PALO ALTO NETWORKS FIREWALL 11.0 ESSENTIALS

Lab 14: Capstone

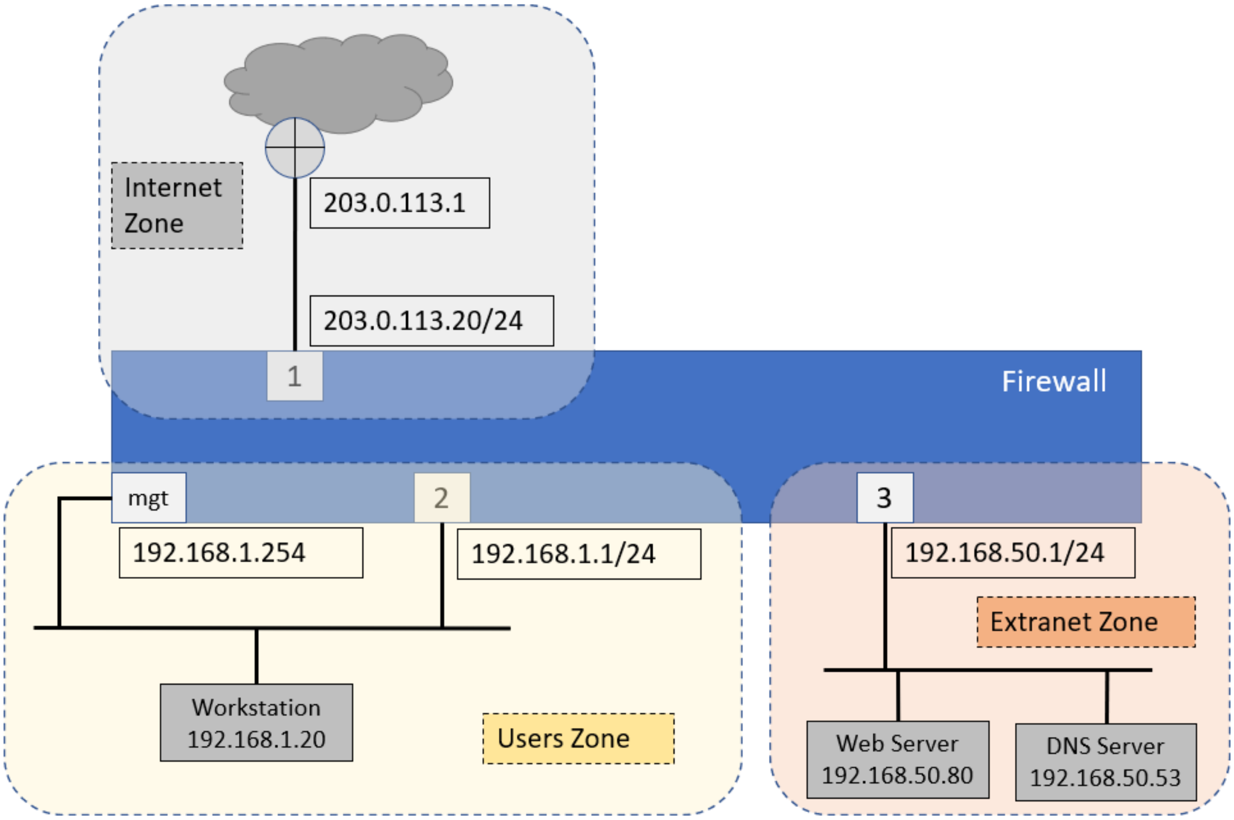
Document Version: 2024-01-15

Contents

Introduction

This comprehensive lab is meant to provide you with additional hands-on firewall experience and to enable you to test your new knowledge and skills. You can refer to your student guide and previous lab exercises.

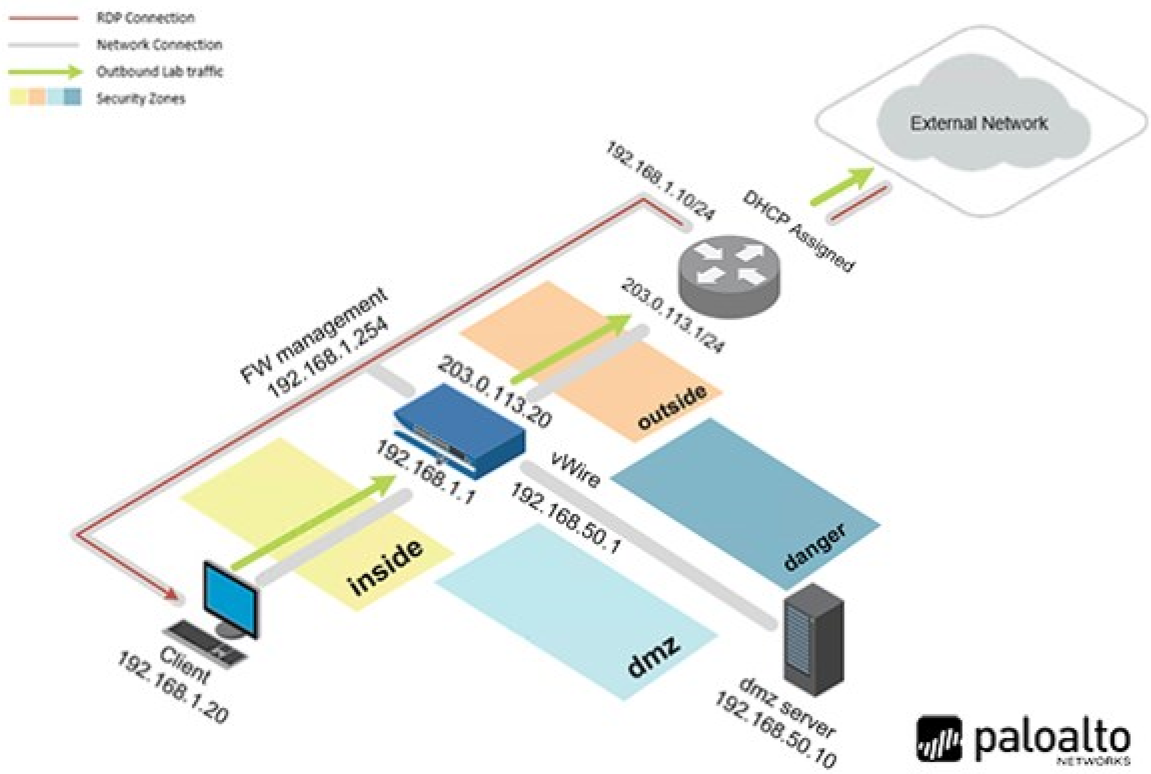
In this scenario, you are a network administrator and recently received a new Palo Alto Networks VM-Series firewall. The firewall's management IP address is 192.168.1.254. You can log in with the username **`admin`** and **`Pal0Alt0!`** as the password. Take special care to use the exact spelling and capitalization for the items you are asked to configure.



Objective

You are being asked to meet multiple configuration objectives. These objectives are listed in the lab exercise sections that follow.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	**192.168.1.20**	`lab-user`	`Pal0Alt0!`
DMZ	**192.168.50.10**	`root`	`Pal0Alt0!`
Firewall	**192.168.1.254**	`admin`	`Pal0Alt0!`
vRouter	**192.168.1.10**	`root`	`Pal0Alt0`

1 Capstone

You are being asked to meet multiple configuration objectives. These objectives are listed in the lab exercise sections that follow.

1.1 Apply a Baseline Configuration to the Firewall

- On the Zorin desktop, select *lab-user*, enter **Pal0Alt0!** for the password.
- For the Palo Alto Firewall, enter **admin** for the user and **Pal0Alt0!** for the password.
- Load and commit the configuration file - **edu-210-11.0a-Capstone-start.xml** to the Firewall.

1.2 Configure Networking

Complete the following objectives:

- Configure three firewall interfaces using the following values:
  - **Ethernet 1/1**: **203.0.113.20/24 - Layer 3**
  - **Ethernet 1/2**: **192.168.1.1/24 - Layer 3**
  - **Ethernet 1/3**: **192.168.50.1/24 - Layer 3**
- Create a virtual router called **VR-1** for all configured firewall interfaces.
- Create a default route for the firewall called **Default-Route.**
- Create an **Interface Management Profile** called **Allow-ping** that allows **ping.**
- Assign the **Allow-ping** Interface Management Profile to **ethernet1/2.**

1.3 Configure Security Zones

Complete the following objectives:

- Create a **Security Zone** called **Internet** and assign **ethernet1/1** to the zone
- Create a **Security Zone** called **Users** and assign **ethernet1/2** to the zone:
  - Configure the **Users Zone** for User-ID
- Create a **Security Zone** called **Extranet** and assign **ethernet1/3** to the zone.

Verify network connectivity from the firewall to other hosts.

- Your internal host can ping **192.168.1.1** and receive a response.
- From the firewall CLI, the following commands are successful:
  - **ping source 203.0.113.20 host 203.0.113.1.**
  - **ping source 203.0.113.20 host 8.8.8.8.**
  - **ping source 192.168.1.1 host 192.168.1.20.**
  - **ping source 192.168.50.1 host 192.168.50.150**

1.4 Configure NAT Policy Rules

Create Source NAT rules to meet the following requirements:

- Rule Name = **Users_to_Internet**
    - From Source Zone **Users** to Destination Zone **Internet.**
    - Use **ethernet1/1** on the firewall as the source translation address.

  Rule Name = **Extranet_to_Internet**
    - From Source Zone **Extranet** to Destination Zone **Internet.**
    - Use **ethernet1/1** on the firewall as the source translation address.
- All NAT rules must include a helpful Description.

1.5 Configure Security Policy Rules

Create Security Policy rules to meet the following requirements:

- For all Security Policy rules, enter a helpful **Description**.
- Modify the **interzone-default** Security Policy rule so that traffic is logged at session end.
- Create a Security Policy rule called **Block_Bad_URLs** with the following characteristics:
    - For all outbound traffic, the URL categories **hacking**, **phishing**, **malware**, and **unknown** must be **blocked** by a Security Policy rule match criterion.
- From the User zone to the Extranet zone, create a Security Policy rule called **Users_to_Extranet** to allow the following applications:
    - **ping**
    - **ssl**
    - **ssh**
    - **dns**
    - **web-browsing**
- From the User zone to the Internet zone, create a Security Policy rule called **Users_to_Internet** to allow the following applications:
    - **ping**
    - **dns**
    - **web-browsing**
    - **ssl**
- From the Extranet zone to the Internet zone, create a Security Policy rule called **Extranet_to_Internet** to allow the following applications:
    - **ping**
    - **dns**
    - **web-browsing**
    - **ssl**

You can consider this objective complete when the following tests are successful:

- The client host can **ping 8.8.8.8** and **google.com.**
- The client host can access **www.paloaltonetworks.com.**
- The client host can browse to the Extranet web server at **http://192.168.50.80.**
- The client host can use **SSH** to access the Extranet host at **192.168.50.150** using the login name **paloalto42** and the password **Pal0Alt0!.**
- The Extranet host can **ping 8.8.8.8** and **google.com.**
- The internal host cannot access **hacker9.com.**

1.6 Create and Apply Security Profiles

Create Security Profiles and a Security Profile Group to meet the following requirements:

- A Corporate **URL Filtering Security Profile** called **Corp-URL** to log access to all web categories.

  You can use the existing default Profile as the basis for your own.
- A Corporate **File Blocking Security Profile** called **Corp-FB** to block dangerous file types.

  You can use the existing strict Profile as the basis for your own.
- A Corporate **Antivirus Security Profile** called **Corp-AV** to block vulnerabilities.

  You can use the existing default Profile as the basis for your own.
- A Corporate **Anti-Spyware Security Profile** called **Corp-AS** to block spyware.

  You can use the existing strict Profile as the basis for your own.
- A Corporate **Vulnerability Protection Security Profile** called **Corp-Vuln** to block viruses.

  You can use the existing strict Profile as the basis for your own.
- A Corporate **WildFire Profile** called **Corp-WF** to send all file types to the public cloud for inspection.

  You can use the existing default Profile as the basis for your own.
- Create a **Security Profile Group** called **Corp-Profiles** and assign the appropriate Security Profiles to it.

  Note: You can leave the Data Filtering Profile set to **None**.
- Apply the **Corp-Profiles Group** to all applicable Security Policy rules.

You can consider this objective complete when the following tests are successful:

- The internal host cannot download a test virus file from **http://192.168.50.80** using **HTTP**.
- The internal host cannot download the **badtarfile.tar** from **http://192.168.50.80/badtarfile.tar.**
- A URL log file entry appears when the client host browses to **https://www.paloaltonetworks.com.**

The lab is now complete; you may end your reservation.