PCNSE$^{\text{Q\&As}}$

Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.x

Pass Palo Alto Networks PCNSE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pcnse.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

To more easily reuse templates and template slacks , you can create term plate variables in place of firewall-specific and appliance-specific IP literals in your configurations.

Which one is the correct configuration?

A. @Panorama

B. #Pancrama

C. andPanorama

D. $Panorama

Correct Answer: D

Create a template and template stack using a variable name for an object. Variable names must start with the dollar sign ("$") symbol. For example, you could use $Panorama as a variable for the Panorama IP address that you want to configure on multiple managed firewalls and appliances https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/panorama- features/configuration-reusability-for-templates-and-template-stacks.html

QUESTION 2

An administrator needs to identify which NAT policy is being used for internet traffic.

From the GUI of the firewall, how can the administrator identify which NAT policy is in use for a traffic flow?

A. From the Monitor tab, click Traffic view and review the information in the detailed log view.

B. From the Monitor tab, click Traffic view, ensure that the Source or Destination NAT columns are included and review the information in the detailed log view.

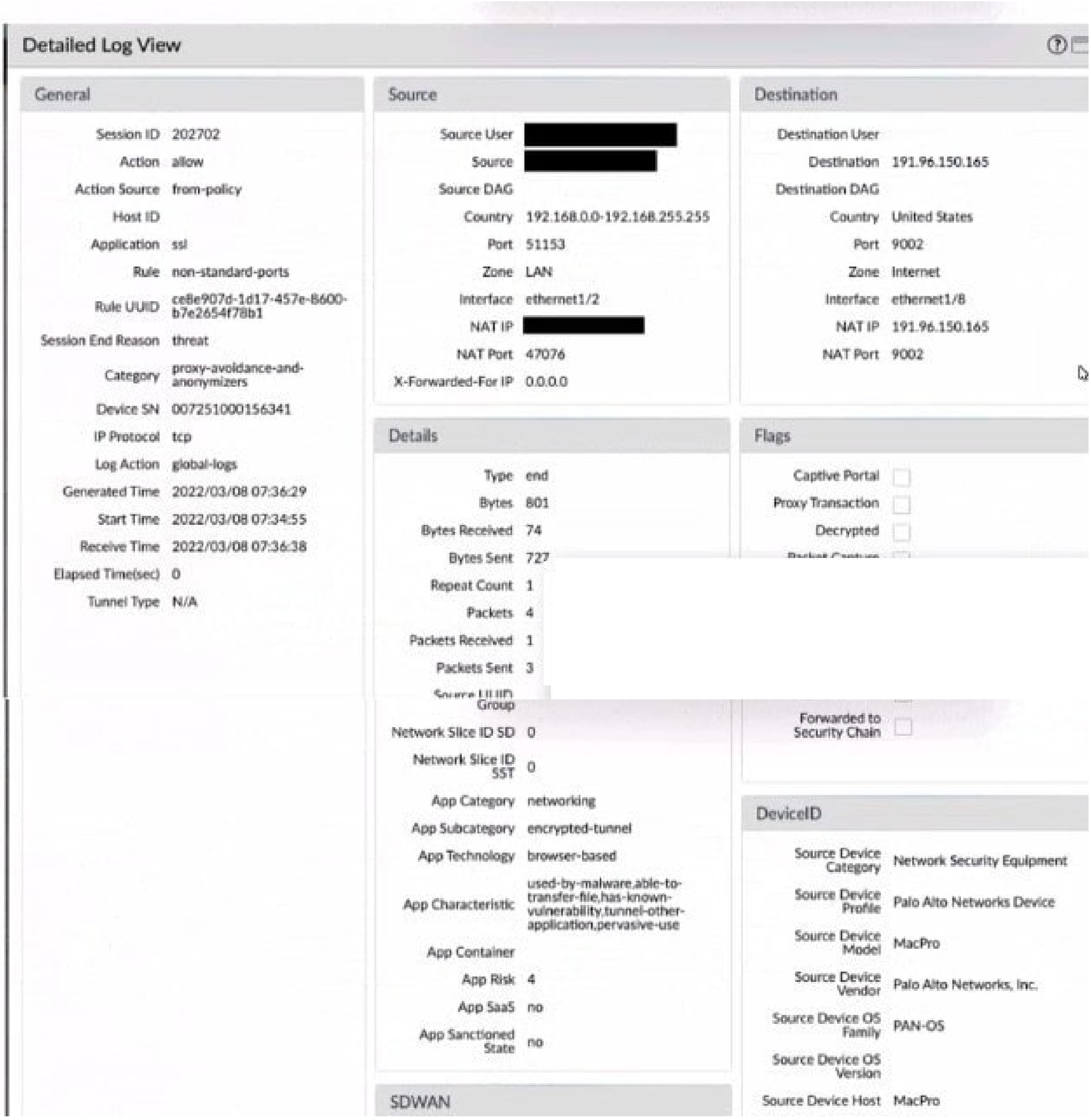
C. From the Monitor tab, click App Scope > Network Monitor and filter the report for NAT rules.

D. From the Monitor tab, click Session Browser and review the session details.

Correct Answer: D

QUESTION 3

Given the screenshot, how did the firewall handle the traffic?



Detailed Log View

General

Session ID	202702
Action	allow
Action Source	from-policy
Host ID	
Application	ssl
Rule	non-standard-ports
Rule UUID	ce8e907d-1d17-457e-8600-b7e2654f78b1
Session End Reason	threat
Category	proxy-avoidance-and-anonymizers
Device SN	007251000156341
IP Protocol	tcp
Log Action	global-logs
Generated Time	2022/03/08 07:36:29
Start Time	2022/03/08 07:34:55
Receive Time	2022/03/08 07:36:38
Elapsed Time(sec)	0
Tunnel Type	N/A

Source

Source User	[redacted]
Source	[redacted]
Source DAG	
Country	192.168.0.0-192.168.255.255
Port	51153
Zone	LAN
Interface	ethernet1/2
NAT IP	[redacted]
NAT Port	47076
X-Forwarded-For IP	0.0.0.0

Destination

Destination User	
Destination	191.96.150.165
Destination DAG	
Country	United States
Port	9002
Zone	Internet
Interface	ethernet1/8
NAT IP	191.96.150.165
NAT Port	9002

Details

Type	end
Bytes	801
Bytes Received	74
Bytes Sent	727
Repeat Count	1
Packets	4
Packets Received	1
Packets Sent	3
Source UUID Group	
Network Slice ID SD	0
Network Slice ID SST	0
App Category	networking
App Subcategory	encrypted-tunnel
App Technology	browser-based
App Characteristic	used-by-malware,able-to-transfer-file,has-known-vulnerability,tunnel-other-application,pervasive-use
App Container	
App Risk	4
App SaaS	no
App Sanctioned State	no

SDWAN

Flags

Captive Portal	□
Proxy Transaction	□
Decrypted	□
Packet Capture	□
Forwarded to Security Chain	□

DeviceID

Source Device Category	Network Security Equipment
Source Device Profile	Palo Alto Networks Device
Source Device Model	MacPro
Source Device Vendor	Palo Alto Networks, Inc.
Source Device OS Family	PAN-OS
Source Device OS Version	
Source Device Host	MacPro

A. Traffic was allowed by policy but denied by profile as encrypted.

B. Traffic was allowed by policy but denied by profile as a threat.

C. Traffic was allowed by profile but denied by policy as a threat.

D. Traffic was allowed by policy but denied by profile as a nonstandard port.

Correct Answer: B

The screenshot shows the threat log which records the traffic that matches a threat signature or is blocked by a security profile. The log entry indicates that the traffic was allowed by the security policy rule "Allow-All" but was denied by the vulnerability protection profile "strict" as a threat. The threat name is "Microsoft Windows SMBv1 Multiple Vulnerabilities

(MS17-010: EternalBlue)" and the action is "reset-both" which means that the firewall reset both the client and server connections. References: : https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/threat-log-fields

QUESTION 4

A company has configured GlobalProtect to allow their users to work from home. A decrease in performance for remote workers has been reported during peak-use hours. Which two steps are likely to mitigate the issue? (Choose TWO)

A. Exclude video traffic

B. Enable decryption

C. Block traffic that is not work-related

D. Create a Tunnel Inspection policy

Correct Answer: AC

This is because excluding video traffic from being sent over the VPN will reduce the amount of bandwidth being used during peak hours, allowing more bandwidth to be available for other types of traffic. Blocking non-work related traffic will also reduce the amount of bandwidth being used, further freeing up bandwidth for work-related traffic. Enabling decryption and creating a Tunnel Inspection policy are not likely to mitigate the issue of decreased performance during peak-use hours, as they do not directly address the issue of limited bandwidth availability during these times.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP3ICAW

QUESTION 5

An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version. What is considered best practice for this scenario?

A. Perform the Panorama and firewall upgrades simultaneously

B. Upgrade the firewall first wait at least 24 hours and then upgrade the Panorama version

C. Upgrade Panorama to a version at or above the target firewall version

D. Export the device state perform the update, and then import the device state

Correct Answer: C

Latest PCNSE Dumps PCNSE Study Guide PCNSE Exam Questions