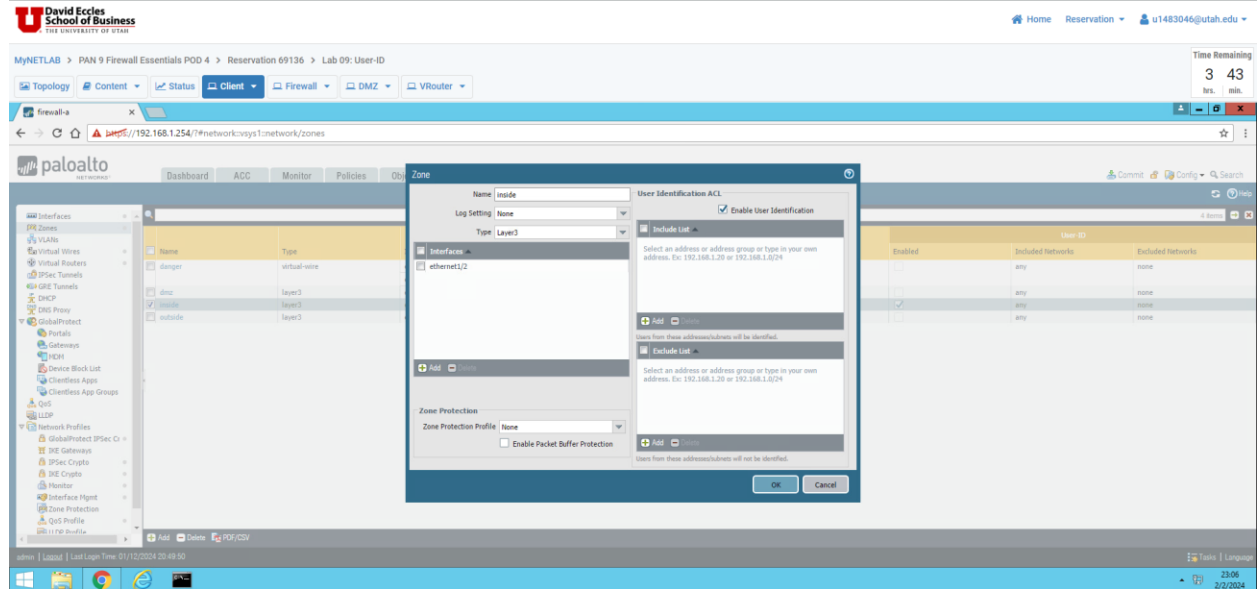


Vu Nguyen

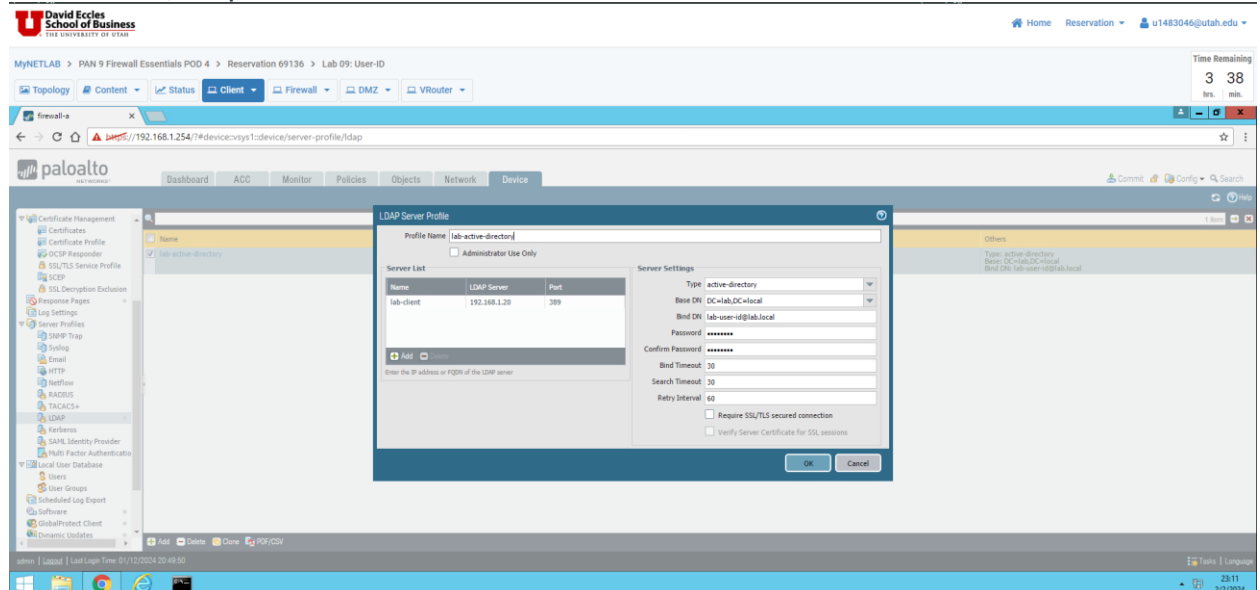
UID: u1483046

Assignment 10 – PANEDU09 – User ID (Lab and Quiz)

1. Section 1.1, Step 3



2. Section 1.2, Step 5



3. Section 1.3, Step 4

David Eccles School of Business THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 4 > Reservation 69136 > Lab 09: User-ID

Topology Content Status Client Firewall DMZ VRouter

Time Remaining 3 35 hrs. min.

Firewall-a x

192.168.1.254/?devicecvys1:device/user-identification

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Group Mapping

Name lab-group-mapping

Server Profile User and Group Attributes Group Include List Custom Group

Available Groups

lab users

lablab.DC=local

Included Groups

lablab users

OK Cancel

Update Interval (sec) default

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

23:14 2/2/2024

4. Section 1.6, Step 2

David Eccles School of Business THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 4 > Reservation 69136 > Lab 09: User-ID

Topology Content Status Client Firewall DMZ VRouter

Time Remaining 3 29 hrs. min.

Firewall-a x

192.168.1.254/?monitortcvys1:monitor/logs/traffic

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Logs

192.168.1.254

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
02/02 23:20:38	end	inside	outside	192.168.1.20	lablab-user	68.142.107.4	80	incomplete	allow	egress-outside	aged-out	132	0
02/02 23:20:38	end	inside	outside	192.168.1.20	lablab-user	172.217.6.78	443	google-base	allow	egress-outside	top-fin	6.9k	0
02/02 23:20:37	end	inside	outside	192.168.1.20	lablab-user	68.142.107.4	80	incomplete	allow	egress-outside	aged-out	132	0
02/02 23:20:31	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	192	0
02/02 23:20:31	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	319	0
02/02 23:20:30	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	207	0
02/02 23:20:30	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	209	0
02/02 23:20:30	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	188	0
02/02 23:20:30	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	220	0
02/02 23:20:30	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	188	0
02/02 23:20:29	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	387	0
02/02 23:20:29	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	385	0
02/02 23:20:29	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	387	0
02/02 23:20:28	end	inside	outside	192.168.1.20	lablab-user	172.217.6.78	443	google-base	allow	egress-outside	top-fin	26.1k	0
02/02 23:20:26	end	inside	outside	192.168.1.20	lablab-user	68.142.107.4	80	incomplete	allow	egress-outside	aged-out	62	0
02/02 23:20:24	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	268	0
02/02 23:20:24	end	inside	outside	192.168.1.20	lablab-user	8.8.8.8	53	dns	allow	egress-outside	aged-out	272	0

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

23:20 2/2/2024

5. Section 1.8, Step 4

David Eccles School of Business
THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 4 > Reservation 69136 > Lab 09: User-ID

Topology Content Status Client Firewall DMZ VRouter

Time Remaining
3 25
hrs. min.

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

paloalto

Dashboard ACC Monitor Policies Objects Network Device

Manual Search

Logs

- Traffic
- Threat
- URL Filtering
- Wildfire Submissions
- Data Filtering
- HIP Match
- Geo-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
- User Activity Report

Rule log: egress-outside-user-id

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	197792 Connection Session ID
02/02 23:23:32	deny	inside	outside	192.168.1.20	lab\lab-user	157.240.11.35	80	facebook-base	reset-both	egress-outside-user-id	policy-deny	621	0
02/02 23:23:32	deny	inside	outside	192.168.1.20	lab\lab-user	157.240.11.35	80	facebook-base	reset-both	egress-outside-user-id	policy-deny	501	0

Displaying logs 1-2 per page DESC

admin | Logout | Last Login Time 01/10/2024 20:49:50

23:24 2/2/2024