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.passapply.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

QUESTION 1

During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

A. check now

B. review policies

C. test policy match

D. download

Correct Answer: B

Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage- new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing-policy- rules

QUESTION 2

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 logging1?

A. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session Start 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

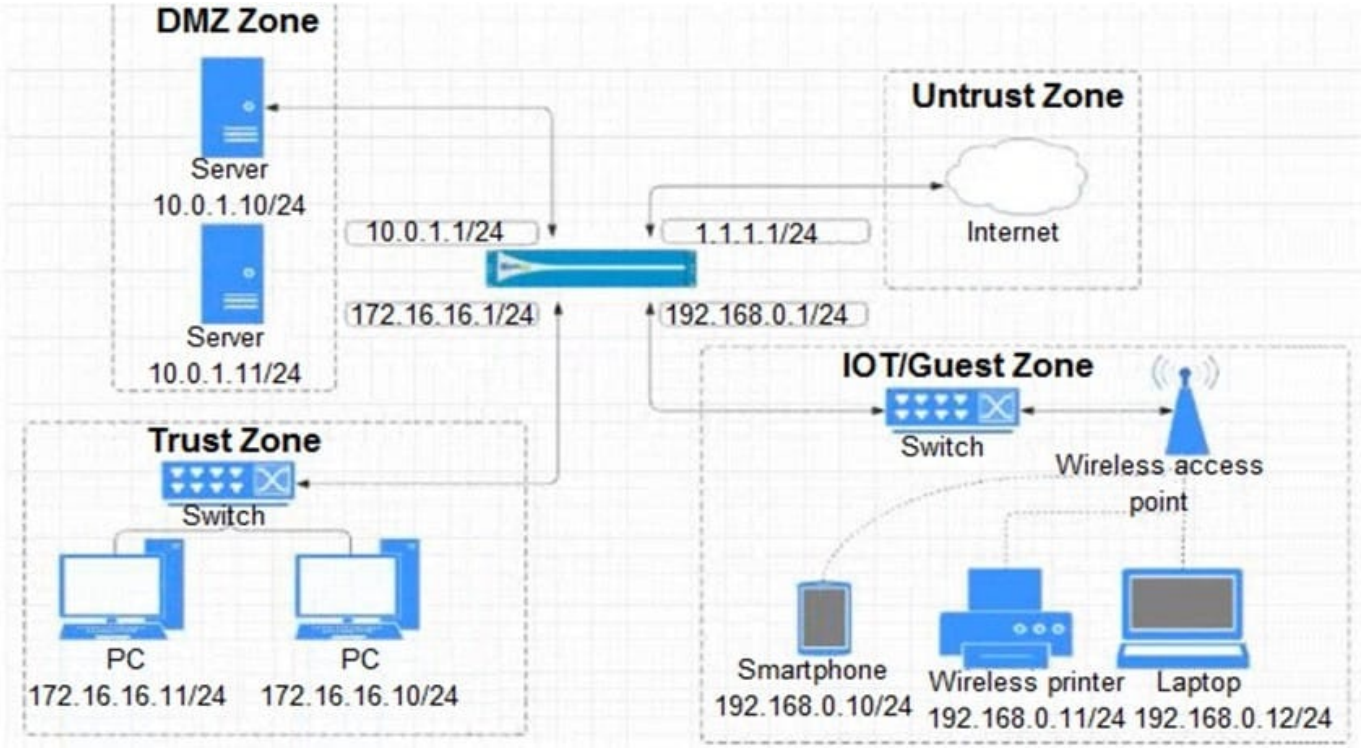
C. This rule has traffic logging enabled by default no further action is required

D. Select the interzone-default rule and click Override on the Actions tab select Log at Session End and click OK

Correct Answer: D

QUESTION 3

View the diagram.



What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?

A.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SI
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	ap de

B.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
04-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default

C.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE		
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	application-default

D.

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	application-default	any	Allow

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

A is incorrect - no internet access, DST addresses are too strictly definedd;

C is incorrect - SRC and DST addresses do not correspond to Zones;

D is incorrect - the SRC address does not match the SRC zone.

QUESTION 4

At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?

A. after clicking Check New in the Dynamic Update window

B. after connecting the firewall configuration

C. after downloading the update

D. after installing the update

Correct Answer: C

QUESTION 5

What is the purpose of the automated commit recovery feature?

A. It reverts the Panorama configuration.

B. It causes HA synchronization to occur automatically between the HA peers after a push from Panorama.

C. It reverts the firewall configuration if the firewall recognizes a loss of connectivity to Panorama after the change.

D. It generates a config log after the Panorama configuration successfully reverts to the last running configuration.

Correct Answer: C

Reference:https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer- panorama/enable-automated-commit-recovery.html

QUESTION 6

An administrator receives a notification about new malware that is being used to attack hosts. The malware exploits a software bug in a common application. Which Security Profile will detect and block access to this threat after the administrator updates the firewall\\'s threat signature database?

A. Vulnerability Profile applied to inbound Security policy rules

B. Antivirus Profile applied to outbound Security policy rules

C. Data Filtering Profile applied to outbound Security policy rules

D. Data Filtering Profile applied to inbound Security policy rules

Correct Answer: A

QUESTION 7

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\\'

Correct Answer: B

QUESTION 8

The administrator profile "SYS01 Admin" is configured with authentication profile "Authentication Sequence SYS01," and the authentication sequence SYS01 has a profile list with four authentication profiles:

Auth Profile LDAP Auth Profile Radius Auth Profile Local Auth Profile TACACS

After a network outage, the LDAP server is no longer reachable. The RADIUS server is still reachable but has lost the "SYS01 Admin" username and password.

What is the "SYS01 Admin" login capability after the outage?

A. Auth KO because RADIUS server lost user and password for SYS01 Admin

B. Auth OK because of the Auth Profile TACACS

C. Auth OK because of the Auth Profile Local

D. Auth KO because LDAP server is not reachable

Correct Answer: C

Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMdXCAW

QUESTION 9

Which information is included in device state other than the local configuration?

A. uncommitted changes

B. audit logs to provide information of administrative account changes

C. system logs to provide information of PAN-OS changes

D. device group and template settings pushed from Panorama

Correct Answer: D

Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface- help/device/device-setup-operations.html

QUESTION 10

The Net Sec Manager asked to create a new Firewall Operator profile with customized privileges.

In particular, the new firewall operator should be able to:

Check the configuration with read-only privilege for LDAP, RADIUS, TACACS+, and SAML as Server profiles to be used inside an Authentication profile.

The firewall operator should not be able to access anything else.

What is the right path m order to configure the new firewall Administrator Profile?

A. Device > Admin Roles > Add > Web UI > Device > Server Profiles Device > Admin Roles > Add > Web UI > disable access to everything else

B. Device > Admin Roles > Add > Web UI > Objects > Server Profiles Device > Admin Roles > Add > Web UI > disable access to everything else

C. Device > Admin Roles > Add >Web UI > Objects > Authentication Profile Device > Admin Roles > Add > Web UI > disable access to everything else

D. Device > Admin Roles > Add > Web UI > Device > Authentication Profile Device > Admin Roles > Add > Web UI > disable access to everything else

Correct Answer: A

QUESTION 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

Correct Answer: ACE

Based on the following source, BCE appear to be the best practices https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

QUESTION 12

When configuring a security policy, what is a best practice for User-ID?

A. Use only one method for mapping IP addresses to usernames.

B. Allow the User-ID agent in zones where agents are not monitoring services.

C. Limit User-ID to users registered in an Active Directory server.

D. Deny WMI traffic from the User-ID agent to any external zone.

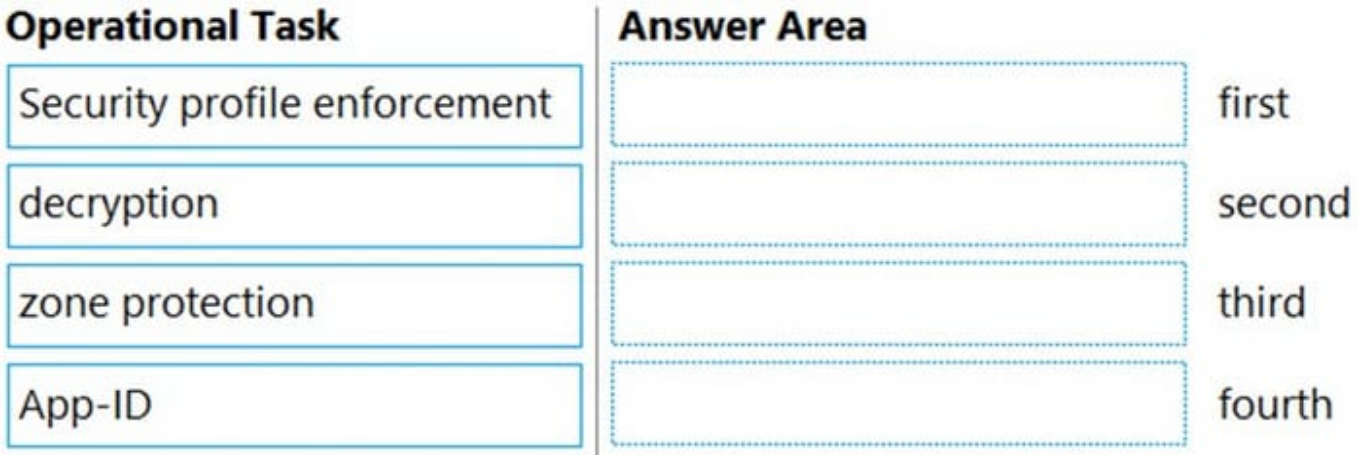
Correct Answer: D

QUESTION 13

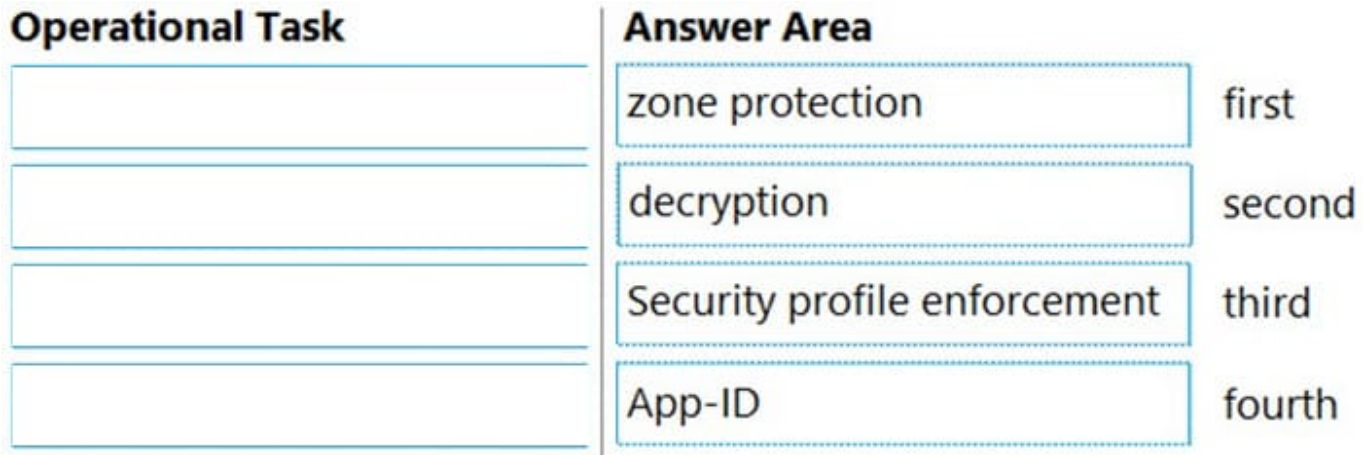
DRAG DROP

Place the steps in the correct packet-processing order of operations.

Select and Place:



Correct Answer:



Reference: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

QUESTION 14

Which two security profile types can be attached to a security policy? (Choose two.)

A. antivirus

B. DDoS protection

C. threat

D. vulnerability

Correct Answer: AD

QUESTION 15

When creating an address object, which option is available to select from the Type drop-down menu?

A. IPv6 Address

B. IP Netmask

C. IPv4 Address

D. IP Address Class

Correct Answer: B