Background:

A remote access VPN is a VPN operates over the internet to establish a connection between a remote user and a corporate network, or any other remote network, securely. The idea behind a remote access VPN is to create an encrypted tunnel between a user and a network to prevent any cybersecurity attacks from acquiring sensitive data. Typically, this is useful in business/corporate settings when employees need a safe way to communicate with their company’s network without risking leaking data or letting unwanted users to gain access to company resources.

In the previous lab, we configured a site-to-site VPN that helps to connect two different sites, i.e. networks, have a way to securely connect with each other. In concept, the VPN technology and the goal is similar as we are trying to connect devices in two different locations securely through a VPN. However, a crucial difference is that remote access involved only a single user device on one side of the tunnel.

Palo Alto firewalls have a specifically to operate remote access VPNs called GlobalProtect. GlobalProtect is primarily a client-based, meaning that it requires that you download a software on your computer in order to access/manage the firewall. However, since GlobalProtect is available on many platforms such as Windows, macOS, iOS, and Android, it isn’t terribly inconvenient to manage.

For this lab, we generated certificate on our computer in order to verify it and connect the outside, the WAN side computer to the gateway.

Lab Summary/Steps:

Step 1: Delete the Virtual Wire

Step 2: Go to device, interfaces, eth1/1, and change virtual wire to default

Graphical user interface, text, application, email

Description automatically generated

Step 3: Create Security zone INTERNET for eth 1/1

Graphical user interface, text, application, email

Description automatically generated

Step 4: Configure it to be L3 and the following address.

Graphical user interface, text, application, email

Description automatically generated

Step 5: For eth1/2, configure security zone INSID and configure the following ip address

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Step 6: Go to Virtual Wire, static routes, and enter the following configurations

Graphical user interface, application

Description automatically generated

Step 7: Go to Security Policies, edit the pre-existing rule

Graphical user interface, text, application, table

Description automatically generated

Step 8: Configure the following for source, destination, and Service/URL

A screenshot of a computer

Description automatically generated

Graphical user interface, application, table

Description automatically generated

Graphical user interface, application

Description automatically generated

Step 9: Under device, go to certificates. Generate a new cert and enter the following configurations:

Graphical user interface, application

Description automatically generated

Step 10: Under SSL/TLS Service Profile, configure this for profile:

Graphical user interface, application

Description automatically generated

Step 11: configure this under local user

Graphical user interface

Description automatically generated

Step 12: Go to authentication profile, add and enter the configs

Graphical user interface, application

Description automatically generated

Step 13: go to advanced and enter the following



Graphical user interface, application

Description automatically generated

Step 14: Configure a tunnel in this way under tunnel interface under network

Graphical user interface, text, application, email

Description automatically generated

Step 15: Create a vpn zone

Graphical user interface, application

Description automatically generated

Step 16: Go to Global Protect Portal. Click add and configure the following

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Step 17: Go to external, add and enter the following

Graphical user interface, application

Description automatically generated

Step 18: Go to IP pools and enter these configs

Graphical user interface, text, application, email

Description automatically generated

Step 19: Now retrieve licenses

Graphical user interface, table

Description automatically generated

Step 20: Login to to global protect by going to your address: <https://192.168.100.240>

Graphical user interface, application

Description automatically generated

Step 21: Download global protect as this is client-based

Graphical user interface, text, application

Description automatically generated

Step 22: Now open the app and connect to the 192.168.100.240

Graphical user interface, text, application

Description automatically generated

Step 23: There you go!

Graphical user interface, application

Description automatically generated

Problems

Conclusion