

Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)



NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

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 firewall 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 7

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

- 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: AD

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.htm

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

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 10

Which statement about service objects is correct?

- A. All applications are predefined by Junos.
- B. All applications are custom defined by the administrator.
- C. All applications are either custom or Junos defined.
- D. All applications in service objects are not available on the vSRX Series device.

Answer: C

Explanation:

"Service objects represent applications and services that can be assigned to a security policy rule. Applications and services can either be predefined by Junos software or custom defined by the administrator."

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 11

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 12

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 16

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 18

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

- A. Juniper ATP Cloud is an on-premises ATP appliance.
- B. Juniper ATP Cloud can be used to block and allow IPs.
- C. Juniper ATP Cloud is a cloud-based ATP subscription.
- D. Juniper ATP Cloud delivers intrusion protection services.

Answer: CD

Explanation:

Juniper ATP Cloud is a cloud-based ATP subscription that delivers advanced threat protection services, such as URL categorization, file reputation analysis, and malware analysis. It is able to quickly and accurately categorize URLs and other web content, and can also provide detailed reporting on web usage, as well as the ability to define and enforce acceptable use policies. Additionally, Juniper ATP Cloud is able to block and allow specific IPs, providing additional protection against malicious content.

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 21

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 26

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

- 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: AC

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.

NEW QUESTION 27

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 28

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 32

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 34

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 35

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 36

You are asked to configure your SRX Series device to block all traffic from certain countries. The solution must be automatically updated as IP prefixes become allocated to those certain countries.

Which Juniper ATP solution will accomplish this task?

- A. Geo IP
- B. unified security policies
- C. IDP
- D. C&C feed

Answer: A

Explanation:

Juniper ATP Geo IP can help to accomplish this task by using geolocation services to determine the geographical location of IP addresses. As IP prefixes get allocated to the countries that you have specified, the Geo IP solution will automatically update the configured firewall policies to block any traffic that is coming from those specific countries.

This is a great solution for blocking specific countries - as it will allow for a more personalized and targeted approach to firewall policies - and thus, to increase the effectiveness of the solution at blocking potential malicious traffic.

NEW QUESTION 39

Which statement about global NAT address persistence is correct?

- A. The same IP address from a source NAT pool will be assigned for all sessions from a given host.
- B. The same IP address from a source NAT pool is not guaranteed to be assigned for all sessions from a given host.
- C. The same IP address from a destination NAT pool will be assigned for all sessions for a given host.
- D. The same IP address from a destination NAT pool is not guaranteed to be assigned for all sessions for a given host.

Answer: A

Explanation:

Use the persistent-nat feature to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address (the public IP address and port created by the NAT device closest to the STUN server). The source NAT rule action can use a source NAT pool (with or without port translation) or an egress interface.

NEW QUESTION 44

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 47

Which statement about NAT is correct?

- A. Destination NAT takes precedence over static NAT.
- B. Source NAT is processed before security policy lookup.
- C. Static NAT is processed after forwarding lookup.
- D. Static NAT takes precedence over destination NAT.

Answer: D

NEW QUESTION 52

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 57

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

- 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: AC

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.

NEW QUESTION 59

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 62

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 64

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 69

Which two services does Juniper Connected Security provide? (Choose two.)

- A. protection against zero-day threats
- B. IPsec VPNs
- C. Layer 2 VPN tunnels
- D. inline malware blocking

Answer: AD

NEW QUESTION 71

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 76

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 79

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 83

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 85

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

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

Answer: C

NEW QUESTION 90

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 92

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 93

What is the number of concurrent Secure Connect user licenses that an SRX Series device has by default?

- A. 3
- B. 4
- C. 2
- D. 5

Answer: C

Explanation:

The number of concurrent Secure Connect user licenses that an SRX Series device has by default is 2. Secure Connect is a feature of Juniper SRX Series devices that allows you to securely connect to remote networks via IPsec VPN tunnels. Each SRX Series device comes with two concurrent Secure Connect user licenses by default, meaning that it can support up to two simultaneous IPsec VPN connections. For more information, please refer to the Juniper Networks SRX Series Services Gateways Security Configuration Guide, which can be found on Juniper's website.

NEW QUESTION 95

.....

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](#)