

DUMPS ARENA

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

Palo Alto Networks PCNSA

Version Demo

Total Demo Questions: 15

Total Premium Questions: 286

Buy Premium PDF

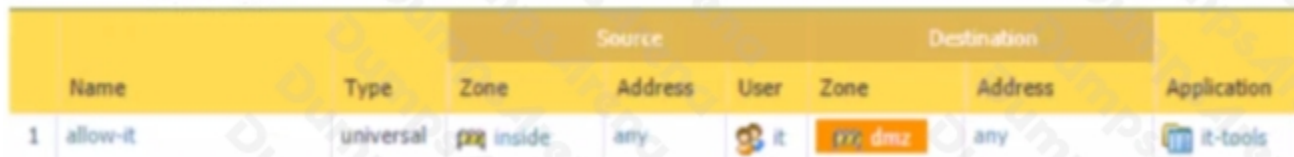
<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Based on the screenshot what is the purpose of the group in User labelled "it"?



	Name	Type	Source			Destination		Application
			Zone	Address	User	Zone	Address	
1	allow-it	universal	inside	any	it	dmz	any	it-tools

- A. Allows users to access IT applications on all ports
- B. Allows users in group "DMZ" to access IT applications
- C. Allows "any" users to access servers in the DMZ zone
- D. Allows users in group "it" to access IT applications

ANSWER: D

QUESTION NO: 2

An administrator is troubleshooting traffic that should match the interzone-default rule. However, the administrator doesn't see this traffic in the traffic logs on the firewall. The interzone-default was never changed from its default configuration.

Why doesn't the administrator see the traffic?

- A. Traffic is being denied on the interzone-default policy.
- B. The Log Forwarding profile is not configured on the policy.
- C. The interzone-default policy is disabled by default
- D. Logging on the interzone-default policy is disabled

ANSWER: D

QUESTION NO: 3

An administrator wishes to follow best practices for logging traffic that traverses the firewall

Which log setting is correct?

- A. Disable all logging
- B. Enable Log at Session End
- C. Enable Log at Session Start

D. Enable Log at both Session Start and End

ANSWER: B

Explanation:

Explanation

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clt5CAC>

QUESTION NO: 4

An administrator is configuring a NAT rule

At a minimum, which three forms of information are required? (Choose three.)

- A. name
- B. source zone
- C. destination interface
- D. destination address
- E. destination zone

ANSWER: B D E

QUESTION NO: 5

Which protocol used to map username to user groups when user-ID is configured?

- A. SAML
- B. RADIUS
- C. TACACS+
- D. LDAP

ANSWER: D

QUESTION NO: 6

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. pattern based application identification

- B. application override policy match
- C. session application identified
- D. application changed from content inspection

ANSWER: A B

Explanation:

Reference: <http://live.paloaltonetworks.com/t5/image/serverpage/image-id/12862i950F549C7D4E6309>

QUESTION NO: 7

What must be configured for the firewall to access multiple authentication profiles for external services to authenticate a non-local account?

- A. authentication sequence
- B. LDAP server profile
- C. authentication server list
- D. authentication list profile

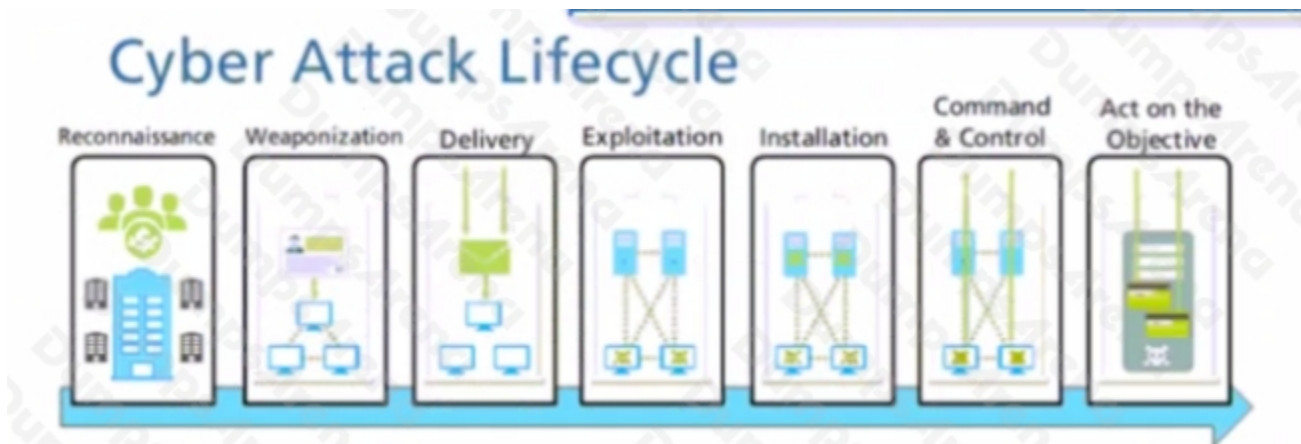
ANSWER: A

Explanation:

References:

QUESTION NO: 8

At which stage of the cyber-attack lifecycle would the attacker attach an infected PDF file to an email?



- A. delivery
- B. command and control
- C. exploitation
- D. reinsurance
- E. installation

ANSWER: A

QUESTION NO: 9

An administrator would like to block access to a web server, while also preserving resources and minimizing half-open sockets. What are two security policy actions the administrator can select? (Choose two.)

- A. Reset server
- B. Reset both
- C. Drop
- D. Deny

ANSWER: A C

QUESTION NO: 10

What are three factors that can be used in domain generation algorithms? (Choose three.)

- A. cryptographic keys
- B. time of day
- C. other unique values
- D. URL custom categories
- E. IP address

ANSWER: A B C

Explanation:

Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection>

QUESTION NO: 11

What are three Palo Alto Networks best practices when implementing the DNS Security Service? (Choose three.)

- A. Implement a threat intel program.
- B. Configure a URL Filtering profile.
- C. Train your staff to be security aware.
- D. Rely on a DNS resolver.
- E. Plan for mobile-employee risk

ANSWER: A B D

QUESTION NO: 12 - (DRAG DROP)

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.

ANSWER:

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.

Explanation:

QUESTION NO: 13

An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.

Which security policy action causes this?

- A. Reset server
- B. Reset both
- C. Deny
- D. Drop

ANSWER: C

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-configuration-backups/revert-firewall-configuration-changes.html>

QUESTION NO: 14

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

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

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

ANSWER: B C

Explanation:

References:

QUESTION NO: 15

What are two valid selections within an Antivirus profile? (Choose two.)

- A. deny
- B. drop
- C. default
- D. block-ip

ANSWER: B C