



Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

NEW QUESTION 1

You want to block executable files ("exe") from being downloaded onto your network. Which UTM feature would you use in this scenario?

- A. IPS
- B. Web filtering
- C. content filtering
- D. antivirus

Answer: B

Explanation:

According to the Juniper Networks official JNCIA-SEC Exam Guide, web filtering is a feature used to control access to web content, including the ability to block specific types of files.

In the scenario mentioned, you want to block executable files from being downloaded, which can be accomplished by using web filtering. The feature allows administrators to configure policies that block specific file types, including "exe" files, from being downloaded.

NEW QUESTION 2

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 3

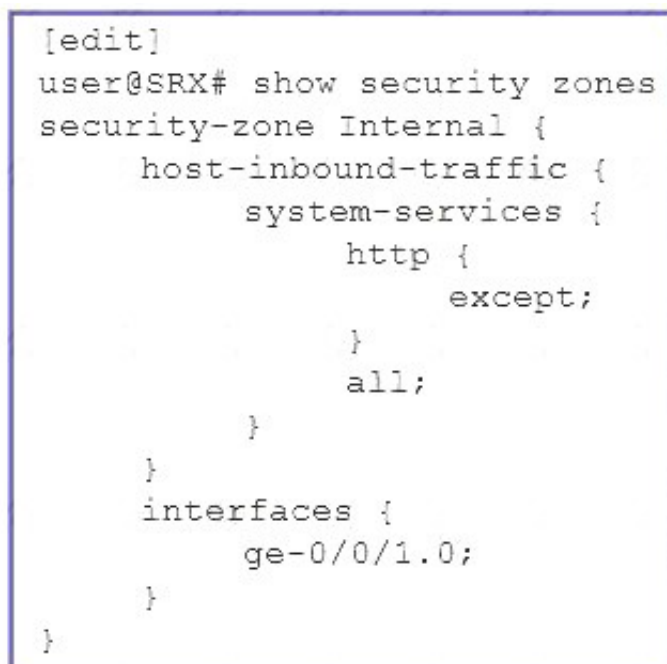
What are two characteristics of a null zone? (Choose two.)

- A. The null zone is configured by the super user.
- B. By default, all unassigned interfaces are placed in the null zone.
- C. All ingress and egress traffic on an interface in a null zone is permitted.
- D. When an interface is deleted from a zone, it is assigned back to the null zone.

Answer: BD

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

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 7

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 8

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 9

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 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

What are three primary match criteria used in a Junos security policy? (Choose three.)

- A. application
- B. source address
- C. source port
- D. class
- E. destination address

Answer: ABE

NEW QUESTION 16

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 20

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 21

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 24

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 27

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 31

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 33

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 35

Which two user authentication methods are supported when using a Juniper Secure Connect VPN? (Choose two.)

- A. certificate-based
- B. multi-factor authentication
- C. local authentication
- D. active directory

Answer: CD

Explanation:

"Local Authentication—In local authentication, the SRX Series device validates the user credentials by checking them in the local database. In this method, the administrator handles change of password or resetting of forgotten password. Here, it requires that an user must remember a new password. This option is not much preferred from a security standpoint.

• External Authentication—In external authentication, you can allow the users to use the same user credentials they use when accessing other resources on the network. In many cases, user credentials are domain logon used for Active Directory or any other LDAP authorization system. This method simplifies user experience and improves the organization's security posture; because you can maintain the authorization system with the regular security policy used by your organization."

<https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-administrator-guide/topic>

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 41

Corporate security requests that you implement a policy to block all POP3 traffic from traversing the Internet firewall. In this scenario, which security feature would you use to satisfy this request?

- A. antivirus
- B. Web filtering
- C. content filtering
- D. antispyware

Answer: C

NEW QUESTION 42

Which IPsec protocol is used to encrypt the data payload?

- A. ESP
- B. IKE
- C. AH
- D. TCP

Answer: A

NEW QUESTION 47

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 50

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 52

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 56

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 60

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 65

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 68

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 73

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 76

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 79

Which statement is correct about Junos security policies?

- A. Security policies enforce rules that should be applied to traffic transiting an SRX Series device.
- B. Security policies determine which users are allowed to access an SRX Series device.
- C. Security policies control the flow of internal traffic within an SRX Series device.
- D. Security policies identity groups of users that have access to different features on an SRX Series device.

Answer: A

Explanation:

The correct statement about Junos security policies is that they enforce rules that should be applied to traffic transiting an SRX Series device. Security policies control the flow of traffic between different zones on the SRX Series device, and dictate which traffic is allowed or denied. They can also specify which application and service requests are allowed or blocked. More information about Junos security policies can be found in the Juniper Networks technical documentation here:

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

NEW QUESTION 84

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 89

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 93

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 94

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 97

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 send 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 99

Which two components are part of a security zone? (Choose two.)

- A. inet.0
- B. fxp0
- C. address book
- D. ge-0/0/0.0

Answer: BD

NEW QUESTION 100

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

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

Answer: C

NEW QUESTION 105

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 110

When creating a site-to-site VPN using the J-Web shown in the exhibit, which statement is correct?

- A. The remote gateway is configured automatically based on the local gateway settings.
- B. RIP, OSPF, and BGP are supported under Routing mode.
- C. The authentication method is pre-shared key or certificate based.
- D. Privately routable IP addresses are required.

Answer: D

NEW QUESTION 113

.....

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](#)