



Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

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

Which two statements are correct about functional zones? (Choose two.)

- A. Functional zones must have a user-defined name.
- B. Functional zone cannot be referenced in security policies or pass transit traffic.
- C. Multiple types of functional zones can be defined by the user.
- D. Functional zones are used for out-of-band device management.

Answer: BD

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 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 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 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 7

An application firewall processes the first packet in a session for which the application has not yet been identified. In this scenario, which action does the application firewall take on the packet?

- A. It allows the first packet.
- B. It denies the first packet and sends an error message to the user.
- C. It denies the first packet.
- D. It holds the first packet until the application is identified.

Answer: D

Explanation:

This is necessary to ensure that the application firewall can properly identify the application and the correct security policies can be applied before allowing any traffic to pass through.

If the first packet was allowed to pass without first being identified, then the application firewall would not know which security policies to apply - and this could potentially lead to security vulnerabilities or breaches. So it's important that the first packet is held until the application is identified.

NEW QUESTION 8

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 9

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 10

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 webserver 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 10

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 14

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

NEW QUESTION 18

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 20

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 21

Which two IKE Phase 1 configuration options must match on both peers to successfully establish a tunnel? (Choose two.)

- A. VPN name
- B. gateway interfaces
- C. IKE mode
- D. Diffie-Hellman group

Answer: CD

NEW QUESTION 23

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 27

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 30

Click the Exhibit button.

```
user@vSRX-VR> ping 10.10.102.10 count 5 routing-instance DMZ
PING 10.10.102.10 (10.10.102.10): 56 data bytes
64 bytes from 10.10.102.10: icmp_seq=0 ttl=64 time=0.037 ms
64 bytes from 10.10.102.10: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 10.10.102.10: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 10.10.102.10: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 10.10.102.10: icmp_seq=4 ttl=64 time=0.070 ms
--- 10.10.102.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.037/0.051/0.070/0.011 ms
user@vSRX-VR>
```

Referring to the exhibit, which two statements are correct about the ping command? (Choose two.)

- A. The DMZ routing-instance is the source.
- B. The 10.10.102.10 IP address is the source.
- C. The 10.10.102.10 IP address is the destination.
- D. The DMZ routing-instance is the destination.

Answer: AC

NEW QUESTION 35

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 37

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 42

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 44

.....

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](#)