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
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.

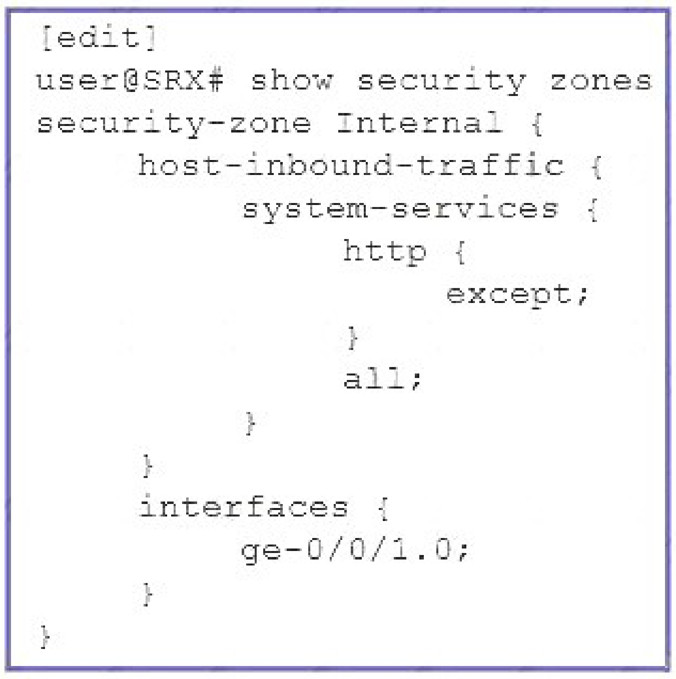
NEW QUESTION 4
What are two Juniper ATP Cloud feed analysis components? (Choose two.)

A. IDP signature feed
B. C&C cloud feed
C. infected host cloud feed
D. US CERT threat feed

Answer: AB

Explanation:
The Juniper ATP Cloud feed analysis components are the IDP signature feed and the C&C cloud feed. The IDP signature feed provides a database of signatures from known malicious traffic, while the C&C cloud feed provides the IP addresses of known command and control servers. The infected host cloud feed and US CERT threat feed are not components of the Juniper ATP Cloud feed analysis.
To learn more about the Juniper ATP Cloud feed analysis components, refer to the Juniper Networks Security Automation and Orchestration (SAO) official documentation, which can be found at https://www.juniper.net/documentation/en_US/sao/topics/concept/security-automation-and-orchestration-overvi
The documentation provides an overview of the SAO platform and an in-depth look at the various components of the Juniper ATP Cloud feed analysis.

NEW QUESTION 5
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 6
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 7
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 8
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 9
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 10
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

NEW QUESTION 10
You are investigating a communication problem between two hosts and have opened a session on the SRX Series device closest to one of the hosts and entered the show security flow session command.
What information will this command provide? (Choose two.)

A. The total active time of the session.
B. The end-to-end data path that the packets are taking.
C. The IP address of the host that initiates the session.
D. The security policy name that is controlling the session.

Answer: CD

NEW QUESTION 12
You want to provide remote access to an internal development environment for 10 remote developers.
Which two components are required to implement Juniper Secure Connect to satisfy this requirement? (Choose two.)

A. an additional license for an SRX Series device
B. Juniper Secure Connect client software
C. an SRX Series device with an SPC3 services card
D. Marvis virtual network assistant

Answer: AB

NEW QUESTION 17
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. You do not want the webservers 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 22
Which statement is correct about static NAT?

A. Static NAT supports port translation.
B. Static NAT rules are evaluated after source NAT rules.
C. Static NAT implements unidirectional one-to-one mappings.
D. Static NAT implements unidirectional one-to-many mappings.

Answer: C

Explanation:
Static NAT (Network Address Translation) is a type of NAT that maps a public IP address to a private IP address. With static NAT, a one-to-one mapping is created between a public IP address and a private IP address. This means that a single public IP address is mapped to a single private IP address, and all incoming traffic to the public IP address is forwarded to the private IP address.

NEW QUESTION 26
You are deploying an SRX Series firewall with multiple NAT scenarios. In this situation, which NAT scenario takes priority?

A. interface NAT
B. source NAT
C. static NAT
D. destination NAT

Answer: A

Explanation:
This is because the interface NAT would allow the connections to pass through the firewall - and thus, would ensure that the appropriate ports are open in order to allow for the connections to be established.
This is a really important step in order to ensure that all of the appropriate traffic is allowed through the SRX Series firewall - and thus, it must be a priority when deploying the firewall.

NEW QUESTION 27
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 31
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 33
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

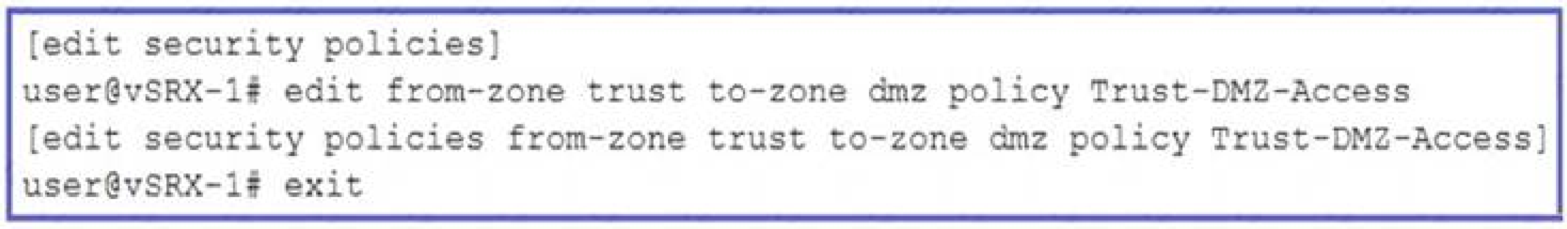
Explanation:
Juniper ATP Cloud is a cloud-based ATP subscription that delivers advanced threat protection services, such as URL categorization, file reputation analysis, and malware analysis. It is able to quickly and accurately categorize URLs and other web content, and can also provide detailed reporting 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 34
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 39
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 43
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 48
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 50
Corporate security requests that you implement a policy to block all POP3 traffic from traversing the Internet firewall.
In this scenario, which security feature would you use to satisfy this request?

A. antivirus
B. Web filtering
C. content filtering
D. antispam

Answer: C

NEW QUESTION 53
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 55
Which IPsec protocol is used to encrypt the data payload?

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

Answer: A

NEW QUESTION 58
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 60
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 63
Which statement about NAT is correct?

A. Destination NAT takes precedence over static NAT.
B. Source NAT is processed before security policy lookup.
C. Static NAT is processed after forwarding lookup.
D. Static NAT takes precedence over destination NAT.

Answer: D

NEW QUESTION 64
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 68
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 70
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 72
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 74
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 75
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 77
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 81
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 84
What is the order in which malware is detected and analyzed?

A. antivirus scanning –> cache lookup –> dynamic analysis –> static analysis
B. cache lookup –> antivirus scanning –> static analysis –> dynamic analysis
C. antivirus scanning –> cache lookup –> static analysis –> dynamic analysis
D. cache lookup –> static analysis –> dynamic analysis –> antivirus scanning

Answer: B

NEW QUESTION 87
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 90
You are configuring an SRX Series device. You have a set of servers inside your private network that need one-to-one mappings to public IP addresses.
Which NAT configuration is appropriate in this scenario?

A. source NAT with PAT
B. destination NAT

C. NAT-T
D. static NAT

Answer: D

Explanation:
https://www.juniper.net/documentation/en_US/day-one-books/nat-and-pat-en.html
And the specific text that would support the above answer is as follows: "Static NAT, which requires manual configuration, is often the most appropriate configuration for mapping one internal address to one external address."

NEW QUESTION 93
Which two traffic types are considered exception traffic and require some form of special handling by the PFE? (Choose two.)

A. SSH sessions
B. ICMP reply messages
C. HTTP sessions
D. traceroute packets

Answer: BD

NEW QUESTION 95
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 send 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 98
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

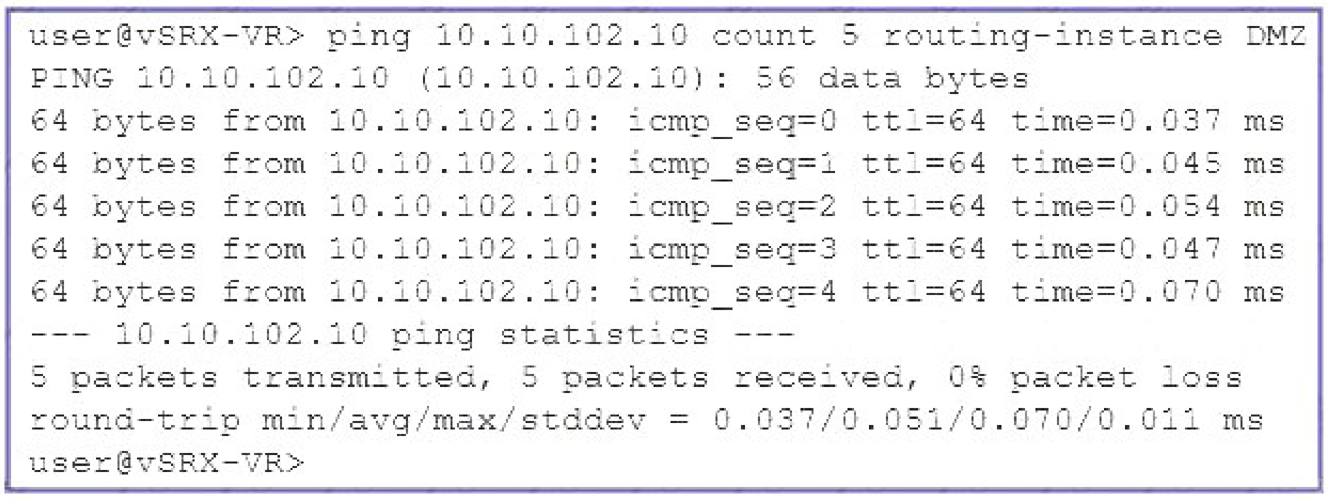
NEW QUESTION 101
Which two statements are correct about IPsec security associations? (Choose two.)

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 103
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 106
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 111
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 113
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 118
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 120
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 123

......