



*Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ---- Guaranteed.*



*PCNSA Dumps  
PCNSA Braindumps  
PCNSA Real Questions  
PCNSA Practice Test  
PCNSA Actual Questions*



**Palo-Alto**

**PCNSA**

*Palo Alto Networks Certified Network Security Administrator*



### Question: 80

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

### Question: 81

Which three types of authentication services can be used to authenticate user traffic flowing through the firewalls data plane? (Choose three )

- A. TACACS
- B. SAML2
- C. SAML10
- D. Kerberos
- E. TACACS+

**Answer:** A,B,D

### Question: 82

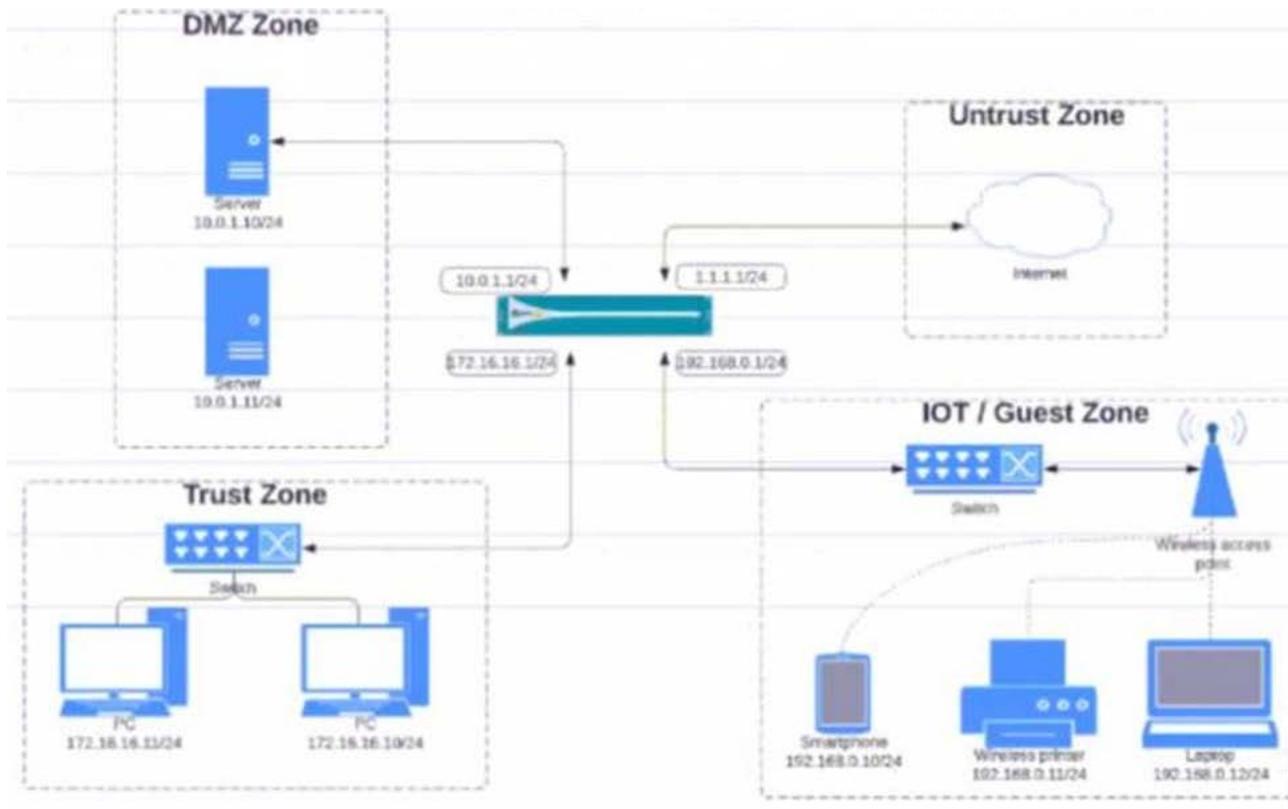
What do you configure if you want to set up a group of objects based on their ports alone?

- A. Application groups
- B. Service groups
- C. Address groups
- D. Custom objects

Answer: B

Question: 83

Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and DMZ servers using SSH, web-browsing and SSL applications.



Which policy achieves the desired results?

A)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
04-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

B)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
03-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	1.1.1.0/24
			Trust	192.168.0.0/24			Untrust	10.0.1.0/24

C)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
02-A	none	universal	IOT-Guest	172.16.18.0/24	any	any	DMZ	any
			Trust	192.168.0.0/24			Untrust	

D)

NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
01-A	none	universal	IOT-Guest	10.0.1.0/24	any	any	DMZ	1.1.1.0/24
			Trust	172.16.16.0/12			Untrust	192.168.0.0/24

- A. Option
- B. Option
- C. Option
- D. Option

Answer: C

Question: 84

Given the detailed log information above, what was the result of the firewall traffic inspection?

Device SN: 007251000154341 IP Protocol: udp Log Action: global-logs Generated Time: 2021/08/27 02:02:49 Receive Time: 2021/08/27 02:02:53 Serial Type: N/A	Interface: ethernet1/4 NAT IP: 67.290.64.58 NAT Port: 24351 X-Forwarded-For-IP: 0.0.0.0	NAT IP: 8.8.4.4 NAT Port: 53
<b>Details</b> Threat Type: spyware Threat ID/Name: Phishing:SSL:116.74in-addr:arpa ID: 108020001 (View in Threat Vault) Category: dns-ghosting Content Version: AppThreat:0-0 Severity: low Repeat Count: 2 File Name: URL: SSL:116.74in-addr:arpa Partial Hash: 0 Pcap ID: 0 Source UUID: Destination UUID: Dynamic User Group: Network Slice ID: 0 Network Slice ID SST: Network Slice ID SD: App Category: networking App Subcategory: infrastructure App Technology: network-protocol App Characteristic: used-by-malware-has-known-vulnerability-perceived-one App Container: App Risk: 3		<b>Flags</b> Captive Portal: <input type="checkbox"/> Proxy Transaction: <input type="checkbox"/> Decrypted: <input type="checkbox"/> Packet Capture: <input type="checkbox"/> Client to Server: <input checked="" type="checkbox"/> Server to Client: <input type="checkbox"/> Tunnel Inspected: <input type="checkbox"/>
<b>DeviceID</b> Source Device Category: Virtual Machine Source Device Profile: VMware Source Device Model: Source Device Vendor: VMware, Inc. Source Device OS Family: Source Device OS Version: Source Device Host: ubuntu-server Source Device MAC: 00:50:56:a2:19:63 Destination Device Category: Destination Device Profile: Destination Device Model:		

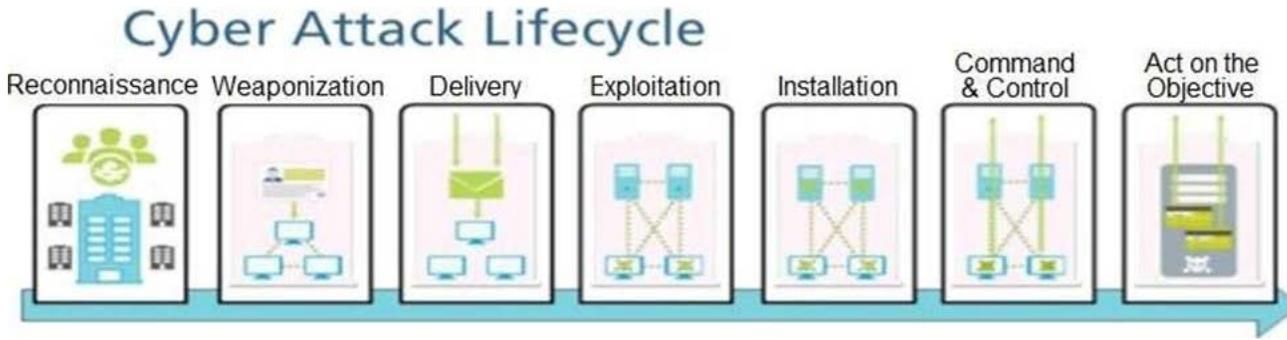
- A. It was blocked by the Vulnerability Protection profile action.
- B. It was blocked by the Anti-Virus Security profile action.
- C. It was blocked by the Anti-Spyware Profile action.

D. It was blocked by the Security policy action.

**Answer:** C

**Question:** 85

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

**Question:** 86

How are Application Filters or Application Groups used in firewall policy?

- A. An Application Filter is a static way of grouping applications and can be configured as a nested member of an Application Group
- B. An Application Filter is a dynamic way to group applications and can be configured as a nested member of an Application Group
- C. An Application Group is a dynamic way of grouping applications and can be configured as a nested member of an Application Group
- D. An Application Group is a static way of grouping applications and cannot be configured as a nested member of Application Group

**Answer:** B

**Question:** 87

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

**Answer: B**

Explanation:

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

**Question: 88**

Which interface does not require a MAC or IP address?

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

**Answer: A**

**Question: 89**

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: B,C**

**Question: 90**

Which administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact and command-and-control (C2) server.

Which security profile components will detect and prevent this threat after the firewall's signature database has been updated?

- A. antivirus profile applied to outbound security policies
- B. data filtering profile applied to inbound security policies
- C. data filtering profile applied to outbound security policies
- D. vulnerability profile applied to inbound security policies

**Answer: C**

**Question: 91**

Which statement is true about Panorama managed devices?

- A. Panorama automatically removes local configuration locks after a commit from Panorama
- B. Local configuration locks prohibit Security policy changes for a Panorama managed device
- C. Security policy rules configured on local firewalls always take precedence

D. Local configuration locks can be manually unlocked from Panorama

**Answer:** D

Explanation:

Reference: <https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/manage-locks-forrestricting-configuration-changes.html>

**Question: 92**

Which solution is a viable option to capture user identification when Active Directory is not in use?

- A. Cloud Identity Engine
- B. group mapping
- C. Directory Sync Service
- D. Authentication Portal

**Answer:** D

**Question: 93**

An internal host wants to connect to servers of the internet through using source NAT.

Which policy is required to enable source NAT on the firewall?

- A. NAT policy with source zone and destination zone specified
- B. post-NAT policy with external source and any destination address
- C. NAT policy with no source of destination zone selected
- D. pre-NAT policy with external source and any destination address

**Answer:** A

**Question: 94**

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:** B,C,E

**Question: 95**

What is a recommended consideration when deploying content updates to the firewall from Panorama?

- A. Before deploying content updates, always check content release version compatibility.

- B. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
- C. Content updates for firewall A/A HA pairs need a defined master device.
- D. After deploying content updates, perform a commit and push to Panorama.

**Answer: D**

Explanation:

Reference: <https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-licenses-and-updates/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/schedule-a-content-update-using-panorama.html>

**Question: 96**

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:

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

**Question: 97**

Which administrator type utilizes predefined roles for a local administrator account?

- A. Superuser
- B. Role-based
- C. Dynamic
- D. Device administrator

**Answer: C**

**Question: 98**

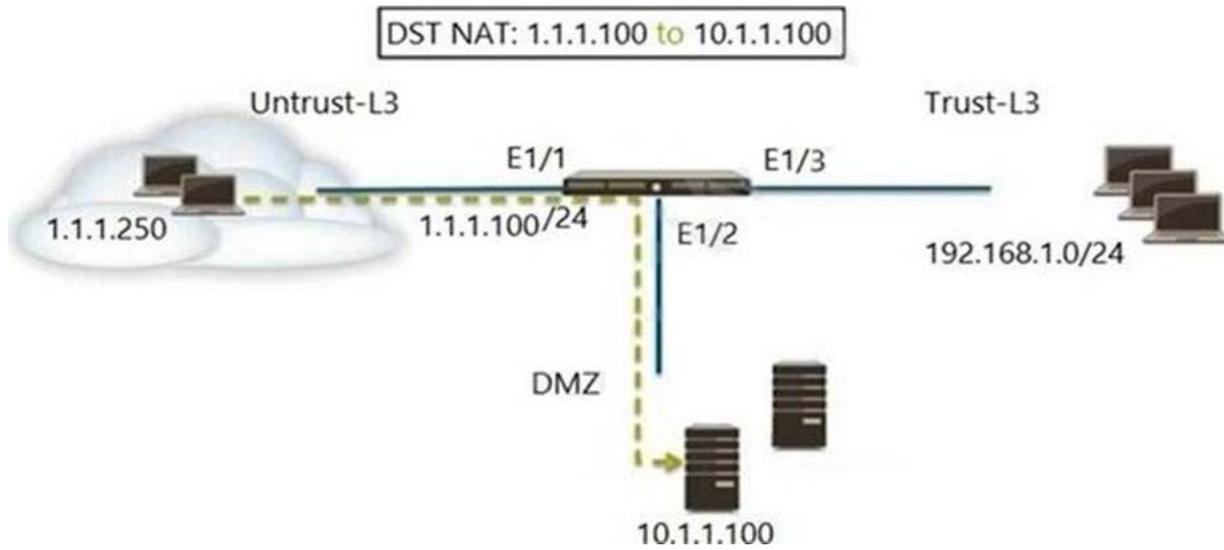
What are the requirements for using Palo Alto Networks EDL Hosting Service?

- A. any supported Palo Alto Networks firewall or Prisma Access firewall
- B. an additional subscription free of charge
- C. a firewall device running with a minimum version of PAN-OS 10.1
- D. an additional paid subscription

**Answer: A**

**Question: 99**

Refer to the exhibit.



A web server in the DMZ is being mapped to a public address through DNAT.

Which Security policy rule will allow traffic to flow to the web server?

- A. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow
- B. Untrust (any) to Untrust (1.1.1.100), web browsing – Allow
- C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow
- D. Untrust (any) to DMZ (1.1.1.100), web browsing – Allow

**Answer: D**

Explanation:

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping>



# SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version is up to date and contains actual questions and answers.***

*Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:*

**Actual Exam Questions:** *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

**Exam Dumps:** *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

**Practice Tests:** *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

**Guaranteed Success:** *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

**Updated Content:** *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

**Technical Support:** *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>  
*Kill your exam at First Attempt....Guaranteed!*