



Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

NEW QUESTION 1

What are three Junos UTM features? (Choose three.)

- A. screens
- B. antivirus
- C. Web filtering
- D. IDP/IPS
- E. content filtering

Answer: BCE

NEW QUESTION 2

Which two statements are correct about functional zones? (Choose two.)

- A. Functional zones must have a user-defined name.
- B. Functional zone cannot be referenced in security policies or pass transit traffic.
- C. Multiple types of functional zones can be defined by the user.
- D. Functional zones are used for out-of-band device management.

Answer: BD

NEW QUESTION 3

What are two Juniper ATP Cloud feed analysis components? (Choose two.)

- A. IDP signature feed
- B. C&C cloud feed
- C. infected host cloud feed
- D. US CERT threat feed

Answer: AB

Explanation:

The Juniper ATP Cloud feed analysis components are the IDP signature feed and the C&C cloud feed. The IDP signature feed provides a database of signatures from known malicious traffic, while the C&C cloud feed provides the IP addresses of known command and control servers. The infected host cloud feed and US CERT threat feed are not components of the Juniper ATP Cloud feed analysis.

To learn more about the Juniper ATP Cloud feed analysis components, refer to the Juniper Networks Security Automation and Orchestration (SAO) official documentation, which can be found at https://www.juniper.net/documentation/en_US/sao/topics/concept/security-automation-and-orchestration-overvi. The documentation provides an overview of the SAO platform and an in-depth look at the various components of the Juniper ATP Cloud feed analysis.

NEW QUESTION 4

What is the correct order in which interface names should be identified?

- A. system slot number → interface media type → port number → line card slot number
- B. system slot number → port number → interface media type → line card slot number
- C. interface media type → system slot number → line card slot number → port number
- D. interface media type → port number → system slot number → line card slot number

Answer: C

NEW QUESTION 5

What is the default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel?

- A. 20 seconds
- B. 5 seconds
- C. 10 seconds
- D. 40 seconds

Answer: B

Explanation:

The default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel is 5 seconds. DPD is a mechanism that enables the IPsec device to detect if the peer is still reachable or if the IPsec VPN tunnel is still active. The DPD interval determines how often the IPsec device sends DPD packets to the peer to check the status of the VPN tunnel. A value of 5 seconds is a common default, but the specific value can vary depending on the IPsec device and its configuration.

NEW QUESTION 6

Click the Exhibit button.

```
[edit security policies]
user@SRX# show
from-zone trust to-zone untrust {
  policy Rule-1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
    }
  }
  policy Rule-2 {
    match {
      source-address any;
      destination-address any;
      application [ junos-ping junos-ssh ];
    }
    then {
      permit;
    }
  }
}
```

You are asked to allow only ping and SSH access to the security policies shown in the exhibit. Which statement will accomplish this task?

- A. Rename policy Rule-2 to policy Rule-0.
- B. Insert policy Rule-2 before policy Rule-1.
- C. Replace application any with application [junos-ping junos-ssh] in policy Rule-1.
- D. Rename policy Rule-1 to policy Rule-3.

Answer: B

NEW QUESTION 7

You want to deploy a NAT solution.

In this scenario, which solution would provide a static translation without PAT?

- A. interface-based source NAT
- B. pool-based NAT with address shifting
- C. pool-based NAT with PAT
- D. pool-based NAT without PAT

Answer: B

Explanation:

Translation of the original source IP address to an IP address from a user-defined address pool by shifting the IP addresses. This type of translation is one-to-one, static, and without port address translation. If the original source IP address range is larger than the IP address range in the user-defined pool, untranslated packets are dropped.

<https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/nat-security-source-and-sourc>

NEW QUESTION 8

Which two statements are correct about the default behavior on SRX Series devices? (Choose two.)

- A. The SRX Series device is in flow mode.
- B. The SRX Series device supports stateless firewalls filters.
- C. The SRX Series device is in packet mode.
- D. The SRX Series device does not support stateless firewall filters.

Answer: AB

NEW QUESTION 9

Which two components are configured for host inbound traffic? (Choose two.)

- A. zone
- B. logical interface
- C. physical interface
- D. routing instance

Answer: AB

NEW QUESTION 10

You are installing a new SRX Series device and you are only provided one IP address from your ISP. In this scenario, which NAT solution would you implement?

- A. pool-based NAT with PAT
- B. pool-based NAT with address shifting
- C. interface-based source NAT
- D. pool-based NAT without PAT

Answer: C

NEW QUESTION 10

You need to collect the serial number of an SRX Series device to replace it. Which command will accomplish this task?

- A. show chassis hardware
- B. show system information
- C. show chassis firmware
- D. show chassis environment

Answer: A

Explanation:

The correct command to collect the serial number of an SRX Series device is the show chassis hardware command [1]. This command will return the serial number of the device, along with other information about the device such as the model number, part number, and version.

This command is available in Junos OS. More information about the show chassis hardware command can be found in the Juniper Networks technical documentation here [1]: https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-chassis-hardwa

NEW QUESTION 13

Which two IPsec hashing algorithms are supported on an SRX Series device? (Choose two.)

- A. SHA-1
- B. SHAKE128
- C. MD5
- D. RIPEMD-256

Answer: AC

NEW QUESTION 17

Which two statements are correct about the integrated user firewall feature?(Choose two.)

- A. It maps IP addresses to individual users.
- B. It supports IPv4 addresses.
- C. It allows tracking of non-Windows Active Directory users.
- D. It uses the LDAP protocol.

Answer: AC

NEW QUESTION 18

When configuring antisipam, where do you apply any local lists that are configured?

- A. custom objects
- B. advanced security policy
- C. antisipam feature-profile
- D. antisipam UTM policy

Answer: A

Explanation:

user@host# set security utm custom-objects url-pattern url-pattern-name <https://www.juniper.net/documentation/us/en/software/junos/utm/topics/topic-map/security-local-list-antisipam-f>

NEW QUESTION 19

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

- A. Juniper ATP Cloud
- B. Websense Redirect
- C. Juniper Enhanced Web Filtering
- D. local blocklist

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.

References:

https://www.juniper.net/documentation/en_US/junos-space-security-director/topics/task/configuration/security-s

https://www.juniper.net/documentation/en_US/junos-space-security-director/topics/task/configuration/security-s

NEW QUESTION 20

You want to enable the minimum Juniper ATP services on a branch SRX Series device. In this scenario, what are two requirements to accomplish this task? (Choose two.)

- A. Install a basic Juniper ATP license on the branch device.
- B. Configure the juniper-atp user account on the branch device.
- C. Register for a Juniper ATP account on <https://sky.junipersecurity.net>.
- D. Execute the Juniper ATP script on the branch device.

Answer: CD

Explanation:

<https://manuals.plus/m/95fded847e67e8f456453182a54526ba3224a61a337c47177244d345d1f3b19e.pdf>

NEW QUESTION 22

Which statement is correct about Web filtering?

- A. The Juniper Enhanced Web Filtering solution requires a locally managed server.
- B. The decision to permit or deny is based on the body content of an HTTP packet.
- C. The decision to permit or deny is based on the category to which a URL belongs.
- D. The client can receive an e-mail notification when traffic is blocked.

Answer: C

Explanation:

Web filtering is a feature that allows administrators to control access to websites by categorizing URLs into different categories such as gambling, social networking, or adult content. The decision to permit or deny access to a website is based on the category to which a URL belongs. This is done by comparing the URL against a database of categorized websites and making a decision based on the policy defined by the administrator.

NEW QUESTION 23

Which two statements are correct about screens? (Choose two.)

- A. Screens process inbound packets.
- B. Screens are processed on the routing engine.
- C. Screens process outbound packets.
- D. Screens are processed on the flow module.

Answer: AD

NEW QUESTION 25

What must be enabled on an SRX Series device for the reporting engine to create reports?

- A. System logging
- B. SNMP
- C. Packet capture
- D. Security logging

Answer: D

NEW QUESTION 29

Which two UTM features should be used for tracking productivity and corporate user behavior? (Choose two.)

- A. the content filtering UTM feature
- B. the antivirus UTM feature
- C. the Web filtering UTM feature
- D. the antispam UTM feature

Answer: AC

NEW QUESTION 31

You are asked to verify that a license for AppSecure is installed on an SRX Series device. In this scenario, which command will provide you with the required information?

- A. user@srx> show system license
- B. user@srx> show services accounting
- C. user@srx> show configuration system
- D. user@srx> show chassis firmware

Answer: A

NEW QUESTION 33

Which two IKE Phase 1 configuration options must match on both peers to successfully establish a tunnel? (Choose two.)

- A. VPN name
- B. gateway interfaces
- C. IKE mode
- D. Diffie-Hellman group

Answer: CD

NEW QUESTION 38

Which Juniper ATP feed provides a dynamic list of known botnet servers and known sources of malware downloads?

- A. infected host cloud feed
- B. Geo IP feed
- C. C&C cloud feed
- D. blacklist feed

Answer: A

NEW QUESTION 41

What is the main purpose of using screens on an SRX Series device?

- A. to provide multiple ports for accessing security zones
- B. to provide an alternative interface into the CLI
- C. to provide protection against common DoS attacks
- D. to provide information about traffic patterns traversing the network

Answer: C

Explanation:

The main purpose of using screens on an SRX Series device is to provide protection against common Denial of Service (DoS) attacks. Screens help prevent network resources from being exhausted or unavailable by filtering or blocking network traffic based on predefined rules. The screens are implemented as part of the firewall function on the SRX Series device, and they help protect against various types of DoS attacks, such as TCP SYN floods, ICMP floods, and UDP floods.

NEW QUESTION 42

You have an FTP server and a webserver on the inside of your network that you want to make available to users outside of the network. You are allocated a single public IP address.

In this scenario, which two NAT elements should you configure? (Choose two.)

- A. destination NAT
- B. NAT pool
- C. source NAT
- D. static NAT

Answer: AB

Explanation:

With single Ip address it is port forwarding. So, destination NAT and a pool address point to the single public IP of the internet facing interface.

NEW QUESTION 47

Which two statements are correct about IPsec security associations? (Choose two.)

- A. IPsec security associations are bidirectional.
- B. IPsec security associations are unidirectional.
- C. IPsec security associations are established during IKE Phase 1 negotiations.
- D. IPsec security associations are established during IKE Phase 2 negotiations.

Answer: AD

Explanation:

The two statements that are correct about IPsec security associations are that they are bidirectional and that they are established during IKE Phase 2 negotiations. IPsec security associations are bidirectional, meaning that they provide security for both incoming and outgoing traffic. IPsec security associations are established during IKE Phase 2 negotiations, which negotiates the security parameters and establishes the security association between the two peers. For more information, please refer to the Juniper Networks IPsec VPN Configuration Guide, which can be found on Juniper's website.

NEW QUESTION 50

You must monitor security policies on SRX Series devices dispersed throughout locations in your organization using a 'single pane of glass' cloud-based solution. Which solution satisfies the requirement?

- A. Juniper Sky Enterprise
- B. J-Web
- C. Junos Secure Connect
- D. Junos Space

Answer: D

Explanation:

Junos Space is a management platform that provides a single pane of glass view of SRX Series devices dispersed throughout locations in your organization. It provides visibility into the security policies of the devices, allowing you to quickly identify and respond to security threats. Additionally, it provides the ability to manage multiple devices remotely and in real-time, enabling you to quickly deploy and update security policies on all devices. For more information, please refer to the Juniper Networks Junos Space Network Director User Guide, which can be found on Juniper's website.

NEW QUESTION 55

You want to prevent other users from modifying or discarding your changes while you are also editing the configuration file.
In this scenario, which command would accomplish this task?

- A. configure master
- B. cli privileged
- C. configure exclusive
- D. configure

Answer: C

NEW QUESTION 57

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

JN0-231 Practice Exam Features:

- * JN0-231 Questions and Answers Updated Frequently
- * JN0-231 Practice Questions Verified by Expert Senior Certified Staff
- * JN0-231 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * JN0-231 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The JN0-231 Practice Test Here](#)