

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

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



NEW QUESTION 1

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 2

Which three Web filtering deployment actions are supported by Junos? (Choose three.)

- A. Use IPS.
- B. Use local lists.
- C. Use remote lists.
- D. Use Websense Redirect.
- E. Use Juniper Enhanced Web Filtering.

Answer: BDE

Explanation:

<https://www.juniper.net/documentation/us/en/software/junos/utm/topics/concept/utm-web-filtering-overview.ht>

NEW QUESTION 3

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 4

Which three operating systems are supported for installing and running Juniper Secure Connect client software? (Choose three.)

- A. Windows 7
- B. Android
- C. Windows 10
- D. Linux
- E. macOS

Answer: ACE

Explanation:

Juniper Secure Connect client software is supported on the following three operating systems: Windows 7, Windows 10, and macOS. For more information, please refer to the Juniper Secure Connect Administrator Guide, which can be found on Juniper's website. The guide states: "The Juniper Secure Connect client is supported on Windows 7, Windows 10, and macOS." It also provides detailed instructions on how to install and configure the software for each of these operating systems.

NEW QUESTION 5

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 6

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 7

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 8

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 9

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. The web servers must use the same address for both connections from the Internet and communication with update servers.

Which NAT type must be used to complete this project?

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

Answer: C

Explanation:

Only static NAT with pool ensures both traffic initiated from inside and outside networks use the same IP address.

NEW QUESTION 10

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 10

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 15

In this scenario, which two IP packets will match the criteria? (Choose two.)

- A. 192.168.1.21
- B. 192.168.0.1
- C. 192.168.1.12
- D. 192.168.22.12

Answer: CD

NEW QUESTION 16

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

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

Answer: BC

Explanation:

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

NEW QUESTION 19

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 21

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 25

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 29

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 32

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 37

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 41

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 44

Which statement is correct about global security policies on SRX Series devices?

- A. The to-zone any command configures a global policy.
- B. The from-zone any command configures a global policy.
- C. Global policies are always evaluated first.
- D. Global policies can include zone context.

Answer: D

NEW QUESTION 47

What is the order of the first path packet processing when a packet enters a device?

- A. security policies → screens → zones
- B. screens → security policies → zones
- C. screens → zones → security policies
- D. security policies → zones → screens

Answer: C

NEW QUESTION 49

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 54

You are configuring an SRX Series device. You have a set of servers inside your private network that need one-to-one mappings to public IP addresses. Which NAT configuration is appropriate in this scenario?

- A. source NAT with PAT
- B. destination NAT
- C. NAT-T
- D. static NAT

Answer: D

Explanation:

https://www.juniper.net/documentation/en_US/day-one-books/nat-and-pat-en.html

And the specific text that would support the above answer is as follows: "Static NAT, which requires manual configuration, is often the most appropriate configuration for mapping one internal address to one external address."

NEW QUESTION 58

Which two traffic types are considered exception traffic and require some form of special handling by the PFE? (Choose two.)

- A. SSH sessions
- B. ICMP reply messages
- C. HTTP sessions
- D. traceroute packets

Answer: BD

NEW QUESTION 59

What are two valid address books? (Choose two.)

- A. 66.129.239.128/25
- B. 66.129.239.154/24
- C. 66.129.239.0/24
- D. 66.129.239.50/25

Answer: AC

Explanation:

Network Prefixes in Address Books

You can specify addresses as network prefixes in the prefix/length format. For example, 203.0.113.0/24 is an acceptable address book address because it translates to a network prefix. However, 203.0.113.4/24 is not acceptable for an address book because it exceeds the subnet length of 24 bits. Everything beyond the subnet length must be entered as 0 (zero). In special scenarios, you can enter a hostname because it can use the full 32-bit address length.

<https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-address>

NEW QUESTION 62

What does the number “2” indicate in interface ge-0/1/2?

- A. the physical interface card (PIC)
- B. the flexible PIC concentrator (FPC)
- C. the interface logical number
- D. the port number

Answer: D

NEW QUESTION 63

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 65

When are Unified Threat Management services performed in a packet flow?

- A. before security policies are evaluated
- B. as the packet enters an SRX Series device
- C. only during the first path process
- D. after network address translation

Answer: D

Explanation:

<https://iosonounrouter.wordpress.com/2018/07/07/how-does-a-flow-based-srx-work/>

NEW QUESTION 69

When transit traffic matches a security policy, which three actions are available? (Choose three.)

- A. Allow
- B. Discard
- C. Deny
- D. Reject
- E. Permit

Answer: CDE

NEW QUESTION 71

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 76

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 77

.....

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