



Free Questions for JN0-231 by certsinside

Shared by Dyer on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two statements are correct about the null zone on an SRX Series device? (Choose two.)

Options:

- A- The null zone is created by default.
- B- The null zone is a functional security zone.
- C- Traffic sent or received by an interface in the null zone is discarded.
- D- You must enable the null zone before you can place interfaces into it.

Answer:

A, C

Explanation:

According to the Juniper SRX Series Services Guide, the null zone is a predefined security zone that is created on the SRX Series device when it is booted. Traffic that is sent to or received on an interface in the null zone is discarded. The null zone is not a functional security zone, so you cannot enable or disable it.

Question 2

Question Type: MultipleChoice

What is the default timeout value for TCP sessions on an SRX Series device?

Options:

A- 30 seconds

B- 60 minutes

C- 60 seconds

D- 30 minutes

Answer:

D

Explanation:

By default, TCP has a 30-minute idle timeout, and UDP has a 60-second idle timeout. Additionally, known IP protocols have a 30-minute timeout, whereas unknown ones have a 60-second timeout. Setting the inactivity timeout is very useful, particularly if you are concerned about applications either timing out or remaining idle for too long and filling up the session table. According to the Juniper SRX Series Services Guide, this can be configured using the 'timeout inactive' statement for the security policy.

Question 3

Question Type: MultipleChoice

What are two logical properties of an interface? (Choose two.)

Options:

- A- link mode
- B- IP address
- C- VLAN ID
- D- link speed

Answer:

B, C

Explanation:

<https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/security-interface-logical.html>

Question 4

Question Type: MultipleChoice

Your company is adding IP cameras to your facility to increase physical security. You are asked to help protect these IoT devices from becoming zombies in a DDoS attack.

Which Juniper ATP feature should you configure to accomplish this task?

Options:

A- IPsec

B- static NAT

C- allowlists

D- C&C feeds

Answer:

D

Explanation:

Juniper ATP should be configured with C&C feeds that contain lists of malicious domains and IP addresses in order to prevent IP cameras from becoming zombies in a DDoS attack.

This is an important step to ensure that the IP cameras are protected from malicious requests - and thus, they will not be able to be used in any DDoS attacks against the facility.

Question 5

Question Type: MultipleChoice

An application firewall processes the first packet in a session for which the application has not yet been identified.

In this scenario, which action does the application firewall take on the packet?

Options:

- A- It allows the first packet.
- B- It denies the first packet and sends an error message to the user.
- C- It denies the first packet.
- D- It holds the first packet until the application is identified.

Answer:

D

Explanation:

This is necessary to ensure that the application firewall can properly identify the application and the correct security policies can be applied before allowing any traffic to pass through.

If the first packet was allowed to pass without first being identified, then the application firewall would not know which security policies to apply - and this could potentially lead to security vulnerabilities or breaches. So it's important that the first packet is held until the application is identified.

Question 6

Question Type: MultipleChoice

Which two addresses are valid address book entries? (Choose two.)

Options:

- A- 173.145.5.21/255.255.255.0
- B- 153.146.0.145/255.255.0.255
- C- 203.150.108.10/24
- D- 191.168.203.0/24

Answer:

A, C

Explanation:

The correct address book entries are:

173.145.5.21/255.255.255.0

203.150.108.10/24

Both of these entries represent a valid IP address and subnet mask combination, which can be used as an address book entry in a Juniper device.

Question 7

Question Type: MultipleChoice

Which two non-configurable zones exist by default on an SRX Series device? (Choose two.)

Options:

- A- Junos-host
- B- functional
- C- null
- D- management

Answer:

A, C

Explanation:

Junos-host and null are two non-configurable zones that exist by default on an SRX Series device. Junos-host is the default zone for all internal interfaces and services, such as management and other loopback interfaces. The null zone is used to accept all traffic that is not explicitly accepted by other security policies, and is the default zone for all unclassified traffic. Both zones cannot be modified or deleted.

Question 8

Question Type: MultipleChoice

Which Web filtering solution uses a direct Internet-based service for URL categorization?

Options:

- A- Juniper ATP Cloud
- B- Websense Redirect
- C- Juniper Enhanced Web Filtering

D- local blacklist

Answer:

C

Explanation:

Juniper Enhanced Web Filtering is a web filtering solution that uses a direct Internet-based service for URL categorization. This service allows Enhanced Web Filtering to quickly and accurately categorize URLs and other web content, providing real-time protection against malicious content. Additionally, Enhanced Web Filtering is able to provide detailed reporting on web usage, as well as the ability to define and enforce acceptable use policies.

Question 9

Question Type: MultipleChoice

Which two statements about user-defined security zones are correct? (Choose two.)

Options:

- A- Users cannot share security zones between routing instances.
- B- Users can configure multiple security zones.
- C- Users can share security zones between routing instances.
- D- User-defined security zones do not apply to transit traffic.

Answer:

B, C

Explanation:

User-defined security zones allow users to configure multiple security zones and share them between routing instances. This allows users to easily manage multiple security zones and their associated policies. For example, a user can create a security zone for corporate traffic, a security zone for guest traffic, and a security zone for public traffic, and then configure policies to control the flow of traffic between each of these security zones. Transit traffic can also be managed using user-defined security zones, as the policies applied to these zones will be applied to the transit traffic as well.

Question 10

Question Type: MultipleChoice

Which two statements about the Junos OS CLI are correct? (Choose two.)

Options:

- A- The default configuration requires you to log in as the admin user.
- B- A factory-default login assigns the hostname Amnesiac to the device.
- C- Most Juniper devices identify the root login prompt using the % character.
- D- Most Juniper devices identify the root login prompt using the > character.

Answer:

A, D

Explanation:

The two correct statements about the Junos OS CLI are that the default configuration requires you to log in as the admin user, and that most Juniper devices identify the root login prompt using the > character. The factory-default login assigns the hostname 'juniper' to the device and the root login prompt is usually identified with the % character. More information about the Junos OS CLI can be found in the Juniper Networks technical documentation here:https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/cli-overview.html.

To Get Premium Files for JN0-231 Visit

<https://www.p2pexams.com/products/jn0-231>

For More Free Questions Visit

<https://www.p2pexams.com/juniper/pdf/jn0-231>

