Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

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

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
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
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
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 6
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 7
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 8
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 9

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
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 10
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 11
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 13
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 16

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 17
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 19
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 22
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 25
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 27
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 28
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 32
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 33
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 36
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 38
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 40
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 45
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 50
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 53
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 55
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 60
Which IPsec protocol is used to encrypt the data payload?

A. ESP
B. IKE
C. AH

D. TCP

Answer: A

NEW QUESTION 63
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 66
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 70
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 71
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 73
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 74
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 75
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 77
What is the default timeout value for TCP sessions on an SRX Series device?

A. 30 seconds
B. 60 minutes
C. 60 seconds
D. 30 minutes

Answer: D

Explanation:
By default, TCP has a 30-minute idle timeout, and UDP has a 60-second idle timeout. Additionally, known IP protocols have a 30-minute timeout, whereas unknown ones have a 60-second timeout. Setting the inactivity timeout is very useful, particularly if you are concerned about applications either timing out or remaining idle for too long and filling up the session table. According to the Juniper SRX Series Services Guide, this can be configured using the 'timeout inactive' statement for the security policy.

NEW QUESTION 78
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 83
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 85
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 90
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 92
SRX Series devices have a maximum of how many rollback configurations?

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

Answer: C

NEW QUESTION 95
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
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 107
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual JN0-231 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the JN0-231 Product From:

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

Money Back Guarantee

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