

Vu Nguyen

UID: u1483046

Assignment 4 - PANEDU 04 – APP ID (Lab and Quiz)

1. Section 1.3, Step 7

The screenshot shows the Palo Alto Networks Panorama interface, specifically the Monitor tab. The left sidebar displays a navigation menu with categories like Traffic, Threat, and Policy. The main pane shows a table of traffic logs. The table has columns for Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, Bytes, and HTTP/2 Connection Session ID. The logs show various applications like google-base, integrated-fp, and top-fm being allowed or denied.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
01/23/2024 03:46:01	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	18.9k	0
01/23/2024 03:45:59	end	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	allow	integrated-fp	top-fm	1.3k	0
01/23/2024 03:45:51	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-rt-from-client	1.3k	0
01/23/2024 03:45:51	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-rt-from-client	1.3k	0
01/23/2024 03:45:51	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	24.8k	0
01/23/2024 03:45:41	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	25.4k	0
01/23/2024 03:45:31	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	18.9k	0
01/23/2024 03:45:21	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-rt-from-client	1.3k	0
01/23/2024 03:45:21	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-rt-from-client	1.4k	0
01/23/2024 03:45:21	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	25.3k	0
01/23/2024 03:45:11	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	25.3k	0
01/23/2024 03:45:01	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	41.7k	0
01/23/2024 03:44:51	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-rt-from-client	1.4k	0
01/23/2024 03:44:41	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	25.6k	0
01/23/2024 03:44:31	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	17.0k	0
01/23/2024 03:44:21	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-rt-from-client	1.4k	0
01/23/2024 03:44:11	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	26.8k	0
01/23/2024 03:44:01	end	inside	outside	192.168.1.20		172.217.78.78	443	google-base	allow	egress-outside	top-fm	25.3k	0

2. Section 1.4, Step 8

The screenshot shows the Palo Alto Networks Panorama interface, specifically the Policy tab. The left sidebar displays a navigation menu with categories like Security, Policy, and Policy Optimizer. The main pane shows a table of Security Policy Rules. A modal window is open, showing the configuration for a Security Policy Rule. The modal has tabs for General, Source, User, Destination, Application, Service/URL, Category, Actions, and Usage. The General tab is selected, showing the rule name, tags, type, and zone. The rule is named 'egress-outside-app-id' and is of type 'universal'. The rule is configured to allow traffic from the 'inside' zone to the 'outside' zone. The modal also shows a list of applications and services that are allowed by the rule.

Name	Tags	Type	Zone
1 egress-outside-app-id	egress	universal	int inside
2 egress-outside	egress	universal	int inside
3 internal-allow-fp	internal	universal	int inside
4 integrated-fp-pert-ba	internal	universal	int inside
5 intrazone-default	none	intrazone	any
6 intrazone-default	none	intrazone	any

3. Section 1.8, Step 2


The screenshot displays the Palo Alto Networks Firewall Essentials web interface. At the top, there's a navigation bar with tabs like Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The 'Monitor' tab is active, showing a 'Logs' section titled 'firewall-traffic'. A sidebar on the left lists various log types such as Threat, URL Filtering, WildFire Submissions, Data Filtering, WFP Hatch, IP Tag, User-ID, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture, App Scope, Summary, Change Monitor, Threat Monitor, Threat Map, Network Monitor, Traffic Map, Session Browser, Botnet, PDF Reports, Manage PDF Summary, and User Activity Report.

The main area shows a table of firewall logs. The table has columns for Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, Bytes, HTTP/2 Connection, and Session ID. The logs show multiple entries for blocked traffic from 192.168.1.254 to 172.217.0.78, all denied by the 'google-base' rule.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection	Session ID
01/23 03:59:49	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:45	end	inside	outside	192.168.1.20	8.8.8.8	53		dns	allow	sgrag-outside-sip-id	app-end	313	0	
01/23 03:59:32	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:32	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:32	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:30	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:30	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:29	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:29	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:29	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:29	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:29	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:29	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:28	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:26	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
01/23 03:59:26	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	

At the bottom, there's a status bar showing 'Displaying logs 1: 20' and 'per page 2500'. The user is logged in as 'u1483046@utah.edu'.

4. Section 1.13, Step 6


David Eccles School of Business
 THE UNIVERSITY OF UTAH

[Home](#)
[Reservation](#)
[u1483046@utah.edu](#)


MYNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 68673 > Lab 04: App-ID

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

Time Remaining
0 12
 hrs. min.

firewall-a

[←](#)
[↻](#)
[🔍](#)
[https://192.168.1.254/#monitorsys1:monitor/logs?traffic](#)


paloalto
 NETWORKING

[Dashboard](#)
[ACG](#)
[Monitor](#)
[Policies](#)
[Objects](#)
[Network](#)
[Device](#)

[Commit](#)
[Config](#)
[Search](#)

[Manual](#)
[Help](#)

Logs

- Traffic
- Threat
- URL Filtering
- Wildfire Submissions
- Data Filtering
- VPN Match
- IP-Tag
- User-ID
- Tunnel Inspection
- Configuration
- System
- Alarms
- Authentication
- Unfiled
- Packet Capture
- App Scan Scope
- Summary
- Change Monitor
- Threat Monitor
- Threat Map
- Network Monitor
- Traffic Map
- Session Browser
- Botnet
- PCF Reports
- Manage PDF Summary
- User Activity Report

```

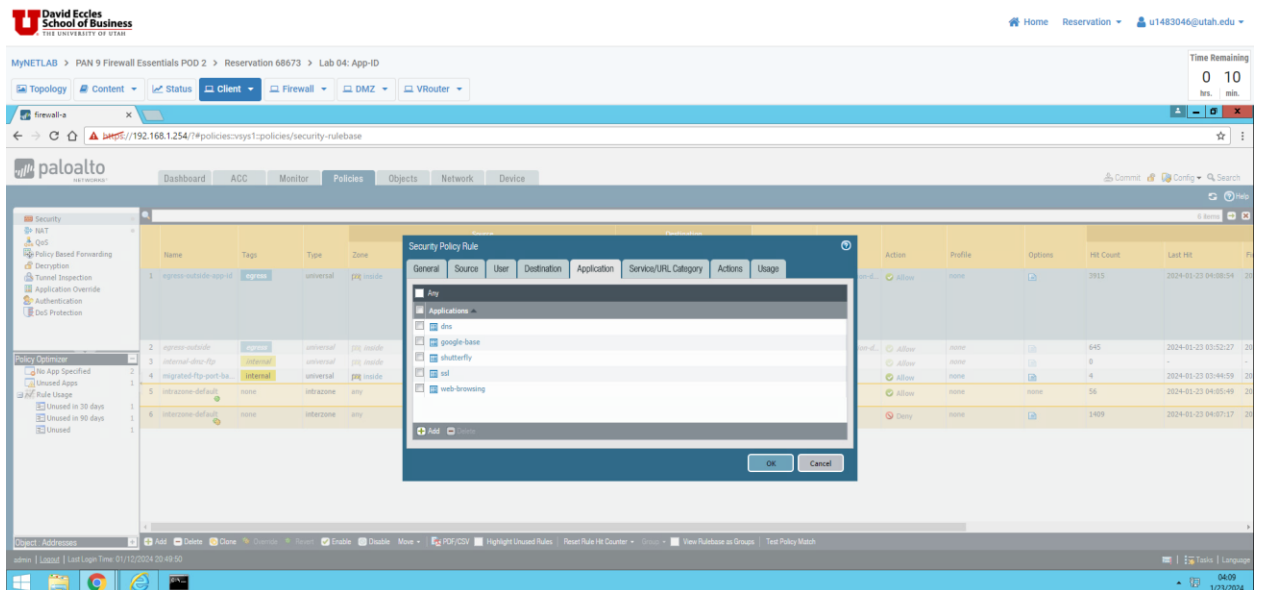
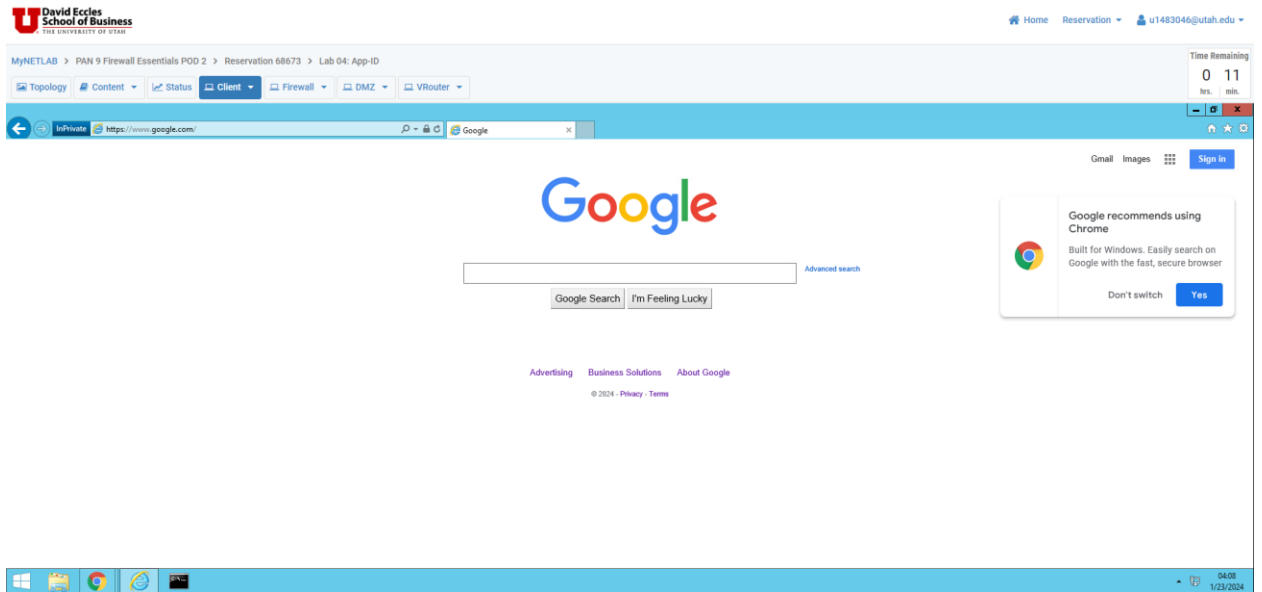
receive_time geq "2024/01/23 03:00:00" AND receive_time leq "2024/01/23 03:59:59" AND (app eq google-base)
      
```

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection	Session ID
🔍	01/23 03:59:59	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:59	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:59	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:59	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:59	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:58	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:56	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:56	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:56	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:56	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:54	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:54	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:54	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:54	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:54	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	
🔍	01/23 03:59:53	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0	

[Resolve](#)
[Resolve](#)
[Highlight Policy Actions](#)

Displaying logs 1-20
 [20](#)
 per page
 [DESC](#)

[Tasks](#)
[Language](#)



(I was running out of time, so I cant wait 15 minutes for the log to load, according to the instruction, I also put the extra picture to proof that I change the google-base to be part of the acceptance)

5. Section 1.14, Step 15

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 68673 > Lab 04: App-ID

Time Remaining
0 08
hrs. min.

Topology Content Status Client Firewall DMZ VRouter

firewall-a

https://192.168.1.254/?monitorcvys1:monitor/logs/traffic

paloalto
NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

Logs

Traffic

Threat

URL Filtering

Wildfire Submissions

Data Filtering

VPN Watch

IP-Tag

User-ID

Tunnel Inspection

Configuration

System

Alarms

Authentication

Unifed

Packet Capture

Summary

App Scope

Change Monitor

Threat Monitor

Network Monitor

Traffic Map

Session Browser

Bitnet

PDF Reports

Manage PDF Summary

User Activity Report

Cisco Configuration Monitor

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
01/23 04:11:33	end	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	allow	internal-dmz-rtp	tcp-fin	1.3K	0
01/23 04:11:26	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	12.7K	0
01/23 04:11:21	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	19.0K	0
01/23 04:11:16	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	32.9K	0
01/23 04:11:14	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-rst-from-client	6.4K	0
01/23 04:11:11	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	65.9K	0
01/23 04:11:10	drop	dmz	outside	192.168.50.10		192.168.42.1	53	not-applicable	deny	interzone-default	policy-deny	88	0
01/23 04:11:05	drop	dmz	outside	192.168.50.10		192.168.42.1	53	not-applicable	deny	interzone-default	policy-deny	88	0
01/23 04:10:56	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	13.0K	0
01/23 04:10:51	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	19.2K	0
01/23 04:10:46	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	33.6K	0
01/23 04:10:46	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-rst-from-client	6.4K	0
01/23 04:10:41	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	62.1K	0
01/23 04:10:36	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	10.0K	0
01/23 04:10:26	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-fin	12.3K	0

Admin | Logout | Last Login Time 01/15/2024 20:49:50

14 1/254 5.678916 Resolve Hostname Highlight Policy Actions

Displaying logs 1 - 20 per page DESC

Tools | Language

04:11 1/23/2024