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
What is the correct order in which interface names should be identified?

A. system slot number –> interface media type –> port number –> line card slot number
B. system slot number –> port number –> interface media type –> line card slot number
C. interface media type –> system slot number –> line card slot number –> port number
D. interface media type –> port number –> system slot number –> line card slot number

Answer: C

NEW QUESTION 3
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 4
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 5
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 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
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 8
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 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
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 10
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 11
You need to collect the serial number of an SRX Series device to replace it. Which command will accomplish this task?

A. show chassis hardware
B. show system information
C. show chassis firmware
D. show chassis environment

Answer: A

Explanation:
The correct command to collect the serial number of an SRX Series device is the show chassis hardware command [1]. This command will return the serial number of the device, along with other information about the device such as the model number, part number, and version.
This command is available in Junos OS. More information about the show chassis hardware command can be found in the Juniper Networks technical documentation here [1]: https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-chassis-hardwa

NEW QUESTION 15
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 19
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 21
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 25
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 29
You are creating Ipsec connections.
In this scenario, which two statements are correct about proxy IDs? (Choose two.)

A. Proxy IDs are used to configure traffic selectors.
B. Proxy IDs are optional for Phase 2 session establishment.
C. Proxy IDs must match for Phase 2 session establishment.

D. Proxy IDs default to 0.0.0.0/0 for policy-based VPNs.

Answer: AB

NEW QUESTION 31
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 36
Which two security features inspect traffic at Layer 7? (Choose two.)

A. IPS/IDP
B. security zones
C. application firewall
D. integrated user firewall

Answer: AC

NEW QUESTION 38
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 40
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 42
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 46
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 49
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 IPsec protocol is used to encrypt the data payload?

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

Answer: A

NEW QUESTION 54
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 58
Which statement about global NAT address persistence is correct?

A. The same IP address from a source NAT pool will be assigned for all sessions from a given host.
B. The same IP address from a source NAT pool is not guaranteed to be assigned for all sessions from a given host.
C. The same IP address from a destination NAT pool will be assigned for all sessions for a given host.
D. The same IP address from a destination NAT pool is not guaranteed to be assigned for all sessions for a given host.

Answer: A

Explanation:
Use the persistent-nat feature to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address (the public IP address and port created by the NAT device closest to the STUN server). The source NAT rule action can use a source NAT pool (with or without port translation) or an egress interface.

NEW QUESTION 61
Which two statements are correct about screens? (Choose two.)

A. Screens process inbound packets.
B. Screens are processed on the routing engine.
C. Screens process outbound packets.
D. Screens are processed on the flow module.

Answer: AD

NEW QUESTION 65
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 67
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 72
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 77
Which statement is correct about Junos security policies?

A. Security policies enforce rules that should be applied to traffic transiting an SRX Series device.
B. Security policies determine which users are allowed to access an SRX Series device.
C. Security policies control the flow of internal traffic within an SRX Series device.
D. Security policies identity groups of users that have access to different features on an SRX Series device.

Answer: A

Explanation:
The correct statement about Junos security policies is that they enforce rules that should be applied to traffic transiting an SRX Series device. Security policies control the flow of traffic between different zones on the SRX Series device, and dictate which traffic is allowed or denied. They can also specify which application and service requests are allowed or blocked. More information about Junos security policies can be found in the Juniper Networks technical documentation here: https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/security-policies-overview.html.

NEW QUESTION 78
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 79
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 83
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 88
What is the order of the first path packet processing when a packet enters a device?

A. security policies –> screens –> zones
B. screens –> security policies –> zones
C. screens –> zones –> security policies
D. security policies –> zones –> screens

Answer: C

NEW QUESTION 92
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 96
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 99
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 104
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 106
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 108
Which two statements are correct about IKE security associations? (Choose two.)

A. IKE security associations are established during IKE Phase 1 negotiations.
B. IKE security associations are unidirectional.
C. IKE security associations are established during IKE Phase 2 negotiations.
D. IKE security associations are bidirectional.

Answer: AD

NEW QUESTION 111
SRX Series devices have a maximum of how many rollback configurations?

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

Answer: C

NEW QUESTION 116
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 117
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 118
You want to prevent other users from modifying or discarding your changes while you are also editing the configuration file.
In this scenario, which command would accomplish this task?

A. configure master
B. cli privileged
C. configure exclusive
D. configure

Answer: C

NEW QUESTION 119
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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 FirstTry

* JN0-231 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year