



# Juniper

## Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### 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

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

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 4

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 5

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](https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-chassis-hardwa)

#### NEW QUESTION 6

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 7**

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 8**

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 9**

When configuring antisпам, where do you apply any local lists that are configured?

- A. custom objects
- B. advanced security policy
- C. antisпам feature-profile
- D. antisпам UTM policy

**Answer:** A

**Explanation:**

user@host# set security utm custom-objects url-pattern url-pattern-name <https://www.juniper.net/documentation/us/en/software/junos/utm/topics/topic-map/security-local-list-antisпам-f>

**NEW QUESTION 10**

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 10**

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 12

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 15

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 20

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 21

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 25

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 29

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 34

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 36

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 38

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 41

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 45

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 50

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 51

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 56

.....

## Relate Links

**100% Pass Your JN0-231 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/JN0-231-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>