

Customer Simulation Lab

Overview 3

Lab Diagram 4

Exercise 1: VM Installation 5

Exercise 2: Panorama 6

Exercise 3: Check Point Migration 7

Exercise 4: Panorama Migration 8

Exercise 5: Clone a Device-Group 9

Exercise 6: ScreenOS Migration 10

Exercise 7: ASA Migration 11

Exercise 8:App-ID Migration – Phase II 12

Exercise 9: App-ID Migration – Phase III 13

Exercise 10:Custom App-IDs 14

Exercise 11: Application Override 15

Exercise 12: API Configuration 16

Revision History 17

# Overview

Welcome to the Palo Alto Networks Customer Simulation Lab. This lab is a series of exercises designed to emulate likely customer scenarios you will experience in the field. This is an opportunity to practice those scenarios and demonstrate your ability to successful execute customer engagements.

Just like in a customer engagement, you have one job to do during this lab: Make the project successful. To do this, you must complete the necessary tasks in the time allotted. It is up to you to figure out what you need to do to be successful.

There are no trick questions or intentionally artificial exercises in this lab. In preparing for this lab, you are expected to have already practiced everything covered here.

Unless otherwise noted, all firewall configurations should be managed by Panorama as much as possible, *keeping in mind best practices*.

These exercises are unproctored, and you are allowed to seek outside assistance. Learning who to talk to when you are stuck on a particular problem is critical for your future success. If you get stuck, try to find the right people to talk to about a particular feature (SMEs, team leads, tek-talk, etc.) rather than relying on someone who has gone through the CSL previously.

If you have any issues with the lab or the written exercises, please ask the lab instructor right away.

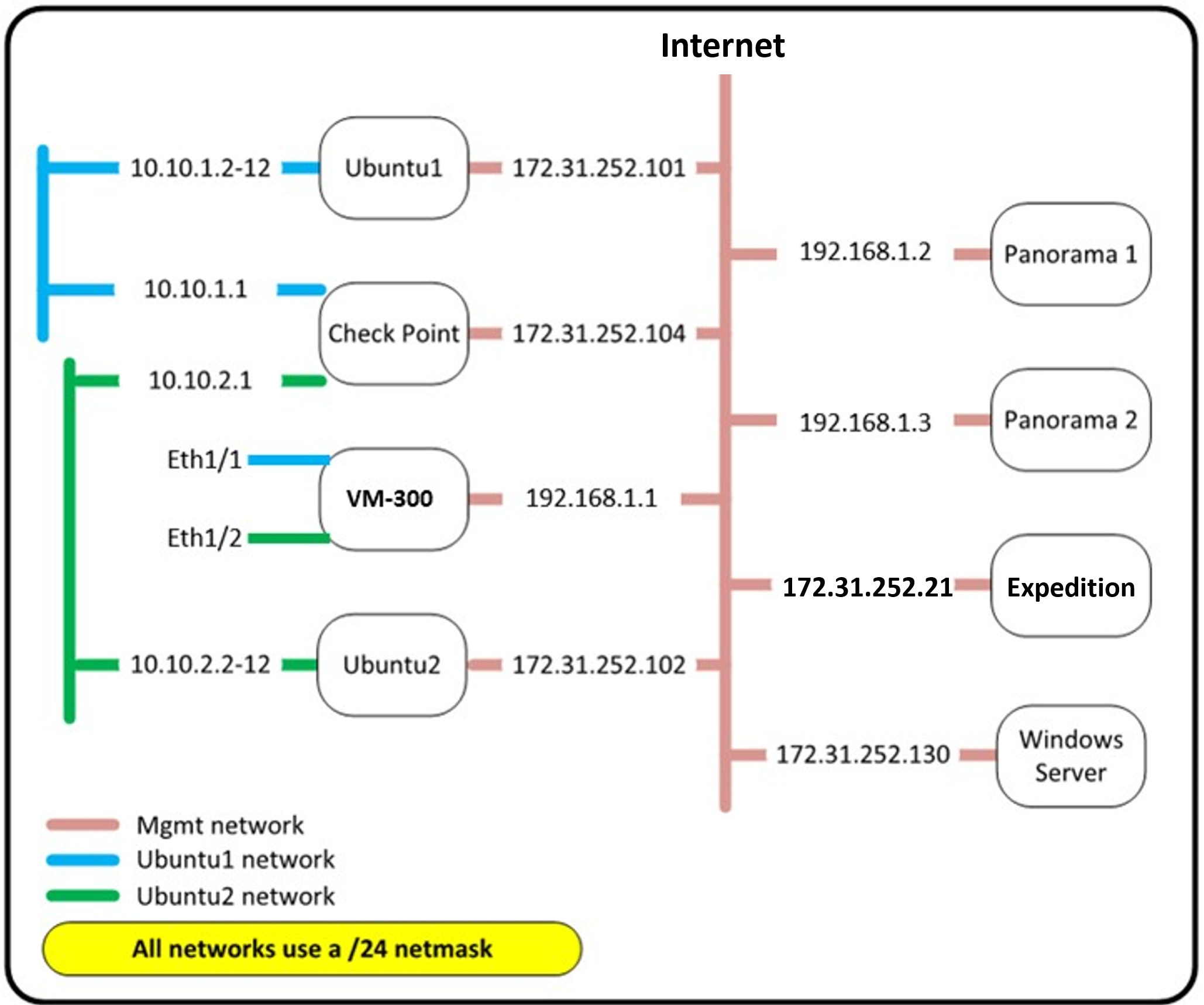
**The logins for lab equipment are shown in each section. If you still have trouble logging in, ask the instructor.**

The instructor is going to be your virtual customer.

Your customer has contracted you for two separate tasks. One task is to perform all of the steps in this lab. The other task is to provide the customer an instructional document of how to do the work that you are performing. His team has no experience with Palo Alto Networks firewalls and will rely heavily on your documentation for their upcoming tasks.

Your customer wants a full document of all the tasks needed to complete the entire implementation. This will include details about the starting configuration and all the steps you performed to progress from one exercise to the next. The document must also cover your **reasons** why certain choices were made during the migration. This documentation will likely take longer than the actual tasks themselves. Please understand, **THE DOCUMENTATION IS THE MOST IMPORTANT PART OF THIS LAB**. The customer is going to give this document to other firewall engineers in the company to use as a template for migrating other similar configurations.

# Lab Diagram



Windows Server Login: Administrator, paloalto

Check Point login: admin, paloalto

Ubuntu Login: panw, paloalto

# Exercise 1: VM Installation

All of the modules in the lab will use a combination of servers and virtual firewalls. All of the VMs are already present. Your first exercise will be to configure one VM series firewall and two Panorama VMs. You must replace the 192.168.1.x management IP addresses with IP’s in the

172.31.252.200 - 240 range.

**Note**: For the remainder of this Customer Simulation Lab, please use PAN-OS version 8.0.x.

Upgrade the firewall and Panoramas to the most recent 8.0.x revision.

At the end of this exercise, all three VMs should be reachable via their 172.31.252.x management interface addresses and should be able to communicate to each other on the management network.

# Exercise 2: Panorama

Configure the two Panorama VMs in HA mode. Get the VM-Series firewall ready to be managed by the two Panoramas, but do not import it into the Panorama yet.

This lab will only deploy one VM firewall, but assume there will eventually a large number of them. Configure templates for the firewall and consider what should be included in the templates with this in mind.

Create at least one template for global configurations and add something to it that should be applied globally.

Create at least one template for the geographic region and add something to it that should be applied regionally.

Configure a device-group for the firewall.

Use the ThreatTuning worksheet to add the log settings and custom reports to the Panorama.

Have the instructor check your configuration before moving to the next exercise.

# Exercise 3: Check Point Migration

In the lab, there is a virtual Check Point firewall currently configured and passing traffic. You will migrate the configuration from this Check Point to the VM-Series firewall that you installed. The Check Point configuration files are located in Box under the Simlab/CP\_Simlab folder.

1. Migrate the configuration ***locally on the firewall, not on the Panoramas***.

During this and all migrations, take detailed notes on what tasks you perform during the exercise. You may find them very helpful if you need to repeat them on similar migrations or when discussing what was done.

There are two servers on either side of the Check Point that are currently passing traffic using NAT. These servers are VMs connected to virtual switches, which are then connected to the Check Point. Feel free to log onto to these servers for any reason. Do not disable the traffic running between the servers and do not disable the NAT.

Please use the following information for this exercise.

Linux Server1:***172.31.252.101***

Linux Server1 Login: *panw/paloalto*

Linux Server2:***172.31.252.102***

Linux Server2 Login: *panw/paloalto*

**Note**: Feel free to change the IP address on the Check Point ports, or change the default gateways on the servers if you must.

**Note**: The 10.10.x.x networks do not require internet access. This is an East-West deployment.

At the end of this exercise, you should see traffic traverse the VM-Series firewall between Ubuntu1 and Ubuntu2. Most (if not all) of your NAT and security policy rules will be used. If you do not see this, troubleshoot the issue until you have resolved connectivity between Ubuntu1 and Ubuntu2 via the VM-Series firewall.

Have the instructor check your configuration before moving to the next exercise.

# Exercise 4: Panorama Migration

Now that the configuration is running on the VM-Series, migrate the configuration to the device-group on the Panoramas. Any configuration on the VM-Series that can be moved to the Panorama device-group should be, keeping in mind best practices. Make it possible for future local policies to take precedence over the Panorama policies.

Make sure that the NAT rules that have been migrated are applied only to the one VM-series firewall. If additional firewalls are added to this device-group in the future, make sure that they do not receive any of the currently configured NAT rules.

Create a rule that blocks all incoming traffic from 15.0.0.0/8 and 16.0.0.0/8. Make sure that this is applied to all managed firewalls and takes precedence over the device-group or local rules. Also configure an explicit deny any rule that is applied after all other rules.

Have the instructor check your configuration before moving to the next exercise.

# Exercise 5: Clone a Device-Group

Now that you have configured a device-group in Panorama, make a copy of that device-group and give it a different name.

At the end of this exercise, you should have two device-groups, both of which have the same number of objects and policies.

Have the instructor check your configuration before moving to the next exercise.

# Exercise 6: App-ID Migration – Phase II

The traffic that is going through the VM firewall has been migrated from the Check Point firewall in a like-for-like manner, and there should be several port-based rules. This was appropriate for Phase I. Now it is time for Phase II.

Complete Phase II using the App-ID adoption function in Expedition to migrate service-base rules to application-based rules in this policy.

At the end of this exercise, for every port-based rule that has had traffic hit it, you should have another application-based policy preceding it with the appropriate application.

Have the instructor check your configuration before moving to the next exercise.

# Exercise 7: App-ID Migration – Phase III

Review the rules from Phase II. Verify the service-based rules that were shadowed by the new application-based rules are no longer being hit. If they are not, remove them.

# Exercise 8: Custom App-IDs

During the application migration, you may have found traffic that was not identified as any application. For any traffic that was not identified, create custom App-IDs for them. Afterwards, verify that no unknown applications are being logged.

Have the instructor check your configuration before moving to the next exercise.

# Exercise 9: Application Override

The VM-Series firewall should have FTP traffic passing through it. The timeout for this application is currently set to the default of 30 minutes. Assume that other servers will be added to the network in the future. Configure all FTP traffic between Ubuntu1 and Ubuntu2 to have a timeout of 24 hours. Any other FTP traffic should not be affected.

# Exercise 10: Documentation Review

Now that the migration part of the task is completed, compile all of the notes that you created during the process into a customer deliverable document. Include your company logo, an executive summary of the tasks that will be outlined in the document and the details. Present this to the customer for review and comments. You may be required to go back and add details that are missing. Refer to the **Example Migration Notes** document in Box to see the quality and detail of document that your customer is used to getting from his vendors.

# Revision History

|  |  |  |
| --- | --- | --- |
| Date | Revision | Comment |
| Jan 2014 | 1.01 | Initial build |
| Mar 2014 | 1.02 | Additional modules – First Beta Test |
| Apr 2014 | 1.03 | Additional modules – API Configuration |
| Apr 2014 | 1.04 | Additional modules – Custom App-ID, App-Override |
| June 2014 | 1.05 | Minor updates |
| Jan 2015 | 1.06 | Updates from David Jipp |
| Feb 2016 | 1.07 | PS Boot Camp update |
| Apr 2016 | 1.08 | PS Boot Camp update |
| June 2016 | 1.09 | PS Boot Camp update |
| Feb 2017 | 1.10 | Edited Labs 3 & 7 |
| April 2017 | 2.0 | Recreated lab in new environment and changed document to suit. |
| July 2017 | 2.01 | Fixed the 10.10.x.3-12 objects in the Simlab Check Point objects file to reflect 10.10.x.2-12. Removed the note in this document that referred to the error. |
| August 2017 | 2.02 | Changed the lab configuration to eliminate the need for instructors to power up the PANW VM’s for the students. The VM’s are now configured with 192.168.1.1, 192.168.1.2, and 192.168.1.3 management IP addresses. |
| October 2017 | 2.03 | Updated lab diagram to reflect a VM-300 instead of a VM-50. |
| April 2018 | 3.0 | Removed Labs 6, 7 and 12 and re-numbered the remainder. Added a documentation lab at the end and added several new paragraphs to account for using the Threat Tuning spreadsheet. Updated the network diagram to reflect Expedition instead of the Migration Tool. |