**Palo alto remote-access vpn (certificate)**

Derek Liu Cybersecurity Period 5

**Setting Up a Remote Access VPN***Derek Liu*

Purpose

The purpose of this lab is a to set up a remote access VPN with a Palo Alto firewall. This lab was done by using self-signed certificates as a method of authentication.

Background Information

A remote access VPN is a type of network that allows a user to securely connect to a network, such as a corporate network from a remote location using the internet as a medium of transport.

A VPN or virtual private network creates a secure and encrypted tunnel between the user’s device and the network which prevents unwanted interception of data. Remote access VPNs are commonly used by businesses and organizations to enable employees or students to access resources and applications from remote locations. This allows for work to be done while people are working from home or travelling.

The VPN maintains a high level of security, so no sensitive information is leaked.

In a previous lab, we configured a site-to-site VPN. The main difference between site-to-site VPNs and remote access VPNs is the usage of the VPNs. Remote access VPNs are used by individuals to connect to a network while site-to-site VPNs are used to connect two ore more private networks together.

Palo Alto firewalls provide a feature called GlobalProtect that is used for establishing a secure connection when setting up a remote access VPN. GlobalProtect is client-based and can be used for a variety of platforms including Windows, macOS, iOS, and Android.

This lab was configured using a self-signed certificate to establish a secure connection. A certificate is a digital document that is used to authenticate a device. The certificate usually contains information such as the owner’s name, public key, and other identifying information. Certificates are usually issued by a trusted third party but in this lab, we created our own certificate. Other options exist such as a pre-shared key (legacy option) or SSL. SSL or Secure Sockets Layer is a security protocol that used a combination of asymmetric and symmetric encryption to secure a connection.

Lab Summary

In this lab, we created a topology like the one shown below. We connected the firewall to the internet (steps can be found in a SOHO configuration lab) and connected the management interface to the internet. Global Protect Client software was downloaded. We generated a self-signed certificate, created an SSL/TLS profile, created a tunnel, and then configured a Global Protect Portal and Gateway. Global Protect software was then distributed to a user device and connection was verified on both ends.

Network Diagrams with IP

Chart

Description automatically generated

Configurations

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

Graphical user interface, application

Description automatically generated

Step 36: Download Global Protect Client

Graphical user interface, text, application

Description automatically generated

Step 37: Run the installer Graphical user interface, text, application, email

Description automatically generated

Step 38: 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

Step 40: Verify Connection

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Problems

The main problem that we encountered was downloading Global Protect onto the device that was in the “remote site.” We couldn’t find a download file on the internet but were able to download it off the Microsoft store (device was configured with Windows OS). However, the Global Protect downloaded off the Microsoft store wouldn’t connect since it was a self-signed certificate and deemed the connection unsecure.

We solved this by configuring the firewall to connect to the internet to retrieve license keys and download Global Protect off Palo Alto servers. The software was then distributed from the firewall to the user devices.

Another problem we ran into was after connecting the firewall to the internet, we forgot to connect the management interface to the internet. This was quickly solved with a layer 1 link from the management interface to an ethernet port on the firewall.

Conclusion

The remote access VPN is a widely used and has a very practical function especially with more people experimenting with working remotely. In this lab, we set up a remote access VPN on a private network with relatively few problems. In the future, we plan on continue working with remote access VPNs but exploring the SSL and TLS protocols.