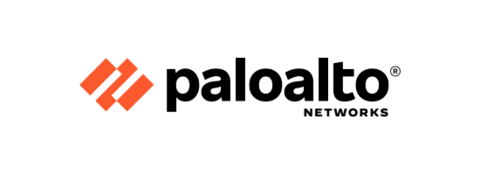


Palo Alto 410 Remote Access with GlobalProtect Configurations

Sophia Zhang | Period 5 Cybersecurity | 2022-2023



**Purpose**

The purpose of this lab was to configure remote access using GloblaProtect on a Palo Alto 410 firewall.

**Background**

Remote access VPNs are very important to organizations since they provide secure access to their internal networks from remote locations. GlobalProtect from Palo Alto, is a popular solution for remote access VPNs. GlobalProtect allows for reliable connectivity and access control for remote users, using VPN technology to make an encrypted tunnel between a device and the network. Most importantly, GlobalProtect ensures that all data stays secure while being transported.

Global Protect has many distinct features that makes it efficient and very popular for remote access VPNs. First, it uses multi-factor authentication, which increases another layer of security for users. It also allows for an ideal experience, since we can easily and seamlessly access the network from many different devices, whether that’s a phone, computer, or desktop.

Also, GlobalProtect is capable of centralized management and monitoring. Centralized management allows administrators to have visibility into connected users, their devices, and everything they are doing. This way, organizations are able to enforce security regulations, detect security breaches, and solve problems quickly and efficiently.

Lastly, GlobalProtect has very efficient access control abilities. Organizations can create smaller policies and rules to control which users are able to gain access to the network. These rules include user identity, location of the device, and type of device. GlobalProtect also uses existing security information, including firewalls and threat prevention systems, to further protect against security breaches and threats.

Because of all of these positive features of GlobalProtect, it is a popular and excellent solutions for organizations who are looking for a way to secure remote access to their networks. There are effective security measures, helping organizations ensure that their networks are safe.

**Lab Procedure**

Step 1: Delete the Virtual Wire.

Step 2: Connect the management interface to the internet (we did this by configuring a WAN port that allowed the firewall to connect to the internet. Then an interface was configured to allow a layer 2 connection to the management interface).

Step 3: Got to Device, interfaces, ethernet1/1, and change the virtual router to default. Graphical user interface, text, application, email

Description automatically generated

Step 4: for security zone, click create new and name it “INTERNET”

Graphical user interface, application

Description automatically generated

Step 5: go to Ipv4 tab and set a static IP address of 192.168.100.240/24

Graphical user interface, text, application, email

Description automatically generated

Step 6: open ethernet 1/2. Set the interface type to layer 3 and virtual router to defaultGraphical user interface, text, application, email

Description automatically generated

Step 7: create a new security zone and name it “INSIDE”

Graphical user interface, application

Description automatically generated

Step 8: go to IPv4 and set a static IP address

Graphical user interface, text, application, email

Description automatically generated

Step 9: Go to Virtual Router, Static routes, and configure the following Graphical user interface, application

Description automatically generated

Step 10: Go to Security Policies, edit the pre-existing rule.Graphical user interface, text, application, table

Description automatically generated

Step 11: configure the following in Source

A screenshot of a computer

Description automatically generated

Step 12: Configure the following in Destination

And tconnectGraphical user interface, application, table

Description automatically generated

Step 13: Configure the following in Service/URL Category

Graphical user interface, application

Description automatically generated

Step 14: Go to certificates and generate a new certificate. Configure the following

Graphical user interface, application

Description automatically generated

Step 15: Go to SSL/TLS Service Profile. Click add and configure the following

Graphical user interface, application

Description automatically generated

Step 16: go to Users, click add, and configure the following

Graphical user interface

Description automatically generated

Step 17: Go to Authentication Profiles, click add, and configure the following

Graphical user interface, application

Description automatically generated

Step 18: Go to Advanced and configure the following



Graphical user interface, application

Description automatically generated

Step 19: Go to Device, interfaces, tunnels, and click add. Configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 20: create a new security zone and name it “VPN”. Enable User Identification

Graphical user interface, application

Description automatically generated

Step 21: Go to Global Protect Portal. Click add and configure the following

Graphical user interface, application

Description automatically generated

Step 22: Go to Authentication and configure the following

Graphical user interface, application

Description automatically generated

Step 23: Click Add and configure the following

Graphical user interface, text, application

Description automatically generated

Step 24: Go to Agents and configure the following

Graphical user interface, application

Description automatically generated

Step 25: click add and configure the following

Graphical user interface, text, application

Description automatically generated

Step 26: Go to External, click add, and configure the following

Graphical user interface, application

Description automatically generated

Step 27: Go to Global Protect Gateway, click add, and configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 28: Go to Authentication and configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 29: Click add and configure the following

Graphical user interface, application

Description automatically generated

Step 30: Go to Agent and configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 31: Go to Client settings, click add, and configure the following

Graphical user interface, application

Description automatically generated

Step 32: Go to IP pools and configure the following

Graphical user interface, text, application, email

Description automatically generated

Step 33: Commit Changes

Graphical user interface, text, application, email

Description automatically generated

Step 34: Go to License and retrieve licenses. Go to GlobalProtect Client and download the latest version

Graphical user interface, table

Description automatically generated

Step 35: Make Certifications

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

Step 36: Put your certificate into the computer you are using global protect on

A screenshot of a computer

Description automatically generated with medium confidence

Step 37: Connect to the other computer using remote access on global protect

A screenshot of a computer

Description automatically generated

Step 38: open the remote user and go to the <https://192.168.100.240>. Log in.

Graphical user interface, application

Description automatically generated

Step 39: Download Global Protect Client

Graphical user interface, text, application

Description automatically generated

Step 40: Run the installer Graphical user interface, text, application, email

Description automatically generated

Step 41: Once it finishes installing, open the Global Protect Client

Graphical user interface, text, application, chat or text message

Description automatically generated

Step 39: connect with 192.168.100.240

Graphical user interface, text, application

Description automatically generated

**Problems**

We had problems factory resetting the Palo Alto 410s. Additionally we had problems configuring IP pools the first time around and had to look through all the configs and update everything. This caused us to have to factory reset again which took a while. After that the configurations themselves went smoothly. For a little while our SOHO wasn’t giving one of our computers a DHCP address, this was due to not automatically obtaining a DHCP DNS. Then we didn’t realize we had to redownload and install all the global protect updates which takes quite a bit of time. We also had to adjust our DHCP pool as for some reason our initial address wasn’t allowing remote access to work. We also weren’t always connected to the correct ports for the remote access to work, but we quickly solved this issue. We had help by other people who were doing this lab to figure out some of our configuration errors but in the end, we got everything up and running.

**Conclusion**

In this lab, we configured remote access on a Palo Alto firewall using GlobalProtect.