Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

https://www.2passeasy.com/dumps/JN0-231/

NEW QUESTION 1
Which three Web filtering deployment actions are supported by Junos? (Choose three.)

A. Use IPS.
B. Use local lists.
C. Use remote lists.
D. Use Websense Redirect.
E. Use Juniper Enhanced Web Filtering.

Answer: BDE

Explanation:
https://www.juniper.net/documentation/us/en/software/junos/utm/topics/concept/utm-web-filtering-overview.ht

NEW QUESTION 2
What are two characteristics of a null zone? (Choose two.)

A. The null zone is configured by the super user.
B. By default, all unassigned interfaces are placed in the null zone.
C. All ingress and egress traffic on an interface in a null zone is permitted.
D. When an interface is deleted from a zone, it is assigned back to the null zone.

Answer: BD

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
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 5
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 6
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 7
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 8
You are installing a new SRX Series device and you are only provided one IP address from your ISP. In this scenario, which NAT solution would you implement?

A. pool-based NAT with PAT
B. pool-based NAT with address shifting
C. interface-based source NAT
D. pool-based NAT without PAT

Answer: C

NEW QUESTION 9
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 10
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 10
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 12
What information does the show chassis routing-engine command provide?

A. chassis serial number
B. resource utilization
C. system version
D. routing tables

Answer: B

NEW QUESTION 16
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 19
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 24
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 25
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 26
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 28
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 32
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 37
Which IPsec protocol is used to encrypt the data payload?

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

Answer: A

NEW QUESTION 42
You are asked to configure your SRX Series device to block all traffic from certain countries. The solution must be automatically updated as IP prefixes become allocated to those certain countries.
Which Juniper ATP solution will accomplish this task?

A. Geo IP
B. unified security policies
C. IDP
D. C&C feed

Answer: A

Explanation:
Juniper ATP Geo IP can help to accomplish this task by using geolocation services to determine the geographical location of IP addresses. As IP prefixes get allocated to the countries that you have specified, the Geo IP solution will automatically update the configured firewall policies to block any traffic that is coming from those specific countries.
This is a great solution for blocking specific countries - as it will allow for a more personalized and targeted approach to firewall policies - and thus, to increase the effectiveness of the solution at blocking potential malicious traffic.

NEW QUESTION 44
You are monitoring an SRX Series device that has the factory-default configuration applied. In this scenario, where are log messages sent by default?

A. Junos Space Log Director
B. Junos Space Security Director
C. to a local syslog server on the management network
D. to a local log file named messages

Answer: C

NEW QUESTION 49
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 53
Which statement is correct about packet mode processing?

A. Packet mode enables session-based processing of incoming packets.
B. Packet mode works with NAT, VPNs, UTM, IDP, and other advanced security services.
C. Packet mode bypasses the flow module.
D. Packet mode is the basis for stateful processing.

Answer: C

NEW QUESTION 58
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 63
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 64
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 65
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 67
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 71
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 75
Which Juniper ATP feed provides a dynamic list of known botnet servers and known sources of malware downloads?

A. infected host cloud feed
B. Geo IP feed
C. C&C cloud feed
D. blocklist feed

Answer: A

NEW QUESTION 79
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 84
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

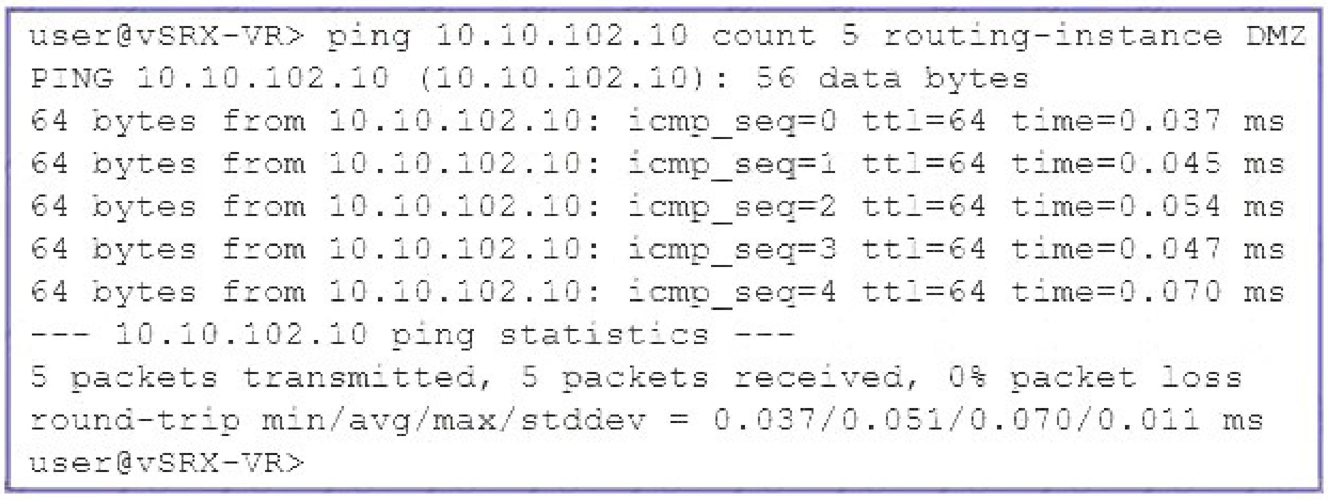
NEW QUESTION 87
Screens on an SRX Series device protect against which two types of threats? (Choose two.)

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 91
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 92
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 94
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 97
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 99
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 103
When transit traffic matches a security policy, which three actions are available? (Choose three.)

A. Allow
B. Discard
C. Deny
D. Reject
E. Permit

Answer: CDE

NEW QUESTION 106
What is the number of concurrent Secure Connect user licenses that an SRX Series device has by default?

A. 3
B. 4
C. 2
D. 5

Answer: C

Explanation:
The number of concurrent Secure Connect user licenses that an SRX Series device has by default is 2. Secure Connect is a feature of Juniper SRX Series devices that allows you to securely connect to remote networks via IPsec VPN tunnels. Each SRX Series device comes with two concurrent Secure Connect user licenses by default, meaning that it can support up to two simultaneous IPsec VPN connections. For more information, please refer to the Juniper Networks SRX Series Services Gateways Security Configuration Guide, which can be found on Juniper's website.

NEW QUESTION 109
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-W eb 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 110
......