



# **Paloalto-Networks**

## **Exam Questions PCNSA**

Palo Alto Networks Certified Network Security Administrator

**NEW QUESTION 1**

A security administrator has configured App-ID updates to be automatically downloaded and installed. The company is currently using an application identified by App-ID as SuperApp\_base. On a content update notice, Palo Alto Networks is adding new app signatures labeled SuperApp\_chat and SuperApp\_download, which will be deployed in 30 days. Based on the information, how is the SuperApp traffic affected after the 30 days have passed?

- A. All traffic matching the SuperApp\_chat, and SuperApp\_download is denied because it no longer matches the SuperApp-base application
- B. No impact because the apps were automatically downloaded and installed
- C. No impact because the firewall automatically adds the rules to the App-ID interface
- D. All traffic matching the SuperApp\_base, SuperApp\_chat, and SuperApp\_download is denied until the security administrator approves the applications

**Answer:** C

**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**

DRAG DROP

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

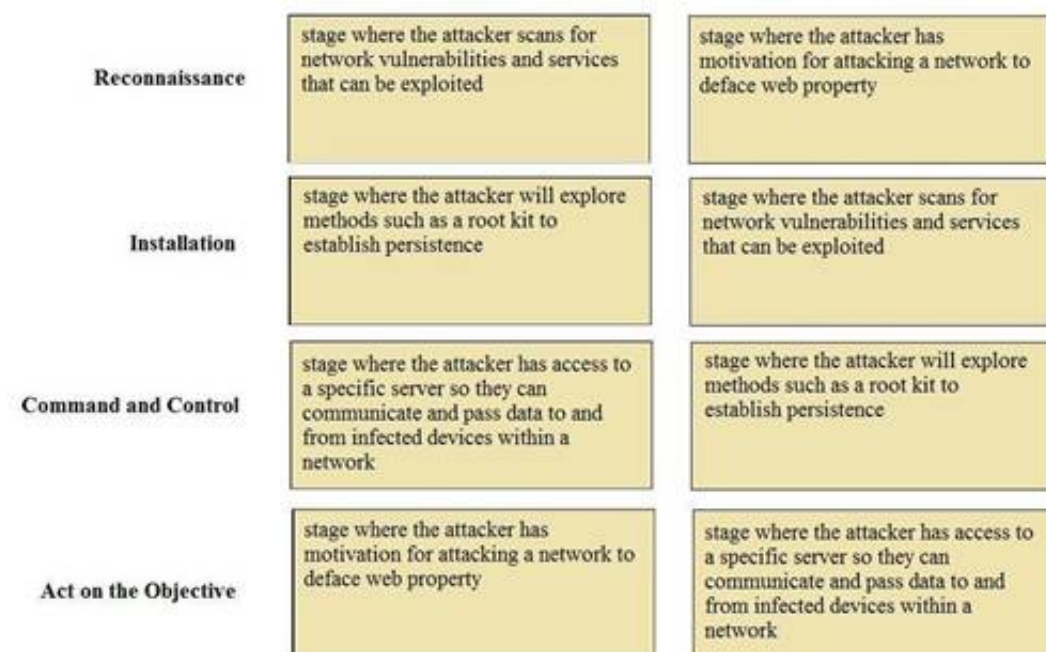
Select and Place:

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:**



#### NEW QUESTION 5

Which two statements are correct about App-ID content updates? (Choose two.)

- A. Updated application content may change how security policy rules are enforced
- B. After an application content update, new applications must be manually classified prior to use
- C. Existing security policy rules are not affected by application content updates
- D. After an application content update, new applications are automatically identified and classified

**Answer:** CD

#### NEW QUESTION 6

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 7

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 8

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 9

Which interface does not require a MAC or IP address?

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

**Answer:** A

#### NEW QUESTION 10

Which two App-ID applications will need to be allowed to use Facebook- chat? (Choose two.)

- A. facebook

- B. facebook-chat
- C. facebook-base
- D. facebook-email

**Answer:** BC

#### NEW QUESTION 10

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 13

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 14

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 16

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.

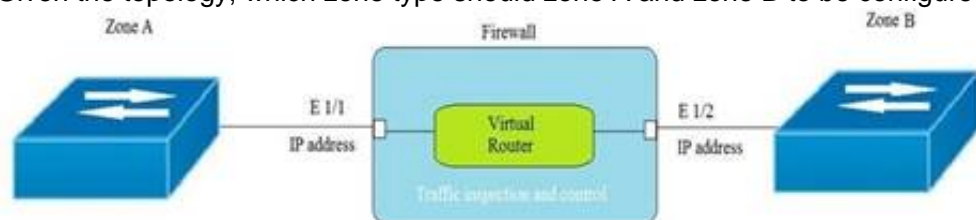
Security Policy: Source Zone: Internal to DMZ Zone services "Application defaults", and action = Allow

- 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 20

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 23

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 24

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

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 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

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 38

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 43

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 45

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 47

.....



## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**