Sarkar, Mohul (Student)

Palo Alto Remote Access VPNs with Certificates Lab

Mohul Sarkar

**Purpose:**

Palo Alto Remote Access VPNs with certificates equips you with the skills needed to secure remote connections

**Background Information on Lab Concepts:**

A remote access VPN is a technology that allows users to securely connect to a private network from a remote location over the internet. It creates a virtual encrypted tunnel between the user's device and the private network, enabling secure communication and access to network resources. Another concept to know is Certificate Authority. a Certificate Authority (CA) is an entity responsible for issuing and managing digital certificates. The CA is a trusted third-party organization that verifies the identity of individuals, devices, or entities and vouches for the authenticity of their public key information.

The VPN connection is established using certificates, which are cryptographic credentials that verify the identities of the communicating parties and facilitate secure communication. The certificates are used to authenticate the remote user's device and the Palo Alto Networks firewall, ensuring that only authorized devices can establish a connection. Once the VPN connection is established, the remote user's device becomes virtually connected to the private network, as if they were physically present within the network infrastructure. This allows the user to securely access resources, applications, and services that are typically only available within the private network. The VPN connection in Palo Alto Remote Access VPNs with Certificates utilizes encryption to protect the confidentiality of the data transmitted over the connection. This ensures that even if the data is intercepted by unauthorized parties, it remains unintelligible and secure.

Another component in this lab is GlobalProtect, GlobalProtect plays a crucial role in handling the client-side configuration and connection establishment. It ensures that the remote user's device is authenticated using certificates, providing a high level of security and trust during the VPN connection setup. GlobalProtect client software is installed on the user's device and enables them to connect to the Palo Alto Networks firewall, establishing a secure tunnel for data transmission.

**Lab Summary:]**

In this lab, I learn how Palo Alto Remote Access VPNs with Certificates enables secure remote access for users by establishing encrypted connections between their devices and Palo Alto Networks firewalls. Using certificates for authentication, it ensures the confidentiality and integrity of data transmitted over public networks. This allows authorized users to securely access private network resources from remote locations while maintaining the highest level of security.

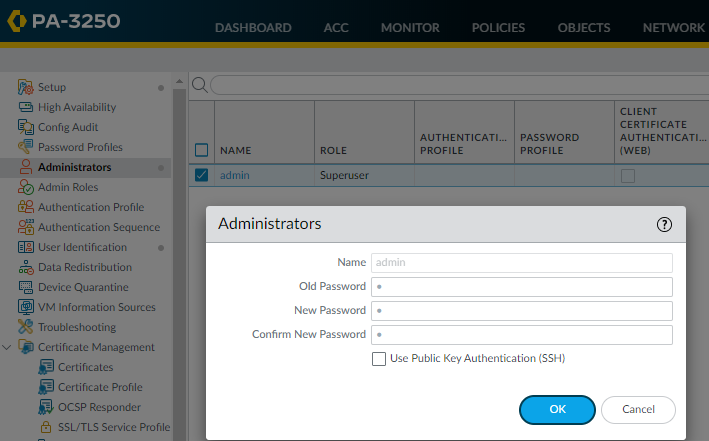
**Lab Commands:**

Step 1- Install your firewall and connect power to it.

Step 2- Gather required information from your network administrator for your firewall

Step 3- Connect your computer to the firewall with an RJ-45 Ethernet cable and on a browser go to https://192.168.1.1.

Step 4- When the Palo Alto interface opens, log in to the firewall using the default username and password (admin/admin).



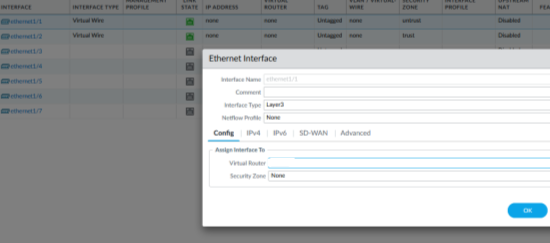
Step 5- Delete the virtual wire in a network environment to remove a virtual wire interface or configuration from a networking device

Step 6-

Connect the management interface to the internet by configuring a WAN port that allows connectivity in the firewall itself

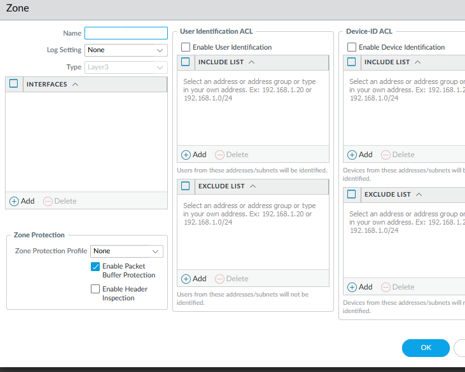
Step 7-

Got to Device > Interfaces > ethernet1/1, and modify the virtual router to default



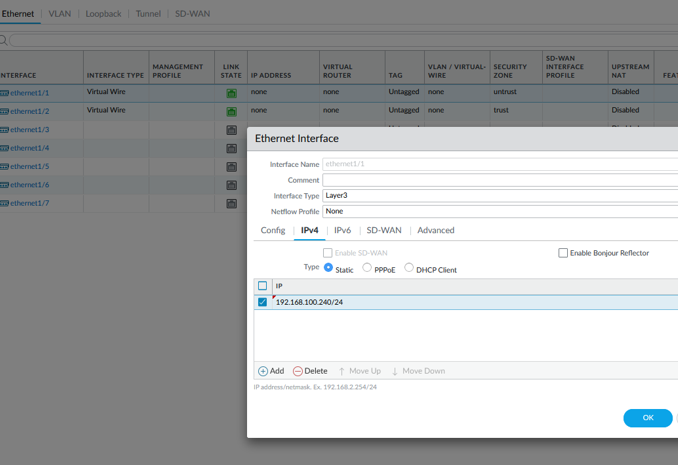
Step 8-

Navigate to Network > Zones and Create a New Zone and name it



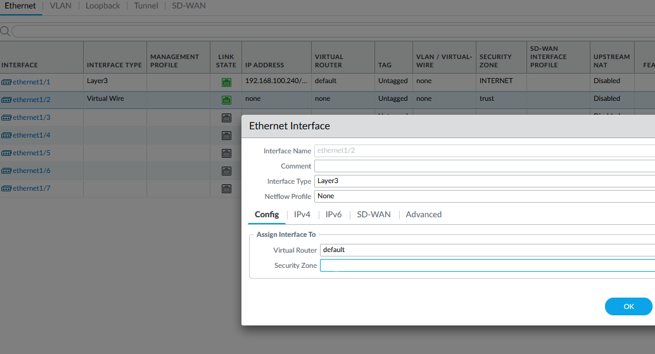
Step 9-

Navigate to Network > Interfaces > Identify the interface on which you want to set a static IP address > In the IPv4 tab, you should see options to configure the IP address settings. Specify the static IP address, subnet mask, and default gateway.



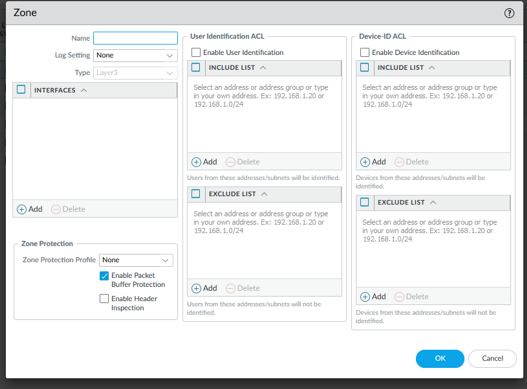
Step 10-

Search in Network > Interfaces > Set the interface type to Layer 3 > Assign the virtual router to default (allowing traffic to be routed between different networks based on the routing table entries in the default virtual router)



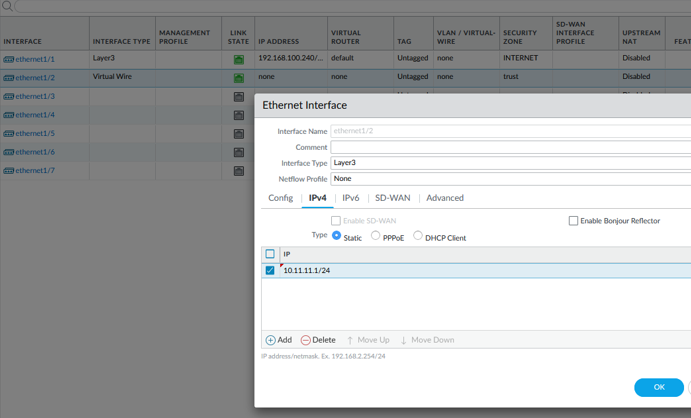
Step 11-

Find Network > Zones > Add a new Zone (the "Inner Traffic" zone is created, which can be used in security policies to define rules for traffic originating from or destined to the internal network)



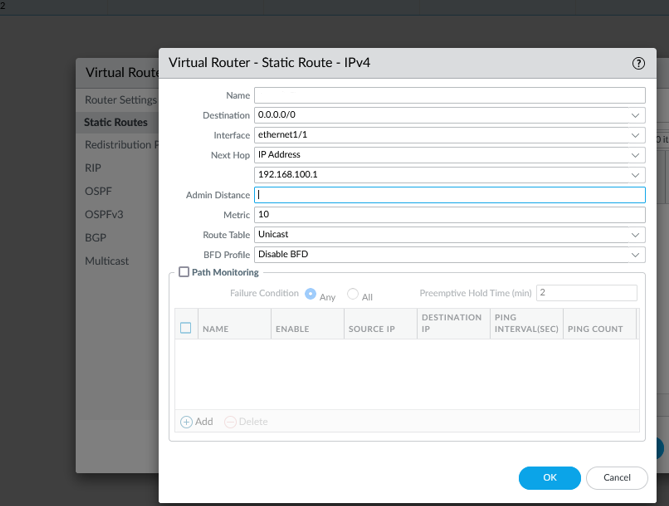
Step 12-

Navigate to Network > Interfaces > Identify the interface on which you want to set a static IP address and set it



Step 13-

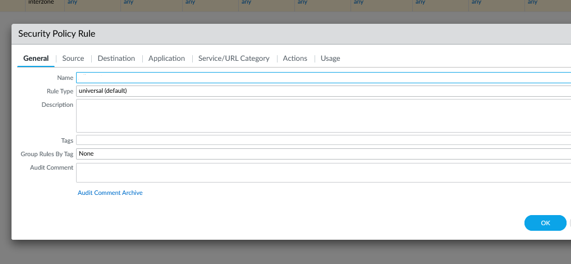
Navigate to Network > Virtual Routers > Select the desired router > Click on Static Routes > Add a new Static Route

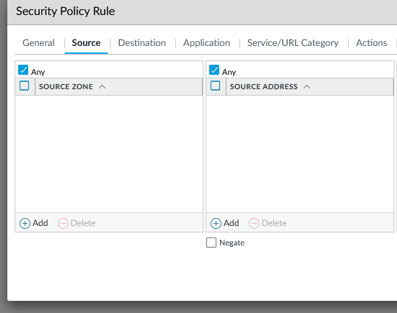


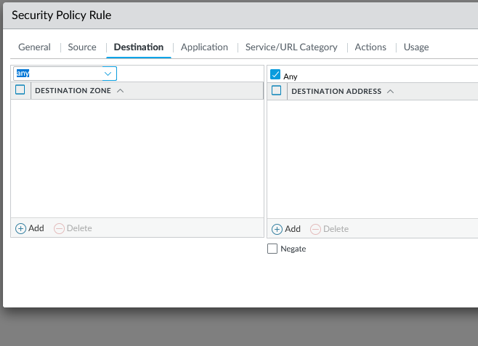
Step 14-

Search for Policies > locate the specific pre-existing rule that you want to edit > modify and save

Within the same tab select Source > and select “any” on Zone and Address > navigate to Destination and set to “any” > finally. Navigate to Service/URL Category > and select “any” on URL category

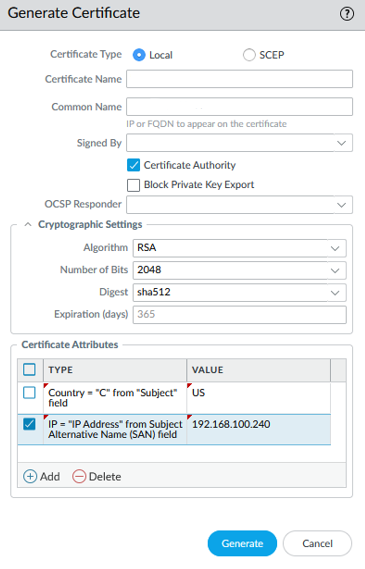






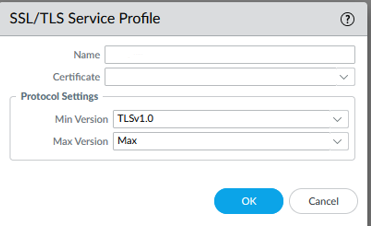
Step 15-

Navigate to Device > Certificates > generate a new certificate > configure certificate settings > save changes



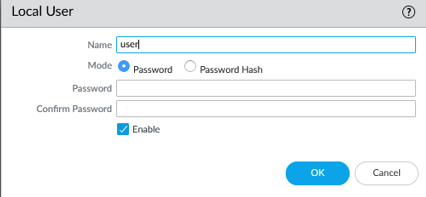
Step 16-

Navigate to Device > SSL/TLS Service Profile > Select Add > Configure profile settings > save changes



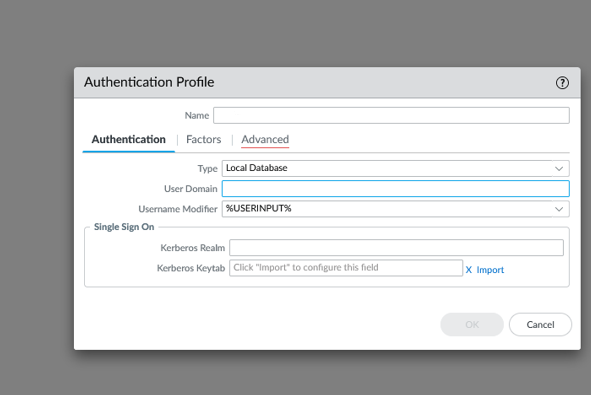
Step 17-

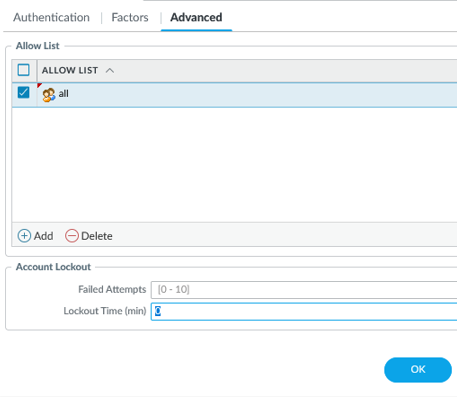
Select Objects > Users > “Add” > Configure user settings > save changes



Step 18-

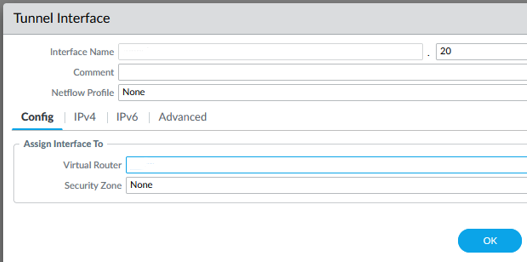
Select Device > Authentication Profiles > “Add” > Configure profile settings > Click on Advanced > set lockout time to 0 and ensure Allow List contains “All” > save changes





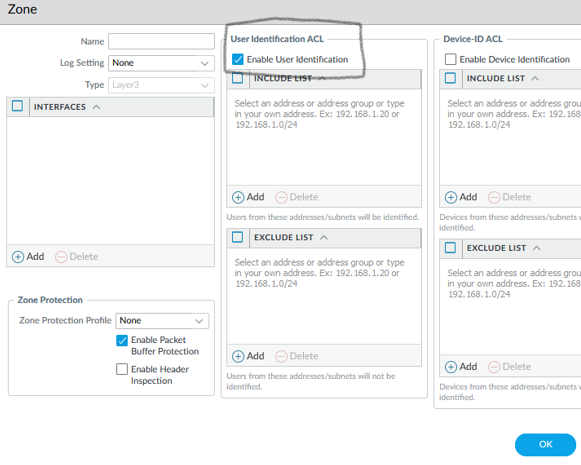
Step 19-

Select Device > Interfaces > Tunnels > “Add” > Configure interface settings > save changes



Step 20-

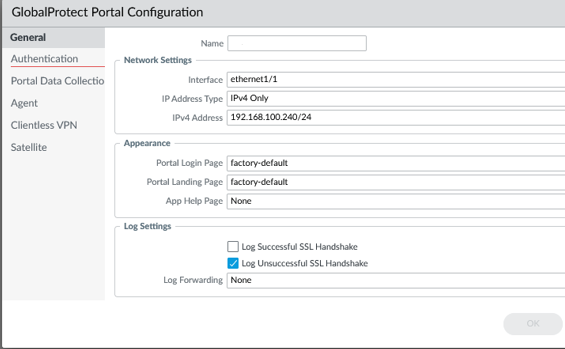
Navigate to Network > Zones > “Add” > Configure zone settings > save changes

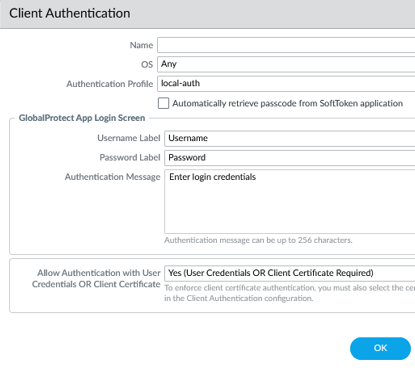


Step 21-

Next, Navigate to Network > GlobalProtect > Portals > “Add” > Configure portal settings > Authentication > enter Client Authentication tab > configure settings > enter Agents tab > nd select the Trusted Root CA > Save Changes

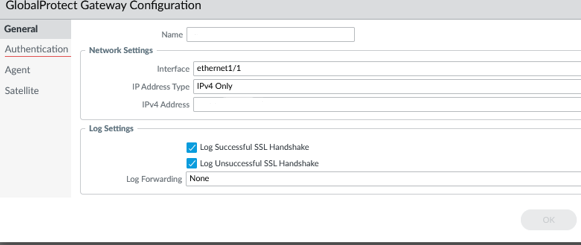
save changes

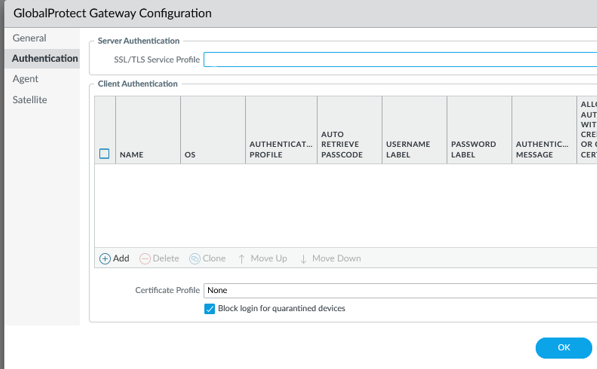


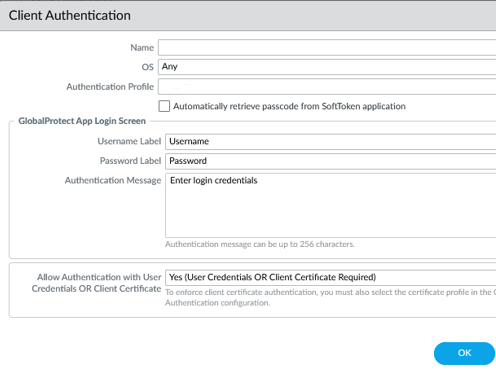


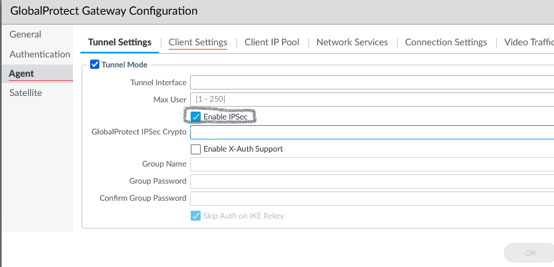
Step 22-

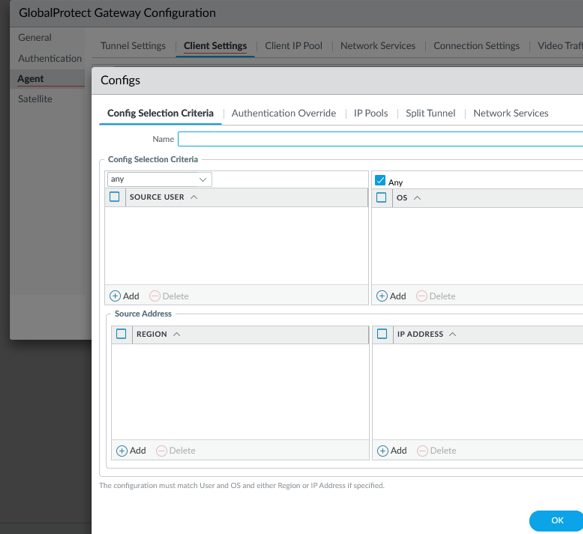
Navigate to Network > GlobalProtect > Gateways > add a new gateway and configure settings > save changes

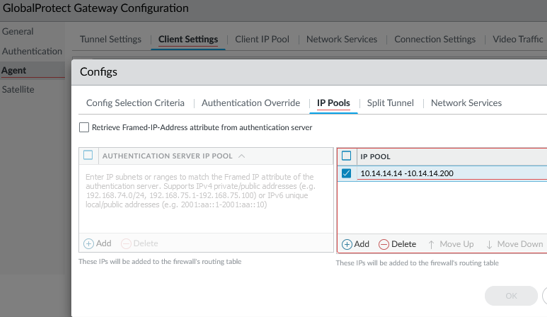






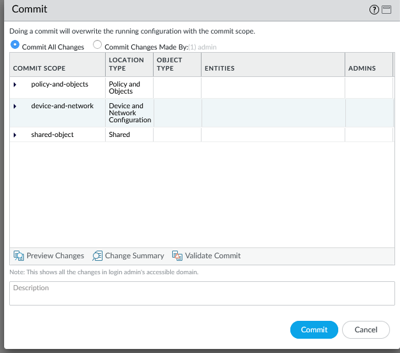






Step 23-

Commit Changes



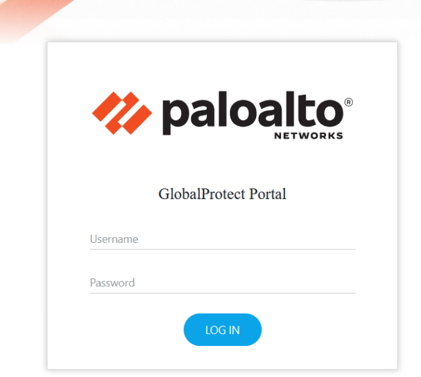
Step 24-

Select Device > Licenses > Retrieve Licenses > Download GlobalProtect Client > Locate the GlobalProtect client > Download the latest version (6.1.0) > Install the GlobalProtect client > Configure GlobalProtect client settings > Save Changes



Step 25-

Open a web browser > type in the assigned IP static address in address bar > Log in > Access Remote User Interface



Step 26-

Download Global Protect Client and Run the Installer



Step 27-

Once Downloaded enter GlobalProtect Client and connect with Static IP address and verify connectivity

Graphical user interface, application

Description automatically generated

Lab Complete.

**Problems:**

When configuring Palo Alto Remote Access VPNs with Certificates, I encountered a few problems along the way. First, I misconfigured certificates, where the certificates weren’t properly generated or installed on the necessary components of the VPN infrastructure. Leading to authentication failures or the inability to establish secure connections. Another challenge that arose from incorrect configuration of the VPN gateway or tunnel settings. As the gateway was not properly configured, clients would not be able to connect or experience connectivity issues. Additionally, conflicts with firewall rules or security policies cause traffic to be blocked or restricted, resulting in connection problems. To address these problems, thorough testing, attention to detail in configuration, and referring to the Palo Alto Networks documentation and support resources can be essential.

**Conclusion:**

From a Palo Alto Remote Access VPNs with Certificates configuration, valuable insights can be gained regarding certificate management, authentication methods, tunnel settings, firewall rules and security policies, client configurations, network infrastructure, and integration with other security features. This includes understanding how certificates are generated and managed, the authentication mechanisms employed, specific tunnel configurations, firewall rules governing VPN connections, client software settings, network infrastructure details, and integration with additional security measures. This knowledge enables administrators to effectively manage and troubleshoot the VPN deployment, ensuring secure and reliable remote access for users.