Vendor: Juniper

Exam Code: JN0-637

Exam Name: Security, Professional (JNCIP-SEC)

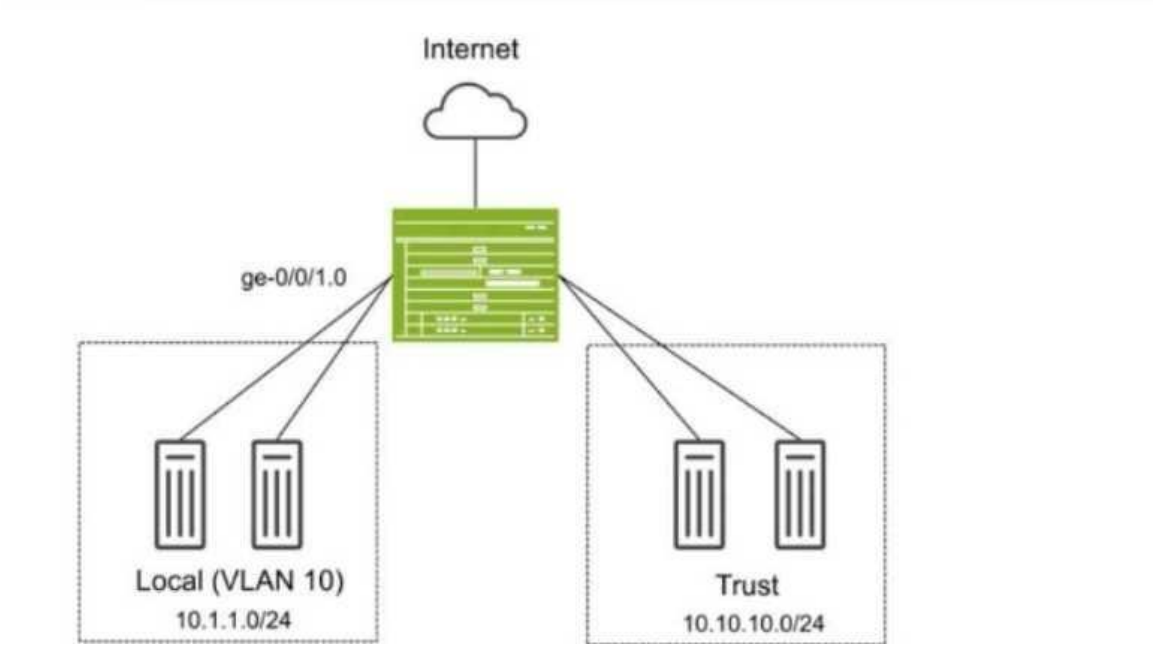
Version: DEMO

QUESTION 1
Which two statements are true about the procedures the Junos security device uses when handling traffic destined for the device itself? (Choose two.)

A. If the received packet is addressed to the ingress interface, then the device first performs a security policy evaluation for the junos-host zone.
B. If the received packet is destined for an interface other than the ingress interface, then the device performs a security policy evaluation for the junos-host zone.
C. If the received packet is addressed to the ingress interface, then the device first examines the host- inbound-traffic configuration for the ingress interface and zone.
D. If the received packet is destined for an interface other than the ingress interface, then the device performs a security policy evaluation based on the ingress and egress zone.

Answer: BC
Explanation:
When handling traffic that is destined for itself, the SRX examines the host-inbound-traffic configuration for the ingress interface and the associated security zone. It evaluates whether the traffic should be allowed based on this configuration. Traffic not addressed to the ingress interface is handled based on security policies within the junos-host zone, which applies to traffic directed to the SRX itself. For more details, refer to Juniper Host Inbound Traffic Documentation.
When handling traffic that is destined for the SRX device itself (also known as host-bound traffic), the SRX follows a specific process to evaluate the traffic and apply the appropriate security policies. The junos-host zone is a special security zone used for managing traffic destined for the device itself, such as management traffic (SSH, SNMP, etc.).

QUESTION 2
Exhibit:



You have deployed an SRX Series device as shown in the exhibit. The devices in the Local zone have recently been added, but their SRX interfaces have not been configured. You must configure the SRX to meet the following requirements:

Devices in the 10.1.1.0/24 network can communicate with other devices in the same network but not with other networks or the SRX.
You must be able to apply security policies to traffic flows between devices in the Local zone.
Which three configuration elements will be required as part of your configuration? (Choose three.)

A. set security zones security-zone Local interfaces ge-0/0/1.0
B. set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan-members 10
C. set protocols l2-learning global-mode switching
D. set protocols l2-learning global-mode transparent-bridge
E. set security zones security-zone Local interfaces irb.10

Answer: ABD
Explanation:
In this scenario, we need to configure the SRX Series device so that devices in the Local zone (VLAN 10, 10.1.1.0/24 network) can communicate with each other but not with other networks or the SRX itself. Additionally, you must be able to apply security policies to traffic flows between the devices in the Local zone.

QUESTION 3
Exhibit:

```
user@peer1> show chassis high-availability information
Node failure codes:
HW Hardware monitoring LB Loopback monitoring
MB Mbuf monitoring SP SPU monitoring
CS Cold Sync monitoring SU Software Upgrade
Node Status: ONLINE
Local-id: 1
Local-IP: 10.10.1.1
HA Peer Information:
Peer Id: 2 IP address: 10.10.1.2 Interface: ge-0/0/1.0
Routing Instance: default
Encrypted: NO Conn State: UP
Cold Sync Status: COMPLETE
Services Redundancy Group: 0
Current State: ONLINE
Peer Information:
Peer Id: 2
SRG failure event codes:
BF BFD monitoring
IP IP monitoring
IF Interface monitoring
CP Control Plane monitoring
Services Redundancy Group: 1
Deployment Type: SWITCHING
Status: ACTIVE
Activeness Priority: 200
Preemption: ENABLED
Process Packet In Backup State: NO
```

```
Control Plane State: READY
System Integrity Check: N/A
Failure Events: NONE
Peer Information:
Peer Id: 2
Status : BACKUP
Health Status: HEALTHY
Failover Readiness: READY
```

Referring to the exhibit, which statement is true?

A. SRG1 is configured in hybrid mode.
B. The ICL is encrypted.
C. If SRG1 moves to peer 2, peer 1 will drop packets sent to the SRG1 interfaces.
D. If SRG1 moves to peer 2, peer 1 will forward packets sent to the SRG1 interfaces.

Answer: D
Explanation:
The exhibit describes a Chassis Cluster configuration with high availability (HA) settings. The key information is related to Service Redundancy Group 1 (SRG1) and its failover behavior between the two peers.
In a typical SRX HA setup with active/backup configuration, if the SRG1 group moves to peer 2 (the backup), peer 1 (previously the active node) will forward packets to peer 2 instead of dropping them. This ensures smooth failover and seamless continuation of services without packet loss. This behavior is part of the active/backup failover process in SRX chassis clusters, where the standby peer takes over traffic processing without disruption.

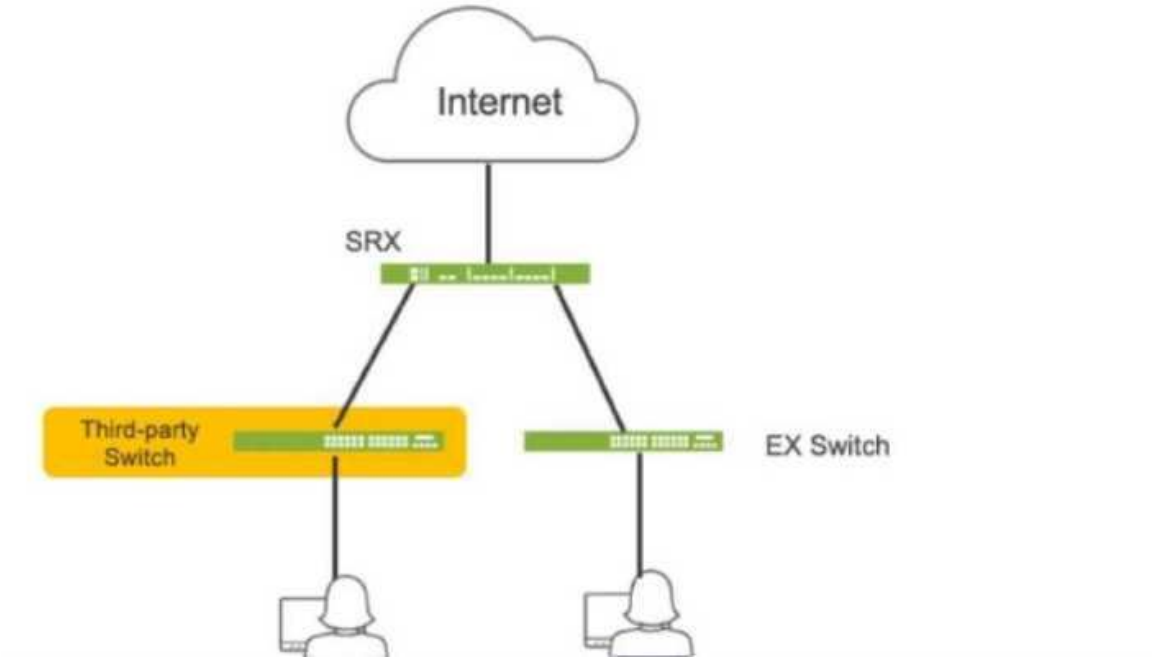
QUESTION 4
You are asked to create multiple virtual routers using a single SRX Series device. You must ensure that each virtual router maintains a unique copy of the routing protocol daemon (RPD) process.
Which solution will accomplish this task?

A. Secure wire
B. Tenant system
C. Transparent mode
D. Logical system

Answer: D
Explanation:
Logical systems on SRX Series devices allow the creation of separate virtual routers, each with its unique RPD process. This segmentation ensures that routing and security policies are isolated across different logical systems, effectively acting like independent routers within a single SRX device.
To create multiple virtual routers on a single SRX Series device, each with its own unique copy of the routing protocol daemon (RPD) process, you need to use logical systems. Logical systems allow for the segmentation of an SRX device into multiple virtual routers, each with independent configurations, including routing instances, policies, and protocol daemons.
A logical system on an SRX device enables you to create multiple virtual instances of the SRX, each operating independently with its own control plane and routing processes. Each logical system gets a separate copy of the RPD process, ensuring complete isolation between virtual

routers. This is the correct solution when you need separate routing instances with their own RPD processes on the same physical device.

QUESTION 5
Click the Exhibit button.



Referring to the exhibit, which three actions do you need to take to isolate the hosts at the switch port level if they become infected with malware? (Choose three.)

A. Enroll the SRX Series device with Juniper ATP Cloud.
B. Use a third-party connector.
C. Deploy Security Director with Policy Enforcer.
D. Configure AppTrack on the SRX Series device.
E. Deploy Juniper Secure Analytics.

Answer: ABC
Explanation:
A. Enroll the SRX Series device with Juniper ATP Cloud. This is essential for the SRX to receive threat intelligence from ATP Cloud, enabling it to identify infected hosts and take action.
B. Use a third-party connector. In this specific scenario, a third-party connector is required to integrate the SRX with the third-party switch. While Juniper has native integration for its EX switches, a connector is necessary to communicate with and manage the third-party switch.
C. Deploy Security Director with Policy Enforcer. Security Director orchestrates the automated response, and Policy Enforcer translates the policies into device-specific commands for the SRX and the third-party switch (via the connector).

QUESTION 6
You want to deploy two vSRX instances in different public cloud providers to provide redundant security services for your network. Layer 2 connectivity between the two vSRX instances is not

possible.
What would you configure on the vSRX instances to accomplish this task?

A. Chassis cluster
B. Secure wire
C. Multinode HA
D. Virtual chassis

Answer: C

QUESTION 7
You are asked to connect two hosts that are directly connected to an SRX Series device. The traffic should flow unchanged as it passes through the SRX, and routing or switch lookups should not be performed. However, the traffic should still be subjected to security policy checks.
What will provide this functionality?

A. MACsec
B. Mixed mode
C. Secure wire
D. Transparent mode

Answer: C
Explanation:
Secure wire mode on SRX devices allows traffic to flow transparently through the firewall without being routed or switched, while still applying security policies. This is ideal for scenarios where traffic inspection is required without altering the traffic path or performing additional routing decisions.
In this scenario, you want traffic to pass through the SRX unchanged (without routing or switching lookups) but still be subject to security policy checks. The best solution for this requirement is Secure Wire.
Secure Wire allows traffic to flow through the SRX without any Layer 3 routing or Layer 2 switching decisions. It effectively bridges two interfaces at Layer 2 while still applying security policies. This ensures that traffic remains unchanged, while security policies (such as firewall rules) can still be enforced.
This is an ideal solution when you need the SRX to act as a "bump in the wire" for security enforcement without changing the traffic or performing complex network lookups.

QUESTION 8
Which role does an SRX Series device play in a DS-Lite deployment?

A. Softwire concentrator
B. STUN server
C. STUN client
D. Softwire initiator

Answer: A

QUESTION 9
Which two statements are correct about the ICL in an active/active mode multinode HA environment? (Choose two.)

A. The ICL is strictly a Layer 2 interface.
B. The ICL uses a separate routing instance to communicate with remote multinode HA peers.
C. The ICL traffic can be encrypted.
D. The ICL is the local device management interface in a multinode HA environment.

Answer: BC

QUESTION 10
Exhibit:

Your company uses SRX Series devices to establish an IPsec VPN that connects Site-1 and the HQ networks. You want VoIP traffic to receive priority over data traffic when it is forwarded across the VPN.
Which three actions should you perform in this scenario? (Choose three.)

A. Enable next-hop tunnel binding.
B. Create a firewall filter that identifies VoIP traffic and associates it with the correct forwarding class.
C. Configure CoS forwarding classes and scheduling parameters.
D. Enable the copy-outer-dscp parameter so that DSCP header values are copied to the tunneled packets.
E. Enable the multi-sa parameter to enable two separate IPsec SAs for the VoIP and data traffic.

Answer: BCE

QUESTION 11
Your IPsec tunnel is configured with multiple security associations (SAs). Your SRX Series device supports the CoS-based IPsec VPNs with multiple IPsec SAs feature. You are asked to configure CoS for this tunnel.
Which two statements are true in this scenario? (Choose two.)

A. The local and remote gateways do not need the forwarding classes to be defined in the same order.
B. A maximum of four forwarding classes can be configured for a VPN with the multi-sa forwarding-classes statement.
C. The local and remote gateways must have the forwarding classes defined in the same order.
D. A maximum of eight forwarding classes can be configured for a VPN with the multi-sa forwarding-classes statement.

Answer: AD

QUESTION 12
The exhibit shows part of the flow session logs.

```
Mar  7 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT:<172.20.201.10/59009->10.0.1.129/22;6,0x0> matched filter
MatchTraffic:
Mar  7 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT: ge-0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Mar  7 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT: find flow: table 0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da
10.0.1.129, sp 59009, dp 22, proto 6, tok 9, conn-tag 0x00000000
Mar  7 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT:  no session found, start first path. in_tunnel - 0x0, from_cp_flag -
0
Mar  7 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT: flow_first_create_session
Mar  7 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT:  flow_first_in_dst_nat: in <ge-0/0/3.0>, out <N/A> dst_adr
10.0.1.129, sp 59009, dp 22
Mar  7 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT:  chose interface ge-0/0/4.0 as incoming nat if.
Mar  7 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
```

Which two statements are true in this scenario? (Choose two.)

A. The existing session is found in the table, and the fast path process begins.
B. This packet arrives on interface ge-0/0/4.0.
C. Junos captures a TCP packet from source address 172.20.101.10 destined to 10.0.1.129.
D. Destination NAT occurs.

Answer: BD

QUESTION 13
You have deployed automated threat mitigation using Security Director with Policy Enforcer, Juniper ATP Cloud, SRX Series devices, Forescout, and third-party switches. In this scenario, which device is responsible for communicating directly to the third-party switches when infected hosts need to be blocked?

A. Forescout
B. Policy Enforcer
C. Juniper ATP Cloud
D. SRX Series device

Answer: B
Explanation:
Policy Enforcer receives these policies and translates them into device-specific commands. It then communicates with the third-party switches (using protocols like SNMP, RADIUS, or vendor-specific APIs) to enforce those commands, such as blocking the infected hosts' MAC addresses or port access.
Centralized Enforcement: Policy Enforcer acts as the central point of enforcement for Security Director policies, ensuring consistent security across the network. Multi-Vendor Support: It can interact with a wide range of network devices, including switches from different vendors. Automation: Policy Enforcer automates the policy enforcement process, enabling rapid response to threats.

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**