Juniper

Exam Questions JN0-231

Security - Associate (JNCIA-SEC)

NEW QUESTION 1
Which two statements are correct about functional zones? (Choose two.)

A. Functional zones must have a user-defined name.
B. Functional zone cannot be referenced in security policies or pass transit traffic.
C. Multiple types of functional zones can be defined by the user.
D. Functional zones are used for out-of-band device management.

Answer: BD

NEW QUESTION 2
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
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 5
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 6
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 7
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 8
Which two IPsec hashing algorithms are supported on an SRX Series device? (Choose two.)

A. SHA-1
B. SHAKE128
C. MD5
D. RIPEMD-256

Answer: AC

NEW QUESTION 9
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 10
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 13
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 15
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 16
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 19
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 21
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 25
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 30
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 32
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 37
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 38
.....

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