Boost up Your Certification Score

# Juniper

## JN0-232

### Juniper Security, Associate




For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/jn0-232

# Latest Version: 6.1

## Question: 1

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, the flow module is 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, the session lookup occurs. 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 through route lookup, NAT processing, and security policy evaluation before 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.

## Question: 2

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: B, C**

Explanation:

SRX Series devices provide content security features that rely on advanced identification mechanisms. File identification is not based merely on file extensions (which can be easily spoofed), but instead on deep inspection techniques:
AppID (Application Identification): AppID is part of the AppSecure suite, allowing the device to classify applications and content regardless of port or protocol. This enables the SRX to detect applications and their related content for enforcement.
Protocol-based file type identification: The SRX can recognize and identify file types embedded within HTTP, FTP, and e-mail (SMTP, IMAP, POP3) protocols. This provides accurate content inspection and filtering, independent of file naming conventions.
Why not the others?
File extensions (Option A) are not reliable for content security, so SRX does not use them.
ALGs (Option D) are used for protocol handling, such as SIP or FTP control channels, not for content identification.

## Question: 3

You are troubleshooting traffic traversing the SRX Series Firewall and require detailed information showing how the flow module is handling the traffic.
How would you accomplish this task?

A. Review the flow session table.
B. Review the forwarding table.
C. Enable flow trace options.
D. Enable firewall filters.

**Answer: C**

Explanation:
When troubleshooting packet handling on an SRX Series device, administrators need to understand exactly how the flow module is processing traffic. The most effective tool for this is the flow traceoptions feature.
Flow traceoptions: Provides detailed per-packet trace information showing each processing step within the flow module. It reveals how traffic is evaluated against session tables, NAT rules, and security policies. This is the recommended method for in-depth troubleshooting.
Why not the others?
The flow session table (Option A) shows only active sessions and counters, not detailed step-by-step handling.
The forwarding table (Option B) relates to routing and forwarding decisions, not flow security processing.
Firewall filters (Option D) can match and log traffic but do not display detailed flow processing steps.
Therefore, the correct method to get detailed information about flow handling is to enable flow traceoptions.

## Question: 4

Click the Exhibit button.

Exhibit

| Security Policies from Trust Zone to Untrust Zone | | | |
|---|---|---|---|
| Src Addr | Dst Addr | Application | Action |
| 172.25.11.0/24 | 10.1.0.0/16 | ftp | deny |
| 172.25.11.0/24 | 10.1.0.0/16 | ssh | permit |
| 172.25.11.0/24 | 10.1.0.0/16 | https | permit |
| 172.25.11.0/24 | any | ping | permit |
| any | any | any | deny |

The exhibit shows a table representing security policies from the trust zone to the untrust zone. In this scenario, which two statements are correct? (Choose two.)

A. SSH requests from the source IP address of 172.25.11.10 are permitted to the destination IP address of 10.1.0.10.
B. Ping command requests from the source IP address of 172.25.11.100 are denied to the destination IP address of 10.1.0.10.
C. FTP requests from the source IP address of 10.1.0.10 are permitted to the destination IP address of 172.25.11.100.
D. FTP requests from the source IP address of 172.25.11.11 are denied to the destination IP address of 10.1.0.10.

**Answer: A, D**

Explanation:
Juniper SRX evaluates security policies sequentially from top to bottom. Once a policy match is found, no further policies are evaluated. In this exhibit:
First Policy (FTP, deny):
Source: 172.25.11.0/24
Destination: 10.1.0.0/16
Application: FTP
Action: deny
⇒ Any FTP traffic from 172.25.11.0/24 to 10.1.0.0/16 is denied.
Second Policy (SSH, permit):
Same source/destination but application = SSH
Action = permit
⇒ SSH traffic from 172.25.11.0/24 to 10.1.0.0/16 is permitted.
Third Policy (HTTPS, permit):
⇒ HTTPS from the same source/destination is permitted.

Fourth Policy (Ping, permit):
Source: 172.25.11.0/24 to any destination
Application: ping
Action: permit
⇒ ICMP echo requests (ping) from 172.25.11.0/24 to any destination are permitted.
Fifth Policy (any → any, deny):
⇒ Serves as a default deny all at the end.
Now checking each option:
Option A: SSH from 172.25.11.10 → 10.1.0.10 matches the SSH permit rule (second policy). ? Correct.
Option B: Ping from 172.25.11.100 → 10.1.0.10 matches the ping permit rule (fourth policy). This traffic is permitted, not denied. ? Incorrect.
Option C: FTP from 10.1.0.10 → 172.25.11.100 is reverse traffic (untrust to trust). The table applies only trust → untrust, so this policy does not apply. ? Incorrect.
Option D: FTP from 172.25.11.11 → 10.1.0.10 matches the first policy (FTP deny rule). ? Correct.
Correct Statements: A, D

## Question: 5

Which statement is correct about source NAT?

A. It translates MAC addresses to private IP addresses.
B. It translates private IP addresses to public IP addresses.
C. It performs bidirectional IP address translation.
D. It performs translation on ingress traffic only.

**Answer: B**

Explanation:
Source NAT (Network Address Translation) is used on SRX devices to allow hosts with private IP addresses to access external networks, such as the Internet. The SRX translates the private IP address of the source host into a public IP address before forwarding traffic toward the destination.
It does not translate MAC addresses (Option A).
NAT is unidirectional in this case: it specifically translates private-to-public in the outbound direction, while the reverse (return traffic) is handled automatically through the session table. It is not a bidirectional translation (Option C).
NAT processing occurs as part of the flow module, not limited only to ingress traffic (Option D).
Therefore, the correct statement is that source NAT translates private IP addresses to public IP addresses.

# Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

# FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

