PCNSA^{Q&As}

Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)

Pass Palo Alto Networks PCNSA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/pcnsa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which operations are allowed when working with App-ID application tags?

A. Predefined tags may be deleted.

B. Predefined tags may be augmented by custom tags.

C. Predefined tags may be modified.

D. Predefined tags may be updated by WildFire dynamic updates.

Correct Answer: B

QUESTION 2

Based on the screenshot presented which column contains the link that when clicked opens a window to display all applications matched to the policy rule?

No App Specified

These are security policies that have no application specified and allow any application on the configured service which can present a security risk. Palo Alto Networks you convert these service only security policies to application based policies.

Name	Service	Traffic (Bytes, 30 days)	App Usage			Compare	Modified
			Apps Allowed	Apps Seen	Days with No New Apps		
3 egress-outside	application-default	25.3G	any	8	8	Compare	2019-06-2...
1 inside-portal	any	372.6M	any	9	8	Compare	2019-06-2...

A. Apps Allowed

B. Name

C. Apps Seen

D. Service

Correct Answer: C

QUESTION 3

Which stage of the cyber-attack lifecycle makes it important to provide ongoing education to users on spear phishing links, unknown emails, and risky websites?

A. reconnaissance

B. delivery

C. exploitation

D. installation

Correct Answer: B

Weaponization and Delivery: Attackers will then determine which methods to use in order to deliver malicious payloads. Some of the methods they might utilize are automated tools, such as exploit kits, spear phishing attacks with malicious

links, or attachments and malvertizing.

Gain full visibility into all traffic, including SSL, and block high-risk applications. Extend those protections to remote and mobile devices. Protect against perimeter breaches by blocking malicious or risky websites through URL filtering. Block

known exploits, malware and inbound command-and-control communications using multiple threat prevention disciplines, including IPS, anti- malware, anti-CnC, DNS monitoring and sinkholing, and file and content blocking. Detect unknown

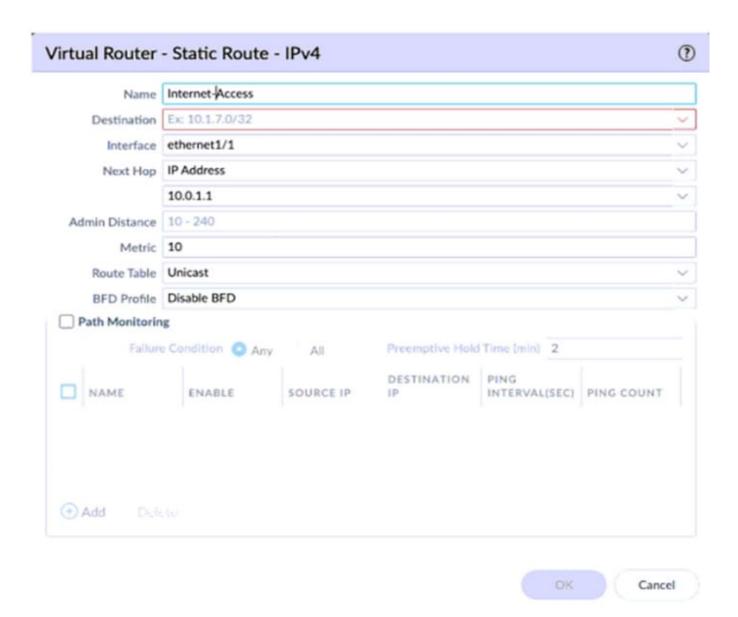malware and automatically deliver protections globally to thwart new attacks.

Provide ongoing education to users on spear phishing links, unknown emails, risky websites, etc.

https://www.paloaltonetworks.com/cyberpedia/how-to-break-the-cyber-attack-lifecycle

QUESTION 4

Ethernet 2/1 has an IP Address of 10.0 1 2 in Zone 'trust' (LAN).

If both interfaces are connected to the same virtual router, which IP address information will an administrator need to enter in the Destination field to access the internet?

Virtual Router - Static Route - IPv4 ⓘ

Name	Internet-Access
Destination	Ex: 10.1.7.0/32 ⌄
Interface	ethernet1/1 ⌄
Next Hop	IP Address ⌄
	10.0.1.1 ⌄
Admin Distance	10 - 240
Metric	10
Route Table	Unicast ⌄
BFD Profile	Disable BFD ⌄

☐ Path Monitoring

Failure Condition ⦿ Any   All   Preemptive Hold Time (min) 2

☐	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

⊕ Add   Delete

OK   Cancel

A. 0.0.0.0

B. 10.0.2.1/32

C. 10.0.1.254/32

D. 0.0.0.0/0

Correct Answer: D

QUESTION 5

Which three factors can be used to create malware based on domain generation algorithms? (Choose three.)

A. Time of day

B. URL custom categories

C. Other unique values

D. Cryptographic keys

E. IP address

Correct Answer: ACD

QUESTION 6

In which threat profile object would you configure the DNS Security service?

A. Antivirus

B. Anti-Spyware

C. WildFire

D. URL Filtering

Correct Answer: B

https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-dns-security#:~:text=To%20enable%20DNS%20Security%2C%20you,to%20a%20security%20policy%20rule.

QUESTION 7

An administrator is reviewing the Security policy rules shown in the screenshot below. Which statement is correct about the information displayed?

A. Eleven rules use the "Infrastructure* tag.

B. The view Rulebase as Groups is checked.

C. There are seven Security policy rules on this firewall.

D. Highlight Unused Rules is checked.

Correct Answer: B

QUESTION 8

Which plane on a Palo Alto Networks Firewall provides configuration, logging, and reporting functions on a separate processor?

A. data

B. network processing

C. management

D. security processing

Correct Answer: C

QUESTION 9

Which statement best describes a common use of Policy Optimizer?

A. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.

B. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.

C. Policy Optimizer can display which Security policies have not been used in the last 90 days.

D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists. Admins can then manually enable policies they want to keep and delete ones they want to remove.

Correct Answer: C

QUESTION 10

Complete the statement. A security profile can block or allow traffic_____

A. on unknown-tcp or unknown-udp traffic

B. after it is matched by a security policy that allows traffic

C. before it is matched by a security policy

D. after it is matched by a security policy that allows or blocks traffic

Correct Answer: B

Security profiles are objects added to policy rules that are configured with an action of allow.

QUESTION 11

Which two protocols are available on a Palo Alto Networks Firewall Interface Management Profile? (Choose two.)

A. HTTPS

B. RDP

C. SCP

D. SSH

Correct Answer: AD

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/use-interface-management-profiles-to-restrict-access

---

QUESTION 12

Which type of administrative role must you assign to a firewall administrator account, if the account must include a custom set of firewall permissions?

A. SAML

B. Multi-Factor Authentication

C. Role-based

D. Dynamic

Correct Answer: C

Reference: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall- administration/manage-firewall-administrators/administrative-role-types.html

---

QUESTION 13

When an ethernet interface is configured with an IPv4 address, which type of zone is it a member of?

A. Layer 3

B. Virtual Wire

C. Tap

D. Tunnel

Correct Answer: A

QUESTION 14

You receive notification about new malware that infects hosts through malicious files transferred by FTP.

Which Security profile detects and protects your internal networks from this threat after you update your firewall\\'s threat signature database?

A. URL Filtering profile applied to inbound Security policy rules.

B. Data Filtering profile applied to outbound Security policy rules.

C. Antivirus profile applied to inbound Security policy rules.

D. Vulnerability Prote ction profile applied to outbound Security policy rules.

Correct Answer: C

Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

QUESTION 15

Which Security policy set should be used to ensure that a policy is applied first?

A. Local firewall policy

B. Shared pre-rulebase

C. Parent device-group pre-rulebase

D. Child device-group pre-rulebase

Correct Answer: B

[PCNSA PDF Dumps](#)   [PCNSA Practice Test](#)   [PCNSA Exam Questions](#)