

JN0-231 Dumps

Security - Associate (JNCIA-SEC)

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



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

You want to block executable files ("exe") from being downloaded onto your network. Which UTM feature would you use in this scenario?

- A. IPS
- B. Web filtering
- C. content filtering
- D. antivirus

Answer: B

Explanation:

According to the Juniper Networks official JNCIA-SEC Exam Guide, web filtering is a feature used to control access to web content, including the ability to block specific types of files.

In the scenario mentioned, you want to block executable files from being downloaded, which can be accomplished by using web filtering. The feature allows administrators to configure policies that block specific file types, including "exe" files, from being downloaded.

NEW QUESTION 3

What is the correct order in which interface names should be identified?

- A. system slot number → interface media type → port number → line card slot number
- B. system slot number → port number → interface media type → line card slot number
- C. interface media type → system slot number → line card slot number → port number
- D. interface media type → port number → system slot number → line card slot number

Answer: C

NEW QUESTION 4

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 5

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 6

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 7

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 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 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 10

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 10

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 13

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 18

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 23

You are assigned a project to configure SRX Series devices to allow connections to your web servers. The web servers have a private IP address, and the packets must use NAT to be accessible from the Internet. The web servers 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 24

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 29

When configuring antispam, where do you apply any local lists that are configured?

- A. custom objects
- B. advanced security policy
- C. antispam feature-profile
- D. antispam UTM policy

Answer: A

Explanation:

user@host# set security utm custom-objects url-pattern url-pattern-name <https://www.juniper.net/documentation/us/en/software/junos/utm/topics/topic-map/security-local-list-antispam-f>

NEW QUESTION 33

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 37

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 41

Which IPsec protocol is used to encrypt the data payload?

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

Answer: A

NEW QUESTION 44

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 45

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 47

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 49

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 52

Which two UTM features should be used for tracking productivity and corporate user behavior? (Choose two.)

- A. the content filtering UTM feature
- B. the antivirus UTM feature
- C. the Web filtering UTM feature
- D. the antispam UTM feature

Answer: AC

NEW QUESTION 53

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 55

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 58

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 62

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 63

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 67

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 72

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 76

Which two services does Juniper Connected Security provide? (Choose two.)

- A. protection against zero-day threats
- B. IPsec VPNs
- C. Layer 2 VPN tunnels
- D. inline malware blocking

Answer: AD

NEW QUESTION 79

Click the Exhibit button.

```

policies {
  from-zone untrust to-zone trust {
    policy permit-all {
      [...]
      then {
        permit;
      }
    }
    policy deny-all {
      [...]
      then {
        deny;
      }
    }
    policy reject-all {
      [...]
      then {
        reject;
      }
    }
  }
}

```

Which two statements are correct about the partial policies shown in the exhibit? (Choose two.)

- A. UDP traffic matched by the deny-all policy will be silently dropped.
- B. TCP traffic matched by the reject-all policy will have a TCP RST sent.
- C. TCP traffic matched from the zone trust is allowed by the permit-all policy.
- D. UDP traffic matched by the reject-all policy will be silently dropped.

Answer: AB

NEW QUESTION 84

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 87

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 90

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 93

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 98

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 102

SRX Series devices have a maximum of how many rollback configurations?

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

Answer: C

NEW QUESTION 106

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 108

.....

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>