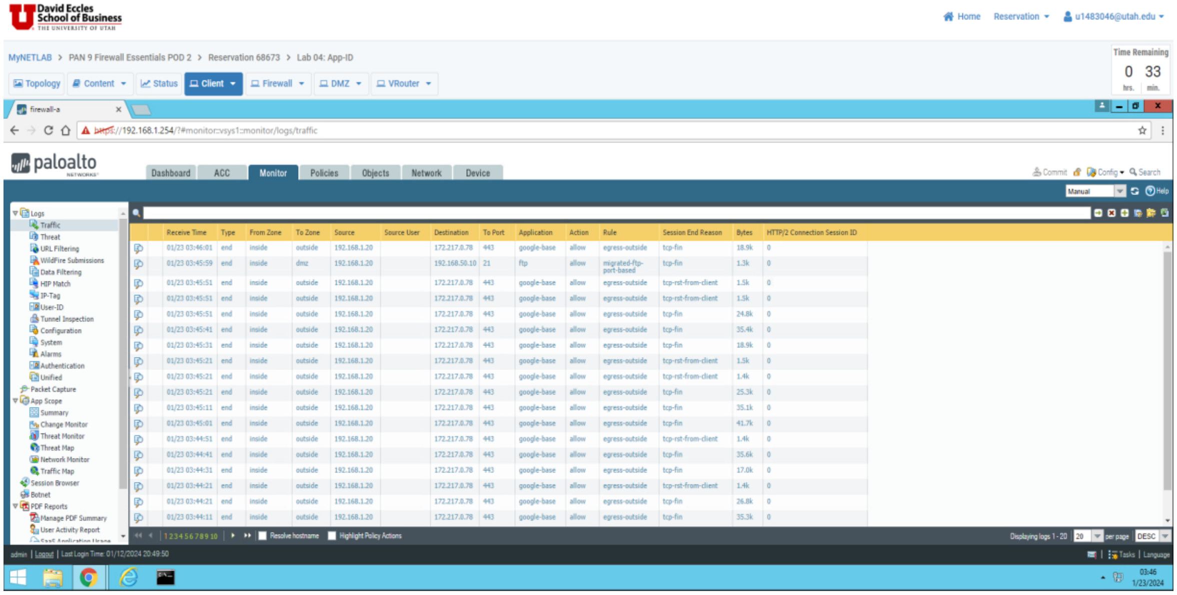
Vu Nguyen

UID: u1483046

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

1. Section 1.3, Step 7

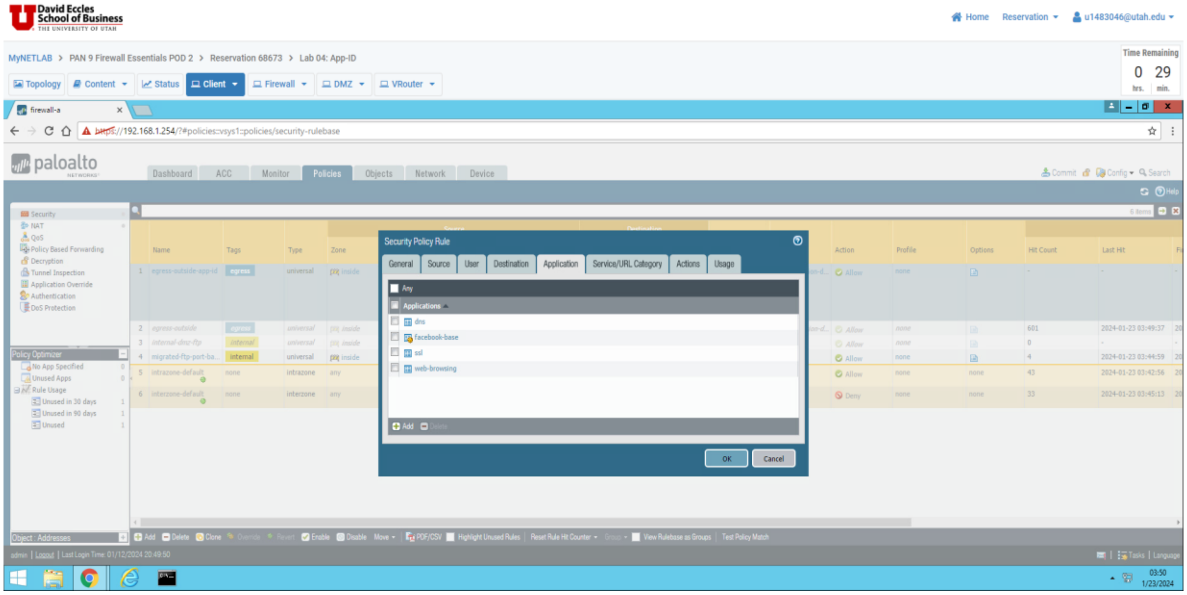


https://192.168.1.254/?#monitor::vsys1::monitor/logs/traffic

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 03:46:01	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	18.9k	0
01/23 03:45:59	end	inside	dmz	192.168.1.20		192.168.50.10	21	ftp	allow	migrated-ftp-port-based	tcp-fin	1.3k	0
01/23 03:45:51	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-rst-from-client	1.5k	0
01/23 03:45:51	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-rst-from-client	1.5k	0
01/23 03:45:51	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	24.8k	0
01/23 03:45:41	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	35.4k	0
01/23 03:45:31	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	18.9k	0
01/23 03:45:21	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-rst-from-client	1.5k	0
01/23 03:45:21	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-rst-from-client	1.4k	0
01/23 03:45:21	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	25.3k	0
01/23 03:45:11	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	35.1k	0
01/23 03:45:01	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	41.7k	0
01/23 03:44:51	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-rst-from-client	1.4k	0
01/23 03:44:41	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	35.6k	0
01/23 03:44:31	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	17.0k	0
01/23 03:44:21	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-rst-from-client	1.4k	0
01/23 03:44:21	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	26.8k	0
01/23 03:44:11	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside	tcp-fin	35.3k	0

admin | Logout | Last Login Time: 01/12/2024 20:49:50

2. Section 1.4, Step 8



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

Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions | Usage

□ Any

□	Applications ▲
□	dns
□	facebook-base
□	ssl
□	web-browsing

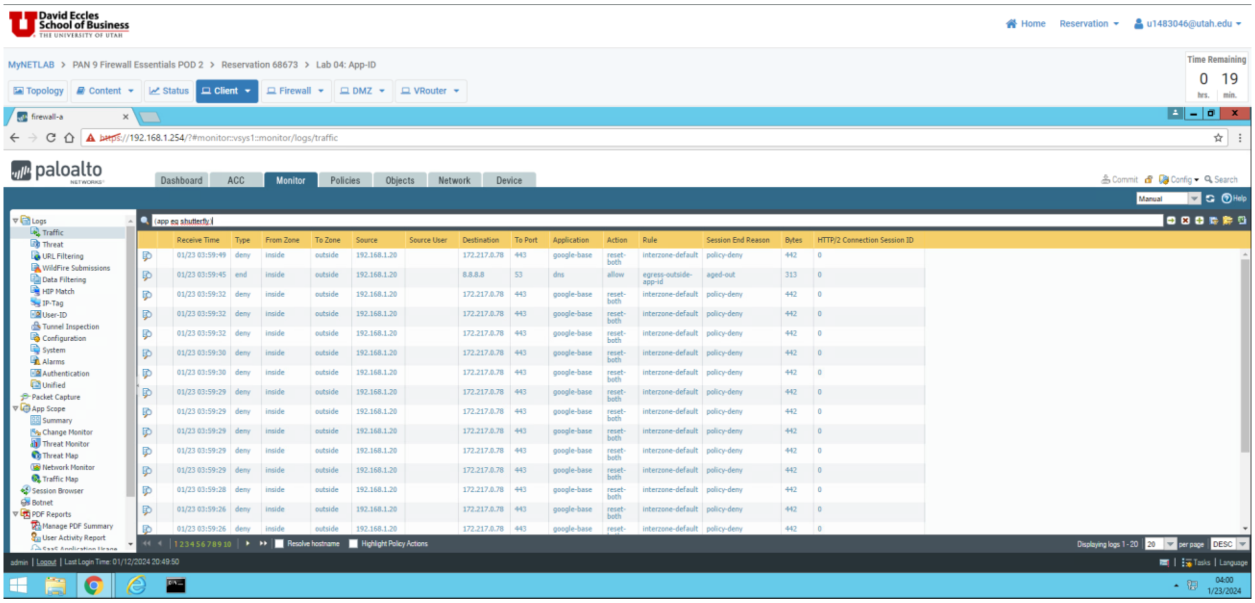
Add Delete

OK Cancel

	Name	Tags	Type	Zone	Action	Profile	Options	Hit Count	Last Hit
1	egress-outside-app-id	egress	universal	inside	Allow	none		-	-
2	egress-outside	egress	universal	inside	Allow	none		601	2024-01-23 03:49:37
3	internal-dmz-ftp	internal	universal	inside	Allow	none		0	-
4	migrated-ftp-port-ba...	internal	universal	inside	Allow	none		4	2024-01-23 03:44:59
5	intrazone-default	none	intrazone	any	Allow	none	none	43	2024-01-23 03:42:56
6	interzone-default	none	interzone	any	Deny	none	none	33	2024-01-23 03:45:13

admin | Logout | Last Login Time: 01/12/2024 20:49:50

3. Section 1.8, Step 2



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

Time Remaining 0 hrs. 19 min.

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

(app eq shutterfly)

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	egress-outside-app-id	aged-out	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 03:59:28	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-	interzone-default	policy-deny	442	0

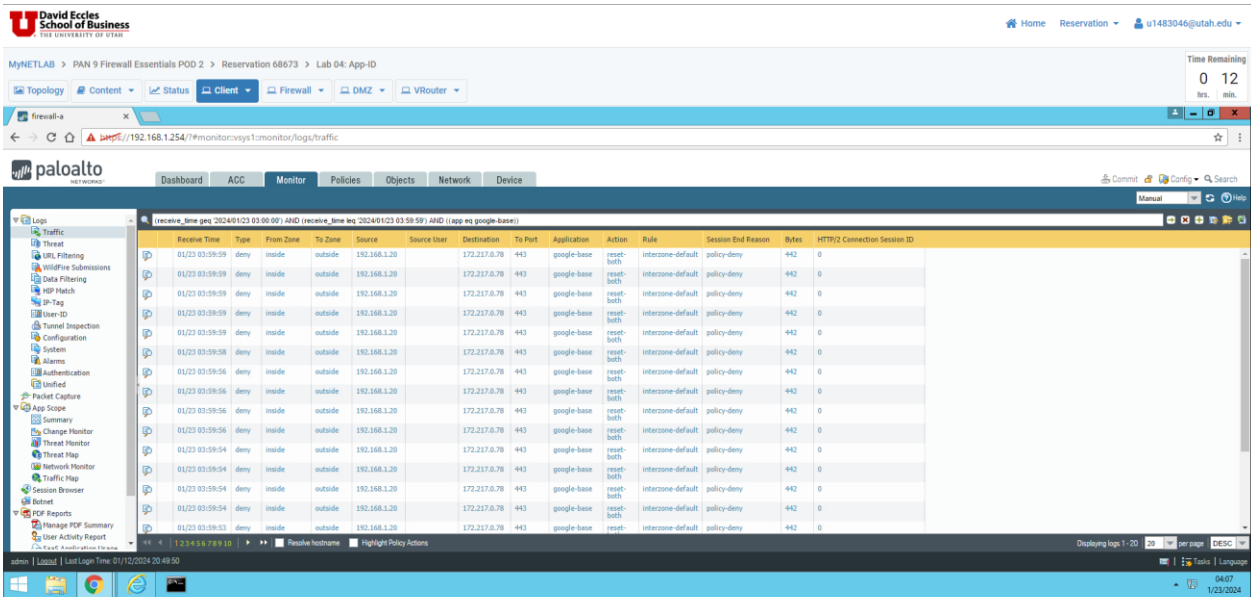
□ Resolve hostname □ Highlight Policy Actions

Displaying logs 1 - 20 20 per page DESC

admin | Logout | Last Login Time: 01/12/2024 20:49:50

04:00
1/23/2024

4. Section 1.13, Step 6



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

Time Remaining 0 hrs. 12 min.

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

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

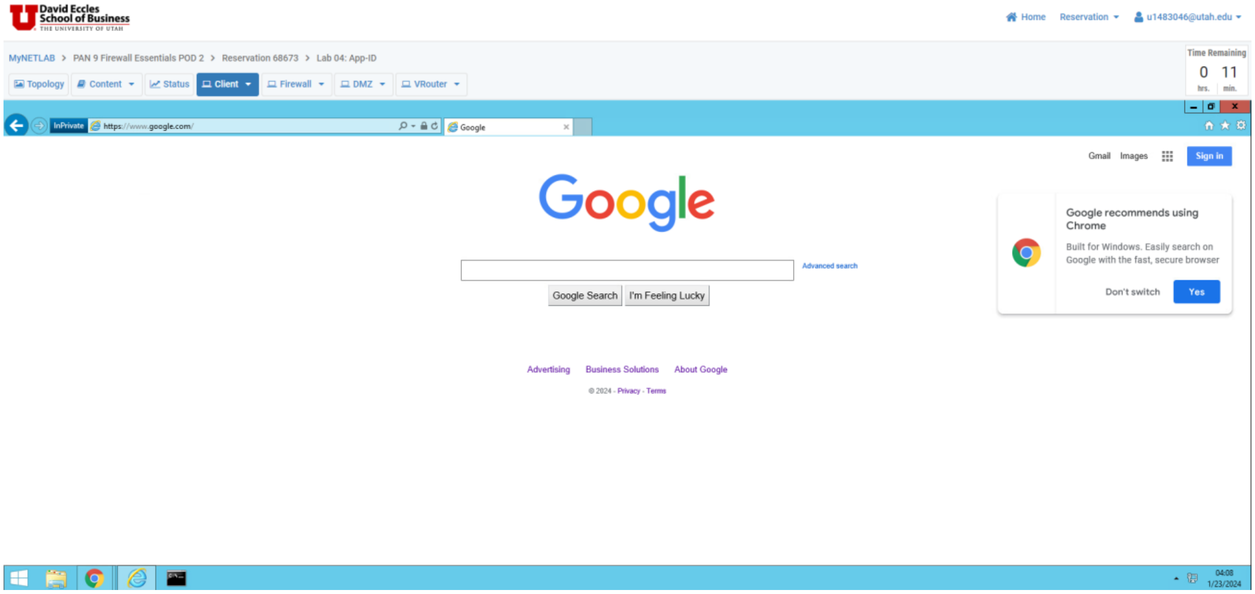
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
01/23 03:59:59	deny	inside	outside	192.168.1.20		172.217.0.78	443	google-base	reset-both	interzone-default	policy-deny	442	0
01/23 03:59:59	deny	inside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

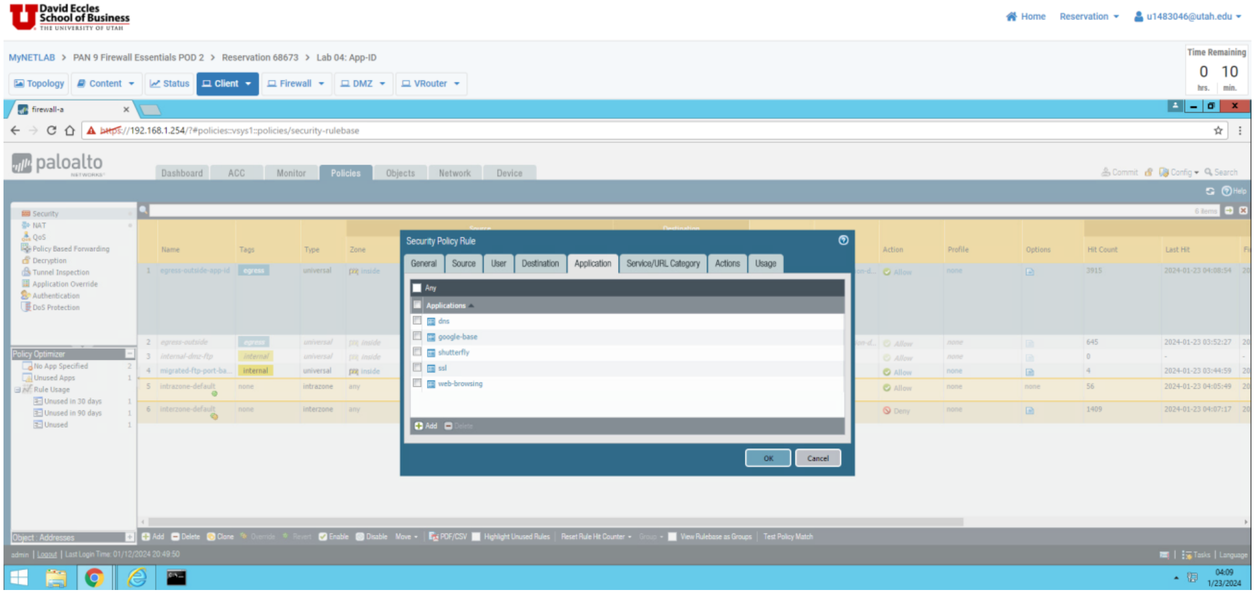
□ Resolve hostname □ Highlight Policy Actions

Displaying logs 1 - 20 20 per page DESC

admin | Logout | Last Login Time: 01/12/2024 20:49:50

04:07
1/23/2024





Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions | Usage

□ Any

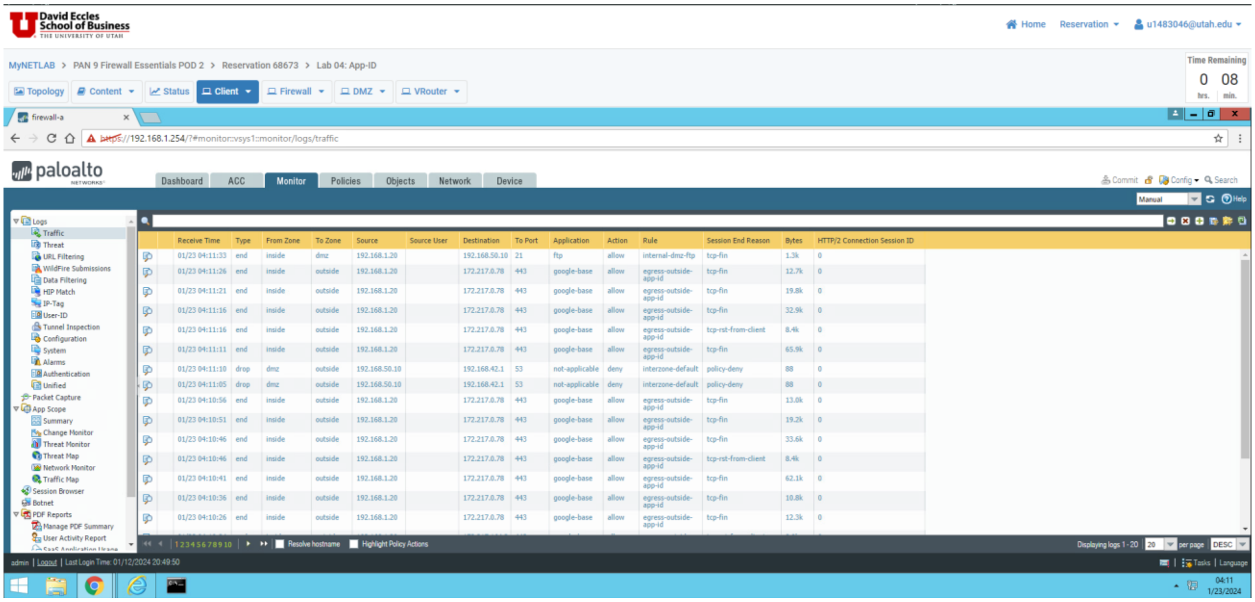
□ Applications
- □ dns
- □ google-base
- □ shutterfly
- □ ssl
- □ web-browsing

Add | Delete

OK | Cancel

(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



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	ftp	allow	internal-dmz-ftp	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	19.8k	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 04:11:16	end	inside	outside	192.168.1.20		172.217.0.78	443	google-base	allow	egress-outside-app-id	tcp-rst-from-client	8.4k	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	8.4k	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	10.8k	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