Paloalto-Networks

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

NEW QUESTION 1
Which firewall plane provides configuration, logging, and reporting functions on a separate processor?

A. control
B. network processing
C. data
D. security processing

Answer: A

NEW QUESTION 2
Which option shows the attributes that are selectable when setting up application filters?

A. Category, Subcategory, Technology, and Characteristic
B. Category, Subcategory, Technology, Risk, and Characteristic
C. Name, Category, Technology, Risk, and Characteristic
D. Category, Subcategory, Risk, Standard Ports, and Technology

Answer: B

NEW QUESTION 3
Actions can be set for which two items in a URL filtering security profile? (Choose two.)

A. Block List
B. Custom URL Categories
C. PAN-DB URL Categories
D. Allow List

Answer: AD

NEW QUESTION 4
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

A. Windows session monitoring via a domain controller
B. passive server monitoring using the Windows-based agent
C. Captive Portal
D. passive server monitoring using a PAN-OS integrated User-ID agent

Answer: C

NEW QUESTION 5
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

A. Create an Application Filter and name it Office Programs, the filter it on the business-systems category, office-programs subcategory
B. Create an Application Group and add business-systems to it
C. Create an Application Filter and name it Office Programs, then filter it on the business-systems category
D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office

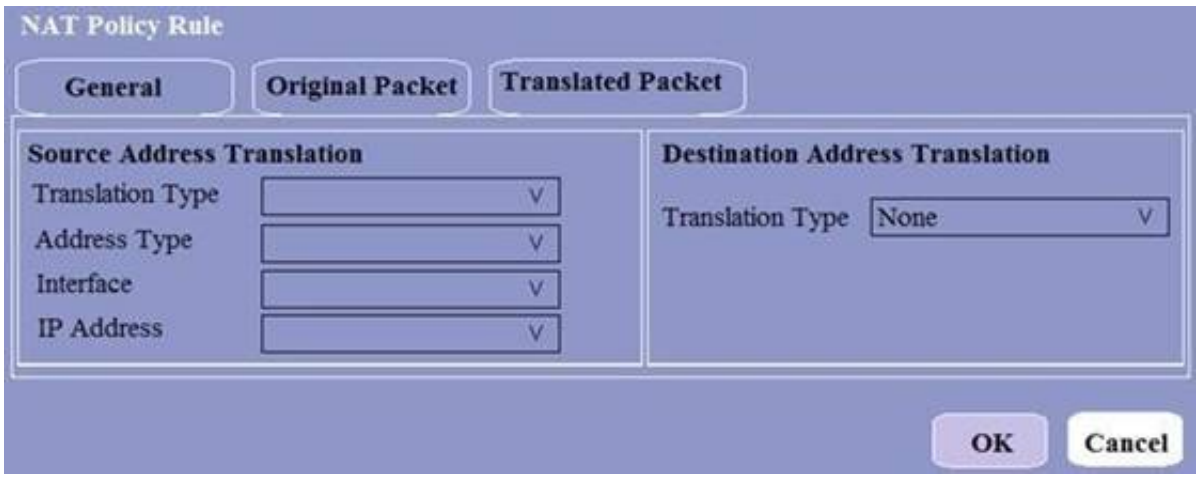
Answer: B

NEW QUESTION 6
Complete the statement. A security profile can block or allow traffic.

A. on unknown-tcp or unknown-udp traffic
B. after it is evaluated by a security policy that allows traffic
C. before it is evaluated by a security policy
D. after it is evaluated by a security policy that allows or blocks traffic

Answer: D

NEW QUESTION 7
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 8
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 9
Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?

A. Windows-based agent deployed on the internal network
B. PAN-OS integrated agent deployed on the internal network
C. Citrix terminal server deployed on the internal network
D. Windows-based agent deployed on each of the WAN Links

Answer: A

NEW QUESTION 10
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 10
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 11
Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone. Complete the security policy to ensure only Telnet is allowed.
Security Policy: Source Zone: Internal to DMZ Zone services “Application defaults”, and action = Allow

A. Destination IP: 192.168.1.123/24
B. Application = ‘Telnet’
C. Log Forwarding
D. USER-ID = ‘Allow users in Trusted’

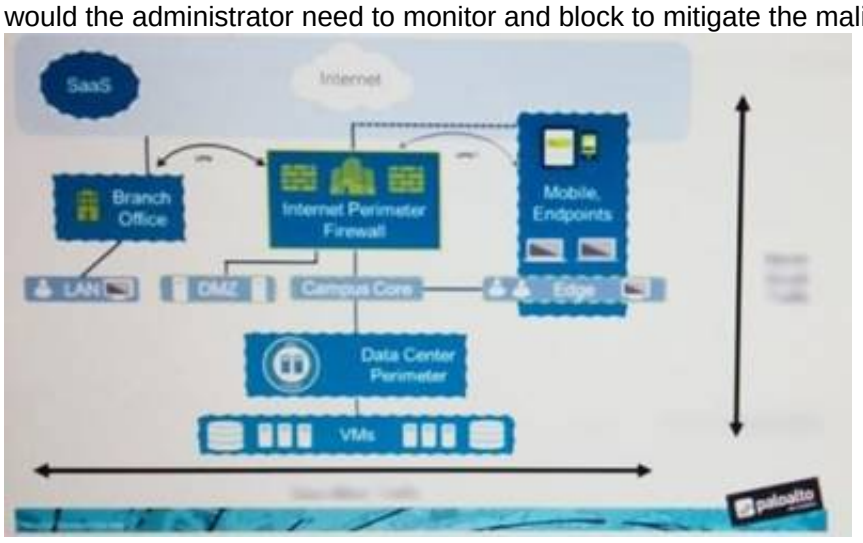
Answer: B

NEW QUESTION 13
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?

A. Threat Prevention License
B. Threat Implementation License
C. Threat Environment License
D. Threat Protection License

Answer: A

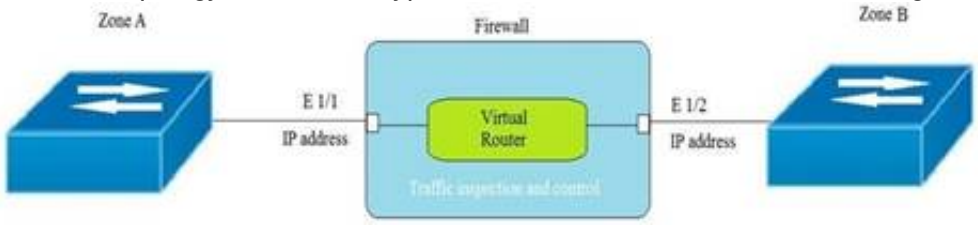
NEW QUESTION 15
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



A. branch office traffic
B. north-south traffic
C. perimeter traffic
D. east-west traffic

Answer: D

NEW QUESTION 17
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 20
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 22
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 26
Which two security profile types can be attached to a security policy? (Choose two.)

A. antivirus
B. DDoS protection
C. threat
D. vulnerability

Answer: AD

NEW QUESTION 30
The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.
Which security profile feature could have been used to prevent the communication with the CnC server?

A. Create an anti-spyware profile and enable DNS Sinkhole
B. Create an antivirus profile and enable DNS Sinkhole
C. Create a URL filtering profile and block the DNS Sinkhole category
D. Create a security policy and enable DNS Sinkhole

Answer: A

NEW QUESTION 34
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 36
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 37
Which file is used to save the running configuration with a Palo Alto Networks firewall?

A. running-config.xml
B. run-config.xml
C. running-configuration.xml
D. run-configuratin.xml

Answer: A

NEW QUESTION 39
.....

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