

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

<https://www.2passeasy.com/dumps/PCNSA/>



NEW QUESTION 1

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 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

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 4

Employees are shown an application block page when they try to access YouTube. Which security policy is blocking the YouTube application?

- A. intrazone-default
- B. Deny Google
- C. allowed-security services
- D. interzone-default

Answer: D

NEW QUESTION 5

Which interface does not require a MAC or IP address?

- A. Virtual Wire
- B. Layer3
- C. Layer2
- D. Loopback

Answer: A

NEW QUESTION 6

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 7

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 8

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 9

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 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 10

To use Active Directory to authenticate administrators, which server profile is required in the authentication profile?

- A. domain controller
- B. TACACS+
- C. LDAP
- D. RADIUS

Answer: C

NEW QUESTION 11

Which interface type is used to monitor traffic and cannot be used to perform traffic shaping?

- A. Layer 2
- B. Tap
- C. Layer 3
- D. Virtual Wire

Answer: B

NEW QUESTION 16

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 18

Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?

- A. Active Directory monitoring
- B. Windows session monitoring
- C. Windows client probing
- D. domain controller monitoring

Answer: A

NEW QUESTION 19

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 23

Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

- A. GlobalProtect
- B. AutoFocus
- C. Aperture
- D. Panorama

Answer: CD

Explanation:

44. Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)

- A. Path monitoring does not determine if route is useable
- B. Route with highest metric is actively used
- C. Path monitoring determines if route is useable
- D. Route with lowest metric is actively used

NEW QUESTION 28

Given the Cyber-Attack Lifecycle diagram, identify the stage in which the attacker can initiate malicious code against a targeted machine.

- A. Exploitation
- B. Installation
- C. Reconnaissance
- D. Act on Objective

Answer: A

NEW QUESTION 33

Which two Palo Alto Networks security management tools provide a consolidated creation of policies, centralized management and centralized threat intelligence. (Choose two.)

- A. GlobalProtect
- B. Panorama
- C. Aperture
- D. AutoFocus

Answer: BD

NEW QUESTION 38

Which statement is true regarding a Prevention Posture Assessment?

- A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
- B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
- C. It provides a percentage of adoption for each assessment area
- D. It performs over 200 security checks on Panorama/firewall for the assessment

Answer: B

NEW QUESTION 40

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PCNSA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PCNSA Product From:

<https://www.2passeasy.com/dumps/PCNSA/>

Money Back Guarantee

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