

# 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

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](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

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 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 want to implement user-based enforcement of security policies without the requirement of certificates and supplicant software. Which security feature should you implement in this scenario?

- A. integrated user firewall
- B. screens
- C. 802.1X
- D. Juniper ATP

**Answer:** D

#### Explanation:

In this scenario, you should implement Juniper ATP (Advanced Threat Prevention). Juniper ATP provides user-based enforcement of security policies without the requirement of certificates and supplicant software. It uses a combination of behavioral analytics, sandboxing, and threat intelligence to detect and respond to advanced threats in real time. Juniper ATP provides robust protection against targeted attacks, malicious insiders, and zero-day malware. For more information, please refer to the Juniper ATP product page on Juniper's website.

#### NEW QUESTION 6

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](https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/cli-overview.htm)

#### NEW QUESTION 7

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 8

What does the number "2" indicate in interface ge—0/1/2?

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

**Answer:** C

#### NEW QUESTION 9

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 10

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 10

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 14

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 19

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 21

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 26

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 31**

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 36**

Which statement is correct about packet mode processing?

- A. Packet mode enables session-based processing of incoming packets.
- B. Packet mode works with NAT, VPNs, UTM, IDP, and other advanced security services.
- C. Packet mode bypasses the flow module.
- D. Packet mode is the basis for stateful processing.

**Answer:** C

**NEW QUESTION 41**

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 44**

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 49**

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/task/configuration/security-zones-overview.html)

[https://www.juniper.net/documentation/en\\_US/junos/topics/reference/configuration-statement/security-zones-de](https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-zones-de)

**NEW QUESTION 51**

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 56

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 57

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 59

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 60

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 64

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/configuration/security-zones-overview-configu)

[https://www.juniper.net/documentation/en\\_US/junos/topics/task/security/security-zones-configuring-shared.htm](https://www.juniper.net/documentation/en_US/junos/topics/task/security/security-zones-configuring-shared.htm)

#### NEW QUESTION 69

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 74

.....

## 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