

PCNSA Dumps

Palo Alto Networks Certified Network Security Administrator

<https://www.certleader.com/PCNSA-dumps.html>



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

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 3

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 4

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 5

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 6

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 7

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 8

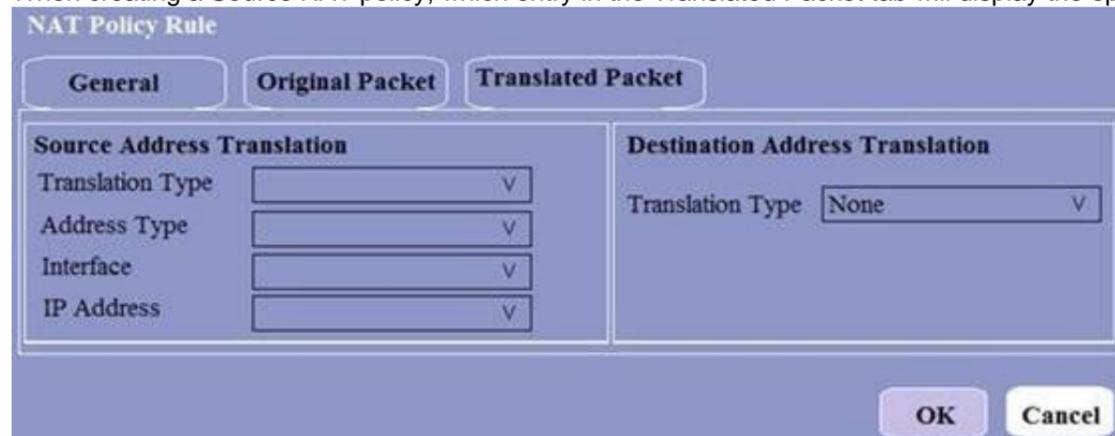
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

- 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 9

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 10

Which interface does not require a MAC or IP address?

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

Answer: A

NEW QUESTION 10

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 14

Based on the security policy rules shown, ssh will be allowed on which port?

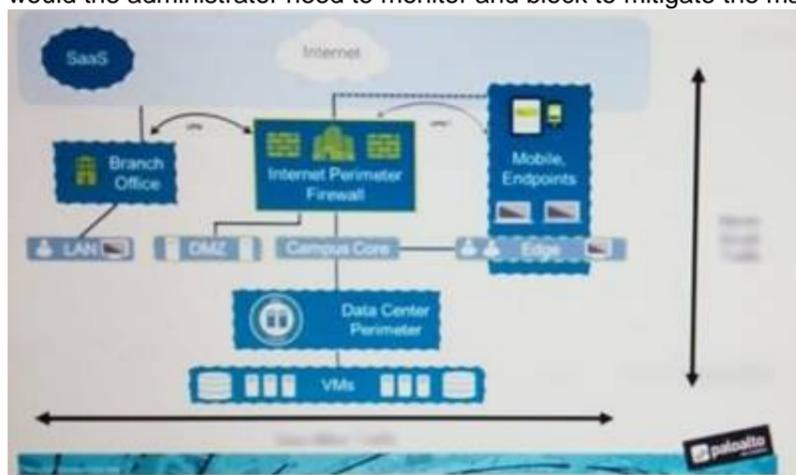
	Name	Type	Source		Destination		Application	Service	URL Category	Action	Profile
			Zone	Address	Zone	Address					
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	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. 80
- B. 53
- C. 22
- D. 23

Answer: C

NEW QUESTION 19

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?

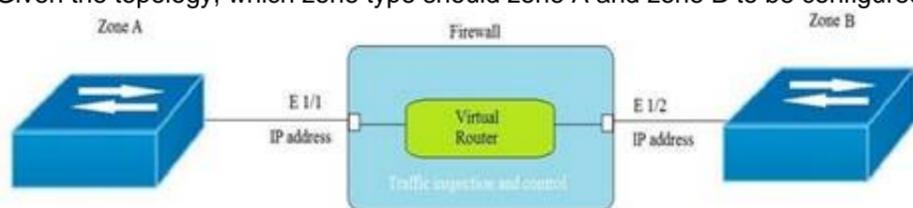


- A. branch office traffic
- B. north-south traffic
- C. perimeter traffic
- D. east-west traffic

Answer: D

NEW QUESTION 21

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 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

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 31

	Name	Tags	Type	Source			Destination		Rule Usage			Application	Service	Action	Profile	
				Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit					First Hit
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

Given the image, which two options are true about the Security policy rules. (Choose two.)

- A. The Allow Office Programs rule is using an Application Filter
- B. In the Allow FTP to web server rule, FTP is allowed using App-ID
- C. The Allow Office Programs rule is using an Application Group
- D. In the Allow Social Networking rule, allows all of Facebook's functions

Answer: BC

NEW QUESTION 34

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 35

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 37

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 40

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 42

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCNSA Exam with Our Prep Materials Via below:

<https://www.certleader.com/PCNSA-dumps.html>