Derek Liu Cybersecurity Period 5

**palo alto soho setup pa410**

**PA-410 SOHO Config***Derek Liu*

Purpose

The purpose of this lab is to explore the configuration process of different models of Palo Alto firewalls. In this case, we will work with a Palo Alto 410 and configure it for a SOHO environment with DHCP and NAT.

Background Information

Palo Alto is a cybersecurity company that specializes in cybersecurity products, including firewalls. In this lab, we will be working with a PA-410. The Palo Alto 410 is considered a next generation firewall as part of the Palo Alto Networks PA-400s series. These firewalls are specifically designed support enterprise branch offices, retail locations, and midsize business. Since they are meant to be deployed in large numbers in a large enterprise, it makes sense for it to be configured easily. Palo Alto allows for Zero Touch Provisioning (ZTP) on the PA-410 which automates the configuration process with the usage of a Panorama management server. However, since we will only be configuring one PA-410, we will not be using ZTP in this lab and configure it manually.

Despite its small size, it has a throughput of up to 2Gps and can support up to 10,000 sessions. In terms of features, it includes application visibility and control, threat prevention, and user authentication. These features can all be easily configured and accessed from a web management interface. While it is common practice to not publicly disclose what networking devices are implemented in a company’s network, some past consumers of Palo Alto firewalls include: Netflix, NASA, and Hilton. This shows that Palo Alto firewalls are a tested and trusted security solution.

Configurations

1. Console into the firewall and access configurations with the credentials of user: admin pass: admin.
2. Disable zero touch provisioning

Text

Description automatically generated

1. Connect to the management interface (MGT) and manually configure the ipv4 address of the computer to 192.168.1.1 255.255.255.0 in order to access the web interface

Graphical user interface, application

Description automatically generated

1. Go to <https://192.168.1.1> and enter the credentials the firewall had you configure in step 1.
2. Got to network – zones and click “add”.

Create three different zones:

* Untrust, Type Layer 3
* Trust-L3, Type Layer 3
* Trust-L2, Type Layer 2

1. Connect ethernet 1/1 to the ISP
2. Go to network – interfaces, select “ethernet 1/1,” and configure the following:

Graphical user interface, text, application, email

Description automatically generated

1. Go the “ipv4” tab and set it as a DHCP client.
2. Go to network-virtual wire and delete the pre-existing virtual wire.
3. Go to network – vlans and click “add.” Configure the following:

* Graphical user interface, text, application

  Description automatically generated

1. Go to Network -> interfaces and configure the remaining interfaces.

For all of them (1/2, 1/3, 1/4) Select the following:

* Interface type: Layer2
* VLAN: Vlan Object
* Security Zone: Trust-L2

1. Go to network – interfaces – vlan and configure the following:

Graphical user interface, text, application, email

Description automatically generated

1. Go to the “ipv4” tab and set a static IP address of 192.168.1.254/24
2. Go to the “Advanced” tab and enable DDNS.
3. Go to Network – DHCP – DHCP server and click “add.” Configure the following.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

1. Go to Objects – Security Profile Groups and click “add.” Configure the following:

Graphical user interface, text, application

Description automatically generated

1. Go to Polices – Security and click “add.” Configure the following:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application, email

Description automatically generated

1. Go to Policies – NAT and click “add.” Configure the following:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

1. Go to Device – Setup – Interfaces. Click the gear icon and configure the following.

Graphical user interface, text, application

Description automatically generated

1. Go to Device – Setup – Services and configure the following:

Graphical user interface, text, application, email

Description automatically generated

1. Click “commit” at the top right of the web interface to save configurations.
2. Change the ipv4 configuration of the computer to DHCP client. At this point, the computer should be able to connect to the ISP through the firewall.

Problems

The Palo Alto firewall product line seem to be very consistent in terms of configuration, so we didn’t run into any significant issues. The only things that were different this time was disabling ZTP and enabling DDNS when a “commit” failed without it enabled.

Conclusion

In this lab we successfully configured a Palo Alto 410 firewall for a SOHO network. This was done through configurate of the Palo Alto through the web interface after we connected an ethernet cable to the management port. While no software updates were done, the firewall can now successfully connect to the internet and also create a DHCP pool and NAT for the trusted interfaces. This lab only differed slightly from the PA220 configuration.