Juniper JN0-637 JNCIP-SEC Practice Questions

Shared by King on 19-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In a multinode HA environment, which service must be configured to synchronize between nodes?

Options:

A- Advanced policy-based routing
B- PKI certificates
C- IPsec VPN
D- IDP

Answer:

B

Question 2

Question Type: MultipleChoice

You have configured the backup signal route IP for your multinode HA deployment, and the ICL link fails.

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

Options:

A- The current active node retains the active role.
B- The active node removes the active signal route.
C- The backup node changes the routing preference to the other node at its medium priority.
D- The active node keeps the active signal route.

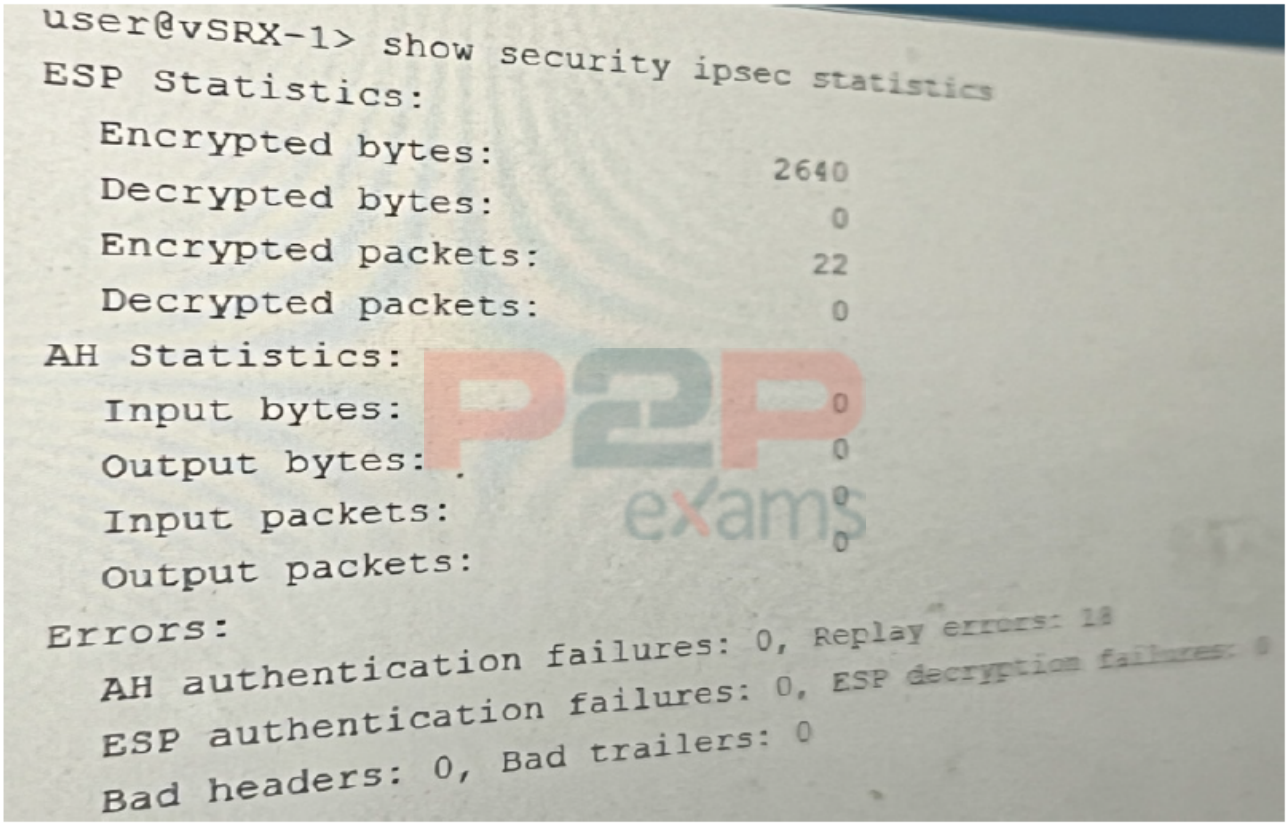
Answer:

A, C

Question 3

Question Type: MultipleChoice

Referring to the exhibit, which two statements are true ?



Options:

A- Every VPN packet that the SRX receives from the VPN peer is outside the ESP sequence window
B- The SRX is sending traffic into the tunnel and out toward the VPN peer.
C- The SRX is not sending any packets to the VPN peer.
D- The SRX is not receiving any packets from the VPN peer.

Answer:

B, D

Question 4

Question Type: MultipleChoice

Which two statements are correct about DNS doctoring?

Options:

A- The DNS ALG must be disabled.
B- Proxy ARP is required if your NAT pool for the server is on the same subnet as the uplink interface.
C- Proxy ARP is required if your NAT pool for the server is on a different subnet as the uplink interface
D- The DNS ALG must be enabled.

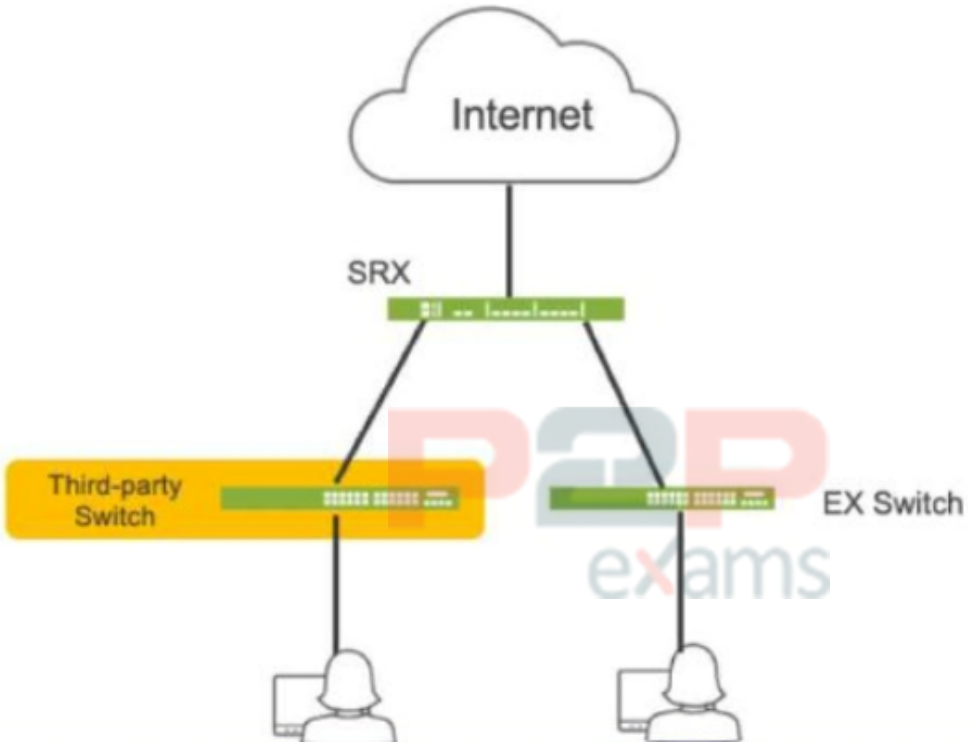
Answer:

B, D

Question 5

Question Type: MultipleChoice

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.)

Options:

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:

A, B, C

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

Question Type: MultipleChoice

You are deploying OSPF over IPsec with an SRX Series device and third-party device using GRE.

Which two statements are correct? (Select two.)

Options:

A- The GRE interface should use lo0 as endpoints.
B- The OSPF protocol must be enabled under the VPN zone.
C- Overlapping addresses are allowed between remote networks.
D- The GRE interface must be configured under the OSPF protocol.

Answer:

A, D

Explanation:

Comprehensive Detailed Step-by-Step Explanation with All Juniper Security Reference

Understanding the Scenario:

Objective: Deploy OSPF over IPsec between an SRX Series device and a third-party device using GRE tunnels.

Components Involved:

GRE (Generic Routing Encapsulation): Encapsulates packets to allow routing protocols like OSPF to run over IPsec tunnels.

IPsec: Provides security for the GRE tunnels.

OSPF: Dynamic routing protocol used over the GRE tunnel.

Option A: The GRE interface should use lo0 as endpoints.

Using the loopback interface (lo0) as the source and destination endpoints for GRE tunnels is a common best practice.

Advantages:

Stability: Loopback interfaces are always up, ensuring the GRE tunnel remains operational even if physical interfaces fail.

Reachability: Provides consistent endpoint IP addresses for GRE tunnels.

Configuration:

Assign IP addresses to lo0 interfaces on both devices.

Configure GRE tunnels to use these lo0 IP addresses as source and destination.

Juniper Networks Documentation:

'Using loopback interfaces as GRE tunnel endpoints ensures stability and consistent reachability for routing protocols over GRE tunnels.'

Source: Configuring GRE Tunnels

Option D: The GRE interface must be configured under the OSPF protocol.

To run OSPF over the GRE tunnel, the GRE interface must be included in the OSPF configuration.

Configuration Steps:

Create GRE Interface:

Example: set interfaces gr-0/0/0 unit 0 tunnel source <source-ip> tunnel destination <destination-ip>

Assign IP Address to GRE Interface:

Example: set interfaces gr-0/0/0 unit 0 family inet address <ip-address>

Include GRE Interface in OSPF:

Example: set protocols ospf area interface gr-0/0/0.0

Result:

OSPF will establish adjacencies over the GRE interface and exchange routing information.

Juniper Networks Documentation:

'To enable OSPF over GRE tunnels, you must include the GRE interfaces in the OSPF configuration.'

Source: OSPF over GRE Configuration

Why Options B and C are Incorrect:

Option B: The OSPF protocol must be enabled under the VPN zone.

Since OSPF is running over the GRE tunnel, which is encapsulated over IPsec, the OSPF packets are encapsulated within GRE and IPsec.

The SRX device does not need to allow OSPF in the security policies or enable OSPF under the VPN zone for GRE-encapsulated traffic.

Security Policies:

The GRE traffic (IP protocol 47) must be permitted through the security policies.

OSPF runs inside the GRE tunnel and does not require additional configuration under the VPN zone.

Juniper Networks Documentation:

'When using GRE over IPsec, routing protocols run over GRE and do not require separate security policies for their control traffic.'

Source: Security Policies for GRE over IPsec

Option C: Overlapping addresses are allowed between remote networks.

Overlapping IP addresses can cause routing conflicts and are generally not recommended.

In a GRE over IPsec scenario, overlapping addresses can lead to issues in routing protocol adjacency and data forwarding.

Best Practice:

Ensure unique IP addressing schemes between remote networks to prevent routing issues.

Juniper Networks Documentation:

'Overlapping IP address spaces can lead to routing ambiguities and should be avoided when configuring GRE tunnels.'

Source: Avoiding Overlapping IP Addresses

Conclusion:

Correct Answers: A and D

Rationale:

Option A is correct because using lo0 as endpoints for GRE provides stability and reliability.

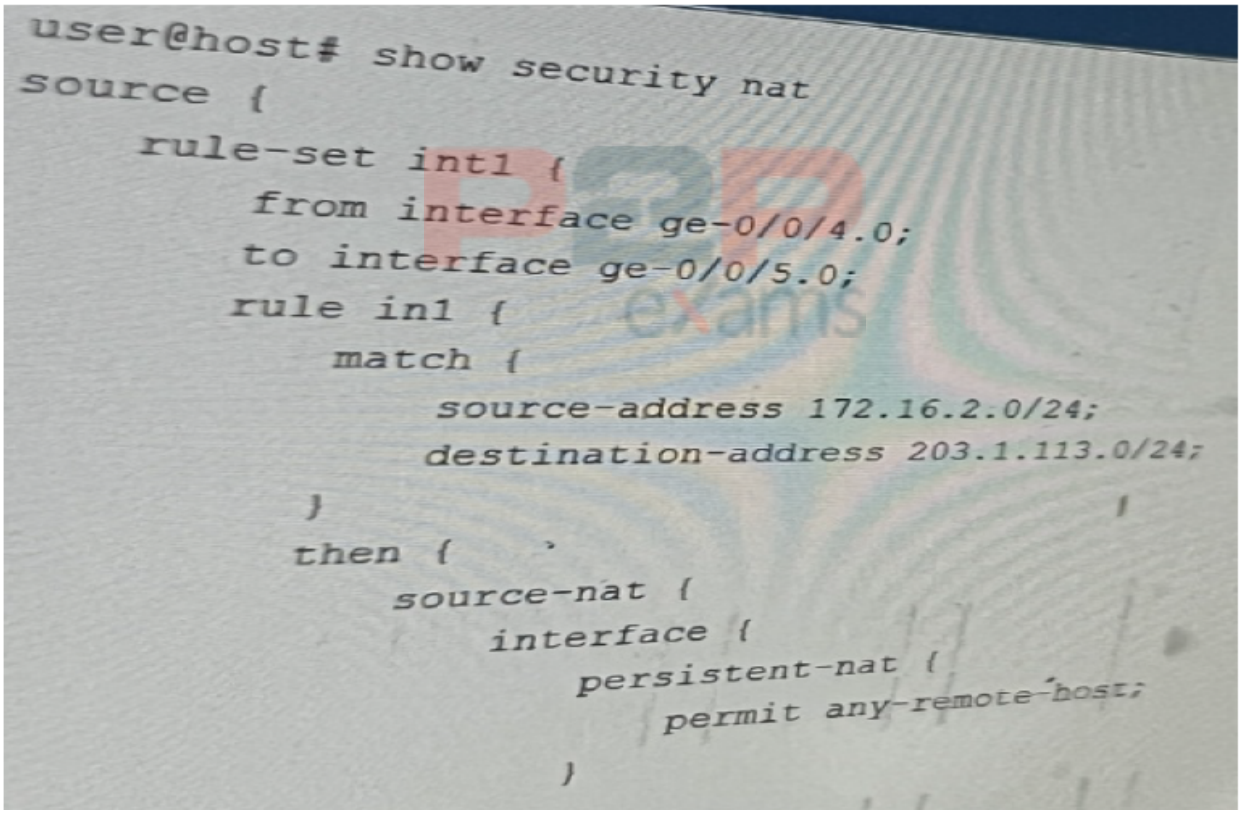
Option D is correct because the GRE interface must be included in the OSPF configuration to enable OSPF over the tunnel.

Question 7

Question Type: MultipleChoice

You Implement persistent NAT to allow any device on the external side of the firewall to

initiate traffic.



Referring to the exhibit, which statement is correct?

Options:

A- The target-host parameter should be used instead of the any-remote-host parameter.
B- The port-overloading parameter needs to be turned off in the NAT source interface configuration
C- The target-host-port parameter should be used instead of the any-remote-host parameter
D- The any-remote-host parameter does not support interface-based NAT and needs an IP pod to work.

Answer:

D

Question 8

Question Type: MultipleChoice

You want to bypass IDP for traffic destined to social media sites using APBR, but it is not working and IDP is dropping the session.

What are two reasons for this problem? (Choose two.)

Options:

A- The session did not properly reclassify midstream to the correct APBR rule.
B- IDP disable is not configured on the APBR rule.
C- The application services bypass is not configured on the APBR rule.
D- The APBR rule does a match on the first packet.

Answer:

A, C

Explanation:

Explanation of Answer A (Session Reclassification):

APBR (Advanced Policy-Based Routing) requires the session to be classified based on the specified rule, which can change midstream as additional packets are processed. If the session was already established before the APBR rule took effect, the traffic may not be correctly reclassified to match the new APBR rule, leading to IDP (Intrusion Detection and Prevention)

processing instead of being bypassed. This can occur especially when the session was already established before the rule change.

Explanation of Answer C (Application Services Bypass):

For APBR to work and bypass the IDP service, the application services bypass must be explicitly configured. Without this configuration, the APBR rule may redirect the traffic, but the IDP service will still inspect and potentially drop the traffic. This is especially important for traffic destined for specific sites like social media platforms where bypassing IDP is desired.

Example configuration for bypassing IDP services:

bash

set security forwarding-options advanced-policy-based-routing profile application-services-bypass

Step-by-Step Resolution:

Reclassify the Session Midstream:

If the traffic was already being processed before the APBR rule was applied, ensure that the session is reclassified by terminating the current session or ensuring the APBR rule is applied from the start.

Command to clear the session:

bash

clear security flow session destination-prefix <ip-address>

Configure Application Services Bypass:

Ensure that the APBR rule includes the application services bypass configuration to properly bypass IDP or any other security services for traffic that should not be inspected.

Example configuration:

bash

set security forwarding-options advanced-policy-based-routing profile application-services-bypass

Juniper Security Reference:

Session Reclassification in APBR: APBR requires reclassification of sessions in real-time to ensure midstream packets are processed by the correct rule. This is crucial when policies change dynamically or new rules are added.

Application Services Bypass in APBR: This feature ensures that security services such as IDP are bypassed for traffic that matches specific APBR rules. This is essential for applications where performance is a priority and security inspection is not necessary.

Question 9

Question Type: MultipleChoice

You want to test how the device handles a theoretical session without generating traffic on the Junos security device.

Which command is used in this scenario?

Options:

A- request security policies check
B- show security flow session
C- show security match-policies
D- show security policies

Answer:

A

Explanation:

The request security policies check command allows you to simulate a session through the SRX device, checking the security policy action that would apply without needing to send real traffic. This helps in validating configurations before actual deployment. For more details, see Juniper Security Policies Testing.

The command request security policies check is used to test how a Junos security device handles a theoretical session without generating actual traffic. This command is useful for validating how security policies would be applied to a session based on various parameters like source and destination addresses, application type, and more.

Explanation of Answer A (request security policies check):

This command allows you to simulate a session and verify which security policies would be applied to the session. It's a proactive method to test security policy configurations without the need to generate real traffic.

Example usage:

bash

request security policies check from-zone trust to-zone untrust source 10.1.1.1 destination 192.168.1.1 protocol tcp application junos-https

Juniper Security Reference:

Security Policies Check: This command provides a way to simulate and verify security policy behavior without actual traffic. Reference: Juniper Security Policy Documentation.

Question 10

Question Type: MultipleChoice

You are using AutoVPN to deploy a hub-and-spoke VPN to connect your enterprise sites.

In this scenario, which two statements are true? (Choose two.)

Options:

A- New spoke sites can be added without explicit configuration on the hub.
B- Direct spoke-to-spoke tunnels can be established automatically.
C- All spoke-to-spoke IPsec communication will pass through the hub.
D- AutoVPN requires OSPF over IPsec to discover and add new spokes.

Answer:

A, C

Question 11

Question Type: MultipleChoice

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?

Options:

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. For further information, see Juniper Logical Systems Documentation.

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.

Explanation of Answer D (Logical System):

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.

Configuration Example:

bash

set logical-systems <logical-system-name> interfaces ge-0/0/0 unit 0

set logical-systems <logical-system-name> routing-options static route 0.0.0.0/0 next-hop 192.168.1.1

Juniper Security Reference:

Logical Systems Overview: Logical systems allow for the creation of multiple virtual instances within a single SRX device, each with its own configuration and control plane. Reference: Juniper Logical Systems Documentation.

Question 12

Question Type: MultipleChoice

Which three statements about persistent NAT are correct? (Select Three)

Options:

A- New sessions can only be initiated from a source towards the reflexive address.
B- New sessions can be initiated from a destination towards the reflexive address.
C- Persistent NAT only applies to source NAT.
D- All requests from an internal address are mapped to the same reflexive address.
E- Persistent NAT applies to both destination and source NAT.

Answer:

B, C, D

P2P exams

Question 13

Question Type: MultipleChoice

A user reports that a specific application is not working properly. This application makes

multiple connection to the server and must have the same address every time from a pool and this behavior needs to be changed.

What would solve this problem?

Options:

A- Use STUN.
B- Use DNS doctoring.
C- Use the address-persistent parameter.
D- Use the persistent-nat parameter.

P2P exams

Answer:

D

To Get Premium Files for JN0-637 Visit

https://www.p2pexams.com/products/jn0-637

For More Free Questions Visit

https://www.p2pexams.com/juniper/pdf/jn0-637

