

Student: Sunil Tiwari

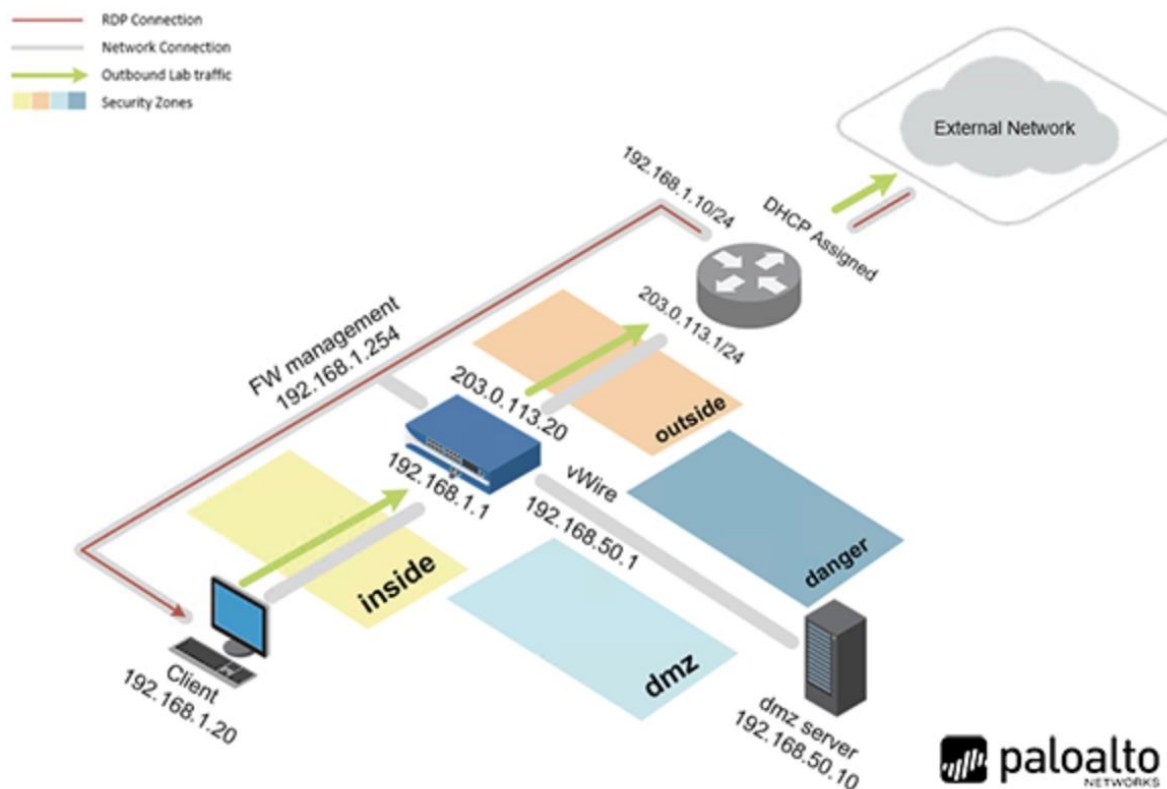
Lab: PANEDU 05B - Content-ID

Date: September 4th, 2025

Objective:

1. Configure and test a Vulnerability Security Profile
2. Configure and test a File Blocking Security Profile
3. Use the Virtual Wire mode and configure the danger zone
4. Generate threats and observe the actions taken

Topology:



Section 1.3 — Review the Logs

Step 4

David Eccles School of Business THE UNIVERSITY OF UTAH

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79553 > Lab 05-B: Content-ID

Time Remaining: 2 34 hrs. min.

Topology Content Status Client Firewall DMZ VRouter

The screenshot shows the Palo Alto Networks Panorama GUI. The 'Log View' tab is selected, displaying a list of logs. A log entry is highlighted, showing details such as 'Receive Time', 'Type', 'Name', 'From Zone', 'To Zone', 'Source address', 'Source User', 'Destination address', 'To Port', 'Application', and 'Action'. The log entry is for a packet capture, showing a packet from 192.168.1.20 to 192.168.1.20, type 'FTP', with a 'vulnerability' action.

Section 1.4 — Update the Vulnerability Profile

Step 7: Reran the ftp-brute.bat script to initiate new FTP brute force attempts. Monitored and reviewed the logs to verify that the attack attempts were successfully reset. The script was allowed to run for a minimum of one minute.

David Eccles School of Business THE UNIVERSITY OF UTAH

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79553 > Lab 05-B: Content-ID

Time Remaining: 2 28 hrs. min.

Topology Content Status Client Firewall DMZ VRouter


The screenshot shows the Palo Alto Networks Panorama GUI. The 'Log View' tab is selected, displaying a list of logs. The logs show multiple 'FTP login Brute Force attempt' entries, all with a 'vulnerability' type and 'reset-both' action. The logs are sorted by 'Receive Time'.

Receive Time	Type	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action
09/04 18:20:49	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:47	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:46	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:45	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:45	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:45	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:44	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:44	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:43	spyware	Suspicious TLS Session	inside	outside	192.168.1.20		142.250.66.78	443	google-base	alert
09/04 18:20:42	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both
09/04 18:20:40	vulnerability	FTP login Brute Force attempt	inside	dmz	192.168.1.20		192.168.50.10	21	Rtp	reset-both

Section 1.5 — Create a Security Profile Groups — Specifies set of Security Profiles that can

be treated as a unit and then added to a Security Profile Rules.

Step 14



David Eccles
School of Business
THE UNIVERSITY OF UTAH

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

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79553 > Lab 05-B: Content-ID

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


Time Remaining

2 20
hrs. min.

firewall-a

192.168.1.254

192.168.1.254/policies/rye1-policies/security-rulebase



Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Commit

Config

Search

Security

NAT

QoS

Policy Based Forwarding

Decryption

Tunnel Inspection

Application Override

Authentication

Content Protection

	Name	Tags	Type	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service
1	egress-outside-content-id	egress	universal	any	any	any	any	any	any	any	any
2	egress-outside	egress	universal	any	any	any	any	any	any	any	any
3	internal-inside-dmz	internal	universal	any	any	any	any	any	any	any	any
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any

Policy Optimizer

No App Specified

Unused Apps

Rule Usage

Unused in 30 days

Unused in 90 days

Unused

Object

Addresses

Add

Delete

Clone

Override

Reset

Export

Import

More

PDF/CSV

Highlight Unused Rules

Reset Rule Hit Counter

View Rulebase as Groups

Test Policy Match

admin

Logout

Last Login Time: 01/13/2025 04:39:52

Tasks

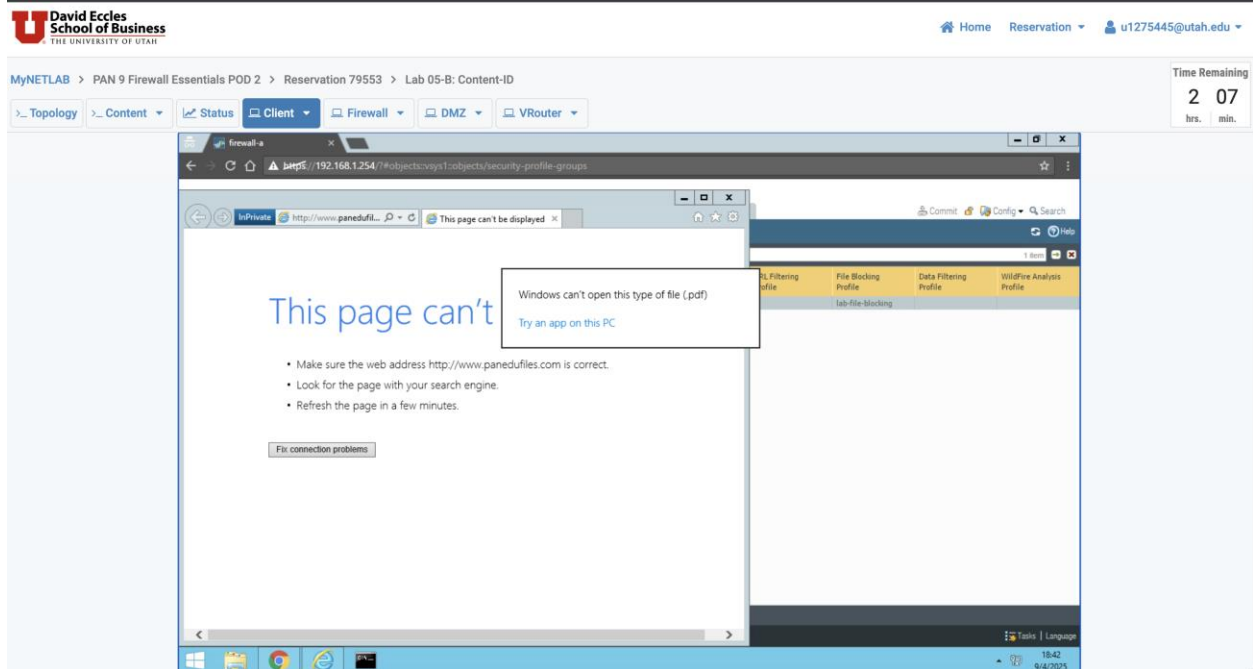
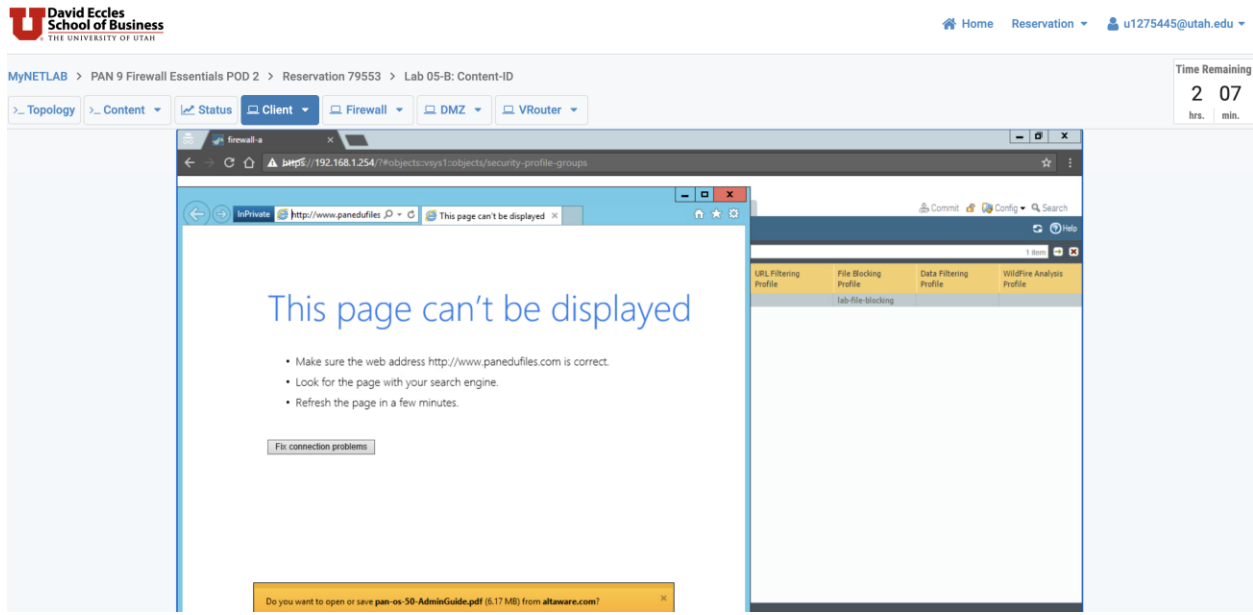
Language

18:29

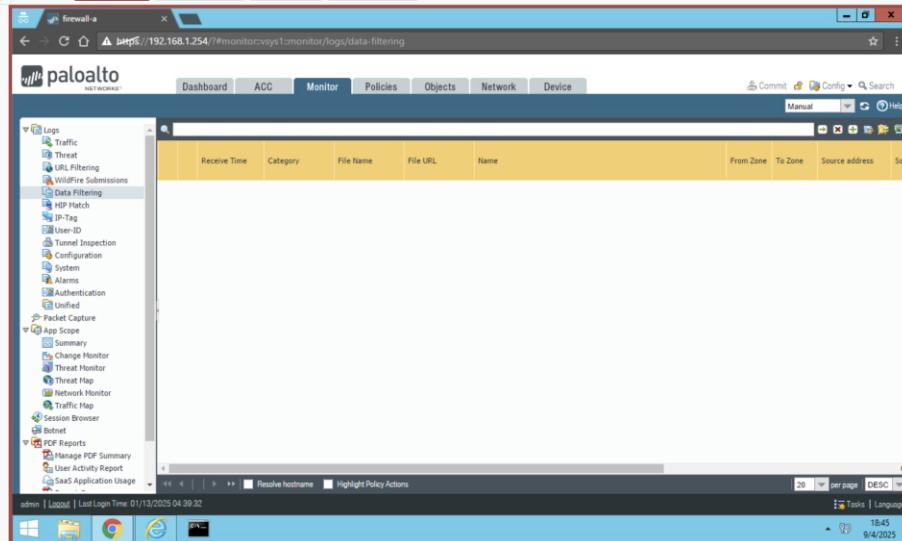
9/4/2025

Section 1.8 —

Step 5: Created a File Blocking rule for pdf file and upon trying to download the file from the site: <http://www.panedufiles.com>, the system blocked the pdf file download.



Per the lab instructions, if this scenario were performed in a real-world environment, the firewall would be expected to block the PDF download and log the event. However, since this is a virtual lab, I encountered an internet connection error while accessing the download site and was therefore unable to capture the logs, as shown below.



Section 1.17 —

For this step, I modified the Security Profile Group lab-spg by setting the file-blocking profile action to “None.” As a result, when executing the command `sh /tg/malware.sh` from putty-traffic-detection, the firewall allowed the file transfer, but still detected and blocked actions based on the identified severity-threat type. The relevant logs were successfully captured, as shown below.

Step 4

MyNETLAB > PAN 9 Firewall Essentials POD 2 > Reservation 79553 > Lab 05-B: Content-ID

Time Remaining
1 37
hrs. 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 logs. The left sidebar contains a navigation menu with options like Traffic, Threat, URL Filter, Data Filter, HRP Match, IP-Tag, User-ID, Tunnel In, Configure, System, Alarms, Unifire, Packet Capt, App Scope, Summary, Change M, Threat M, Network M, Traffic M, Session Mon, Botnet, PDF Reports, Manage P, and User Acti. The main area shows a table of logs with columns: Receive Time, Type, Name, From Zone, To Zone, Source address, Source User, Destination address, To Port, Application, Action, and Severity. The logs show several 'spyware' events detected by 'Content-ID' and one 'vulnerability' event related to 'Trojan-Win32.Asmort.d/ap'. The severity levels range from 'informational' to 'high'.

Receive Time	Type	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action	Severity
05/04 19:07:40	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:07:10	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:07:01	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:06:40	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:06:31	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:06:23	vulnerability	Trojan-Win32.Asmort.d/ap	danger	danger	10.10.10.10		192.168.1.121	25	smtp	reset-both	high
05/04 19:06:22	vulnerability	Ransom-Win32.Jacky.pe	danger	danger	10.10.10.10		192.168.1.121	25	smtp	reset-both	high
05/04 19:06:10	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:05:51	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:05:30	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:05:21	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:05:00	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:04:50	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational
05/04 19:04:12	spyware	Suspicious TLS Evasion Found	inside	outside	192.168.1.20		142.250.68.78	443	google-base	alert	informational