PALO ALTO NETWORKS EDU-210

Lab 14: Capstone

Document Version: 2020-06-26

Contents

Introduction 3
Objectives........ 3
Lab Topology 4
Theoretical Lab Topology 4
Lab Settings 5
14 Active/Passive High Availability 6
14.0 Load Lab Configuration 6
14.1 Configure Interfaces and Zones 9
14.2 Configure Security and NAT Policy Rules 10
14.3 Create and Apply Security Profiles 11
14.4 Configure GlobalProtect 13

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.

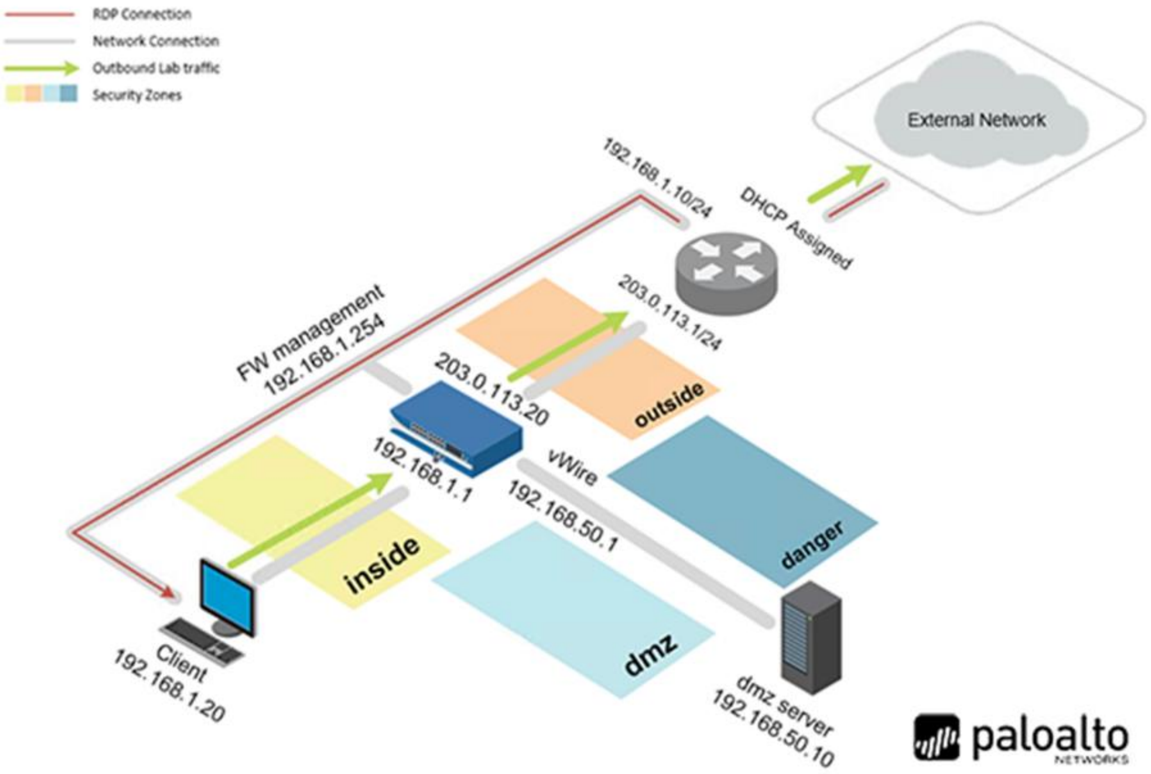
In this scenario, you are a network administrator and recently received a new Palo Alto Networks VM-Series firewall. The firewall's management IP address is 192.168.1.254. You can log in with the default username and password. You also have been given permission to use your own naming conventions for firewall objects such as security zones, Security profiles, address groups, and tags.

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

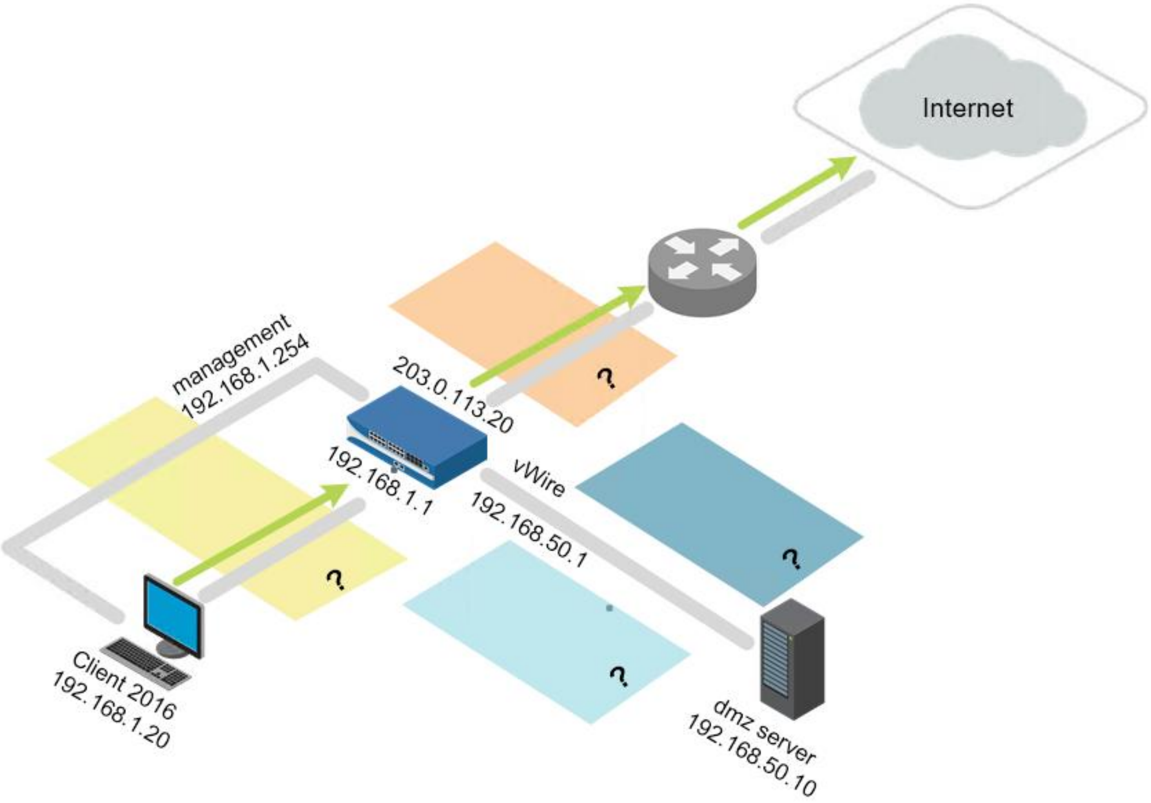
Objectives

- Configure interfaces and zones
- Configure security and NAT policy rules
- Create and apply security profiles
- Configure GlobalProtect

Lab Topology



Theoretical 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`	`Train1ng$`
Firewall	192.168.1.254	`admin`	`Train1ng$`

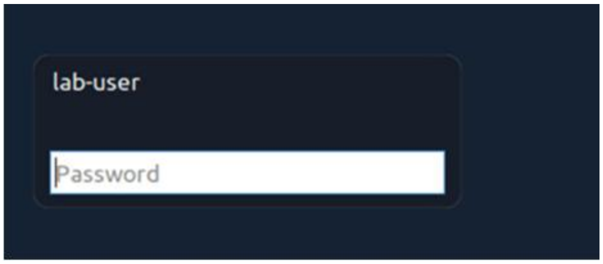
14 Active/Passive High Availability

14.0 Load Lab Configuration

1. Launch the **Client** virtual machine to access the graphical login screen.

> To launch the console window for a virtual machine, you may access by either clicking on the machine's graphic image from the topology page or by clicking on the machine's respective tab from the navigation bar.

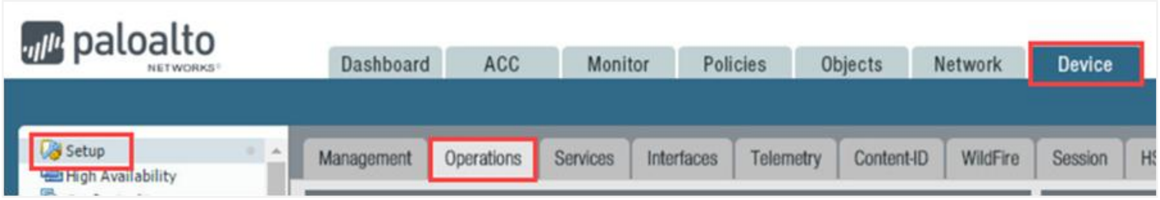
2. Log in as `lab-user` using the password `Train1ng$`.



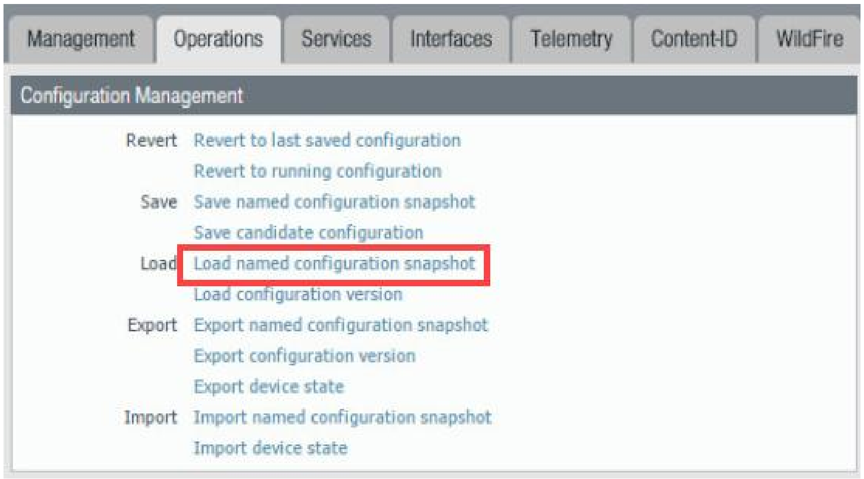
3. Launch the **Chromium Web Browser** and connect to `https://192.168.1.254.`
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall using the following:

Parameter	Value
Name	`admin`
Password	`Train1ng$`

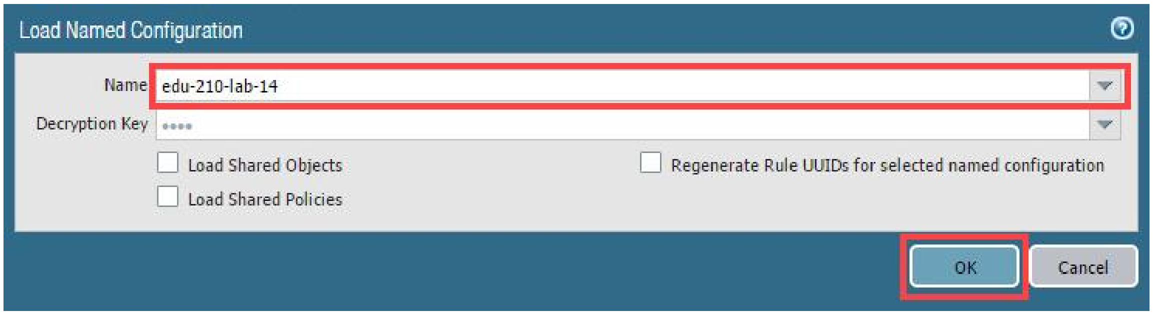
6. In the web interface, select **Device > Setup > Operations**.



7. Click **Load named configuration snapshot**:


Management
Operations
Services
Interfaces
Telemetry
Content-ID
WildFire
Configuration Management
Revert
Revert to last saved configuration
Revert to running configuration
Save
Save named configuration snapshot
Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version
Export device state
Import
Import named configuration snapshot
Import device state

8. Click the dropdown list next to the *Name* text box and select **edu-210-lab-14.xml**. Click **OK**.


Load Named Configuration

Name: edu-210-lab-14

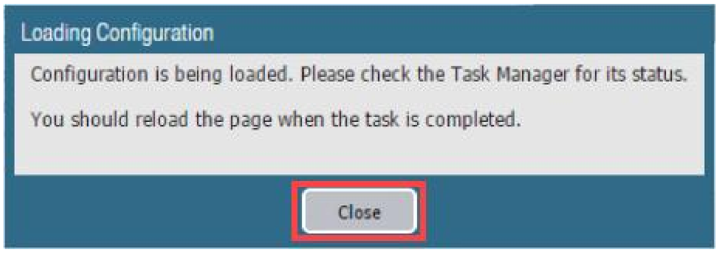
Decryption Key: ••••

□ Load Shared Objects

□ Regenerate Rule UUIDs for selected named configuration

□ Load Shared Policies

9. Click **Close**.

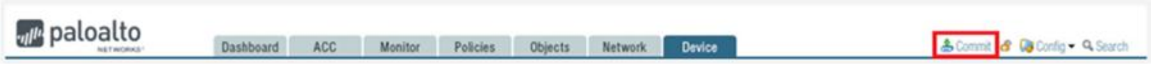

Loading Configuration

Configuration is being loaded. Please check the Task Manager for its status.

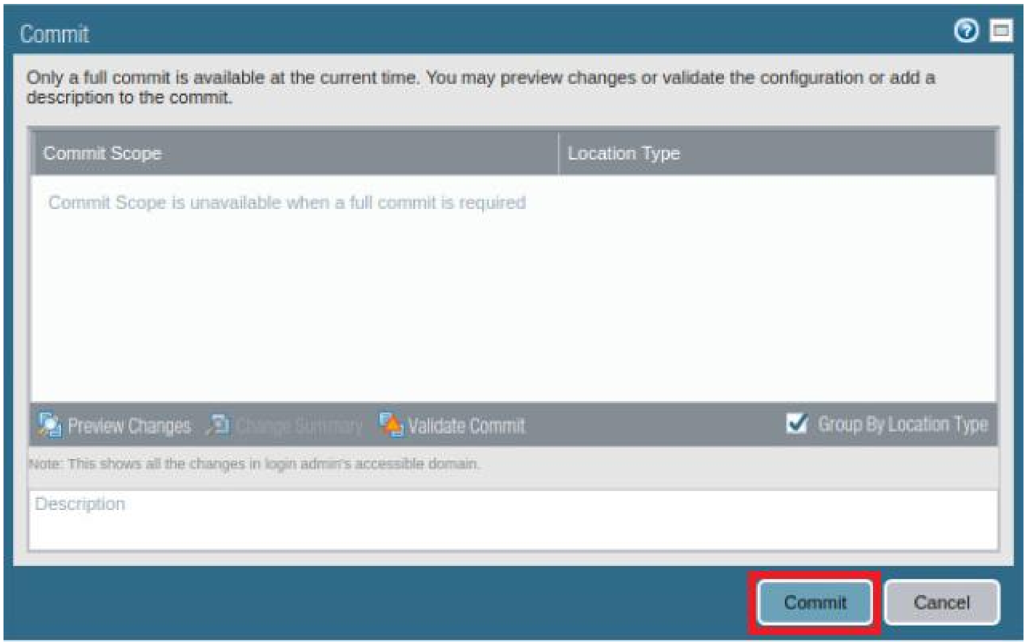
You should reload the page when the task is completed.

> The following instructions are the steps to execute a **"Commit All"** as you will perform many times throughout these labs.

10. Click the **Commit** link at the top-right of the web interface.



11. Click **Commit** and wait until the commit process is complete.



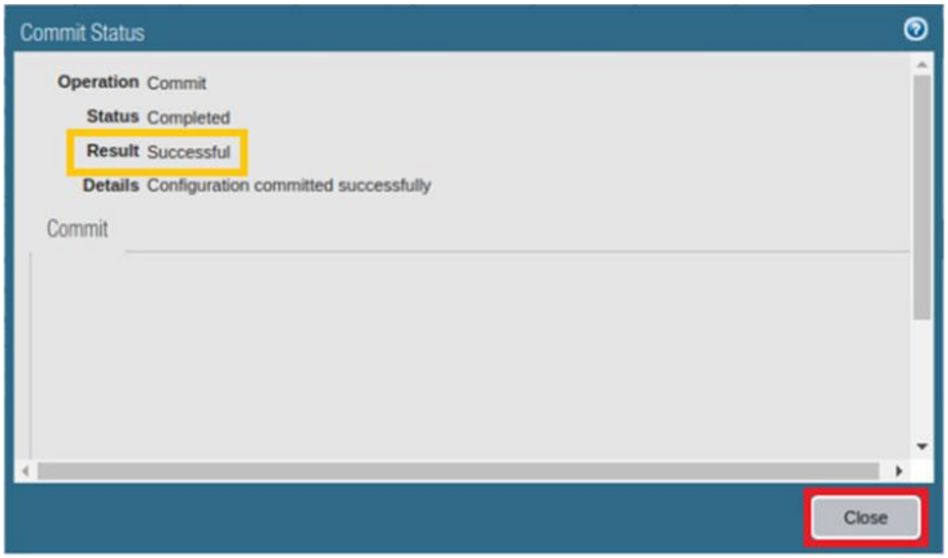
Commit

Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	

Note: This shows all the changes in login admin's accessible domain.

12. Once completed successfully, click **Close** to continue.



Commit Status

Operation Commit
Status Completed
Result Successful
Details Configuration committed successfully

13. Leave the firewall web interface open to continue with the next task.

14.1 Configure Interfaces and Zones

Complete the following objectives:

- Configure a default gateway on the virtual router:
  - Ethernet 1/1: 203.0.113.1
- Configure three firewall interfaces using the following values:
  - Ethernet 1/1: 203.0.113.20/24 - Layer 3: Public network-facing interface
  - Ethernet 1/2: 192.168.1.1/24 - Layer 3: Internal network-facing interface
  - Ethernet 1/3: 192.168.50.1/24 - Layer 3: DMZ network-facing interface
- Create security zones for each network area of interest: DMZ, internal, and public. Name these zones whatever you like.
- Create a virtual router for all configured firewall interfaces.
- Create and assign an Interface Management Profile that enables 192.168.1.1 to respond to ping requests.

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

- Your internal host can ping 192.168.1.1.
- 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 192.168.1.10
ping source 192.168.50.1 host 192.168.50.10
```

14.2 Configure Security and NAT Policy Rules

Create or modify the Security and NAT policy rules to address the following objectives:
Note: *Optional tags can be helpful for identifying important rules.*

- IP addresses 192.168.1.20 and 192.168.1.254 require access to the internet.
- Create and assign unique tags for the Security and NAT Policy Rules.
- A separate Security policy rule is required that allows the 192.168.1.0/24 network to access the internet.
- Only the DMZ host 192.168.50.10 requires access to the internet.
- Facebook, Twitter, YouTube, 2600.org, and Reddit URLs must be blocked for users on the 192.168.1.0/24 network.
- The URL categories web-advertisements, phishing, malware, and unknown must be blocked by a Security policy rule match criterion.
- Internal hosts 192.168.1.20 and 192.168.1.254 need to access the DMZ host for the following applications: SSH, SSL, web-browsing, FTP, and ping. Access must be limited to the applications' default ports.
- Traffic matching the interzone default Security policy rule must log all traffic at the session end.
- Configure appropriate NAT rules

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

- The internal host can ping 8.8.8.8 and google.com.
- The internal host cannot access twitter.com, youtube.com, reddit.com, and 2600.org.
- The internal host can access http://192.168.50.10/block-list.txt.
- The internal host can use FTP to access the DMZ host at 192.168.50.10 using the login name `lab-user` and the password `paloalto`.
- The internal host can use SSH to access the DMZ host at 192.168.50.10 using the login name `lab-user` and the password `paloalto`.
- The DMZ host can ping 8.8.8.8 and google.com.

14.3 Create and Apply Security Profiles

Create Security Profile Groups and apply them to the applicable Security policy rules to meet the following objectives:

- A three-tiered URL filtering scheme is required:

  Tier 1: Allow access to only URL categories government, financial-services, reference-and-research, and search-engines
  Tier 2: Allow access to only the URL category online-storage-and-backup
  Tier 3: Allow access to all URL categories

- The Tier 3 URL filtering must apply to the internal host.
- The Tier 2 URL filtering must apply to the DMZ host.
- The Tier 1 URL filtering must apply to the network 192.168.1.0/24.

Note: The Security policy rule, specifically matching 192.168.1.20, must be evaluated before the entire network segment.

- The Facebook, Twitter, YouTube, and Reddit applications must be blocked for everyone.
- All Security policy rules allowing internet access must leverage Antivirus, Anti-Spyware, and Vulnerability Protection profiles.
- The firewall must reset the client and the server when a virus is detected in HTTP traffic.
- The firewall must reset the client and the server when medium-, high-, or critical-level spyware is detected.
- The Anti-Spyware Security Profile must use the DNS Sinkhole feature for Palo Alto Networks DNS Signatures and consult a custom External Dynamic List that references http://192.168.50.10/dns-sinkhole.txt.
- The dns-sinkhole.txt file must contain the domain name phproxy.org.
- The firewall must reset the client and server when high- or critical-level vulnerabilities are detected.
- WildFire analysis must be enabled on all Security policy rules that allow internet access.
- The File Blocking feature must block PE file types and any multi-level-encoded files for access between the internet and the 192.168.1.0/24 network segment.

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

- Three URL filtering configurations have been created and applied to the appropriate Security policy rule(s).
- The DMZ host can ping box.net.
- The internal host can access box.net.
- The internal host cannot download an Eicar test virus (2016.eicar.org) using HTTP.

- A WildFire test file (http://wildfire.paloaltonetworks.com/publicapi/test/pe) gets reported to the WildFire cloud when it is downloaded to the internal host.
- A DNS request to phproxy.org initiated by an **nslookup** command on the internal host results in a sinkhole event recorded in the Threat log.

14.4 Configure GlobalProtect

Configure GlobalProtect to meet the requirements listed in the following objectives:

- User access is provided through an external gateway.
- The GlobalProtect portal and external gateway can authenticate users using either LDAP or a local user group configured on the firewall.
- The external gateway provides an IP address pool in the range 172.16.5.200 to 172.16.5.250.
- The tunnel interface must be assigned to a new and separate security zone.
- A Security policy rule must allow internet access for hosts using the external gateway IP pool.
- The external gateway requires the use of IPsec.
- One or more certificates are required for the portal and external gateway.
- A Security policy rule must be created to allow the internal host access to the portal and external gateway. This access might require the use of a no-NAT rule.

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

- The internal host can successfully connect to the portal and external gateway.
- The internal host receives an IP pool address when connected to the external gateway.
- The internal host can access paloaltonetworks.com when connected to the external gateway.

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