A close up of a sign

Description automatically generated

**Purpose**

This lab is essentially a walkthrough of the configuration of the Global Protect VPN, which allows separate desktops to remotely connect with devices on external networks. This common configuration allows for seamless communication between remote devices while ensuring security and functionality.

**Background Information**

A VPN, standing for virtual private network, is a digital, nonphysical connection between a computer and a remote server that is owned by a VPN provider. This creates a point-to-point connection from a remote area while also encrypting all personal data and IP addresses, and safely bypass blocked websites and firewalls.

So why do people use VPNs? VPNs are widely incorporated in school or office environments to allow staff and students to access exclusive resources securely from remote locations, which is especially useful when working from home nowadays. VPNs are also used to mask one’s IP address, leave their browsing history untraceable, and access sites that would usually be blocked in a certain region. VPNs are also a secure method of blocking ISPs from tracking your browsing history and ensuring that your personal data remains private, as connections to one’s ISP can easily lead to malicious activity.

A VPN tunnel is a secure and private connection between a client and VPN server which keeps data travel encrypted over the Internet. Tunneling conceals a client’s IP address and secures their data, which is a good option for when you’re operating a device on an unsecure public network. In order to set up a VPN tunnel, you must first select a VPN service to connect your device to the VPN server and establish a tunnel. Then, the tunnel encrypts data into “ciphertext,” which is then decrypted once it reaches the VPN server. Lastly, the data travels back to the user with the same encryption, ensuring safe data transmission both ways at all times.

On our Palo Alto PA-220 firewall, we implemented the GlobalProtect VPN, which is the VPN developed by Palo Alto Networks. GlobalProtect allows users to benefit from the safeguards of a VPN in conjunction with firewall safety. Like the usual VPN, the GlobalProtect VPN allows users to remotely access a company’s resources across any device and uses strong encryption protocols such as SSL and IPSec to protect data communications. GlobalProtect also, however, has a feature that includes Palo Alto’s Next-Generation Firewall securities that adds additional protection in data transfer, ensuring that *only* secure devices may connect to the network. GlobalProtect is designed to be highly scalable with different organizations and provides high visibility when monitoring users accessing the network. In this lab, we are using the GlobalProtect VPN to connect a desktop to our remote network.

**Lab Configurations**

First, enter the GUI and click on “Device.” Under “Certificates” click “Generate” at the bottom of the screen.

**A screenshot of a computer

Description automatically generated**

The specific certificate configurations are shown below.

1. Create a **Local** Certificate, naming it *RootCert*. Make sure that the Certificate Authority box is checked.Under Cryptographic Settings, choose the RSA Algorithm, 2048 Bits, and sha256 for Digest. The configuration should save:

**A screenshot of a computer

Description automatically generated**

1. Now, create a new Local Certificate, called *IntermediateCert* and make sure this certificate is **Signed Off** by the *RootCert* we initially generated.

A screenshot of a computer

Description automatically generated

1. Create one last certificate called *ServerCert,* which will be **Signed Off** by the *IntermediateCert* in step 2. Make sure that the certificate’s **Common Name** is the IP address of your GlobalProtect Portal. Do not choose Certificate Authority for this certificate. The configuration should save like this:

**A screenshot of a computer

Description automatically generated**

Under “SSL/TLS Service Profile,” click “Add.” Name the new profile *SSL-TLS-Server.* Set Certificate to *ServerCert.* Set the Min Version to TLSv1.0 and Max Version to Max.

**A screenshot of a computer

Description automatically generated**

On the GUI sidebar, go to the “Certificate Profile” and click “Add.” Name the profile *Client-CertProfile* and click the “Add” button to make sure *RootCert* and *IntermediateCert* are added.

**A screenshot of a computer

Description automatically generated**

Enter the Run Dialog window and type “mmc” and click “OK” to open.

**A screenshot of a computer error

Description automatically generated**

Click “File” at the top left corner and navigate to “Add/Remove Snap-in.” Select “Certificates” 🡪 “Add” 🡪 “OK.” **A screenshot of a computer

Description automatically generated**

Now, import the following Certificates to the following folders: *ServerCert* to *Personal* folder, *RootCert* to *Trusted Root Certification* folder, and *IntermediateCert* to *Trusted Root Certification Authorities.* The folders are shown below:

**A screenshot of a computer

Description automatically generated**

Go to the “Network” tab at the top of the GUI and select “Interfaces” 🡪 “Tunnel.” Add a new interface called “tunnel” and put the Virtual Router to default and Security Zone to Untrust-L3, a security zone that we created in a previous lab.

**A screenshot of a computer

Description automatically generated**

Go to the “GlobalProtect” tab on the left and go to “Portals” to configure a new portal:

**A screenshot of a computer

Description automatically generated**

Instead of clicking OK, check the tabs on the left to make sure the following configurations are made:

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

Now, configure the GlobalProtect Gateway Configuration:

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

Go to the “Device” tab on the GUI and enter “Users.” Create a new Local User and make a memorable name and password for the user. This will be used to sign into the remote desktop later on.

**A screenshot of a computer

Description automatically generated**

Commit all changes:

**A screenshot of a computer

Description automatically generated**

On a separate client, enter the IP address of your portal to reach this webpage. Sign in using the Local User account created earlier.

**A screenshot of a login screen

Description automatically generated**

Download the client:

**A screenshot of a computer

Description automatically generated**

Make sure you establish an administrator account through Settings. Here, the account is named “Flora.” Enter the IP of the computer and click “Connect.”

**A screenshot of a computer

Description automatically generated**

Enter the administrator’s password for safety:

**A screenshot of a computer security login

Description automatically generated**

All steps have been completed, and now the new client will be able to remotely operate the same screen as the other desktop!

**A screenshot of a computer

Description automatically generated**

**Problems**

The first issue we came across was with unforeseen problems with our firewall starting up. We were not able to access the GUI although the internet connection was stable, and the firewall kept resetting every few minutes. Trying a full factory reset did not help either and we finally realized that the PA-220 itself was malfunctioning, so we ended up using a different one as the issue remained within the hardware.

When troubleshooting near the end of the lab, we realized that one of the default gateways was incorrectly configured and we had overlapping IP addresses. When we realized that we were unable to connect to the Internet, we immediately had the intuition that there could be an issue with the default gateway, since this had occurred in a previous lab. The IP address of the default gateway and the VPN portal were mixed up within the GUI, and was an easy fix as we could easily switch out the overlapping IP addresses.

We were also unable to retrieve licenses on the remote desktop, which we eventually fixed by uploading the licenses into a flash drive and downloading them onto the new client.

When first launching the Remote Access session, we were unable to sign in. By redownloading GlobalProtect and creating a new local administrator user, we were able to sign in and launch the Remote Access desktop to prove that the VPN worked.

**Conclusion**

VPNs are very commonly implemented in the real world, and learning the skills used in this lab is a key step towards becoming an effective cybersecurity engineer. Working through this specific scenario taught us to expand corporate networks to be more accessible for remote users and reinforced concepts, such as authentication and troubleshooting, from our previous labs in this course.

**Signoff**

A paper with a logo

Description automatically generated