Juniper

Exam Questions JN0-232

Security - Associate (JNCIA-SEC)

NEW QUESTION 1
You are not able to ping an interface on an SRX Series Firewall. Which two actions should you take to solve this issue? (Choose two.)

A. Assign the interface to a security zone.
B. Create a security policy to allow ping traffic.
C. Assign the interface to the null zone.
D. Configure the ICMP protocol for host-inbound-traffic.

Answer: AD

NEW QUESTION 2
Which two statements are correct about security zones? (Choose two.)

A. An interface can exist in multiple security zones.
B. Interfaces in the same security zone must share the same routing instance.
C. Interfaces in the same security zone must use separate routing instances.
D. A security zone can contain multiple interfaces.

Answer: BD

Explanation:
Option B:Correct. Interfaces in the same security zone must belong to the same routing instance; zones cannot span multiple routing instances.
Option D:Correct. A security zone can contain multiple interfaces, allowing grouping of similar trust levels (e.g., multiple LAN subnets in a trust zone).
Option A:Incorrect. An interface can belong to only one zone at a time.
Option C:Incorrect. Interfaces within the same zone cannot be split across routing instances.
Correct Statements:Interfaces in the same zone must share the same routing instance, and a zone can contain multiple interfaces.
[Reference:Juniper Networks –Security Zones and Routing Instances, Junos OS Security Fundamentals., ,]

NEW QUESTION 3
When does screening occur in the flow module?

A. before session lookup
B. during policy lookup
C. during route lookup
D. after session lookup

Answer: A

Explanation:
In Juniper SRX flow-based packet processing, theflow moduleis responsible for security functions such as screening, session management, NAT, and policy enforcement. The processing order is critical:
Screens are applied before any session lookup.This ensures that packets are inspected for anomalies, floods, or protocol violations before consuming resources for session management. Examples of these screens include TCP SYN flood protection, ICMP flood protection, and port scanning protection.
After screening, thesession lookupoccurs. At this point, the firewall checks whether the packet belongs to an existing session in the session table. If a matching session is found, the packet bypasses policy evaluation and is forwarded according to the session state.
If no existing session is found, the packet continues throughroute lookup, NAT processing, and security policy evaluationbefore a new session is created.
Thus,screening occurs before the session lookup, protecting the system early in the flow process. This design ensures efficiency by dropping malicious or malformed traffic before allocating session resources.
[Reference:Juniper Networks –SRX Series Services Gateways Security Processing (Flow Module Sequence), Junos OS Security Fundamentals, Official Course Guide., ,]

NEW QUESTION 4
Click the Exhibit button.

Exhibit

```
user@SRX> show security policies policy-name https-access detail
Policy: https-access, action-type: permit, services-offload:not-configured , State: enabled, Index: 9, Scope
Policy: 0
  Policy Type: Configured
  Sequence number: 1
  From zone: Trust, To zone: Untrust
  Source vrf group:
    any
  Destination vrf group:
    any
  Source addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Destination addresses:
    any-ipv4(global): 0.0.0.0/0
    any-ipv6(global): ::/0
  Application: junos-https
    IP protocol: tcp, ALG: 0, Inactivity timeout: 1800
      Source port range: [0-0]
      Destination ports: 443
  Source identity feeds:
    any
  Destination identity feeds:
    any
  Per policy TCP Options: SYN check: No, SEQ check: No, Window scale: No
  Session log: at-close
```

Referring to the exhibit, which two statements are correct? (Choose two.)

A. This security policy uses a non-default inactivity timeout.
B. This security policy is the second security policy in the list.
C. This security policy permits HTTPS traffic.
D. This security policy is a zone-based security policy.

Answer: AC

NEW QUESTION 5
Which two statements are correct about unified security policies? (Choose two.)

A. Traffic that matches a unified policy will not be evaluated by traditional security policy.
B. Dynamic applications in unified security policies analyze traffic based on Layer 4 information.
C. Traffic that matches a traditional policy will not be evaluated by unified security policy.
D. Dynamic applications in unified security policies analyze traffic based on Layer 7 information.

Answer: AD

NEW QUESTION 6
You are troubleshooting first path traffic not passing through an SRX Series Firewall. You have determined that the traffic is ingressing and egressing the correct interfaces using a route lookup.
In this scenario, what is the next step in troubleshooting why the device may be dropping the traffic?

A. Verify that the interfaces are in the correct security zones.
B. Verify the routing protocol being used.
C. Verify that source NAT is occurring.
D. Verify that the correct ALG is being used.

Answer: A

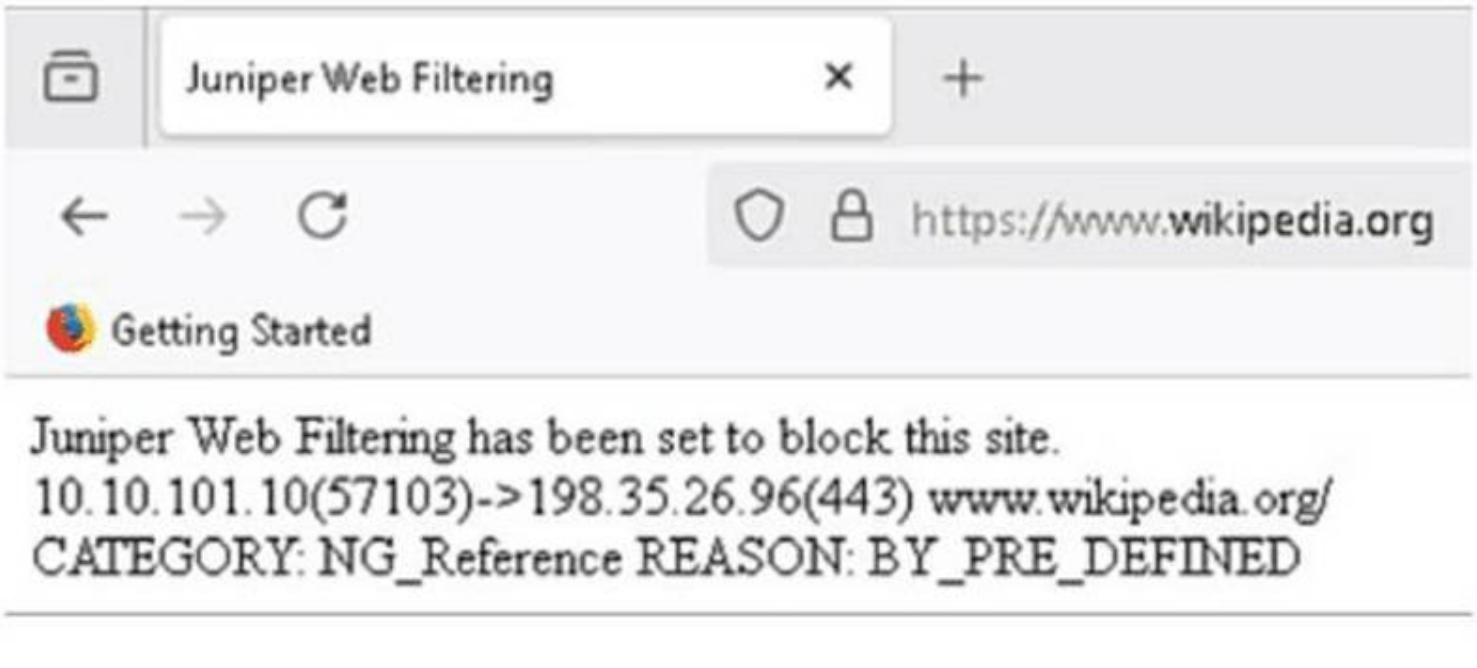
NEW QUESTION 7
You are asked to enable trace options to debug the packet flow.
In this scenario, which flag would you configure at the [edit security flow traceoptions] hierarchy?

A. packet-dump
B. general
C. state
D. basic-datapath

Answer: A

NEW QUESTION 8
Click the Exhibit button.

Exhibit



Referring to the exhibit, which two statements are correct? (Choose two.)

A. The URL matches a predefined Web filtering category.
B. The NextGen Web Filtering type is being used.
C. The SRX firewall does not have an SSL proxy configuration.
D. This is a custom Web filtering block message.

Answer: AB

NEW QUESTION 9
Which statement is correct about exception traffic?

A. Exception traffic is only handled on the Packet Forwarding Engine.
B. Exception traffic is rate-limited on the connection between the Packet Forwarding Engine and the Routing Engine.
C. Exception traffic is anything that is rejected by security policies and requires additional processing.
D. Exception traffic refers to malformed IP packets received on the Packet Forwarding Engine.

Answer: B

NEW QUESTION 10
What is transit traffic in the Junos OS?

A. It is traffic that is processed solely through the forwarding plane.
B. It is traffic that is rate-limited to prevent denial-of-service attacks.
C. It is traffic that is processed by the control plane.
D. It is traffic that requires special handling by the Routing Engine.

Answer: A

NEW QUESTION 10
Which two statements about SRX Series zones are correct? (Choose two.)

A. The null zone allows the use of security policies to log dropped control plane traffic.
B. The functional zone is used to define the management interface on smaller SRX Series Firewalls.
C. A security zone processes intra-zone traffic without a security policy.
D. The Junos-host zone allows the use of security policies to control access to the SRX Series Firewall.

Answer: CD

NEW QUESTION 12
Which security policy action will cause traffic to drop and a message to be sent to the source?

A. permit
B. next-policy
C. deny
D. reject

Answer: D

NEW QUESTION 16
Which two characteristics of destination NAT and static NAT are correct? (Choose two.)

A. Static NAT automatically creates a matching rule for the opposite direction.

B. Destination NAT requires address range sizes that match the devices being translated.
C. Static NAT uses Port Address Translation.
D. Destination NAT supports port forwarding.

Answer: AD

NEW QUESTION 18
Which two security policies are installed by default on SRX 300 Series Firewalls? (Choose two.)

A. a security policy to allow all traffic from the untrust zone to the trust zone
B. a security policy to allow all traffic from the trust zone to the untrust zone
C. a security policy to allow all traffic from the management zone to the trust zone
D. a security policy to allow all traffic from the trust zone to the trust zone

Answer: BD

NEW QUESTION 22
A new packet arrives on an interface on your SRX Series Firewall that is assigned to the trust security zone.
In this scenario, how does the SRX Series Firewall determine the egress security zone?

A. by performing a session lookup
B. by examining the destination port
C. by performing a route lookup
D. by examining the ingress security zone properties

Answer: C

NEW QUESTION 27
You want to verify the effectiveness of Web filtering on the SRX Series Firewall. How would you accomplish this task?

A. by installing a local NGWF server
B. by checking the file extensions of blocked content
C. by examining the content filtering policies
D. by attempting to access permitted or blocked URLs

Answer: D

Explanation:
The simplest and most direct method of verifying Web filtering effectiveness isto attempt to access permitted and blocked URLs.
Option A:Installing a local NGWF server is not required; NGWF queries Juniper??s cloud.
Option B:File extension checking applies to content filtering, not web filtering.
Option C:Examining policies shows configuration but does not verify enforcement.
Option D:Correct. Attempting to browse URLs that should be blocked or allowed confirms the Web filtering policy is effective.
Correct Method:Attempt to access permitted or blocked URLs
[Reference:Juniper Networks –Verifying Web Filtering Configuration, Junos OS Security Fundamentals.,]

NEW QUESTION 28
You want to enable NextGen Web Filtering in SRX Series devices.
In this scenario, which two actions will accomplish this task? (Choose two.)

A. Generate a CA-signed certificate.
B. Generate a self-signed certificate.
C. Configure an SSL initiation profile.
D. Configure an SSL proxy profile.

Answer: BD

NEW QUESTION 29
You have a situation where legitimate traffic is incorrectly identified as malicious by your screen options.
In this scenario, what should you do?

A. Enable all screen options.
B. Discard the traffic immediately.
C. Increase the sensitivity of the screen options.
D. Use the alarm-without-drop configuration parameter.

Answer: D

NEW QUESTION 33
Which two statements about management functional zones are correct? (Choose two.)

A. The management functional zone is used to control the management-related traffic that is allowed to access your device.
B. The management functional zone contains all available revenue ports until they are assigned to a user-defined security zone.
C. The management functional zone is automatically created on the SRX Series Firewalls.
D. The management functional zone cannot be referenced in any security policies.

Answer:

AC

NEW QUESTION 34
You want to use Avira Antivirus.
Which two actions should you perform to satisfy this requirement? (Choose two.)

A. Restart the management daemon (mgd) to load the components.
B. Enable the Avira engine in operational mode.
C. Reboot the SRX Series device to load the components.
D. Enable the Avira engine in configuration mode.

Answer: CD

Explanation:
The SRX Series devices support third-party antivirus scanning engines such asAvira. To use the Avira antivirus engine, administrators must explicitly enable the engine and ensure that the required components are properly loaded.
Enable in configuration mode:
The Avira antivirus engine must be enabled under UTM configuration mode. This step ensures the SRX device uses the Avira scanning engine for antivirus inspection.
Example:
set security utm feature-profile anti-virus avira-engine enable
Reboot the SRX device:
A system reboot is required after enabling the Avira engine to load the Avira antivirus components into memory.
Without a reboot, the Avira engine will not become active.
Why not the others?
Restarting themgdprocess (Option A) only reloads the management daemon and does not load antivirus engines.
Enabling inoperational mode(Option B) is not supported; the configuration must be applied in configuration mode.
Therefore, the correct actions to use Avira Antivirus are:Enable the Avira engine in configuration mode (Option D) and reboot the SRX device (Option C).
[Reference:Juniper Networks –Junos OS UTM and Antivirus Configuration, Junos OS Security Fundamentals, Official Course Guide.,]

NEW QUESTION 37
Which two statements about the host-inbound-traffic parameter in a zone configuration are correct? (Choose two.)

A. Deleting the host-inbound-traffic parameter blocks console access to the firewall.
B. Deleting the host-inbound-traffic parameter blocks SSH access to the firewall.
C. The host-inbound-traffic parameter is implicitly configured in the management zone.
D. The host-inbound-traffic parameter is explicitly configured in a security zone.

Answer: BD

NEW QUESTION 40
You are asked to reduce security configuration complexity on your external facing firewalls. You notice that a previous administrator included hundreds of private subnet NAT rules covering various RFC1918 addresses. You want to replace all these rules with a single rule covering all RFC1918 addresses.
Which rule would you use in this scenario?

A. set security nat source rule-set private-to-pub rule RFC1918 match source-address [10.0.0.0/8 192.168.0.0/16 172.16.0.0/12]
B. set security nat source rule-set private-to-pub rule RFC1918 match source-address [10.0.0.0/8 192.16.0.0/12 172.168.0.0/16]
C. set security nat source rule-set private-to-pub rule RFC1918 match source-address [10.0.0.0/8 172.168.0.0/16 192.0.2.0/24 203.1.113.0/24]
D. set security nat source rule-set private-to-pub rule RFC1918 match source-address [10.0.0.0/8 192.168.0.0/16 172.16.0.0/12 192.0.2.0/24]

Answer: A

NEW QUESTION 42
What are two ways that an SRX Series device identifies content? (Choose two.)

A. It identifies and inspects the file extension of each file.
B. It uses AppID.
C. It identifies file types in HTTP, FTP, and e-mail protocols.
D. It uses ALGs.

Answer: BC

NEW QUESTION 43
Which two statements are correct about NAT and security policy processing? (Choose two.)

A. The security policy is evaluated before destination NAT.
B. The security policy is evaluated after source NAT.
C. The security policy is evaluated before source NAT.
D. The security policy is evaluated after destination NAT.

Answer: BD

NEW QUESTION 45
Which two statements are correct about security zones and functional zones? (Choose two.)

A. Traffic entering an interface in a functional zone cannot exit any other transit interface.
B. Traffic entering transit interfaces can exit an interface in a functional zone.

C. Traffic entering an interface in a functional zone can exit any other transit interface.
D. Traffic entering transit interfaces cannot exit an interface in a functional zone.

Answer: AD

Explanation:
Functional zones(e.g., junos-host, management, null) are not used for forwarding transit traffic. They are used to manage traffic destined to or from the SRX device itself.
Option A:Correct. If traffic enters through a functional zone interface, it is meant for the SRX, not for transit, so it cannot exit another interface.
Option D:Correct. Transit interfaces handle forwarding traffic, but they cannot send that traffic out through a functional zone interface.
Option B and C:Incorrect, because functional zones are strictly control-plane, not transit forwarding zones.
Correct Statements:A and D
[Reference:Juniper Networks –Security Zones vs. Functional Zones, Junos OS Security Fundamentals.,]

NEW QUESTION 48
What is the purpose of assigning logical interfaces to separate security zones in Junos OS?

A. to simplify the configuration of network interfaces
B. to manage routing protocols and updates
C. to control traffic that traverses different VLANs using security policies
D. to enable network monitoring through SNMP

Answer: C

NEW QUESTION 50
Click the Exhibit button.

Exhibit

```
[edit security policies from-zone Trust to-zone Trust]
user@SRX# show
policy allow-all {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```

Which type of policy is shown in the exhibit?

A. global policy
B. inter-zone policy
C. intra-zone policy
D. default policy

Answer: C

NEW QUESTION 55
Which statement is correct about capturing transit packets on an SRX Series Firewall?

A. You can capture transit packets on the egress interface using a firewall filter.
B. You can capture transit packets by using a firewall filter on the loopback interface.
C. You can capture transit packets by using the tcpdump utility in the shell.
D. You can capture transit packets using sampling and port mirroring.

Answer: D

Explanation:
Transit traffic is defined as traffic that passesthroughthe SRX (not destined to the Routing Engine). To capture transit traffic:
Sampling and port mirroring (Option D)are the correct supported methods for capturing or exporting transit traffic. Sampling allows captured packets to be sent to a file or collector, while port mirroring sends a copy to a monitoring interface.
Option A:Firewall filters on an egress interface cannot directly capture packets; they can only count, accept, discard, or sample. Sampling itself is separate.
Option B:Loopback interface (lo0) is for control-plane traffic, not transit traffic.
Option C:tcpdump is not supported on SRX as a tool for capturing transit packets; the operational command monitor traffic interface is used, but sampling/port mirroring is the recommended scalable approach.
Correct Method:Sampling and port mirroring
[Reference:Juniper Networks –Traffic Monitoring and Troubleshooting, Junos OS Security Fundamentals.,]

NEW QUESTION 58
Content filtering supports which two of the following protocols? (Choose two.)

A. SMTP
B. SNMP
C. TFTP
D. HTTP

Answer: AD

Explanation:
Content filtering on SRX devices inspects and controls specific file types transferred across certain application protocols:
SMTP (Option A):Supported. Content filtering can block specific file attachments in emails.
HTTP (Option D):Supported. Content filtering can block downloads of specific file types over web traffic.
SNMP (Option B):Not supported; SNMP is a management protocol, not a content delivery protocol.
TFTP (Option C):Not supported by content filtering.
Correct Protocols:SMTP and HTTP
[Reference:Juniper Networks –Content Security and Filtering Supported Protocols, Junos OS Security Fundamentals.,]

NEW QUESTION 59
When a new traffic flow enters an SRX Series device, in which order are these processes performed?

A. screens ?? security policies ?? zones ?? routes
B. screens ?? routes ?? zones ?? security policies
C. routes ?? zones ?? screens ?? security policies
D. screens ?? zones ?? security policies ?? routes

Answer: B

Explanation:
The packet flow fornew trafficon SRX is processed in a defined order:
Screens (Option B, Step 1):Packets are first checked by screens for anomalies such as floods, malformed packets, or protocol violations.
Route Lookup (Step 2):The destination IP is checked in the routing table to determine the egress interface.
Zone Determination (Step 3):Once the ingress and egress interfaces are known, their associated zones are identified.
Security Policies (Step 4):With both zones determined, the packet is evaluated against the configured security policies.
Other options list incorrect sequences, either moving routing later or placing policies before zone determination, which is not possible.
Correct Processing Order:screens ?? routes ?? zones ?? security policies
[Reference:Juniper Networks –Packet Flow and Security Processing Order, Junos OS Security Fundamentals., ,]

NEW QUESTION 63
.....

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

JN0-232 Practice Exam Features:

* JN0-232 Questions and Answers Updated Frequently

* JN0-232 Practice Questions Verified by Expert Senior Certified Staff

* JN0-232 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* JN0-232 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year