Juniper JN0-232 JNCIA-SEC Practice Questions

Shared by Cox on 19-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which solution will add antivirus features to your SRX Series device?

Options:

A- IDP
B- Content Security
C- NAT
D- firewall filters

P2P exams

Answer:

B

Explanation:

Content Security is the Juniper solution that adds antivirus capabilities to SRX Series Firewalls. Juniper Content Security includes several UTM-style services, such as antivirus, antispam, content filtering, and web filtering. The antivirus feature scans supported traffic to detect and block malicious files or virus-related content according to configured profiles and policies. IDP provides intrusion detection and prevention signatures, but it is not the specific solution that adds antivirus scanning. NAT translates IP addresses and ports and has no antivirus function. Firewall filters provide stateless packet filtering and traffic classification, not file-based malware inspection. Therefore, Content Security is the correct answer for adding antivirus features to an SRX Series device.

P2P exams

Question 2

Question Type: MultipleChoice

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

Options:

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:

B, D

Explanation:

SSH Access (Option B): Host-inbound-traffic controls traffic destined to the SRX device itself (management/control plane). If host-inbound-traffic is not configured to allow SSH, then SSH access to the firewall is blocked.

Explicit Zone Configuration (Option D): For user-defined security zones, host-inbound-traffic must be explicitly configured to allow specific services (SSH, ICMP, SNMP, etc.).

Console Access (Option A): Console access is not controlled by host-inbound-traffic. Console access is always available directly.

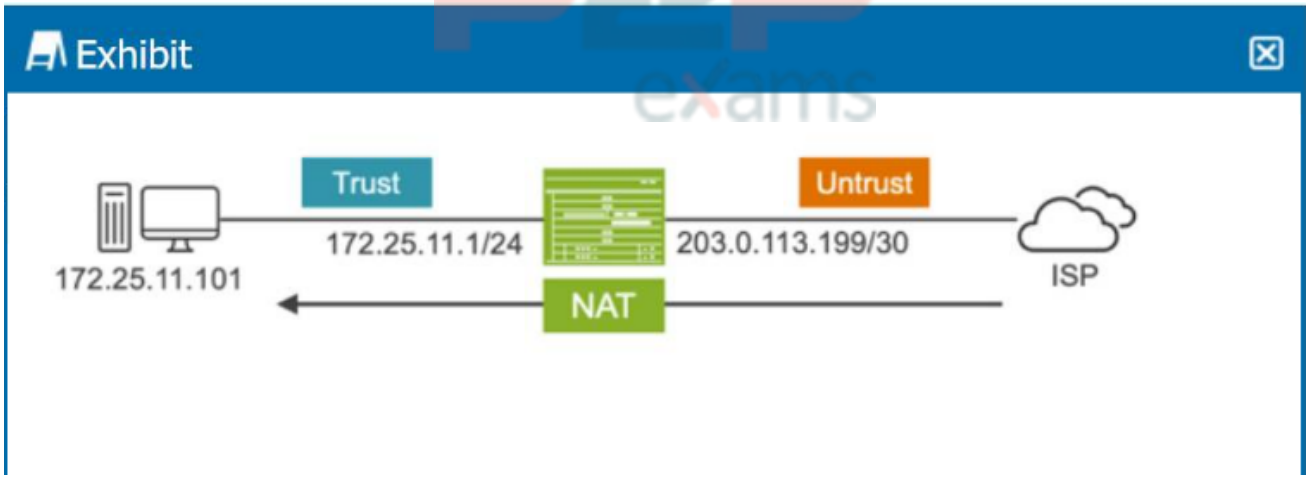
Management Zone (Option C): In the management functional zone, host-inbound-traffic is implicitly allowed for management services, so this is not explicitly required.

Correct Statements: B and D

Question 3

Question Type: MultipleChoice

Click the Exhibit button.



You must ensure that sessions can only be established from the external device. Referring to the exhibit, which type of NAT is being performed?

Options:

A- destination NAT only
B- source NAT only
C- static PAT only
D- static NAT and source NAT

Answer:

A

Explanation:

From the exhibit:

The internal host (172.25.11.101) is located in the Trust zone.

The external address (203.0.113.199/30) is used for communication with the ISP.

The requirement is that sessions can only be initiated from the external device (the ISP or untrust side) toward the internal host.

This requirement matches the behavior of Destination NAT:

Destination NAT only (Option A): Maps the external/public IP (203.0.113.199) to the internal/private IP (172.25.11.101). This allows inbound connections to be translated and sent to the internal host. The internal host cannot initiate outbound sessions, since the translation only applies to inbound traffic.

Source NAT only (Option B): Used for outbound sessions from internal private IPs to the Internet. This does not meet the requirement.

Static PAT (Option C): Maps a single port of a public IP to a private IP/port. The exhibit does not indicate a port-based translation.

Static NAT and source NAT (Option D): Would provide bidirectional communication, allowing sessions to be initiated in both directions. This contradicts the requirement.

Correct NAT Type: Destination NAT only

Question 4

Question Type: MultipleChoice

You want to show the effectiveness of your SRX Series Firewall content filter.

Which operational mode command would you use in this scenario?

Options:

A- show security utm anti-spam status
B- show security utm anti-virus status
C- show security web filtering status
D- show security utm content-filtering statistics

Answer:

D

P2P exams

Explanation:

To verify and demonstrate the effectiveness of content filtering on an SRX firewall, administrators use operational mode commands that display UTM statistics.

The command show security utm content-filtering statistics provides detailed counters showing how many connections were inspected, how many were blocked, and other related metrics.

This is the correct way to measure and demonstrate filtering effectiveness.

Commands in options A, B, and C provide status information for antispam, antivirus, and web filtering features, but they do not provide content filter effectiveness statistics.

Question 5

Question Type: MultipleChoice

P2P exams

Which statement about the flow module is correct in the context of destination NAT?

Options:

A- The flow module performs NAT during both first path and fast path processing.
B- The flow module performs NAT only for source IP addresses.
C- The flow module performs NAT only during fast path processing.
D- The flow module performs NAT only during first path processing.

Answer:

A

Explanation:

In SRX flow-based processing, the first packet of a new session goes through first path processing, where NAT rule lookup, route lookup, security policy evaluation, and session creation occur. Destination NAT is performed before security policy evaluation, so the translated destination address is used when matching the policy. After the session is created, later packets use fast path processing and follow the cached session information, including the NAT translation state created for the session. Therefore, the flow module is involved with NAT behavior in both first path and fast path processing. Option B is incorrect because destination NAT changes destination addresses, not only source addresses. Options C and D are incomplete because NAT lookup and session installation occur during first path, while established NAT translations are applied during fast path.

Question 6

Question Type: MultipleChoice

Referring to the exhibit, which two statements are correct about the traffic flow shown in the exhibit? (Choose two.)

```
user@SRX> show security flow session
Session ID: 264487, Policy name: dns/6, Timeout: 2, Session State: Valid
In: 10.20.30.40/53726 --> 203.0.113.1/53;udp, Conn Tag: 0x0, If: ge-0/0/4.0,
Pkts: 1, Bytes: 65,
Out: 203.0.113.1/53 --> 192.0.2.1/21423;udp, Conn Tag: 0x0, If: ge-0/0/3.0,
Pkts: 1, Bytes: 140,
```

Options:

A- There is no change to the original source IP address.
B- The original destination IP address was translated to a new destination IP address.
C- There is no change to the original destination IP address.
D- The original source IP address was translated to a new source IP address.

Answer:

C, D

Explanation:

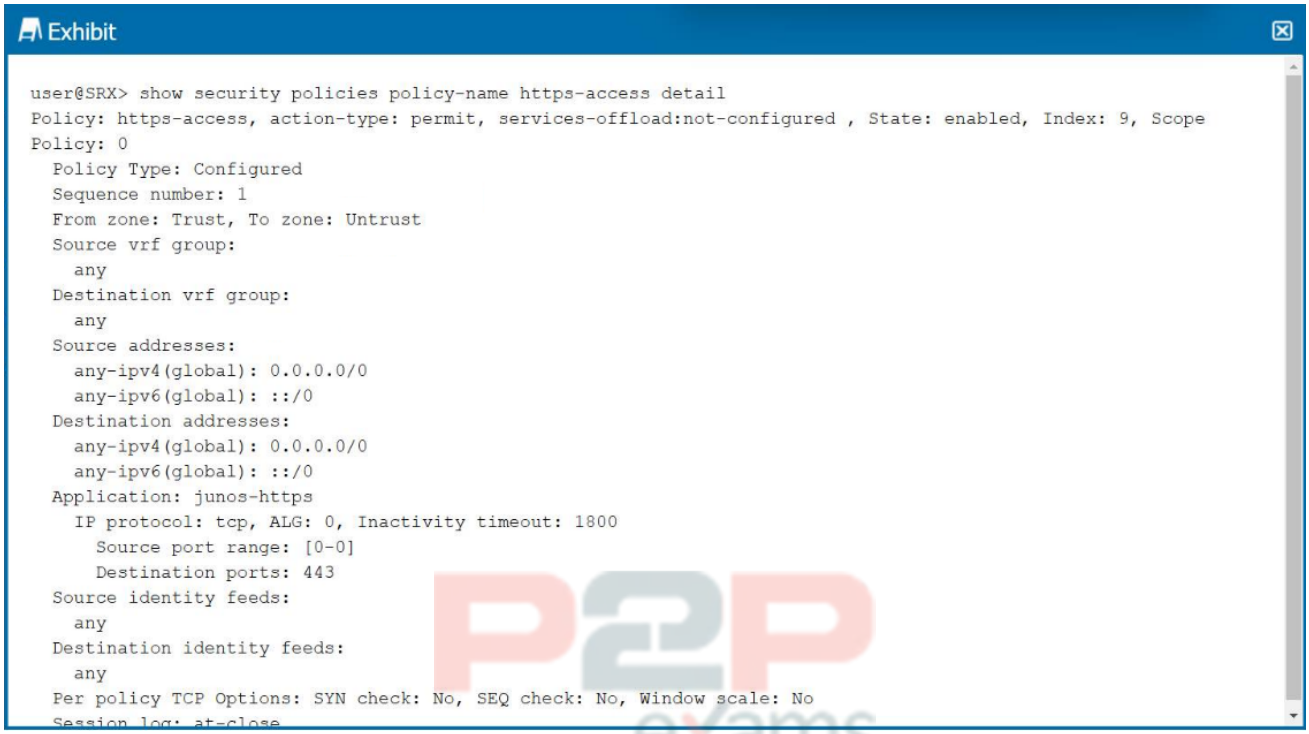
The session output shows the original flow entering with source address 10.20.30.40 and

destination address 203.0.113.1. The return or translated side shows the source address represented as 192.0.2.1 while the destination address remains 203.0.113.1. This indicates source NAT behavior because the original source IP address is translated to a new source IP address. There is no destination NAT in the exhibit because the destination IP address does not change. In Junos source NAT, the firewall translates the source address, commonly to an interface address or address pool, while preserving the destination address unless another NAT type is also configured. Therefore, the correct statements are that the destination remains unchanged and the source address is translated.

Question 7

Question Type: MultipleChoice

Click the Exhibit button.



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

Options:

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:

A, C

Explanation:

From the exhibit output:

Policy Information:

Policy: https-access, action-type: permit

From zone: Trust, To zone: Untrust

Application: junos-https

IP protocol: tcp, Destination port: 443

Inactivity timeout: 1800

Sequence number: 1

Analysis:

Option A: Correct. The default inactivity timeout for flow sessions is 60 seconds for TCP without activity. This policy shows an inactivity timeout of 1800 seconds, which is non-default.

Option B: Incorrect. The policy shows Sequence number: 1, which means it is the first policy, not the second.

Option C: Correct. The policy explicitly matches application junos-https (TCP port 443) and has an action of permit. Therefore, it allows HTTPS traffic.

Option D: Incorrect. This is clearly a zone-based policy, but the question asks for two correct statements. Between the four options, the explicitly correct ones are A and C.

Correct Statements: This security policy uses a non-default inactivity timeout, and this security policy permits HTTPS traffic.

Question 8

Question Type: MultipleChoice

Which two statements correctly describe static NAT? (Choose two.)

Options:

A- It requires address ranges of the same size.
B- Address pools are necessary.
C- No address pools are necessary.
D- It performs PAT.

Answer:

A, C

Explanation:

Static NAT creates a fixed one-to-one mapping between real and mapped addresses. Juniper documentation describes static NAT as mapping one IP subnet to another IP subnet and states that translation is limited to one-to-one mappings or address blocks of the same size. This makes option A correct. Juniper also states that no address pools are necessary for static NAT, which makes option C correct. Address pools are commonly associated with source NAT or destination NAT pool configurations, not the basic static NAT mapping model. Static NAT can support static port mapping in specific configurations, but the general static NAT behavior tested here is one-to-one address translation, not dynamic PAT. Therefore, the correct answers are A and C.

To Get Premium Files for JN0-232 Visit

https://www.p2pexams.com/products/jn0-232

For More Free Questions Visit

https://www.p2pexams.com/juniper/pdf/jn0-232

