

## Exam Questions PCNSA

Palo Alto Networks Certified Network Security Administrator

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



### NEW QUESTION 1

DRAG DROP

Match the Palo Alto Networks Security Operating Platform architecture to its description.

Select and Place:

Threat Intelligence Cloud	Drag answer here	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Drag answer here	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Drag answer here	Inspects processes and files to prevent known and unknown exploits.

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Threat Intelligence Cloud	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.	Identifies and inspects all traffic to block known threats.
Next-Generation Firewall	Identifies and inspects all traffic to block known threats.	Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Advanced Endpoint Protection	Inspects processes and files to prevent known and unknown exploits.	Inspects processes and files to prevent known and unknown exploits.

### NEW QUESTION 2

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 3

How many zones can an interface be assigned with a Palo Alto Networks firewall?

- A. two  
B. three  
C. four  
D. one

Answer: BC

Explanation:

Palo Alto Networks User-ID Agent Setup

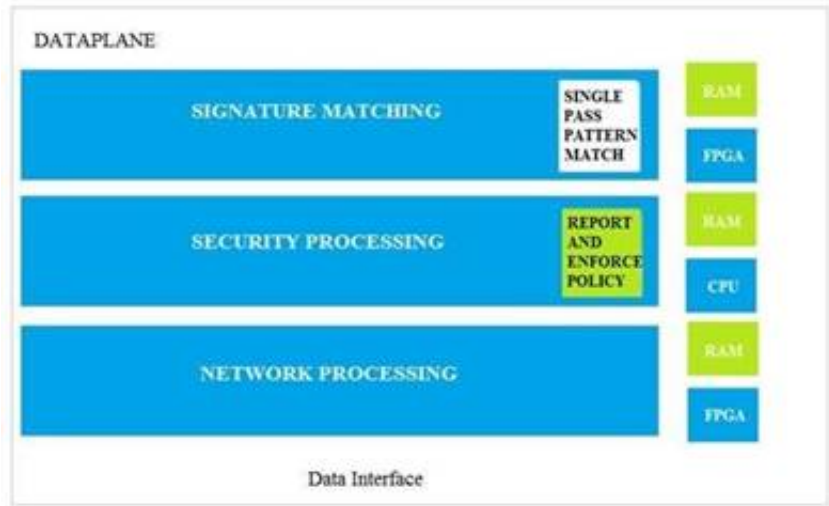
Enable Security Log ✓  
Server Log Monitor Frequency (sec) 15  
Enable Session ✓  
Server Session Read Frequency (sec) 10  
Novell eDirectory Query Interval (sec) 30  
Syslog Service Profile  
Enable Probing  
Probe Interval (min) 20  
Enable User Identification Timeout ✓  
User Identification Timeout (min) 45  
Allow matching usernames without domains  
Enable NTLM  
NTLM Domain  
User-ID Collector Name

5. Which two configuration settings shown are not the default? (Choose two.)

- A. Enable Security Log
- B. Server Log Monitor Frequency (sec)
- C. Enable Session
- D. Enable Probing

NEW QUESTION 4

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 5

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 6

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

	Name	Type	Source		Destination						
			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 7

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 8

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 9

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

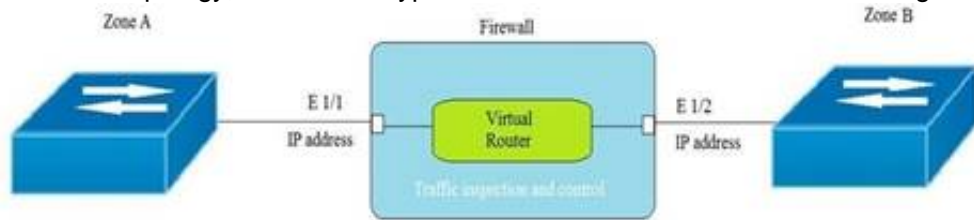
- A. Threat Prevention License
- B. Threat Implementation License
- C. Threat Environment License
- D. Threat Protection License

Answer: A

### NEW QUESTION 10



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 10

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 15

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 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 19

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 24

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 28**

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 33**

.....

## 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