

Vu Nguyen

UID: u1483046

Assignment 7 – PANEDU06 – URL Filtering (Lab and Quiz)

1. Section 1.3, Step 6

The screenshot shows the Palo Alto Networks firewall logs for the rule 'egress-outside-ur'. The logs display several entries where access to news sites was denied. The table below summarizes the log entries:

Receive Time	URL Category	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 22:20:22	news-sites	deny	inside	outside	192.168.1.20		151.101.0.81	80	web-browsing	reset both	egress-outside-ur	threat	496	0
02/02 22:20:22	news-sites	deny	inside	outside	192.168.1.20		151.101.0.81	80	web-browsing	reset both	egress-outside-ur	policy-deny	496	0
02/02 22:20:08	news-sites	deny	inside	outside	192.168.1.20		23.61.209.108	80	web-browsing	reset both	egress-outside-ur	threat	620	0
02/02 22:20:08	news-sites	deny	inside	outside	192.168.1.20		23.61.209.108	80	web-browsing	reset both	egress-outside-ur	policy-deny	500	0
02/02 22:20:02	news-sites	deny	inside	outside	192.168.1.20		23.48.184.236	80	web-browsing	reset both	egress-outside-ur	threat	618	0
02/02 22:20:02	news-sites	deny	inside	outside	192.168.1.20		23.48.184.236	80	web-browsing	reset both	egress-outside-ur	policy-deny	496	0

2. Section 1.5, Step 3

The screenshot shows a web browser window displaying a 'Web Page Blocked' message. The message states: 'Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.' The user is 192.168.1.20, the URL is avsforum.com/, and the category is url-block-list. A smaller inset window shows a similar message for the URL gizmodo.com/.

3. 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 3 > Reservation 69135 > Lab 06: URL Filtering

Topology Content Status Client Firewall DMZ VRouter

firewall-a

192.168.1.254/?monitorcvsys1:monitor/logs/url

palalto

Dashboard AGG Monitor Policies Objects Network Device

Logs Traffic Threat URL Filtering Wildfire Submissions Data Filtering HDP Match In-Tap 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 PDF Reports Manage PDF Summary User Activity Report

Receive Time	Category	URL Category List	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action	Headers Inserted	HTTP2 Connection Session ID
02/02 22:28:27	url-block-list	url-block-list-not-resolved	gismoto.com/	inside	outside	192.168.1.20		151.101.2.166	web-browsing	block-url		0
02/02 22:28:27	url-block-list	url-block-list-not-resolved	gismoto.com/	inside	outside	192.168.1.20		151.101.2.166	web-browsing	block-url		0
02/02 22:28:16	url-block-list	url-block-list-not-resolved	overforum.com/	inside	outside	192.168.1.20		151.101.1.91	web-browsing	block-url		0
02/02 22:28:16	url-block-list	url-block-list-not-resolved	overforum.com/	inside	outside	192.168.1.20		151.101.1.91	web-browsing	block-url		0
02/02 22:28:22	news-sites	news-sites-not-resolved	bbc.com/	inside	outside	192.168.1.20		151.101.0.81	web-browsing	block-url		0
02/02 22:28:22	news-sites	news-sites-not-resolved	bbc.com/	inside	outside	192.168.1.20		151.101.0.81	web-browsing	block-url		0
02/02 22:28:08	news-sites	news-sites-not-resolved	foxnews.com/	inside	outside	192.168.1.20		23.61.209.108	web-browsing	block-url		0
02/02 22:28:08	news-sites	news-sites-not-resolved	foxnews.com/	inside	outside	192.168.1.20		23.61.209.108	web-browsing	block-url		0
02/02 22:28:02	news-sites	news-sites-not-resolved	marbot.com/	inside	outside	192.168.1.20		23.46.194.236	web-browsing	block-url		0
02/02 22:28:02	news-sites	news-sites-not-resolved	marbot.com/	inside	outside	192.168.1.20		23.46.194.236	web-browsing	block-url		0

Displaying logs 1 - 10 per page

2/2/2024 22:29

4. Section 1.7, Step 12

David Eccles School of Business THE UNIVERSITY OF UTAH

Home Reservation u1483046@utah.edu

MyNETLAB > PAN 9 Firewall Essentials POD 3 > Reservation 69135 > Lab 06: URL Filtering

Topology Content Status Client Firewall DMZ VRouter

firewall-a

192.168.1.254/?policies:cvsys1:policies/security-rulebase

palalto

Dashboard AGG Monitor Policies Objects Network Device

Security NAT QoS Policy Based Forwarding Decryption Tunnel Inspection Application Override Authentication DDoS Protection Policy Optimizer Unused Apps Rule Usage Unused in 30 days Unused in 90 days Unused

Name	Tags	Type	Zone	Address	Source	Destination	Service	URL Category	Action	Profile	Options	Hit Count	Last H
1 internal-inside-dmz	internal	universal	any	any			application-d	any	Allow			21	2024-4
2 ingress-outside-uf	egress	universal	any	any			application-d	any	Allow			468	2024-4
3 ingress-outside	egress	universal	any	any			application-d	any	Allow			1022	2024-4
4 danger-simulated-tr	none	universal	any	any			application-d	any	Allow			0	-
5 intrazone-default	none	intrazone	any	any			any	any	Allow	none		17	2024-4
6 interzone-default	none	interzone	any	any			any	any	Deny	none		0	-

Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

Warnings

Close

Object: Addresses Add Delete Done Download Revert Enable Disable Move PDF/CSV Highlight Unused Rules Reset Rule Hit Counter View Rulebase as Groups Test Policy Match

2/2/2024 22:39

5. Section 1.9, Step 2

