

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

<https://www.2passeasy.com/dumps/JN0-231/>



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

Click the Exhibit button.

```
[edit]
user@SRX# show security zones
security-zone Internal {
    host-inbound-traffic {
        system-services {
            http {
                except;
            }
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
```

What is the purpose of the host-inbound-traffic configuration shown in the exhibit?

- A. to permit host inbound HTTP traffic and deny all other traffic on the internal security zone
- B. to deny and log all host inbound traffic on the internal security zone, except for HTTP traffic
- C. to permit all host inbound traffic on the internal security zone, but deny HTTP traffic
- D. to permit host inbound HTTP traffic on the internal security zone

Answer: C

NEW QUESTION 5

Which Juniper Networks solution uses static and dynamic analysis to search for day-zero malware threats?

- A. firewall filters
- B. UTM
- C. Juniper ATP Cloud
- D. IPS

Answer: C

Explanation:

Malware Sandboxing
Detect and stop zero-day and commodity malware within web, email, data center, and application traffic targeted for Windows, Mac, and IoT devices. <https://www.juniper.net/us/en/products/security/advanced-threat-prevention.html>

NEW QUESTION 6

You have configured a UTM feature profile.
Which two additional configuration steps are required for your UTM feature profile to take effect? (Choose two.)

- A. Associate the UTM policy with an address book.
- B. Associate the UTM policy with a firewall filter.
- C. Associate the UTM policy with a security policy.
- D. Associate the UTM feature profile with a UTM policy.

Answer: CD

Explanation:

For the UTM feature profile to take effect, it must be associated with a security policy and a UTM policy. The security policy defines the traffic flow and the actions that should be taken on the traffic, while the UTM policy defines the security features to be applied to the traffic, such as antivirus, intrusion prevention, and web filtering. The UTM feature profile provides the necessary configuration for the security features defined in the UTM policy.

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

You are investigating a communication problem between two hosts and have opened a session on the SRX Series device closest to one of the hosts and entered the show security flow session command.
What information will this command provide? (Choose two.)

- A. The total active time of the session.
- B. The end-to-end data path that the packets are taking.
- C. The IP address of the host that initiates the session.
- D. The security policy name that is controlling the session.

Answer: CD

NEW QUESTION 9

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?

- 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.

NEW QUESTION 10

You are assigned a project to configure SRX Series devices to allow connections to your web servers. The web servers have a private IP address, and the packets must use NAT to be accessible from the Internet. You do not want the web servers to initiate connections with external update servers on the Internet using the same IP address as customers use to access them.
Which two NAT types must be used to complete this project? (Choose two.)

- A. static NAT

- B. hairpin NAT
- C. destination NAT
- D. source NAT

Answer: CD

NEW QUESTION 10

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 14

Which statement is correct about static NAT?

- A. Static NAT supports port translation.
- B. Static NAT rules are evaluated after source NAT rules.
- C. Static NAT implements unidirectional one-to-one mappings.
- D. Static NAT implements unidirectional one-to-many mappings.

Answer: C

Explanation:

Static NAT (Network Address Translation) is a type of NAT that maps a public IP address to a private IP address. With static NAT, a one-to-one mapping is created between a public IP address and a private IP address. This means that a single public IP address is mapped to a single private IP address, and all incoming traffic to the public IP address is forwarded to the private IP address.

NEW QUESTION 17

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 18

Which two criteria should a zone-based security policy include? (Choose two.)

- A. a source port
- B. a destination port
- C. zone context
- D. an action

Answer: AB

Explanation:

A security policy is a set of statements that controls traffic from a specified source to a specified destination using a specified service. A policy permits, denies, or tunnels specified types of traffic unidirectionally between two points.

Each policy consists of:

A unique name for the policy.

A from-zone and a to-zone, for example: user@host# set security policies from-zone untrust to-zone untrust A set of match criteria defining the conditions that must be satisfied to apply the policy rule. The match criteria are based on a source IP address, destination IP address, and applications. The user identity firewall provides greater granularity by including an additional tuple, source-identity, as part of the policy statement.

A set of actions to be performed in case of a match—permit, deny, or reject. Accounting and auditing elements—counting, logging, or structured system logging. <https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-policy-c>

NEW QUESTION 22

You want to verify the peer before IPsec tunnel establishment. What would be used as a final check in this scenario?

- A. traffic selector
- B. perfect forward secrecy
- C. st0 interfaces
- D. proxy ID

Answer: D

Explanation:

The proxy ID is used as a final check to verify the peer before IPsec tunnel establishment. The proxy ID is a combination of local and remote subnet and protocol, and it is used to match the traffic that is to be encrypted. If the proxy IDs match between the two IPsec peers, the IPsec tunnel is established, and the traffic is encrypted.

NEW QUESTION 25

Your ISP gives you an IP address of 203.0.113.0/27 and informs you that your default gateway is 203.0.113.1. You configure destination NAT to your internal server, but the requests sent to the webserver at 203.0.113.5 are not arriving at the server. In this scenario, which two configuration features need to be added? (Choose two.)

- A. firewall filter
- B. security policy
- C. proxy-ARP
- D. UTM policy

Answer: BC

NEW QUESTION 27

What information does the show chassis routing-engine command provide?

- A. chassis serial number
- B. resource utilization
- C. system version
- D. routing tables

Answer: B

NEW QUESTION 29

You are creating Ipsec connections.

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

- A. Proxy IDs are used to configure traffic selectors.
- B. Proxy IDs are optional for Phase 2 session establishment.
- C. Proxy IDs must match for Phase 2 session establishment.
- D. Proxy IDs default to 0.0.0.0/0 for policy-based VPNs.

Answer: AB

NEW QUESTION 34

Click the Exhibit button.

```
[edit security policies]
user@vSRX-1# edit from-zone trust to-zone dmz policy Trust-DMZ-Access
[edit security policies from-zone trust to-zone dmz policy Trust-DMZ-Access]
user@vSRX-1# exit
```

Referring to the exhibit, a user is placed in which hierarchy when the exit command is run?

- A. [edit security policies from-zone trust to-zone dmz] user@vSRX-1#
- B. [edit] user@vSRX-1#
- C. [edit security policies] user@vSRX-1#
- D. user@vSRX-1>

Answer: A

NEW QUESTION 36

Unified threat management (UTM) inspects traffic from which three protocols? (Choose three.)

- A. FTP
- B. SMTP
- C. SNMP
- D. HTTP
- E. SSH

Answer: ABD

Explanation:

<https://www.inetzero.com/blog/unified-threat-management-deeper-dive-traffic-inspection/>

NEW QUESTION 40

You are monitoring an SRX Series device that has the factory-default configuration applied. In this scenario, where are log messages sent by default?

- A. Junos Space Log Director
- B. Junos Space Security Director
- C. to a local syslog server on the management network
- D. to a local log file named messages

Answer: C

NEW QUESTION 44

Which feature would you use to protect clients connected to an SRX Series device from a SYN flood attack?

- A. security policy
- B. host inbound traffic
- C. application layer gateway
- D. screen option

Answer: D

Explanation:

A screen option in the SRX Series device can be used to protect clients connected to the device from a SYN flood attack. Screens are security measures that you can use to protect your network from various types of attacks, including SYN floods. A screen option specifies a set of rules to match against incoming packets, and it can take specific actions such as discarding, logging, or allowing the packets based on the rules.

NEW QUESTION 49

Which security policy type will be evaluated first?

- A. A zone policy with no dynamic application set
- B. A global with no dynamic application set
- C. A zone policy with a dynamic application set
- D. A global policy with a dynamic application set

Answer: D

NEW QUESTION 50

Which statement is correct about unified security policies on an SRX Series device?

- A. A zone-based policy is always evaluated first.
- B. The most restrictive policy is applied regardless of the policy level.
- C. A global policy is always evaluated first.
- D. The first policy rule is applied regardless of the policy level.

Answer: A

NEW QUESTION 51

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

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

Answer: AC

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.

References:

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-zones-overview.html

https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-zones-de

NEW QUESTION 56

What is an IP addressing requirement for an IPsec VPN using main mode?

- A. One peer must have dynamic IP addressing.
- B. One peer must have static IP addressing.
- C. Both peers must have dynamic IP addresses.
- D. Both peers must have static IP addressing.

Answer: D

NEW QUESTION 59

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 62

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

- 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.

NEW QUESTION 66

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 70

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 73

What are two functions of Juniper ATP Cloud? (Choose two.)

- A. malware inspection
- B. Web content filtering
- C. DDoS protection
- D. Geo IP feeds

Answer: AD

Explanation:

Juniper Advanced Threat Prevention (ATP) Cloud is a security service that helps organizations protect against advanced threats by providing real-time threat intelligence and automated response capabilities. It combines a cloud-based threat intelligence platform with the security capabilities of Juniper Networks security devices to provide comprehensive protection against advanced threats. The two functions of Juniper ATP Cloud include malware inspection and Geo IP feeds. The malware inspection component provides real-time protection against known and unknown threats by analyzing suspicious files and determining if they are malicious. The Geo IP feeds provide a global view of IP addresses and their associated countries, allowing organizations to identify and block traffic from known malicious countries.

NEW QUESTION 74

What is the order in which malware is detected and analyzed?

- A. antivirus scanning → cache lookup → dynamic analysis → static analysis
- B. cache lookup → antivirus scanning → static analysis → dynamic analysis
- C. antivirus scanning → cache lookup → static analysis → dynamic analysis
- D. cache lookup → static analysis → dynamic analysis → antivirus scanning

Answer: B

NEW QUESTION 78

Click the Exhibit button.

```

policies {
  from-zone untrust to-zone trust {
    policy permit-all {
      [...]
      then {
        permit;
      }
    }
    policy deny-all {
      [...]
      then {
        deny;
      }
    }
    policy reject-all {
      [...]
      then {
        reject;
      }
    }
  }
}

```

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

- A. UDP traffic matched by the deny-all policy will be silently dropped.
- B. TCP traffic matched by the reject-all policy will have a TCP RST sent.
- C. TCP traffic matched from the zone trust is allowed by the permit-all policy.
- D. UDP traffic matched by the reject-all policy will be silently dropped.

Answer: AB

NEW QUESTION 80

Screens on an SRX Series device protect against which two types of threats? (Choose two.)

- A. IP spoofing
- B. ICMP flooding
- C. zero-day outbreaks
- D. malicious e-mail attachments

Answer: AB

Explanation:

ICMP flood

Use the ICMP flood IDS option to protect against ICMP flood attacks. An ICMP flood attack typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.

The threshold value defines the number of ICMP packets per second (pps) allowed to be sent to the same destination address before the device rejects further ICMP packets.

IP spoofing

Use the IP address spoofing IDS option to prevent spoofing attacks. IP spoofing occurs when an invalid source address is inserted in the packet header to make the packet appear to come from a trusted source.

<https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/topic-map/security-introdu>

NEW QUESTION 82

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 83

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 87

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

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

Answer: AD

NEW QUESTION 90

What are two features of the Juniper ATP Cloud service? (Choose two.)

- A. sandbox
- B. malware detection
- C. EX Series device integration
- D. honeypot

Answer: AB

NEW QUESTION 95

SRX Series devices have a maximum of how many rollback configurations?

- A. 40
- B. 60
- C. 50
- D. 10

Answer: C

NEW QUESTION 100

When operating in packet mode, which two services are available on the SRX Series device? (Choose two.)

- A. MPLS
- B. UTM
- C. CoS
- D. IDP

Answer: AC

NEW QUESTION 101

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

- 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: BC

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.

References:

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-zones-overview-configu

https://www.juniper.net/documentation/en_US/junos/topics/task/security/security-zones-configuring-shared.htm

NEW QUESTION 105

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 110

In J-Web, the management and loopback address configuration option allows you to configure which area?

- A. the IP address of the primary Gigabit Ethernet port
- B. the IP address of the Network Time Protocol server
- C. the CIDR address
- D. the IP address of the device management port

Answer: D

Explanation:

J-Web is a web-based interface for configuring and managing Juniper devices. The management and loopback address configuration option in J-Web allows you to configure the IP address of the device management port, which is used to remotely access and manage the device.

NEW QUESTION 115

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual JN0-231 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the JN0-231 Product From:

<https://www.2passeasy.com/dumps/JN0-231/>

Money Back Guarantee

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 FirstTry
- * JN0-231 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year