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

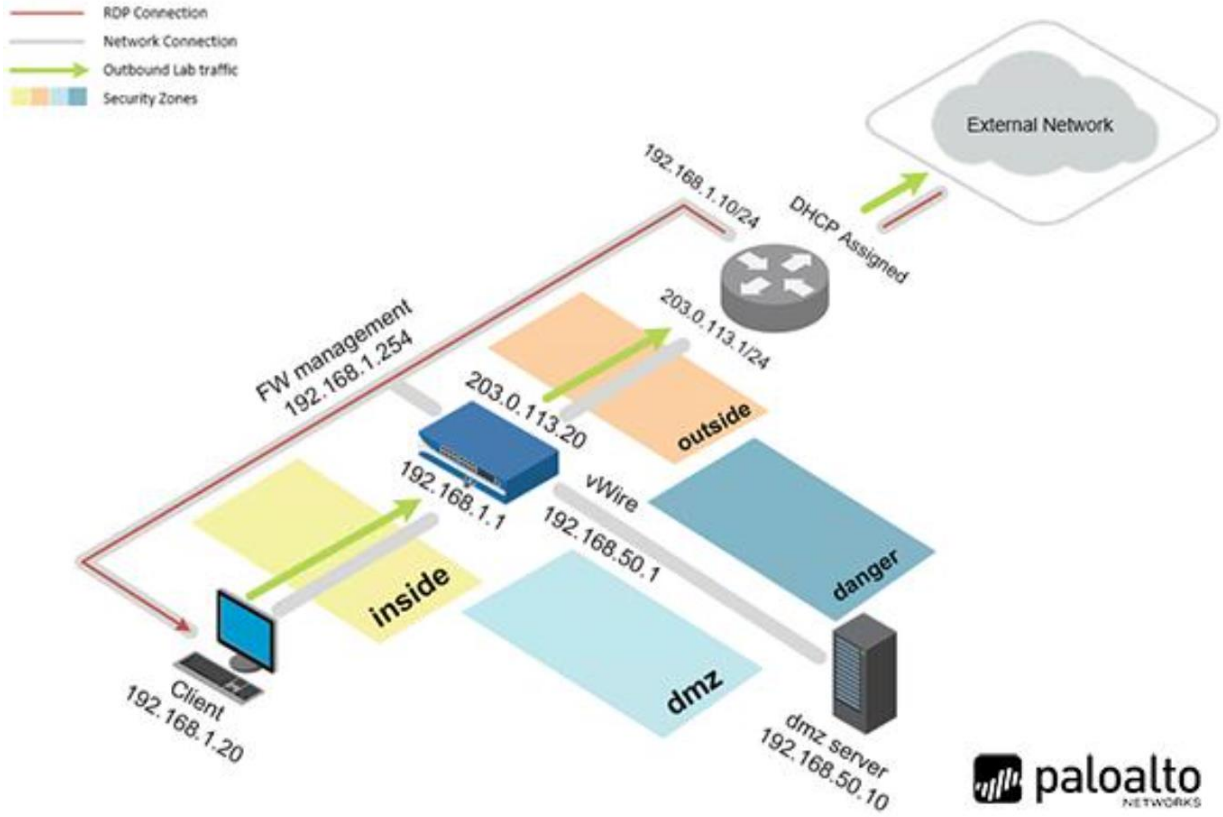
1.5 Create FTP Service

1.6 Create a Destination NAT Policy

1.7 Create a Security Policy Rule

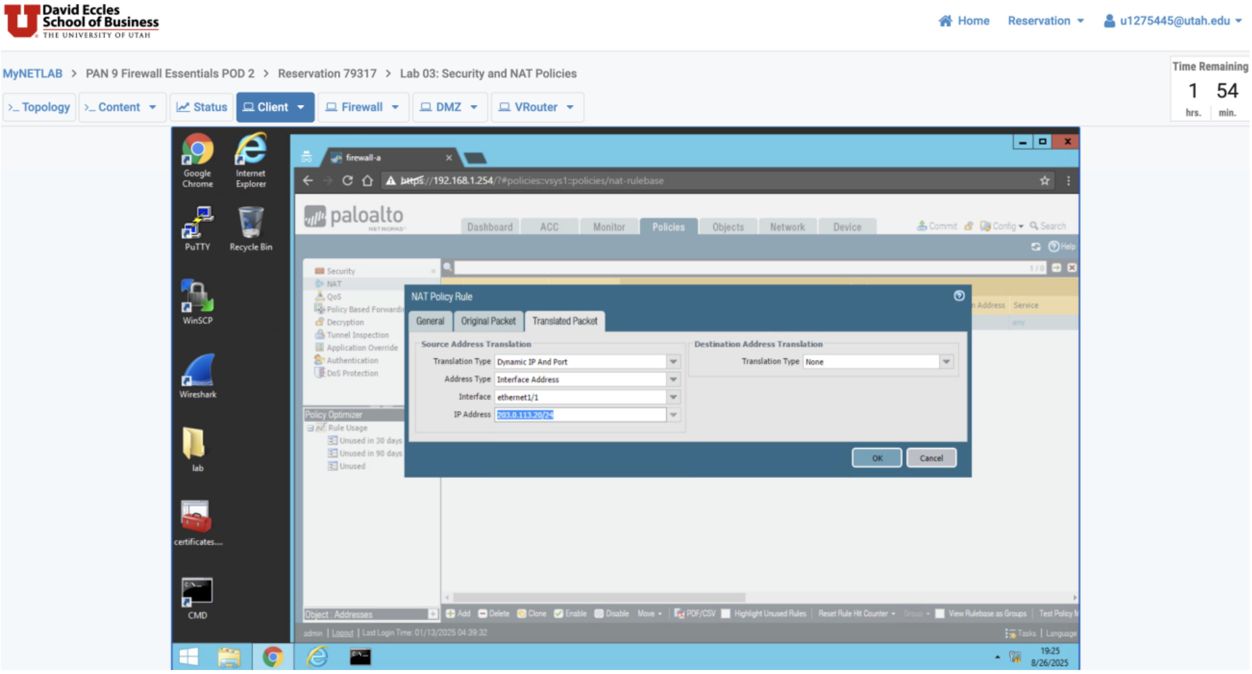
1.8 Test the Connection

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.


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 hrs. 54 min.
https://192.168.1.254/?#policies::vsys1::policies/nat-rulebase
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
OK
Cancel

NAT Policy Rule — Translated Packet

Source Address Translation

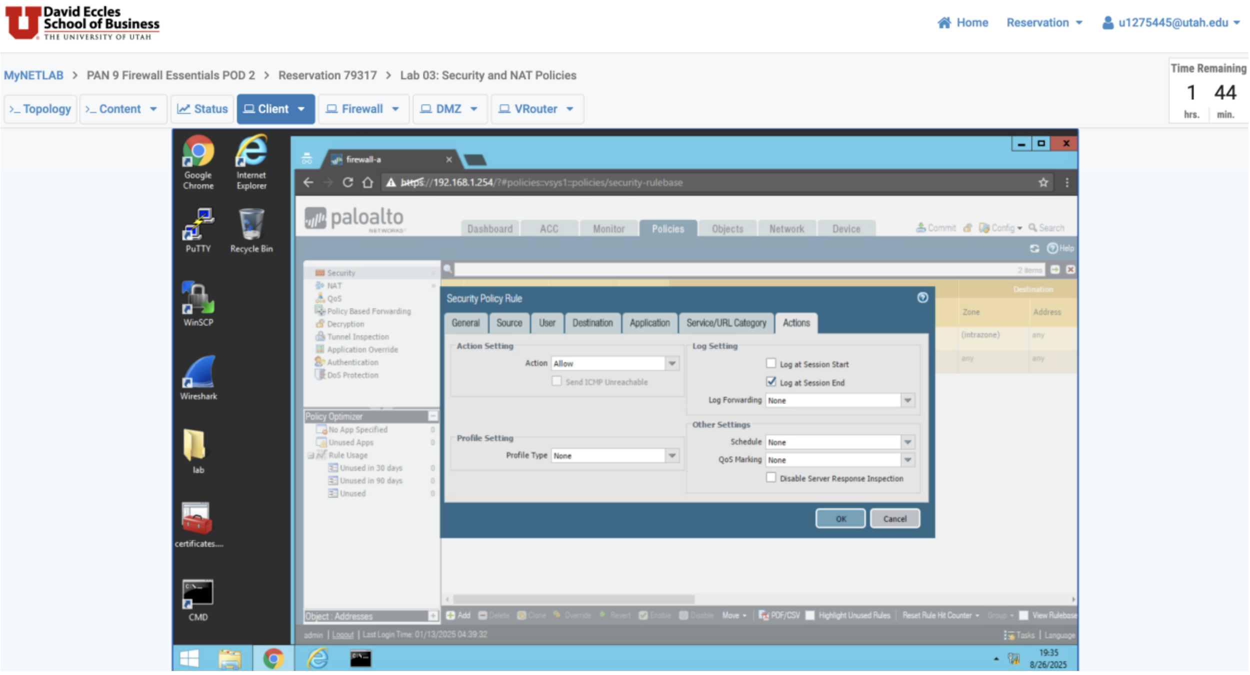
- Translation Type: Dynamic IP And Port
- Address Type: Interface Address
- Interface: ethernet1/1
- IP Address: 203.0.113.20/24

Destination Address Translation

- Translation Type: None

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.



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 hrs. 44 min.
https://192.168.1.254/?#policies::vsys1::policies/security-rulebase
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
OK
Cancel

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

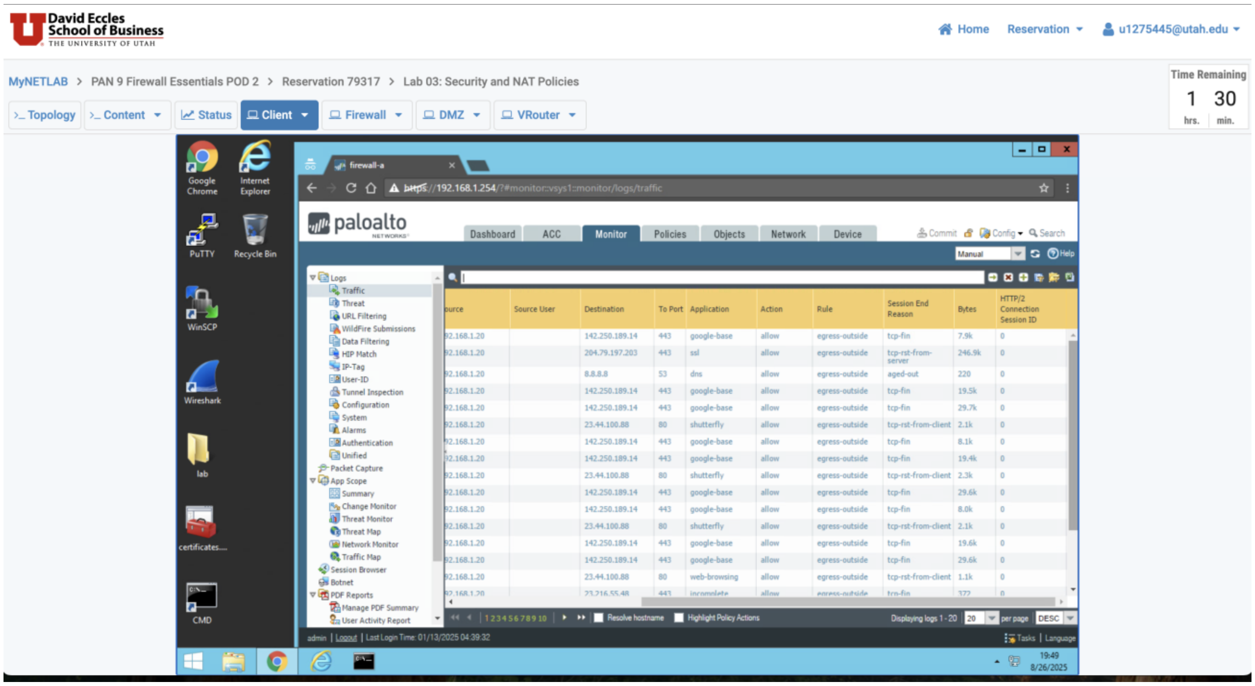
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

## Section 1.4: Verify Internet Connectivity

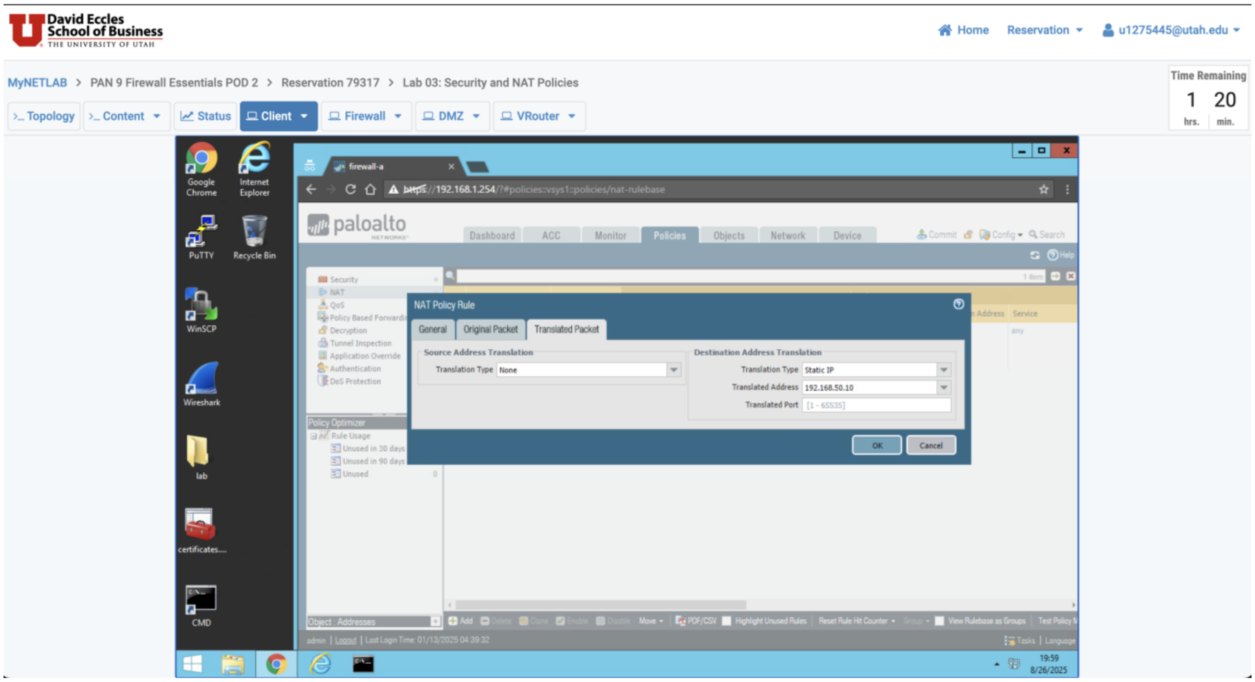
Step 3: To test egress (outbound) connectivity from the internal to the external network, the websites www.msn.com and www.shutterfly.com were accessed. The following screenshot shows the captured traffic logs at the end of the sessions, corresponding to the Security Policy created in Section 1.3, Step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



| ource | Source User | Destination | To Port | Application | Action | Rule | Session End Reason | Bytes | HTTP/2 Connection Session ID |
|---|---|---|---|---|---|---|---|---|---|
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 7.9k | 0 |
| 92.168.1.20 | | 204.79.197.203 | 443 | ssl | allow | egress-outside | tcp-rst-from-server | 246.9k | 0 |
| 92.168.1.20 | | 8.8.8.8 | 53 | dns | allow | egress-outside | aged-out | 220 | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 19.5k | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 29.7k | 0 |
| 92.168.1.20 | | 23.44.100.88 | 80 | shutterfly | allow | egress-outside | tcp-rst-from-client | 2.1k | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 8.1k | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 19.4k | 0 |
| 92.168.1.20 | | 23.44.100.88 | 80 | shutterfly | allow | egress-outside | tcp-rst-from-client | 2.3k | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 29.6k | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 8.0k | 0 |
| 92.168.1.20 | | 23.44.100.88 | 80 | shutterfly | allow | egress-outside | tcp-rst-from-client | 2.1k | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 19.6k | 0 |
| 92.168.1.20 | | 142.250.189.14 | 443 | google-base | allow | egress-outside | tcp-fin | 29.6k | 0 |
| 92.168.1.20 | | 23.44.100.88 | 80 | web-browsing | allow | egress-outside | tcp-rst-from-client | 1.1k | 0 |
| 92.168.1.20 | | 23.216.55.48 | 443 | incomplete | allow | egress-outside | tcp-fin | 372 | 0 |

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.


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

https://192.168.1.254/?#policies::vsys1::policies/nat-rulebase

NAT Policy Rule

Source Address Translation

Translation Type: None

Destination Address Translation

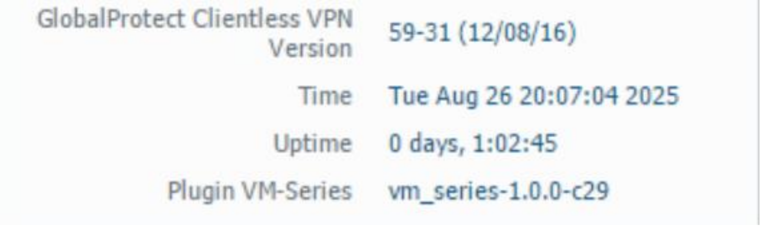
Translation Type: Static IP

Translated Address: 192.168.50.10

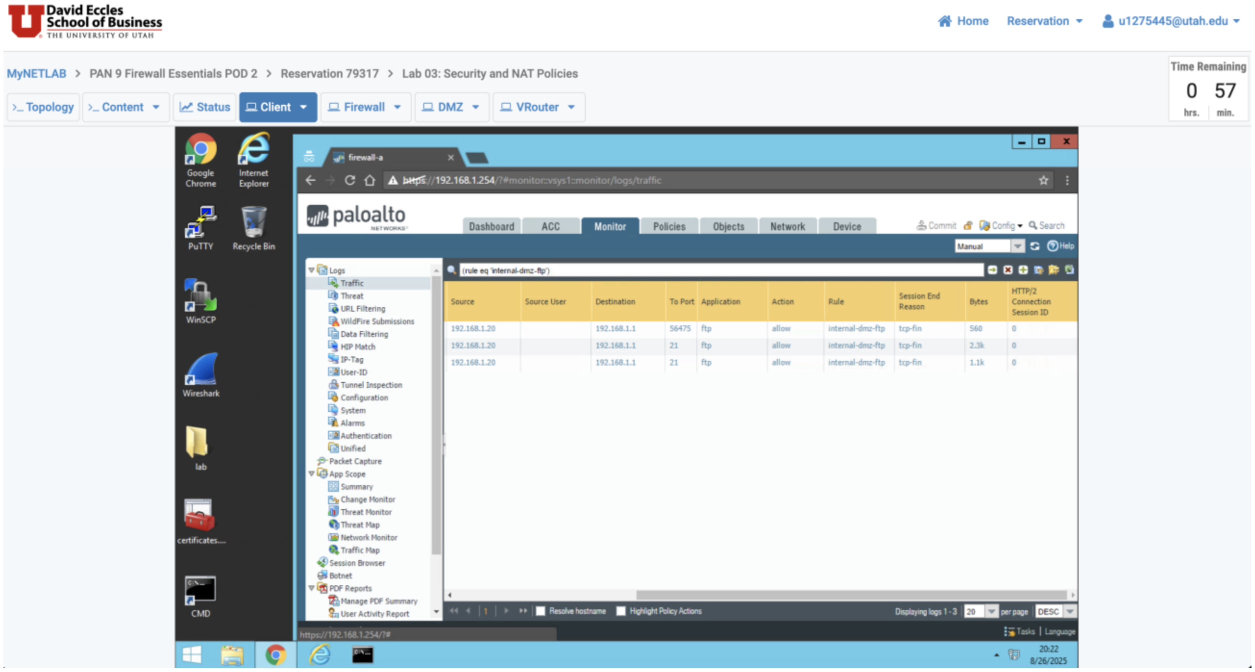
Translated Port: [1 - 65535]

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 Version | 59-31 (12/08/16) |
| Time | Tue Aug 26 20:07:04 2025 |
| Uptime | 0 days, 1:02:45 |
| Plugin VM-Series | vm_series-1.0.0-c29 |



https://192.168.1.254/?#monitor::vsys1::monitor/logs/traffic

(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 - 3 20 per page

https://192.168.1.254/?#

20:22
8/26/2025