

Course: IS6572 - Fall 2025

Date: 08-26-2025

Lab: Palo Alto Firewall Security and NAT Policies

This lab is continuation after the Interface Configuration lab. This lab is focused on setting up the NAT and Security Policies to allow the systems within the lab topology to communicate to the outside world.

Objectives:

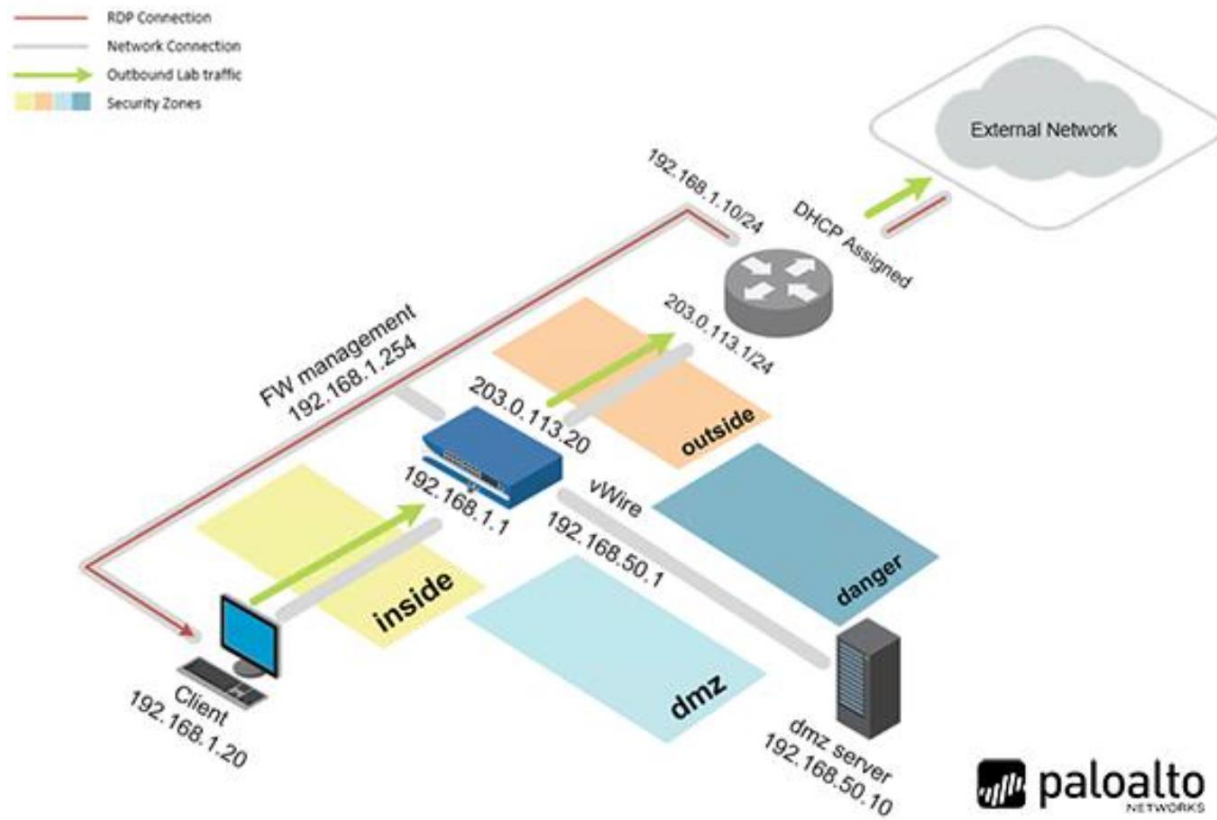
1. Create tags for later use with Security policy rules
2. Create a basic source NAT rule to allow outbound access and an associated Security policy rule to allow the traffic
3. Create a destination NAT rule for FTP server and an associated Security policy rule to allow the traffic

Lab Settings: Security and NAT Policies

Load Lab Configuration

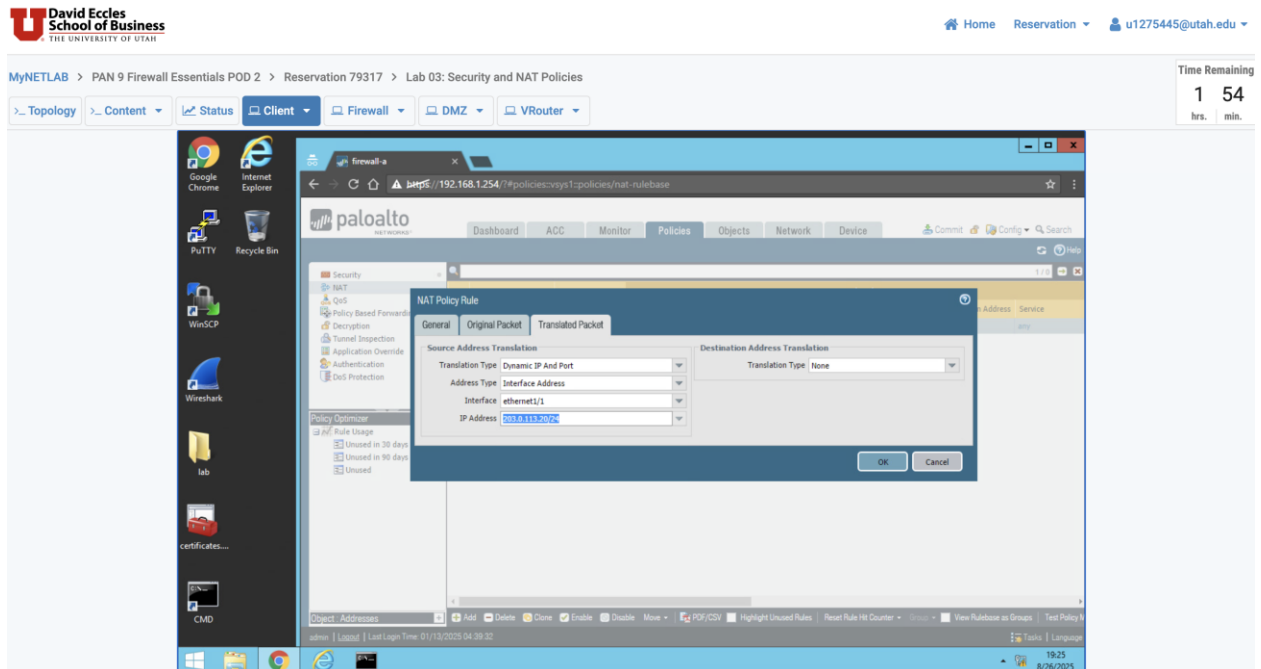
- 1.1 Create Tags
- 1.2 Create a Source NAT Policy
- 1.3 Create Security Policy Rules
- 1.4 Verify Internet Connectivity
- 1.5 Create FTP Service
- 1.6 Create a Destination NAT Policy
- 1.7 Create a Security Policy Rule
- 1.8 Test the Connection

Lab Topology:




Section 1.2: Create a Source NAT Policy

Step 5: Screenshot below shows setup where packet from dynamic IP and port is translated to Source IP of 203.0.113.20/24 at interface ethernet1/1.



Section 1.3: Create Security Policy Rules

Step 8: Following Screenshot shows the Security Policy created for the traffic that exits inside to outside traffic in addition to mandatory log at the end of each session.



David Eccles
School of Business
THE UNIVERSITY OF UTAH

HomeReservationu1275445@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79317 > Lab 03: Security and NAT Policies

Time Remaining
1 44
hrs. min.

TopologyContentStatusClientFirewallDMZVRouter

Google ChromeInternet ExplorerPuTTYRecycle BinWinSCPWinscpWinSCPWireSharklabcertificates...CMD

firewall-a

https://192.168.1.254/?#policies=vsys1:policies/security-rulebase

palalto

DashboardACCMonitorPoliciesObjectsNetworkDevice

CommitConfigSearchHelp

Security

test

QoS

Policy Based Forwarding

Decryption

Tunnel Inspection

Application Override

Authentication

DOS Protection

Policy Objects

Log No App Specified

Unused Apps

Rule Usage

Unused in 30 days

Unused in 90 days

Unused

Object: Addresses

Add

Import

Clone

Download

Revert

Lock

Disable

More

PDF/CSV

Highlight Unused Rules

Reset Rule Hit Counter

Group

View Rulebase

General

Source

User

Destination

Application

Service/URL Category

Actions

Action Setting

Action: Allow

Send ICMP Unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

Schedule: None

QoS Marking: None

Disable Server Response Inspection

OKCancel

Destination

Zone

Address

(Intrazone)

any

any

any

19:35 8/26/2025

Section 1.4: Verify Internet Connectivity

Step 3: To test egress (outbound) connectivity from the internal to the external network, the websites www.msn.com and www.shutterfly.com were accessed. The following screenshot shows the captured traffic logs at the end of the sessions, corresponding to the Security Policy created in Section 1.3, Step 8.

David Eccles School of Business THE UNIVERSITY OF UTAH

Home Reservation u1275445@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79317 > Lab 03: Security and NAT Policies

Time Remaining: 1 hrs. 30 min.

Topology Content Status Client Firewall DMZ VRouter

The screenshot displays the Palo Alto Networks firewall management interface. The 'Monitor' tab is active, showing a list of traffic logs. The logs table includes columns for Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, Bytes, and HTTP2 Connection Session ID. The logs show traffic from 192.168.1.20 to various destinations, including google-base, sbl, and shutterfly. The actions are 'allow' and the rules are 'egress-outside'. The session end reasons are 'tcp-fin' and 'tcp-rst-from-client'.

Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP2 Connection Session ID
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	7.9K	0
192.168.1.20		204.79.197.203	443	sbl	allow	egress-outside	tcp-rst-from-server	246.9K	0
192.168.1.20		8.8.8.8	53	dns	allow	egress-outside	aged-out	220	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	19.5K	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	29.7K	0
192.168.1.20		23.44.100.88	80	shutterfly	allow	egress-outside	tcp-rst-from-client	2.1K	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	8.1K	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	19.4K	0
192.168.1.20		23.44.100.88	80	shutterfly	allow	egress-outside	tcp-rst-from-client	2.1K	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	29.6K	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	8.0K	0
192.168.1.20		23.44.100.88	80	shutterfly	allow	egress-outside	tcp-rst-from-client	2.1K	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	19.6K	0
192.168.1.20		142.250.189.14	443	google-base	allow	egress-outside	tcp-fin	29.6K	0
192.168.1.20		23.44.100.88	80	web-browsing	allow	egress-outside	tcp-rst-from-client	1.1K	0
192.168.1.20		75.716.55.48	443	unrecorded	allow	egress-outside	tcp-fin	177	0


admin | Logout | Last Login Time: 01/13/2025 04:39:32

Displaying logs 1 - 20 per page DESC

19:49 8/26/2025

Section 1.6: Create a Destination NAT Policy

Step 5: Below, I configured Destination NAT Policy. The setup involved initiating a connection from the Windows host (192.168.1.20) to the firewall's interface IP (192.168.1.1). The firewall then translated this connection to the DMZ server at 192.168.50.10.



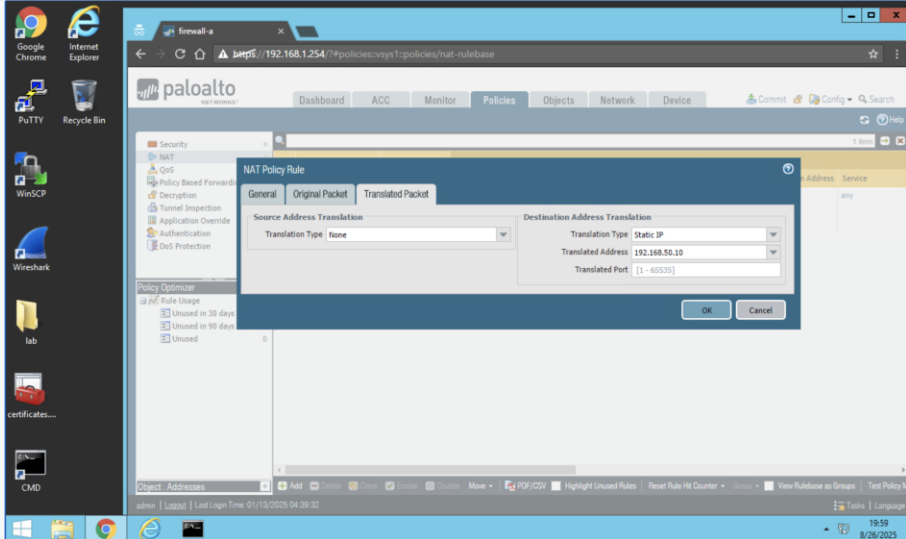
David Eccles
School of Business
THE UNIVERSITY OF UTAH

[Home](#) [Reservation](#) [u1275445@utah.edu](#)

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79317 > Lab 03: Security and NAT Policies

[Topology](#) [Content](#) [Status](#) [Client](#) [Firewall](#) [DMZ](#) [VRouter](#)

Time Remaining
1 20
hrs. min.



The screenshot displays the Palo Alto Networks firewall configuration interface. A 'NAT Policy Rule' dialog box is open, showing the 'General' tab. The 'Source Address Translation' section has 'Translation Type' set to 'None'. The 'Destination Address Translation' section has 'Translation Type' set to 'Static IP', 'Translated Address' set to '192.168.50.10', and 'Translated Port' set to '[1 - 65535]'. The background shows the 'Policies' tab with a list of rules and a 'Policy Optimizer' section.

Section 1.8: Testing Security Policy Rule connection for Logs View.

Step 9: In this section, I created a Security Policy rule to allow internal access to the DMZ FTP service, with logging enabled for any DMZ-related events starting at 20:15 and lasting for the next 5 minutes. The first screenshot below shows the time settings configured when the Security Policy was applied on the firewall. The following screenshot displays the successful traffic log entries generated after accessing the DMZ.

GlobalProtect Clientless VPN

Version59-31 (12/08/16)

TimeTue Aug 26 20:07:04 2025

Uptime0 days, 1:02:45

Plugin VM-Seriesvm_series-1.0.0-c29

David Eccles
School of Business
THE UNIVERSITY OF UTAH

HomeReservationu1275445@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79317 > Lab 03: Security and NAT Policies

Time Remaining
057
hrs. min.

Google Chrome

Internet Explorer

PutTY

WinSCP

Wireshark

lab

certificates...

CMD

firewall-a

https://192.168.1.254/?#monitor%3A%3Amonitor/logs/traffic

paloalto

DashboardACCMonitorPoliciesObjectsNetworkDevice

CommitConfigSearch

ManualHelp

Logs

(rule eq internal-dmz-ftp)

Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
192.168.1.20		192.168.1.1	56475	ftp	allow	internal-dmz-ftp	tcp-fin	560	0
192.168.1.20		192.168.1.1	21	ftp	allow	internal-dmz-ftp	tcp-fin	2.3k	0
192.168.1.20		192.168.1.1	21	ftp	allow	internal-dmz-ftp	tcp-fin	1.1k	0

Displaying logs 1 - 328 per pageDESC

Internet/192.168.1.254/ftp

20:22
8/26/2025