A black background with a black square

Description automatically generated with medium confidencew

**GlobalProtect VPN on**

**Palo Alto PA-220**

Ryan Chen

1/14/2024

**Purpose:**

This lab simulates a production environment where customers/end-users/employees need to access an internal network from an untrusted, external network. For this purpose, a VPN is used in order to tunnel traffic into the network so that users can access the network from anywhere. Palo Alto provides the GlobalProtect VPN service for this task, and this lab focuses on its configuration and use.

**Background Information:**

A VPN, or virtual private network, is a commonly used service that provides a multitude of different privacy, security, and convenience functions. At its core, they work by encrypting traffic between an end-user and the server, allowing a secure connection to be established from anywhere. Given that this traffic is encrypted, it is near impossible for an adversary to read it. Even if they do manage to get hold of the traffic by sniffing it off the network, they will be unable to read it.

For this reason, VPN’s are commonly used in order to secure traffic from an unsecure network. By establishing this secure connection, attacks like a MITM (Man in the Middle) become less of a threat, since traffic is encrypted. Likewise, people also use VPN’s for their ability to “tunnel” traffic. This refers to the ability to establish a connection that emulates the device directly on a local network. This is useful for many different use cases, but commonly required by companies when employees are doing remote work. In order to keep company traffic secure even from an unsecure network, companies can configure a VPN to tunnel employee traffic back into the network. This allows employees to work remotely on company networks, all while keeping traffic secure.

Now that we know the basic use cases of a VPN, we can start to cover how it works at a base level. In order for a VPN to work, end users must connect through an application configured by the VPN provider. This application works by establishing a secure connection through the use of certificates and encryption, allowing end user traffic to be encrypted in transit and decrypted by the VPN at the end. In our case, we generate certificates on the firewall, and then download and install them on our end user devices. This makes our device trust the VPN provider, enabling future communication.

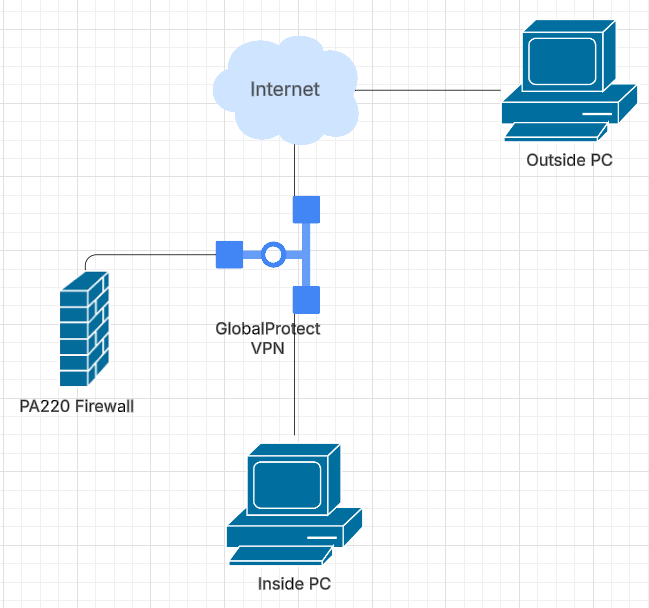
Finally, one of the key concepts of this lab is remote access. For this purpose, we use the RDP (Remote Desktop Protocol) provided by Windows. This protocol allows us to configure one machine inside the network as a server, and the other machine as a end user that will ultimately establish a connection to the server to demonstrate that the VPN is working. RDP gives us the ability to remotely view another Windows desktop, a common use case for companies that want to enable employees to do remote work.

**Lab Summary:**

As previously mentioned, the first step to our lab is to generate and install certificates on both our firewall and our end user devices. This is crucial to allowing the VPN to ultimately establish a connection between server and client through an insecure intermediate network. Next, we need to create a tunnel interface that all VPN traffic will go through. This is important, as the tunnel needs to allow traffic to flow from an insecure region (outward facing interface) into our private network. We will use this later when configuring our client.

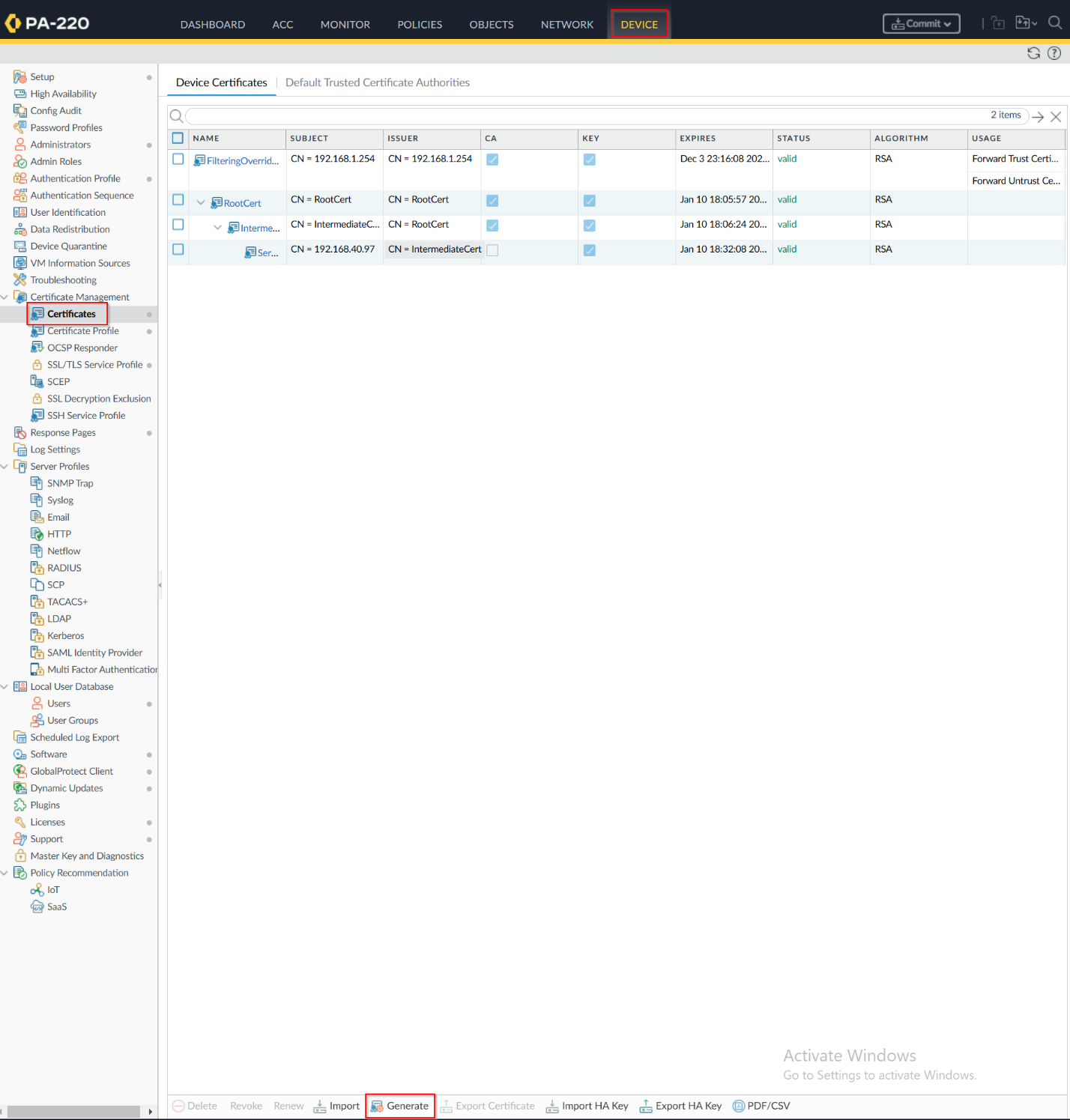
Finally, the actual VPN server has to be configured. To simplify deployment, we use Palo Alto’s GlobalProtect service, making a VPN much easier to create. After configuring this, we should be done with the VPN side of our lab. After allowing RDP on one of our machines, we should be able to connect using the VPN into the local network, from where we can RDP to prove that the VPN works.

**Network Diagram:**

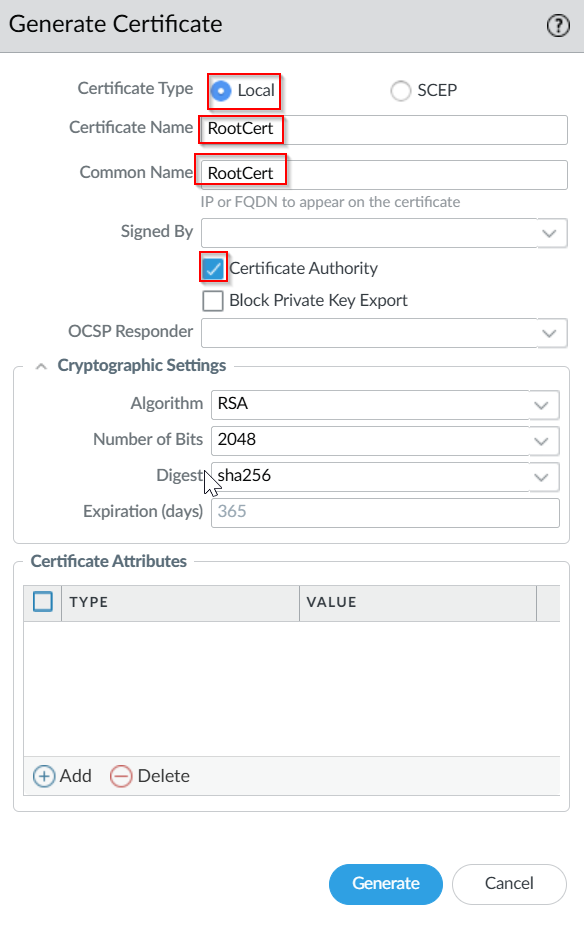
****

**Lab Commands:**

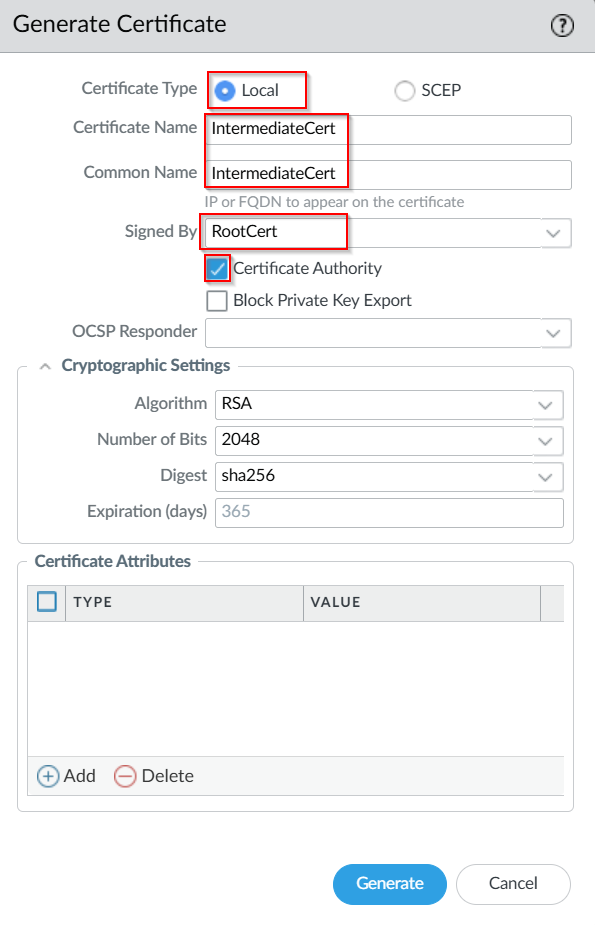
1. To begin, we need to generate certificates that will be used in order to prove that our server is trustworthy to the client. These include a root and intermediate certificate that the client end user machines will later download and import. Navigate to Certificates > Generate.



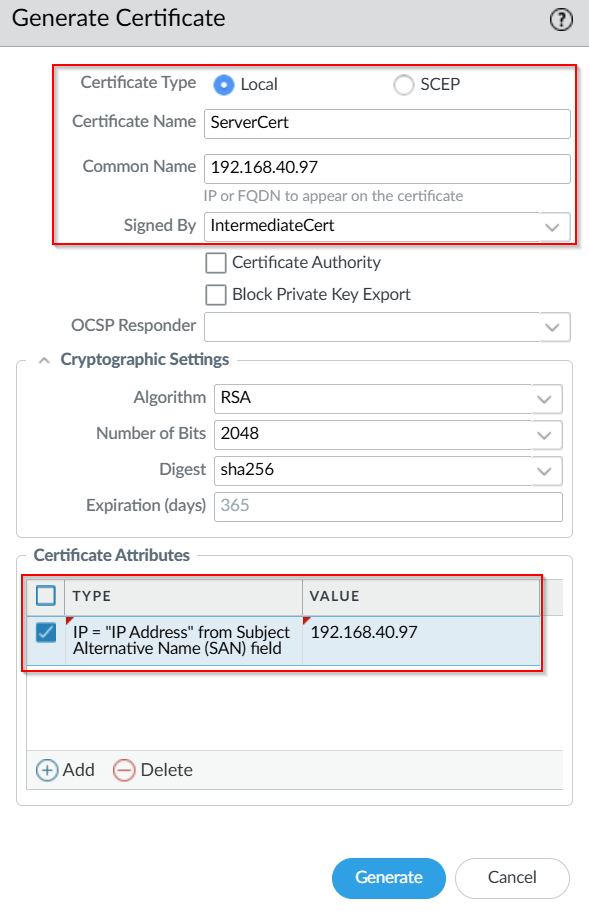
1. First, create the root certificate. Note that it must be a certificate authority.



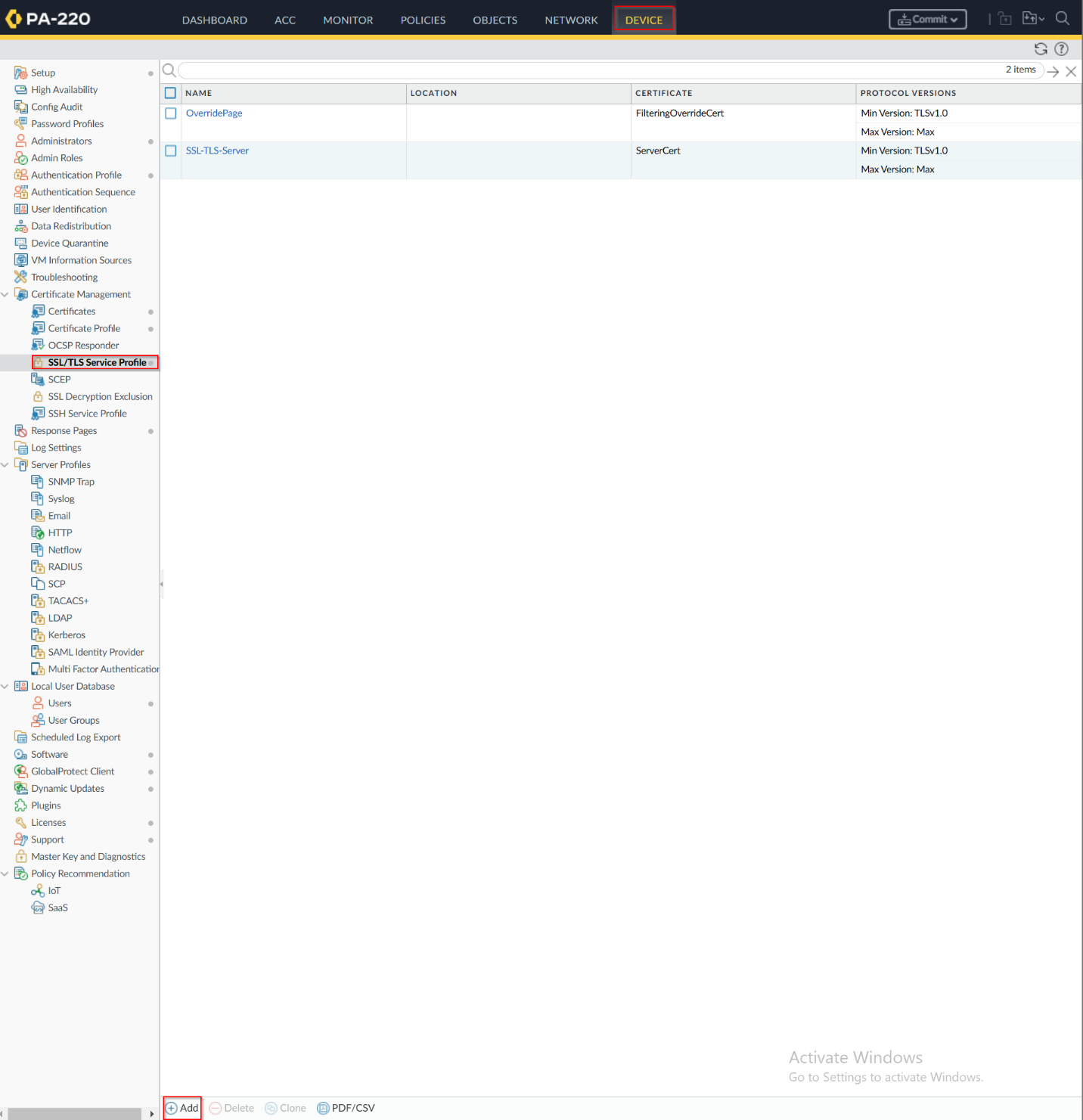
1. Next, generate an Intermediate certification. This should be signed by the root certificate and also be a certificate authority, which will be necessary later for end devices.

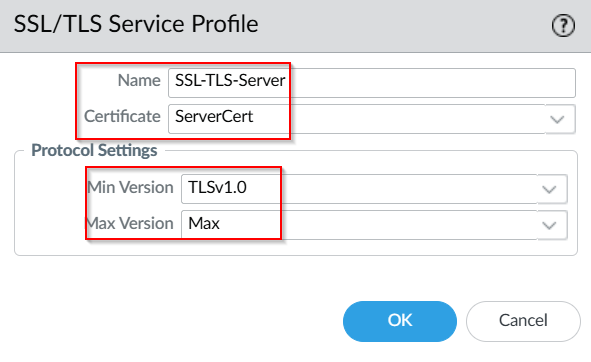
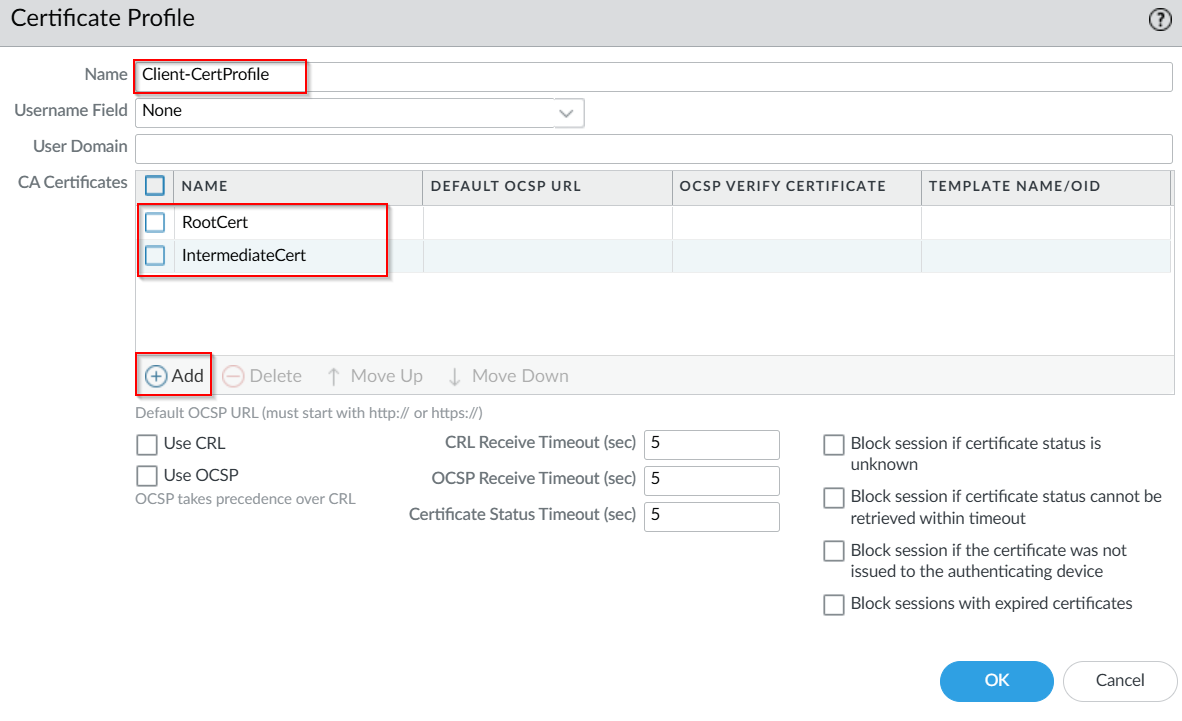
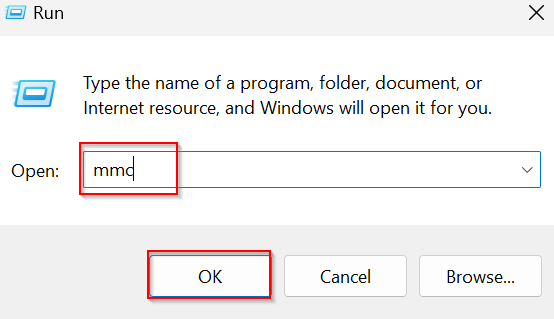
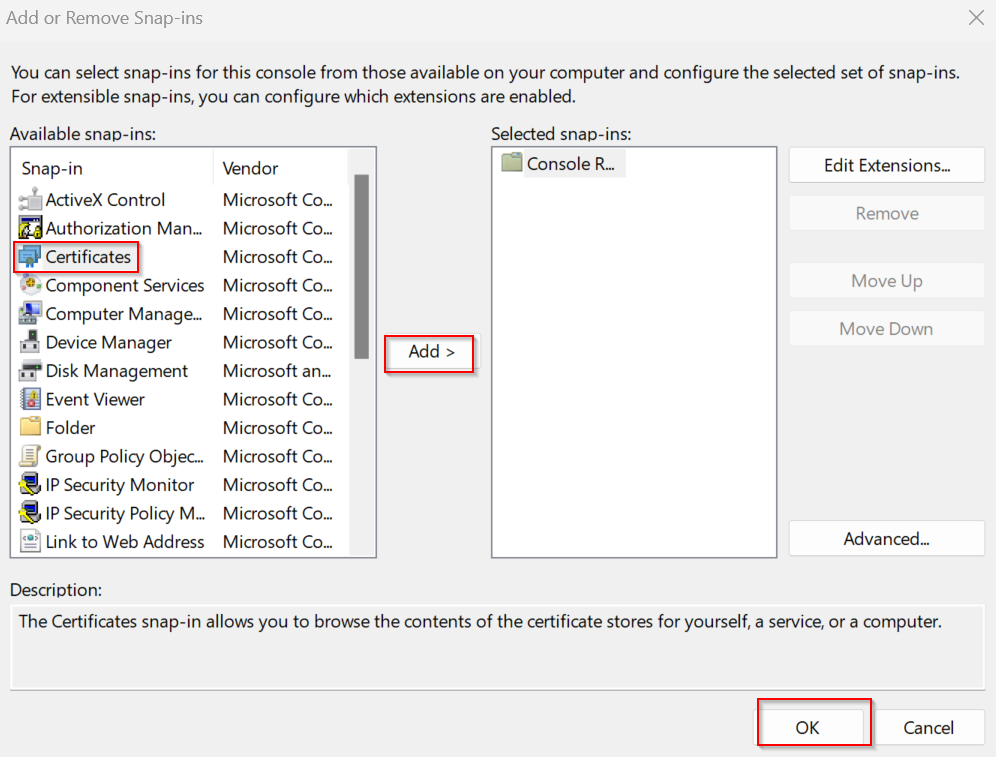
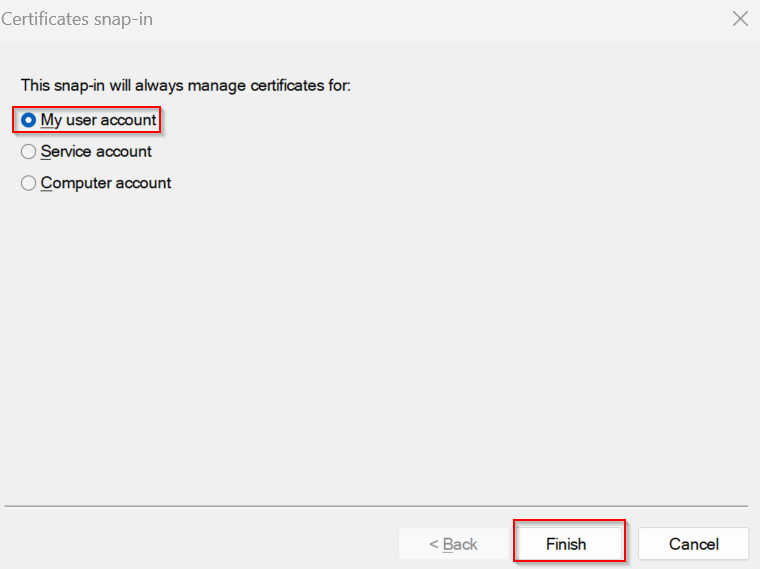
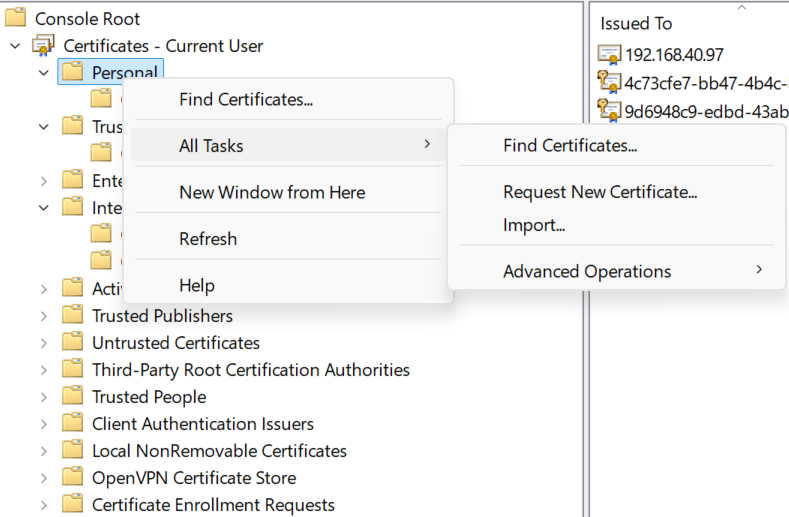
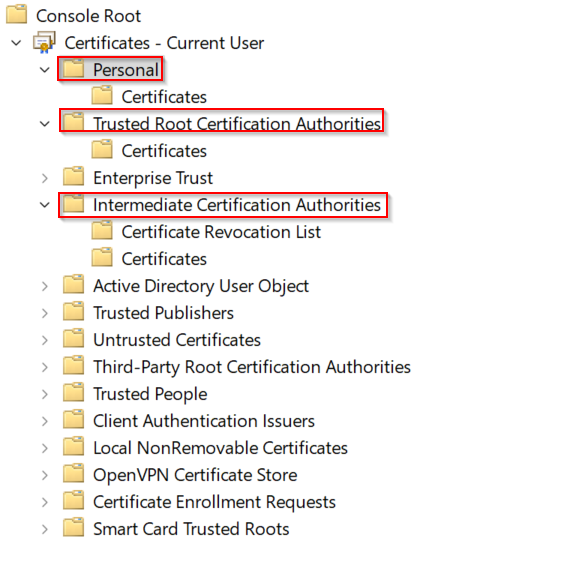
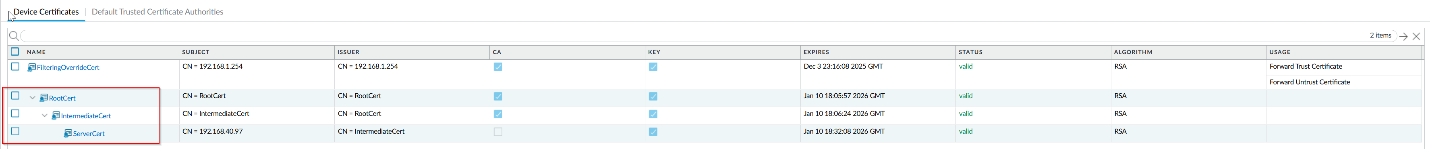
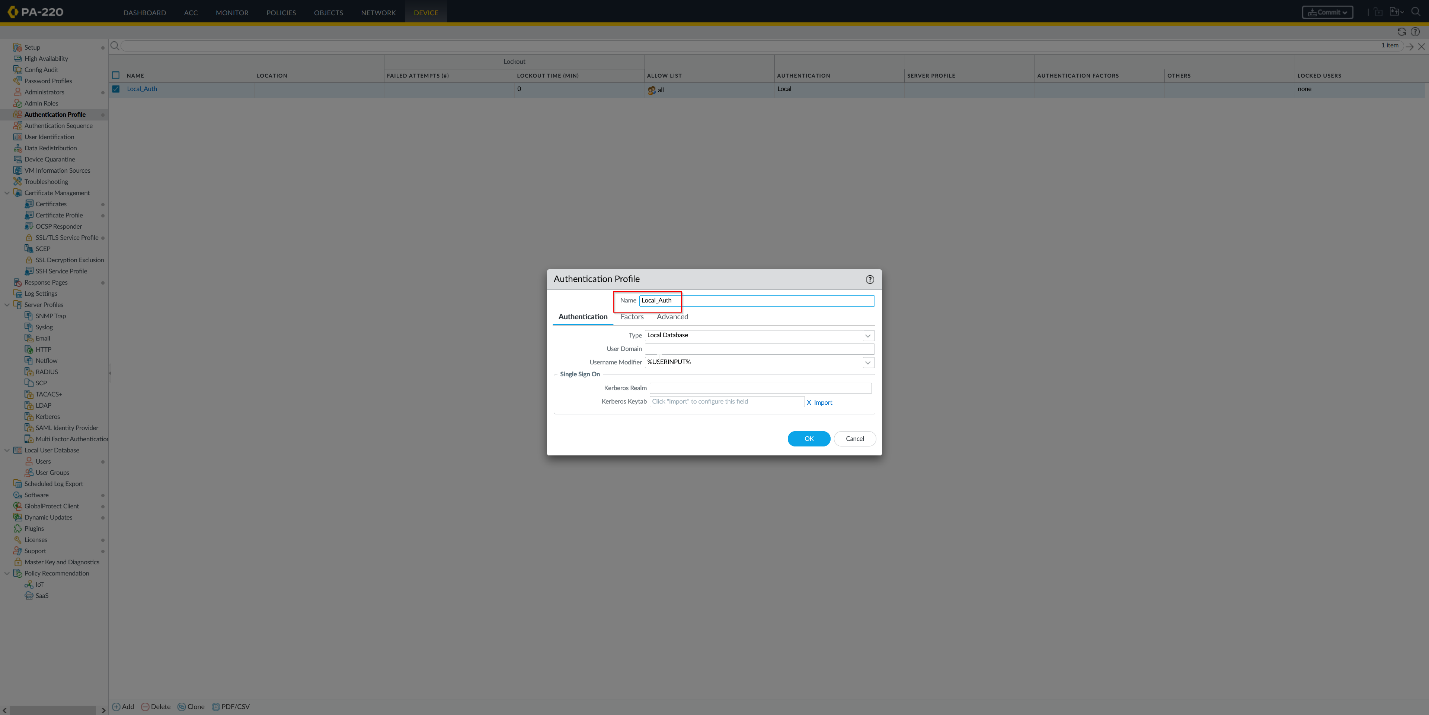
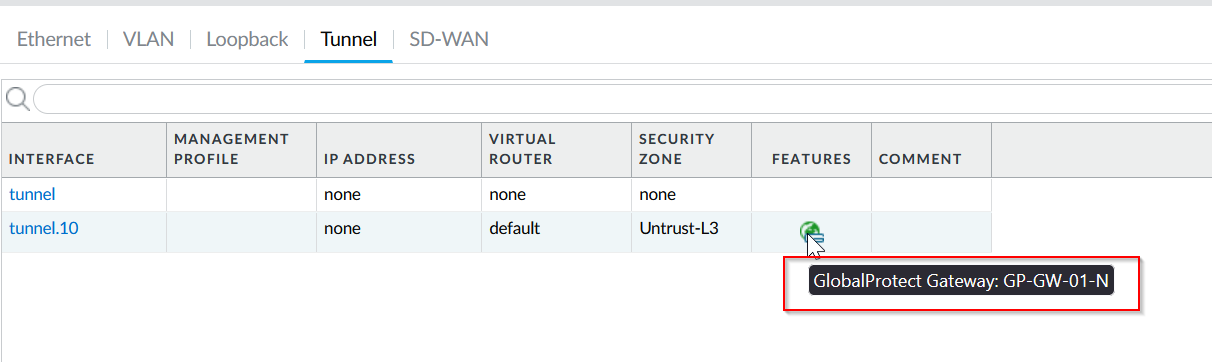
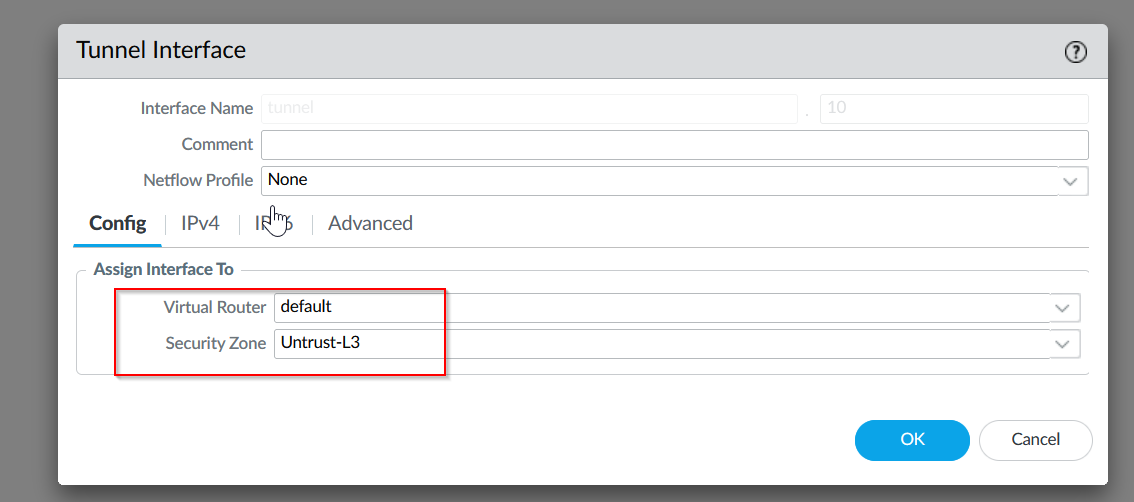
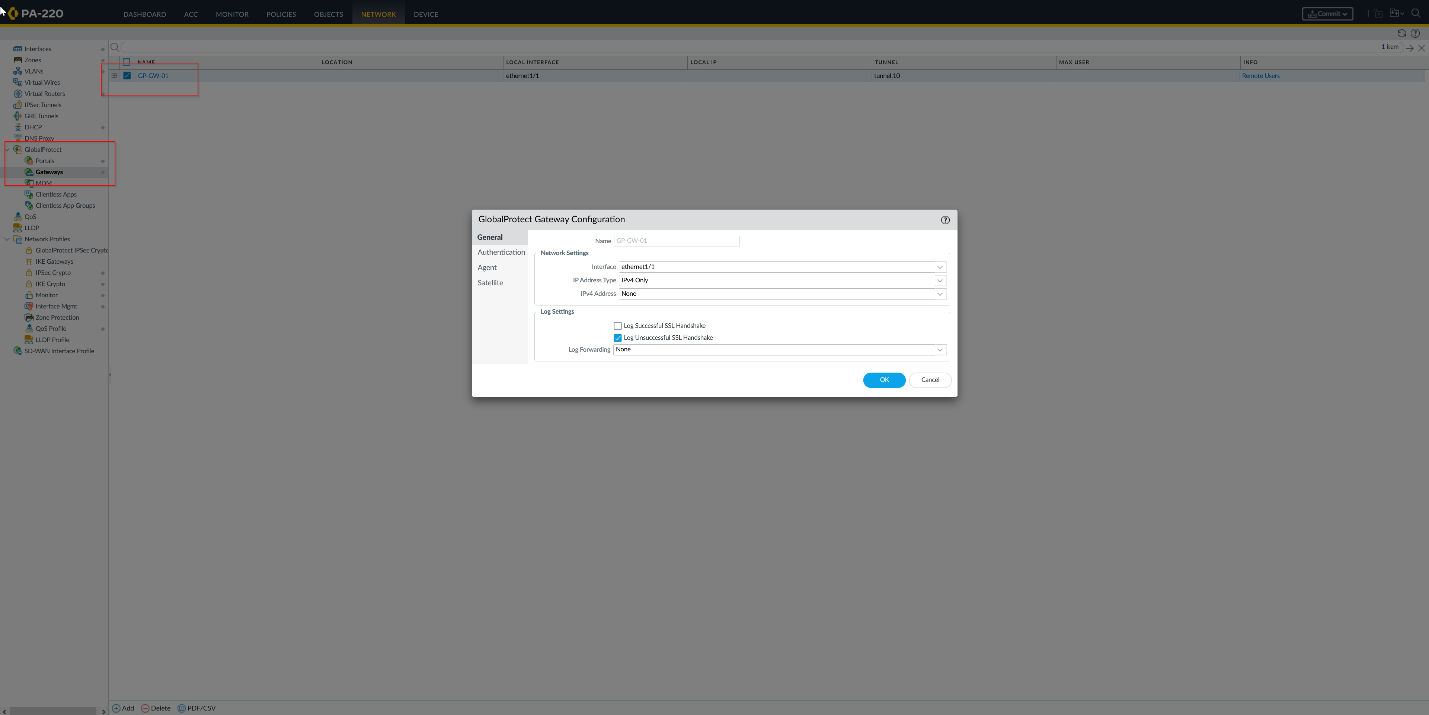


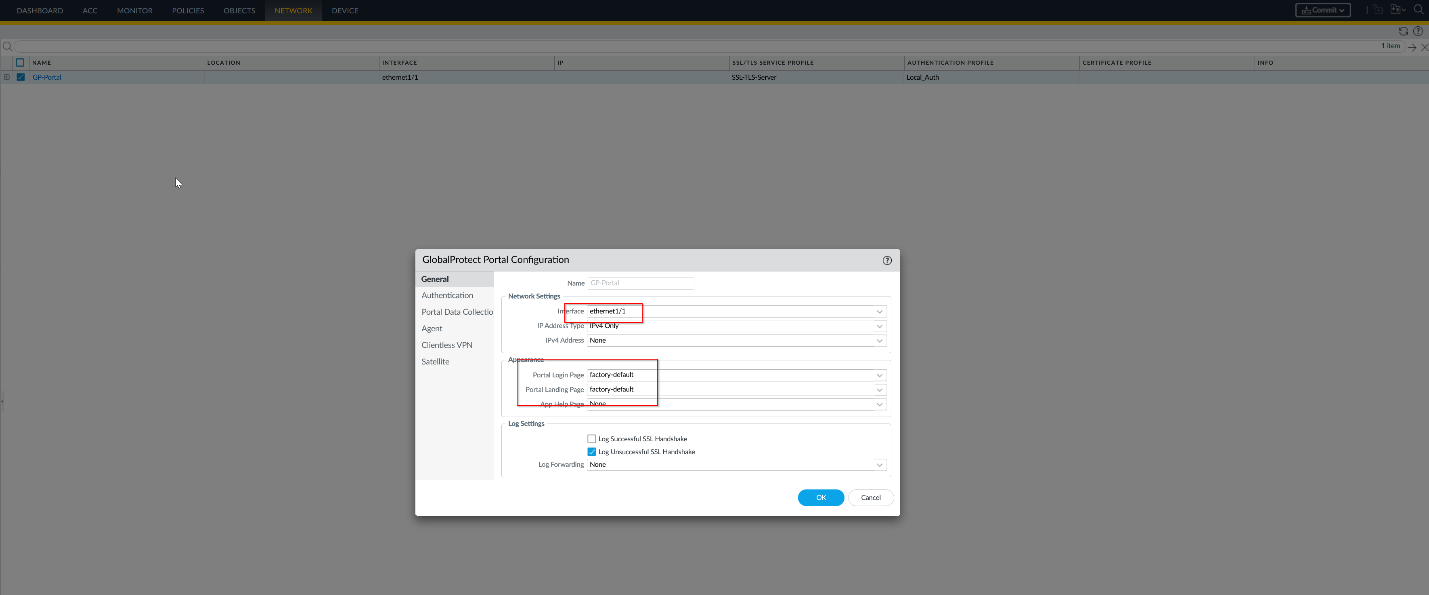
1. Finally, create a server certificate. Note that this will not be installed on end users’ devices and thus does not need to be a certificate authority. Make sure to point this certificate to the corresponding IP address of your outward facing interface.

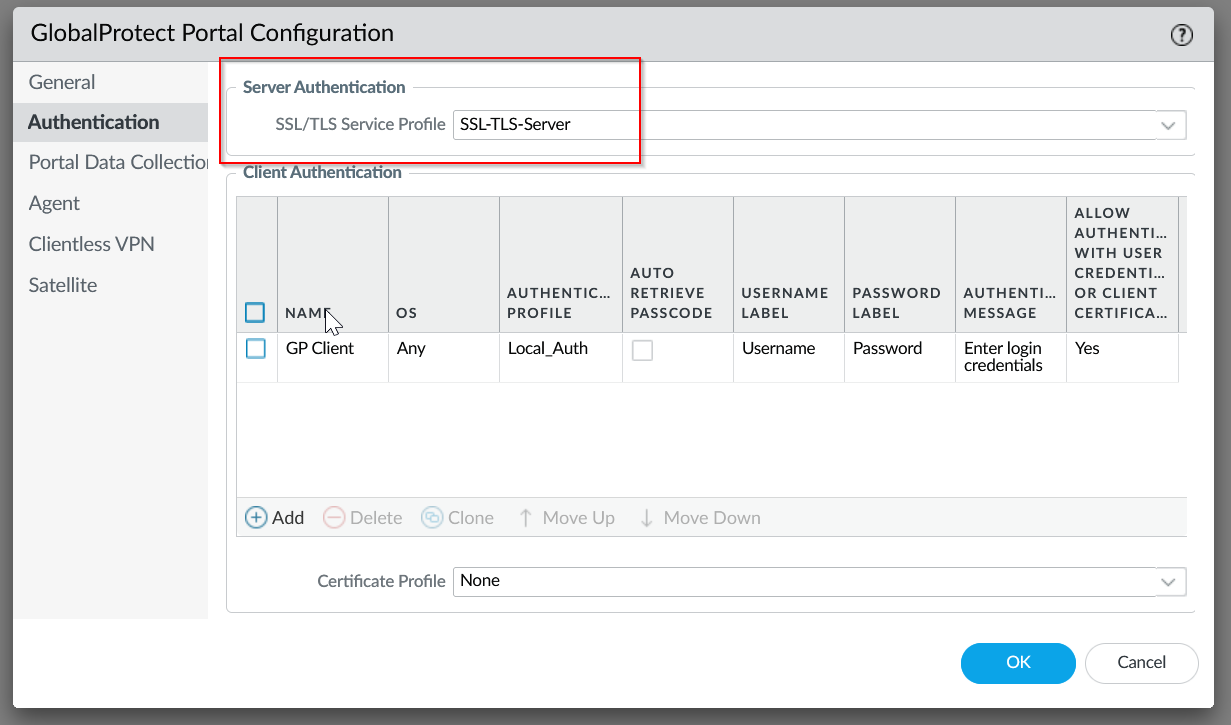
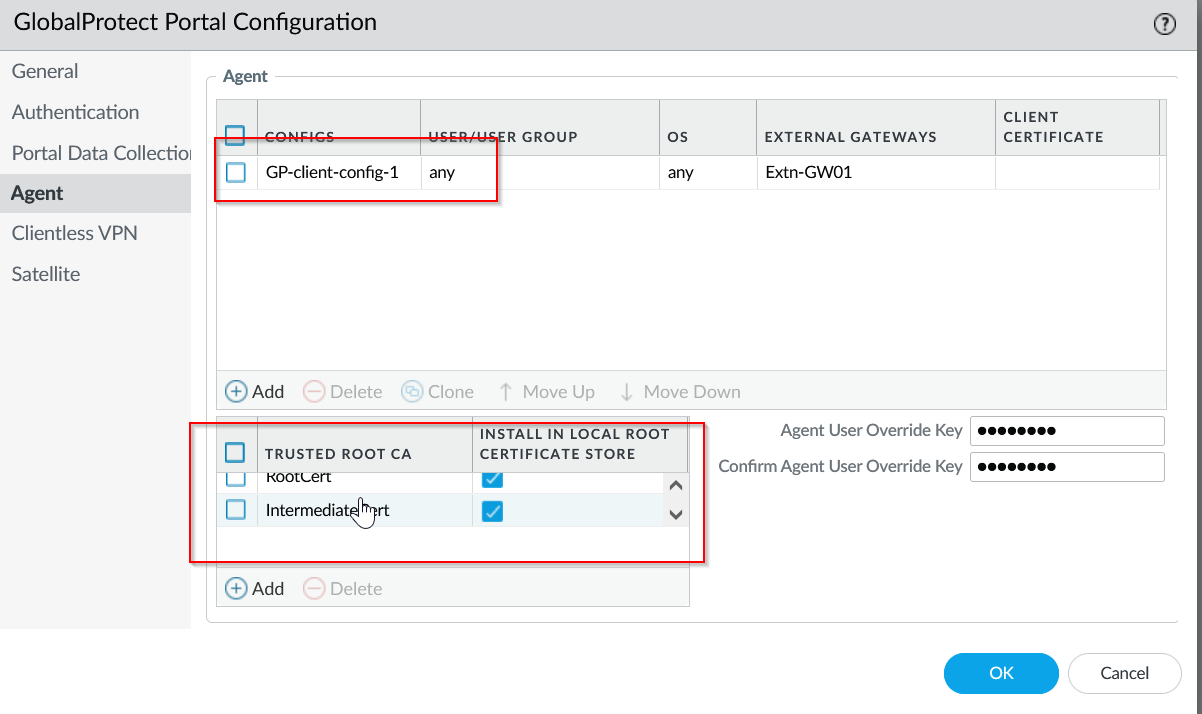
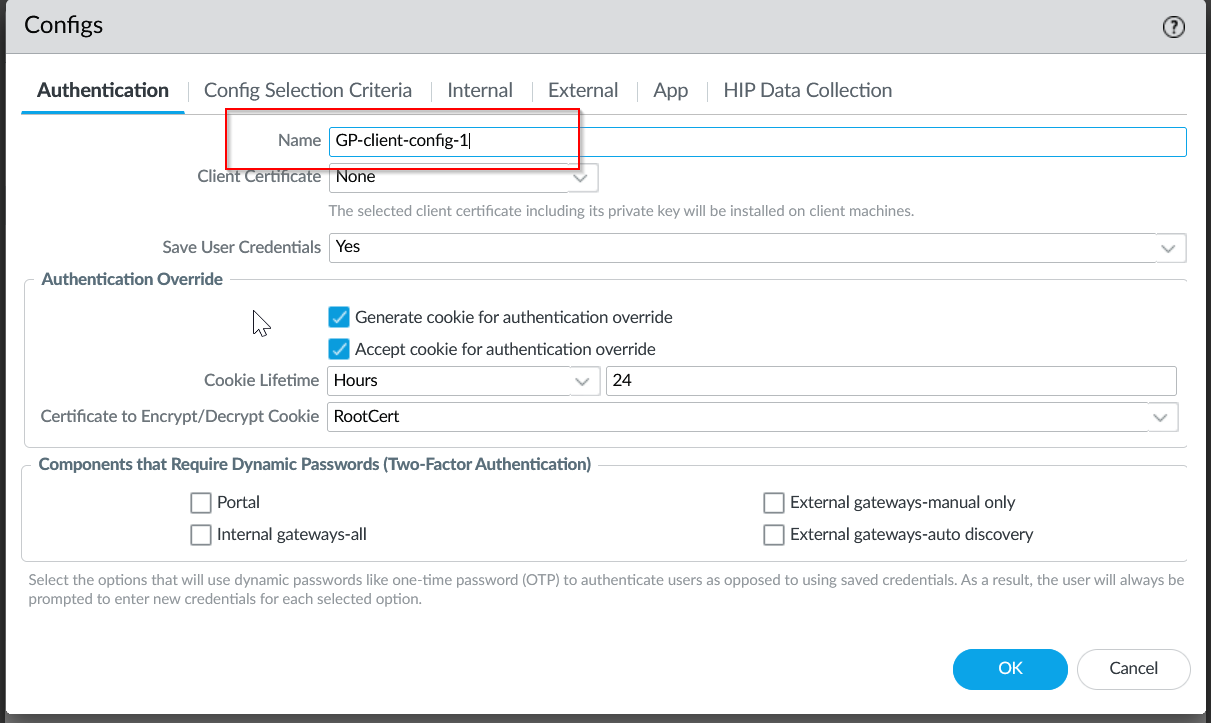
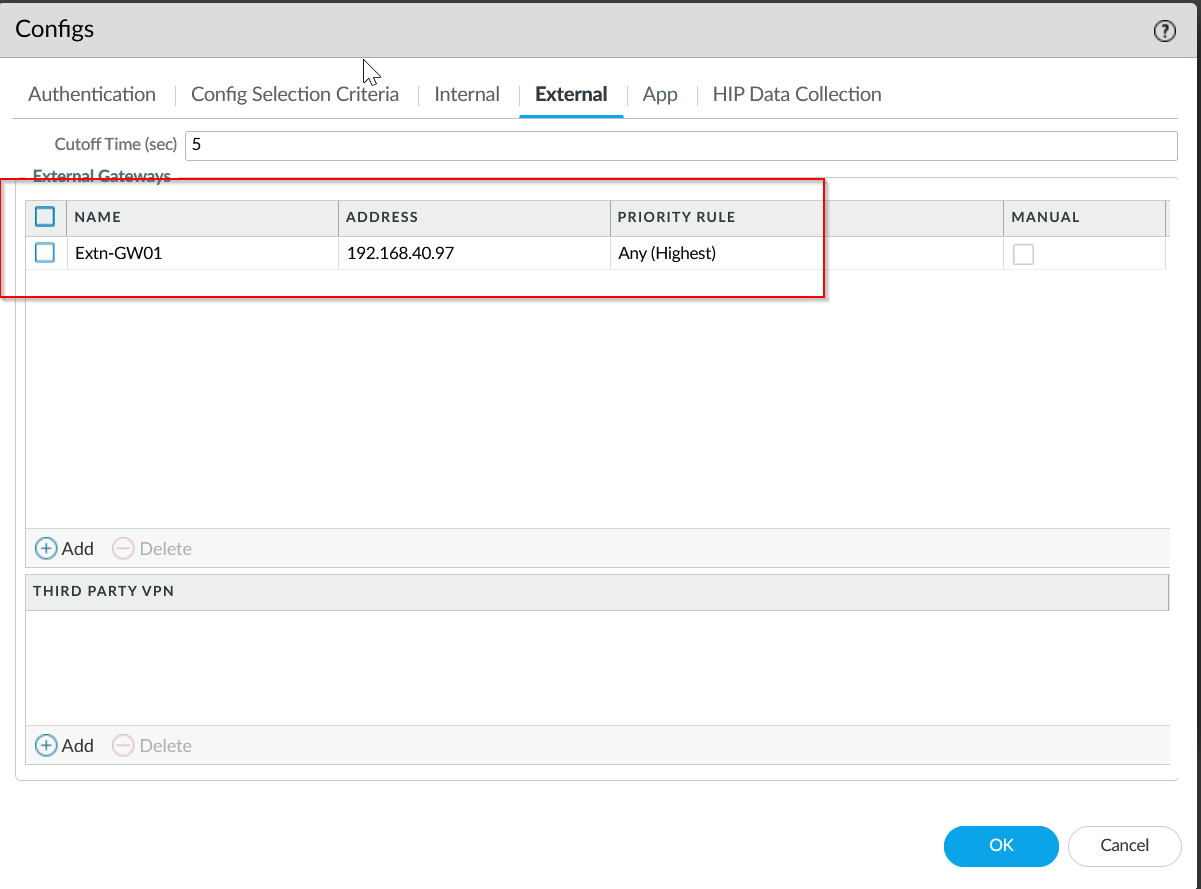
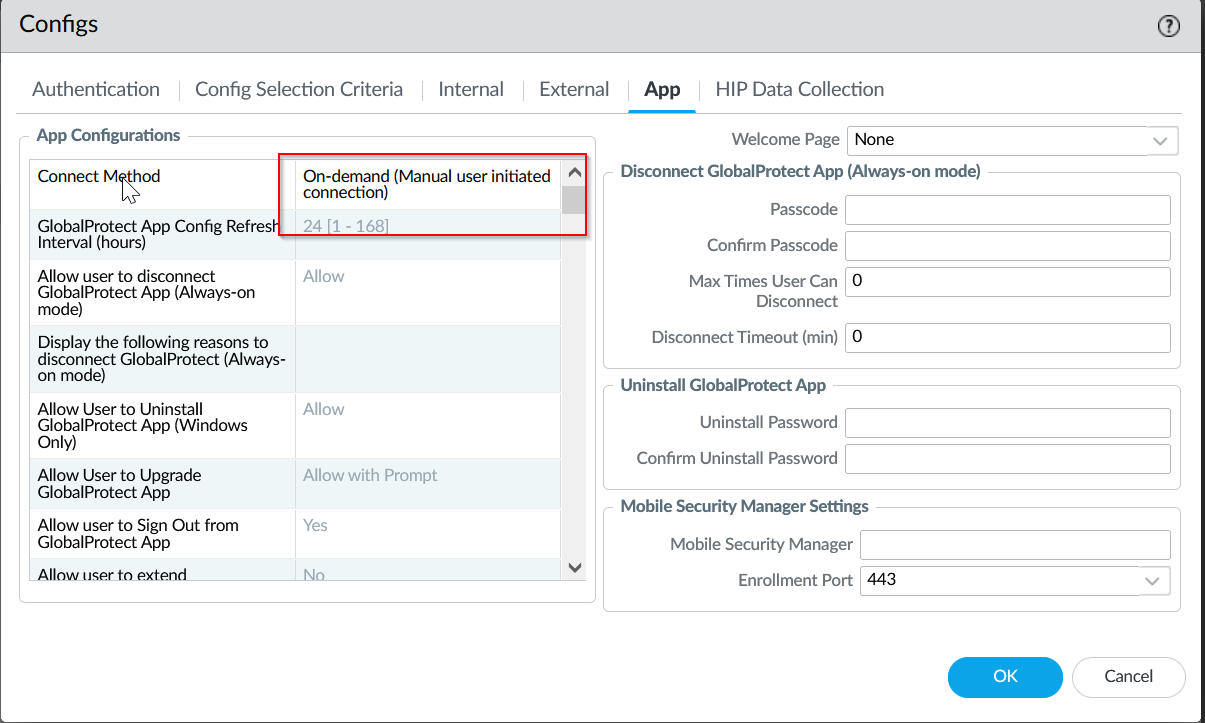
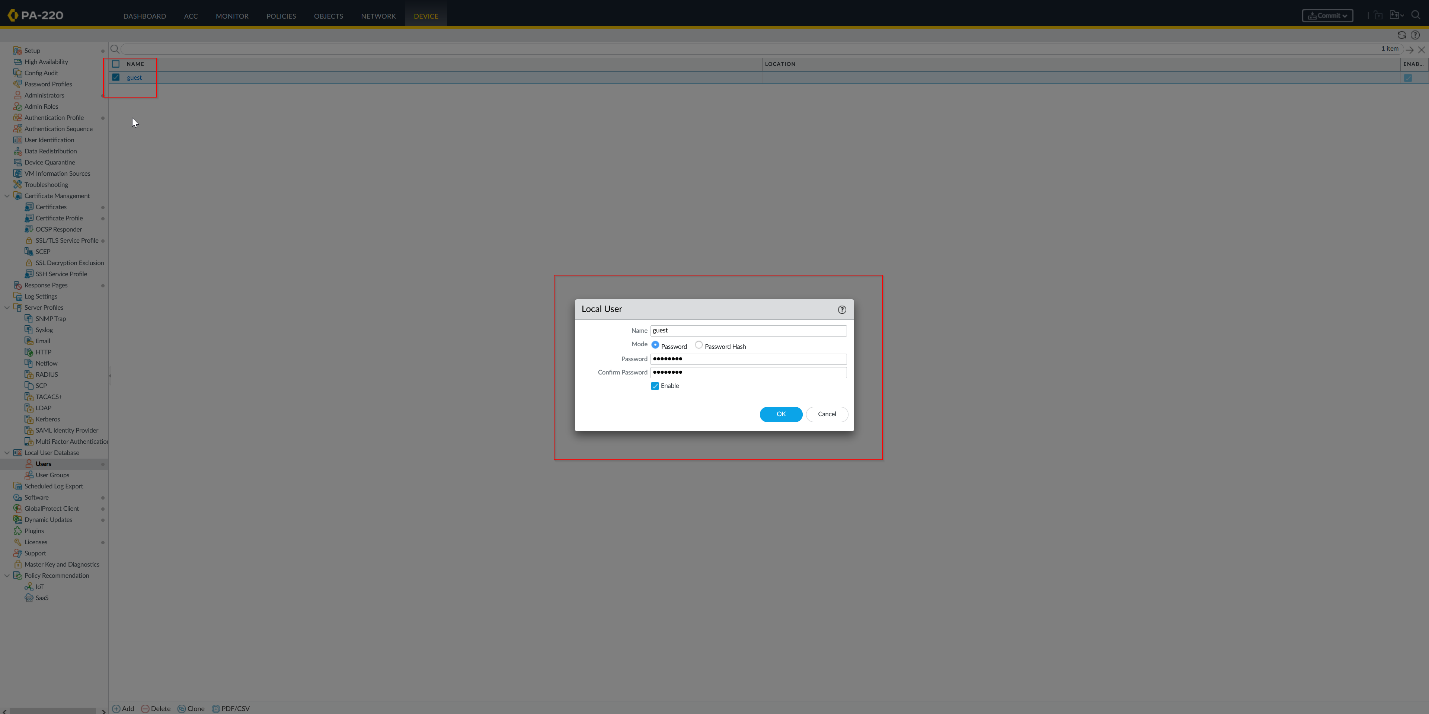
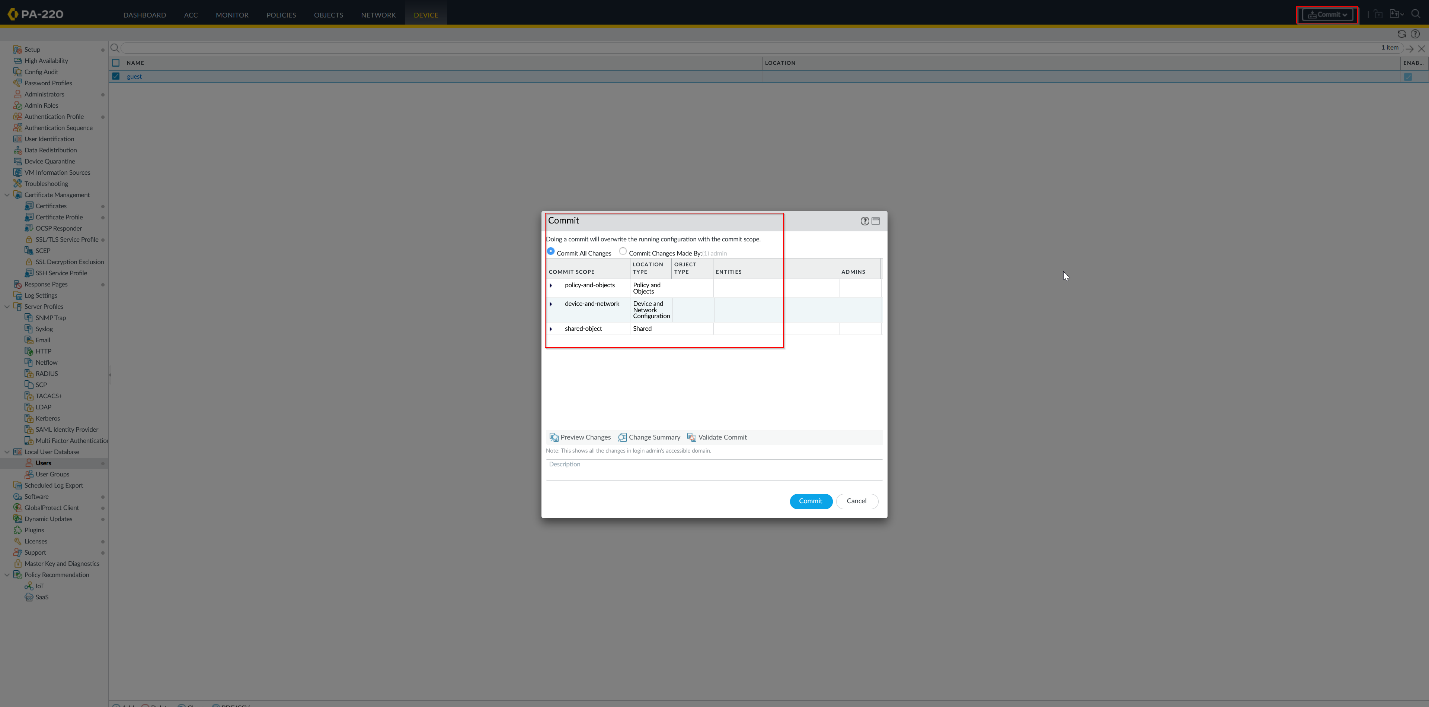
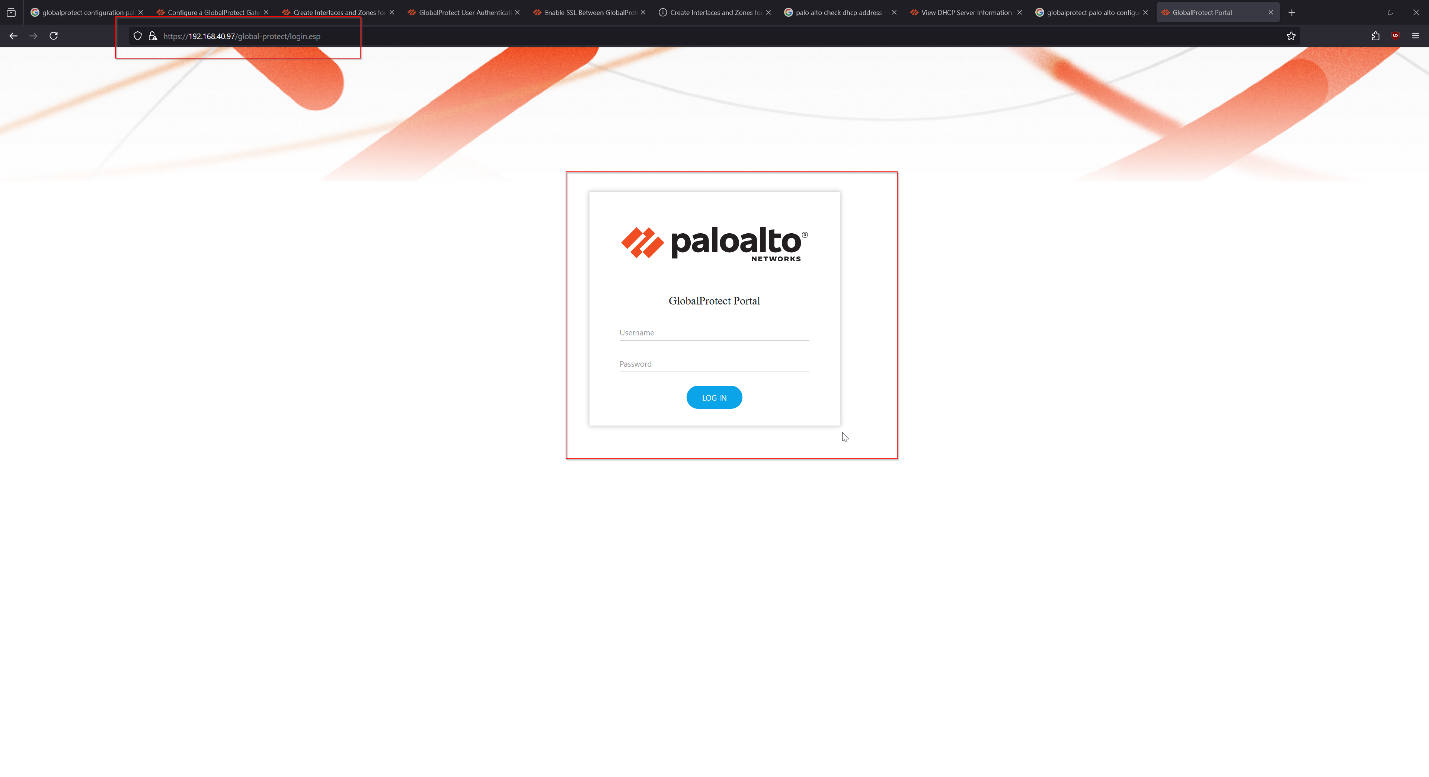
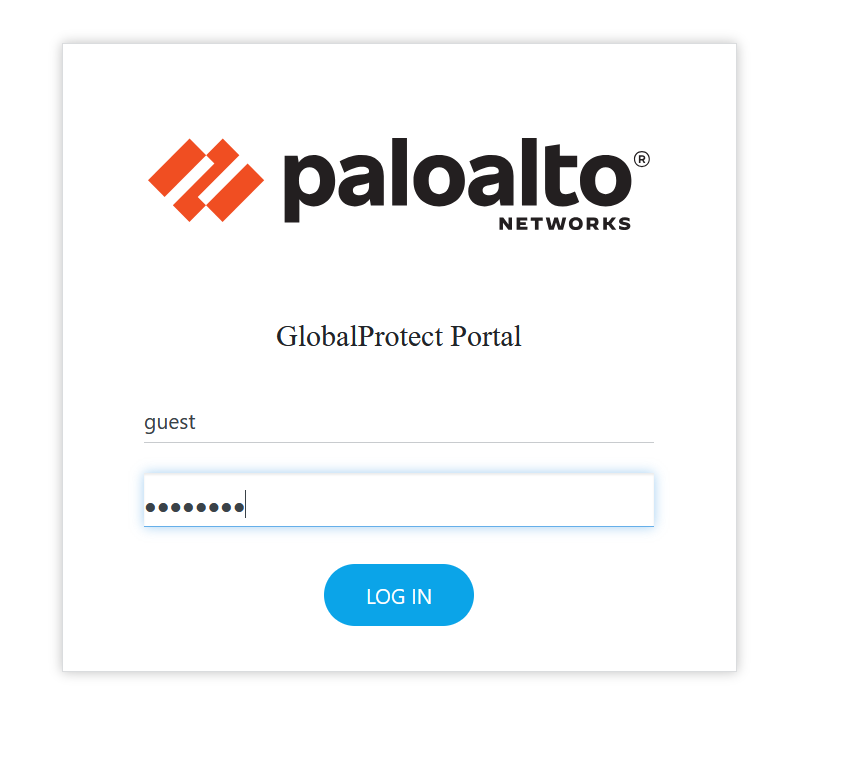
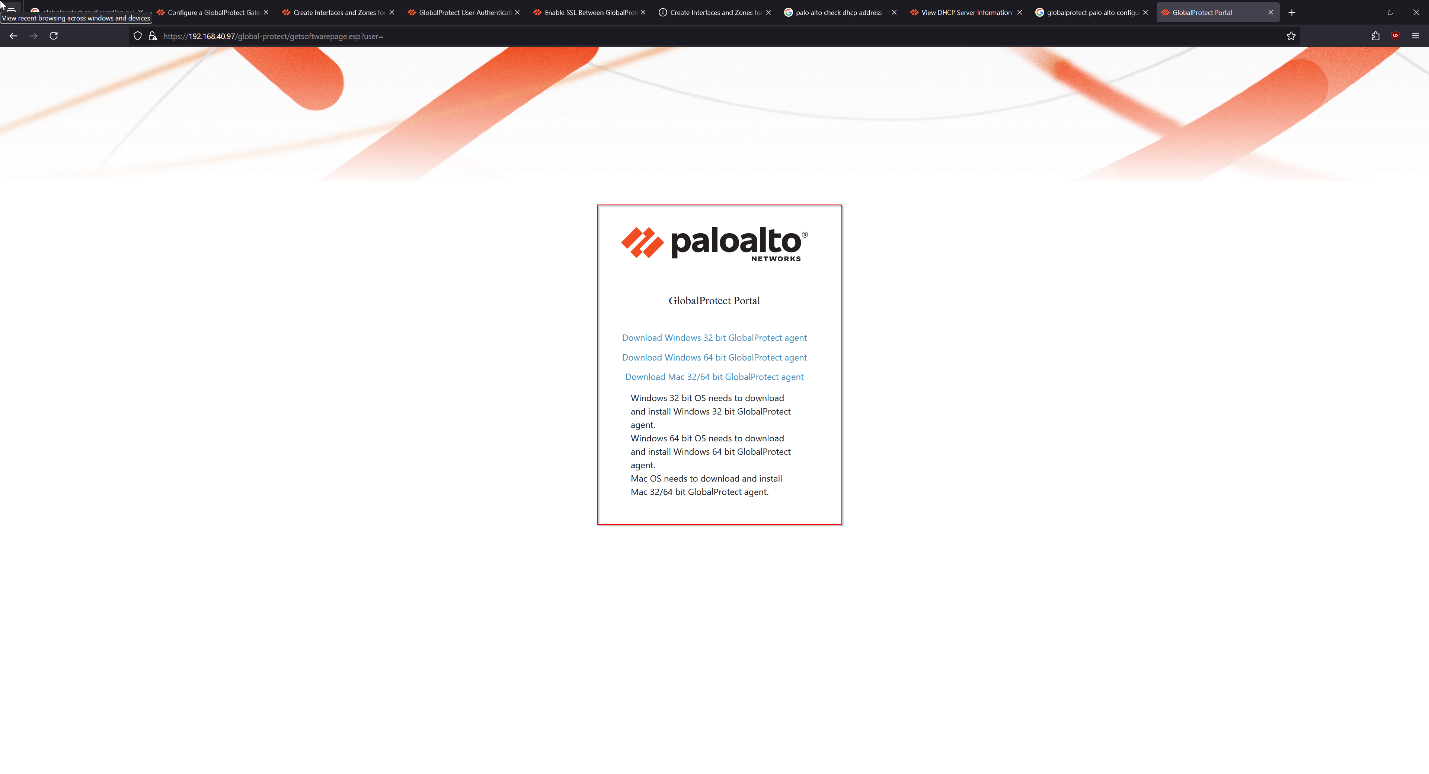
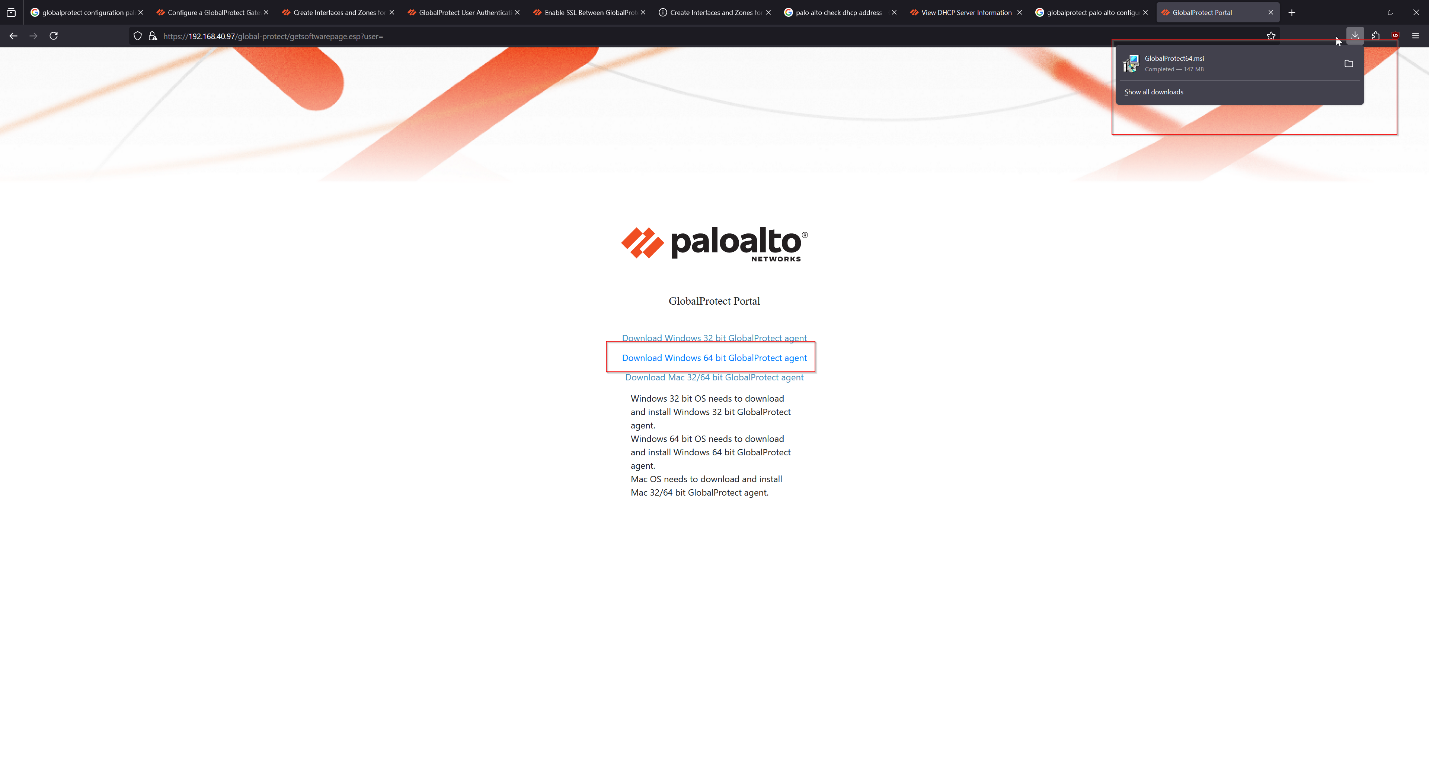
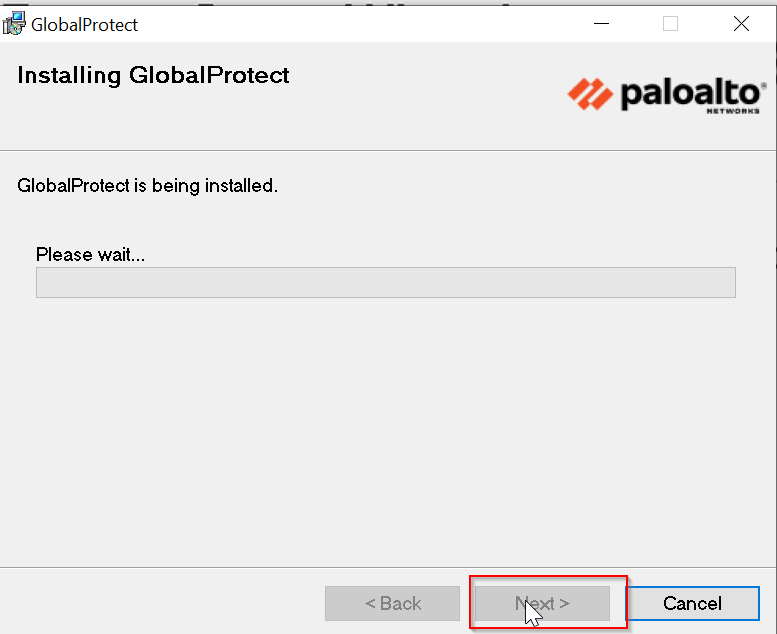
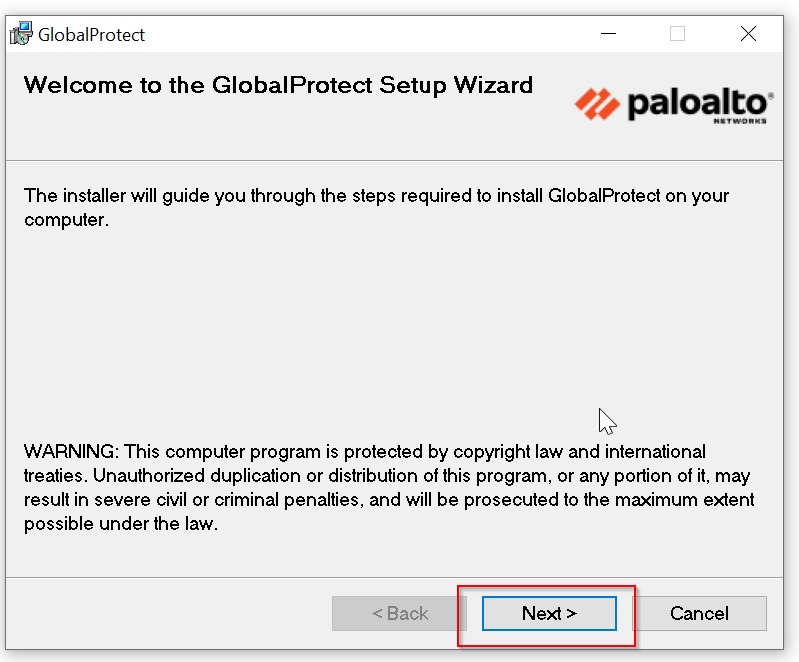
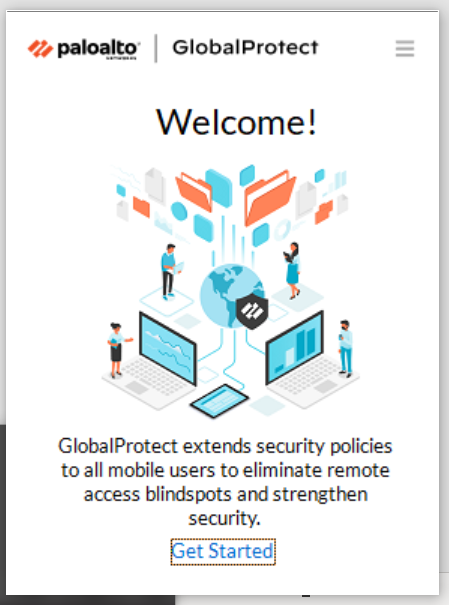
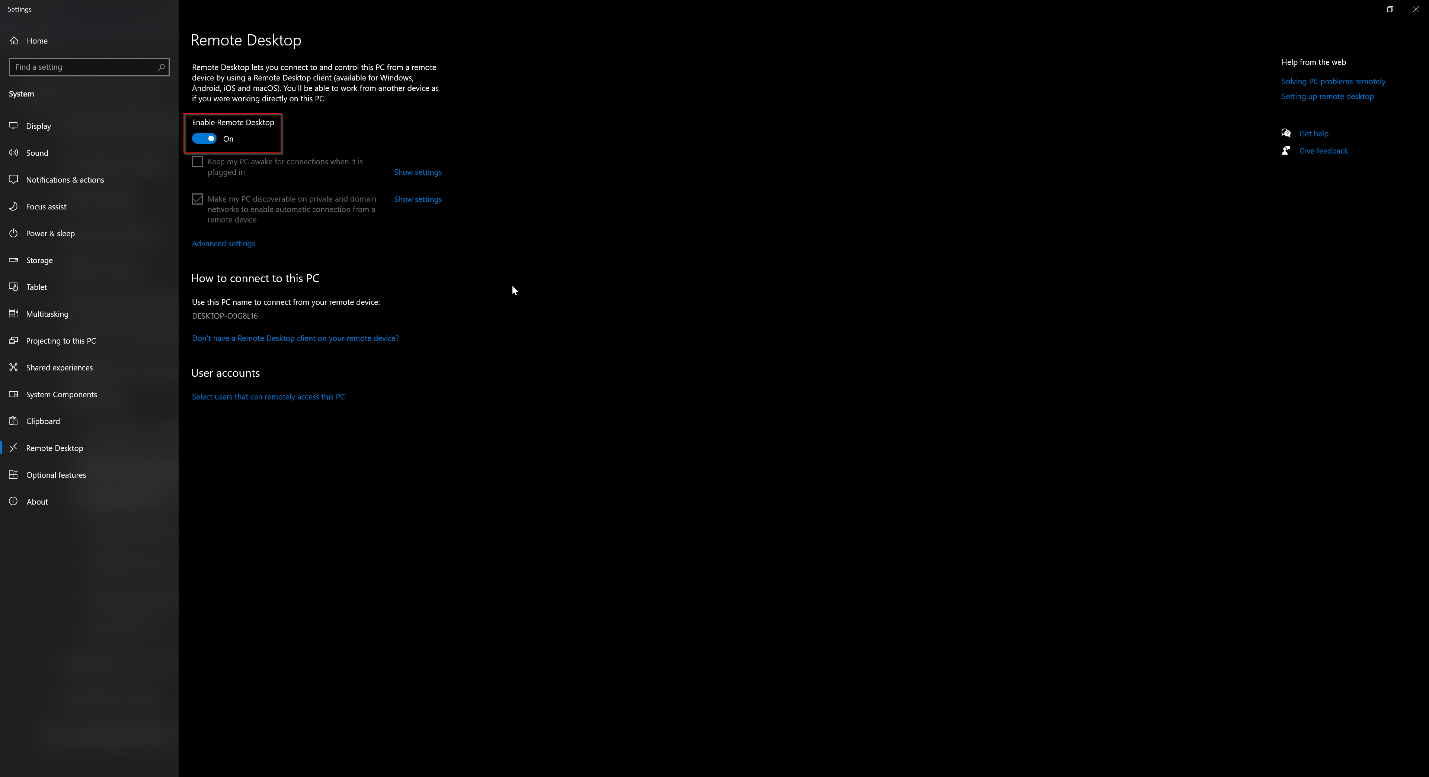
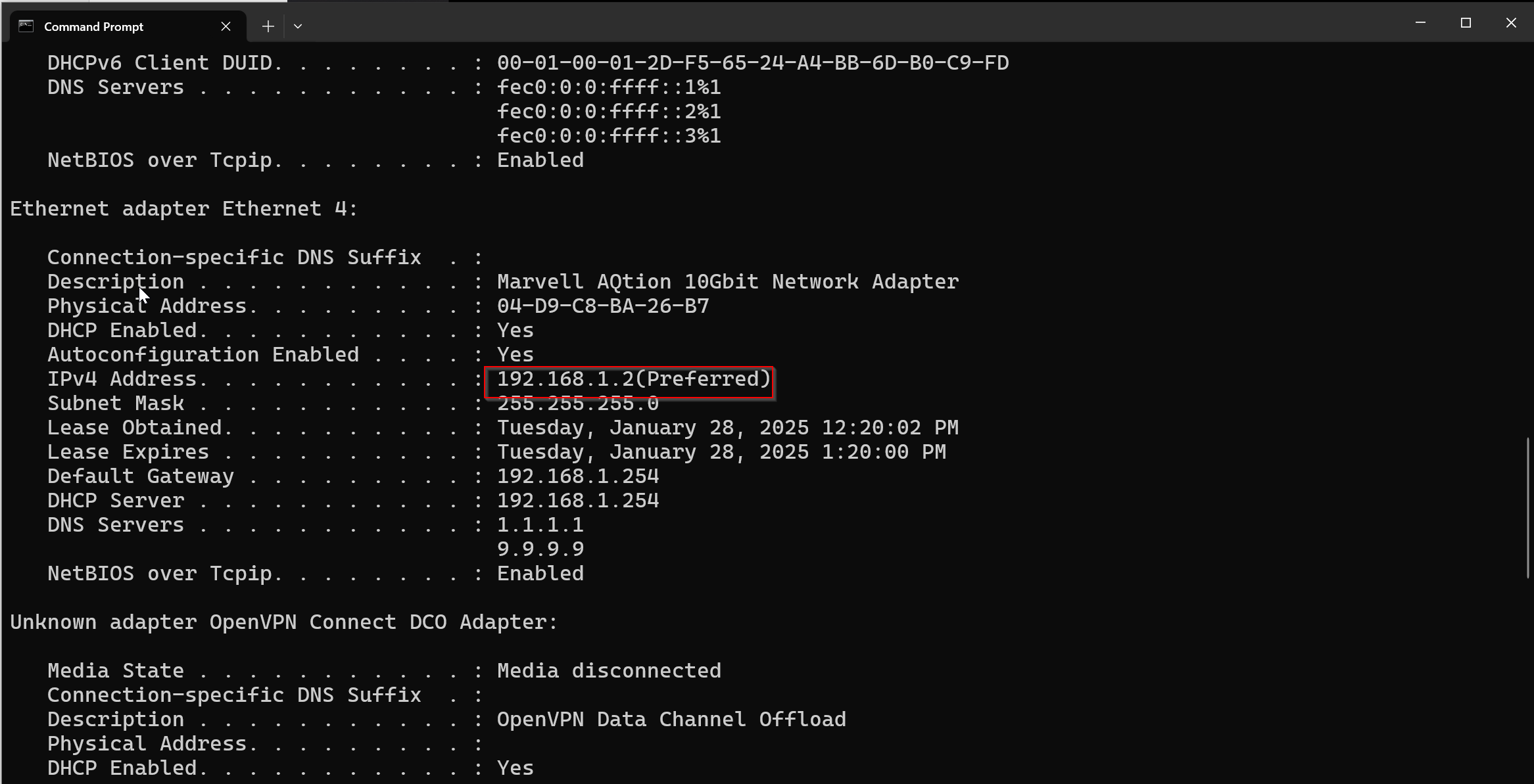
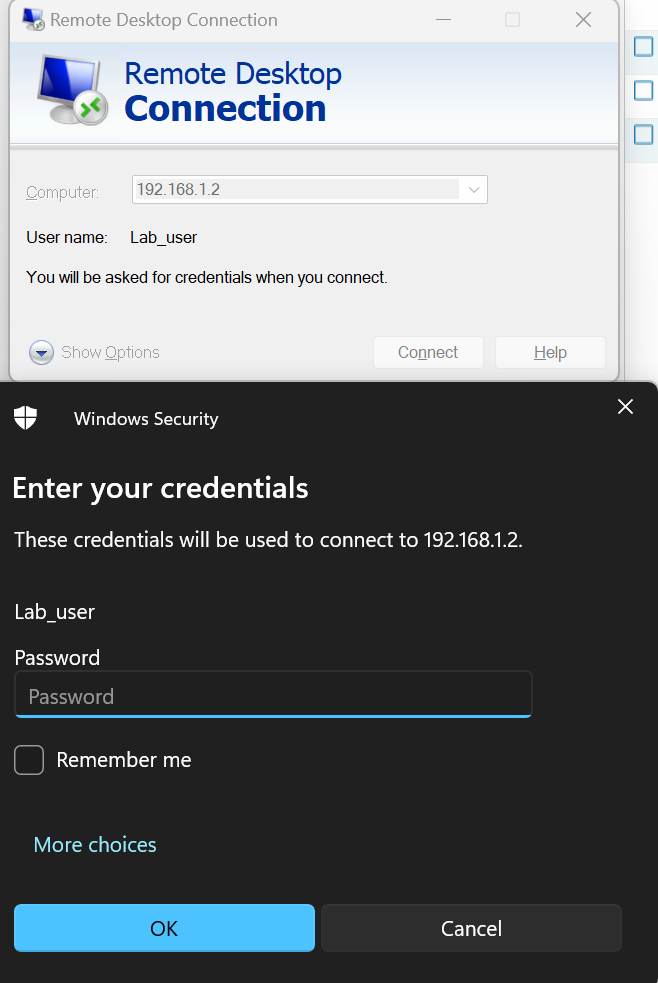
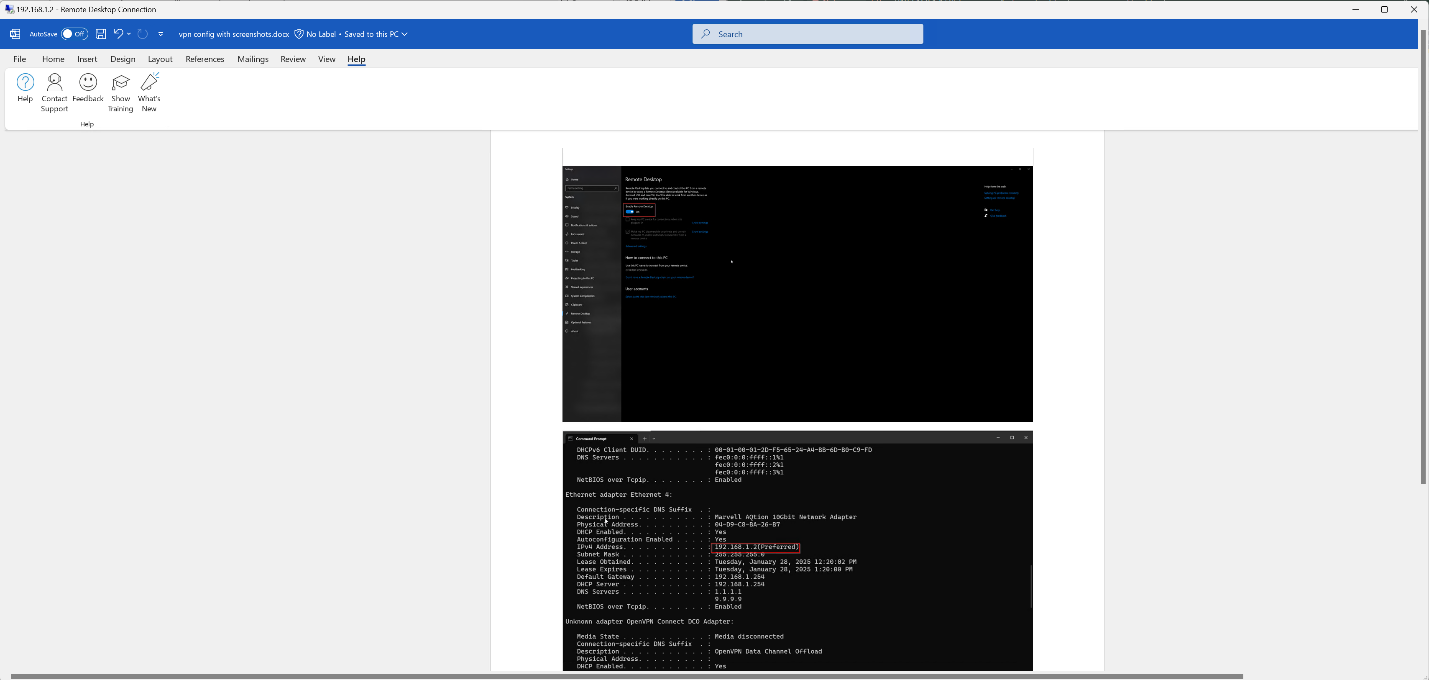
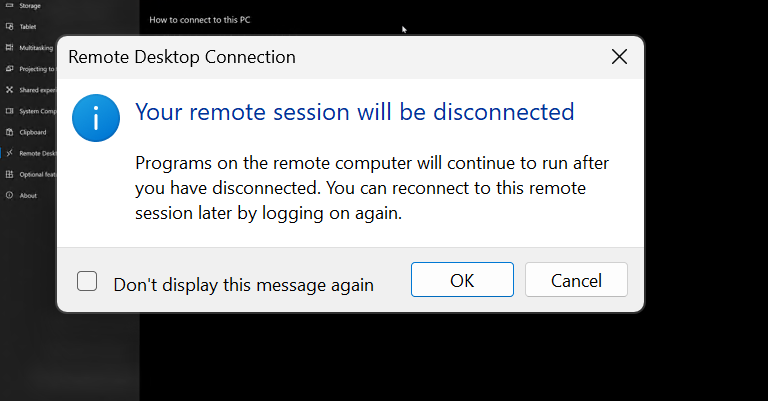


1. Next, we need to navigate to SSL/TLS Service Profiles and create a new profile for our VPN to encrypt traffic. This was previously done in URL filtering, but needs to be done again.



1. Create the server profile as mentioned. 
2. The server profile should include the root certificate and the intermediate certificate. 
3. Now, install the certificates on end user devices. Open Windows MMC. 
4. Add the certificates as a snap in and set it to be local.  
5. Install the certificates as Trusted Root certificates.  
6. Now, we can continue with setting up the actual GlobalProtect. Verify that the Device Certificates are correctly created as so. They should be in a hierarchy. 
7. Now, navigate to Device > Authentication Profile. Create a new “Local\_Auth” authentication profile. This will be used for authenticating users with GlobalProtect. 
8. Next, create a tunnel for the GlobalProtect traffic. This interface will be used to “tunnel” the traffic from the insecure outside network into the inside network. 
9. The tunnel should be set as a Untrust-L3 zone, since it is taking in traffic from the outside. 
10. Finally, we can create our GlobalProtect portal. Navigate to Network > GlobalProtect and create a new portal. Enter the following: 

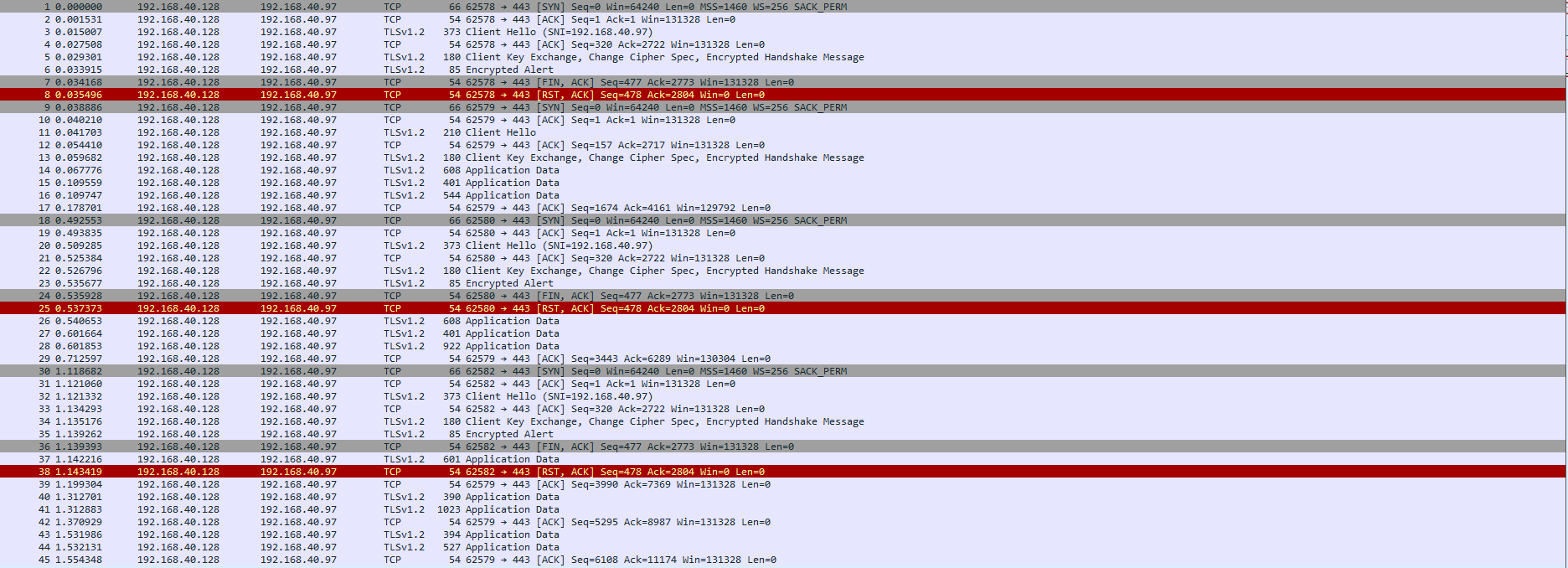


1. Select the SSL/TLS profile that was created in the previous steps for the authentication section. 
2. For the agent section, add your root and intermediate certifications created earlier, and create a new agent. 
3. Your agent should follow these settings: 
4. Make sure to set the external gateway. This is important! It must be the IP address of your outward facing address, otherwise end users will be unable to reach your setup. 
5. The connection type should be On Demand, allowing users to connect whenever they want. 
6. Create it, and navigate to Device > Users. We can finally create our local user for testing now. 
7. After we finish this, we are done with configuration. Commit changes and proceed to testing. 
8. Navigate to the outward facing IP address. It should show the GlobalProtect portal. This is where we will download our VPN client on our end devices. 
9. Input the credentials of our test user that we just created. 
10. After a successful login, we can download our GlobalProtect VPN that is hosted by our firewall. 
11. In this case, since we are running Windows, we should use the Windows 64 bit variant. 
12. Download and install the GlobalProtect client. 
13. After a successful installation, GlobalProtect client should look like this. 
14. Our final step is to configure RDP normally, as if we were using it locally. Since the VPN will tunnel our end user into the local network, we can test our RDP with local configurations, then test it when our VPN is on. To enable RDP, navigate to the Windows settings and turn it on. 
15. Find the IP address of the RDP host using “ipconfig” in a CMD terminal. This will give you the local address that we will use to connect. 
16. Now, we can enable the VPN client with the address that we previously configured of the outward facing interface. 
17. Notice that you receive an IP address inside the network. This is from the tunneling. Now, we can successfully initiate an RDP connection with the host.
18. Success! Note that the RDP connection works, and we are looking at the host machine. 
19. Disconnect the VPN client. Our configuration is now complete. 

**Packet Captures:**

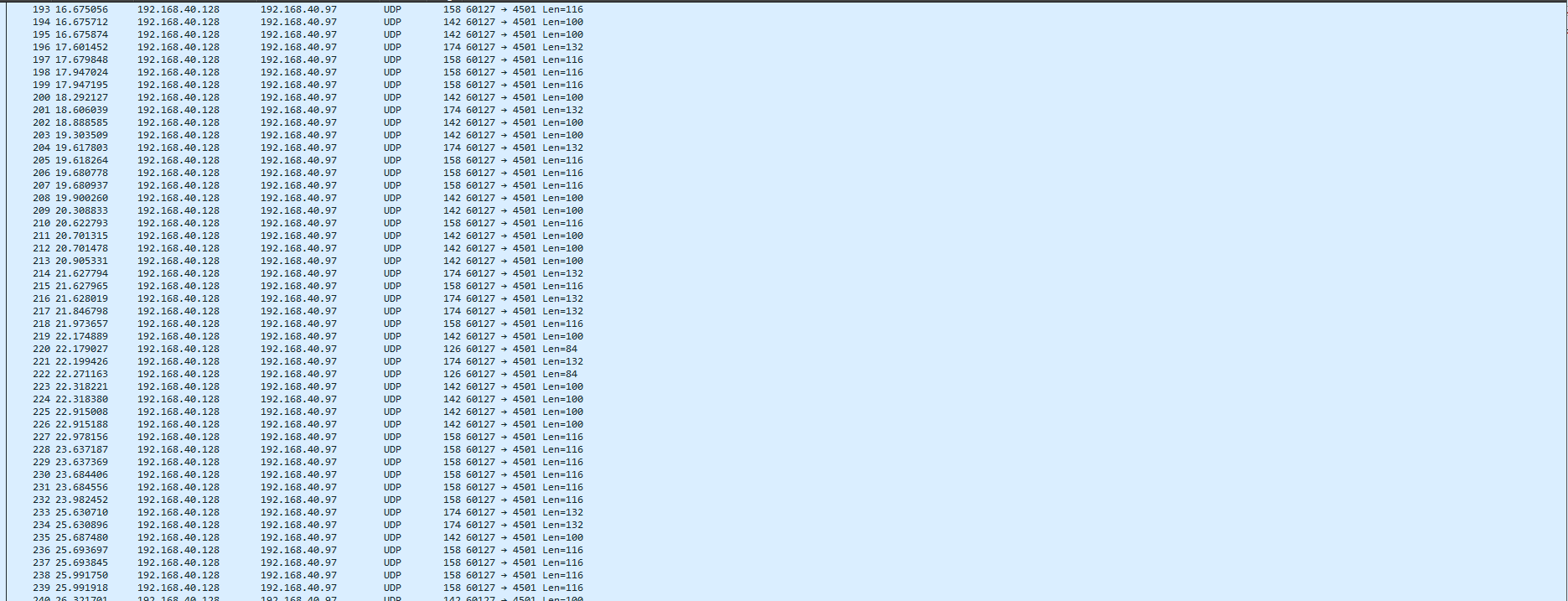
Packet captures most accurately display the functions of our VPN. We can see that the packet capture on the interface from the external network (the side that connects into our local network via VPN) has all encrypted traffic exiting. On the other hand, captures from inside our local network on the machine hosting RDP have unencrypted traffic. Conceptually, this functions exactly as expected. Our VPN should tunnel encrypted traffic through an external, insecure network into our internal network, where it is then unencrypted to communicate with internal services.

First, let’s take a look at the external computers captures:

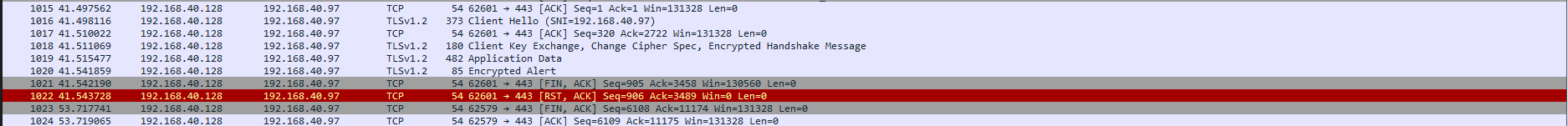


We initially see a back and forth, which is the VPN connecting. This establishes the connection through exchanges of certificates and keys, which are used for the rest of the session.

From there, all we can see is UDP traffic:

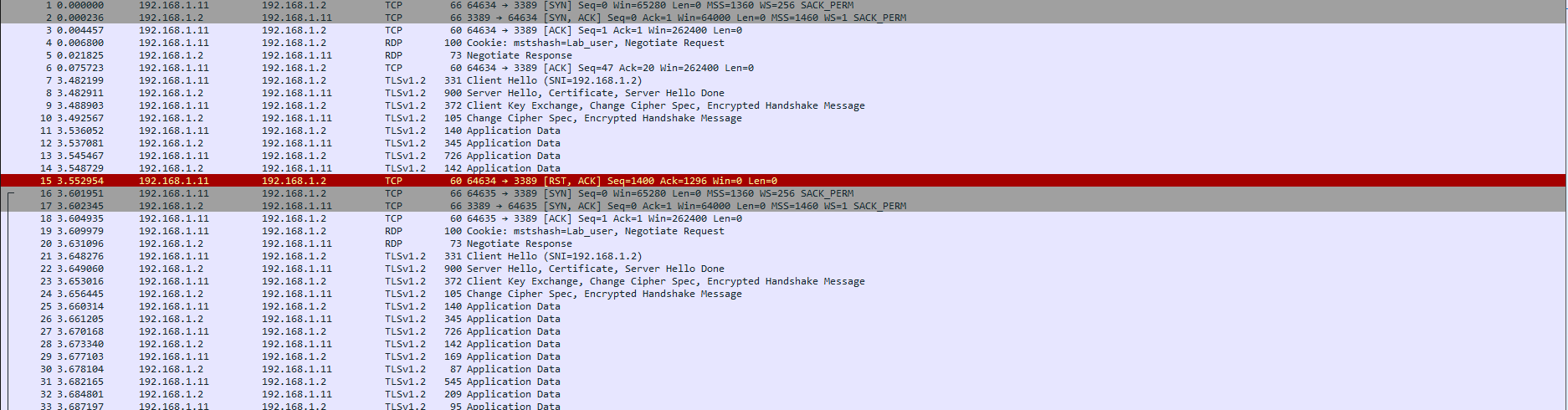


This continues for the rest of the session, until we finally disconnect from the VPN with a SYN ACK.



This UDP traffic does not show labelled as RDP, even though we know that it is. This is because it is encrypted. RDP itself runs off UDP in order for fastest speed, which is how we know that this traffic is the RDP connection. This proves that the VPN is correctly encrypting our traffic. A middle man would not be able to decrypt this traffic without the necessary certificates and keys, ensuring security in the connection.

Now, let’s take a look at how this differs from the traffic inside the network. We see the unencrypted version now:



Note that the RDP packets are now labelled, and that application data is sent unencrypted. This is expected, since we are capturing data from the local side, after the VPN packets have already been decrypted by our firewall.

Finally, we see a stream of RDP packets, mirroring those of the UDP packets we previously saw. The only difference is that this time, they are unencrypted.



As we can see, the VPN functions as expected, encrypting traffic between an unsecured network in order to connect to another, local network in a secure manner.

**Problems:**

1. **Not Downloading PA GlobalProtect Agent Files**

When we first configuring the VPN, we mistakenly thought that the actual GlobalProtect client files would come pre-installed and available to install on our portal page. However, this is not the case. The “.msi” files need to be retrieved from the Palo Alto servers, from which they can then be downloaded on end user devices through the portal. This mistake has us debugging for a while, because the links on our portal would always download a dummy file. Initially, we thought this was because of an incorrect configuration with the GlobalProtect portal, thus leaving us guessing what the issue.

1. **“Fake” Public Address – Internal Lab Network**

Since this lab is done a “shared” setting – meaning that we are emulating a production environment inside our class – we have to use an internal address as our “public” address. Due to the number of groups in our class, as well as security concerns, it would be impossible to assign everybody a public address for testing. Because of this, our teacher has a LAN that all groups should consider as a “public” network, simulating the broader internet. Due to not understanding this difference at first, we didn’t know what address to put as our outward facing portal.

**Conclusion:**

This lab is a great introduction to understanding both how VPN’s work and why they work. In order to configure the VPN server, we first needed to understand the principles behind a VPN, and how they tie together. Furthermore, this lab did a good job at introducing the GlobalProtect VPN service, and how to deploy it in an industry setting.

VPN Configuration Signoff Sheet

Ryan Chen, P3-4 Cisco Cybersecurity, Mr. Mason

