Sarkar, Mohul (Student)

Palo Alto Site to Site VPN with Certificates Lab

Mohul Sarkar

**Purpose:**

The purpose of configuring Palo Alto Site to Site VPN with certificates is to provide me a more secure and scalable solution for creating a VPN tunnel between two sites. Certificates are digital documents that are used to authenticate the identity of a device or user. When configuring a VPN with certificates, each device is issued a unique digital certificate that is used to establish the identity of that device. This provides more security compared to using shared secret keys, as it is more difficult for an unauthorized user to access with there being a digital certificate. Additionally, using certificates in a VPN configuration allows for more scalability in larger environments. With shared secret keys, each device must have the same key configured, which can become cumbersome and difficult to manage in large-scale environments. Using certificates, on the other hand, allows for more granular control over which devices are authorized to connect to the VPN. Configuring a Palo Alto Site to Site VPN with certificates also requires an understanding of PKI concepts, such as certificate authorities, certificate revocation lists, and certificate chaining. This provides me an opportunity to gain hands-on experience with these concepts and learn how they are used in real-world networking scenarios**.**

**Background Information on Lab Concepts:**

Site-to-Site VPN tunnels are a type of VPN connection that allow two or more networks located in different physical locations to securely communicate with each other over the public Internet. Site-to-Site VPN tunnels are commonly used by organizations to connect their branch offices or remote sites to their corporate headquarters or data centers, providing a secure and cost-effective means of connecting geographically dispersed networks. Site-to-Site VPN tunnels are established by configuring VPN gateways at each end of the connection. The VPN gateways encrypt and decrypt the data packets that are transmitted between the two networks, ensuring that the data is secure and cannot be intercepted or read by unauthorized parties. There are several benefits to using Site-to-Site VPN tunnels are that it provides secure communications between networks, ensuring that data transmitted between the networks is protected from unauthorized access. They can be less expensive than dedicated leased lines or other private network connections, since they utilize the public Internet infrastructure. Additionally, Site-to-Site connections are scalable and can be easily configured to support additional sites or users as needed. To set up a Site-to-Site VPN tunnel, organizations typically need to configure VPN gateways at each end of the connection, along with appropriate firewall rules and network configurations. The VPN gateways are configured to authenticate each other using pre-shared keys or digital certificates, and to negotiate encryption and decryption algorithms to secure the communication between the networks.

**Lab Summary:**

A lab to configure a Palo Alto Site to Site VPN with certificates involves setting up a secure VPN tunnel between two sites using digital certificates to authenticate each device. The lab typically requires the use of PKI concepts, such as certificate authorities, certificate revocation lists, and certificate chaining. The lab provides a valuable learning experience for me, as it allows me to gain experience with configuring Palo Alto devices and working with advanced security concepts such as PKI and IPsec.

**Lab Commands:**

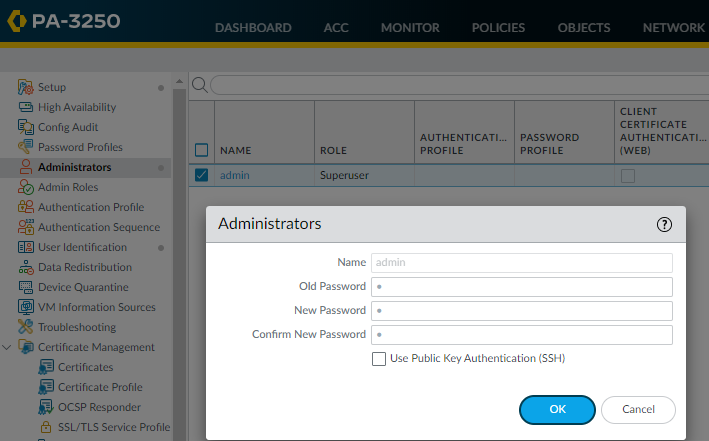
Step 1- Install your firewall and connect power to it.

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.

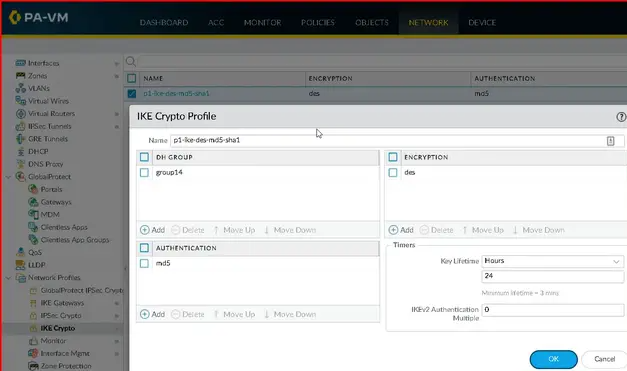
Step 4- When the Palo Alto interface opens, log in to the firewall using the default username and password (admin/admin).

Step 5- Set a unique password for the admin account.



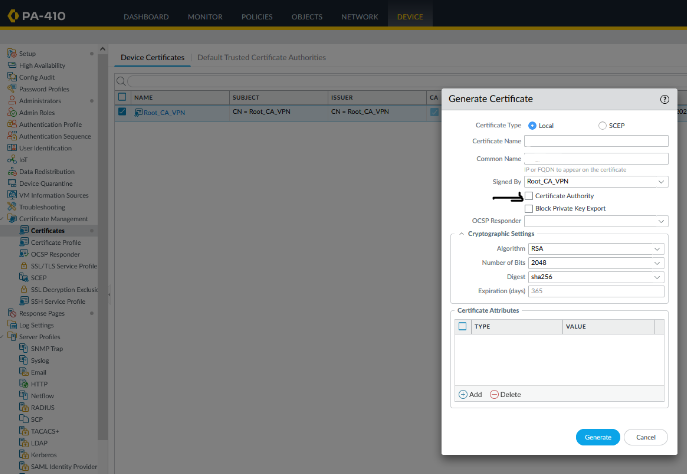
Once you have created a secure account to be able to log onto all firewalls in use, you can begin the Site to Site with certificates configuration

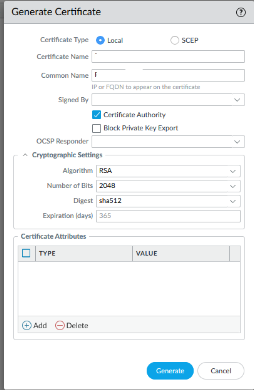
Step 6- Navigate to Network > Network Profiles > IKE Crypto and create IKE Crypto Profile



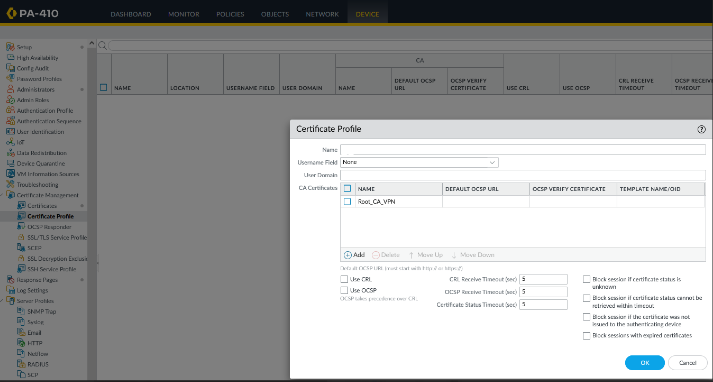
Step 7) Navigate to Network Profiles > IKE Gateways and “add” a new IKE Gateway

Step 8) Navigate to Certificate Management > Certificates and generate a new certificate

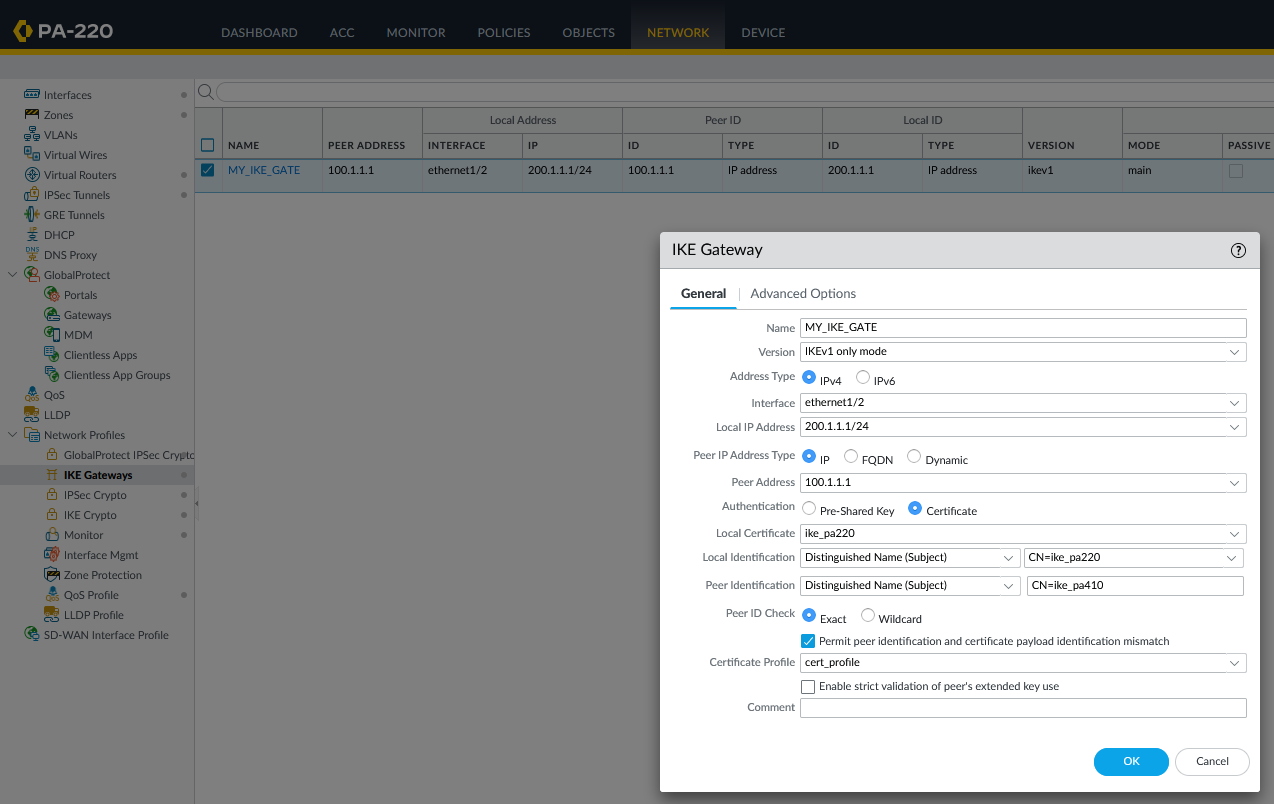




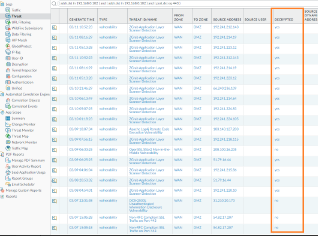
Step 9) Name the certificate profile and select the CA Certificate you generated before and go to the Certificate Authority and check that box off to initiate the certificate configuration



Step 10) Assign Certificate to IKE Gateway in Network Profiles > IKE Gateways to the Gateway you previously created and select Certifcate instead of Pre-Shared Keys and configure the following settings with addresses given by IP Administrators.



Step 11) Navigate to Monitor > Logs > Threat and look at the “Decrypted” tab to check functionality of VPN



**Problems:**

Some problems I had on this lab was first I had certificate validation errors. The certificate validation process failed because the certificates were not properly signed. I needed to troubleshoot certificate errors by checking the certificates and their associated policies. Another issue I had was incorrect peer device settings. I double-checked the settings for the other device and ensured that they match with the settings on the Palo Alto device and fixed it.

**Conclusion:**

One of the main advantages of using certificates in a Site-to-Site VPN is that they provide an additional layer of security. Certificates are unique digital identifiers that can be used to verify the identity of the devices that are communicating over the VPN tunnel. This helps to prevent unauthorized access and ensure that only trusted devices are able to communicate with each other. Another advantage of using certificates is that they can simplify the configuration process. Certificates can be automatically generated and distributed to the devices that will be using them, making it easier to manage the VPN connection over time.