Hands-on Workshop

Prisma Access

http://www.paloaltonetworks.com

Last Update: 20191028

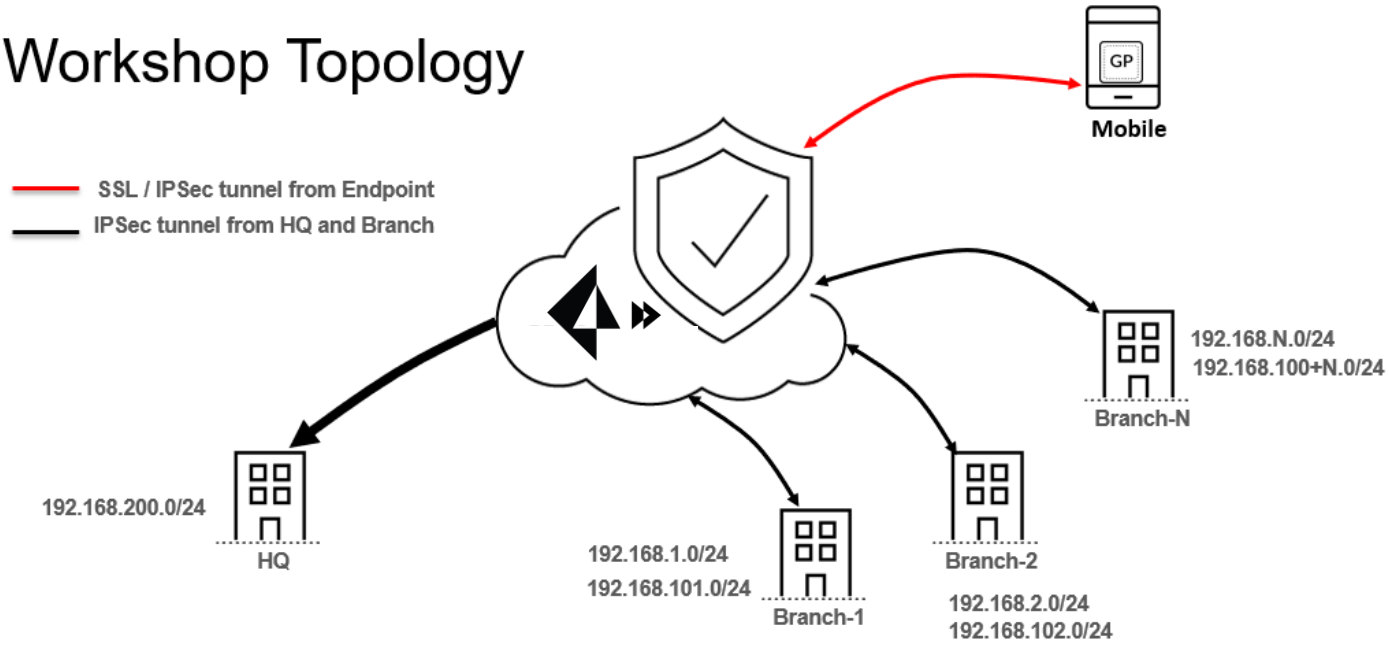
Table of Contents

Workshop Goals

The objective of this workshop is to help you understand Prisma Access, its use cases and get yourselves familiar with how to configure Prisma Access:

- to efficiently secure mobile users' traffic,
- to provide next-gen secure remote access to internal applications
- to secure branch offices consistently and in an operationally efficient way

Network Diagram



Each attendee gets a completely separate environment that would be used to simulate a branch office. The environment includes:

- **NGFW-Branch:** PA VM-Series firewall (this could have been any routing device capable of setting IPSec tunnel using standard IKE / IPSec)
- **win7-subnet1:** Windows VM in Subnet 1
- **win7-subnet2:** Windows VM in Subnet 2
- **win7-mobile:** Windows VM (that simulates a remote mobile user)
- **Panorama:** Read-only access to Panorama.

How to access your environment

- Login credentials for NGFW-Branch
  - Username / Password: admin / Ignite19
- Login credentials for win7-subnet1, win7-subnet2, win7-mobile & Panorama:
  - Username / Password: student / Ignite19
- Login Credentials for GlobalProtect:
  - Username: employee[ID] (where ID is your student-id / seat number)
  - Password: Ignite19

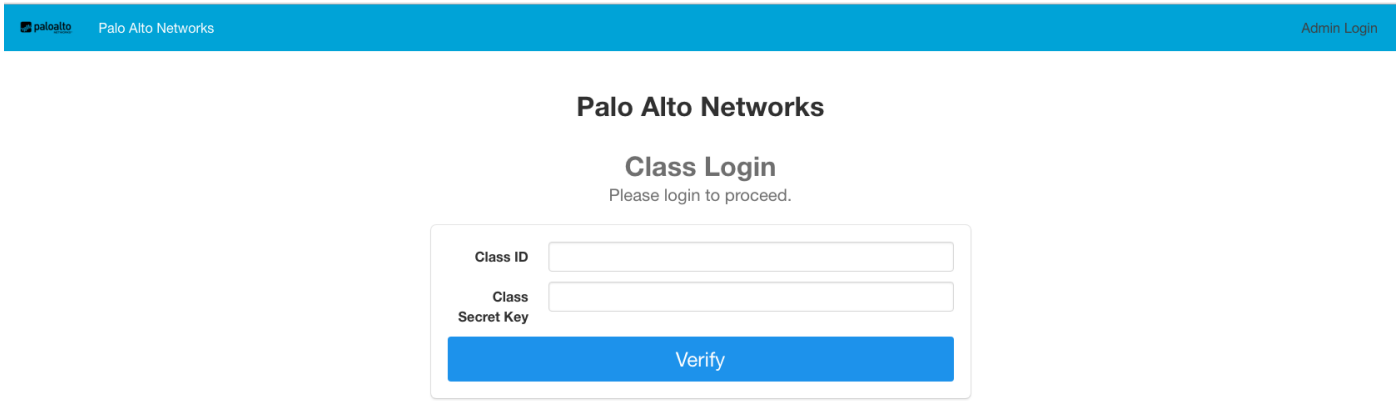
Activity 0 – Log in to the Workshop Portal

In this activity, you will:

- Log in to the Hands-On Workshop from your laptop
- Test connectivity

Step 1: First, make sure your laptop is installed with a modern browser that supports HTML5. We recommend using the latest version of Firefox, Chrome or Internet Explorer.

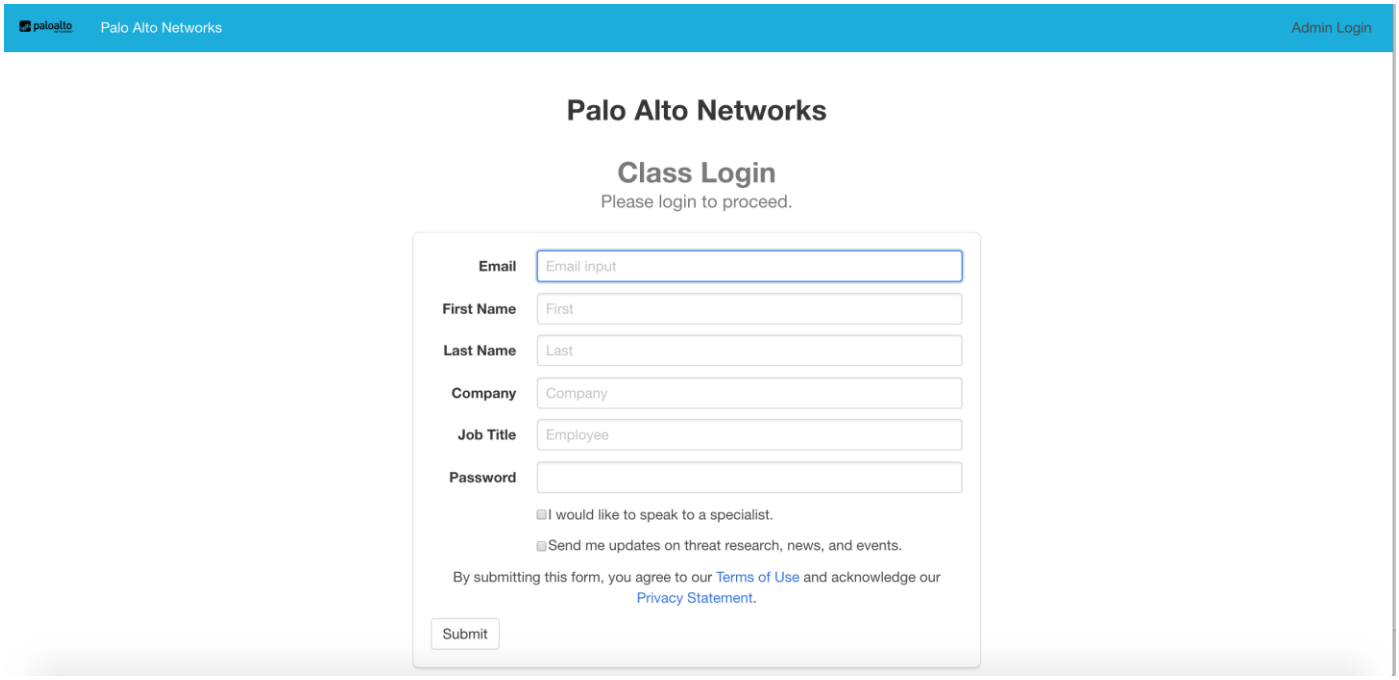
Step 2: Go to class URL. The instructor will provide you with the class URL and login credentials.



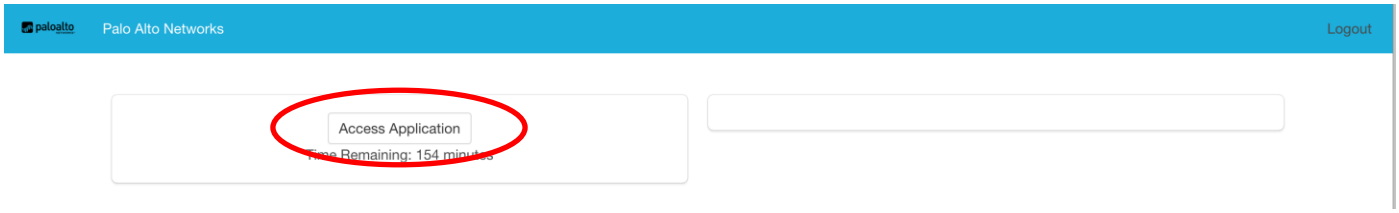
Step 3: Enter your assigned Class ID and Class Secret Key.

Step 4: Click **Verify** to start your lab environment.

Step 5: Fill the Class Login form and click Submit



Step 6: Click Access Application



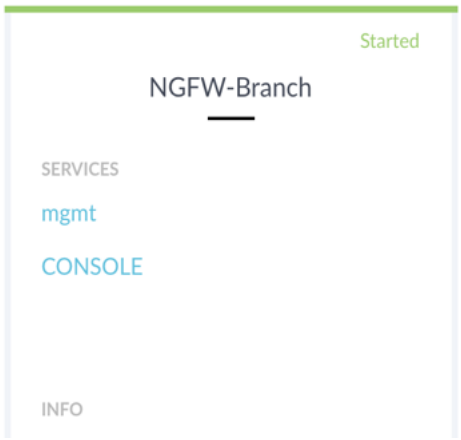
Step 7: You should see 5 VMs in the next screen.

NGFW-Branch and **Panorama** GUI can be accessed using their **mgmt**. link. **win7-mobile, win7-subnet1** and **win7-subnet2** can be accessed via their corresponding **Console** link.

Activity 1 – Configure On-Premise Network

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.

1. **Change the IPv4 interface addresses for ethernet1/2 and ethernet1/4**
    i. Login to VM-Series firewall web console (Credentials: ***admin / Ignite19)***
    Step 1: Click on the **mgmt** link for the **NGFW-Branch** virtual machine.



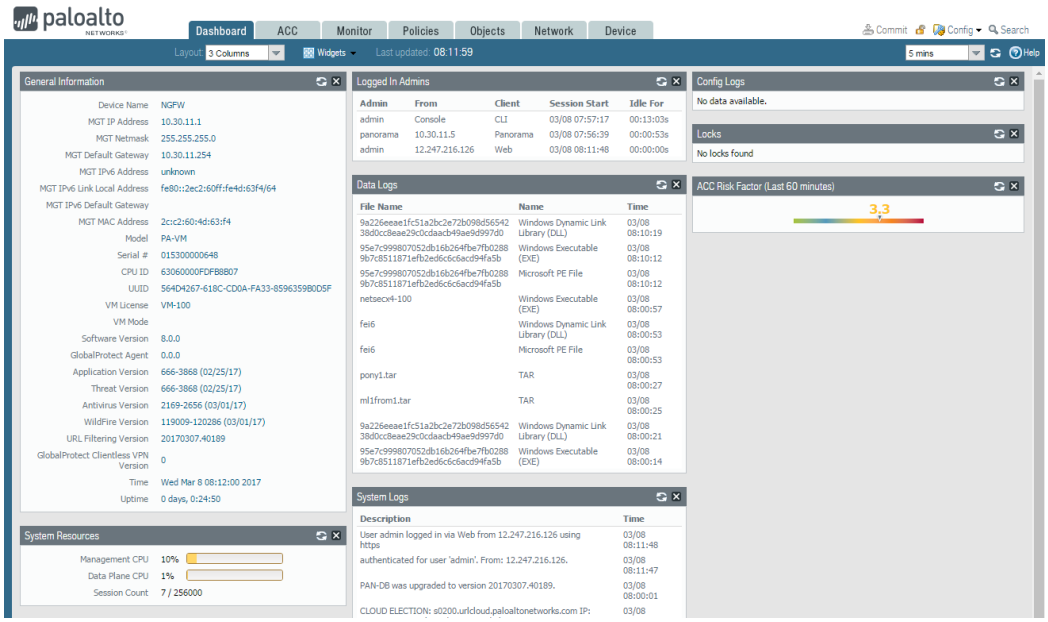
Accept any self-signed certificate prompt that you may get.

Step 2: You are now on the NGFW login page.

Log in with the following:

Name: ***admin***

Password: ***Ignite19***



b. Navigate to Network > Interfaces > Ethernet Page. You will see that all 4 interfaces are down:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router
ethernet1/1	Layer3			172.16.1.1/24	default
ethernet1/2	Layer3	Ping		192.168.99.1/24	default
ethernet1/3	Layer3			172.16.2.1/24	default
ethernet1/4	Layer3	Ping		192.168.199.1/24	default

c. Click ethernet1/2
   i. Click IPv4
   ii. Update the IP address from 192.168.99.1/24 to 192.168.**X**.1/24
   X is your student-ID.

   For example, if your student-ID is 1 then set it to 192.168.1.1/24
   And if your student-ID is 25 then set it to 192.168.25.1/24

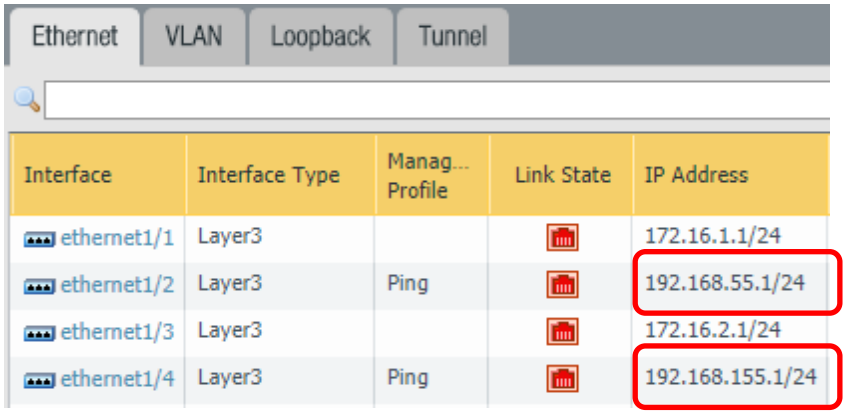
   iii. Click Advanced tab
   iv. Change the Link State to UP

d. Click ethernet1/4
   i. Click IPv4
   ii. Update the IP address from 192.168.199.1/24 to 192.168.**Y**.1/24
   Y is your student-ID+100.

   For example, if your student-ID is 1 then set it to 192.168.101.1/24
   And if your student-ID is 25 then set it to 192.168.125.1/24

   iii. Click Advanced tab
   iv. Change the Link State to UP

For example, for student 55, after the change it would look like this:



e. Set Link State of interfaces ethernet 1/1 and ethernet 1/3 to UP
   i. Click ethernet1/1
   ii. Click Advanced tab
   iii. Change the Link State to UP
   iv. Repeat this for ethernet 1/3

2. Change the IPv4 interface addresses for tunnel.1 and tunnel.2

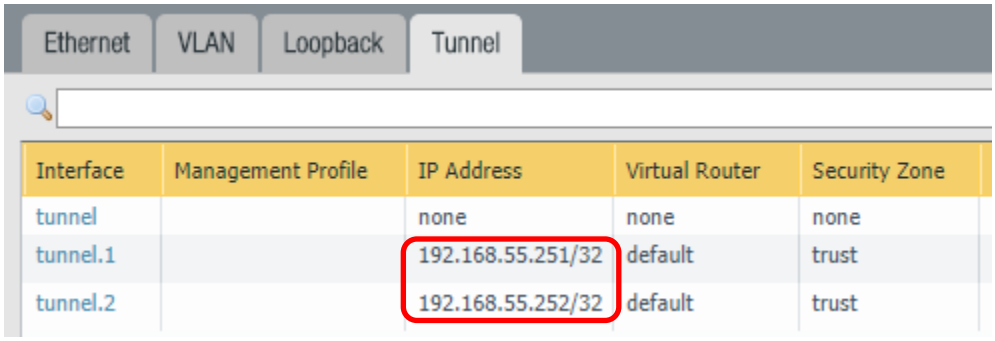
a. In the VM-Series firewall, Navigate to Network > Interfaces > Tunnel page
b. Click tunnel.1
   i. Click IPv4
   ii. Update the IP address from 192.168.99.251/24 to 192.168.**X**.251/32
   X is your student-ID.

   For example, if your student-ID is 1 then set it to 192.168.1.251/32
   And if your student-ID is 25 then set it to 192.168.25.251/32

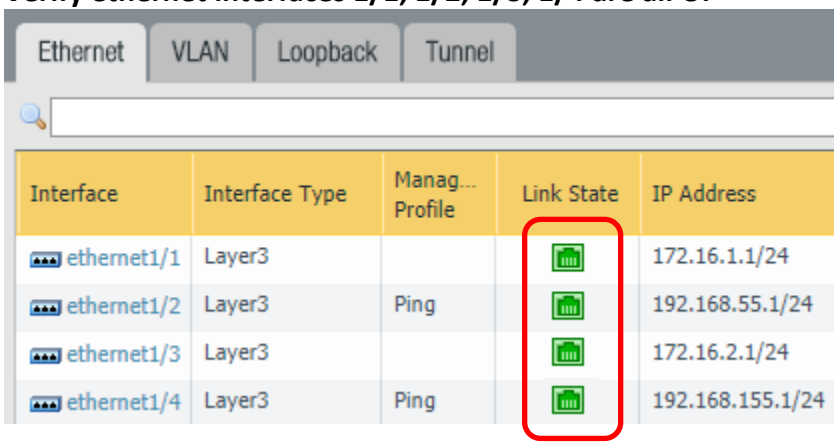
c. Click tunnel.2
   i. Click IPv4
   ii. Update the IP address from 192.168.199.252/24 to 192.168.**X**.252/32
   X is your student-ID

   For example, if your student-ID is 1 then set it to 192.168.1.252/32
   And if your student-ID is 25 then set it to 192.168.25.252/32

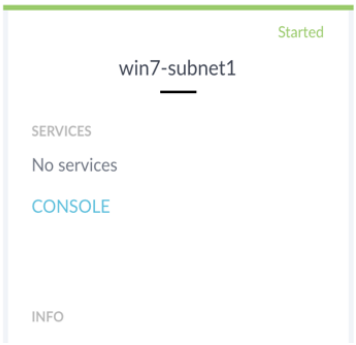
For example, for student 55, after the change it would look like this:



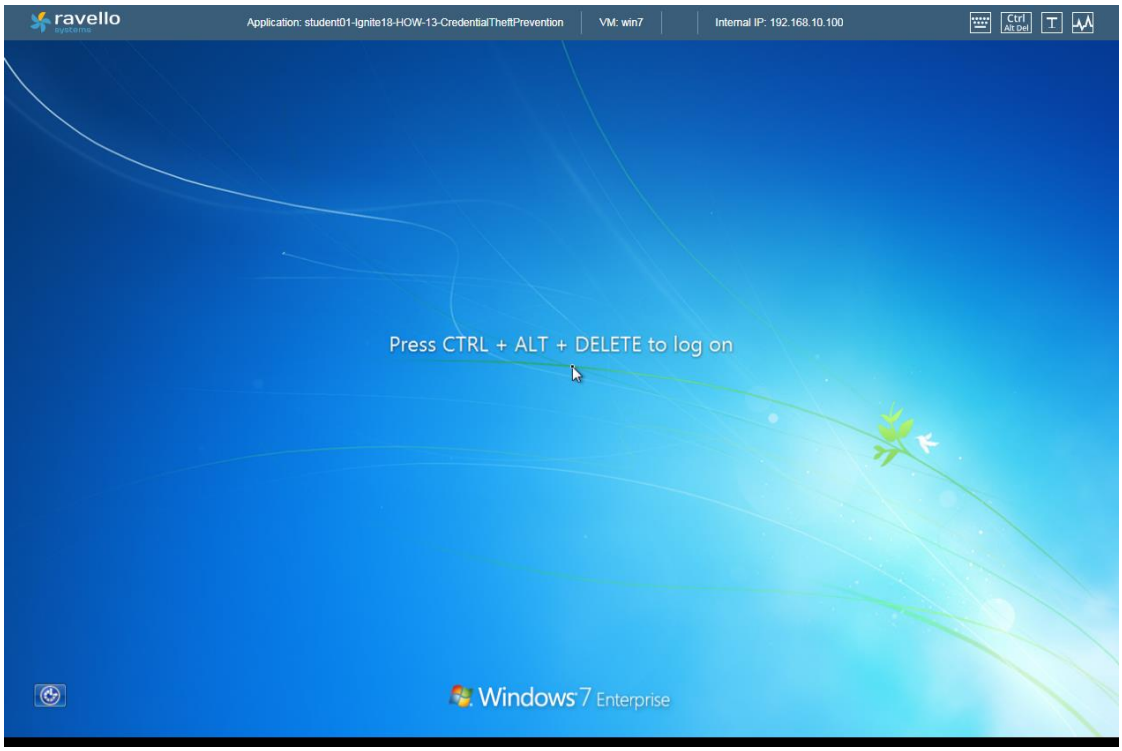
3. **Commit** your changes.
4. **Verify ethernet interfaces 1/1, 1/2, 1/3, 1/4 are all UP**



5. **Update Branch Network Subnets**
    a. **Set the IP address for win7-subnet 1**
        i. Log in to **win7-subnet1** (***student / Ignite19***)
        Step 1: Click on the **CONSOLE** link for the **Windows** virtual machine. This will open a new window. You may need to disable pop-up blockers on your browser.



Step 2: You will be connected to the **Windows desktop** through your browser.



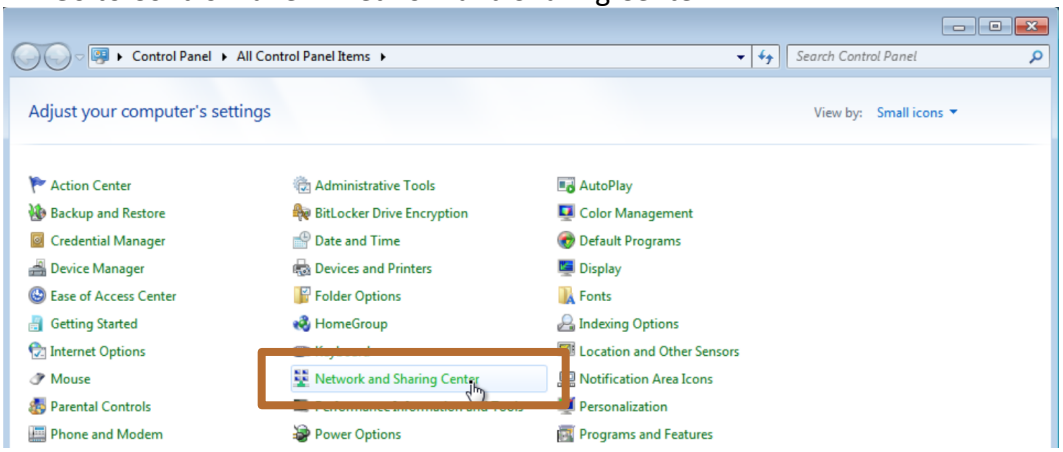
Click the **Ctrl Alt Del** 

icon in the upper right-hand corner.

Step 3: Log in with the following credentials:

Username: ***student***
Password: ***Ignite19***

ii. Go to Control Panel > Network and Sharing Center



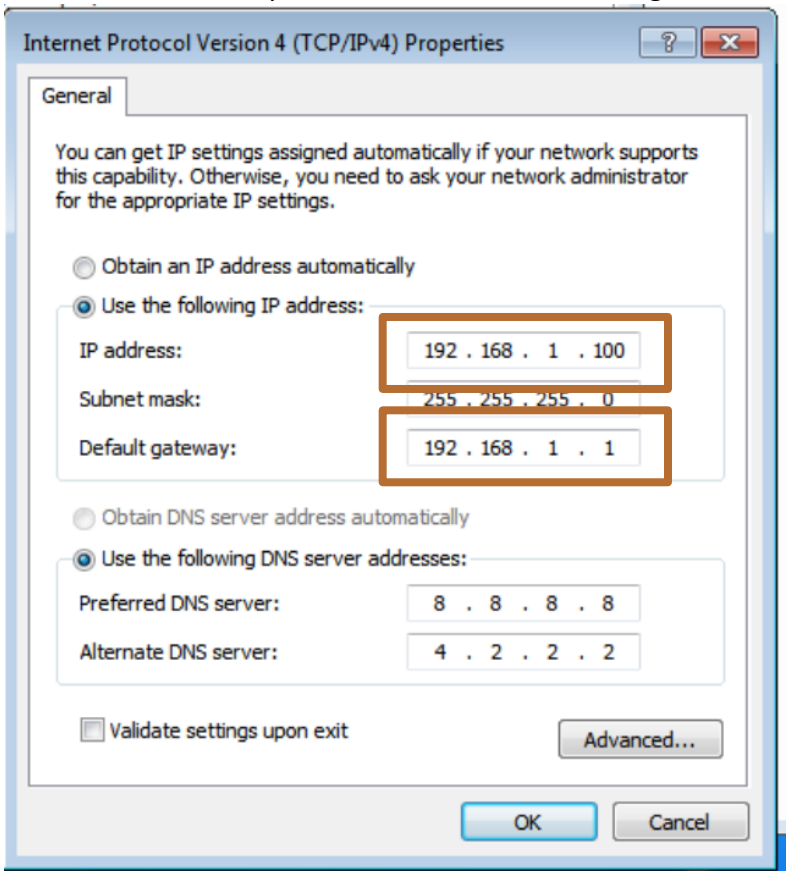
iii. Click on Change adapter settings
iv. Double click Local Area Connection 3
v. Click Properties
vi. Select Internet Protocol Version 4 (TCP/IPv4)
vii. Click Properties
viii. Update the IP address and the Default Gateway.

1. IP address: 192.168.**X**.100
2. Default Gateway: 192.168.**X**.1

X is your student ID

3. Click OK and then close remaining windows

ix. For example, Student 1, after the change would have



x. Verify you can ping the default gateway.

For example, if you are Student-ID is 1, then Ping 192.168.1.1
And if you are Student-ID is 25, then Ping 192.168.25.1

b. Set the IP address for win7-subnet 2

i. Log in to **win7-subnet2** (***student / Ignite19***)

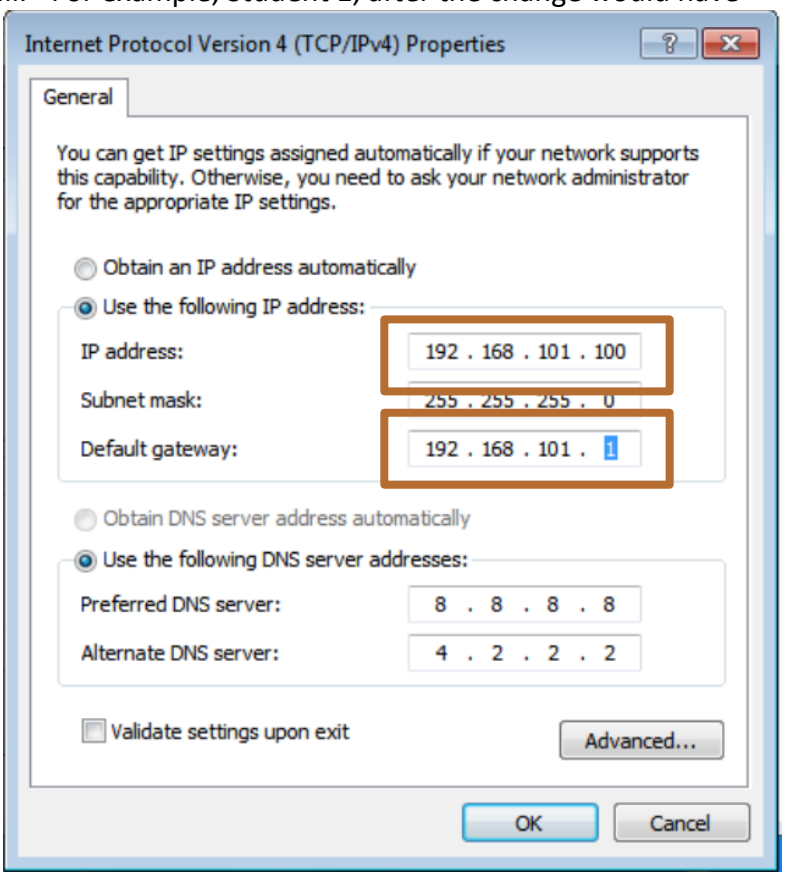
ii. Follow the steps to change the IP address and Default Gateway.

1. IP address: 192.168.**Y**.100
2. Default Gateway: 192.168.**Y**.1

Y is your Student ID + 100

3. Click OK and then close remaining windows.

iii. For example, Student 1, after the change would have



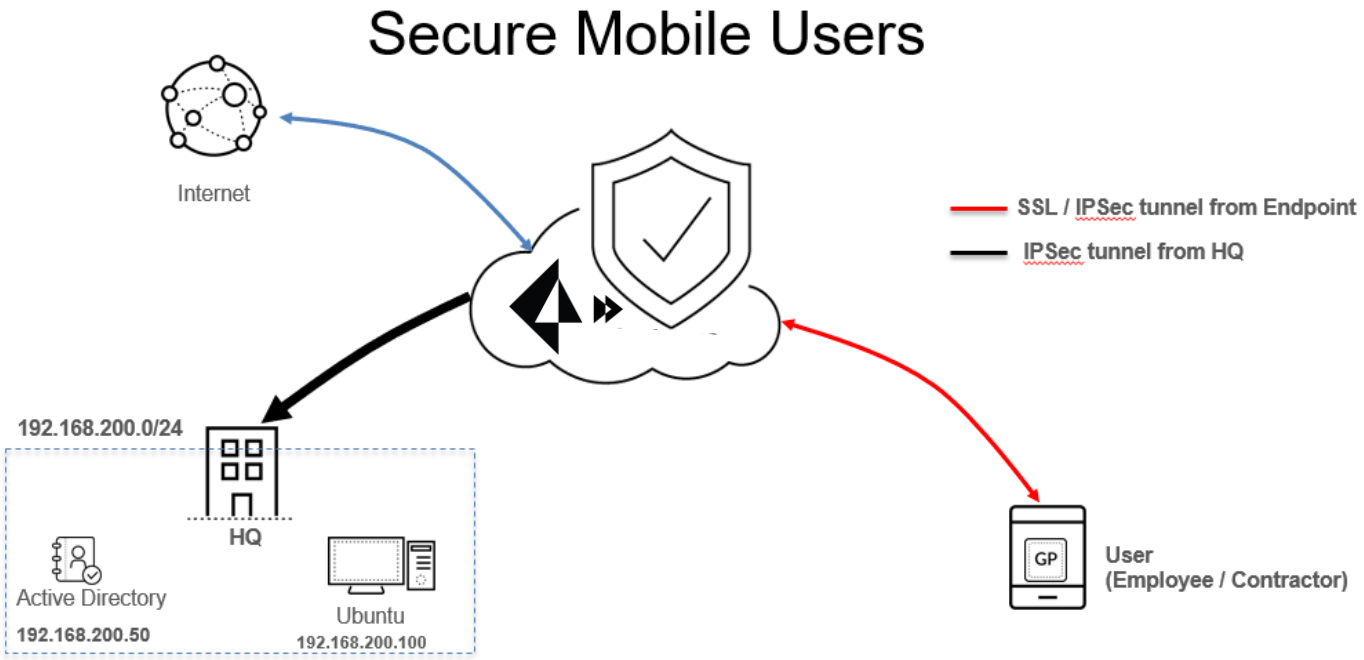
iv. Verify you can ping the default gateway

For example, if you are Student-ID is 1, then Ping 192.168.101.1
And if you are Student-ID is 25, then Ping 192.168.125.1

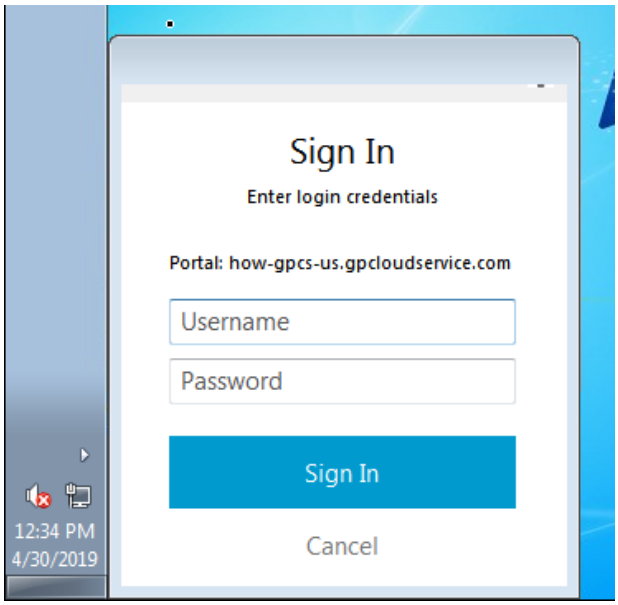
Troubleshooting: If you can't ping successfully, make sure the interfaces ethernet1/1, ethernet1/2, ethernet1/3, ethernet1/4 in your NGFW-Branch are UP.

Activity 2 – Secure Mobile Users Internet Traffic

Prisma Access helps secure your mobile users internet traffic, providing a Clean Internet Pipe. Portals and Gateways are offered across multiple regions in the Cloud. The GlobalProtect Agent on the users' endpoint automatically determines the best Gateway for the user, sets up a tunnel and takes the users' traffic through this tunnel. Security inspection for the users' traffic happens closer to where the user is, removing the need to back-haul users' traffic to HQ or the Data Center (DC) for the purpose of security inspection and threat prevention.



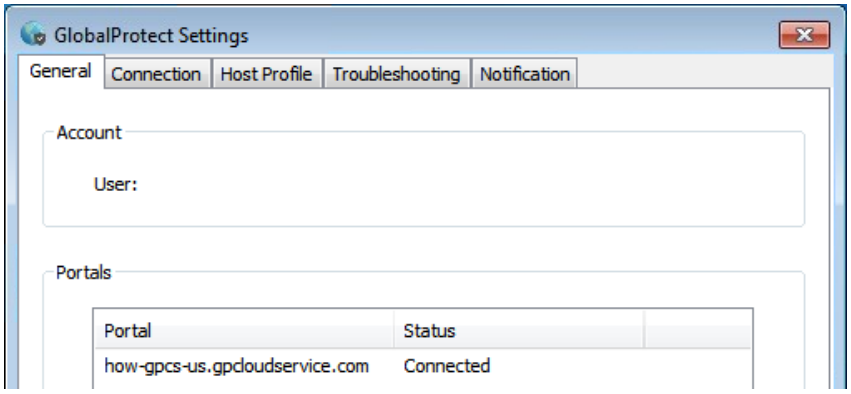
1. Log in to the **win7-mobile** VM (***student / Ignite19***)
2. The GlobalProtect App will be launched, and you will see this screen:



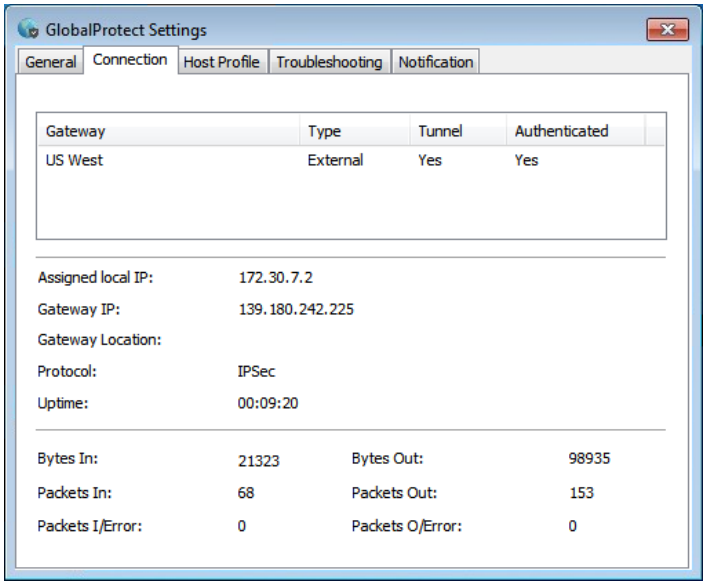
3. Enter the following:
   USERNAME: ***contractor[id]*** PASSWORD: ***Ignite19***
   For example: contractor44 / Ignite19

   Click **Sign In.** A tunnel from your mobile device to GPCS will be established. This will take a minute.

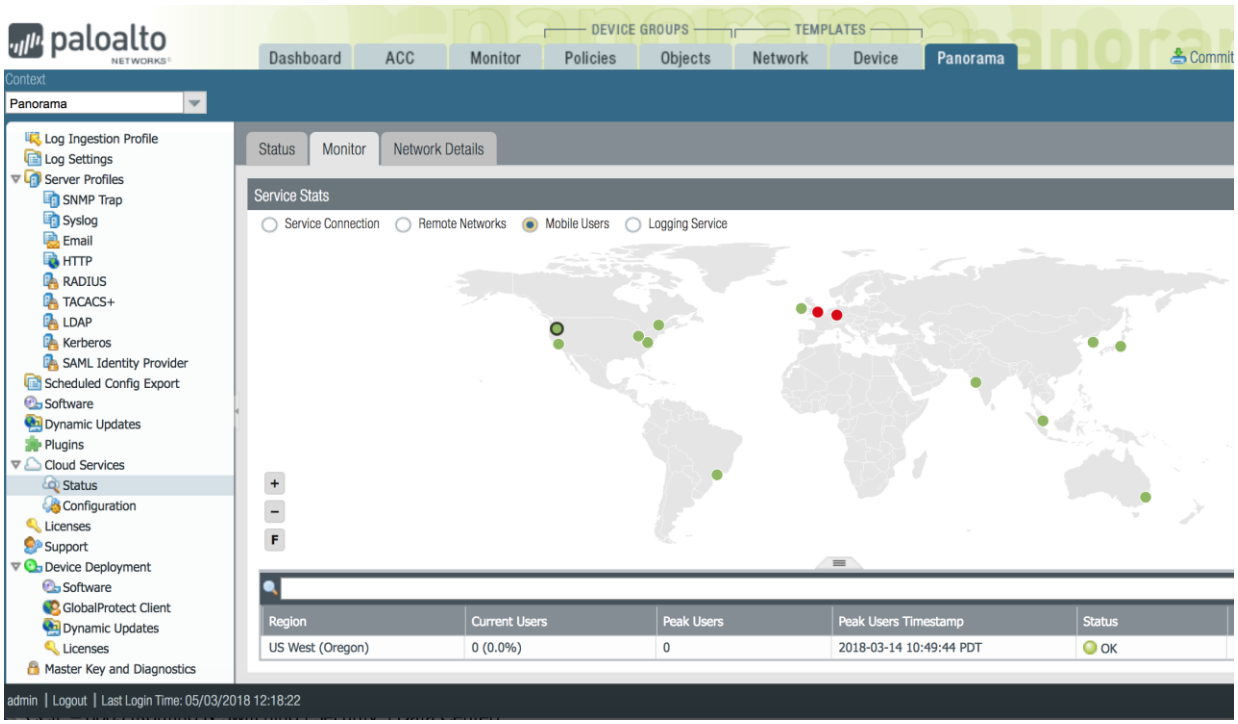
4. Click the hamburger ☰ icon and then **Settings** to bring up the **GlobalProtect Settings** window.



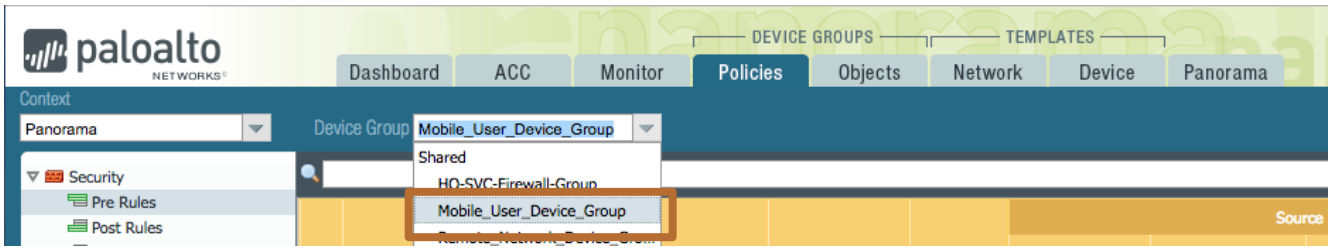
5. Click the **Connection** tab to see the connection details.



6. You will now check to see where students in the class are connected to.
    a. Login to Panorama (student / Ignite19)
    b. Navigate to Panorama > Cloud Services > Status > Monitor > **Mobile Users**
    c. The largest green bubble on the map indicates where the most users are connected to. Click on that bubble, and you will see the number of users connected to that gateway. You are likely connected to that.


paloalto
NETWORKS
DEVICE GROUPS
TEMPLATES
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Panorama
Commit
Context
Panorama
Log Ingestion Profile
Log Settings
Server Profiles
SNMP Trap
Syslog
Email
HTTP
RADIUS
TACACS+
LDAP
Kerberos
SAML Identity Provider
Scheduled Config Export
Software
Dynamic Updates
Plugins
Cloud Services
Status
Configuration
Licenses
Support
Device Deployment
Software
GlobalProtect Client
Dynamic Updates
Licenses
Master Key and Diagnostics
Status
Monitor
Network Details
Service Stats
Service Connection
Remote Networks
Mobile Users
Logging Service
Region
Current Users
Peak Users
Peak Users Timestamp
Status
US West (Oregon)
0 (0.0%)
0
2018-03-14 10:49:44 PDT
OK
admin | Logout | Last Login Time: 05/03/2018 12:18:22

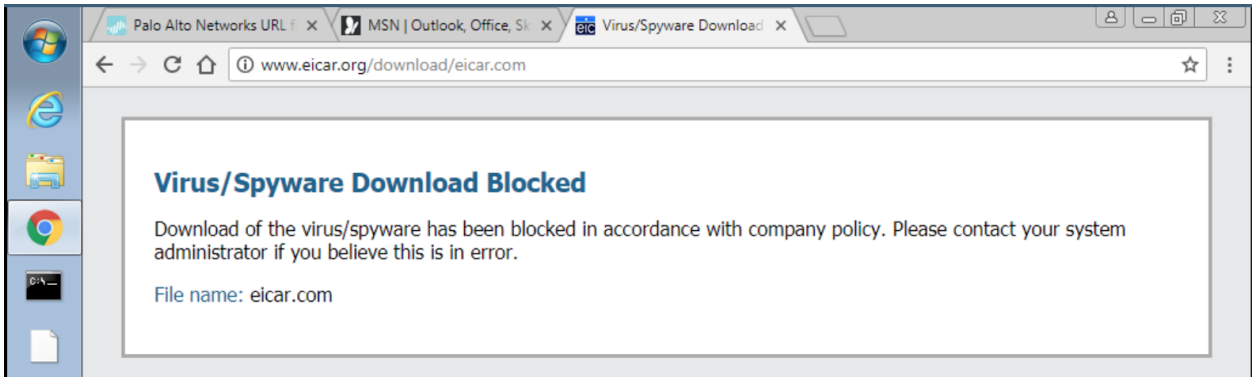
7. In Panorama, review the Security Policies under Mobile Users Device Group.
    a. Navigate to Device Groups > Policies > Mobile_User_Device_Group



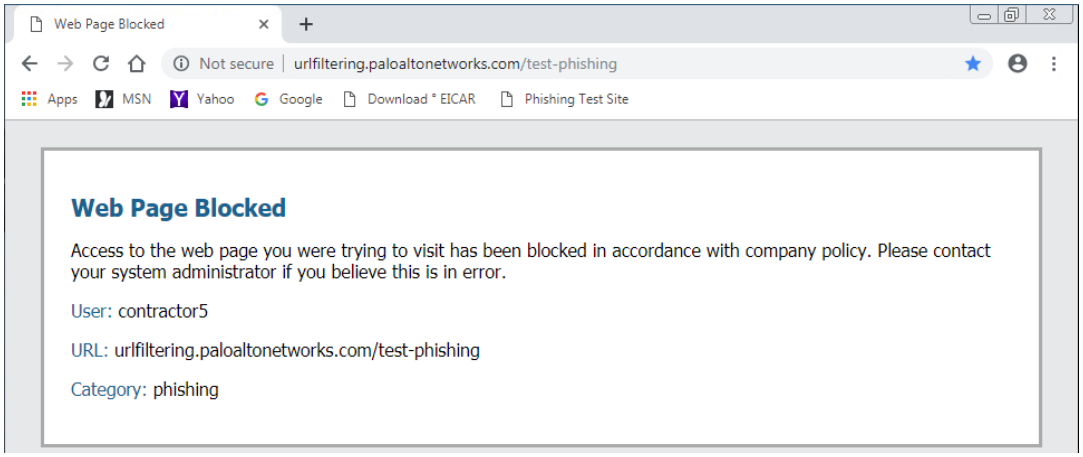
    b. Review the Policies, check the Security Profiles.
    What access does the user (employee or a contractor) have?
    What security features are enabled under the Security Profiles in the Secure-Internet-Traffic policy?

8. From **win7-mobile**, open Chrome and use bookmarks to browse to www.msn.com or www.yahoo.com or www.google.com . You should be able to successfully browse to MSN, Yahoo and Google.

9. Use bookmarks in Chrome to browse to www.eicar.org/download/eicar.com
You should observe that you have been blocked access to the page, as it is identified as a security Threat.



10. Use bookmarks in Chrome to browse to urlfiltering.paloaltonetworks.com/test-phishing
    You should observe that you have been blocked access to the page, as it is identified as a phishing URL. If it does not work, make sure you access the URL with http:// and not https://



Summary:

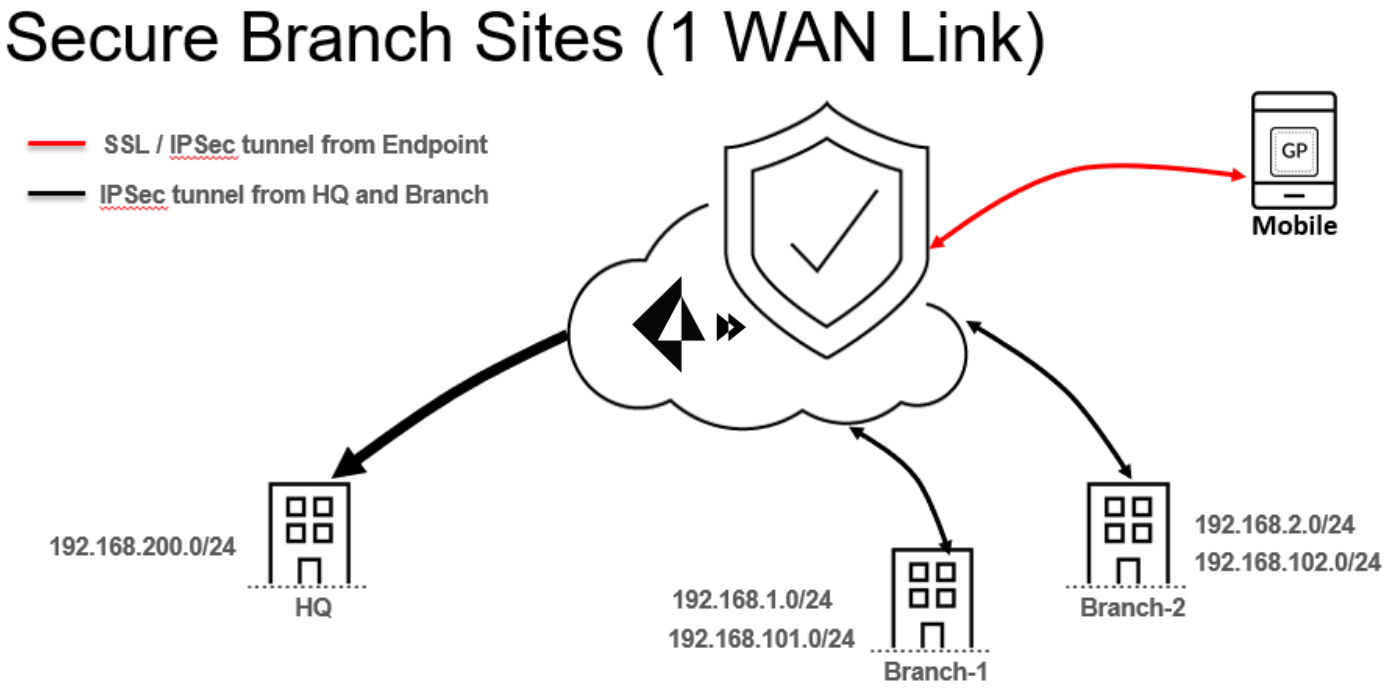
- ✓ Security is delivered from the cloud and closer to where the users are.
- ✓ Security capabilities such as URL Filtering, Threat Prevention and WildFire are included.
- ✓ Removes the need to back-haul users traffic to the HQs or the data center.

Activity 3 – Secure Branch Sites (1 WAN Link)

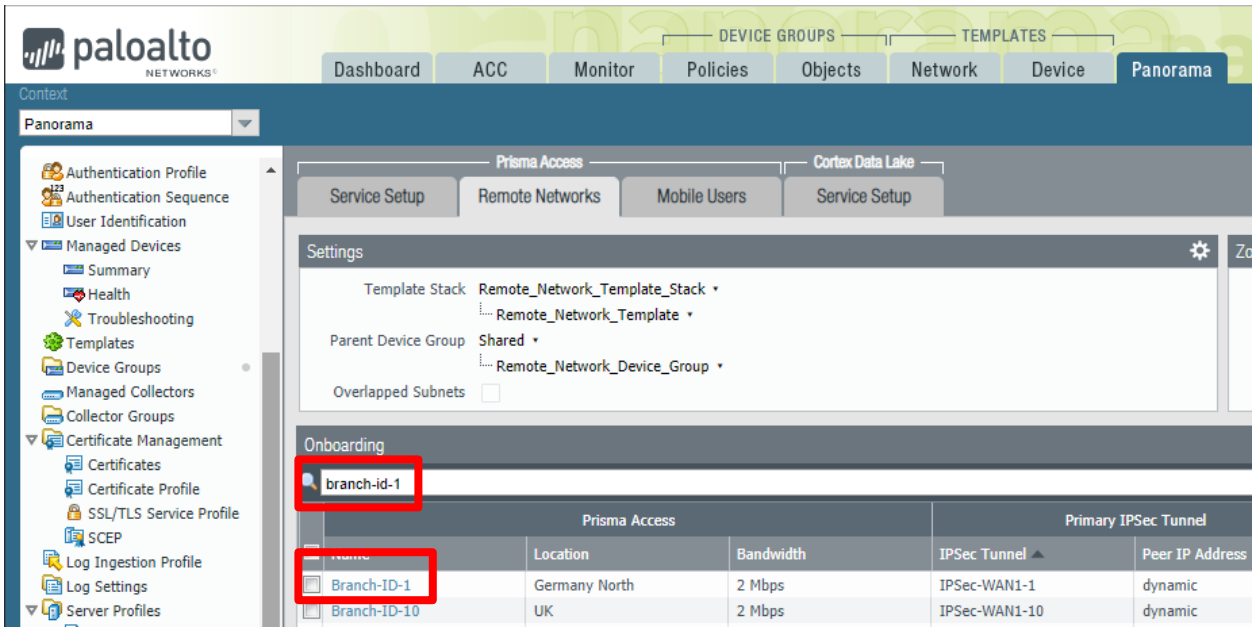
Prisma Access provides consistent security for all your branch offices. All the branch sites have the same set of security policies and controls. You can on-board your branch sites to any of the regions in the Cloud that is supported by Prisma Access.

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

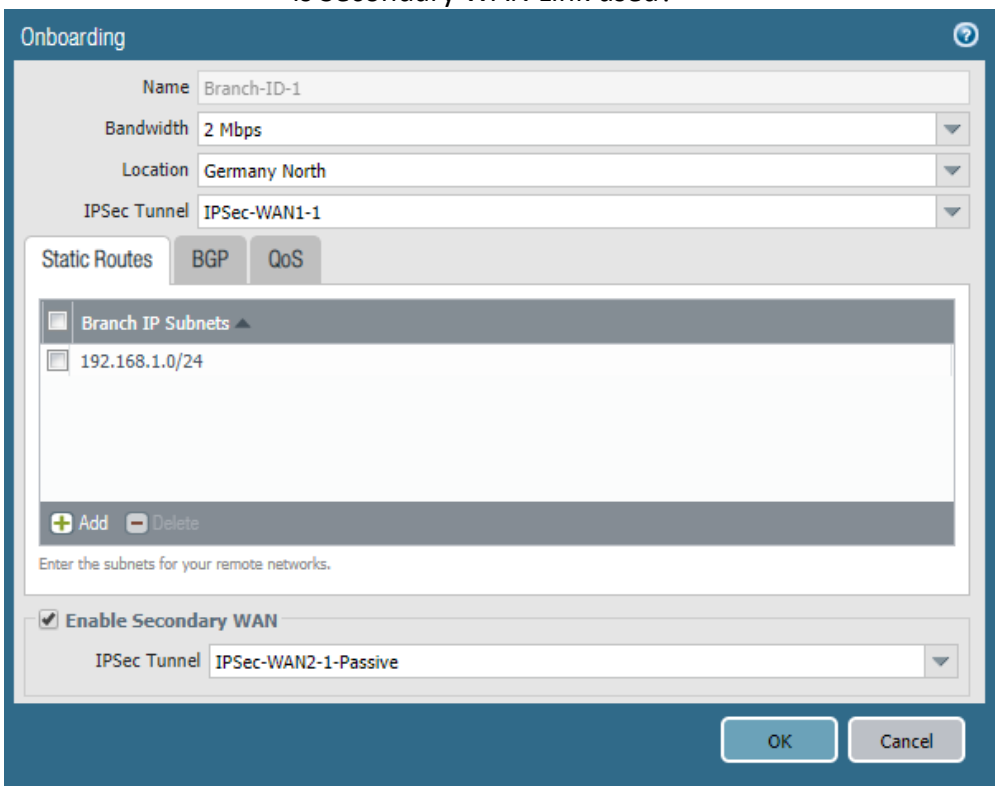
In this workshop you will use VM-Series firewall as the on-premise device.



1. Login to Panorama (***student / Ignite19***)
2. Navigate to Panorama > Cloud Services > Configuration > Remote Networks
3. Search for the configuration corresponding to your branch.

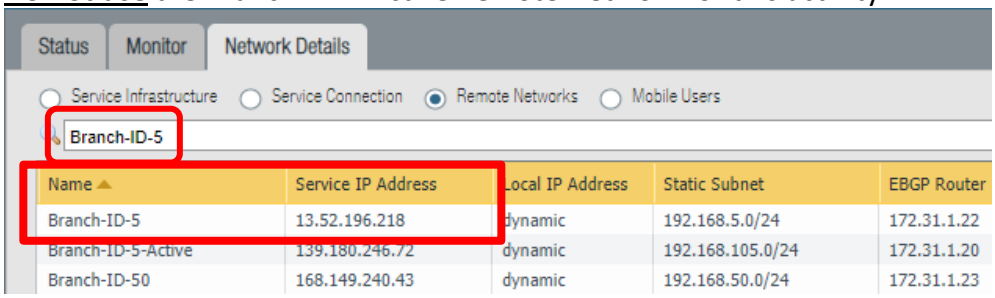


4. Review the configuration for Branch-ID-[student-ID].
    - What Bandwidth should be used for your branch?
    - What Region in the cloud should your branch set up a tunnel with?
    - What IPSec Tunnel profile should your branch use?
    - What are your Branch Subnets that can be reached via this tunnel?
    - Is Secondary WAN Link used?

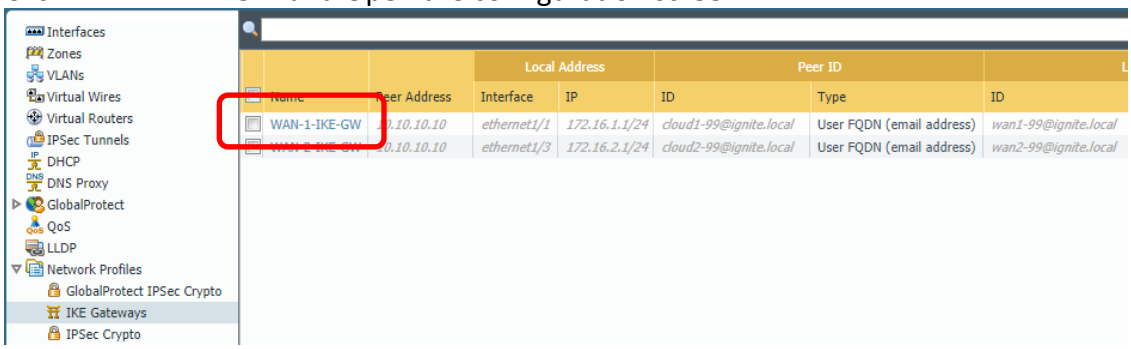


5. Identify the Service IP Address of the IPSec Peer in the Cloud. Service IP address is the IP address of the instance in GPCS to which you need to set up an IPSec tunnel from your branch.

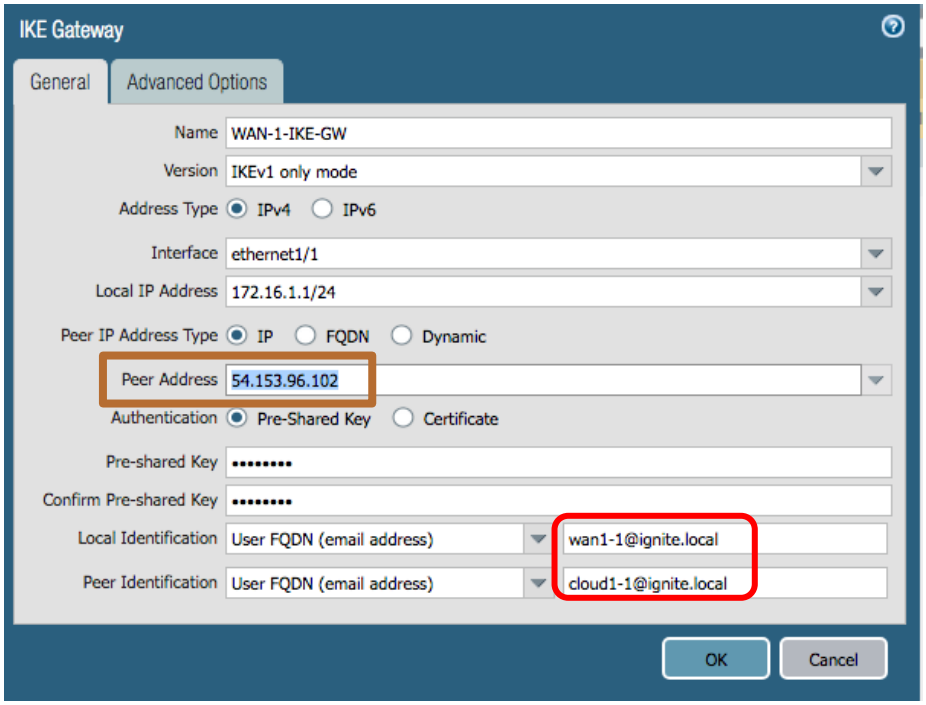
a. Navigate to Panorama > Cloud Services > Status > Network Details > Remote Networks
b. Search for your Branch and get the corresponding Service IP Address and write it down. You will need this later.
Do not use the Branch-ID-*-Active Remote Network for this activity.



6. Set up IPsec tunnel to that Service IP Address in GPCS using 1st WAN link (Ethernet1/1)
   a. Login to on-premise device (NGFW-Branch in this workshop)
      i. Credentials (***admin / Ignite19***)
   b. Navigate to Network > Network Profiles > IKE Gateways
   c. Click WAN-1-IKE -GW and Open the configuration screen

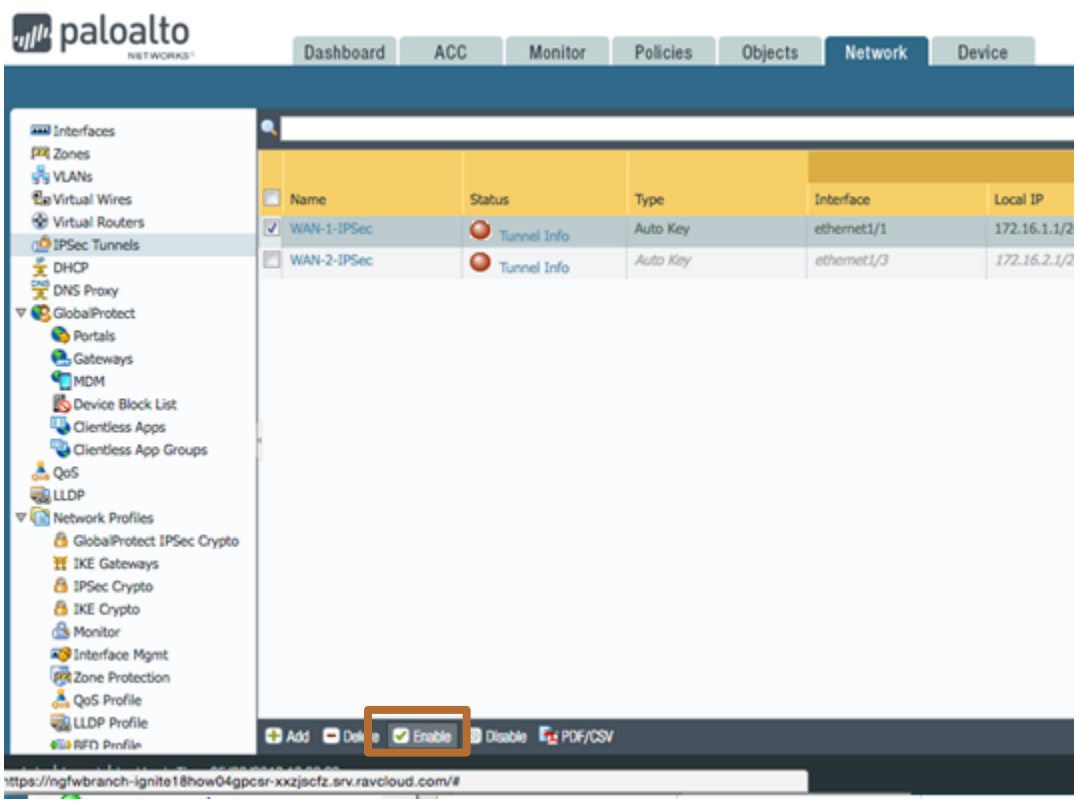


   d. Update the Peer Address (10.10.10.10) with the Service IP Address you obtained from the Panorama.
   Also change the wan1-99@ignite.local and cloud1-99@ignite.local identifiers, replacing 99 with your student-id. For example: wan1-1@ignite.local and cloud1-1@ignite.local for student ID #1

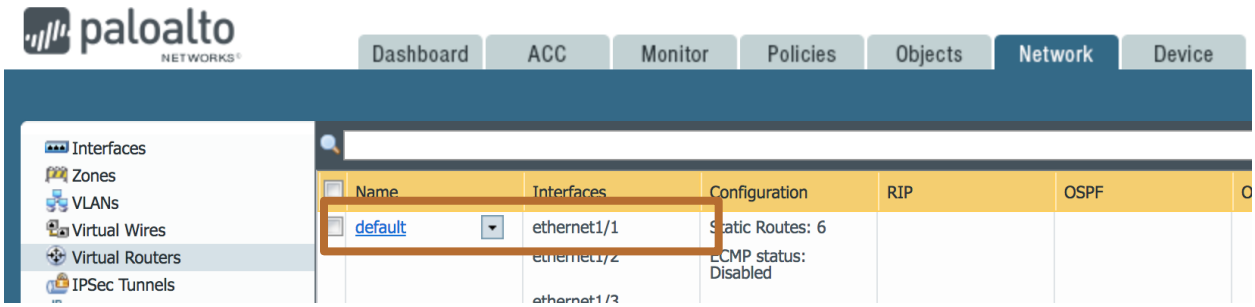


e. Select WAN-1-IKE-GW and Enable it.

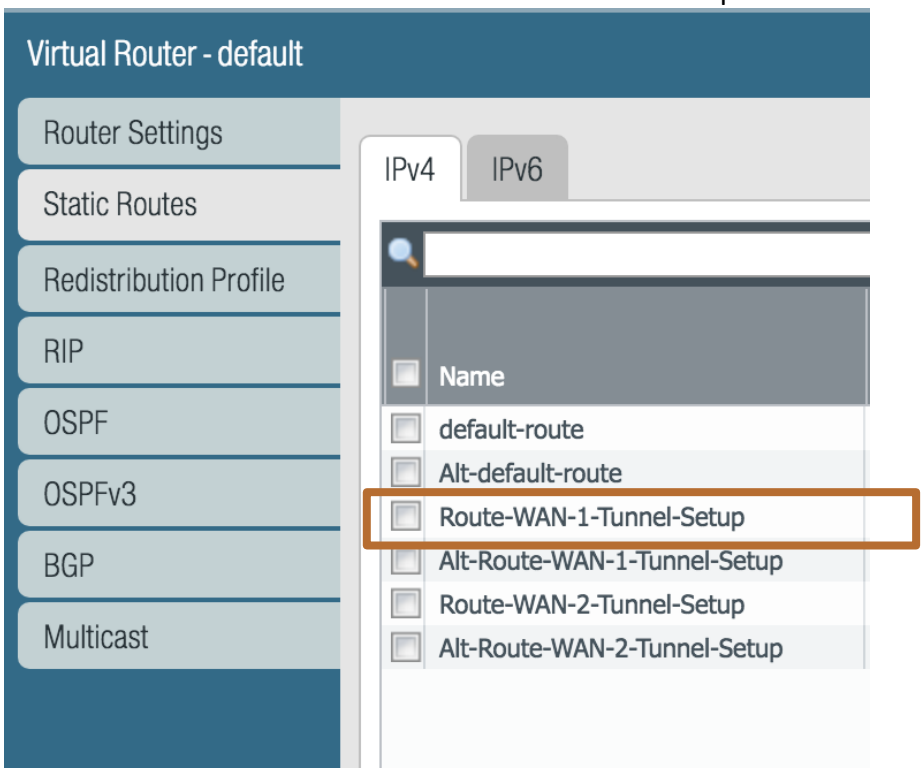
f. Go to Network > IPSec Tunnels and Select WAN-1-IPSec and Enable it.



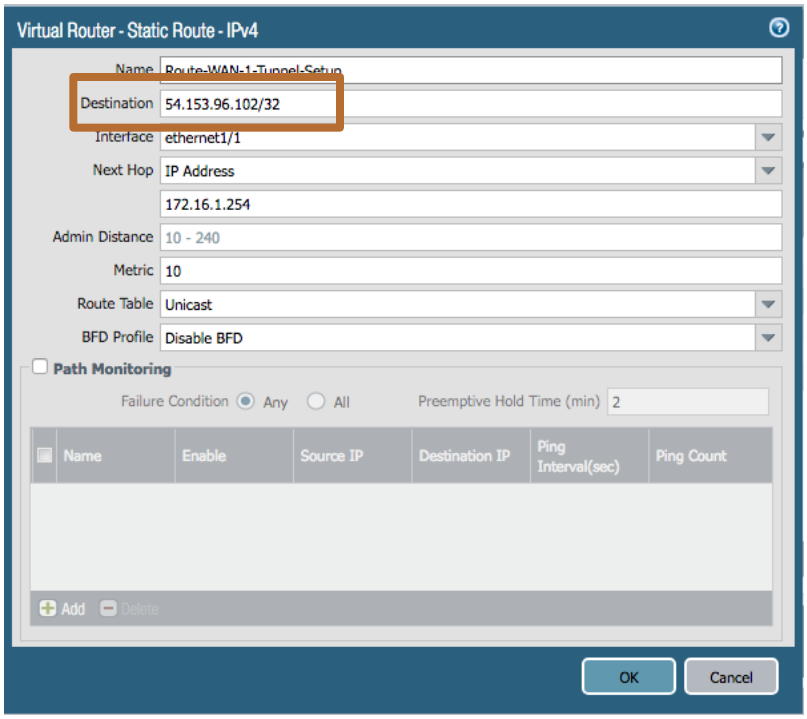
7. Update the Routing Table
    a. Navigate to Network > Virtual Routers > default



    b. Click Static Routes and Click Route-WAN-1-Tunnel-Setup

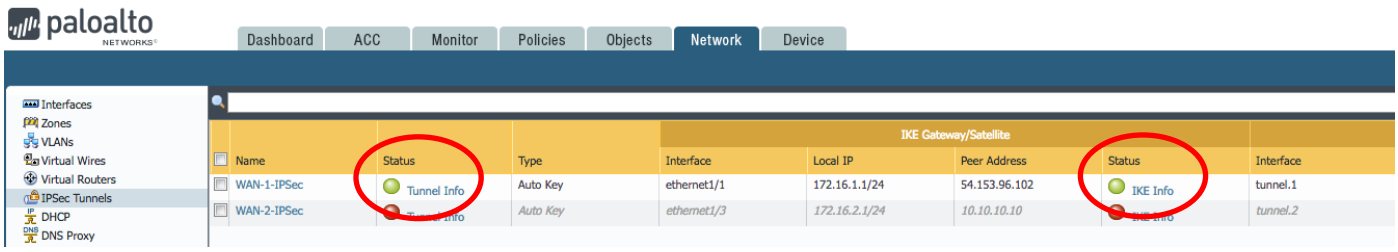


    c. Update the Destination with Service IP Address you obtained from the Panorama for your Branch. Please use /32 address. This will allow the tunnel to be set up with Prisma Access over ethernet1/1



d. Commit the changes on the VM-Series Firewall.

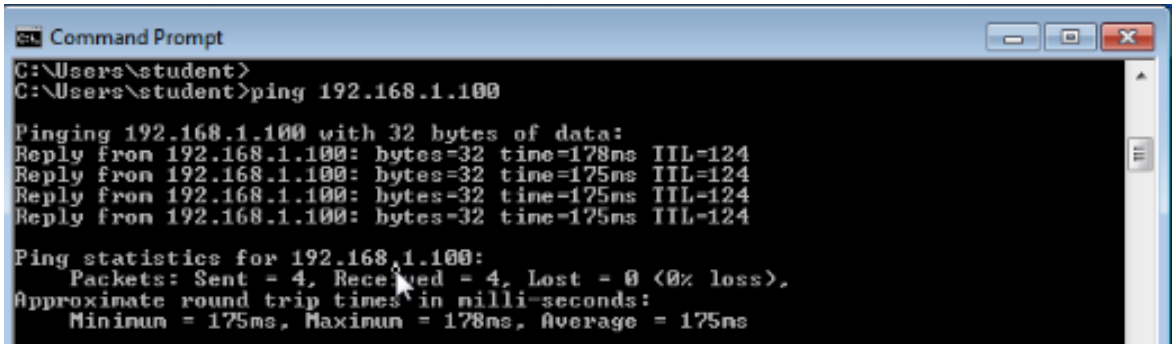
8. After the successful commit, Verify Tunnel is UP
    a. Navigate to Network > IPSec Tunnels and verify Tunnel Info and IKE Info are green



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

- IKE gateway settings - make sure you have the correct Peer IP address and the peer identifier.
- Confirm the IKE gateway and IPSec tunnels are enabled.
- Verify the Virtual Router settings are specified as above
- Check the System Logs and determine if IKE phase 1 and IKE phase 2 came up.

9. **Verify your branch office is secured**
    a. From **win7-mobile** VM, as a remote user (contractor[id]) connected to Prisma Access, access resources inside your branch. To access win7-subnet1, Ping 192.168.<student-id>.100

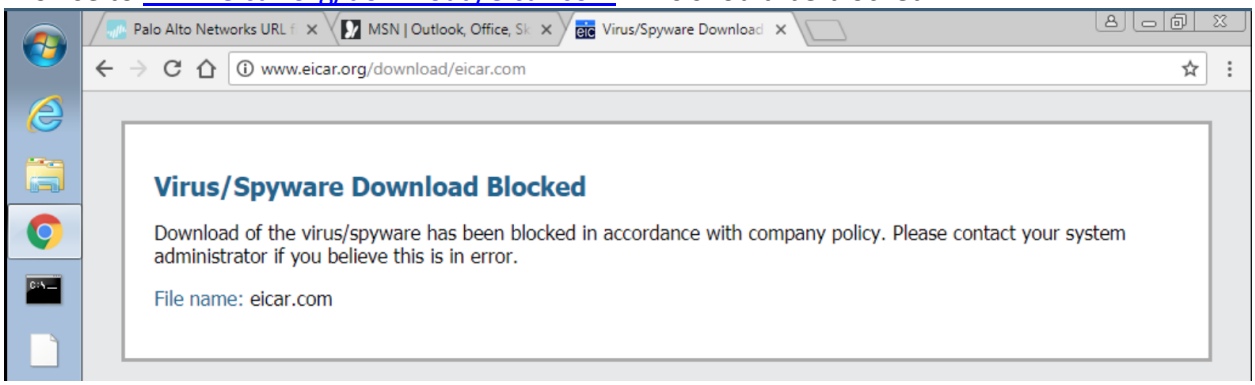


At this time, you should be able to access other branch resources as well, if they are connected to Prisma Access. For example: 192.168.25.100 if Student #25 has completed the tunnel set up successfully.

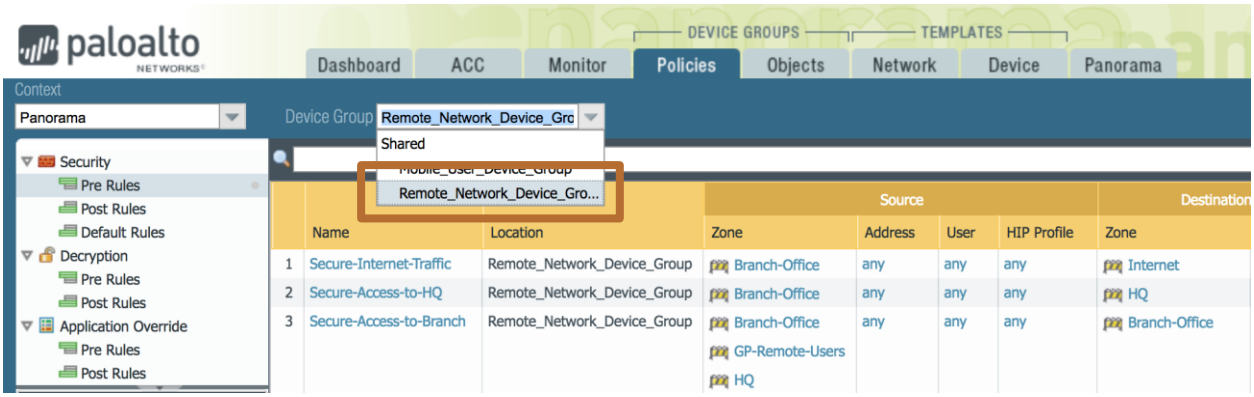
Troubleshooting: If you can't ping successfully, make sure that you are :

- Connected to the correct Portal address for the class
- You are connected as employee[ID] GlobalProtect

10. As a user inside the branch, access internet
    a. Log in to win7-subnet1 VM (***student / Ignite19***)
    b. Browse to www.yahoo.com. This should be successful
    c. Browse to www.eicar.org/download/eicar.com. This should be blocked.



    d. In the Panorama, review the Security Policies for Remote_Network_Device_Group.



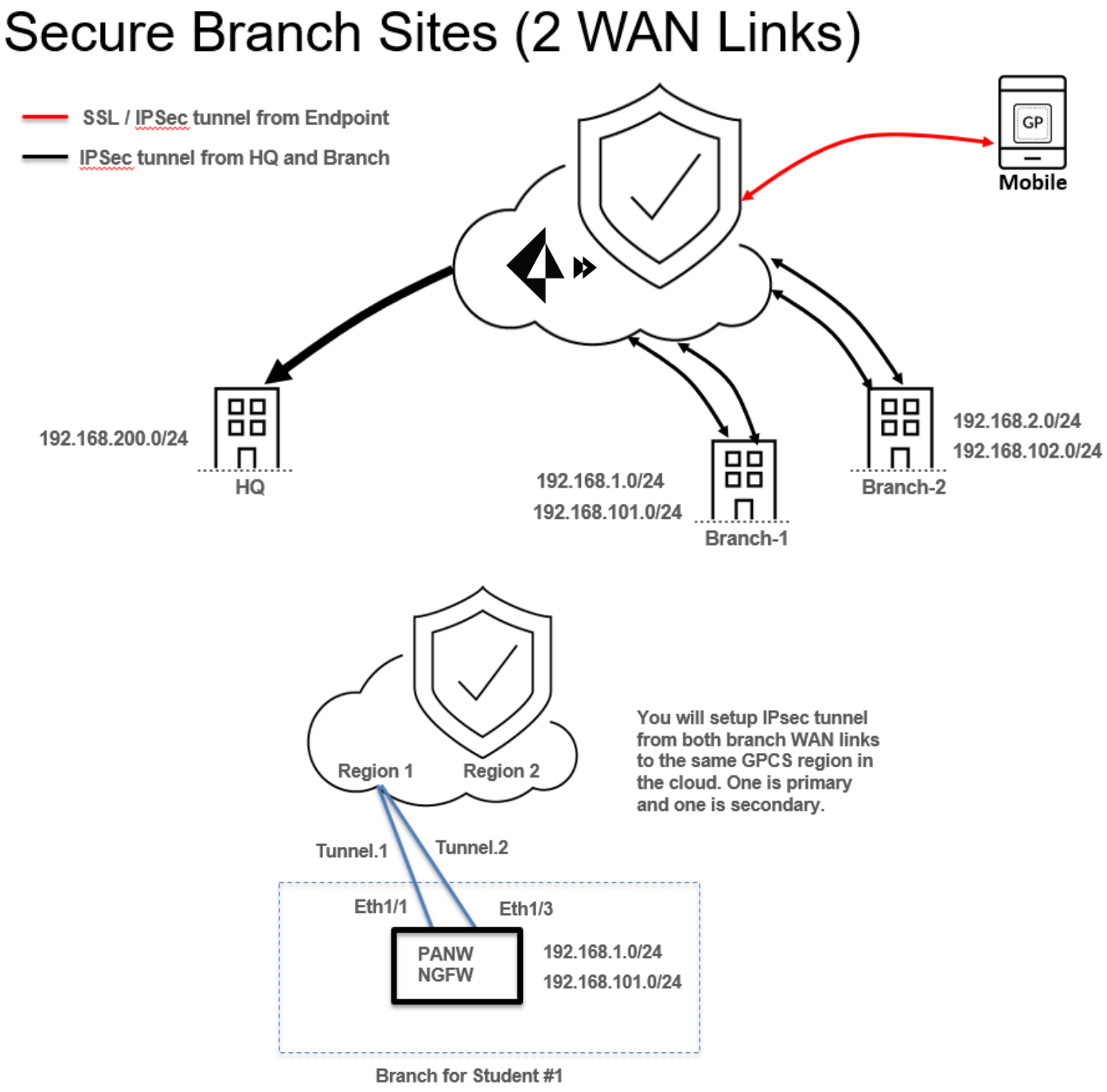
11. As a user inside the branch, access HQ.
    a. From win7-subnet1 Ping 192.168.200.50 should be successful.

Summary:

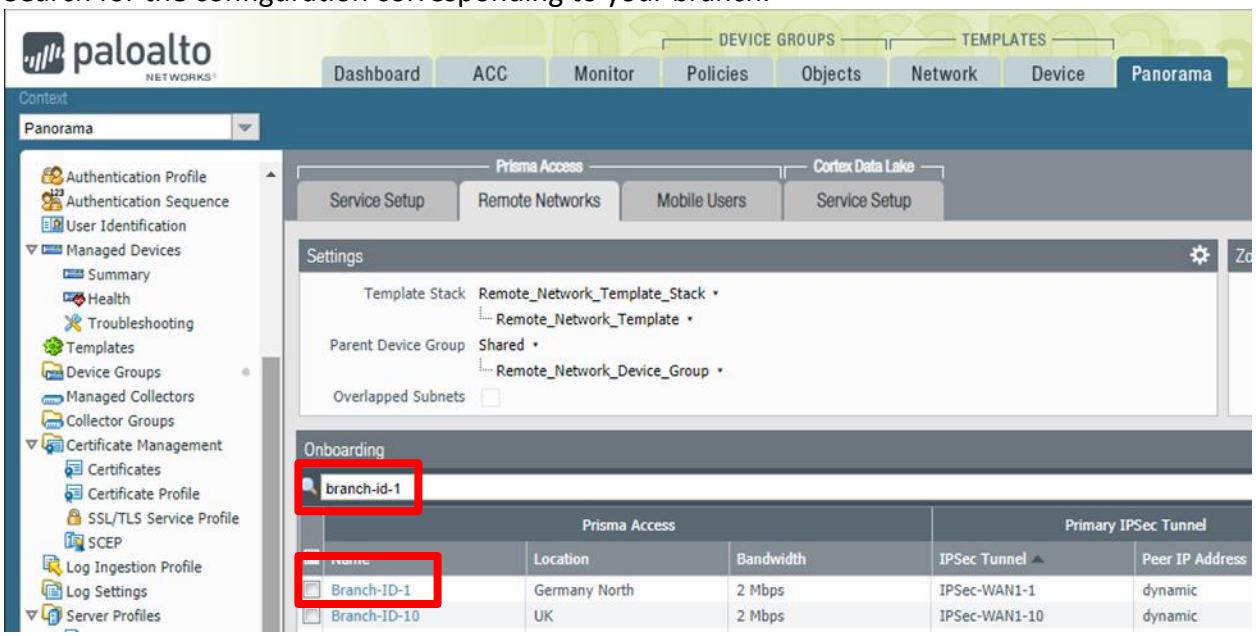
- ✓ Branch offices secured by Prisma Access
- ✓ Secured consistently and operationally efficiently
- ✓ Enables secure communication between
  - Remote mobile users and the branch
  - Remote branch offices
  - Remote branch offices and HQ

Activity 4 – Securing Branch Offices with 2 WAN Links (Primary / Secondary)

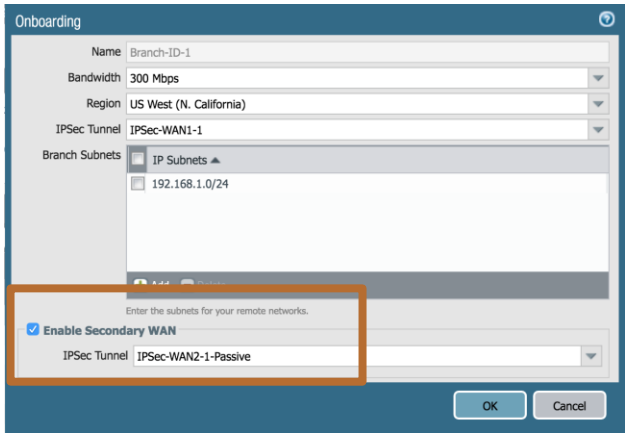
You can on-board your remote network or branch office using more than 1 WAN link. In this activity, you will on-board using 2 WAN links and use the 2nd WAN link as a Secondary or Back-up. The Secondary Tunnel will become active in case the tunnel through Primary WAN link is identified as DOWN.



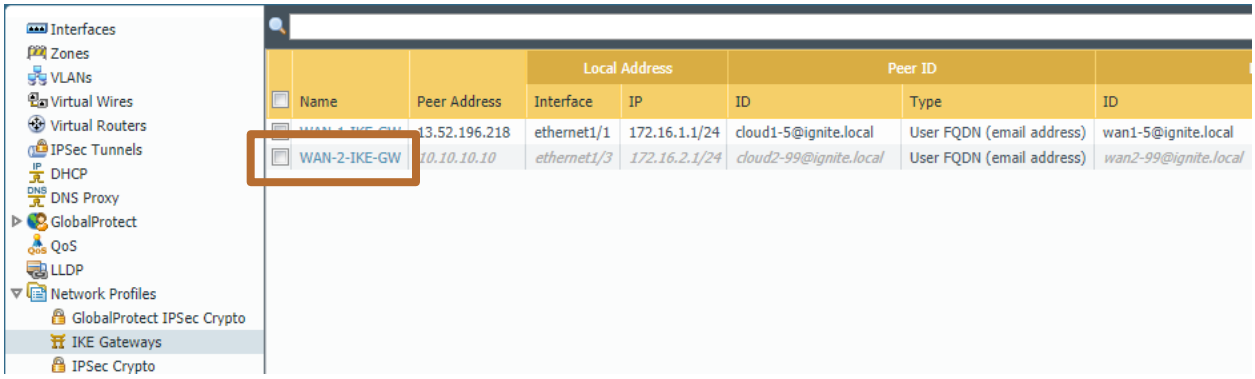
1. Login to Panorama (***student / Ignite19***)
2. Navigate to Panorama > Cloud Services > Configuration > Remote Networks
3. Search for the configuration corresponding to your branch.



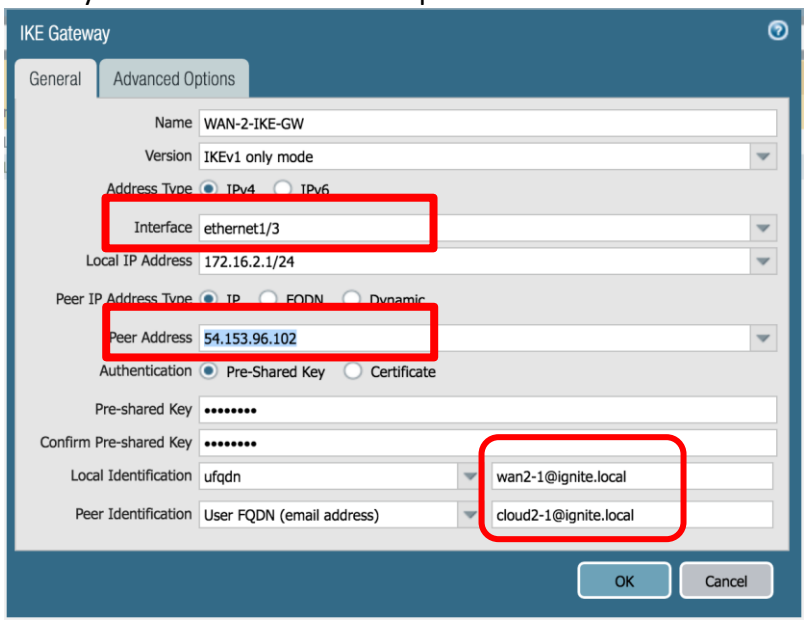
4. Review the configuration you will see that Secondary WAN Link that has been already configured in the Panorama



5. Set up IPsec tunnel to Prisma Access using 2nd WAN link (Ethernet1/3)
    a. Log in to on-premise device (NGFW-Branch in this workshop)
        i. Credentials (***admin / Ignite19***)
    b. Navigate to Network > Network Profiles > IKE Gateways
    c. Click WAN-2-IKE -GW and Open the configuration screen

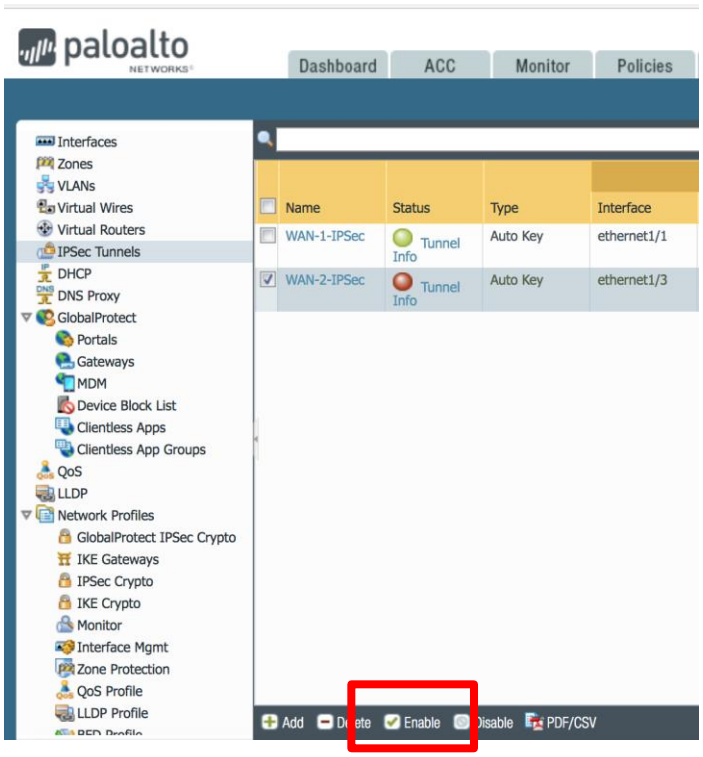


d. Update the Peer Address (10.10.10.10) with the Service IP Address you obtained from the Panorama previously. You are using the same Service IP as the WAN-1-IKE-GW.
Also change the wan2-99@ignite.local and cloud2-99@ignite.local identifiers, replacing 99 which your student-id. For example:

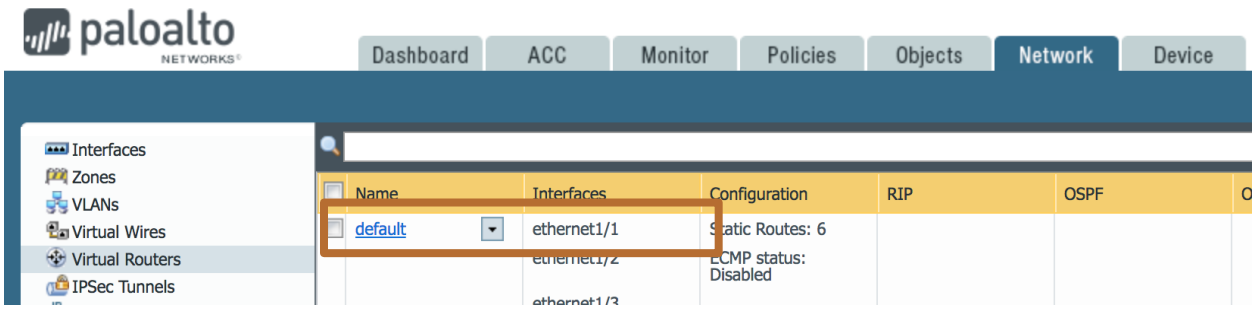


e. Select WAN-2-IKE-GW and Enable it

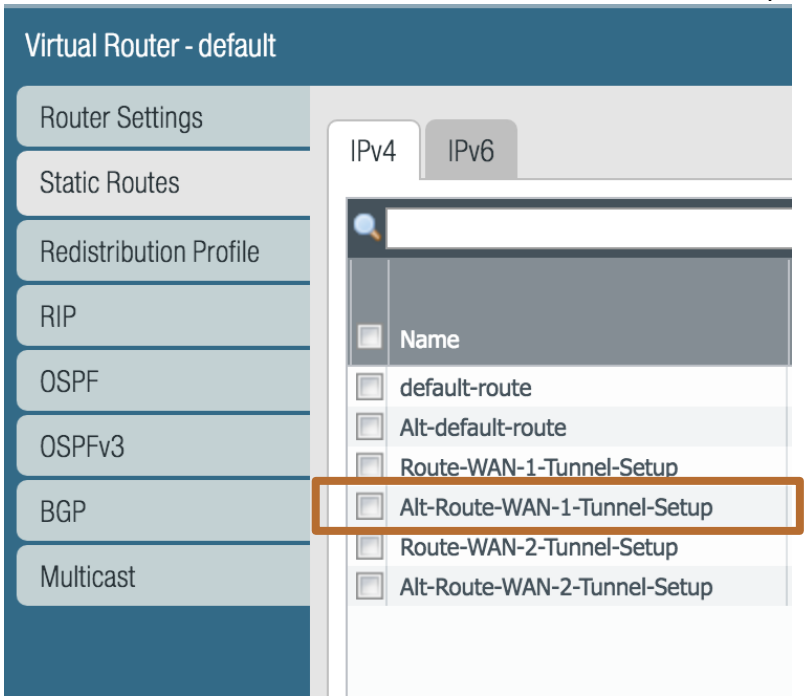
f. Navigate to IPSec Tunnels and Select WAN-2-IPSec and Enable it.



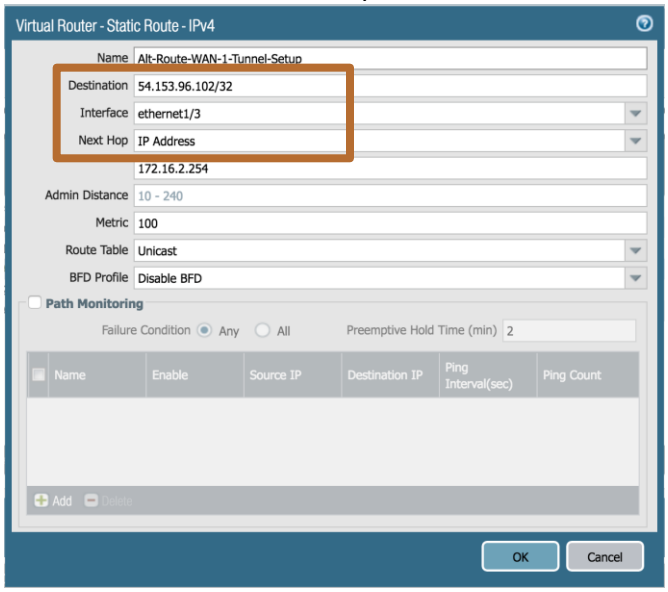
6. Update the Routing Table
    a. Navigate to Network > Virtual Routers > default



b. Click Static Routes and Click Alt-Route-WAN-1-Tunnel-Setup

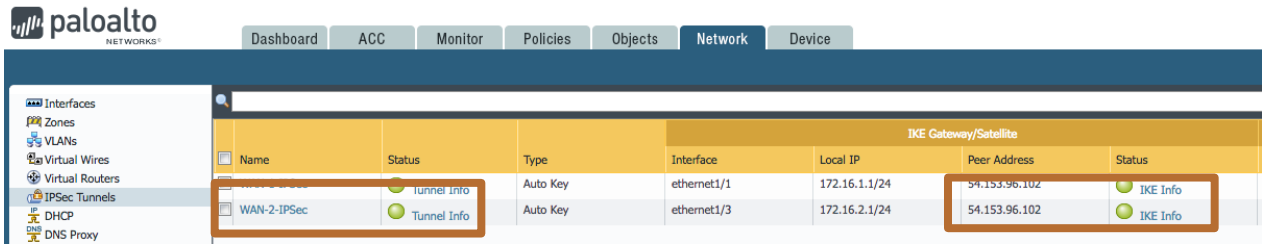


c. Update the Destination with Service IP Address you obtained from the Panorama for your Branch. This is the same IP as Route-WAN-1-Tunnel-Setup. Please use /32 address. This will allow the tunnel to be set up with Prisma Access over ethernet1/3.

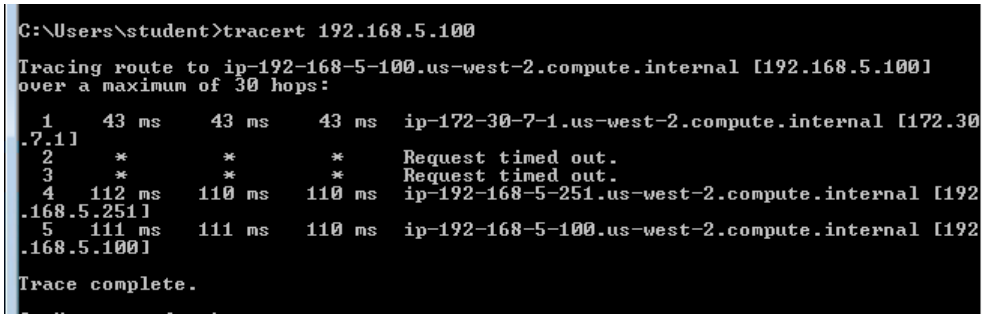


d. Commit the changes on the VM-Series Firewall.

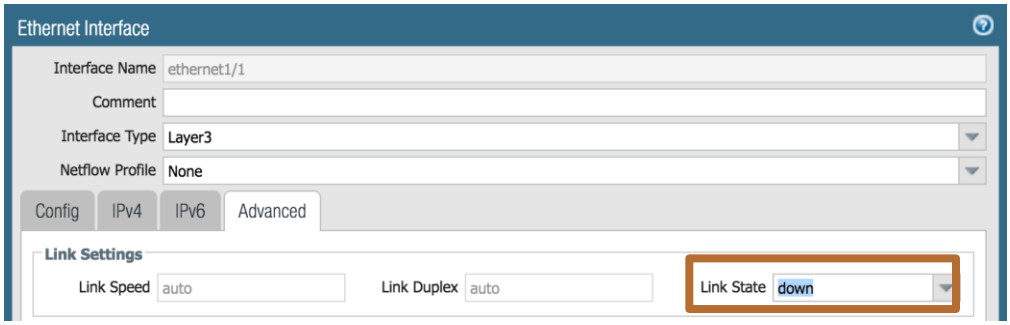
7. After the successful commit, Verify WAN-2-IPSec Tunnel is UP
    a. Navigate to Network > IPSec Tunnels and verify Tunnel Info and IKE Info are green



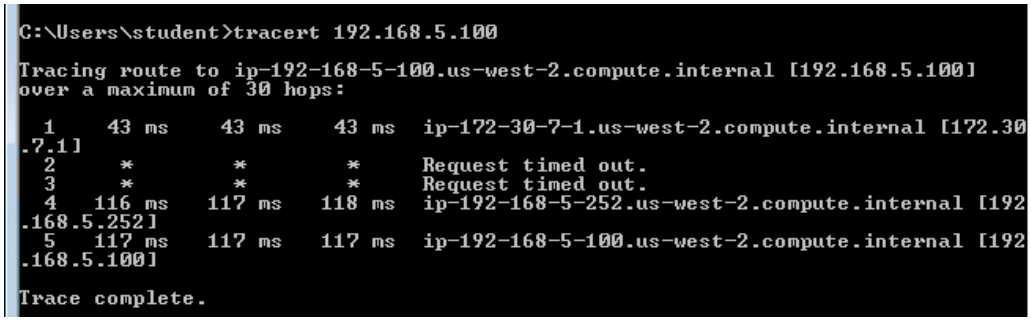
8. Now, both tunnels are UP, verify connectivity and failover to secondary tunnel
    a. As a remote mobile user (**win7-mobile** VM), trace route to branch subnet 1 (192.168.X.100) Where X is your Student #ID. Note that your traffic travels through tunnel.1 (ip-192.168.X.251-*)



    b. Bring down the ethernet1/1 interface
        i. From the NGFW, navigate to Network > Interface > Ethernet > ethernet1/1
        ii. Switch to Advanced Tab and Set the Link State to Down



    c. Commit
    d. Wait for the tunnel to failover. Give it couple of minutes. And then check the connectivity and check the trace route. Note that your traffic travels through tunnel.2 (ip-192.168.X.252-*)



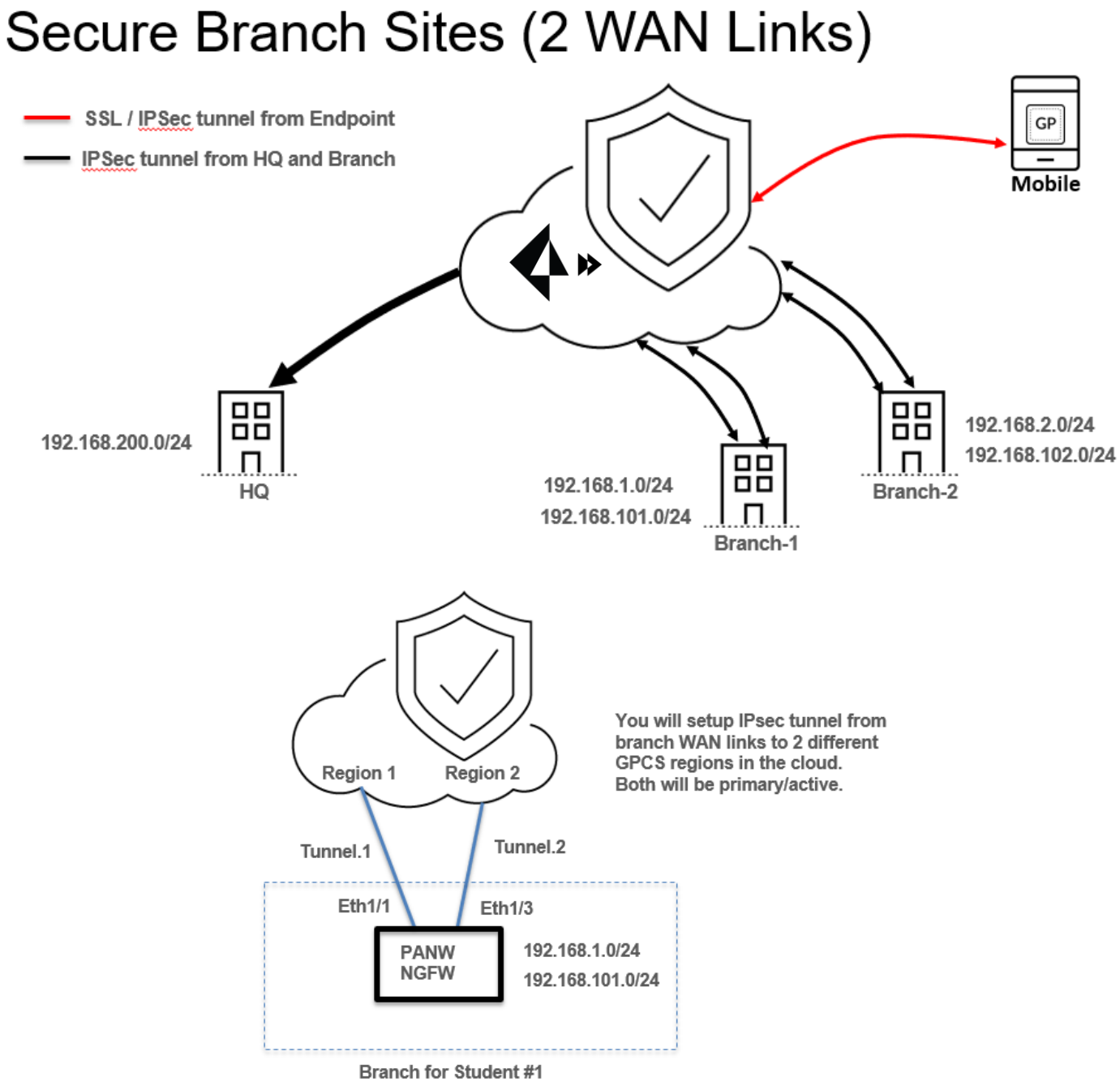
9. Bring up ethernet1/1
10. Commit

Summary:

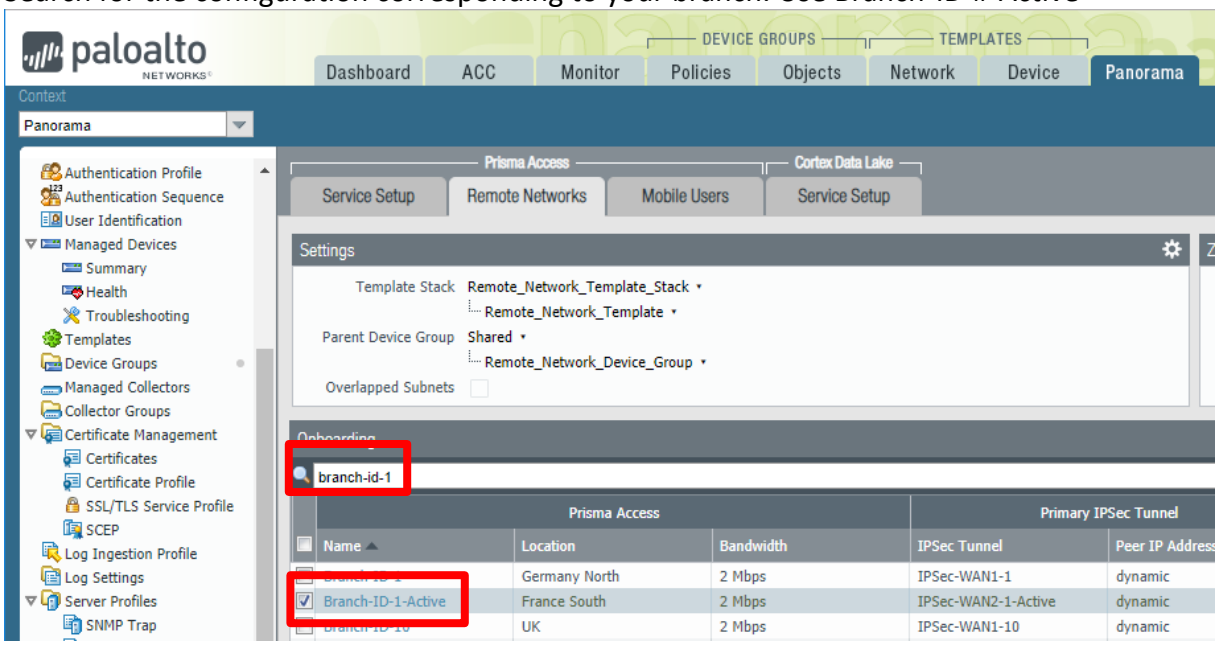
- ✓ Branch offices can be on-boarded to Prisma Access using 2 WAN links.
- ✓ Prisma Access monitors the tunnel and automatically falls back to using the Secondary WAN link.

Activity 5 – Securing Branch Offices with 2 active WAN links

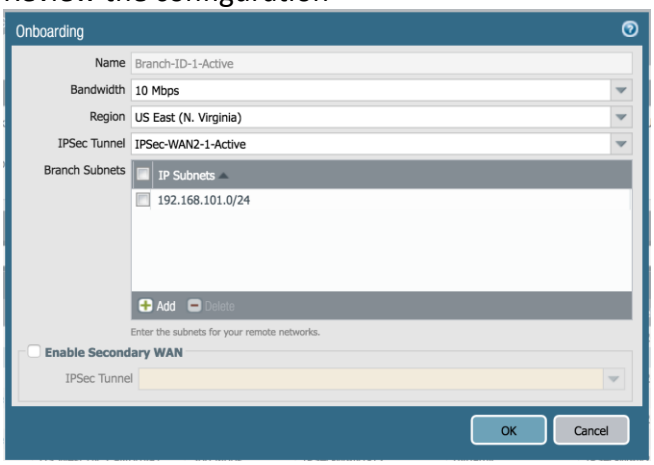
From your remote branch office, you can also have more than one actively used connection to Prisma Access. You will configure them as individual Remote Networks configuration in the Panorama and specify their individual Bandwidth requirement and Region in the Cloud.



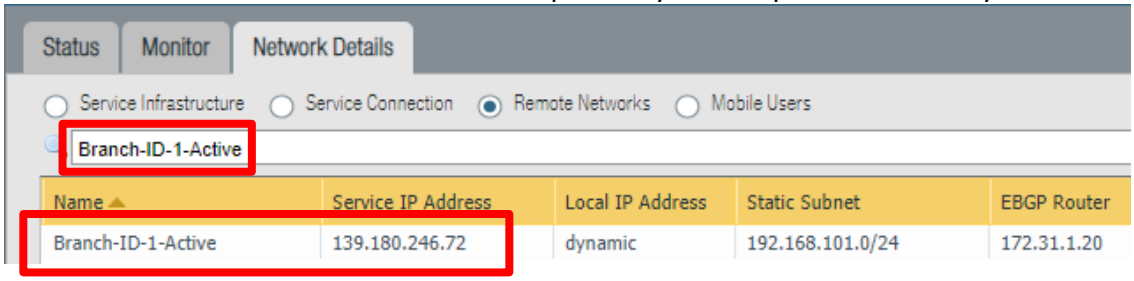
1. Login to Panorama (***student / Ignite19***)
2. Navigate to Panorama > Cloud Services > Configuration > Remote Networks
3. Search for the configuration corresponding to your branch. Use Branch-ID-#-Active



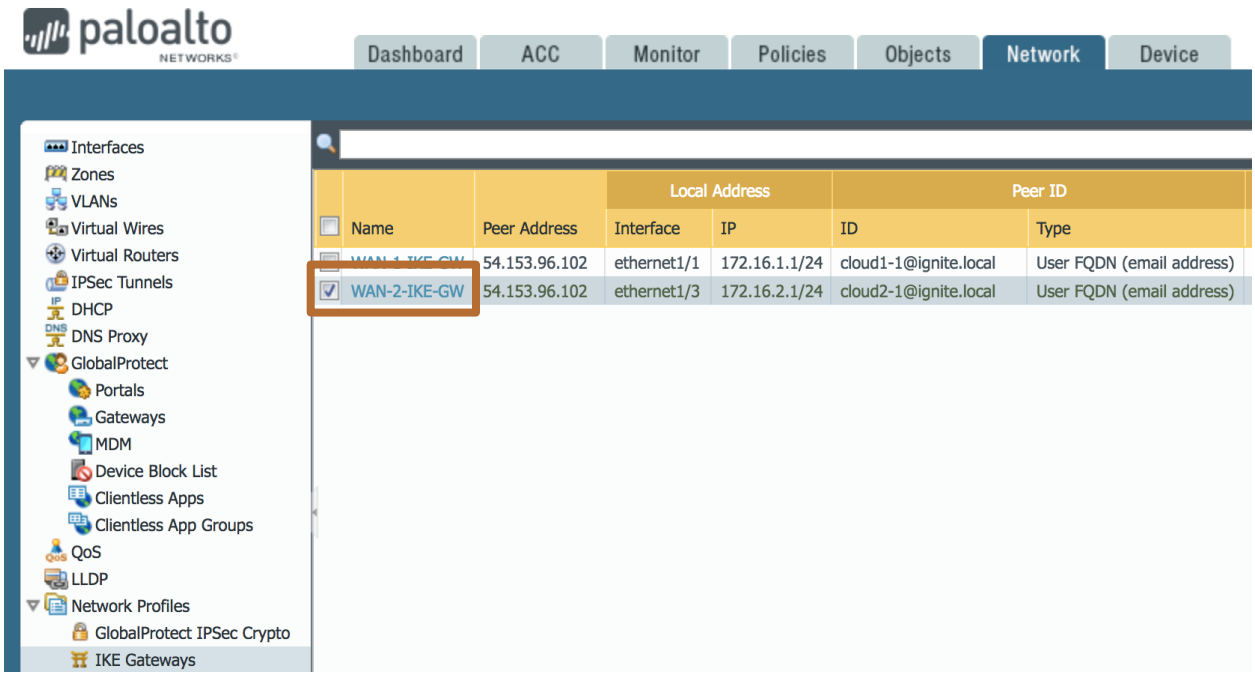
4. Review the configuration



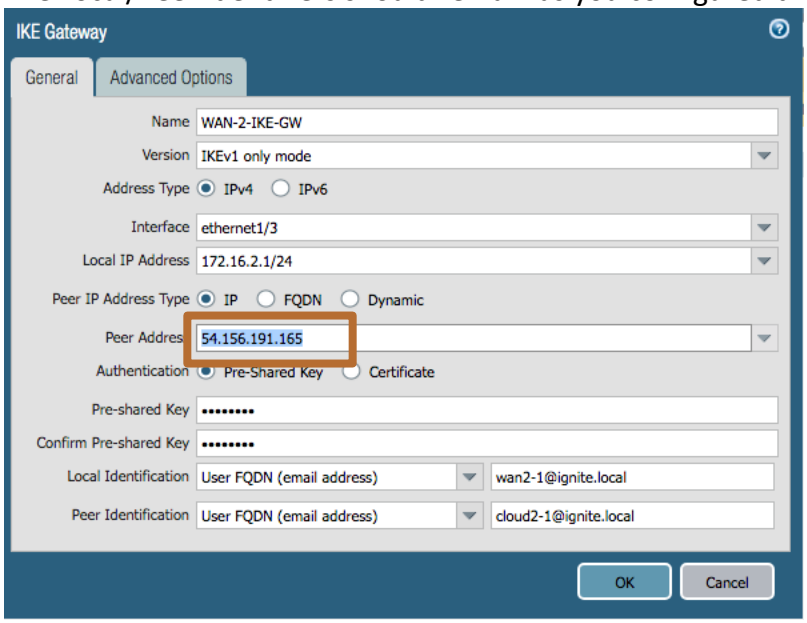
5. Navigate to Cloud Services > Status > Network Details > Remote Networks
    a. Locate and write down the Service IP Address in the Cloud for your Branch. Use Branch-ID-#-Active. You will need this in the later step when you set up a tunnel from your branch.



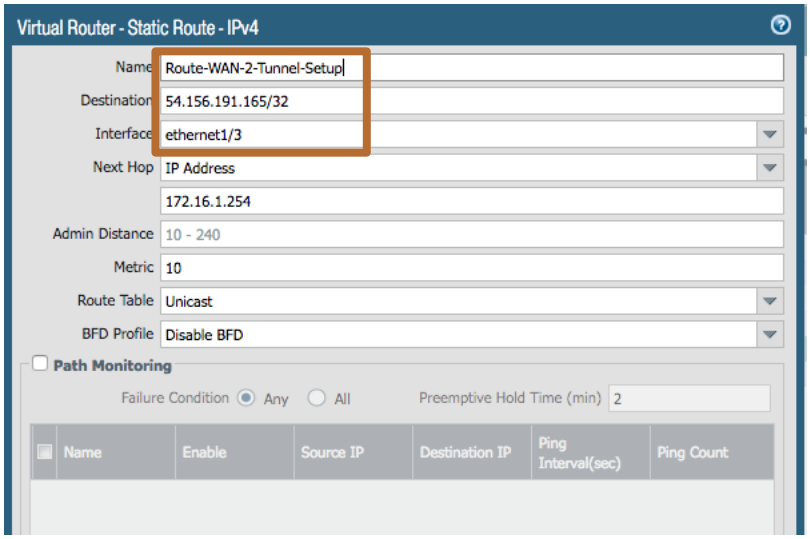
6. Set up IPsec tunnel to Prisma Access using 2nd WAN link (Ethernet1/3)
    b. Login to on-premise device (NGFW-Branch in this workshop)
        i. Credentials (***admin / Ignite19***)
    c. Navigate to Network > Network Profiles > IKE Gateways
    d. Click WAN-2-IKE -GW and Open the configuration screen

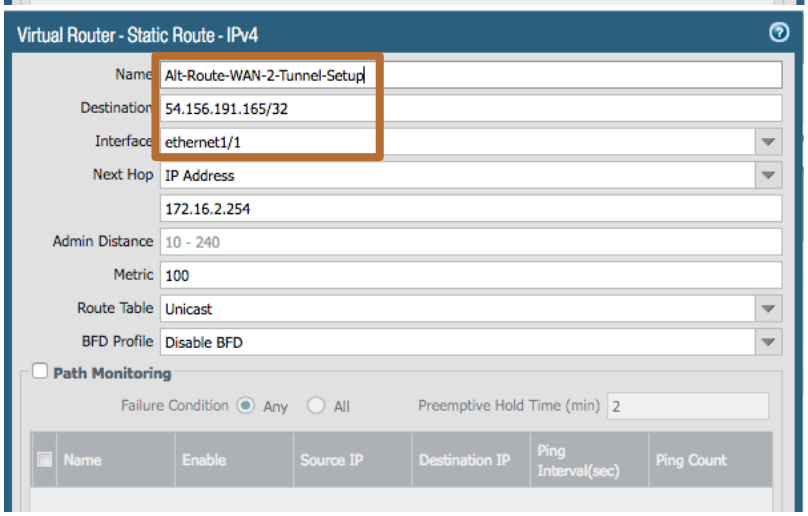


    e. Update the Peer Address with the Service IP Address you obtained from the Panorama. The Local/Peer Identifiers should remain as you configured them previously.



f. Update the Routing Table. Set the Route for Service IP address to be reachable via Ethernet1/3





g. Commit

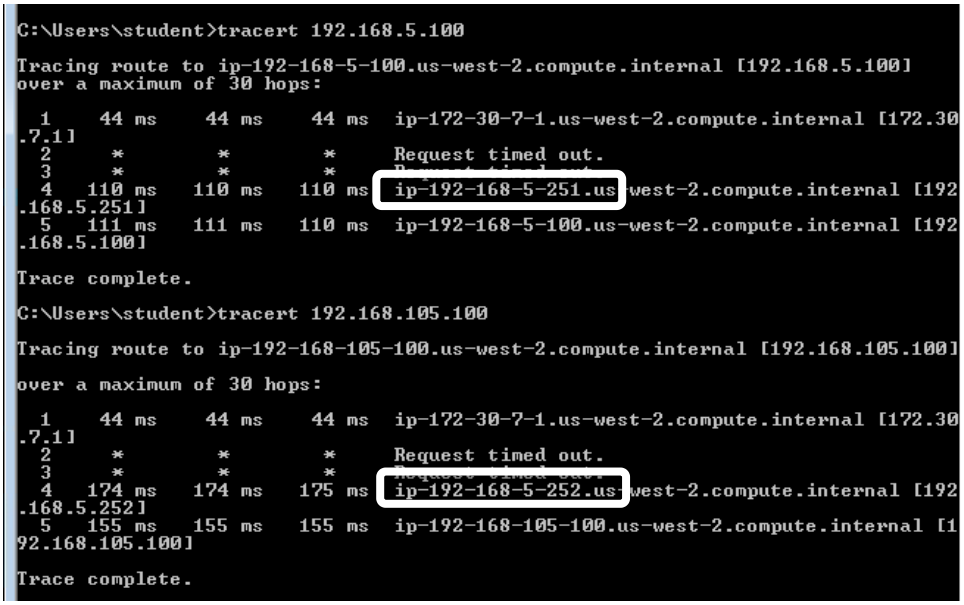
h. Verify WAN-2-IPSec Tunnel is UP

i. From **win7-mobile**, as a remote mobile user connected to Prisma Access, verify you can reach both the subnets in your branch

Ping 192.168.x.100 – where X is your Student # ID

Ping 192.168.Y.100 – where Y is your Student # ID+100

You can verify that both tunnels are actively used by doing tracert for both destinations.



Summary:

- ✓ Branch offices can be on-boarded to Prisma Access using 2 WAN links.
- ✓ Prisma Access can be configured to use both the WAN links actively.

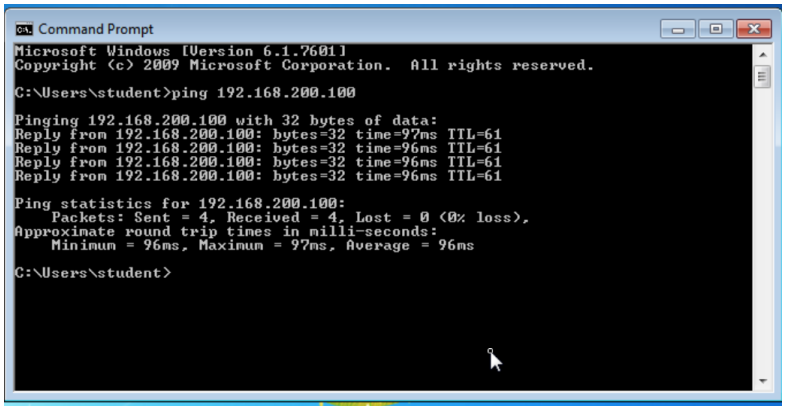
Activity 6 – Next Generation Secure Remote Access

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.

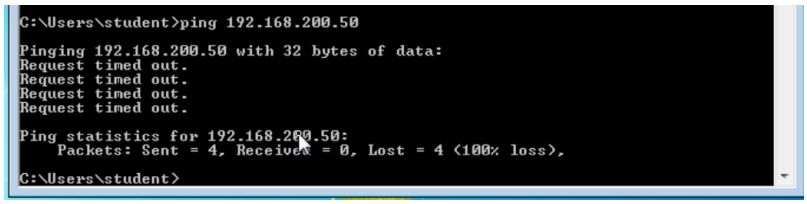
Prisma Access allows administrators to control access to enterprise applications based on User / User-Groups, device compliance state and or the specific application being accessed.

- **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.

2. Controlled access for Contractors
    a. From **win7-mobile**, verify you are connected
    b. As a contractor, connected to Prisma Access, access the Ubuntu machine in the HQ
    Ping 192.168.200.100 should be successful



    c. Now, access the Windows AD Server in the HQ
    Ping 192.168.200.50 should NOT be successful



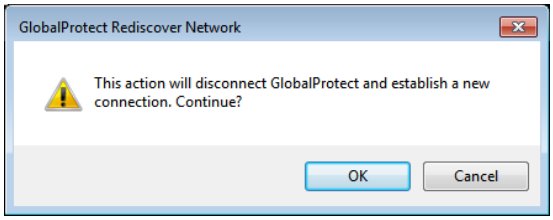
d. In the Panorama, review the Security Policies under Mobile User Device Group for User-ID, HIP, App-ID and Service Port

3. Controlled access for Employees

a. Launch GlobalProtect Agent

b. Click on Settings > Refresh Connection

c. Click OK for confirmation.



d. When prompted for User credentials again, login as Privileged User.
Credentials (***employee[id] / Ignite19***)
For example: employee44 / Ignite19

e. As a privileged user, you should be able to access both the Ubuntu and the Windows AD Server in HQ.
   i. Ping 192.168.200.100 should be successful

ii. Ping 192.168.200.50 should be successful

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