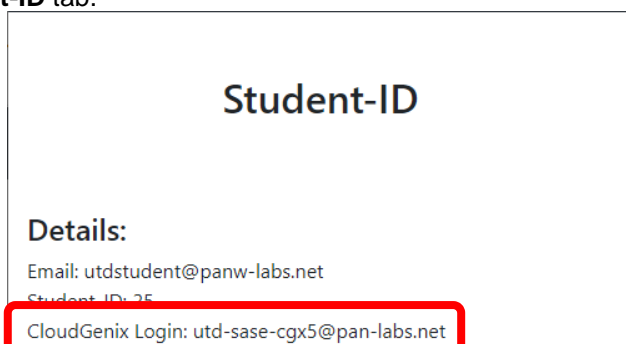
Typically, all other solutions require a third party NetFlow collector to gain these types of insights, which is yet another system to manage and maintain just to gain visibility into the applications on your network. Even if such a system was properly configured to collect and analyze the data, because the information is being collected from a packet-based architecture, a book-ended solution is required. Otherwise, key performance indicators will be missing.

With Prisma SD-WAN, you gain immediate visibility into the changes made to the policy and application performance from a variety of perspectives. All of this without having to set up a third party NetFlow collector or some add-on to the base platform.

Let's explore the analytics captured and displayed for the top applications.

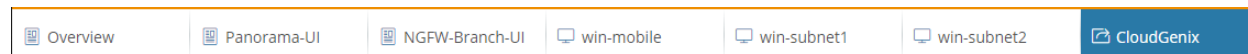
Task 1 – Log in to CloudGenix Portal

Step 1: Click the **Student-ID** tab.



Retrieve your assigned **CloudGenix Login**.

Step 2: Click the **CloudGenix** tab.



Step 3: Enter your assigned login.



Click **Login**.

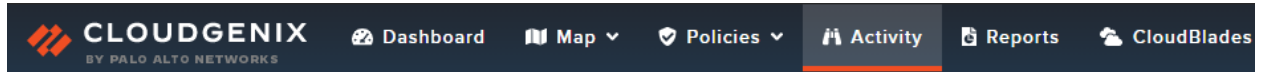
Step 4: Click into the **Password** field. Select your assigned login.



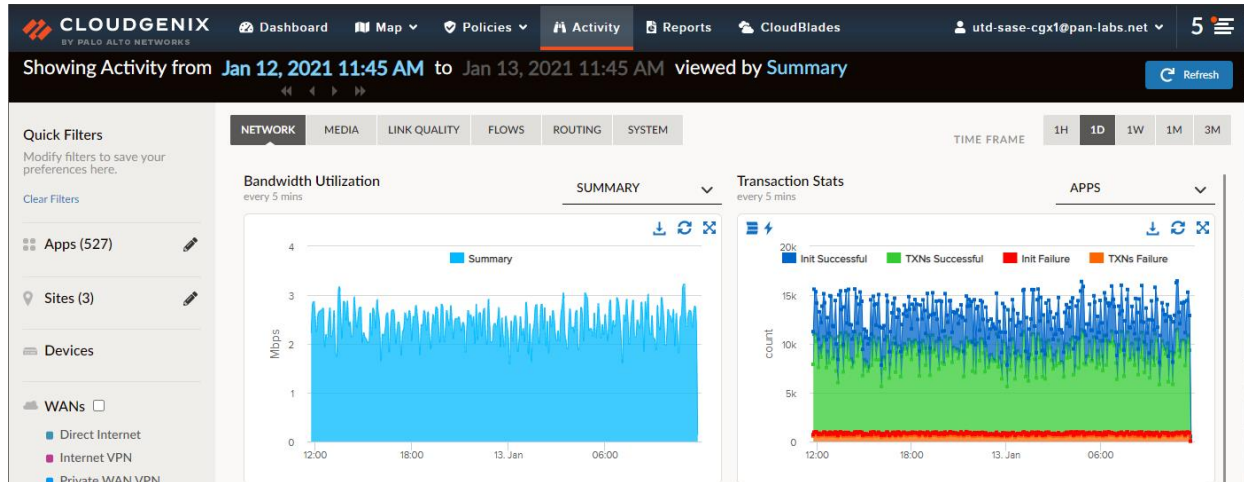
Click **Login**.

Task 2 – Network Analytics

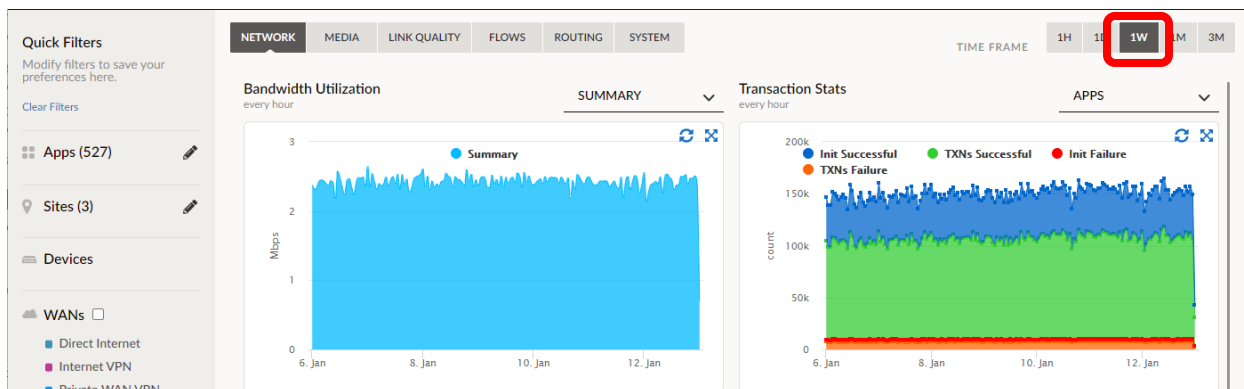
Step 1: Click the **Activity** tab. Then click **Network** if not already selected.



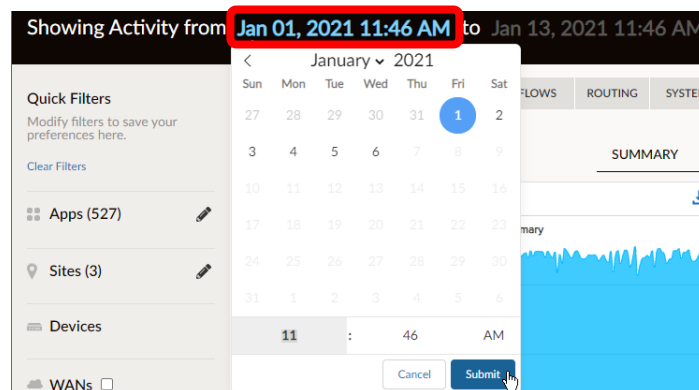
Network analytics will be shown. The default **Time Frame** is last day (1D).



Step 2: Click **1W** from **Time Frame**, the graphs will update for the selected period of time.



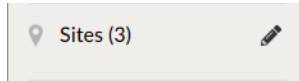
Click the date (in blue) and pick another day. Click **Submit**.



Up to 3 months of granular data is available.



Click **1D** from **Time Frame** to set the graphs back to the default view.


Step 3: In the left-hand column, under **Quick Filters**, click the pencil icon  for **Sites**.




Select **Branch 1**.

Select a Site - (3 Shown)

SEARCH
Search by Name, Address  ADMIN STATE (MODE)
All 

VIEWING
All 

Branch 1 selected - Clear  ONLY SHOW SELECTED

SITE	ADDRESS	ADMIN STATE (MODE)
<input checked="" type="radio"/> Branch 1	1600 Pennsylvania Ave NW 1 Washington, DC 20500	Control
<input type="radio"/> Branch 2	11 North 4th Street St. Louis, MO 63102	Control
<input type="radio"/> Branch 3	Alcatraz Main Cell House Pier 39 Concourse San Francisco, CA 94133	Control

Click **Submit**.

Click **Not yet** on the window prompting you to update charts.



Update charts to show data from the selected filters.


APPS	SITES
N/A	1
DEVICES	WANS
N/A	N/A
PATHS	
N/A	


Step 4: Again, under **Quick Filters**, click the pencil icon  for **Apps**.

In the drop-down box for **VIEWING > Top Apps by...**, select **Traffic Volume**.

Select Applications - (527 Shown)


SEARCH
Search by Name  CATEGORY
All 

VIEWING
All Apps 

TYPE
All 

ONLY SHOW SELECTED

CATEGORY	TYPE
saas	System
saas	System

Top Apps by...
Traffic Volume 
Initiation Failure
Transaction Failure
New TCP flow

Click **Select All**.

Select Applications - (10 Shown)

SEARCH
Search by Name CATEGORY All

VIEWING TOP APPS BY...
Traffic Volume TYPE All

10 selected - Clear **Select All** ONLY SHOW SELECTED

NAME	CATEGORY	TYPE
<input checked="" type="checkbox"/> Dropbox	saas	System
<input checked="" type="checkbox"/> WebPoS	enterprise	Custom
<input checked="" type="checkbox"/> Marketo	saas	System
<input checked="" type="checkbox"/> LinkedIn	saas	System

Apps Definition Version: 000003.000034

Cancel Submit

Verify **WebPoS** is selected.

Click **Submit**.

Click **Update**

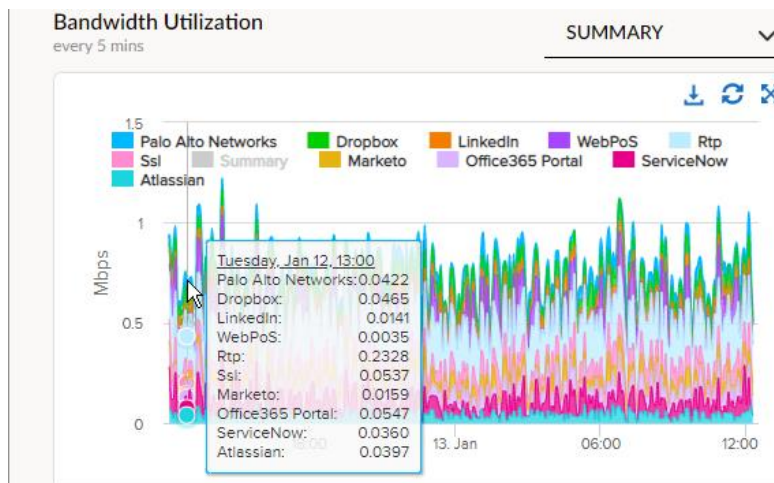
Update charts to show data from the selected filters.

APPS	SITES
10	1
DEVICES	WANS
N/A	N/A
PATHS	
N/A	

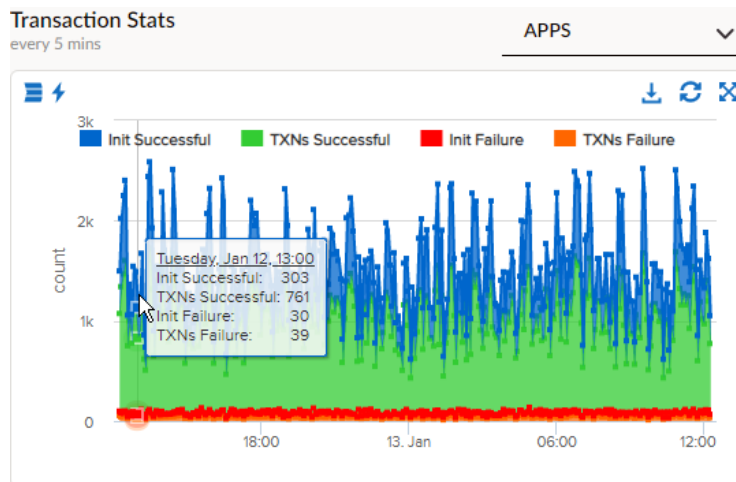
Not yet **Update**

Step 5: Both the **Bandwidth Utilization** and **Transaction Stats** graphs have updated with new information.

The **Bandwidth Utilization** graph details the how much bandwidth each of the top 10 applications are using over the course of the past 1 day, measured at 5-minute increments.



Transaction Stats provides full accounting for TCP applications.



Init Successful - Quantity of successful TCP 3-way handshakes.

TXNs Successful - The number of successful TCP transactions after a 3-way handshake is established.

Init Failure - Quantity of failed TCP 3-way handshakes.

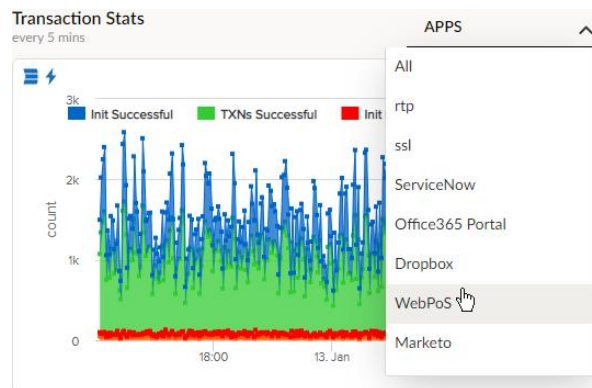
TXNs Failure - The number of failed TCP transactions after a 3-way handshake is established.

Init Failures can be indicative of a few issues:

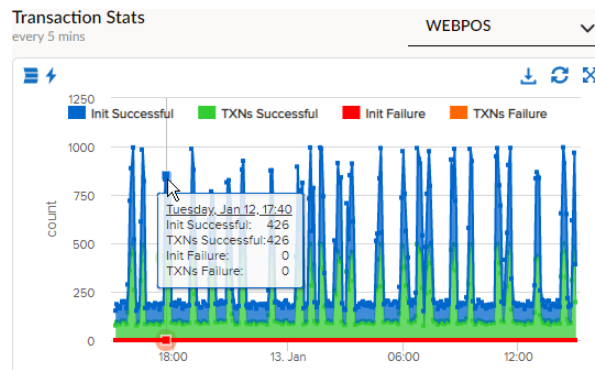
- Application Issues - The application could be down or experiencing intermittent issues
- Firewall Issues - Incorrect firewall rules may be blocking traffic
- Network issues beyond the reach of SD-WAN (ie in the data center)

Transaction (TXN) Failures usually represent loss somewhere in the network path, inside or outside of the direct control of the app-fabric.

Step 6: Click **APPS** on the **Transaction Stats** window and select **WebPoS**.

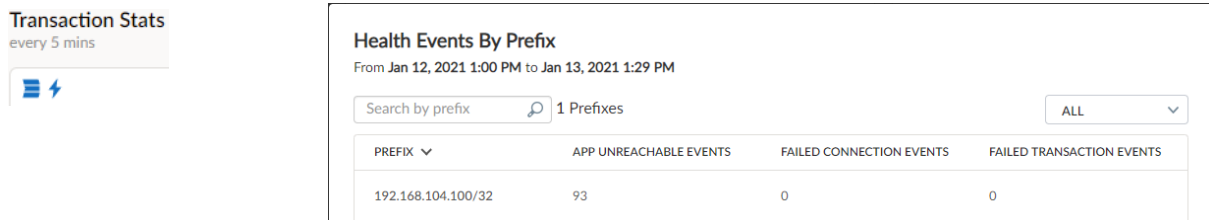


The Prisma SD-WAN also captures and aggregates transaction stats on a per app, per server basis.



Note: WebPoS is a user-defined custom L7 application. We'll explore what this means in the next activity.

Click the blue lightning bolt ⚡ in the top-left of the **Transaction Stats** window. A new page is displayed with accounting of transaction statistics for WebPoS on a per prefix (server) basis.

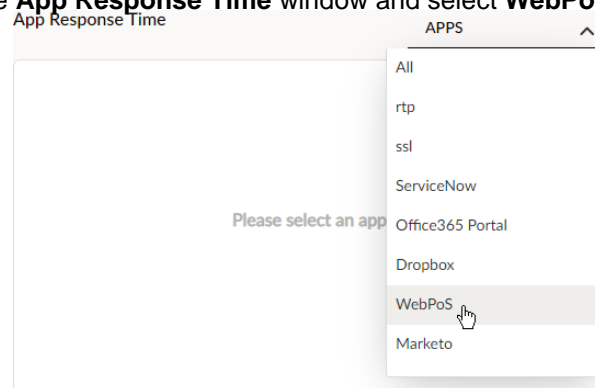


Application health event definitions:

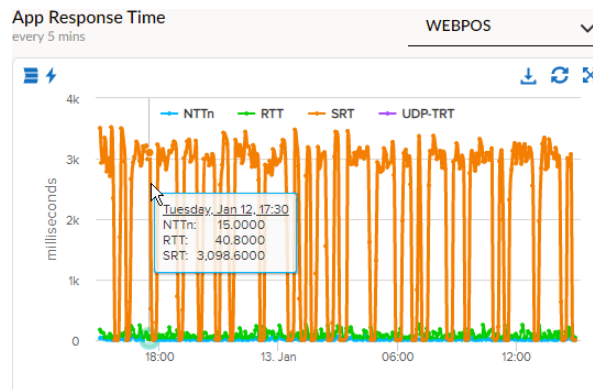
- **App Unreachable Events** - The number of periods (10 second interval) the given prefix is unreachable
- **Failed Connection Events** - The number of failed flows (3-Way Handshake) in the given time period
- **Failed Transaction Events** - The number of failed transactions (Retransmission required) in the given time period

Click anywhere outside the window to return to the **Network Analytics** page.

Step 7: Click **APPS** on the **App Response Time** window and select **WebPoS**.



The **App Response Time** details for **WebPoS** will be displayed.



The Prisma SD-WAN measures application performance as close as possible to the user, which is at the branch. In fact, many CloudGenix customers refer to this graph as their **Time to Innocence** graph. Application Performance is measured across several key metrics including:

- **Server Response Time (SRT)** - SRT represents the amount of time the server is waiting to fetch data before putting it on the wire.
- **Round Trip Time (RTT)** - RTT represents the round trip time of the TCP traffic while on the wire.
- **Network Transmission Time, Normalized (NTTn)** - Time consumed by the network for processing application requests normalized to an iMIX packet size.
- **UDP Transaction Round Trip (UDP-TRT)** - If DNS is the selected application, this metric is used to gauge the DNS response time.

Real World Applicability

CloudGenix “Time To Innocence”



A global manufacturing organization had recently deployed Office 365 to their global workforce using their legacy SD-WAN solution and the internet as a transport. Very quickly the end users began to experience performance issues with many applications. This set off a series of troubleshooting sessions to diagnose the issue. At the conclusion Microsoft had determined that the network was to blame. This put the network team in a position where they were required to prove to IT leadership that the network was not the issue.

Unfortunately, their legacy SD-WAN solution required bookends (a device on each end of the connection) in order to provide visibility into the performance of the network - something not practical nor possible with most SaaS solutions.

This gap in performance data forced the network team to evaluate solutions capable of monitoring and measuring application traffic in more granular detail, without the need to deploy an appliance in the Microsoft Office 365 cloud.

They brought in Prisma SD-WAN as one of the potential solutions to evaluate. After understanding how the CloudGenix system works they quickly deployed the solution at a branch where many users were complaining.

After a very short amount of time monitoring the picture became clear. The RTT (Round Trip Time) values between the branch and the Office 365 front end were within acceptable values. However, there were periods of time where the SRT (Server Response Time) was spiking to several thousand milliseconds for long periods of time.

With this new information the network team went back to Microsoft and helped them identify when and where issues were occurring. This set about a rapid replacement of their legacy SD-WAN with the Prisma SD-WAN.

Next, we'll explore how Prisma SD-WAN identifies and measures real-time media applications.

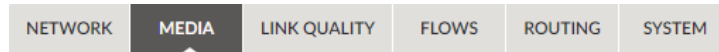
Task 3 – Media Analytics

Due to the sensitive nature of real-time media applications the Prisma SD-WAN measures and treats them separately out of the box. For example, the system measures the quality of each voice and video call in high detail - no synthetic probes are used.

Let's explore this by reviewing actual RTP audio traffic at Branch 1.

Step 1: Under **Quick Filters**, click **Clear Filters**.

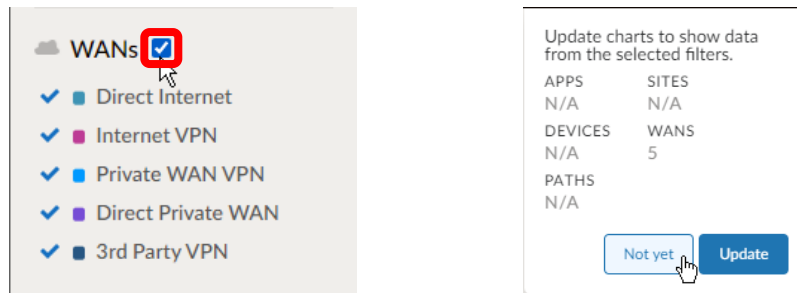
Step 2: Click **Media** to display the media analytics.



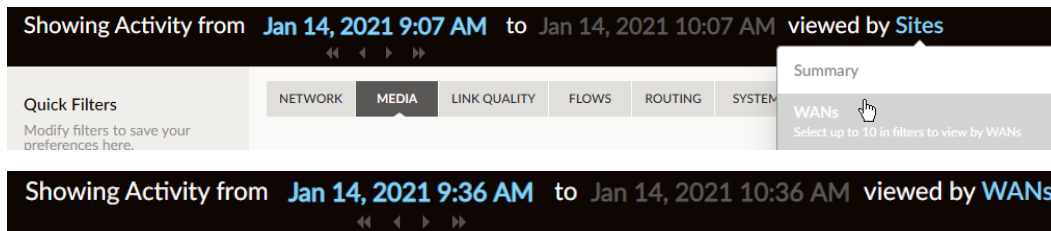
Step 3: Select **1H** from the **Time Frame** selector.



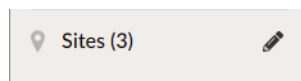
Step 4: From **Quick Filters**, click the checkbox for **WANs**. Select **Not yet** when prompted to update charts.



Step 5: From the top of the page, change **viewed by Sites** to **viewed by WANs**.



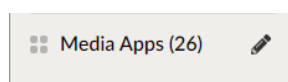
Step 6: Under **Quick Filters**, click the pencil icon for **Sites**.



Select **Branch 1** and then click **Submit**.

Click **Not yet** when prompted to update charts.

Step 7: Under **Quick Filters**, click the pencil icon for **Media Apps**.



Under **Search**, type *rtp* and then select *rtp*.

Select Media Applications - (1 Shown)

SEARCH CATEGORY All

VIEWING All Media Apps TYPE All

"rtp" selected - Clear ONLY SHOW SELECTED

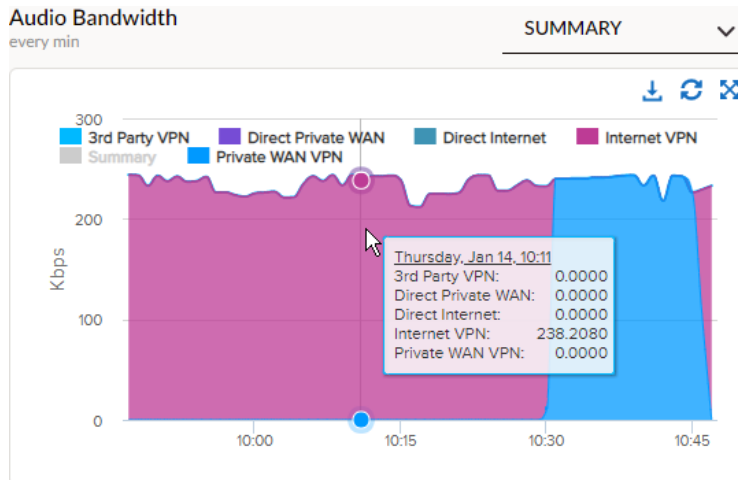
NAME	CATEGORY	TYPE
<input checked="" type="radio"/> rtp	streaming	System

Click **Submit**.

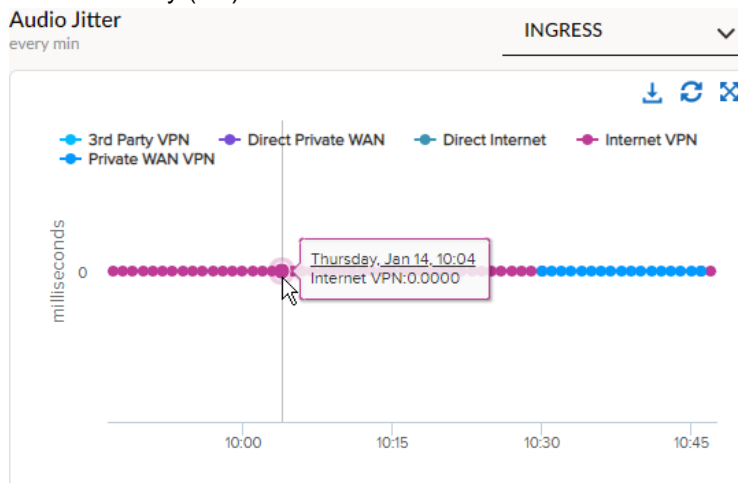
Click **Update** when prompted to update charts.

Step 8: Media analytics for the RTP audio sessions are now displayed.

Audio Bandwidth - The amount of bandwidth that the RTP audio streams are consuming.

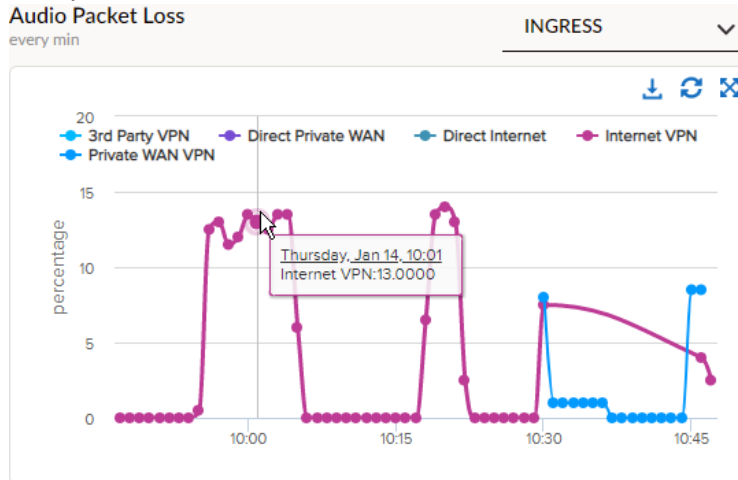


Audio Jitter - The variance in delay (ms) of the RTP audio traffic.



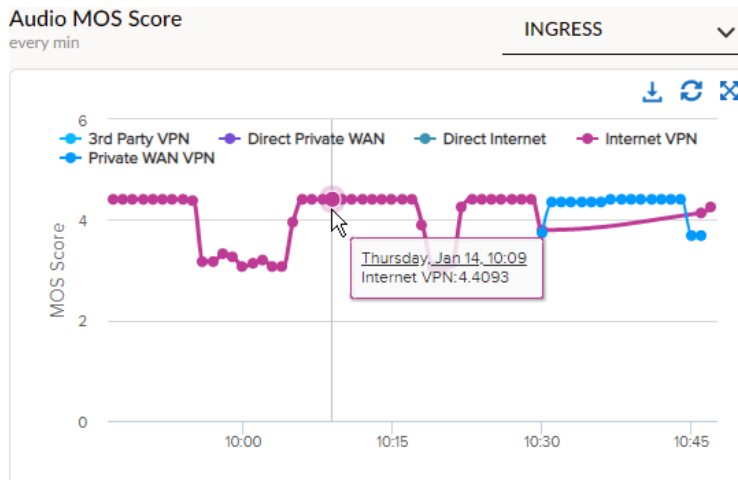
Note there is no jitter in this environment.

Audio Packet Loss - The packet loss % of the RTP audio traffic.



Note that extreme network conditions have been introduced into this environment to cause the Prisma SD-WAN to react to quality issues.

Audio MOS Score - The Mean Opinion Score of the audio traffic calculated using industry standard metrics.



Note that the above metrics default to displaying the **Ingress** metrics, which are measured on the traffic coming into the branch site from the WAN. Egress traffic is measured from the branch LAN going to the WAN. The view can easily be changed between **Ingress** and **Egress** on each individual graph.



Real World Applicability

Two companies merged and were required to connect the network under a new uniform solution. One company used MPLS exclusively along with centralized applications in a colocation facility. The other company used only internet VPN for WAN transport and relied exclusively on Microsoft Azure for IaaS. Needless to say, finding a new network solution to meet the requirements of both companies was challenging and a versatile solution was desired.

In the meantime, the Columbus, OH branch repeatedly complained about voice quality issues running over the internet. They went as far as adding a dedicated internet connection for voice but, this didn't provide much relief. As such, once the Prisma SD-WAN rollout began this was one of the first sites to be deployed.

However, a few days after deploying the voice issues still persisted. Had Prisma SD-WAN failed to correct the issue?

The network administrator dug into the details of the situation and found that ingress (traffic coming into the site from the internet) VoIP traffic for the UCaaS solution was clean - no signs of issues. He then looked at egress (traffic coming into the LAN) and found many spikes of packet loss of up to 18.5%.

Next, he reviewed the interface statistics on the Prisma SD-WAN ION hardware and found there were hundreds of thousands of errors in the past 24 hours. After some additional troubleshooting on the switch it was determined that the cable running between the switch and the ION was bad.

To summarize, without proper data the administrator spent an entire year operating under the assumption that VoIP issues were caused by a WAN transport issue. However, it was as simple as a bad cable that was used to connect the switch to the WAN. With proper visibility the administrator was able to identify the issue within just a few minutes.


Next, we'll explore how the Prisma SD-WAN measures link quality.

Task 4 – Link Quality

Step 1: Under **Quick Filters**, click **Clear Filters**.

Step 2: Click **Link Quality** to display the media analytics.



Step 3: Under **Quick Filters**, click the pencil icon  for **Sites**.

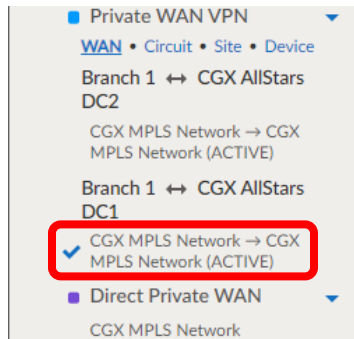
Select **Branch 1** and click **Submit**.

Click **Not yet** when prompted to update charts.

Step 4: Under **Quick Filters**, click **Active**.

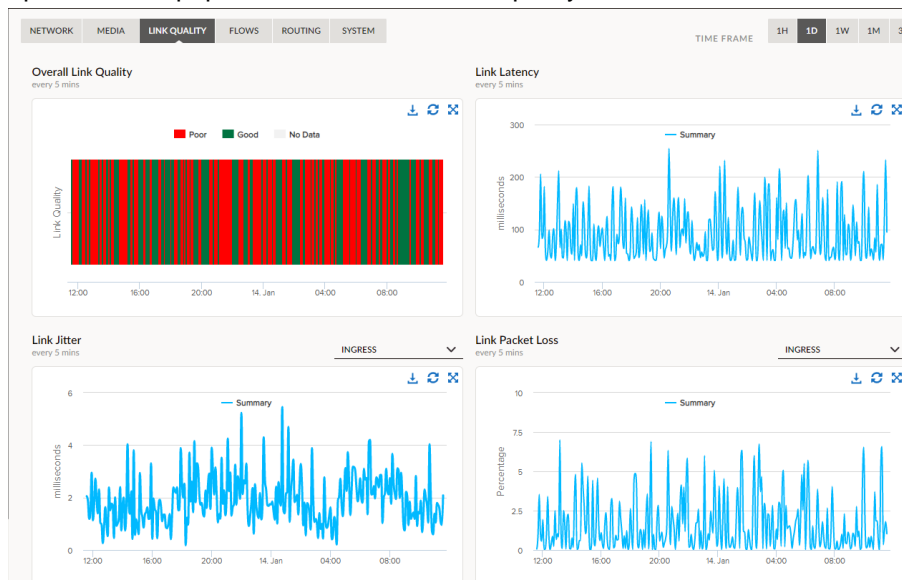


Select the VPN between **Branch 1** and **CGX AllStars DC1**.



Click **Update** when prompted to update charts.

Step 5: The graphs are now populated with detailed link quality metrics.



- **Overall Link Quality** - A simple chart representing whether the link is generally good enough (or not) to support a real-time media session. By default, a good link is defined as have less than 150ms of latency, 50ms of jitter, and 3% packet loss. This can be tuned on a per app / per connection basis.
- **Link Latency** - The round-trip latency between Branch 1 and DC 1.
- **Link Jitter** - The uni-directional jitter between Branch 1 and DC 1.
- **Link Packet Loss** - The uni-directional packet loss between Branch 1 and DC 1.
- **Link MoS** - A synthetic calculation of the Mean Opinion Score based upon the link metrics.

Real World Applicability

A global engineering firm paid premium prices for their high-quality, high-bandwidth MPLS connections. However, many sites still experienced random issues causing user performance issues with the traffic running over MPLS.

As is the norm with most Prisma SD-WAN proof-of-value trials, the solution was deployed at the site with the most user complaints. Once deployed the network administrators had instant visibility into the health of all transports and applications.

They reviewed the link quality of the MPLS connection and found immediate issues. The packet loss was spiking well above acceptable thresholds, up to 6% during business hours.

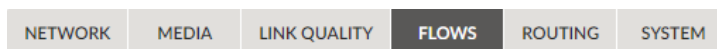
With this new information the network team was able to go back to carrier with precise information detailing the time and severity of the issues, leading to further investigation by the carrier, and ultimate resolution. The engineering firm proceeded to roll out the app-fabric at over 100 global locations on several continents.


Task 5 – Flow Browser

The Prisma SD-WAN keeps a record of every application session that passes through the system. This provides the ability to view granular details about the session not possible with other solutions, all with no increase in overhead.

Step 1: Under **Quick Filters**, click **Clear Filters**.

Step 2: Click **Flows** to display the media analytics.



Step 3: Under **Quick Filters**, click the pencil icon  for **Sites**.

Select **Branch 1** and click **Submit**.

Click **Update** when prompted to update charts.

Step 4: The **Flow Browser** will display the most recent 1000 flows.

Each column can be clicked to sort the data. Click the **PKTS** (packets) column twice to sort by the number of packets from highest to lowest.

SRC	SRC PORT	DST	DST PORT	POLICY	SEC ACTION	APPLICATION	PROTOCOL	PATH	FLOW DIR	PKTS	VOL	START TIME	LAST ACTIVITY
192.168.20.100	0	192.168.100.10	53	Network Services dns-Policy (QoS)	Allow	dns	UDP	Spectrum Cable to Circuit to Verizon Internet (#2)	LAN > WAN	75632	7.847 MB	Dec 28 2020, 02:06:45.815	Jan 14 2021, 11:59:23.088
192.168.20.103	18542	192.168.200.10	6100	Corp Voice Critical_VoIP_Apps (QoS)	Allow	rtp	UDP	Spectrum Cable to Circuit to Comcast Biz Internet	LAN > WAN	57408	13.778 MB	Jan 14 2021, 11:27:19.748	Jan 14 2021, 11:58:23.337

Step 5: Click the **SRC** (source) IP of the top TCP flow.

SRC	SRC PORT	DST	DST PORT	POLICY	SEC ACTION	APPLICATION	PROTOCOL	PATH	FLOW DIR	PKTS	VOL
192.168.20.100	0	192.168.100.10	53	Network Services dns-Policy (QoS)	Allow	dns	UDP	Spectrum Cable to Circuit to Verizon Internet (#2)	LAN > WAN	75632	7.847 MB

A new scrollable window will display with the flow details.


Flow Detail

ITEM	
Source IP (Port):	192.168.20.100 (0)
Destination IP (Port):	192.168.100.10 (53)
Application Name:	dns
Application Category:	net-discovery
Alt Application:	dns
Path Policy Set:	Corporate_Policy_Set
Path Policy Rule:	Network Services
Path Network Context:	None
Path Source Prefix:	None
Path Destination Prefix:	None
QoS Policy Set:	PriorityPolicySet
QoS Policy Rule:	

Close Advanced Info

Each row provides detailed information about the flow. We'll cover some of the top used information:

- Flow Decision Bitmap - A detailed accounting of why a flow decision was made.
- Hovering over the Flow Decision Data (click Advanced Info) will reveal additional information about the path selection determination for the flow.
- Source IP (Port)
- Destination (Port)
- Application name
- Path Information - What Path policy criteria was matched to.
- QoS Information - What QoS policy criteria was matched to.
- Security Information - What Security policy (ZBFW) criteria was matched.
- Chosen WAN Path - What path did App-fabric chose for the application session.
- EndPoint - Which DC or Service Group was chosen to send the traffic to (if applicable).
- Domain Detected - What domain (if any) was detected for the flow.
- Start and end time of the flow.
- DSCP Fields Detected
- TCP Specific Fields - Similar to wireshark, the app-fabric provides TCP accounting for each flow. This includes OOO, SACK, Retransmits, RST, SYN, and FIN counts. This information is useful when troubleshooting application / network issues.
- VLAN ID
- Application Performance Metrics - Just like at the application/site level, the App-Fabric provides performance accounting on a per application session basis. This information is crucial in separating server issues from network issues.

Step 6: Under **Quick Filters**, click the pencil icon  for **Apps**.

Under **Search**, type *rtp* and then select **rtp**.

Select Applications - (1 Shown)

SEARCH
rtp

CATEGORY
All

VIEWING
All Apps

TYPE
All

1 selected - [Clear](#) ONLY SHOW SELECTED

NAME	CATEGORY	TYPE
<input checked="" type="checkbox"/> rtp	streaming	System

Click **Submit**.

Click **Update** when prompted to update charts.

Step 7: The list of RTP flows will be displayed.

NETWORK	MEDIA	LINK QUALITY	FLOWS	ROUTING	SYSTEM	TIME FRAME							
						1H	1D	1W	1M	3M			
<p>Note: Only the last 1000 records for the given time range will be shown. If you don't find a specific app or flow of interest, try filtering by "Apps". > Advanced Query</p>													
SRC	SRC PORT	DST	DST PORT	POLICY	SEC ACTION	APPLICATION	PROTOCOL	PATH	FLOW DIR	PKTS	VOL	START TIME	LAST ACTIVITY
192.168.20.103	18542	192.168.200.100	6100	Corp Voice Critical_VoIP_Apps (QoS)	Allow	rtp	UDP	Spectrum Cable to Circuit to Comcast Biz Internet	LAN > WAN	104318	25.036 MB	Jan 14 2021, 11:27:19.748	Jan 14 2021, 12:23:33.345
192.168.20.104	17572	192.168.200.100	6101	Corp Voice Critical_VoIP_Apps (QoS)	Allow	rtp	UDP	Spectrum Cable to Circuit to Comcast Biz Internet	LAN > WAN	30856	7.405 MB	Jan 14 2021, 10:54:14.569	Jan 14 2021, 11:38:57.884

Step 8: Click the **SRC** (source) IP of the top TCP flow.

A new scrollable window will display with the flow details.

Flow Detail

ITEM	
Flow Decision Bitmap:	0x0c019802, 0x00000611, 0x00000000, 0x00000000
Source IP (Port):	192.168.20.103 (18542)
Destination IP (Port):	192.168.200.100 (6100)
Application Name:	rtp
Application Category:	streaming
Alt Application:	rtp
Path Policy Set:	Corporate_Policy_Set
Path Policy Rule:	Corp Voice
Path Network Context:	None
Path Source Prefix:	None
Path Destination Prefix:	None
QoS Policy Set:	Corporate_QoS_Policy_Set

Close Advanced Info

Just like a TCP application you will have detailed information about the RTP call. However, instead of TCP specific metrics there will be real-time media specific metrics including:

- Flow Decision Bitmap - A detailed accounting of why a flow decision was made.
- Hovering over the Flow Decision Data will reveal additional information about the path selection determination for the flow.
- Source IP (Port)
- Destination (Port)
- Application name
- Path Information - What Path policy criteria was matched to.
- QoS Information - What QoS policy criteria was matched to.
- Security Information - What Security policy (ZBFW) criteria was matched to.
- Chosen WAN Path - What path did App-fabric chose for the application session.
- EndPoint - Which DC or Service Group was chosen to send the traffic to (if applicable).
- Domain Detected - What domain (if any) was detected for the flow.
- Start and end time of the flow
- DSCP Fields Detected
- Codec - The detected codecs used throughout the life of the call in each direction.
- VLAN ID
- RTM Performance - Bidirectionally measure Min/Max/Average
 - Packet loss
 - Jitter
 - MoS

End of Activity 8

Activity 9 – Prisma SD-WAN: Application Policy

In this activity, you will:

- Examine application policies that ensure performance and compliance

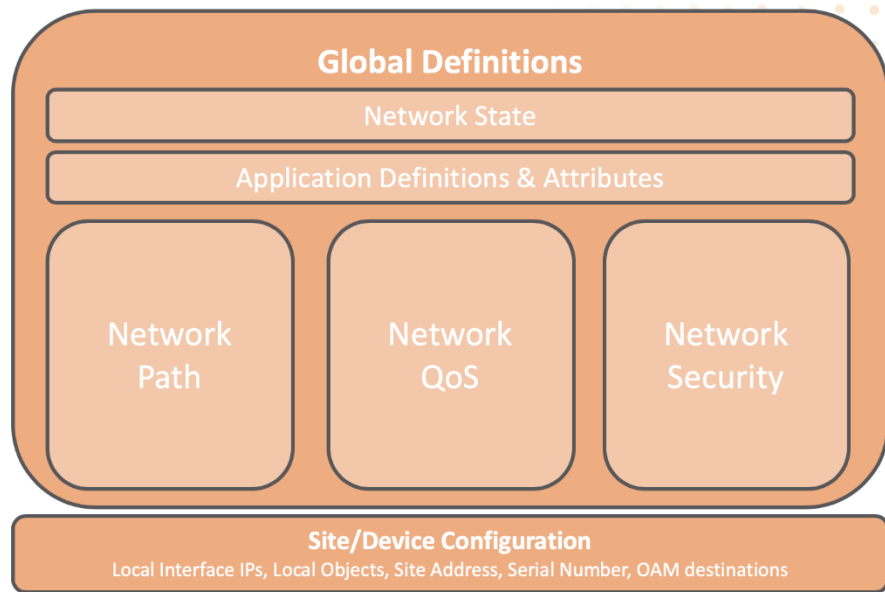
Abstract and Simplify

App-Network-Device Network Configuration Hierarchy

Legacy Template



CloudGenix SD-WAN API Model



The Prisma SD-WAN provides a complete policy framework designed to fit the needs of the user and the application. This is achieved by applying Path, QoS, Security, and NAT (if applicable) rules on a per-application basis.

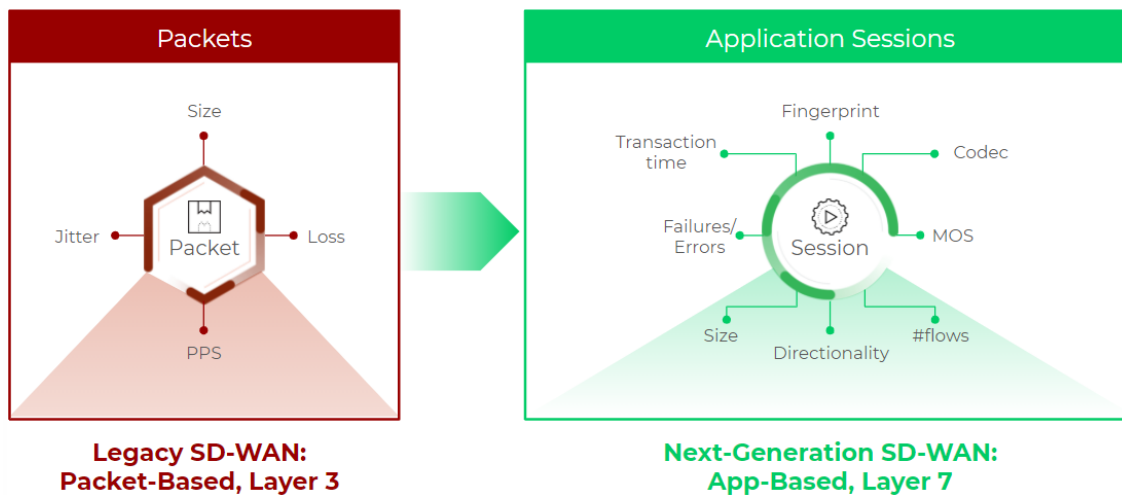
Consider an organization that has recently made the shift to adopt cloud services such as Microsoft Office 365 and Salesforce. To date its security policy dictated that all traffic destined for the Internet must transit through the centralized data center firewalls via the private WAN. After numerous complaints about application performance for Office 365 and Salesforce, the security team grants an exception to allow both of these applications to go direct to the Internet since they are encrypted and trusted applications.

Given that Prisma SD-WAN is an application-defined architecture that operates at the application-session level, the network administrator is enabled to easily accomplish the task of selectively sending Office 365 and Salesforce traffic direct to the Internet.

In this activity we'll verify that the operations team has correctly configured the system to achieve the user intent by reviewing:

- Application Definitions
- Path Policies
- QoS Policies

Task 1 – Application Definitions



As the name suggests, the Prisma SD-WAN is an application-based system. Not only does Prisma SD-WAN use a purpose-built application ID engine to perform app identification, it is an essential component of the system. In other words, it's not a feature that can be turned on or off, but, a core part of how the system works.

The system has two main types of application definitions:

System Apps

- These are applications maintained by the Palo Alto Networks team for commonly used applications.
- There are over 500 applications out of the box.
- Application definitions are automatically updated as needed, typically 1-2 times per quarter.
- Users can optionally add overrides to the default system applications.

Custom Apps

- These are applications created and maintained by the customer.

Both **System Apps** and **Custom Apps** can match on many criteria

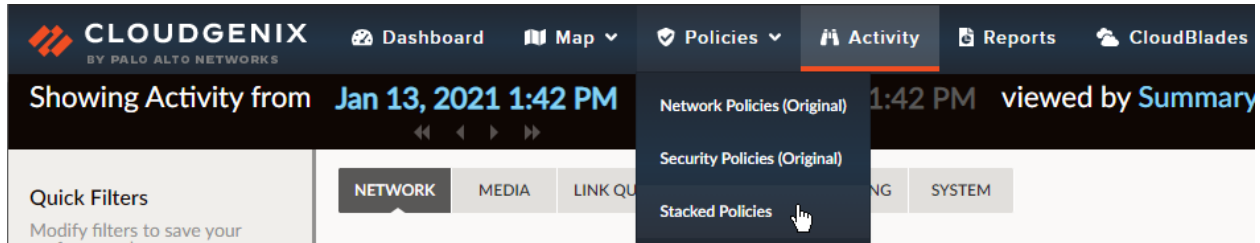
- **L7 Rule** - Use a domain name to match the application.
- **L3/L4 Rule** - Use a combination of Prefix filters (source and/or destination), protocols, and port numbers to match the application.
- **Signature** - Some system applications also leverage deep packet inspect and a subsequent signature to identify the application.

Each application definition includes configuration options that help the system determine how to handle the traffic. These options are:

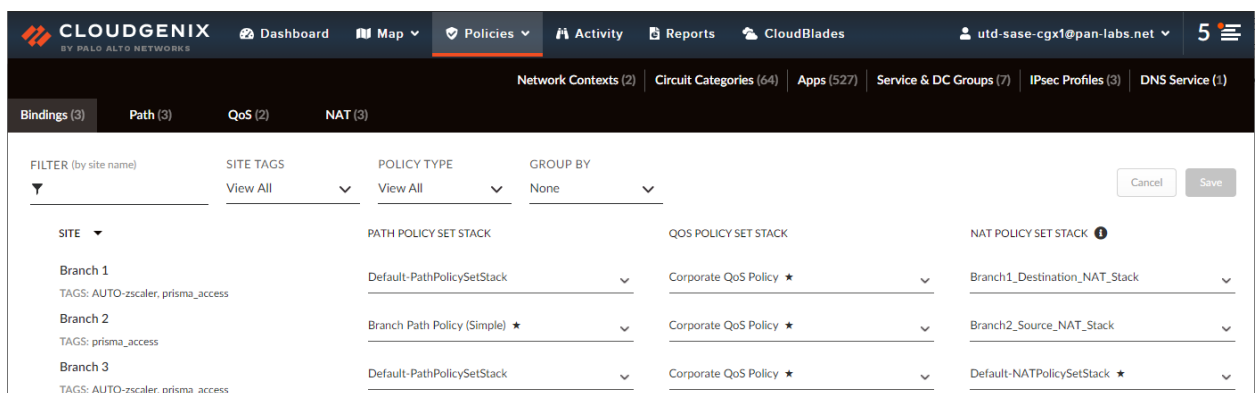
- **App Category** - Used primarily for organizational purposes.
- **Transfer Type** - The designated transfer type has an impact on how QoS is applied to any app sessions that match the application definition.
- **Ingress Traffic Percentage** - During the path selection process this helps the system determine if the application is upload heavy or download heavy and it will place the session on the appropriate link.
- **Connection Idle Timeout** - The amount of time that a session will stay active in the system with no packets observed on the wire.
- **Path Affinity** - Enable the system to group sessions of a like application onto the same link.
- **Using App Reachability Detection** - The Prisma SD-WAN system is capable of detecting brown-out conditions for all TCP applications. This detection can be disabled selectively on a per-application basis.

- **Network Scan App** - In some networks customers leverage automated scanning utilities to discover vulnerable systems. These systems sometimes flood the network with traffic across all ports. In order to prioritize this traffic properly below that of production traffic, it can be defined as a Network Scan App. This is typically done using source prefix filters in the application definition.

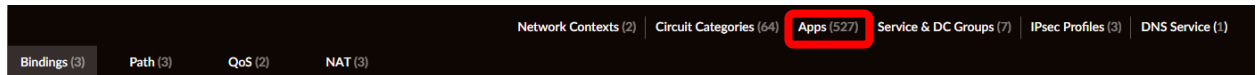
Step 1: Click the **Policies** tab, and then select **Stacked Policies**.



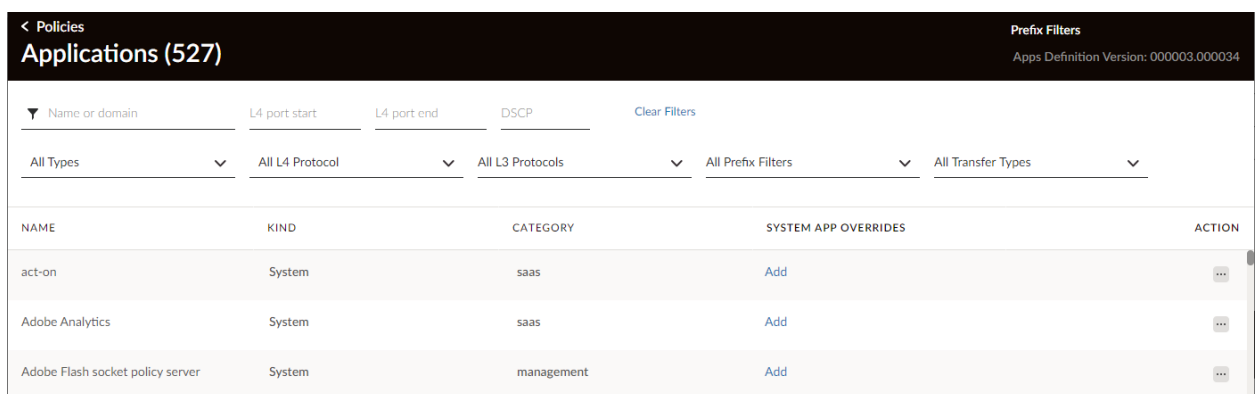
The **Policy Bindings** are now displayed.



Step 2: Click **Apps**

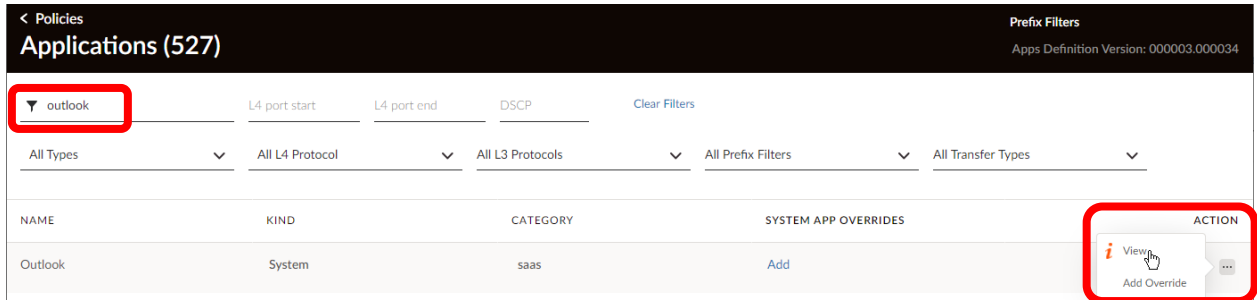


This displays a full list of all **Application Definitions**.



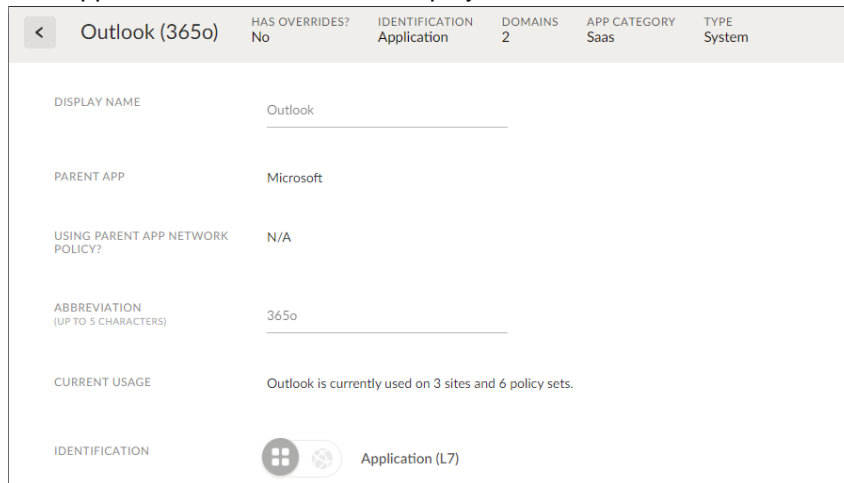
Note that they can be sorted and filtered in many ways.

Step 3: In the **Name or domain** filter box, type **outlook**.



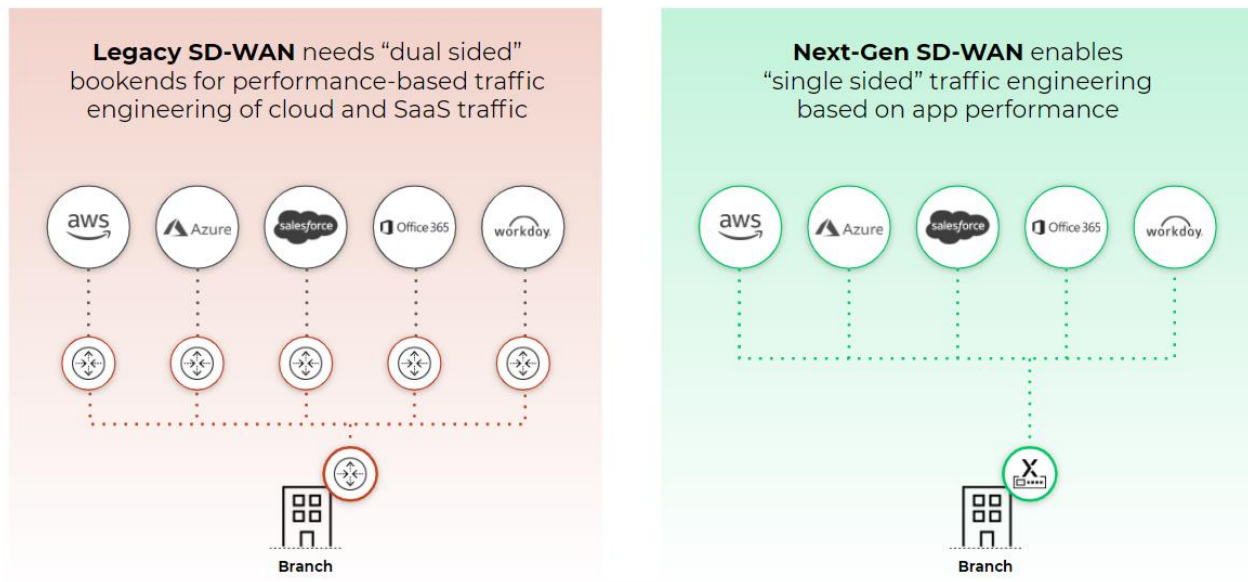
Under **Action**, click the ellipses and then select **View**.

The Outlooks system application definition will be displayed.



Next, we will look how applications are used in path policies.

Task 2 – Path Policies



Path policies determine how the various paths available to the Prisma SD-WAN are used to fulfill business intent.

There is significant control in the path policy framework. Match criteria include:

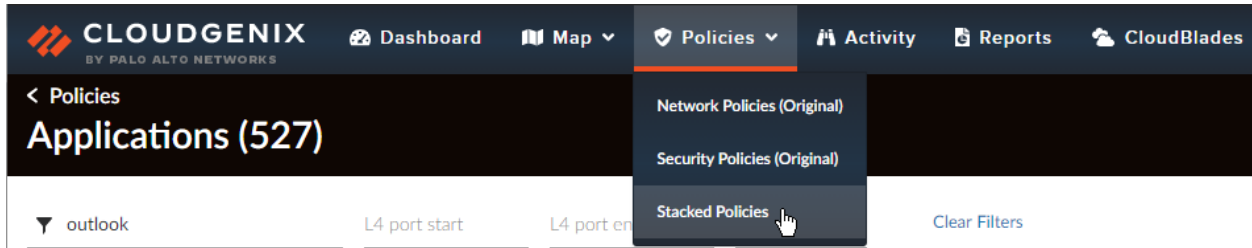
- **Context** - An optional identifier applied at the device interface level used to signify certain types of networks or users. Guest and PoS (point of sale) are commonly used Contexts.
- **Prefixes** - Global and local prefix filters can be optionally matched as source and/or destination criteria.
- **Apps** - Both system and custom (user-defined) applications can be matched.

Path selection options include:

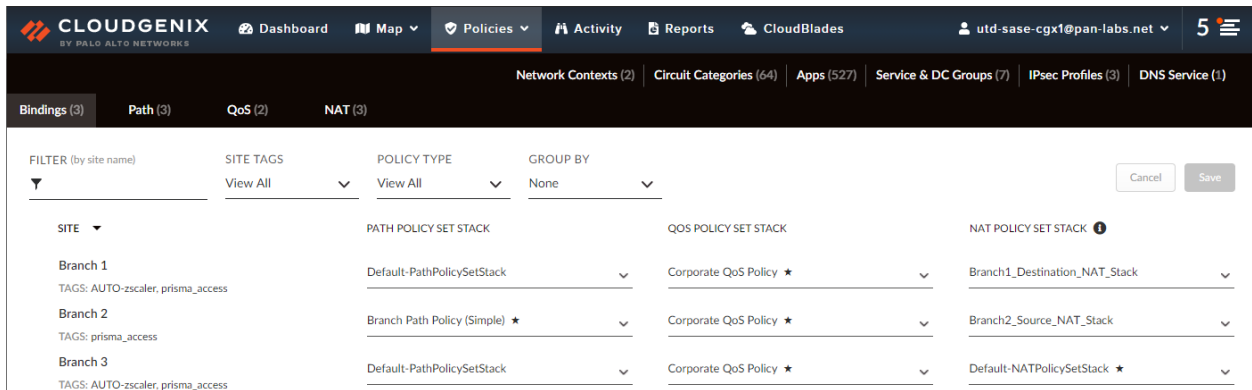
- **Paths** - Granular control of which site connections are used to forward traffic.
- **Active** - Paths that are actively used to forward traffic in a load-shared manner.
- **Backup** - Paths that are used when active paths are down or when quality issues occur.
- **L3 Failure Path** - Paths that are used only when all active and backup paths are down.
- **Service and DC Groups**
- **Service Group** - Used to direct traffic to a 3rd Party service group. A common example would be to send untrusted traffic to Palo Alto Networks Prisma Access solution for further security inspection.
- **DC Group** - One or more CloudGenix Data Center locations that can be used as transit points.

Since we have approval from the security team to send Salesforce and Office 365 traffic directly onto the internet to maximize performance, we'll explore how to verify the change was made successfully by the operations team.

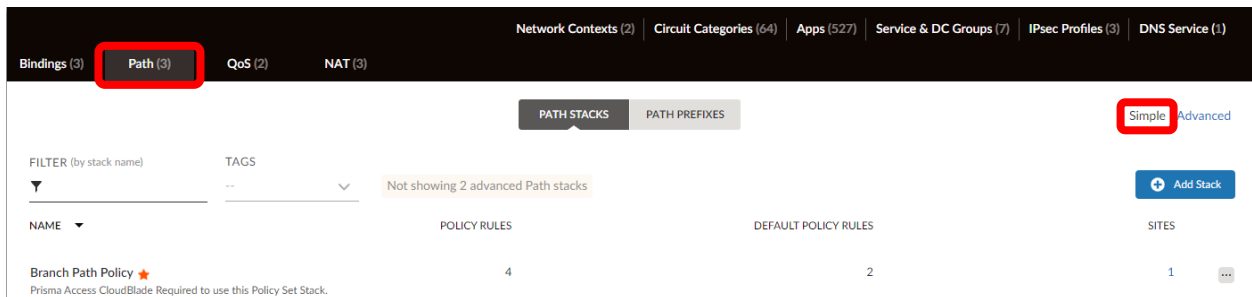
Step 1: Click the **Policies** tab, and then select **Stacked Policies**.



The **Policy Bindings** are now displayed.

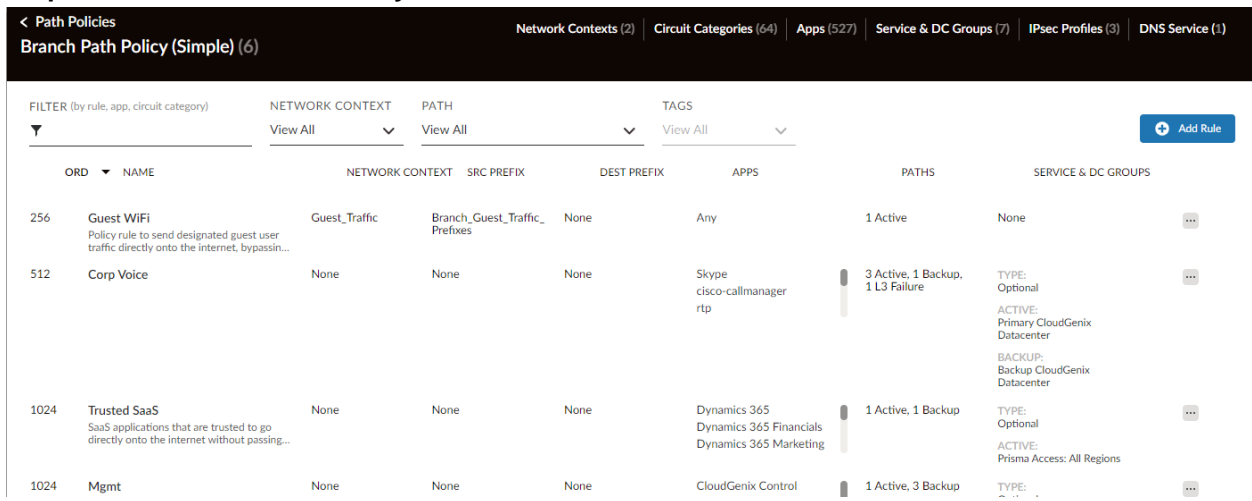


Step 2: Click the **Path** tab and then **Simple**.

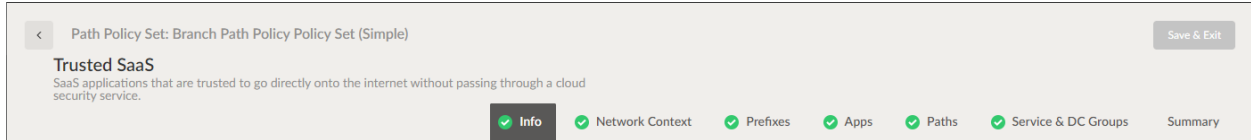


The **Branch Path Policy** is displayed.

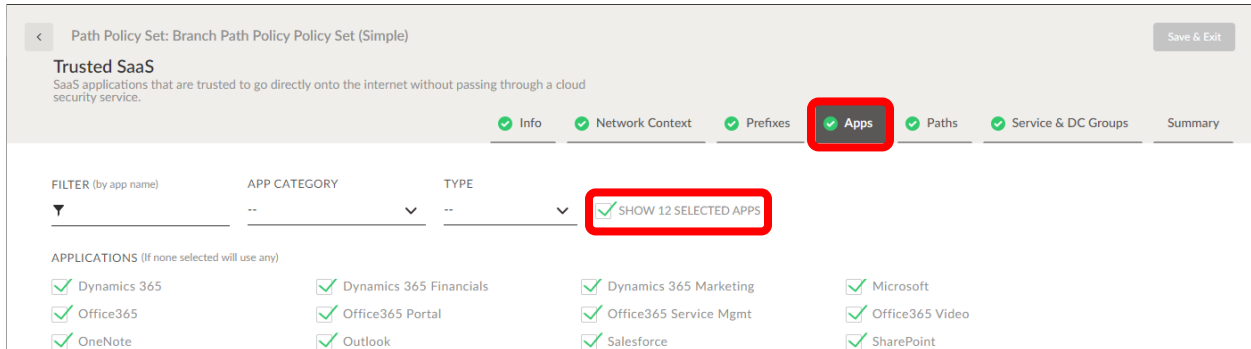
Step 3: Click **Branch Path Policy** to view the list of rules.



Step 4: Click on the **Trusted SaaS** policy.

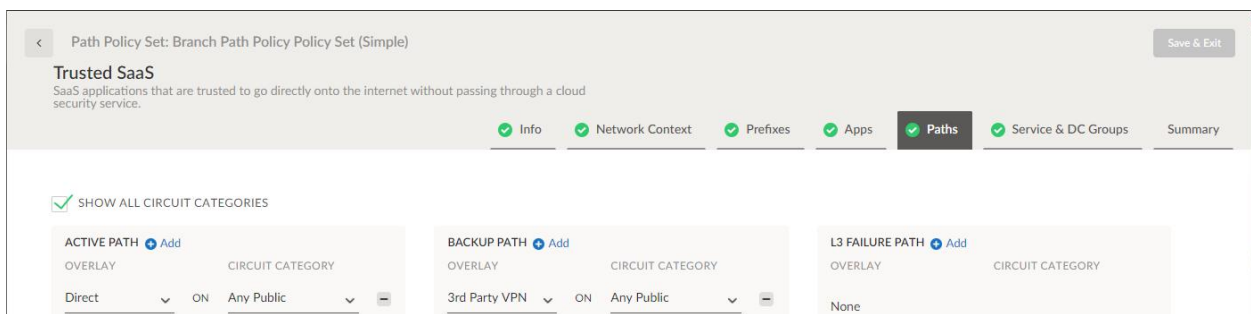


Click on the **Apps** tab and then select the checkbox for **Show X Selected Apps**.



Note that, in this rule, both Salesforce and Office365 have been selected.

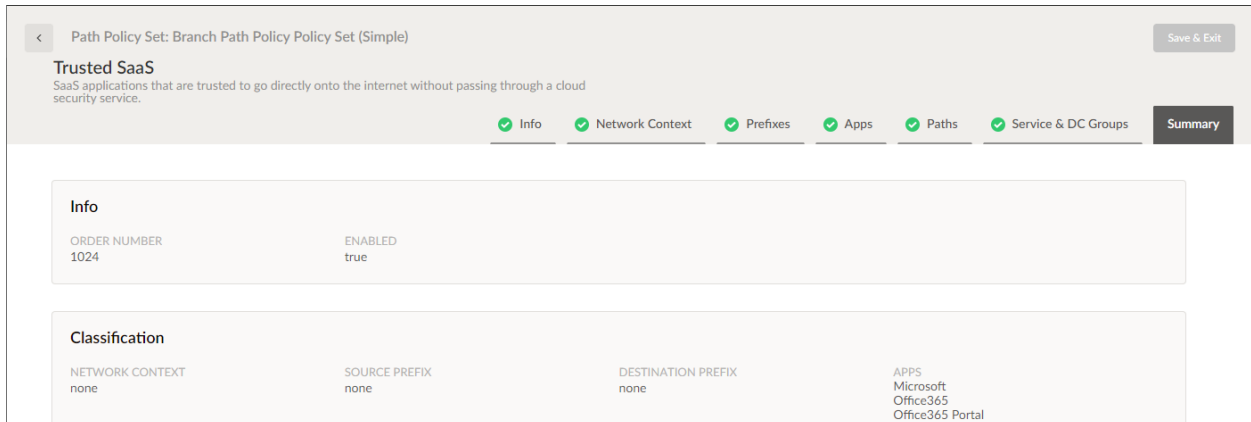
Step 5: Click on the **Paths** tab.



Note the path selection configuration:

- **Active Path** - Direct on Ethernet Internet
- **Backup Path** - Direct on Internet Cable
- **L3 Failure Path** - Direct on Metered 3G/4G/LTE

Step 6: Click on the **Summary** tab to view all the settings for the Trusted SaaS path policy rule.

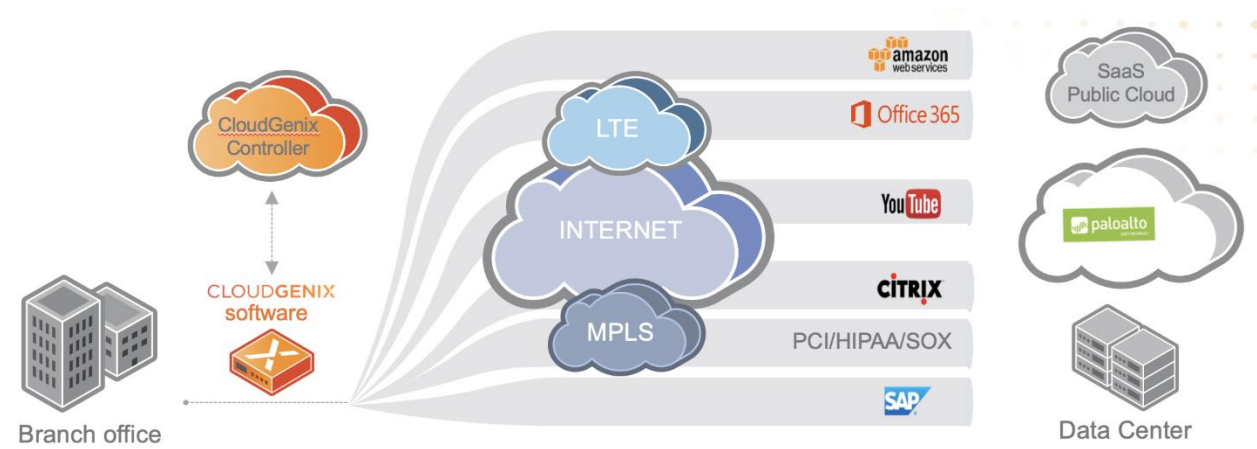


Step 7: Click on the back arrow at the top left-hand corner of the page.



Next, we will look at how applications are used in QoS policies.

Task 3 – QoS Policies



The Prisma SD-WAN system follows a simple QoS model utilizing shaping. There are four top level queues called **Priority** levels:

- Platinum
- Gold
- Silver
- Bronze

Each **Priority** (top-level queue) is allocated a configurable percentage share of the circuit bandwidth. This value is leveraged to shape traffic in times of congestion.

Each **Priority** level has 4 sub-queues, one for each transfer type:

- Real-Time Audio
- Real-Time Video
- Transactional
- Bulk

This is a view into how the bandwidth percentages are allocated:

Priority and Queue Configuration

ADD BREAKPOINT (1 of 4 defined)

0 - 10000 Mbps **RESET**

Platinum Clear 50 %				Gold Clear 25 %			
Audio	Video	Transactional	Bulk	Audio	Video	Transactional	Bulk
30	20	30	20	30	20	30	20

Silver Clear 15 %				Bronze Clear 10 %			
Audio	Video	Transactional	Bulk	Audio	Video	Transactional	Bulk
30	20	30	20	30	20	30	20

The transfer type is specified in the application definition which was covered earlier in this task.

In our example the company uses a wide variety of applications to conduct business. Specifically, the sales division uses the salesforce.com SaaS application as the primary CRM system. We will ensure that the operations team has mapped both applications into the Gold queue.

Step 1: Click the **Policies** tab, and then select **Stacked Policies**.

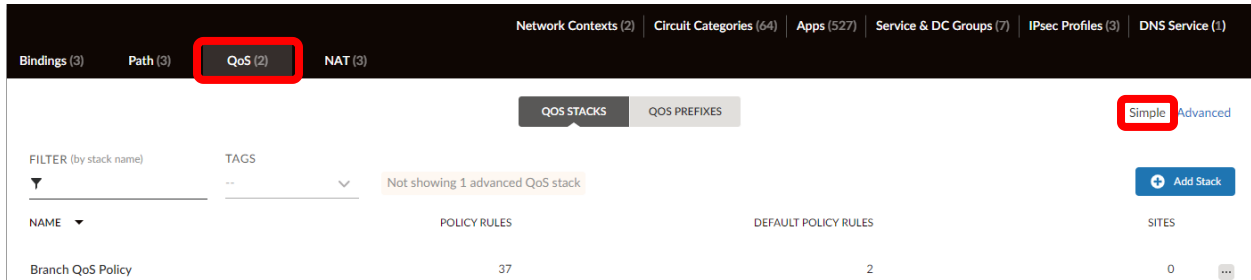
The screenshot shows the CloudGenix interface with the 'Policies' dropdown menu open. The 'Stacked Policies' option is highlighted. The breadcrumb path is 'Path Policies > Branch Path Policy (Simple) (6)'. Other menu items include 'Network Policies (Original)', 'Security Policies (Original)', and 'Stacked Policies'.

The **Policy Bindings** are now displayed.

The screenshot shows the 'Policy Bindings' table in the CloudGenix interface. The table has columns for 'SITE', 'POLICY TYPE', and 'GROUP BY'. The 'POLICY TYPE' column is expanded to show 'PATH POLICY SET STACK', 'QoS POLICY SET STACK', and 'NAT POLICY SET STACK'. The 'SITE' column lists 'Branch 1', 'Branch 2', and 'Branch 3'. The 'GROUP BY' column shows 'Default-PathPolicySetStack', 'Corporate QoS Policy', and 'Default-NATPolicySetStack'.

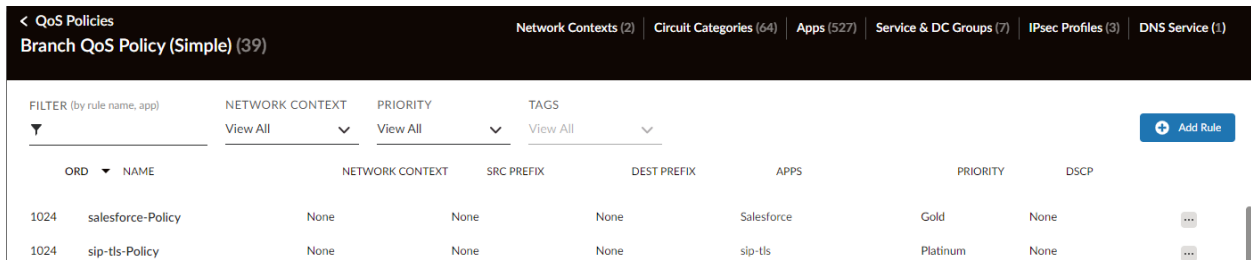
SITE	POLICY TYPE	GROUP BY
Branch 1 TAGS: AUTO-zscaler, prisma_access	Default-PathPolicySetStack	Corporate QoS Policy
Branch 2 TAGS: prisma_access	Branch Path Policy (Simple)	Corporate QoS Policy
Branch 3 TAGS: AUTO-zscaler, prisma_access	Default-PathPolicySetStack	Corporate QoS Policy

Step 2: Click the **QoS** tab and then **Simple**.

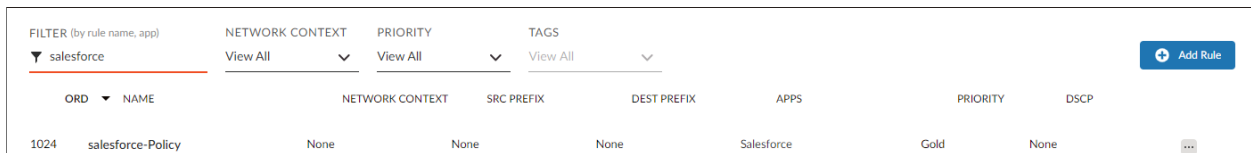


The **Branch QoS Policy** is displayed.

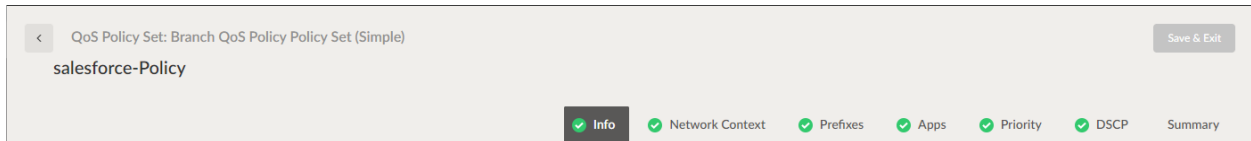
Step 3: Click on **Branch QoS Policy** to view the list of rules.



Step 4: In the **Filter (by rule, name, app)** box, type **salesforce**.



Step 5: Click on **salesforce-Policy**.

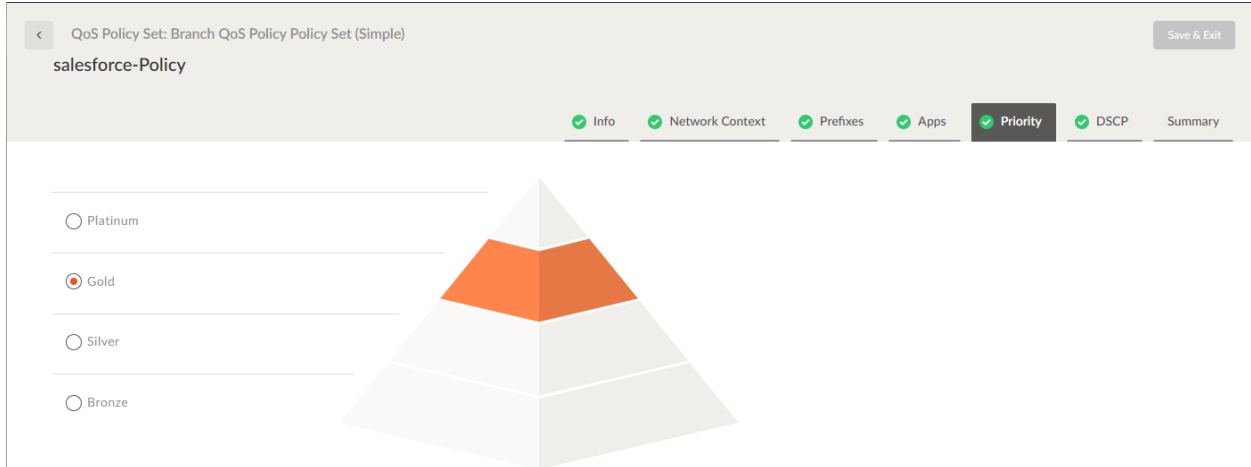


Click on the **Apps** tab and then select the checkbox for **Show 1 Selected App**.



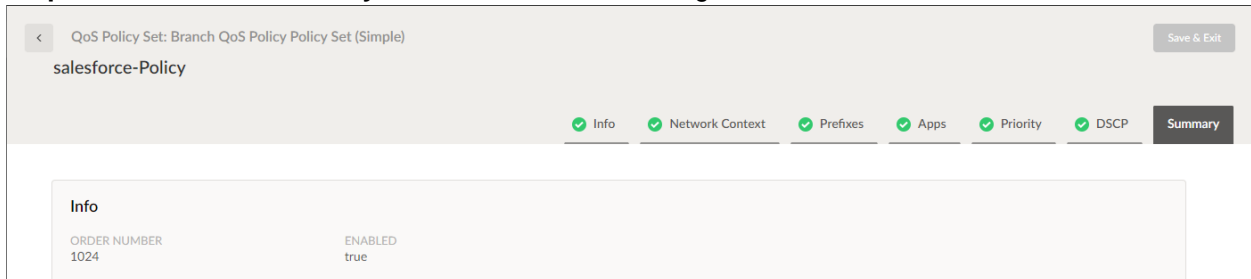
Note that, in this rule, only **Salesforce** has been selected.

Step 6: Click on the **Priority** tab.

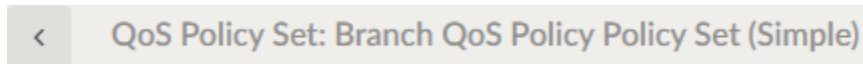


Confirm that Gold is the selected priority.

Step 7: Click on the **Summary** tab to view the entire configuration.



Step 8: Click on the back arrow at the top left-hand corner of the page.



End of Activity 9

Activity 10 – Prisma SD-WAN: Application Defined

In this activity, you will:

- Review the network infrastructure that enables policy enforcement

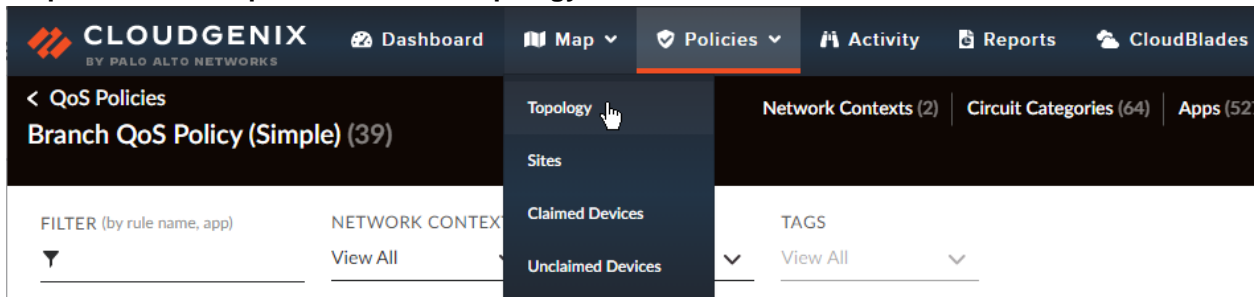
The foundation of the Prisma SD-WAN system is that it is application defined. It is comprised of the sites and devices and is responsible for the identification of applications, application monitoring, inter-site VPN connections, connections to 3rd party services, and policy instantiation.

In this section we'll explore how the logical application fabric is configured and built.

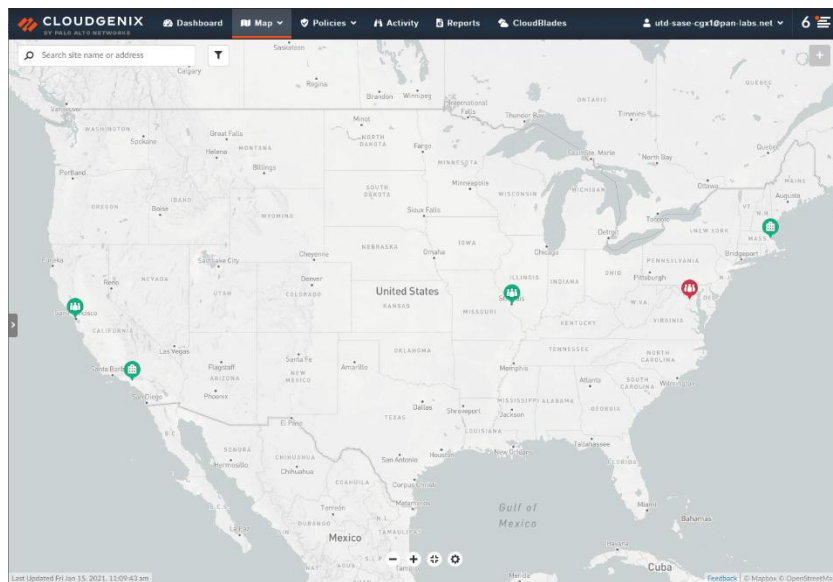
Let's get started by reviewing the topology.

Task 1 – Topology

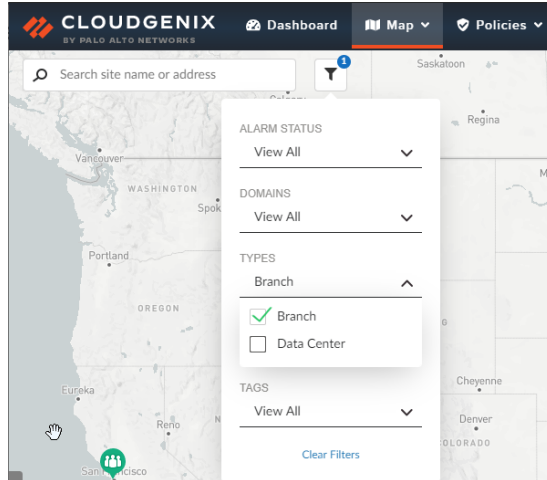
Step 1: Click on **Map** and then select **Topology**.



The map is displayed. By default, all sites are visible but can be filtered.

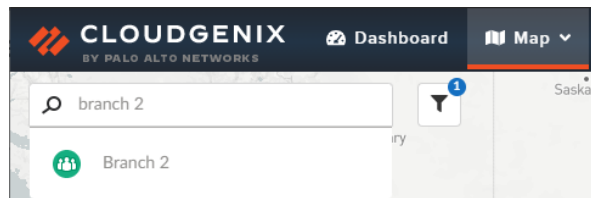


Step 2: Click on the filter icon. Expand **Types** and select **Branch**.



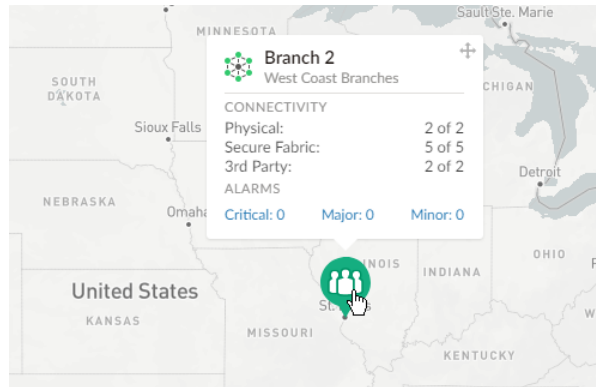
Only branch sites are shown.

Step 3: In the **Search site name or address** box, type **branch 2**.



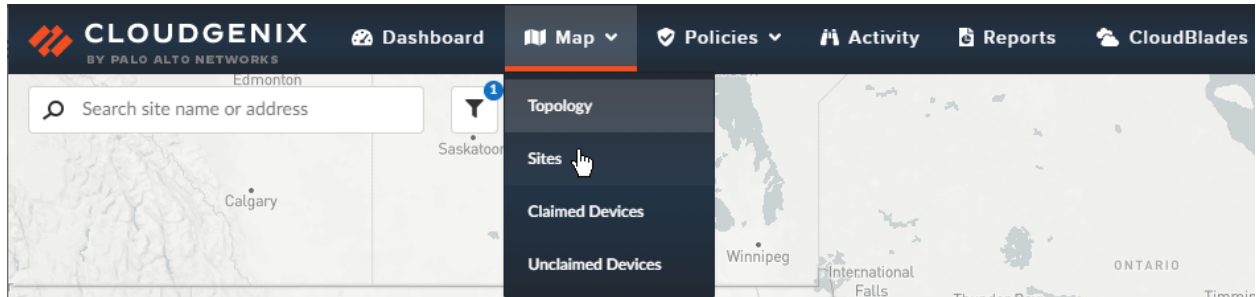
Select **Branch 2**.

Branch 2 is centered on the map.

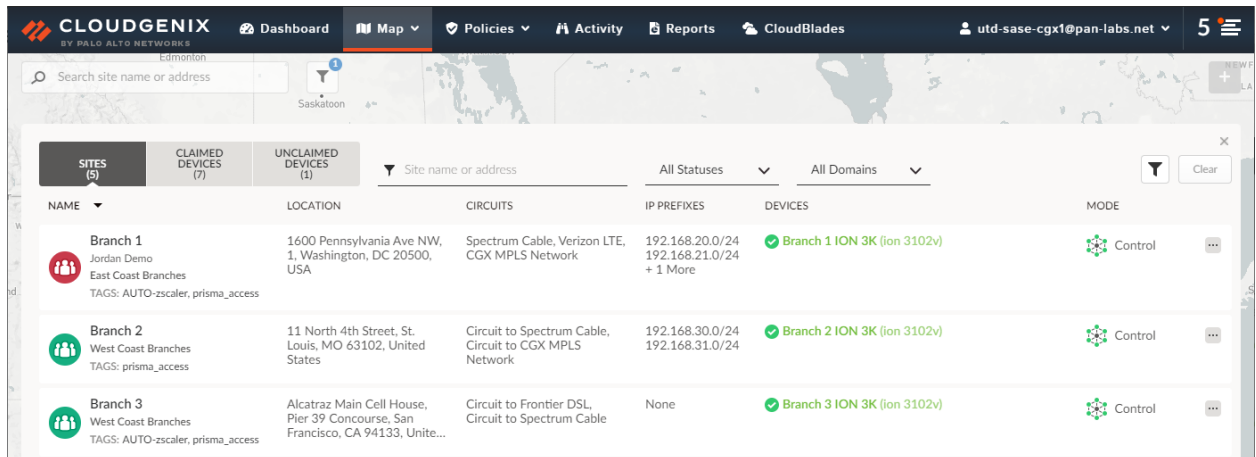


Task 2 – Site Review

Step 1: Click on **Map** and then select **Sites**.

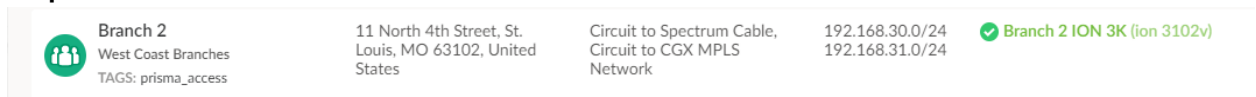


A list of sites is displayed.

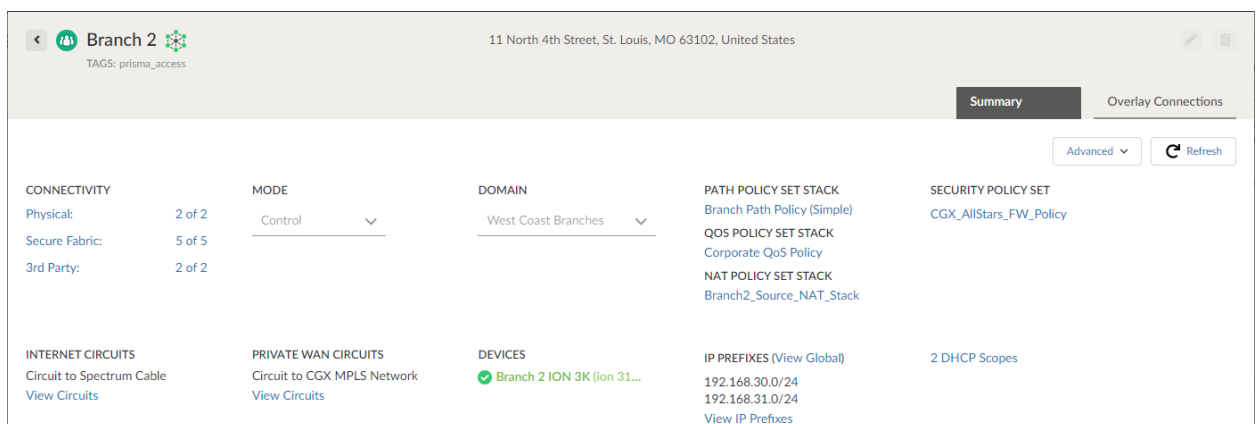


You can search for sites by name or address as well as filter the list of sites using multiple criteria.

Step 2: Click on **Branch 2**.



The site overview panel will be displayed.



This panel provides a single point to configure and manage the branch, including:

Connectivity

- **Physical** - The state of the Internet and Private WAN connections.
- **Secure Fabric** - State and configuration of the CloudGenix VPNs between sites.
- **3rd Party** - The state of the traditional IPSEC Tunnels used to connect to services such as Prisma Access for Remote Networks.

Alarms

- A list of all standing alarms organized by alarm severity.
- If alarms are present, they can be clicked, and additional details viewed with the events widget.

Circuits

- Internet - Site-level configuration information for public internet circuits.
- Private WAN - Site-level configuration information for private circuits including MPLS and P2P links.

Devices - List of devices assigned to the site.

Task 3 – Physical Connectivity

Each CloudGenix site is connected by one or more physical connections.

Step 1: To view the physical connection, click on **Physical**.

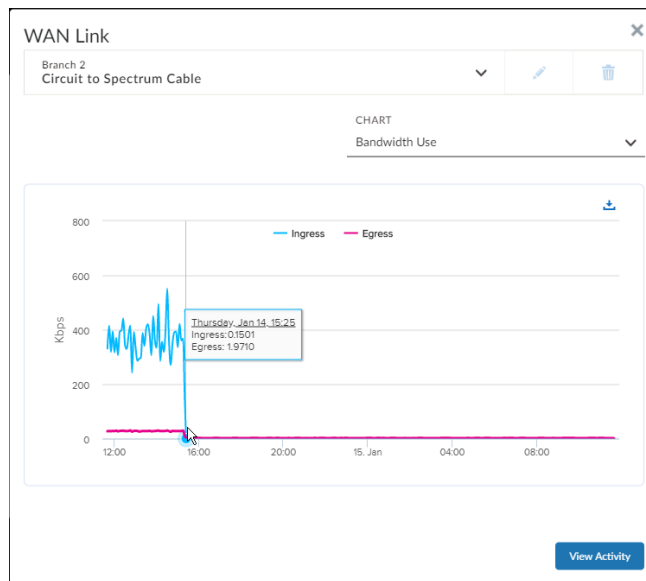
The screenshot shows the configuration page for 'Branch 2' at '11 North 4th Street, St. Louis, MO 63102, United States'. The 'CONNECTIVITY' section is highlighted with a red box, showing 'Physical: 2 of 2', 'Secure Fabric: 5 of 5', and '3rd Party: 2 of 2'. Other sections include 'MODE' (Control), 'DOMAIN' (West Coast Branches), and several policy set stacks.

Step 2: Click on **Circuit to Spectrum Cable**.

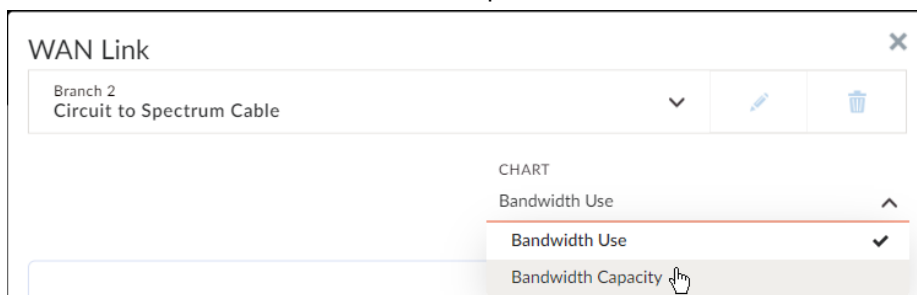
The screenshot shows a 'Connectivity' table with columns: Link Name, Type, Status, and Admin Up. The 'Circuit to Spectrum Cable' entry is highlighted with a red box. The table also includes filter options for link name, type, status, and admin up.

Link Name	Type	Status	Admin Up
Circuit to CGX MPLS Network	Physical	Up	N/A
Circuit to Spectrum Cable	Physical	Up	N/A

The **ingress** and **egress** underlay utilization of the Spectrum Cable connection will be displayed:




Step 3: To view the measured bandwidth, click the drop-down for **Chart** and select **Bandwidth Capacity**.



The Prisma SD-WAN system performs automatic carrier bandwidth capacity measurements. This is done in a manner that does not affect performance of the connection by using a custom algorithm. The system provides a view of throughput over time on a per connection basis which can be utilized to hold your carrier accountable.



Step 4: Click on the  in the top right-hand corner of the **WAN Link** view to return to the **Connectivity** view.

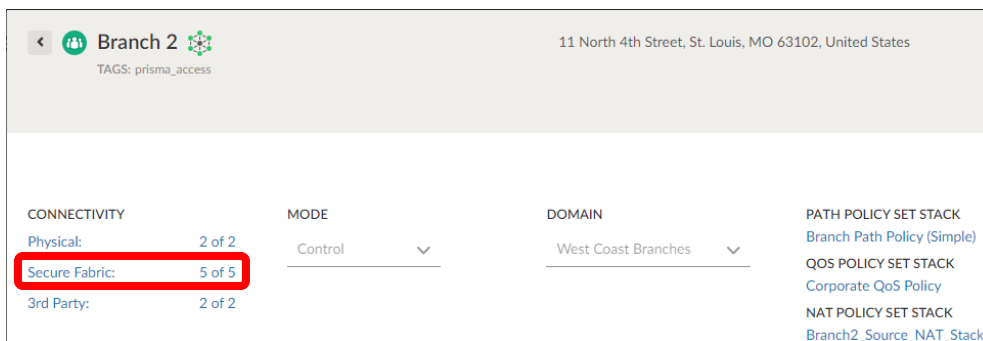
Click on the  in the top right-hand corner of the **Connectivity** view to return to the **Site Overview** panel.

Task 4 – Secure Fabric

The Secure Fabric is the collection of VPNs between CloudGenix sites and services such as Prisma Access for Remote Networks.

The fabric supports multiple topologies including hub and spoke (default), partial mesh, and full mesh.

Step 1: To view the secure fabric links, click on **Secure Fabric**.



Branch 2
TAGS: prisma_access
11 North 4th Street, St. Louis, MO 63102, United States

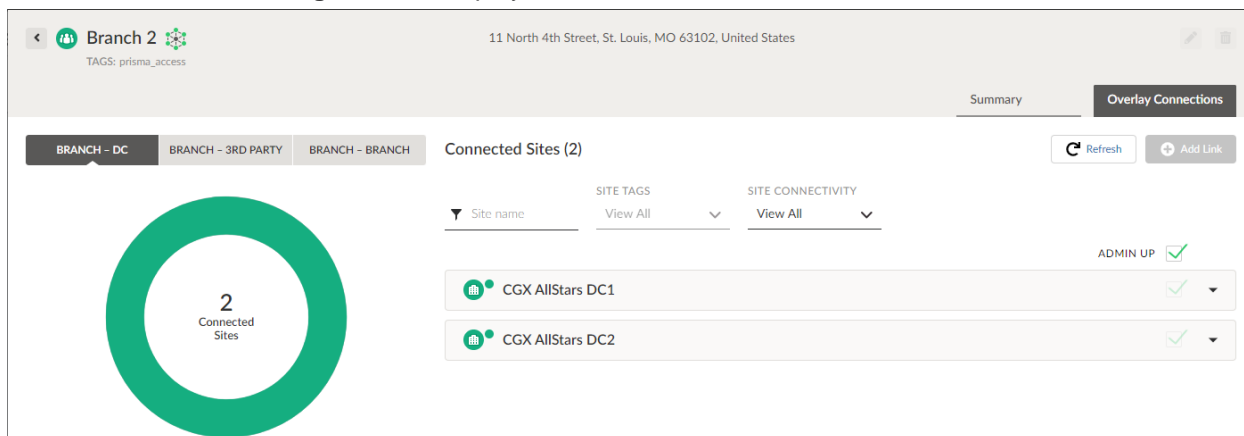
CONNECTIVITY
Physical: 2 of 2
Secure Fabric: 5 of 5
3rd Party: 2 of 2

MODE
Control

DOMAIN
West Coast Branches

PATH POLICY SET STACK
Branch Path Policy (Simple)
QOS POLICY SET STACK
Corporate QoS Policy
NAT POLICY SET STACK
Branch2_Source_NAT_Stack

The **Secure Fabric Management** is displayed.



Branch 2
TAGS: prisma_access
11 North 4th Street, St. Louis, MO 63102, United States

Summary Overlay Connections

BRANCH - DC BRANCH - 3RD PARTY BRANCH - BRANCH

Connected Sites (2) Refresh Add Link

2 Connected Sites

Site name	SITE TAGS	SITE CONNECTIVITY	ADMIN UP
CGX AllStars DC1	View All	View All	✓
CGX AllStars DC2	View All	View All	✓

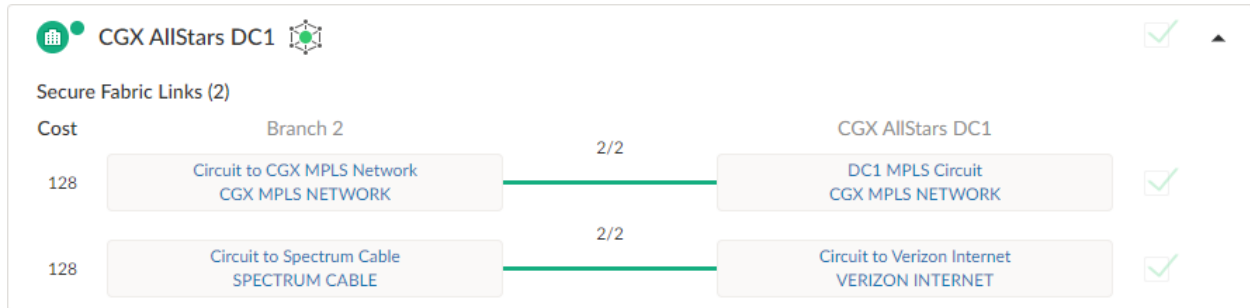
Connectivity is organized into 3 tabs:

- **Branch to DC** - Tunnels to CloudGenix hub locations.
- **Branch to Branch** - Tunnels from one CloudGenix branch to another CloudGenix branch.
- **Branch to 3rd Party** - IPSEC Tunnels connecting to services such as Prisma Access.

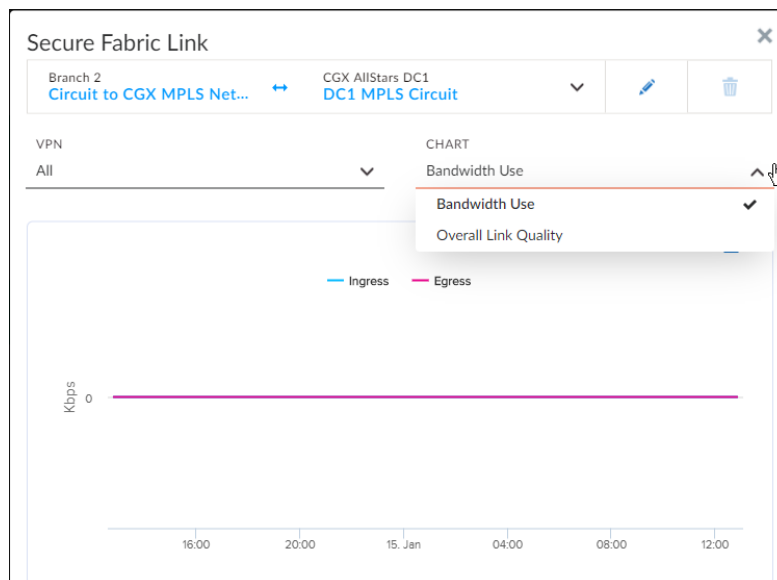
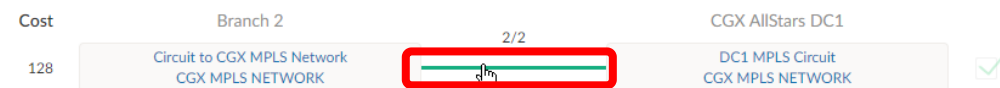
Each tab will:

- Detail the state of the tunnels.
- Allow an administrator to build new tunnels (Branch to Branch only).
- Allow an administrator to control the admin state (Up / Down) of a tunnel.
- View additional information about the tunnel such as:
 - Bandwidth Use
 - Link Quality

Step 2: Click on **CGX AllStars DC1** to view additional tunnel information.

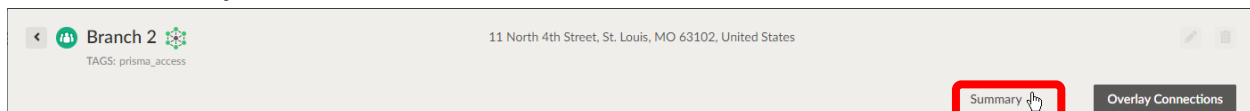


Click on the first green line to view **Bandwidth Use** and **Overall Link Quality**.



Step 3: Click on the **X** in the top right-hand corner of the **Secure Fabric Link** view.

Click the **Summary** tab.



Task 5 – Devices

The physical or virtual devices are called IONs - Instant On Networks.

Step 1: To view the **Device** configuration, click on **Branch 2 ION 3K**.

The screenshot shows the configuration page for Branch 2. The 'DEVICES' section is highlighted with a red box, showing 'Branch 2 ION 3K (ion 31...)' with a green checkmark. Other sections include CONNECTIVITY (Physical: 2 of 2, Secure Fabric: 5 of 5, 3rd Party: 2 of 2), MODE (Control), DOMAIN (West Coast Branches), PATH POLICY SET STACK (Branch Path Policy (Simple), QoS Policy Set Stack, NAT Policy Set Stack), SECURITY POLICY SET (CGX_AllStars_FW_Policy), INTERNET CIRCUITS (Circuit to Spectrum Cable), PRIVATE WAN CIRCUITS (Circuit to CGX MPLS Network), and IP PREFIXES (192.168.30.0/24, 192.168.31.0/24).

The **Basic Info** is displayed for this ION device.

The screenshot shows the 'Basic Info' tab for Branch 2 ION 3K. Fields include: DEVICE NAME (Branch 2 ION 3K), DESCRIPTION, TAGS, MODEL (ion 3102v), SERIAL NUMBER (564d4f54-15d8-6a11-b9d7-d68a7a0de4f2), SOFTWARE VERSION (5.4.3-b9), ENABLE L3 DIRECT PRIVATE WAN FORWARDING? (Yes), ENABLE L3 LAN FORWARDING? (Yes), APPLICATION REACHABILITY PROBE (Enabled), and SOURCE INTERFACE (None).

Step 2: Click on the **Interface Config** tab.

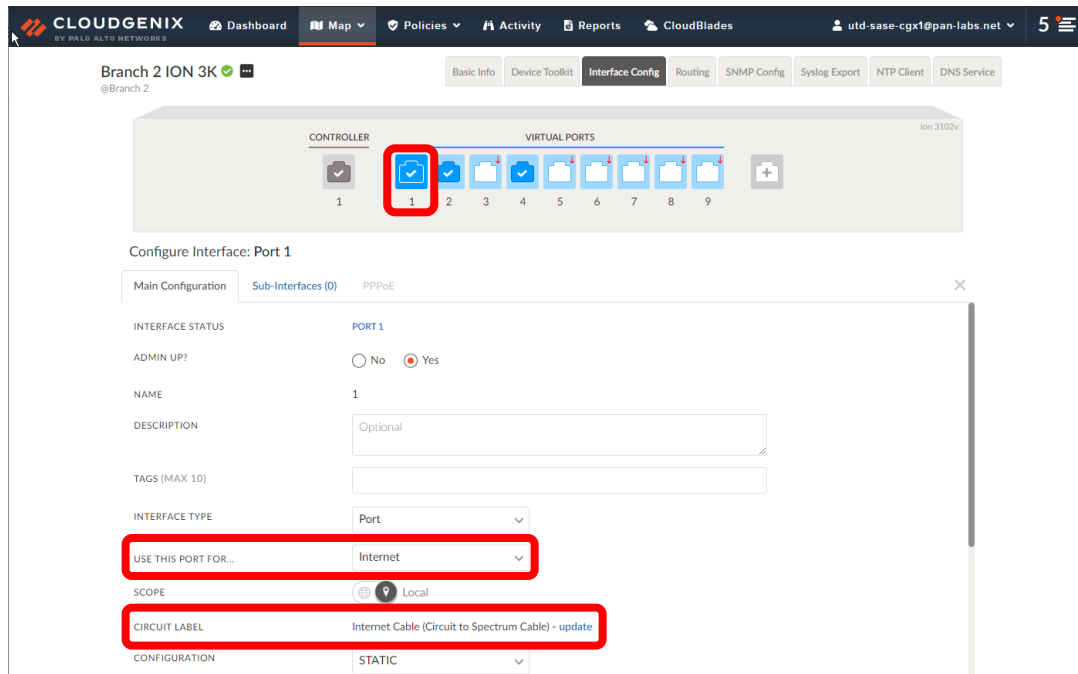
The screenshot shows the configuration page for Branch 2 ION 3K with the 'Interface Config' tab highlighted by a red box.

Interfaces are displayed in a visual and list format.

The screenshot shows the 'Interface Config' tab for Branch 2 ION 3K. It features a visual representation of the device with a CONTROLLER and VIRTUAL PORTS (1-9). Below is a table of interfaces:

INTERFACES	TYPE	ADMIN STATUS	CONFIGURATION	CIRCUITS
2.30 on Port 2	Sub-Interface	Up	LAN • STATIC	--
2.31 on Port 2	Sub-Interface	Up	LAN • STATIC	--

Step 3: Click on Port 1.



Note that the interface is used for Internet and there is an internet circuit label attached. When this is set, the system automatically configures many parameters, including:

- Firewall rules are configured to only allow IPSEC and ESP inbound from the internet to the device.
- A NAT boundary is defined and any traffic that is configured (via policy) to go direct on the internet will be automatically NATd to the interface IP address.
- CloudGenix VPN tunnels are automatically established to all hub nodes.

There are many more configuration options available including SNMP, Routing, Syslog, NTP, etc.

End of Activity 10

Activity 11 - Feedback on Ultimate Test Drive

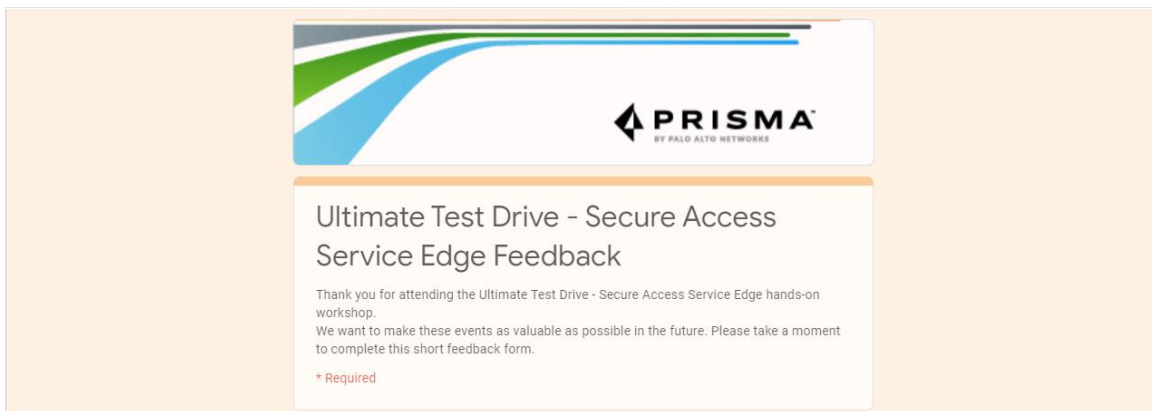
Thank you for attending the Ultimate Test Drive workshop. We hope you enjoyed the presentation and the labs that we have prepared for you. Please take a few minutes to complete the online survey form to tell us what you think.

Task 1 – Take the online survey

Step 1: In your lab environment, click the **Survey** tab.



Step 2: Please complete the survey and let us know what you think about this workshop.



End of Activity 11.

Appendix-1: Network Diagram

LAB SETUP

UTD-SASE Network Diagram

