

Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

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



NEW QUESTION 1

DRAG DROP

Match the Cyber-Attack Lifecycle stage to its correct description.

Select and Place:

Reconnaissance	Drag answer here	stage where the attacker has motivation for attacking a network to deface web property
Installation	Drag answer here	stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control	Drag answer here	stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective	Drag answer here	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reconnaissance	stage where the attacker scans for network vulnerabilities and services that can be exploited	stage where the attacker has motivation for attacking a network to deface web property
Installation	stage where the attacker will explore methods such as a root kit to establish persistence	stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network	stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective	stage where the attacker has motivation for attacking a network to deface web property	stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network

NEW QUESTION 2

Which statement is true regarding a Best Practice Assessment?

- A. The BPA tool can be run only on firewalls
- B. It provides a percentage of adoption for each assessment data
- C. The assessment, guided by an experienced sales engineer, helps determine the areas of greatest risk where you should focus prevention activities
- D. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture

Answer: B

NEW QUESTION 3

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

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

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

Answer: D

NEW QUESTION 4

Which interface does not require a MAC or IP address?

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

Answer: A

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

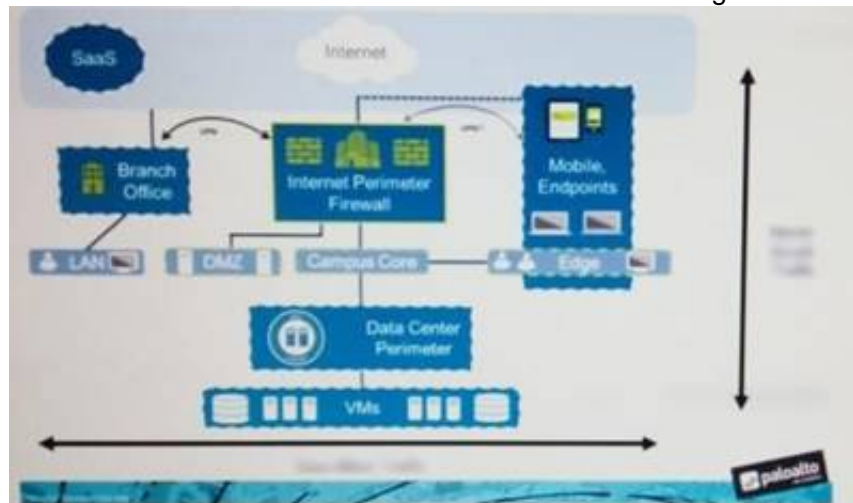
Users from the internal zone need to be allowed to Telnet into a server in the DMZ zone. Complete the security policy to ensure only Telnet is allowed.
 Security Policy: Source Zone: Internal to DMZ Zone services "Application defaults", and action = Allow

- 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 7

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?

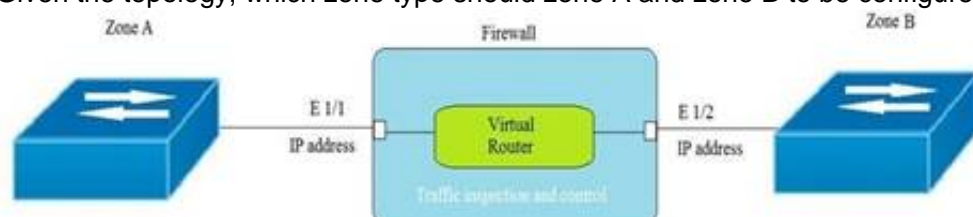


- A. branch office traffic
- B. north-south traffic
- C. perimeter traffic
- D. east-west traffic

Answer: D

NEW QUESTION 8

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 9

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 10

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 10

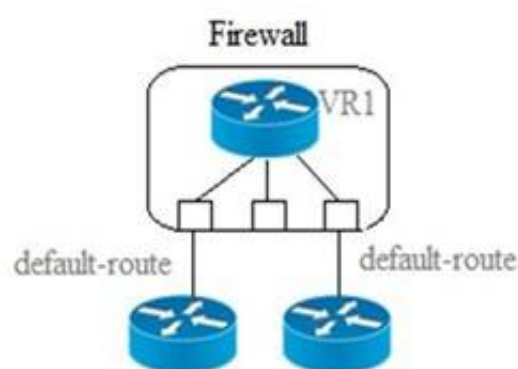
Which Palo Alto Networks firewall security platform provides network security for mobile endpoints by inspecting traffic deployed as internet gateways?

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

Answer: CD

Explanation:

Multiple Static Default Routes



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 12

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 17

In the example security policy shown, which two websites would be blocked? (Choose two.)

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

- A. LinkedIn
- B. Facebook
- C. YouTube
- D. Amazon

Answer: AB

NEW QUESTION 20

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 25

.....

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