Palo Alto Remote access VPN with Certificates

By: Jordan Abu-Zahra

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

Remote access VPN authentication offers several advantages over traditional username and password-based methods. Certificates provide a higher level of security because they are unique digital credentials tied to specific users or devices. They are issued by a trusted certificate authority which helps to validate the identity of the user of device requesting access.

The first step to setting up a remote access VPN with Palo Alto is to generate and enroll certificates for the remote users or devices that will be connecting to the VPN. This can be done through the Certificate Authority or and internal Publik Key infrastructure. The certificates can be issued based on user identities or device identifiers. Once the certificates are obtained, they need to be configured on the Palo Alto networks firewall. This involves importing the Certificate authority root certificate and any intermediate certificates as well as configuring the VPN gateway to trust these certificates. The nest step is to configure the Palo Alto Networks firewall or VPN gateway to accept the certificate-based authentication, this involves creating an authentication profile that specifies the certificate-based authentication method. The profile should include settings such as the Certificate Authority certificate, certificate revocation checks, and other parameters and for each remote user or device a corresponding VPN client configuration needs to be set up, this configuration includes importing the user or device certificate that specifies the VPN gateway address and the configuring other VPN parameters such as encryption settings and DNS configuration. Then after configurations are in place you should test the remote access VPN connectivity with certificate-based authentication. This includes verifying that certificates are properly recognized and validated by the VPN gateway and that users can successfully establish a secure connection. In conclusion you should use Palo Alto to configure you firewalls since it has so many features to help you secure your network.

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

A problem we ran into was downloading Global Protect, in the remote site tab we could not find a download file on the internet be we were able to get it off the Microsoft store, but that lead to an issue where our self-signed certificate was deemed unsecure so we were denied connection and we fixed this by having our firewall retrieve licenses keys and then we were able to download Global Protect off Palo Alto servers.

Conclusion

In conclusion we learned how to set up a remote access VPN with certificates and are able to establish a secure connection.