

➤ **Vendor: Palo Alto Networks**

➤ **Exam Code: PCNSA**

➤ **Exam Name: Palo Alto Networks Certified Network Security Administrator**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [November/2021](#))**

[Visit Braindump2go and Download Full Version PCNSA Exam Dumps](#)

QUESTION 196

Which tab would an administrator click to create an address object?

- A. Objects
- B. Monitor
- C. Device
- D. Policies

Answer: A

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-addresses>

QUESTION 197

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

Which log setting is correct?

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

Answer: D

Explanation:

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

QUESTION 198

Which two firewall components enable you to configure SYN flood protection thresholds? (Choose two.)

- A. QoS profile
- B. DoS Protection profile
- C. Zone Protection profile
- D. DoS Protection policy

Answer: BC

QUESTION 199

[PCNSA Exam Dumps](#) **[PCNSA Exam Questions](#)** **[PCNSA PDF Dumps](#)** **[PCNSA VCE Dumps](#)**

<https://www.braindump2go.com/pcnsa.html>

An administrator would like to see the traffic that matches the interzone-default rule in the traffic logs. What is the correct process to enable this logging?

- A. Select the interzone-default rule and click Override; on the Actions tab, select Log at Session End and click OK.
- B. Select the interzone-default rule and edit the rule; on the Actions tab, select Log at Session End and click OK.
- C. Select the interzone-default rule and edit the rule; on the Actions tab, select Log at Session Start and click OK.
- D. This rule has traffic logging enabled by default; no further action is required.

Answer: B

QUESTION 200

The Palo Alto Networks NGFW was configured with a single virtual router named VR-1. What changes are required on VR-1 to route traffic between two interfaces on the NGFW?

- A. Add static routes to route between the two interfaces
- B. Add interfaces to the virtual router
- C. Add zones attached to interfaces to the virtual router
- D. Enable the redistribution profile to redistribute connected routes

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/virtual-routers.html>

QUESTION 201

An administrator wants to prevent users from submitting corporate credentials in a phishing attack. Which Security profile should be applied?

- A. antivirus
- B. anti-spyware
- C. URL-filtering
- D. vulnerability protection

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention.html#idc77030dc-6022-4458-8c50-1dc0fe7cffe4>

QUESTION 202

Which two rule types allow the administrator to modify the destination zone? (Choose two.)

- A. interzone
- B. shadowed
- C. intrazone
- D. universal

Answer: A

QUESTION 203

What is the main function of Policy Optimizer?

- A. reduce load on the management plane by highlighting combinable security rules
- B. migrate other firewall vendors' security rules to Palo Alto Networks configuration

[PCNSA Exam Dumps](#) [PCNSA Exam Questions](#) [PCNSA PDF Dumps](#) [PCNSA VCE Dumps](#)

<https://www.braindump2go.com/pcnsa.html>

- C. eliminate "Log at Session Start" security rules
- D. convert port-based security rules to application-based security rules

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer.html>

QUESTION 204

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

	Name	Type	Source			Destination		Application	Service	Action
			Zone	Address	User	Zone	Address			
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

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

Answer: C

QUESTION 205

Which action results in the firewall blocking network traffic without notifying the sender?

- A. Drop
- B. Deny
- C. No notification
- D. Reset Client

Answer: A

QUESTION 206

Assume that traffic matches a Security policy rule but the attached Security Profiles is configured to block matching traffic.

Which statement accurately describes how the firewall will apply an action to matching traffic?

- A. If it is a block rule, then Security Profile action is applied last.
- B. If it is an allow rule, then the Security policy rule is applied last.
- C. If it is a block rule, then the Security policy rule action is applied last.
- D. If it is an allowed rule, then the Security Profile action is applied last.

Answer: D

QUESTION 207

Which Security profile can you apply to protect against malware such as worms and Trojans?

- A. antivirus
- B. data filtering
- C. vulnerability protection
- D. anti-spyware

Answer: A

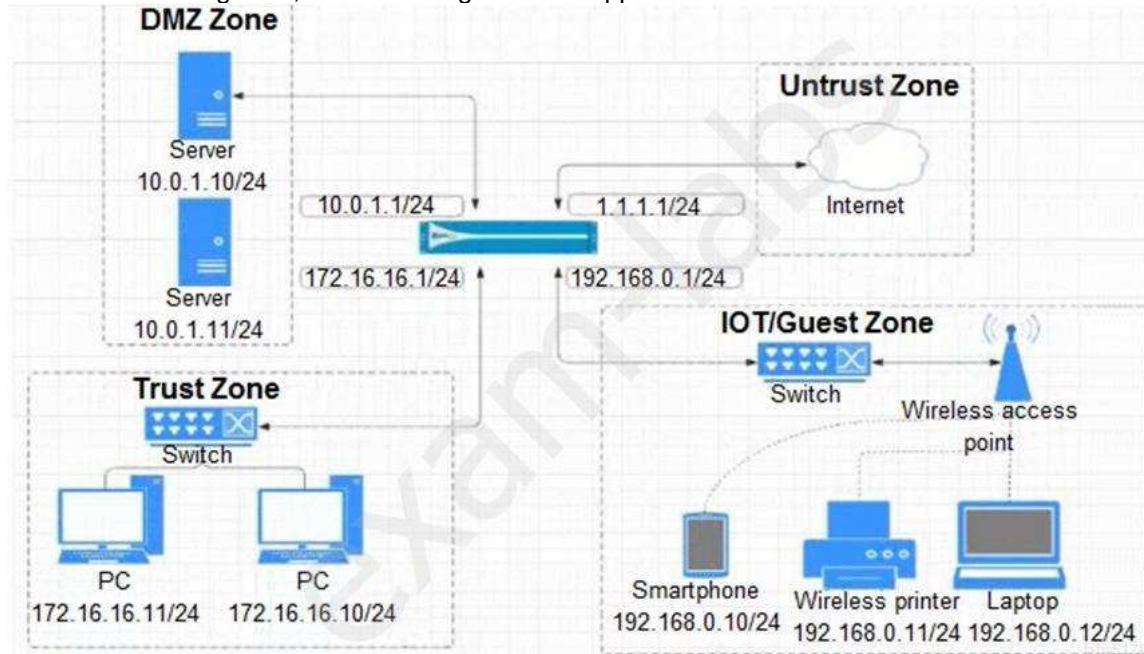
QUESTION 208

Given the network diagram, traffic should be permitted for both Trusted and Guest users to access general Internet and

[PCNSA Exam Dumps](#) [PCNSA Exam Questions](#) [PCNSA PDF Dumps](#) [PCNSA VCE Dumps](#)

<https://www.braindump2go.com/pcnsa.html>

DMZ servers using SSH, web-browsing and SSL applications.



Which policy achieves the desired results?

- A.
- | NAME | TAGS | TYPE | Source | | | | |
|------|------|-----------|--|--|------|--------|--|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE |
| 03-A | none | universal | <input checked="" type="checkbox"/> IOT-Guest
<input checked="" type="checkbox"/> Trust | <input checked="" type="checkbox"/> 172.16.16.0/24
<input checked="" type="checkbox"/> 192.168.0.0/24 | any | any | <input checked="" type="checkbox"/> DMZ
<input checked="" type="checkbox"/> Untrust |
- B.
- | NAME | TAGS | TYPE | Source | | | | |
|------|------|-----------|--|--|------|--------|--|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE |
| 04-A | none | universal | <input checked="" type="checkbox"/> IOT-Guest
<input checked="" type="checkbox"/> Trust | <input checked="" type="checkbox"/> 172.16.16.0/24
<input checked="" type="checkbox"/> 192.168.0.0/24 | any | any | <input checked="" type="checkbox"/> DMZ
<input checked="" type="checkbox"/> Untrust |
- C.
- | NAME | TAGS | TYPE | Source | | | | |
|------|------|-----------|--|---|------|--------|--|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE |
| 01-A | none | universal | <input checked="" type="checkbox"/> IOT-Guest
<input checked="" type="checkbox"/> Trust | <input checked="" type="checkbox"/> 10.0.1.0/24
<input checked="" type="checkbox"/> 172.16.16.0/12 | any | any | <input checked="" type="checkbox"/> DMZ
<input checked="" type="checkbox"/> Untrust |
- D.
- | NAME | TAGS | TYPE | Source | | | | |
|------|------|-----------|--|--|------|--------|--|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE |
| 02-A | none | universal | <input checked="" type="checkbox"/> IOT-Guest
<input checked="" type="checkbox"/> Trust | <input checked="" type="checkbox"/> 172.16.18.0/24
<input checked="" type="checkbox"/> 192.168.0.0/24 | any | any | <input checked="" type="checkbox"/> DMZ
<input checked="" type="checkbox"/> Untrust |

Answer: B

QUESTION 209

Which license is required to use the Palo Alto Networks built-in IP address EDLs?

- A. DNS Security
- B. Threat Prevention
- C. WildFire
- D. SD-Wan

Answer: B

QUESTION 210

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: A

Explanation:

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

QUESTION 211

A Security Profile can block or allow traffic at which point?

- A. on either the data plane or the management plane
- B. after it is matched to a Security policy rule that allows or blocks traffic
- C. after it is matched to a Security policy rule that allows traffic
- D. before it is matched to a Security policy rule

Answer: C

QUESTION 212

Which type of address object is "10.5.1.1/0.127.248.2"?

- A. IP netmask
- B. IP subnet
- C. IP wildcard mask
- D. IP range

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/use-address-object-to-represent-ip-addresses/create-an-address-object.html>

QUESTION 213

Which component is a building block in a Security policy rule?

- A. decryption profile
- B. destination interface

[PCNSA Exam Dumps](#) [PCNSA Exam Questions](#) [PCNSA PDF Dumps](#) [PCNSA VCE Dumps](#)

<https://www.braindump2go.com/pcnsa.html>

- C. timeout (min)
- D. application

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/building-blocks-in-a-security-policy-rule.html>

QUESTION 214

You have been tasked to configure access to a new web server located in the DMZ.

Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10.1.1.0/24 network to 192.168.1.0/24?



- A. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/2 with a next-hop of 172.16.1.2.
- B. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next-hop of 192.168.1.10
- C. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next-hop of 172.16.1.2.
- D. Add a route with the destination of 192.168.1.0/24 using interface Eth 1/3 with a next-hop of 192.168.1.254.

Answer: C

QUESTION 215

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

QUESTION 216

Selecting the option to revert firewall changes will replace what settings?

- A. the candidate configuration with settings from the running configuration
- B. dynamic update scheduler settings
- C. the running configuration with settings from the candidate configuration
- D. the device state with settings from another configuration

Answer: D

Explanation:

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

QUESTION 217

An administrator has configured a Security policy where the matching condition includes a single application, and the action is deny.

If the application's default deny action is reset-both, what action does the firewall take?

- A. It silently drops the traffic.
- B. It silently drops the traffic and sends an ICMP unreachable code.
- C. It sends a TCP reset to the server-side device.
- D. It sends a TCP reset to the client-side and server-side devices.

Answer: D

QUESTION 218

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

- A. SAML 2.0
- B. Kerberos
- C. TACACS
- D. TACACS+
- E. SAML 1.0

Answer: ABD

QUESTION 219

Which objects would be useful for combining several services that are often defined together?

- A. application filters
- B. service groups
- C. shared service objects
- D. application groups

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/objects/objects-services.html>