Vendor: Juniper

Exam Code: JN0-336

Exam Name: Security, Specialist (JNCIS-SEC)

Version: DEMO

QUESTION 1
You want to use user identity information to secure your network. Which two actions must you perform on your SRX Series Firewall to accomplish this task? (Choose two.)

A. Create security policies that include user identity configuration
B. Add user accounts to the Active Directory Domain Users group
C. Configure an identity provider on your SRX Series Firewall.
D. Add the user identity feature license to your SRX Series Firewall.

Answer: AC
Explanation:
To use user identity on the SRX, the firewall must be configured with an identity provider so it can obtain and map user login information, and security policies must reference user identity so traffic enforcement can be based on authenticated users or groups.

QUESTION 2
You are asked to onboard an SRX Series device to Junos Space Security Director, but it is not working. In this scenario, what are three areas that should be reviewed? (Choose three.)

A. chassis serial number
B. SSH port number
C. active security policies
D. authentication credentials
E. IP address

Answer: BDE
Explanation:
Successful onboarding requires the SRX to be reachable at the correct IP address, accessed through the proper SSH port, and authenticated with valid credentials so Security Director can connect and manage the device.

QUESTION 3
When creating an IPsec tunnel, which type of encryption uses public and private keys?

A. symmetric encryption
B. asymmetric encryption
C. DES encryption
D. AES encryption

Answer: B
Explanation:
Asymmetric encryption relies on a public and private key pair, which is used during IPsec key exchange operations such as IKE to securely establish shared keys between peers.

QUESTION 4
What is a function of the Juniper Identity Management Service?

A. encrypting user e-mail
B. logging malicious code sent through ingress and egress ports
C. encrypting network data traffic

D. maintaining a centralized authentication table

Answer: D
Explanation:
The Juniper Identity Management Service maintains centralized user-to-IP mapping information, allowing SRX devices to enforce security policies based on authenticated user identities rather than only IP addresses.

QUESTION 5
Which three different objects would be created, modified, cloned, and deleted in the Shared Objects workspace of Junos Space Security Director? (Choose three.)

A. geo IP
B. IP address
C. audit logs
D. policy enforcement groups
E. policy rules

Answer: ABD
Explanation:
In the Shared Objects workspace, administrators manage reusable objects such as geographic IP objects, IP address objects, and policy enforcement groups. These objects can be created, modified, cloned, and deleted for use across multiple policies and devices.

QUESTION 6
Which two services would an SRX Series device use to connect to an LDAP server for identity-aware security policies? (Choose two.)

A. Active Directory
B. TACACS+
C. RADIUS
D. JIMS

Answer: AD
Explanation:
Identity-aware policies can use Active Directory through LDAP for user information, and the SRX can also obtain user identity mappings from JIMS, which integrates with LDAP directories such as AD.

QUESTION 7
Using Junos Space Security Director, you want to configure a unique firewall policy for a specific SRX Series device. Which firewall policy rules you would satisfy the requirement?

A. all devices policy prerules
B. group policy prerules
C. device policy rules
D. all devices policy postrules

Answer: C
Explanation:
Device-specific policy rules apply only to the selected SRX device, allowing you to create a

unique firewall policy that does not affect any other devices managed by Security Director.

QUESTION 8
Which IDP action is also referred to as a silent discard?

A. no action
B. close client and server
C. ignore connection
D. drop packet

Answer: C
Explanation:
The ignore connection action silently discards traffic that matches the IDP rule without sending any reset or notification, which is why it is known as a silent discard.

QUESTION 9
What does the exhibit indicate when you have configured a single IPsec VPN on an SRX Series Firewall?

```
user@SRX> show security ipsec statistics
ESP Statistics:
 Encrypted bytes:              4424
 Decrypted bytes:              3581
 Encrypted packets:              19
 Decrypted packets:              17
AH Statistics:
 Input bytes:                     0
 Output bytes:                    0
 Input packets:                   0
 Output packets:                  0
Errors:
 AH authentication failures: 0, Replay errors: 0
 ESP authentication failures: 0, ESP decryption failures: 0
 Bad headers: 0, Bad trailers: 0
```

A. The IPsec VPN has encountered errors during packet transmission.
B. The IPsec VPN is established, and traffic is passing through.
C. The IPsec VPN is not established.
D. The IPsec VPN is established, but no traffic is passing through.

Answer: B
Explanation:
The statistics show both encrypted and decrypted packets with no authentication or decryption failures. This confirms that the tunnel is established and traffic is successfully passing through it.

QUESTION 10
Which two statements are correct about redundant fabric interfaces in a chassis cluster? (Choose two.)

A. fab0 and fab1 are located on both node0 and node1.
B. fab0 is located on node0, whereas fab1 is located on node1.
C. The media type must be the same for each redundant fabric interface.
D. The media type can be different for each redundant fabric interface.

Answer: AC
Explanation:
Each node contains both fabric interfaces (fab0 and fab1), providing redundancy for control and data synchronization. Both interfaces must use the same media type so that the fabric links remain compatible and stable across the cluster.

QUESTION 11
Which two statements accurately describe the role of hashing in VPNs? (Choose two.)

A. Hashing compresses data in VPN communications.
B. Hashing generates a fixed-size string of characters.
C. Hashing encrypts data to ensure confidentiality.
D. Hashing verifies that data has not been altered during transmission.

Answer: BD
Explanation:
Hashing produces a fixed-size output from input data and is used in VPNs to ensure data integrity by detecting any alteration during transmission.

QUESTION 12
What are two causes that end the processing of rules in IDP? (Choose two.)

A. when a rule is matched in the rule base with an action of close
B. when a terminal rule is matched in the rule base
C. when any rule is matched in the exempt rule base
D. when a rule is matched in the rule base with an action of ignore

Answer: BC
Explanation:
IDP rule processing stops when traffic matches a terminal rule, and it also stops when traffic matches an exempt rule, because exempt rules immediately exclude the traffic from further IDP inspection.

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**