DUMPSARENA

Security, Specialist (JNCIS-SEC)

Juniper JN0-335

Version Demo

Total Demo Questions: 10

Total Premium Questions: 65

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

You are asked to block malicious applications regardless of the port number being used.

In this scenario, which two application security features should be used? (Choose two.)

A. AppFW

B. AppQoE

C. APPID

D. AppTrack

ANSWER: A C

Explanation:

you can block applications and users based on network access policies, users and their job roles, time, and application signatures2. You can also use Juniper Advanced Threat Prevention (ATP) to find and block commodity and zero-day cyberthreats within files, IP traffic, and DNS requests1

QUESTION NO: 2

You have deployed an SRX300 Series device and determined that files have stopped being scanned.

In this scenario, what is a reason for this problem?

A. The software license is a free model and only scans executable type files.

B. The infected host communicated with a command-and-control server, but it did not download malware.

C. The file is too small to have a virus.

D. You have exceeded the maximum files submission for your SRX platform size.

ANSWER: D

Explanation:

You have exceeded the maximum files submission for your SRX platform size: This statement is correct because file scanning on SRX300 Series device has a limit on the number of files that can be submitted per minute based on the platform size3. For example, SRX320 has a limit of 10 files per minute3.

QUESTION NO: 3

Which two statements are correct about the cSRX? (Choose two.)

A. The cSRX supports firewall, NAT, IPS, and UTM services.

B. The cSRX only supports Layer 2 "bump-in-the-wire" deployments.

C. The cSRX supports BGP, OSPF. and IS-IS routing services.

D. The cSRX has three default zones: trust, untrust, and management

ANSWER: A D

Explanation:

The two statements that are correct about the cSRX are that it supports firewall, NAT, IPS, and UTM services, and that it has three default zones: trust, untrust, and management. The cSRX is a software-defined security solution that provides comprehensive network security capabilities and is designed for virtualized environments. It supports firewall, NAT, IPS, and UTM services to protect against threats, as well as BGP, OSPF, and IS-IS routing services for routing functionality. Additionally, the cSRX has three default zones: trust, untrust, and management. The trust zone is used to define traffic that is allowed to enter the network, the untrust zone is used to define traffic that should be blocked from entering the network, and the management zone is used to manage the device itself. The cSRX does not support Layer 2 "bump-in-the-wire" deployments.

QUESTION NO: 4

You want to use IPS signatures to monitor traffic.

Which module in the AppSecure suite will help in this task?

A. AppTrack

B. AppQoS

C. AppFW

D. APPID

ANSWER: C

Explanation:

The AppFW module in the AppSecure suite provides IPS signatures that can be used to monitor traffic and detect malicious activities. AppFW also provides other security controls such as Web application firewall, URL filtering, and application-level visibility.

QUESTION NO: 5

You are asked to create an IPS-exempt rule base to eliminate false positives from happening.

Which two configuration parameters are available to exclude traffic from being examined? (Choose two.)

A. source port

B. source IP address

C. destination IP address

D. destination port

ANSWER: B

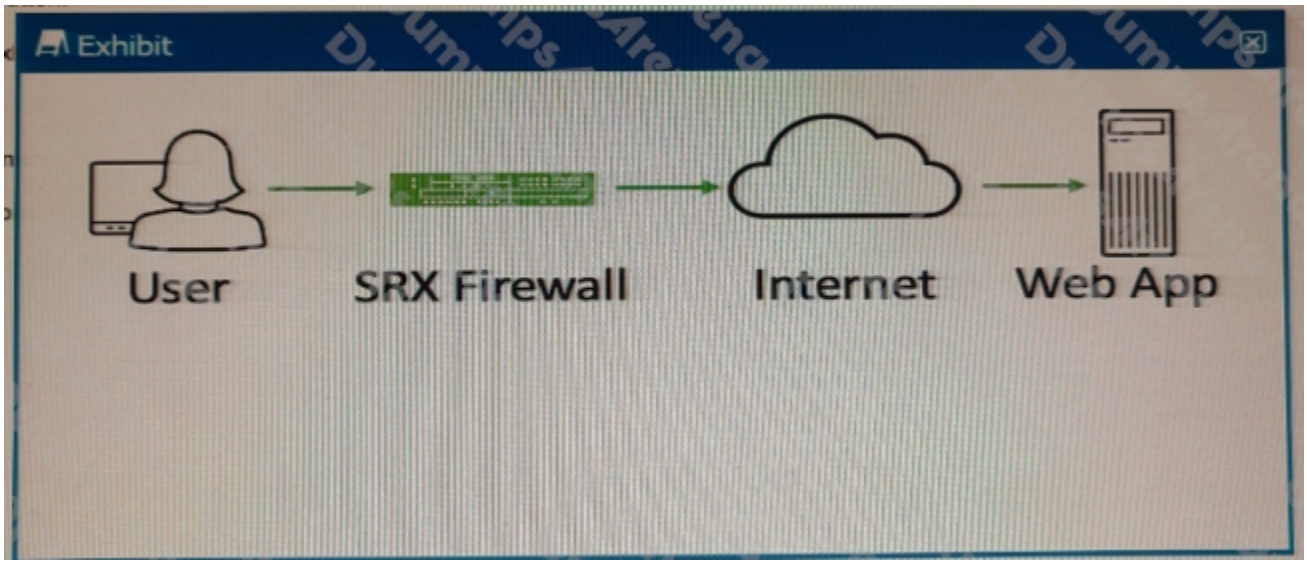
Explanation:

To exclude traffic from being examined by IPS, you can use the source IP address and/or destination port as criteria for the exemption. This is achieved by configuring an IPS-exempt rule base that includes specific exemption rules based on these criteria.

Reference: Juniper Networks. JNCIS-SEC Study Guide: Chapter 8, Intrusion Prevention System (IPS).

QUESTION NO: 6

Exhibit



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

A. forward proxy

B. client protection proxy

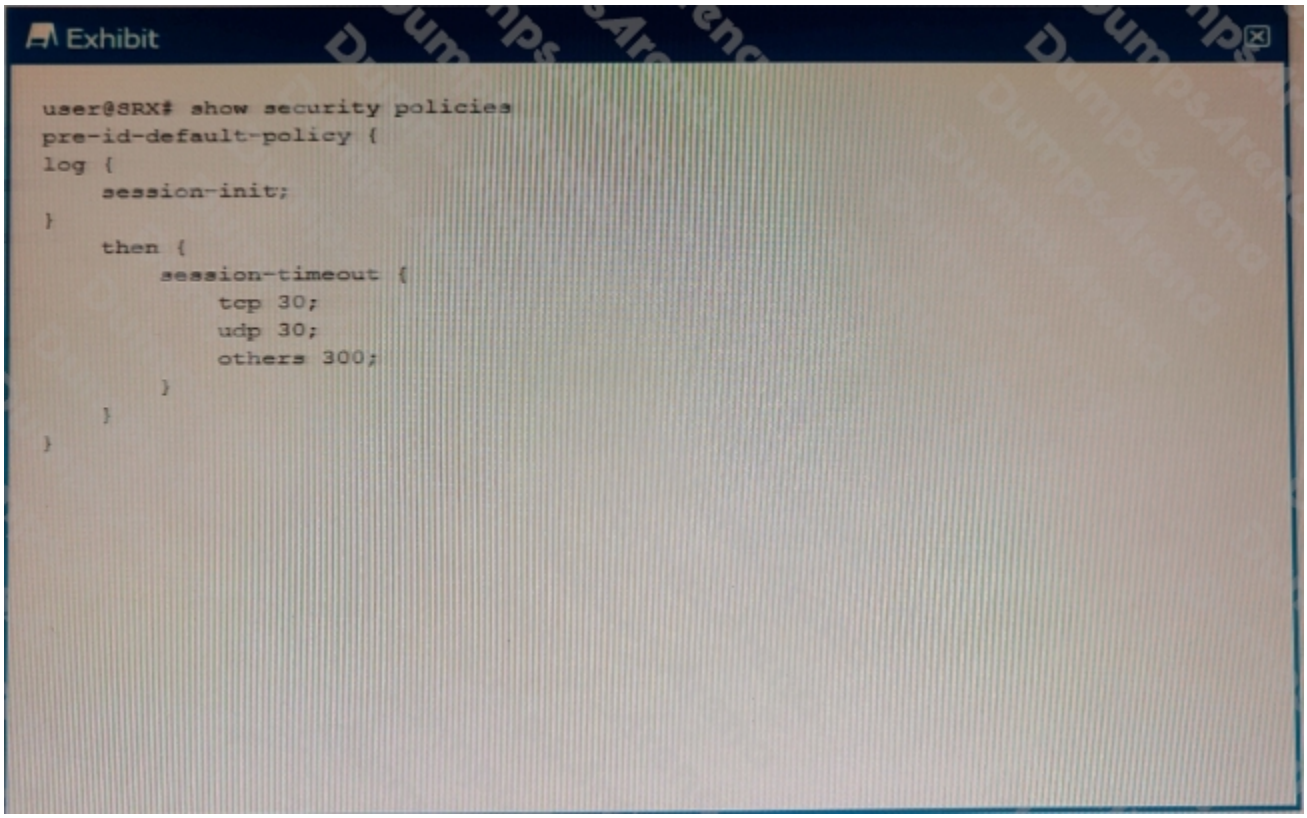
C. server protection proxy

D. reverse proxy

ANSWER: B C

QUESTION NO: 7

Exhibit



Which two statements are correct about the configuration shown in the exhibit? (Choose two.)

A. The session-class parameter in only used when troubleshooting.

B. The others 300 parameter means unidentified traffic flows will be dropped in 300 milliseconds.

C. Every session that enters the SRX Series device will generate an event

D. Replacing the session-init parameter with session-lose will log unidentified flows.

ANSWER: B C

Explanation:

The configuration shown in the exhibit is for a Juniper SRX Series firewall. The session-init parameter is used to control how the firewall processes unknown traffic flows. With the session-init parameter set to 300, any traffic flows that the firewall does not recognize will be dropped after 300 milliseconds. Additionally, every session that enters the device, whether it is known or unknown, will generate an event, which can be used for logging and troubleshooting purposes. The session-lose parameter is used to control how the firewall handles established sessions that are terminated.

QUESTION NO: 8

What are two types of system logs that Junos generates? (Choose two.)

A. SQL log files

B. data plane logs

C. system core dump files

D. control plane logs

ANSWER: B D

Explanation:

The two types of system logs that Junos generates are control plane logs and data plane logs. Control plane logs are generated by the Junos operating system and contain system-level events such as system startup and shutdown, configuration changes, and system alarms. Data plane logs are generated by the network protocol processes and contain messages about the status of the network and its components, such as routing, firewall, NAT, and IPS. SQL log files and system core dump files are not types of system logs generated by Junos.

QUESTION NO: 9

Which method does the IoT Security feature use to identify traffic sourced from IoT devices?

A. The SRX Series device streams metadata from the IoT device transit traffic to Juniper ATP Cloud Juniper ATP Cloud.

B. The SRX Series device streams transit traffic received from the IoT device to Juniper ATP Cloud.

C. The SRX Series device identifies IoT devices using their MAC address.

D. The SRX Series device identifies IoT devices from metadata extracted from their transit traffic.

ANSWER: D

Explanation:

The metadata is used to identify the type of device, its associated activities and its threat profile. This information is used to determine the appropriate security policy for the device. For more information on IoT Security, please refer to the Juniper Security, Specialist (JNCIS-SEC) study guide.

QUESTION NO: 10

You want to manually failover the primary Routing Engine in an SRX Series high availability cluster pair.

Which step is necessary to accomplish this task?

A. Issue the set chassis cluster disable reboot command on the primary node.

B. Implement the control link recover/ solution before adjusting the priorities.

C. Manually request the failover and identify the secondary node

D. Adjust the priority in the configuration on the secondary node.

ANSWER: A

Explanation:

In order to manually failover the primary Routing Engine in an SRX Series high availability cluster pair, you must issue the command "set chassis cluster disable reboot" on the primary node. This command will disable the cluster and then reboot the primary node, causing the secondary node to take over as the primary node. This is discussed in greater detail in the Juniper Security, Specialist (JNCIS-SEC) Study Guide (page 68).