Free Questions for JN0-335 by dumpshq

Shared by Whitney on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two sources are used by Juniper Identity Management Service (JIMS) for collecting username and device IP addresses? (Choose two.)

Options:

A- Microsoft Exchange Server event logs

B- DNS

C- Active Directory domain controller event logs

D- OpenLDAP service ports

Answer:

B, C

Explanation:

Juniper Identity Management Service (JIMS) collects username and device IP addresses from both DNS and Active Directory domain controller event logs. DNS is used to resolve hostnames to IP addresses, while Active Directory domain controller event logs are used to

get information about user accounts, such as when they last logged in.

Question 2

Question Type: MultipleChoice

You are asked to ensure that if the session table on your SRX Series device gets close to exhausting its resources, that you enforce a more aggress.ve age-out of existing flows.

In this scenario, which two statements are correct? (Choose two.)

Options:

A- The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the low-watermark value is met.

B- The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the high-watermark value is met.

C- The high-watermark configuration specifies the percentage of how much of the session table is left before disabling a more aggressive age- out timer.

D- The high-watermark configuration specifies the percentage of how much of the session table can be allocated before applying a more aggressive age-out timer

Answer:

B, D

Explanation:

The early-ageout configuration specifies the timeout value, in seconds, that will be applied once the high-watermark value is met. The high-watermark configuration specifies the percentage of how much of the session table can be allocated before applying a more aggressive age-out timer. This ensures that the session table does not become full and cause traffic issues, and also ensures that existing flows are aged out quickly when the table begins to get close to being full.

Question 3

Question Type: MultipleChoice

What are three capabilities of AppQoS? (Choose three.)

Options:

A- re-write DSCP values

B- assign a forwarding class

C- re-write the TTL

D- rate-limit traffic

E- reserve bandwidth

Answer:

A, B, E

Explanation:

AppQoS (Application Quality of Service) is a Junos OS feature that provides advanced control and prioritization of application traffic. With AppQoS, you can classify application traffic, assign a forwarding class to the traffic, and apply quality of service (QoS) policies to the traffic. You can also re-write DSCP values and reserve bandwidth for important applications. However, AppQoS does not re-write the TTL or rate-limit traffic.

Source: Juniper Networks, Security, Specialist (JNCIS-SEC) Study Guide. Chapter 3: AppSecure. Page 66-67.

Question 4

Question Type: MultipleChoice

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.)

Options:

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.

Question 5

Question Type: MultipleChoice

Which statement about security policy schedulers is correct?

Options:

A- Multiple policies can use the same scheduler.

B- A policy can have multiple schedulers.

C- When the scheduler is disabled, the policy will still be available.

D- A policy without a defined scheduler will not become active

Answer:

A

Explanation:

Schedulers can be defined and reused by multiple policies, allowing for more efficient management of policy activation and deactivation. This can be particularly useful for policies that need to be activated during specific time periods, such as business hours or maintenance windows.

Question 6

Question Type: MultipleChoice

Which two statements are true about Juniper ATP Cloud? (Choose two.)

Options:

A- Dynamic analysis is always performed to determine if a file contains malware.

B- If the cache lookup determines that a file contains malware, performed to verify the results.

C- Dynamic analysis is not always necessary to determine if a file contains malware.

D- If the cache lookup determines that a file contains malware, static analysis is not performed to verify the results.

Answer:

C, D

Explanation:

Dynamic analysis is not always necessary to determine if a file contains malware, as the ATP Cloud uses a cache lookup to quickly identify known malicious files. If the cache lookup determines that a file contains malware, static analysis is not performed to verify the results. This information can be found on the Juniper website here:https://www.juniper.net/documentation/en_US/release-independent/security/jnpr-security-srx-series/information-products/topic-collection/jnpr-security-srx-resources.html#id-jnpr-security-srx-resources-atp-cloud.