Vendor: Juniper

Exam Code: JN0-232

Exam Name: Security, Associate (JNCIA-SEC)

Version: DEMO

QUESTION 1
You are troubleshooting traffic traversing the SRX Series Firewall and require detailed information showing how the flow module is handing the traffic.

How would you accomplish this task?

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

Answer: C
Explanation:
To obtain detailed, step-by-step information on how the SRX flow module is processing traffic, you enable flow trace options. This feature captures flow-level diagnostics, showing session creation, NAT, policy matches, and packet disposition, making it ideal for deep troubleshooting.

QUESTION 2
Referring to the exhibit, which statement is correct?

```
[edit security policies from-zone Trust to-zone Untrust]
user@SRX# show
policy policy1 {
    match {
        source-address any;
        destination-address any;
        application junos-http;
    }
    then {
        permit;
    }
}
policy policy2 {
    match {
        source-address any;
        destination-address any;
        application junos-https;
    }
    then {
        permit;
    }
}
policy policy3 {
    match {
        source-address any;
        destination-address any;
        application junos-http;
    }
    then {
        deny;
    }
}
```

A. `policy2` will be shadowed because it matches the same application as `policy1`.
B. `policy3` will be shadowed because it matches the same application as `policy1`.

C. `policy1` will be shadowed because it matches the same application as `policy3`.
D. None of the policies will be shadowed.

Answer: B
Explanation:
In Junos security policies, rules are evaluated sequentially from top to bottom, and once a match occurs, the subsequent policies are not checked. In the configuration shown, policy1 allows junos-http traffic, and policy3 also matches the same application (junos-http) but denies it. Because policy1 appears first and already permits this traffic, policy3 will never be evaluated for that same traffic type. Therefore, policy3 is shadowed by policy1.

QUESTION 3
Which two statements are correct about enabling the Avira Antivirus engine on an SRX Series Firewall? (Choose two.)

A. A license is required.
B. A license is not required.
C. A reboot is required.
D. A reboot is not required.

Answer: AD
Explanation:
The Avira Antivirus engine requires a valid license to be enabled and function on SRX Series Firewalls.

Enabling or switching to the Avira engine does not require a reboot; the change takes effect dynamically after committing the configuration.

QUESTION 4
Which statement is correct about exception traffic?

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

Answer: C
Explanation:
Exception traffic refers to packets that require special handling by the Routing Engine (RE) rather than being processed normally by the Packet Forwarding Engine (PFE). To protect the RE from overload, this traffic is rate-limited on the internal connection between the PFE and RE.

QUESTION 5
Which two products will allow security policy management on SRX Series devices? (Choose two.)

A. Juniper Mist
B. Security Director
C. JIMS
D. JSA

Answer: BC
Explanation:
Security Director is Juniper's centralized management platform for configuring and managing security policies across SRX Series devices.

JIMS (Juniper Identity Management Service) integrates with SRX devices to provide identity-based policy management, enabling policies that reference user or group identities.

QUESTION 6
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 trust 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 untrust zone to the trust zone
D. a security policy to allow all traffic from the management zone to the trust zone

Answer: AC
Explanation:
A policy allowing all traffic from the trust zone to the trust zone, permitting internal communication.

A policy allowing all traffic from the untrust zone to the trust zone, which is implicitly denied, does not exist by default - however, the second default policy allows all traffic within the same zone, such as intra-zone communication (trust-to-trust).

QUESTION 7
What are three requirements for creating a custom application? (Choose three.)

A. You must define the port number.
B. You must define the security policy.
C. You must define the application name.
D. You must define the source address.
E. You must define the protocol.

Answer: ACE
Explanation:
To create a custom application on an SRX Series Firewall, you must define:
- The port number, which specifies where the application listens or communicates.
- The application name, which uniquely identifies the custom application within the configuration.
- The protocol (such as TCP or UDP), which determines how traffic is handled and matched for that application.

QUESTION 8
When a new traffic flow enters an SRX Series device, in which order are these processes performed?

A. screens --> zones --> security policies --> routes
B. routes --> zones --> screens --> security policies
C. screens --> routes --> zones --> security policies
D. screens --> security policies --> zones --> routes

Answer: C
Explanation:
When a new traffic flow enters an SRX Series Firewall, the processing order is:
1. Screens – Detect and block malicious or abnormal packets.
2. Routes – Determine the forwarding path based on the routing table.
3. Zones – Identify the source and destination security zones.
4. Security Policies – Evaluate the defined policies to permit or deny the traffic.

QUESTION 9
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
Explanation:
Generate a self-signed certificate (or use a CA-signed one) to allow the SRX to decrypt and inspect SSL traffic for web filtering.

Configure an SSL proxy profile to enable SSL inspection, which is required for NextGen Web Filtering to identify and control encrypted web traffic.

QUESTION 10
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. This is a custom Web filtering block message.
D. The SRX firewall does not have an SSL proxy configuration.

Answer: AB
Explanation:
The block page shows CATEGORY: NG_Reference and REASON BY_PRE_DEFINED, indicating that the URL was matched and blocked based on a predefined Web filtering category.

The category name begins with NG_, which denotes a NextGen (NG) Web Filtering category, so the NextGen Web Filtering type is being used.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**