

## Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

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



#### 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

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

What is the default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel?

- A. 20 seconds
- B. 5 seconds
- C. 10 seconds
- D. 40 seconds

**Answer:** B

#### Explanation:

The default value of the dead peer detection (DPD) interval for an IPsec VPN tunnel is 5 seconds. DPD is a mechanism that enables the IPsec device to detect if the peer is still reachable or if the IPsec VPN tunnel is still active. The DPD interval determines how often the IPsec device sends DPD packets to the peer to check the status of the VPN tunnel. A value of 5 seconds is a common default, but the specific value can vary depending on the IPsec device and its configuration.

#### NEW QUESTION 5

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 6

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

#### NEW QUESTION 9

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 10

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 10

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)

[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 14

You are assigned a project to configure SRX Series devices to allow connections to your webservers. The webservers have a private IP address, and the packets must use NAT to be accessible from the Internet. The webservers 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 18

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 19

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 24

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)

[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 25

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 28

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 33

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 35

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 40

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 43

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 48

Which two statements are correct about global policies? (Choose two.)

- A. Global policies are evaluated after default policies.
- B. Global policies do not have to reference zone context.
- C. Global policies are evaluated before default policies.
- D. Global policies must reference zone contexts.

**Answer:** BC

#### Explanation:

Global policies are used to define rules for traffic that is not associated with any particular zone. This type of policy is evaluated first, before any rules related to specific zones are evaluated.

For more detailed information about global policies, refer to the Juniper Networks Security Policy Overview guide, which can be found at

[https://www.juniper.net/documentation/en\\_US/junos/topics/reference/security-policy-overview.html](https://www.juniper.net/documentation/en_US/junos/topics/reference/security-policy-overview.html). The guide provides an overview of the Juniper Networks security policy architecture, as well as detailed descriptions of the different types of policies and how they are evaluated.

#### NEW QUESTION 52

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 54

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 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 61**

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 64**

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

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

**Answer:** C

**NEW QUESTION 66**

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 71**

.....

## 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 First Try
- \* JN0-231 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year