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
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 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
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 5
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 6
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 7
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 8
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 9
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 10
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 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 14
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 19
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 20
Which IPsec protocol is used to encrypt the data payload?

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

Answer: A

NEW QUESTION 22
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 25
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 29
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 33
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 36
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 41
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 45
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 47

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 50
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 53
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 55
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 58
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 59
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 64
......

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

100% Actual & Verified — Instant Download, Please Click
Order The JN0-231 Practice Test Here