

**PALO ALTO REMOTE ACCESS GLOBAL PROTECT**

****Brendon Ahn | Cybersecurity | 2022-2023

**Purpose:**

To configure remote access with Global Protect on a palo alto 410 firewall

**Background:**

Global Protect is a service offered by Palo Alto and requires a download off the firewalls. Global Protect has many useful features for remote access VPNS. It has multi-factor authentication, and you can easily access another device on the network if you are connected to it.

Remote access VPNS are useful to companies that want to access devices from remote places. As long as you are on the network you can connect to any device on it. Say you are trying to access a laptop of an employee who’s not at work. You could easily connect to their device and look at the resources you need. It has reliable connectivity and encryption tunnels that prevent people with malintent from abusing the Global Protect

Global Protect has separate centralized management and monitoring. This reinforces the security of doing Global Protect. The remote access may seem like a risk, but the traffic has enough encryption that you shouldn’t worry about any hackers. Organizations are able to control everything, make policies, amongst other things using this centralization, which makes Global Protect quite efficient.

The process of configuring it is actually simpler than configuring site to site. It requires certificates which you are able to self-sign. The process consists of setting up policies, proxies, DHCP and Global Protect Clients. The lab doesn’t have many issues and it doesn’t require any additional steps other than being on the network for machines not including the firewall. You have to download the Global Protect updates in order to uses it. You can set this on an automatic update and install to make this process a lot faster and for it to require less maintenance.

**Lab Summary:**

We had to learn how to configure remote access and set up a certificate to do remote access another machine using global protect from Palo Alto.

**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:**

We successfully configured remote access using global protect on Palo Alto 410s and accessed a machine on the same network remotely.