# Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1
Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?
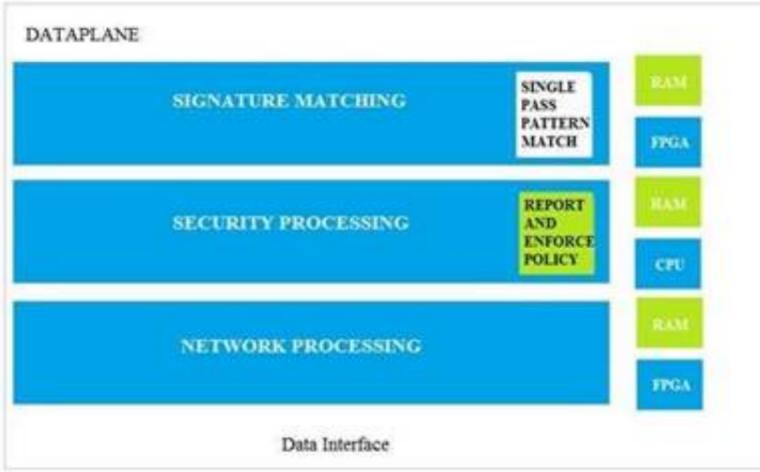
A. Signature Matching
B. Network Processing
C. Security Processing
D. Security Matching

Answer: A

NEW QUESTION 2
DRAG DROP
Match the Cyber-Attack Lifecycle stage to its correct description.
Select and Place:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 3
When creating a Source NAT policy, which entry in the Translated Packet tab will display the options Dynamic IP and Port, Dynamic, Static IP, and None?
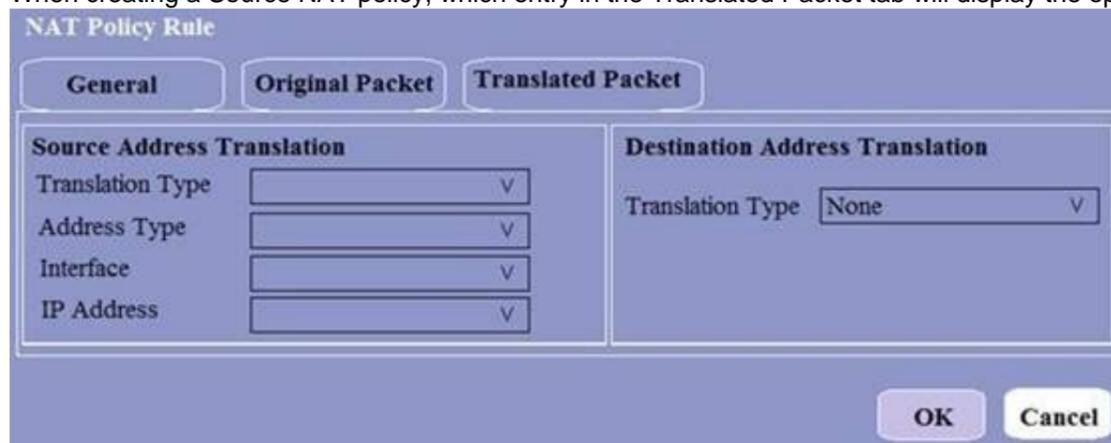
A. Translation Type
B. Interface
C. Address Type
D. IP Address

Answer: A

NEW QUESTION 4
A company moved its old port-based firewall to a new Palo Alto Networks NGFW 60 days ago. Which utility should the company use to identify out-of-date or unused rules on the firewall?

A. Rule Usage Filter > No App Specified
B. Rule Usage Filter >Hit Count > Unused in 30 days
C. Rule Usage Filter > Unused Apps
D. Rule Usage Filter > Hit Count > Unused in 90 days

Answer: D

NEW QUESTION 5
What are two differences between an implicit dependency and an explicit dependency in App- ID? (Choose two.)

A. An implicit dependency does not require the dependent application to be added in the security policy
B. An implicit dependency requires the dependent application to be added in the security policy
C. An explicit dependency does not require the dependent application to be added in the security policy
D. An explicit dependency requires the dependent application to be added in the security policy

Answer: AD

NEW QUESTION 6
Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping. What is the quickest way to reset the hit counter to zero in all the security policy rules?

A. At the CLI enter the command reset rules and press Enter
B. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule
C. Reboot the firewall
D. Use the Reset Rule Hit Counter > All Rules option

Answer: D

NEW QUESTION 7
Your company requires positive username attribution of every IP address used by wireless devices to support a new compliance requirement. You must collect IP –to-user mappings as soon as possible with minimal downtime and minimal configuration changes to the wireless devices themselves. The wireless devices are from various manufactures.
Given the scenario, choose the option for sending IP-to-user mappings to the NGFW.

A. syslog
B. RADIUS
C. UID redistribution
D. XFF headers

Answer: A

NEW QUESTION 8
An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated? (Choose two.)

A. vulnerability protection profile applied to outbound security policies
B. anti-spyware profile applied to outbound security policies
C. antivirus profile applied to outbound security policies

D. URL filtering profile applied to outbound security policies

Answer: BD

NEW QUESTION 9
In which stage of the Cyber-Attack Lifecycle would the attacker inject a PDF file within an email?

A. Weaponization
B. Reconnaissance
C. Installation
D. Command and Control
E. Exploitation

Answer: A

NEW QUESTION 10
Identify the correct order to configure the PAN-OS integrated USER-ID agent.
3. add the service account to monitor the server(s)
2. define the address of the servers to be monitored on the firewall
4. commit the configuration, and verify agent connection status
1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

A. 2-3-4-1
B. 1-4-3-2
C. 3-1-2-4
D. 1-3-2-4

Answer: D

NEW QUESTION 10
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?
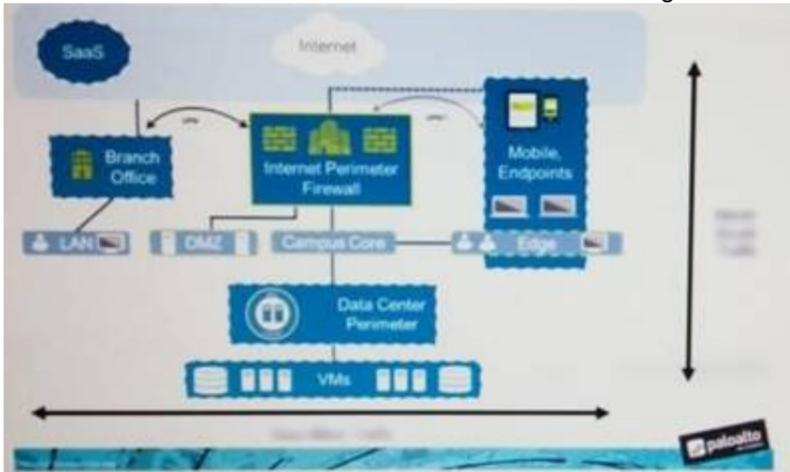
A. branch office traffic
B. north-south traffic
C. perimeter traffic
D. east-west traffic

Answer: D

NEW QUESTION 11
Given the topology, which zone type should zone A and zone B to be configured with?
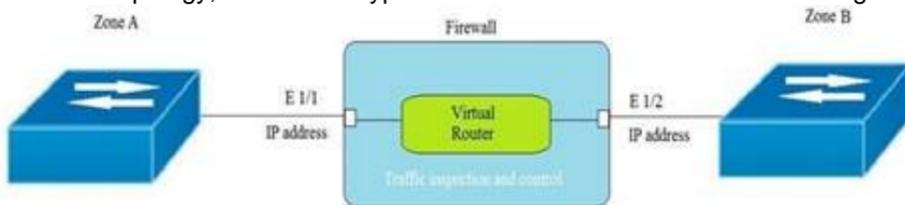
A. Layer3
B. Tap
C. Layer2
D. Virtual Wire

Answer: A

NEW QUESTION 13
Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

A. Root
B. Dynamic

C. Role-based
D. Superuser

Answer: C

NEW QUESTION 16
Which administrator type utilizes predefined roles for a local administrator account?

A. Superuser
B. Role-based
C. Dynamic
D. Device administrator

Answer: C

NEW QUESTION 21
What are three differences between security policies and security profiles? (Choose three.)

A. Security policies are attached to security profiles
B. Security profiles are attached to security policies
C. Security profiles should only be used on allowed traffic
D. Security profiles are used to block traffic by themselves
E. Security policies can block or allow traffic

Answer: BCE

NEW QUESTION 25

	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Rule Usage Hit Count	Rule Usage Last Hit	Rule Usage First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

Given the image, which two options are true about the Security policy rules. (Choose two.)

A. The Allow Office Programs rule is using an Application Filter
B. In the Allow FTP to web server rule, FTP is allowed using App-ID
C. The Allow Office Programs rule is using an Application Group
D. In the Allow Social Networking rule, allows all of Facebook's functions

Answer: BC

NEW QUESTION 27
Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?

A. global
B. intrazone
C. interzone
D. universal

Answer: D

NEW QUESTION 29
Which five Zero Trust concepts does a Palo Alto Networks firewall apply to achieve an integrated approach to prevent threats? (Choose five.)

A. User identification
B. Filtration protection
C. Vulnerability protection
D. Antivirus
E. Application identification
F. Anti-spyware

Answer: ACDEF

NEW QUESTION 34
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PCNSA Practice Exam Features:

* PCNSA Questions and Answers Updated Frequently

* PCNSA Practice Questions Verified by Expert Senior Certified Staff

* PCNSA Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PCNSA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The PCNSA Practice Test Here