

Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)



NEW QUESTION 1

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 2

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 3

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 web server 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 4

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 5

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 6

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 7

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 8

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 9

Which IPsec protocol is used to encrypt the data payload?

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

Answer: A

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 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 13

You are asked to verify that a license for AppSecure is installed on an SRX Series device. In this scenario, which command will provide you with the required information?

- A. user@srx> show system license
- B. user@srx> show services accounting
- C. user@srx> show configuration system
- D. user@srx> show chassis firmware

Answer: A

NEW QUESTION 16

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 20

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 25

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. 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 27

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 32

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 33

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 sent 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 37

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 38

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 42

In J-Web, the management and loopback address configuration option allows you to configure which area?

- A. the IP address of the primary Gigabit Ethernet port
- B. the IP address of the Network Time Protocol server
- C. the CIDR address
- D. the IP address of the device management port

Answer: D

Explanation:

J-Web is a web-based interface for configuring and managing Juniper devices. The management and loopback address configuration option in J-Web allows you to configure the IP address of the device management port, which is used to remotely access and manage the device.

NEW QUESTION 46

.....

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](#)