Juniper

JN0-335 Exam

Security, Specialist

Questions & Answers
Demo

Version: 4.0

Question: 1

Regarding static attack object groups, which two statements are true? (Choose two.)

A. Matching attack objects are automatically added to a custom group.
B. Group membership automatically changes when Juniper updates the IPS signature database.
C. Group membership does not automatically change when Juniper updates the IPS signature database.
D. You must manually add matching attack objects to a custom group.

Answer: BC

Explanation:

static attack object groups are predefined groups of attack objects that are included in Juniper's IPS signature database. These groups do not change automatically when Juniper updates the database2.

Question: 2

You are deploying a new SRX Series device and you need to log denied traffic.
In this scenario, which two policy parameters are required to accomplish this task? (Choose two.)

A. session-init
B. session-close
C. deny
D. count

Answer: BC

Explanation:

you need to create a global firewall rulebase that matches RT_FLOW_SESSION_DENY events2. To do this, you need to specify two policy parameters: deny and session-close3.

Question: 3

You are asked to reduce the load that the JIMS server places on your Which action should you take in this situation?

A. Connect JIMS to the RADIUS server
B. Connect JIMS to the domain Exchange server
C. Connect JIMS to the domain SQL server.

D. Connect JIMS to another SRX Series device.

	Answer: D

Explanation:

JIMS server is a Juniper Identity Management Service that collects user identity information from different authentication sources for SRX Series devices12. It can connect to SRX Series devices and CSO platform in your network1.

JIMS server is a service that protects corporate resources by authenticating and restricting user access based on roles2. It connects to SRX Series devices and CSO platform to provide identity information for firewall policies1. To reduce the load that JIMS server places on your network, you should connect JIMS to another SRX Series device1. This way, you can distribute the identity information among multiple SRX Series devices and reduce network traffic.

Question: 4

Which two statements about unified security policies are correct? (Choose two.)

A. Unified security policies require an advanced feature license.
B. Unified security policies are evaluated after global security policies.
C. Traffic can initially match multiple unified security policies.
D. APPID results are used to determine the final security policy

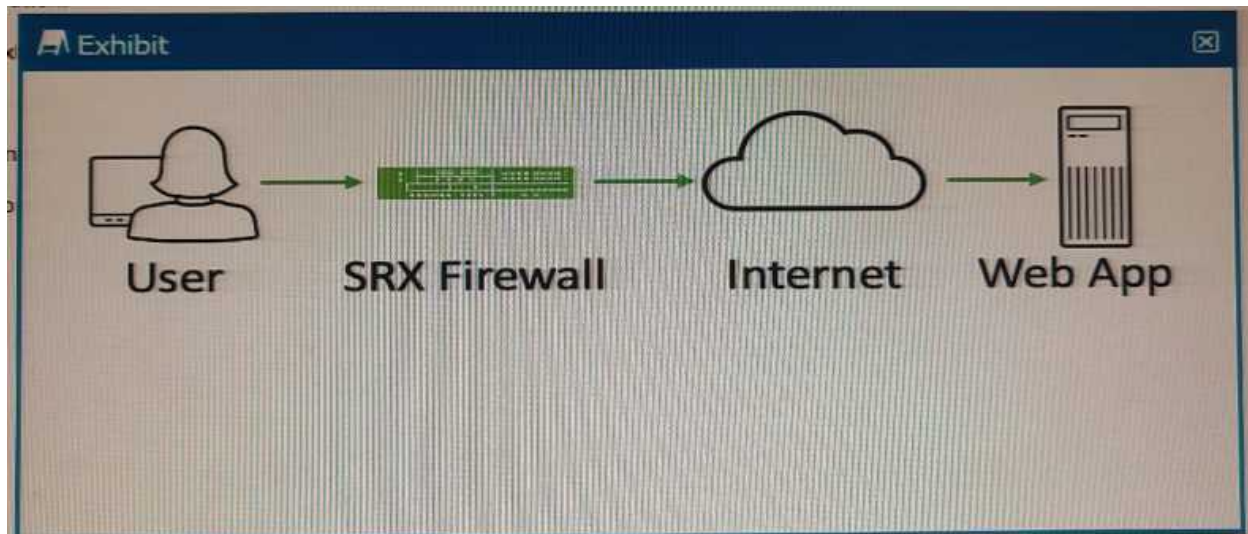|	**Answer: CD**

Explanation:

unified security policies are security policies that enable you to use dynamic applications as match conditions along with existing 5-tuple or 6-tuple matching conditions12. They simplify application-based security policy management at Layer 7 and provide greater control and extensibility to manage dynamic applications traffic3

Question: 5

Exhibit

Referring to the exhibit, which two statements describe the type of proxy used? (Choose two.)

A. forward proxy
B. client protection proxy
C. server protection proxy
D. reverse proxy

Answer: BC

Explanation:

1. Client protection proxy: This statement is correct because a forward proxy can also be called a client protection proxy since it protects the user's identity and computer information from the web server4.
2. Server protection proxy: This statement is correct because a reverse proxy can also be called a server protection proxy since it protects the web server's identity and location from the user4.