Free Questions for PCNSA by vceexamstest

Shared by Long on 29-01-2024

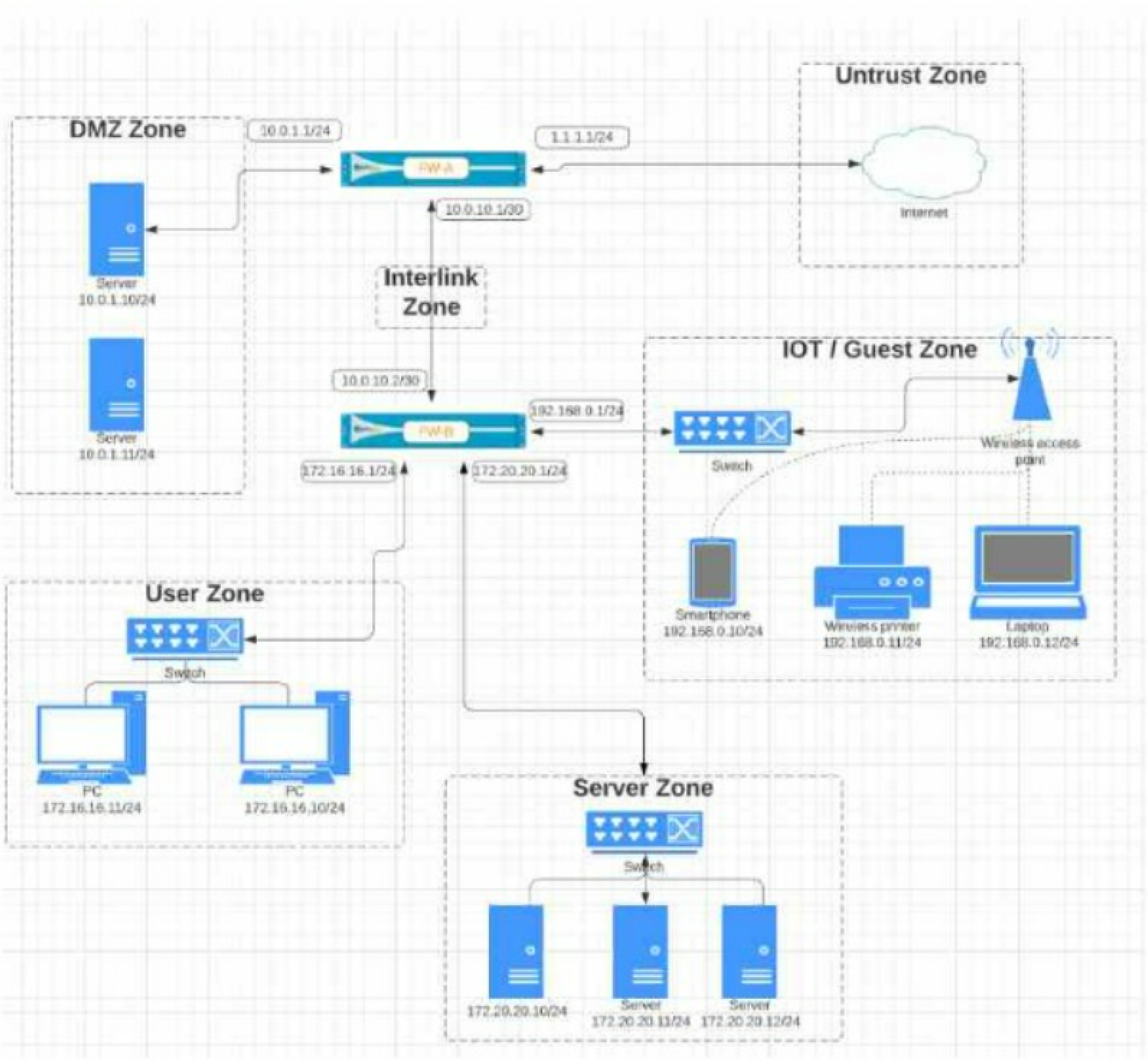
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Review the Screenshot:

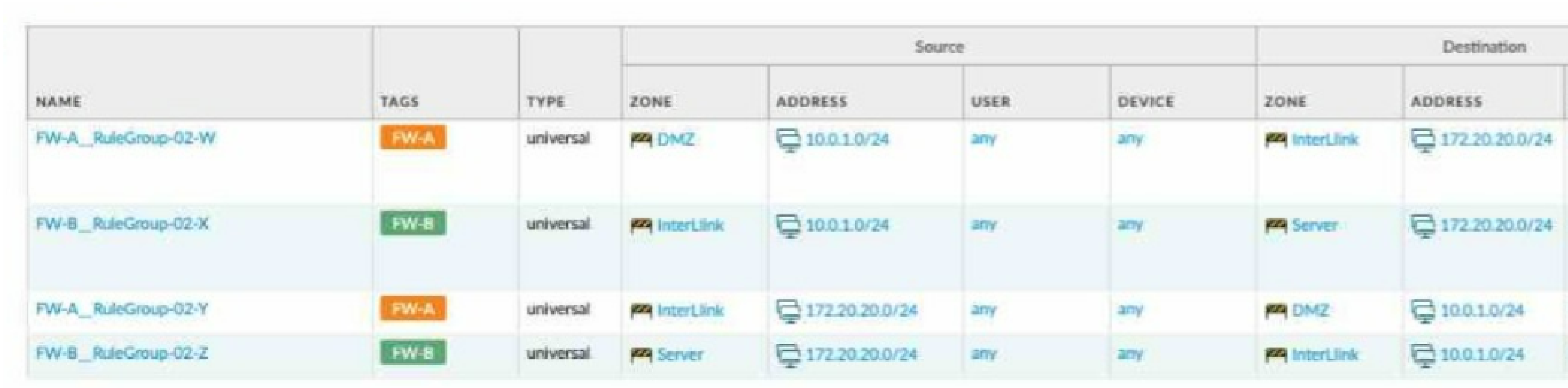

DMZ Zone
10.0.1.1/24
FW-A
1.1.1.1/24
Untrust Zone
Internet
10.0.10.1/30
Server
10.0.1.10/24
Interlink Zone
Server
10.0.1.11/24
IOT / Guest Zone
10.0.10.2/30
192.168.0.1/24
FW-B
Switch
Wireless access point
172.16.16.1/24
172.20.20.1/24
Smartphone
192.168.0.10/24
Wireless printer
192.168.0.11/24
Laptop
192.168.0.12/24
User Zone
Switch
PC
172.16.16.11/24
PC
172.16.16.10/24
Server Zone
Switch
172.20.20.10/24
Server
172.20.20.11/24
Server
172.20.20.12/24

Given the network diagram, traffic must be permitted for SSH and MYSQL from the DMZ to the SERVER zones, crossing two firewalls. In addition, traffic should be permitted from the

SERVER zone to the DMZ on SSH only.

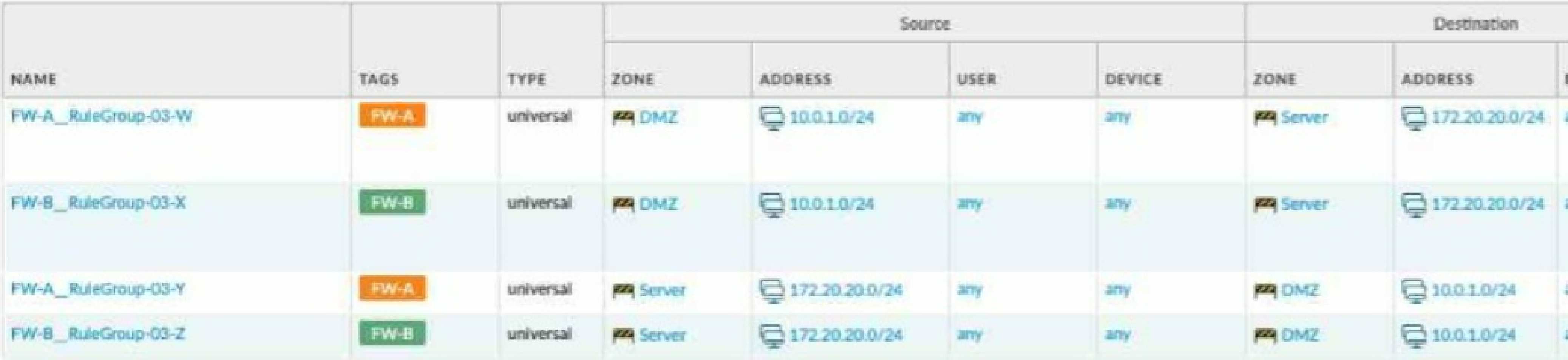
Which rule group enables the required traffic?

A)



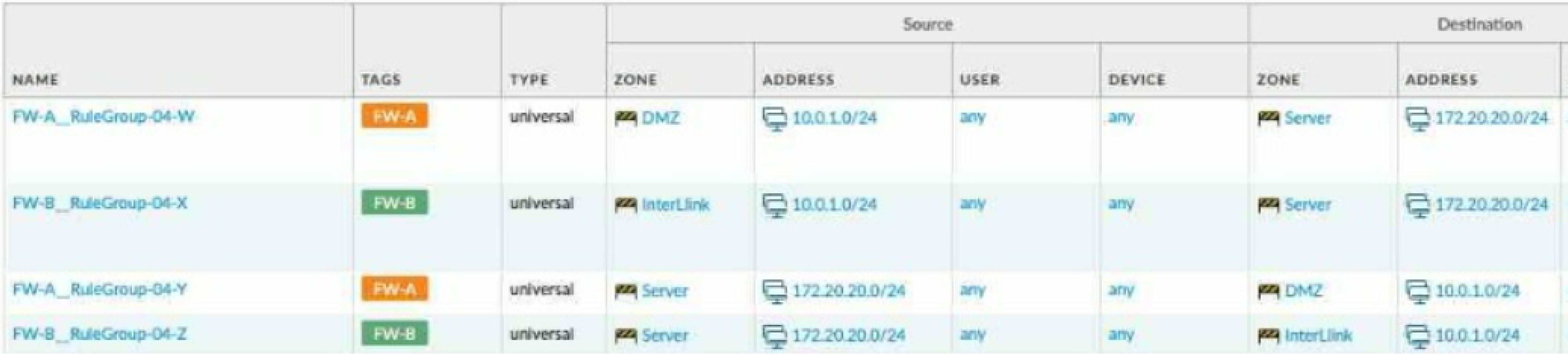
			Source				Destination	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
FW-A_RuleGroup-02-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	InterLlink	172.20.20.0/24
FW-B_RuleGroup-02-X	FW-B	universal	InterLlink	10.0.1.0/24	any	any	Server	172.20.20.0/24
FW-A_RuleGroup-02-Y	FW-A	universal	InterLlink	172.20.20.0/24	any	any	DMZ	10.0.1.0/24
FW-B_RuleGroup-02-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLlink	10.0.1.0/24

B)



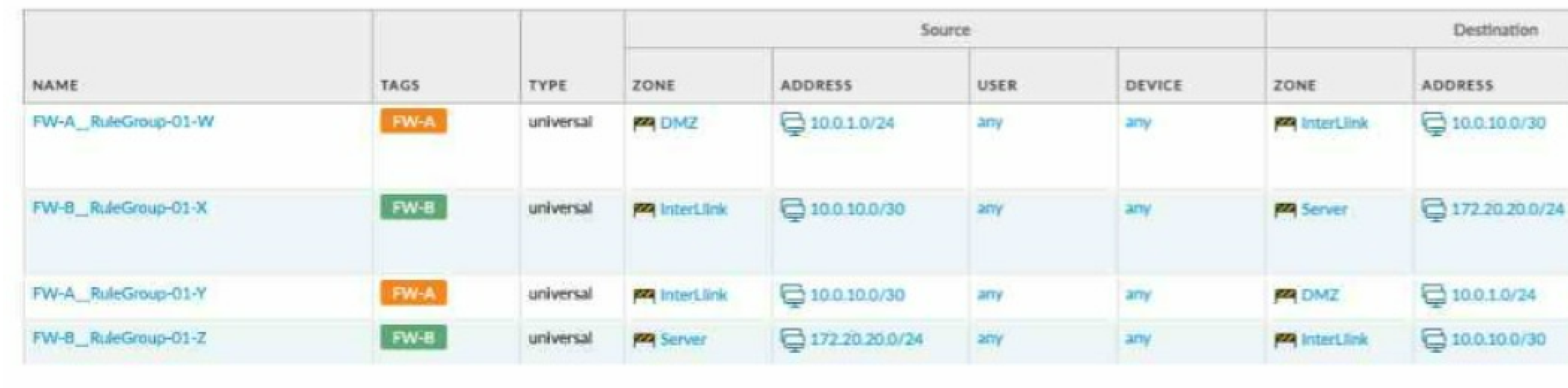
NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
FW-A_RuleGroup-03-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24
FW-B_RuleGroup-03-X	FW-B	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24
FW-A_RuleGroup-03-Y	FW-A	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24
FW-B_RuleGroup-03-Z	FW-B	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24

C)



NAME	TAGS	TYPE	Source				Destination	
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
FW-A_RuleGroup-04-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	Server	172.20.20.0/24
FW-B_RuleGroup-04-X	FW-B	universal	InterLlink	10.0.1.0/24	any	any	Server	172.20.20.0/24
FW-A_RuleGroup-04-Y	FW-A	universal	Server	172.20.20.0/24	any	any	DMZ	10.0.1.0/24
FW-B_RuleGroup-04-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLlink	10.0.1.0/24

D)



			Source				Destination	
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
FW-A_RuleGroup-01-W	FW-A	universal	DMZ	10.0.1.0/24	any	any	InterLink	10.0.10.0/30
FW-B_RuleGroup-01-X	FW-B	universal	InterLink	10.0.10.0/30	any	any	Server	172.20.20.0/24
FW-A_RuleGroup-01-Y	FW-A	universal	InterLink	10.0.10.0/30	any	any	DMZ	10.0.1.0/24
FW-B_RuleGroup-01-Z	FW-B	universal	Server	172.20.20.0/24	any	any	InterLink	10.0.10.0/30

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

B

Explanation:

Option B enables the required traffic by allowing SSL and web-browsing from UNTRUST to DMZ, denying SSH from UNTRUST to DMZ, allowing MYSQL from DMZ to SERVER, and allowing SSH from SERVER to DMZ. Option A allows SSH from UNTRUST to DMZ, which is not required. Option C denies all the required traffic.Option D denies all traffic from UNTRUST to TRUST, which is irrelevant to the question

https://www.paloaltonetworks.com/services/education/palo-alto-networks-certified-network-security-administrator

Question 2

Question Type: MultipleChoice

In the PAN-OS Web Interface, which is a session distribution method offered under NAT Translated Packet Tab to choose how the firewall assigns sessions?

Options:

A- Destination IP Hash b

B- Concurrent Sessions

C- Max Sessions

D- IP Modulo

Answer:

D

Explanation:

The IP Modulo session distribution method assigns sessions to dataplane processors (DPs) based on the modulo of the source and destination IP addresses. This method is suitable for environments that use NAT with a large number of translated IP addresses and ports. It ensures that sessions with the same source and destination IP addresses are processed by the same DP, regardless of the port numbers.This can improve performance and avoid out-of-order packets.

Question 3

Question Type: **MultipleChoice**

Which CLI command will help confirm if FQDN objects are resolved in the event there is a shadow rule?

Options:

A- >show system fqdn

B- >request fqdn show system

C- >request show system fqdn

D- >request system fqdn show

Answer:

A

Explanation:

The show system fqdn command displays the FQDN objects configured on the firewall and their resolved IP addresses. This can help confirm if the FQDN objects are resolved correctly and if they match the expected traffic. A shadow rule is a rule that is never matched because a preceding rule covers the same traffic. If a shadow rule uses FQDN objects, it is possible that the FQDN objects are not resolved or have different IP addresses than the traffic, causing the rule to be ineffective.

Question 4

Question Type: **MultipleChoice**

An administrator should filter NGFW traffic logs by which attribute column to determine if the entry is for the start or end of the session?

Options:

A- Receive Time

B- Type

C- Destination

D- Source

Answer:

B

Explanation:

The Type attribute column in the NGFW traffic logs indicates whether the log entry is for the start or end of the session. The possible values are START, END, DROP, DENY, and INVALID. The START value means that the log entry is for the start of the session, and the END value means that the log entry is for the end of the session.The other values indicate that the session was terminated by the firewall for various reasons12.Reference:Traffic Log Fields,Session Log Best Practices

Question 5

Question Type: MultipleChoice

Which feature enables an administrator to review the Security policy rule base for unused rules?

Options:

A- Security policy tags

B- Test Policy Match

C- View Rulebase as Groups

D- Policy Optimizer

Answer:

D

Explanation:

The Policy Optimizer feature enables an administrator to review the Security policy rule base for unused rules, unused applications, and shadowed rules. The Policy Optimizer provides information and recommendations to help optimize the Security policy rules and reduce the attack surface.The Policy Optimizer can also identify rules that can be converted to use App-ID instead of port-based criteria12.Reference:Policy Optimizer,Tips & Tricks: How to Identify Unused Policies on a Palo Alto Networks Device

Question 6

Question Type: MultipleChoice

What two actions can be taken when implementing an exception to an External Dynamic List? (Choose two.)

Options:

A- Exclude an IP address by making use of wildcards.

B- Exclude a URL entry by making use of regular expressions.

C- Exclude an IP address by making use of regular expressions.

D- Exclude a URL entry by making use of wildcards.

Answer:

A, B

Question 7

Question Type: **MultipleChoice**

Which two options does the firewall use to dynamically populate address group members? (Choose two.)

Options:

A- IP Addresses

B- Tags

C- MAC Addresses

D- Tag-based filters

Answer:

B, D

Explanation:

A dynamic address group populates its members dynamically using look ups for tags and tag-based filters. Tags are metadata elements or attribute-value pairs that are registered for each IP address. Tag-based filters use logical and and or operators to match the tags and determine the membership of the dynamic address group. For example, you can create a dynamic address group that includes all IP addresses that have the tags "web-server" and "linux". You can also use static tags as part of the filter criteria.Reference:Policy Object: Address Groups,Use Dynamic Address Groups in Policy,Statics vs. Dynamic Address Objects Groups

Question 8

Question Type: MultipleChoice

What must first be created on the firewall for SAML authentication to be configured?

Options:

A- Server Policy

B- Server Profile

C- Server Location

D- Server Group

Answer:

B

Explanation:

A server profile identifies the external authentication service and instructs the firewall on how to connect to that authentication service and access the authentication credentials for your users. To configure SAML authentication, you must create a server profile and register the firewall and the identity provider (IdP) with each other. You can import a SAML metadata file from the IdP to automatically create a server profile and populate the connection, registration, and IdP certificate information.Reference:Configure SAML Authentication,Set Up SAML Authentication,Introduction to SAML

Question 9

Question Type: MultipleChoice

Within a WildFire Analysis Profile, what match criteria can be defined to forward samples for analysis?

Options:

A- Application Category

B- Source

C- File Size

D- Direction

Answer:

D

Explanation:

A WildFire Analysis Profile allows you to specify which files or email links to forward for WildFire analysis based on the application, file type, and transmission direction (upload or download) of the traffic. The direction match criteria determines whether the file or email link was sent from the source zone to the destination zone (upload) or from the destination zone to the source zone (download). You can also select both directions to forward files or email links regardless of the direction of the traffic.Reference:Security Profile: Wildfire Analysis,Objects > Security Profiles > WildFire Analysis

Question 10

Question Type: MultipleChoice

In order to attach an Antivirus, Anti-Spyware and Vulnerability Protection security profile to your Security Policy rules, which setting must be selected?

Options:

A- Policies > Security > Actions Tab > Select Group-Profiles as Profile Type

B- Policies > Security > Actions Tab > Select Default-Profiles as Profile Type

C- Policies > Security > Actions Tab > Select Profiles as Profile Type

D- Policies > Security > Actions Tab > Select Tagged-Profiles as Profile Type

Answer:

C

Explanation:

To enable the firewall to scan the traffic that it allows based on a Security policy rule, you must also attach Security Profiles ---including URL Filtering, Antivirus, Anti-Spyware, File Blocking, and WildFire Analysis---to each rule. To attach a Security Profile to a Security policy rule, you must select Profiles as the Profile Type in the Actions tab of the rule. This allows you to choose from the predefined or custom Security Profiles that you have configured. Group-Profiles, Default-Profiles, and Tagged-Profiles are not valid options for attaching Security Profiles to Security policy rules.Reference:Set Up a Basic Security Policy,Security Profiles,Updated Certifications for PAN-OS 10.1

Question 11

Question Type: MultipleChoice

Which security profile should be used to classify malicious web content?

Options:

A- URL Filtering

B- Antivirus

C- Web Content

D- Vulnerability Protection

Answer:

A

Explanation:

URL Filtering is a security profile that allows you to classify web content based on the URL category and reputation of the website. URL Filtering can help you block access to malicious web content, such as phishing, malware, or command and control sites, as well as enforce acceptable use policies for web browsing. URL Filtering uses the PAN-DB cloud service to provide up-to-date information on the URL categories and reputations of millions of websites. You can configure URL Filtering policies to allow, block, alert, continue, or override web requests based on the URL category and reputation, as well as customize the response pages and exceptions for different user groups.Reference:URL Filtering,Set Up a Basic Security Policy,Updated Certifications for PAN-OS 10.1

Question 12

Question Type: **MultipleChoice**

Where in the PAN-OS GUI can an administrator monitor the rule usage for a specified period of time?

Options:

A- Objects > Schedules

B- Policies > Policy Optimizer

C- Monitor > Packet Capture

D- Monitor > Reports

Answer:

B

Explanation:

The Policy Optimizer is a feature in the PAN-OS GUI that allows an administrator to monitor the rule usage for a specified period of time, as well as optimize the security policies based on the traffic logs and recommendations. The Policy Optimizer can help the administrator to improve the security posture, reduce the attack surface, and simplify the policy management. The Policy Optimizer can be accessed from Policies > Policy Optimizer in the PAN-OS GUI.Reference:Policy Optimizer,View Policy Rule Usage,Updated Certifications for PAN-OS 10.1