Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

NEW QUESTION 1
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 2
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 3
You have configured a UTM feature profile.
Which two additional configuration steps are required for your UTM feature profile to take effect? (Choose two.)

A. Associate the UTM policy with an address book.
B. Associate the UTM policy with a firewall filter.
C. Associate the UTM policy with a security policy.
D. Associate the UTM feature profile with a UTM policy.

Answer: CD

Explanation:
For the UTM feature profile to take effect, it must be associated with a security policy and a UTM policy. The security policy defines the traffic flow and the actions that should be taken on the traffic, while the UTM policy defines the security features to be applied to the traffic, such as antivirus, intrusion prevention, and web filtering. The UTM feature profile provides the necessary configuration for the security features defined in the UTM policy.

NEW QUESTION 4
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 5
Which order is correct for Junos security devices that examine policies for transit traffic?

A. zone policies global policies default policies
B. default policies zone policies global policies
C. default policies global policies zone policies
D. global policies zone policies default policies

Answer: A

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 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 8
When configuring antispam, where do you apply any local lists that are configured?

A. custom objects
B. advanced security policy
C. antispam feature-profile
D. antispam 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-antispam-f

NEW QUESTION 9
Which statement is correct about Web filtering?

A. The Juniper Enhanced Web Filtering solution requires a locally managed server.
B. The decision to permit or deny is based on the body content of an HTTP packet.
C. The decision to permit or deny is based on the category to which a URL belongs.
D. The client can receive an e-mail notification when traffic is blocked.

Answer: C

Explanation:
Web filtering is a feature that allows administrators to control access to websites by categorizing URLs into different categories such as gambling, social networking, or adult content. The decision to permit or deny access to a website is based on the category to which a URL belongs. This is done by comparing the URL against a database of categorized websites and making a decision based on the policy defined by the administrator.

NEW QUESTION 10
What are two logical properties of an interface? (Choose two.)

A. link mode
B. IP address
C. VLAN ID
D. link speed

Answer: BC

Explanation:
https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/securi

NEW QUESTION 11
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 12
What is an IP addressing requirement for an IPsec VPN using main mode?

A. One peer must have dynamic IP addressing.
B. One peer must have static IP addressing.
C. Both peers must have dynamic IP addresses.
D. Both peers must have static IP addressing.

Answer: D

NEW QUESTION 13
Which two statements are correct about the null zone on an SRX Series device? (Choose two.)

A. The null zone is created by default.
B. The null zone is a functional security zone.
C. Traffic sent or received by an interface in the null zone is discarded.
D. You must enable the null zone before you can place interfaces into it.

Answer: AC

Explanation:
According to the Juniper SRX Series Services Guide, the null zone is a predefined security zone that is created on the SRX Series device when it is booted. Traffic that is sent to or received on an interface in the null zone is discarded. The null zone is not a functional security zone, so you cannot enable or disable it.

NEW QUESTION 14
Your company is adding IP cameras to your facility to increase physical security. You are asked to help protect these loT devices from becoming zombies in a DDoS attack.
Which Juniper ATP feature should you configure to accomplish this task?

A. IPsec
B. static NAT
C. allowlists
D. C&C feeds

Answer: D

Explanation:
Juniper ATP should be configured with C&C feeds that contain lists of malicious domains and IP addresses in order to prevent IP cameras from becoming zombies in a DDoS attack.
This is an important step to ensure that the IP cameras are protected from malicious requests - and thus, they will not be able to be used in any DDoS attacks against the facility.

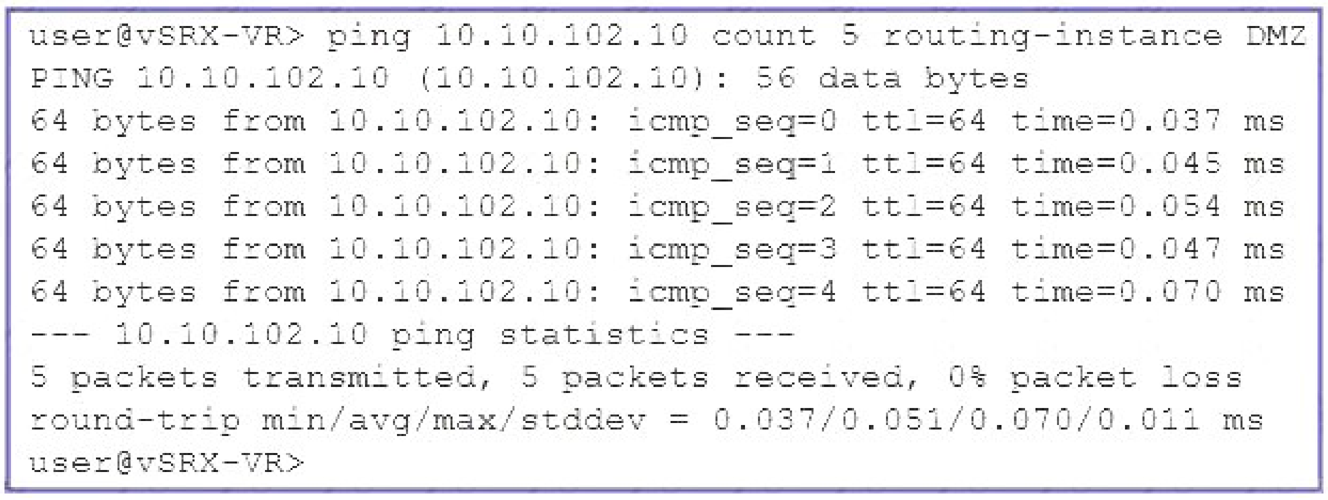
NEW QUESTION 15
What are two valid address books? (Choose two.)

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 16
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 17
What does the number “2” indicate in interface ge-0/1/2?

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

Answer: D

NEW QUESTION 18
Which two components are part of a security zone? (Choose two.)

A. inet.0
B. fxp0
C. address book
D. ge-0/0/0.0

Answer: BD

NEW QUESTION 19
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 20
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 21
......