

JN0-231 Dumps

Security - Associate (JNCIA-SEC)

<https://www.certleader.com/JN0-231-dumps.html>



NEW QUESTION 1

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 2

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 3

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 4

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 5

Which two components are configured for host inbound traffic? (Choose two.)

- A. zone
- B. logical interface
- C. physical interface
- D. routing instance

Answer: AB

NEW QUESTION 6

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 7

What are three primary match criteria used in a Junos security policy? (Choose three.)

- A. application
- B. source address
- C. source port
- D. class
- E. destination address

Answer: ABE

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 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 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 10

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 11

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 14

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 19

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 24

In this scenario, which two IP packets will match the criteria? (Choose two.)

- A. 192.168.1.21
- B. 192.168.0.1
- C. 192.168.1.12
- D. 192.168.22.12

Answer: CD

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 28

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 30

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 32

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 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 41

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 44

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 46

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 48

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 53

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 58

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 61

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 63

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 67

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 70

What is the order in which malware is detected and analyzed?

- A. antivirus scanning → cache lookup → dynamic analysis → static analysis
- B. cache lookup → antivirus scanning → static analysis → dynamic analysis
- C. antivirus scanning → cache lookup → static analysis → dynamic analysis
- D. cache lookup → static analysis → dynamic analysis → antivirus scanning

Answer: B

NEW QUESTION 71

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 74

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 79

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 80

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 83

What are two features of the Juniper ATP Cloud service? (Choose two.)

- A. sandbox
- B. malware detection
- C. EX Series device integration
- D. honeypot

Answer: AB

NEW QUESTION 86

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 91

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 92

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 96

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 100

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 104

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-Web 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 106

When creating a site-to-site VPN using the J-Web shown in the exhibit, which statement is correct?

- A. The remote gateway is configured automatically based on the local gateway settings.
- B. RIP, OSPF, and BGP are supported under Routing mode.
- C. The authentication method is pre-shared key or certificate based.
- D. Privately routable IP addresses are required.

Answer: D

NEW QUESTION 109

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your JN0-231 Exam with Our Prep Materials Via below:

<https://www.certleader.com/JN0-231-dumps.html>