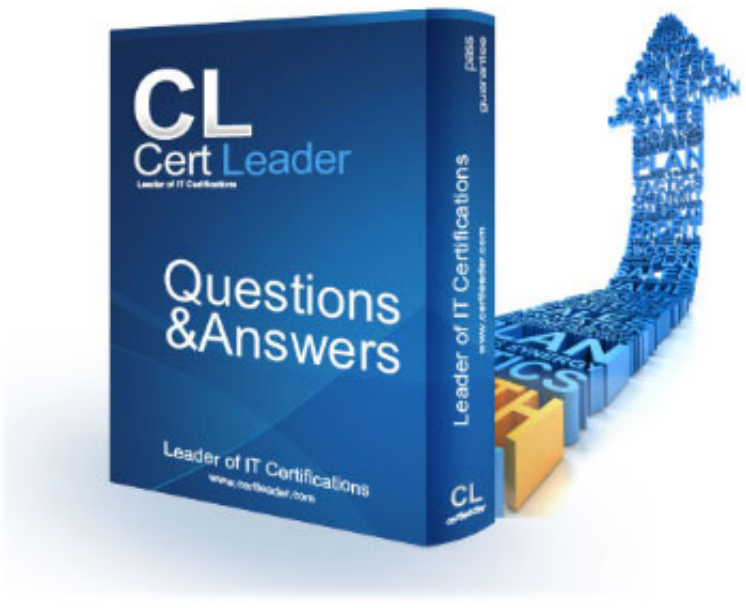
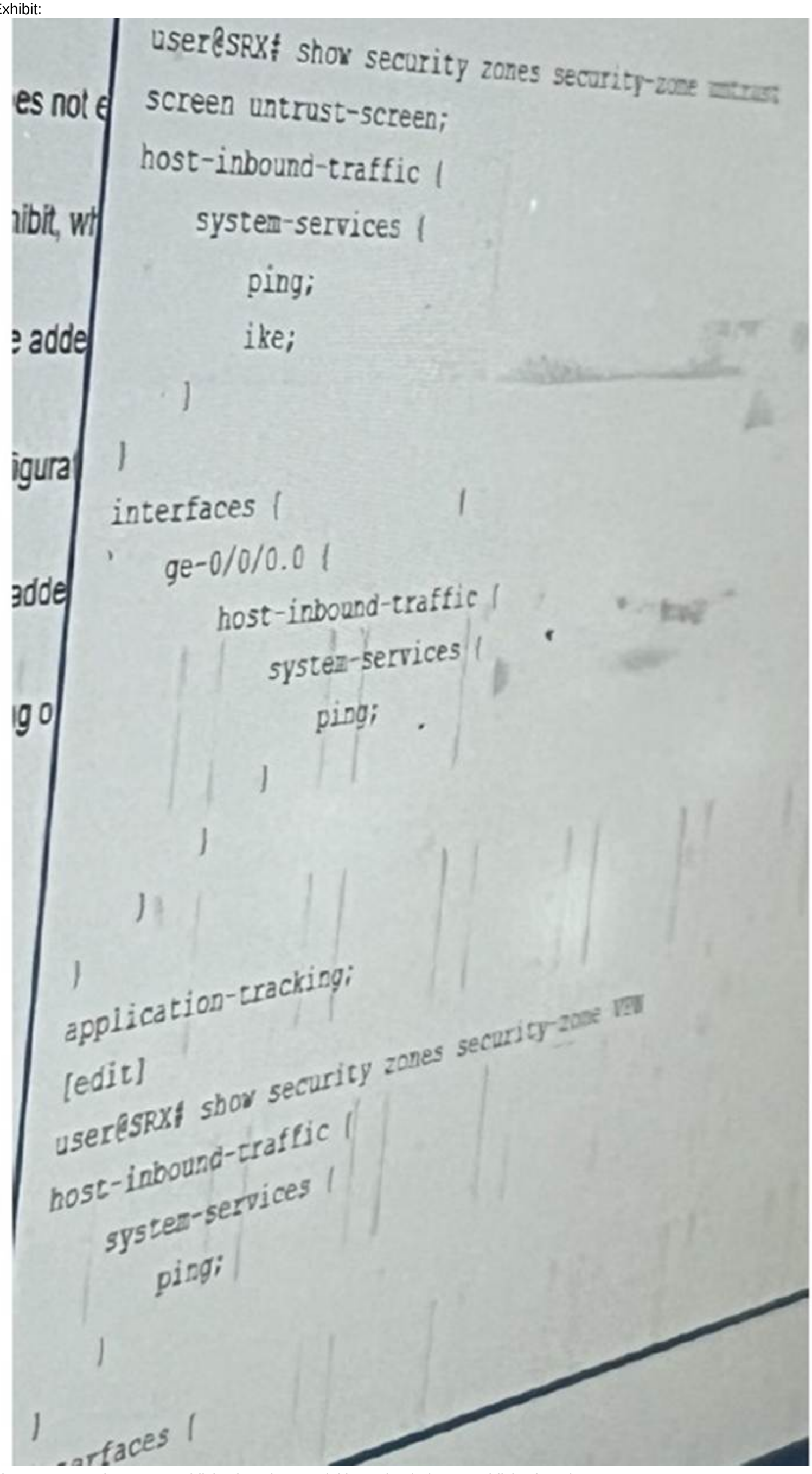
JN0-637 Dumps

Security - Professional (JNCIP-SEC)

https://www.certleader.com/JN0-637-dumps.html



NEW QUESTION 1
Exhibit:

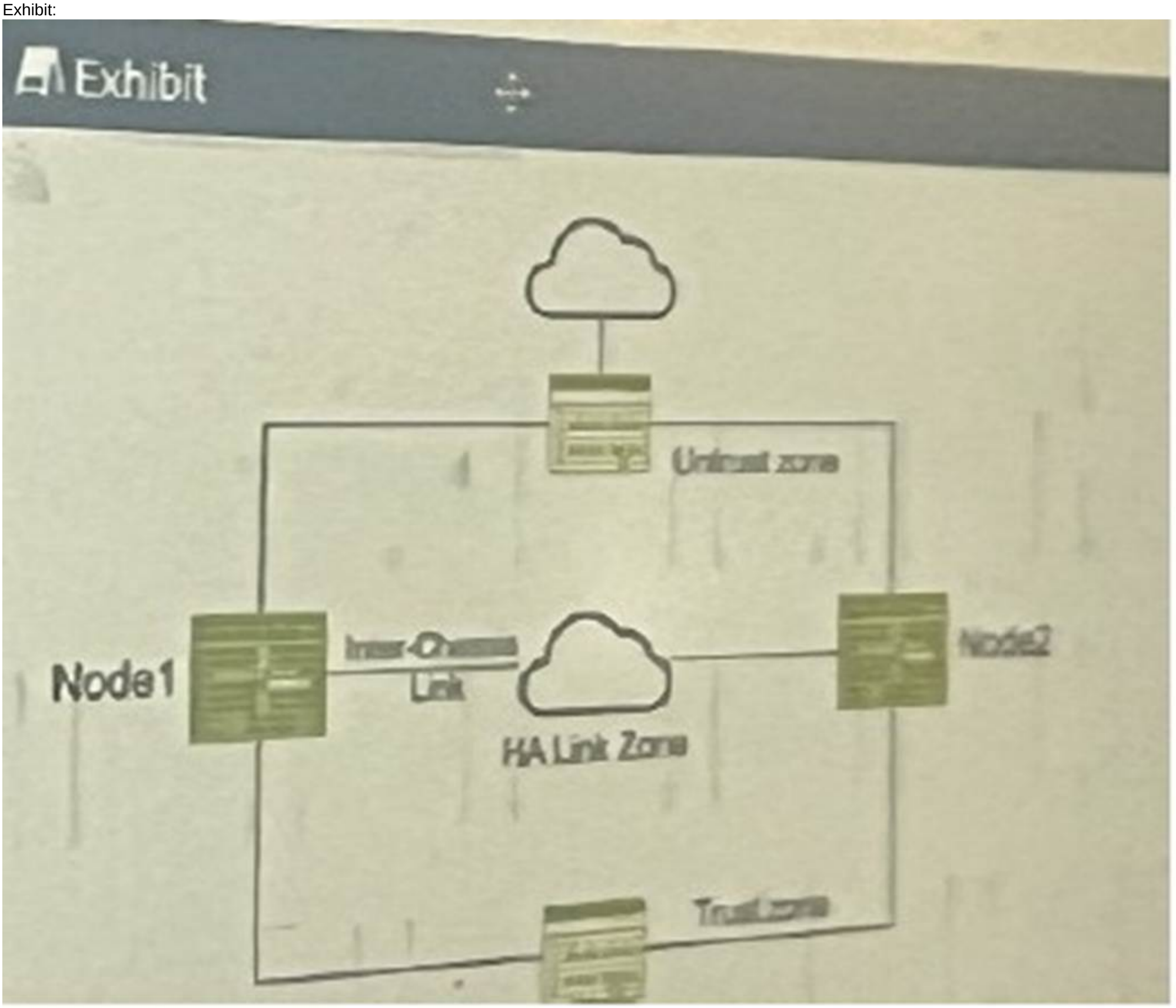


The Ipsec VPN does not establish when the peer initiates, but it does establish when the SRX series device initiates. Referring to the exhibit, what will solve this problem?

A. IKE needs to be added for the host-inbound traffic on the VPN zone.
B. The screen configuration on the untrust zone needs to be modified.
C. IKE needs to be added to the host-inbound traffic directly on the ge-0/0/0 interface.
D. Application tracking on the untrust zone needs to be removed.

Answer: C

NEW QUESTION 2
Exhibit:



You have deployed a pair of SRX series devices in a multimode HA environment. You need to enable IPsec encryption on the interchassis link.
Referring to the exhibit, which three steps are required to enable ICL encryption? (Choose three.)

A. Install the Junos IKE package on both nodes.
B. Enable OSPF for both interchassis link interfaces and tum on the dynamic-neighbors parameter.
C. Configure a VPN profile for the HA traffic and apply to both nodes.
D. Enable HA link encryption in the IPsec profile on both nodes.
E. Enable HA link encryption in the IKE profile on both nodes,

Answer: ACD

Explanation:
? A. Install the Junos IKE package on both nodes. While I previously stated that IKE
is usually included in the base Junos OS image, it's essential to ensure that the necessary IKE package is indeed installed and enabled on both SRX nodes to support ICL encryption.
? C. Configure a VPN profile for the HA traffic and apply it to both nodes. This
dedicated VPN profile defines the security parameters (encryption algorithms, authentication, etc.) specifically for the ICL traffic.
? D. Enable HA link encryption in the IPsec profile on both nodes. Within the IPsec
profile, you must explicitly enable ICL encryption to ensure that all traffic traversing the interchassis link is protected.
Why E is incorrect:
? E. Enable HA link encryption in the IKE profile on both nodes. While securing IKE negotiations is important, it's typically handled within the IPsec profile itself when configuring ICL encryption on SRX devices.

NEW QUESTION 3
What are three requirements to run OSPF over GRE over IPsec? (Choose Three)

A. The GRE interface must be configured in OSPF Area 0.
B. The OSPF interface must be placed in a zone and must have GRE configured
C. Overlapping addresses should exist between remote networks.
D. The GRE interface must be placed in a zone and must have OSPF configured in is host
E. Overlapping addresses should not exist between remote networks.

Answer: BDE

NEW QUESTION 4
Exhibit:

```
user@srx> show ethernet-switching global-information
Global Configuration:
MAC aging interval     : 300
MAC learning           : Enabled
MAC statistics         : Disabled
MAC limit Count        : 65536
MAC limit hit          : Disabled
MAC packet action drop: Disabled
MAC+IP aging interval : IPv4 - 1200 seconds
                        IPv6 - 1200 seconds
MAC+IP limit Count     : 65536
MAC+IP limit reached   : No
LE  aging time         : 1200
LE  VLAN aging time    : 1200
Global Mode            : Transparent bridge
RE state               : Master
```

Referring to the exhibit, which two statements are correct? (Choose two.)

A. You cannot secure intra-VLAN traffic with a security policy on this device.
B. You can secure inter-VLAN traffic with a security policy on this device.
C. The device can pass Layer 2 and Layer 3 traffic at the same time.
D. The device cannot pass Layer 2 and Layer 3 traffic at the same time.

Answer: BC

Explanation:
The exhibit provides information about an SRX Series device operating in transparent mode (Layer 2) and Layer 3 routing at the same time. Let??s break down the correct answers:
? Explanation of Answer B (Secure Inter-VLAN Traffic with a Security Policy):
? Explanation of Answer C (Pass Layer 2 and Layer 3 Traffic Simultaneously):
Juniper Security Reference:
? Mixed Mode Overview: Juniper SRX devices in mixed mode can operate as both a Layer 2 switch and a Layer 3 router, allowing it to pass traffic at both layers simultaneously. Reference: Juniper Mixed Mode Documentation.
==========

NEW QUESTION 5
Which two elements are necessary to configure a rule under an APBR profile? (Choose Two)

A. instance type
B. match condition
C. then action
D. RIB group

Answer: BC

Explanation:
Here's why those elements are necessary for configuring a rule under an APBR profile:
? B. Match condition: This defines the criteria for matching traffic to the APBR rule. It can include:
? C. Then action: This specifies the action to take when traffic matches the rule. The primary action in APBR is:
Why other options are incorrect:
? A. Instance type: While routing instances are used in APBR, the "instance type" itself is not configured within the APBR rule. You define the instance type separately when configuring the routing instance.
? D. RIB group: RIB groups are used for route management and are not directly involved in APBR rule configuration.

NEW QUESTION 6
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 HApeers.
C. The ICL traffic can be encrypted.
D. The ICL is the local device management interface in a multinode HA environment.

Answer: BC

NEW QUESTION 7
Which two statements are correct about DNS doctoring?

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: BD

NEW QUESTION 8
Which two statements are correct about automated threat mitigation with Security Director? (Choose two.)

A. It works with third-party switches.
B. It provides endpoint protection by running a Juniper ATP Cloud agent on the servers.
C. It provides endpoint protection by running a Juniper ATP Cloud agent on EX Series devices.
D. It works with SRX Series devices.

Answer: AD

NEW QUESTION 9
In a multinode HA environment, which service must be configured to synchronize between nodes?

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

Answer: B

NEW QUESTION 10
A company has acquired a new branch office that has the same address space as one of its local networks, 192.168.100.0/24. The offices need to communicate with each other.
Which two NAT configurations will satisfy this requirement? (Choose two.)

A. [edit security nat source]user@OfficeA# show rule-set OfficeBtoA { from zone OfficeB;to zone OfficeA; rule 1 {match {source-address 192.168.210.0/24; destination-address 192.168.200.0/24;}then {source-nat { interface; }}}}
B. [edit security nat static]user@OfficeA# show rule-set From-Office-B { from interface ge-0/0/0.0;rule 1 { match {destination-address 192.168.200.0/24;}then { static-nat {prefix { 192.168.100.0/24; }}}}}
C. [edit security nat static]user@OfficeB# show rule-set From-Office-A { from interface ge-0/0/0.0;rule 1 { match {destination-address 192.168.210.0/24;}then { static-nat {prefix { 192.168.100.0/24; }}}}}
D. [edit security nat source]user@OfficeB# show rule-set OfficeAtoB { from zone OfficeA;to zone OfficeB; rule 1 {match {source-address 192.168.200.0/24; destination-address 192.168.210.0/24;}then {source-nat { interface; }}}}

Answer: BC

Explanation:
* 1. Static NAT Configuration at Office A (Option B):
? Configuration:
[edit security nat static]
user@OfficeA# show rule-set From-Office-B { from interface ge-0/0/0.0;
rule 1 { match {
destination-address 192.168.200.0/24;
}
then { static-nat {
prefix { 192.168.100.0/24; }
}
}
}
}
? Explanation:
Reference:
Juniper Networks Documentation: "Configuring Static NAT"
* 2. Static NAT Configuration at Office B (Option C): Configuration:
[edit security nat static]
user@OfficeB# show rule-set From-Office-A { from interface ge-0/0/0.0;
rule 1 { match {
destination-address 192.168.210.0/24;
}
then { static-nat {
prefix { 192.168.100.0/24; }
}

}
}
}
* Explanation:
from interface ge-0/0/0.0;: Specifies the interface through which the traffic is received.
Matching Traffic:
destination-address 192.168.210.0/24;: Matches packets destined for 192.168.210.0/24. Action:
static-nat { prefix { 192.168.100.0/24; } }: Translates the destination address to 192.168.100.0/24.
Result:
Office A sends packets to 192.168.210.0/24, which are translated to 192.168.100.0/24
upon arrival at Office B.
Reference:
Juniper Networks Documentation: "Configuring Static NAT"
Why Options A and D are Incorrect:
Option A and Option D use Source NAT, which is typically used for translating the source IP address of outgoing traffic.
Source NAT with interface-based translation may not resolve overlapping IP issues effectively because it doesn't provide a one-to-one mapping of the overlapping addresses.
In scenarios with overlapping networks, Static NAT is preferred as it allows for consistent and predictable address translation, essential for two-way communication.
Key Juniper Concepts: Static NAT:
Provides a one-to-one mapping between local and global addresses. Useful for scenarios where bidirectional communication is required. Reference: Juniper Networks Day One Book "Advanced NAT Concepts" Source NAT:
Typically used for translating private IP addresses to public IP addresses for outbound traffic.
Interface-based Source NAT translates the source IP to the IP address of the egress interface.
Not ideal for resolving overlapping IP spaces in bidirectional communication.
Additional References:
Juniper TechLibrary:
"Understanding NAT in SRX Series Devices" "Configuring NAT for Overlapping Networks" Juniper Forums and Knowledge Base Articles:
Discussions on resolving overlapping IP address spaces using Static NAT.
Conclusion:
By implementing Static NAT configurations as shown in Options B and C, both offices can effectively communicate despite having overlapping IP address spaces. Static NAT ensures that IP addresses are uniquely translated, avoiding conflicts and enabling seamless connectivity between the two networks.

NEW QUESTION 10
What is the advantage of using separate st0 logical units for each spoke connection?

A. It is easy to configure even when managing many st0 units.
B. It facilitates scalability.
C. Junos devices can exchange NHTB data automatically using this method.
D. It enables assignments of different settings to each logical unit.

Answer: D

NEW QUESTION 11
You have deployed an SRX Series device at your network edge to secure Internet-bound sessions for your local hosts using source NAT. You want to ensure that your users are able to interact with applications on the Internet that require more than one TCP session for the same application session.
Which two features would satisfy this requirement? (Choose two.)

A. address persistence
B. STUN
C. persistent NAT
D. double NAT

Answer: AC

Explanation:
Address persistence ensures that the same NAT IP address is used for all sessions originating from a single source IP. Persistent NAT maintains connections for applications needing multiple sessions, like VoIP. Additional details are available in Juniper NAT Documentation.
For applications that require multiple TCP sessions for the same application session (such as VoIP or certain online games), the SRX device needs to handle NAT properly to maintain session continuity. Here??s what helps:
? Address Persistence (Answer A): Address persistence ensures that multiple
sessions initiated by the same internal host are mapped to the same external IP address. This is crucial for applications that use multiple TCP sessions to maintain a stateful connection with the external server.
Command Example: bash
set security nat source persistent-nat address-persistence
? Persistent NAT (Answer C): This feature allows the external server to initiate new
connections to the internal client using the same NAT translation. It's essential for applications that require consistent NAT mappings across multiple sessions.
Command Example: bash
set security nat source persistent-nat permit target-host-port
These features ensure that applications with multiple TCP sessions work seamlessly across NAT.
: Juniper NAT and persistent NAT documentation.
==========

NEW QUESTION 15
You are asked to configure tenant systems.
Which two statements are true in this scenario? (Choose two.)

A. A tenant system can have only one administrator.
B. After successful configuration, the changes are merged into the primary database for each tenant system.
C. Tenant systems have their own configuration database.

D. You can commit multiple tenant systems at a time.

Answer: CD

Explanation:
Each tenant system maintains its own configuration database, isolating configurations from others, enhancing security and operational efficiency. Junos OS supports multiple concurrent commit operations across tenant systems. Further details are covered in the Juniper Tenant System Guide.
When configuring tenant systems on an SRX device, the following principles apply:
? Tenant Systems Have Their Own Configuration Database (Answer C): Each tenant system has its own isolated configuration database, ensuring that changes made in one tenant system do not affect others. This allows for multi-tenant environments where different tenants can have independent configurations.
? Commit Multiple Tenant Systems Simultaneously (Answer D): The system allows for multiple tenant systems to be committed at the same time, simplifying management when working with multiple tenants. This is particularly useful in large environments where multiple logical systems or tenants need updates simultaneously.
: Juniper documentation on tenant systems and configuration databases.
==========

NEW QUESTION 17
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?

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):
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.
==========

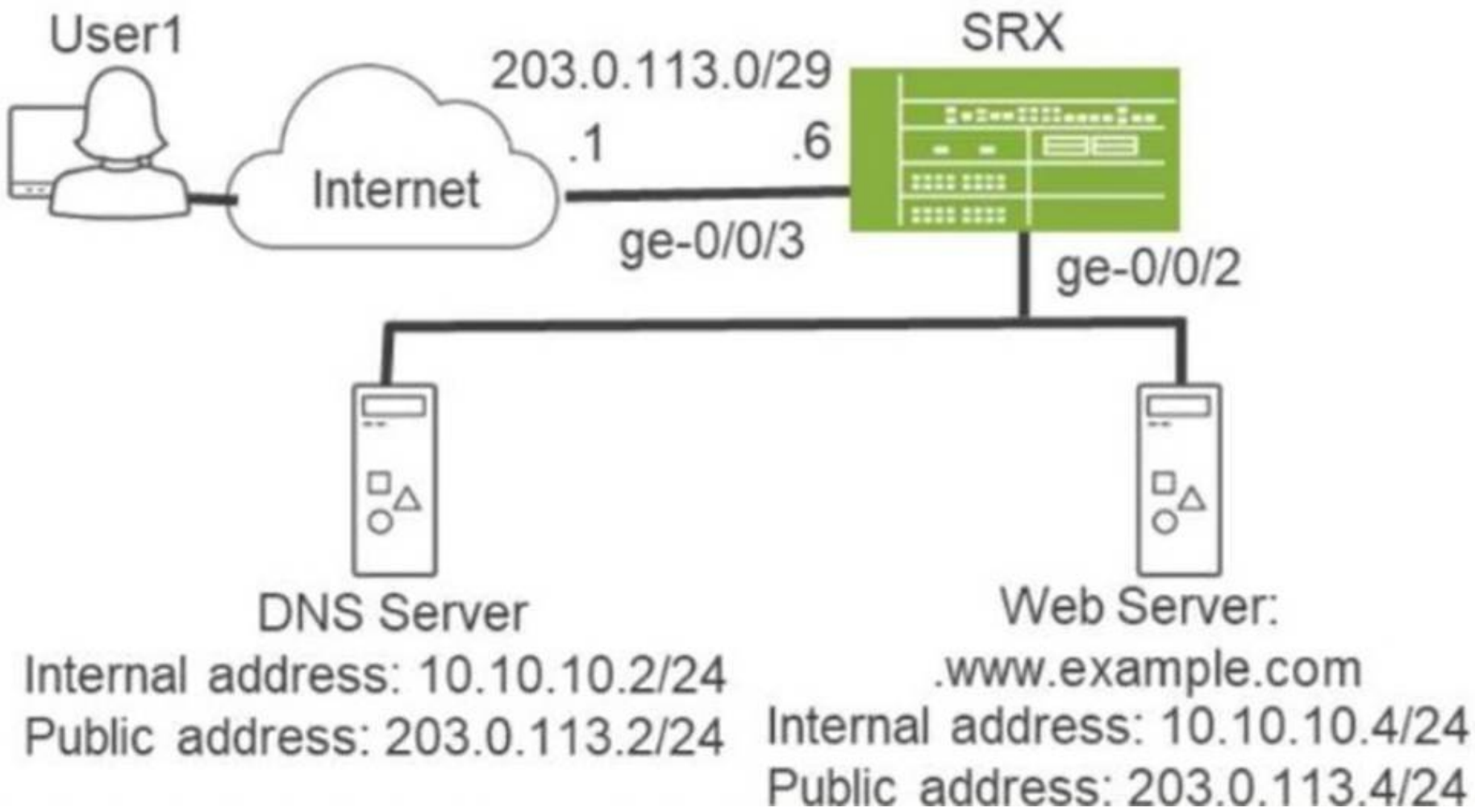
NEW QUESTION 22
You are asked to see if your persistent NAT binding table is exhausted. Which show command would you use to accomplish this task?

A. show security nat source persistent-nat-table summary
B. show security nat source summary
C. show security nat source pool all
D. show security nat source persistent-nat-table all

Answer: D

Explanation:
The command show security nat source persistent-nat-table all provides a comprehensive view of all entries in the persistent NAT table, enabling administrators to monitor and manage resource exhaustion. Refer to Juniper NAT Monitoring Guide for more.
In Junos OS, when persistent NAT is configured, a binding table is created to keep track of NAT sessions and ensure that specific hosts are allowed to initiate sessions back to internal hosts. To check if the persistent NAT binding table is full or exhausted, the correct
command must display the entire table.
? Correct Command (D):
? Incorrect Options:
Juniper References:
? Juniper Persistent NAT Documentation: Describes the persistent NAT binding table and the commands used to monitor its status.

NEW QUESTION 26
Exhibit:



You are asked to ensure that Internet users can access the company's internal webserver using its FQDN. However, the internal DNS server's A record only points to the webserver's private address.
Referring to the exhibit, which two actions are required to complete this task? (Choose two.)

A. Disable the DNS ALG.
B. Configure static NAT for both the DNS server and the webserver.
C. Configure destination NAT for both the DNS server and the webserver.
D. Configure proxy ARP on ge-0/0/3.

Answer: BD

Explanation:
In the scenario where internal users are trying to access the company's web server via its FQDN but the DNS server resolves to a private IP, two key actions are needed:
? Static NAT (Answer B): Since the internal DNS server resolves the web server to
its private IP address (10.10.10.4/24), you need to configure static NAT for both the DNS server and the webserver. This will ensure that requests coming from the internet will be translated to the web server's public IP (203.0.113.4) and the DNS server??s public IP (203.0.113.2).
Example Command: bash
set security nat static rule-set public-to-private from zone untrust
set security nat static rule-set public-to-private rule dns-server match destination-address 203.0.113.2/32
set security nat static rule-set public-to-private rule dns-server then static-nat-prefix 10.10.10.2/32
set security nat static rule-set public-to-private rule web-server match destination-address 203.0.113.4/32
set security nat static rule-set public-to-private rule web-server then static-nat-prefix 10.10.10.4/32
? Proxy ARP (Answer D): The SRX needs to respond to ARP requests for the public
IP addresses of both the DNS and webserver on the interface facing the internet (ge-0/0/3). This allows the SRX to handle requests directed at the public IPs.
Example Command:
set interfaces ge-0/0/3 unit 0 family inet proxy-arp interface-address 203.0.113.2/32 set interfaces ge-0/0/3 unit 0 family inet proxy-arp interface-address 203.0.113.4/32 These two configurations allow external users to access the internal web server via its public IP, as resolved by the DNS server.
: Juniper NAT and proxy ARP documentation.
==========

NEW QUESTION 29
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.)

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: AC

NEW QUESTION 32
You are asked to establish IBGP between two nodes, but the session is not established. To troubleshoot this problem, you configured trace options to monitor BGP protocol message exchanges.

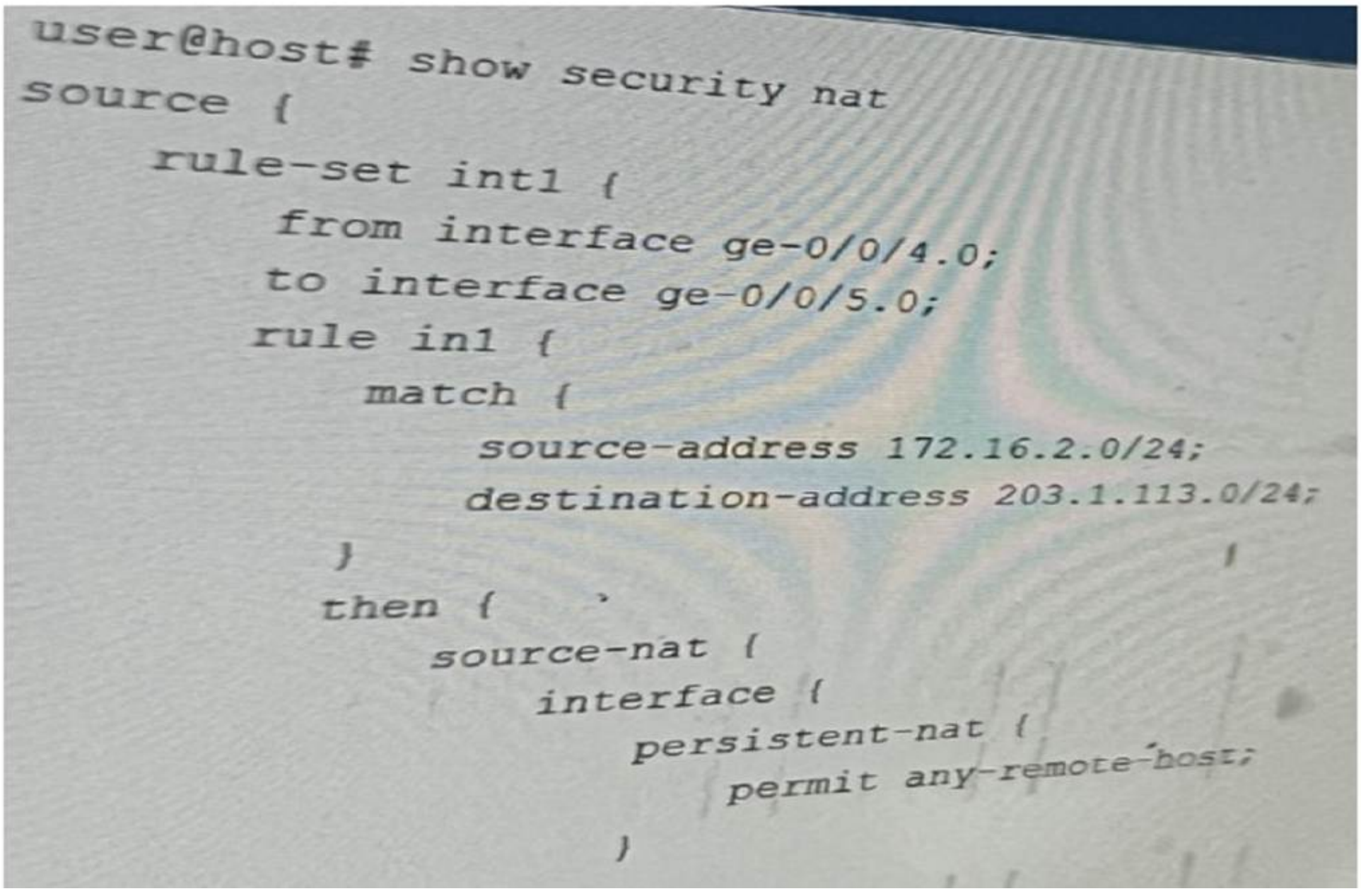
```
Mar  7 02:38:15 02:38:15.353921:CID-0:THREAD_ID-01:RT: <192.168.2.1/54882->192.168.1.1/179;6,0x0 > matched filter ibgp-
traffic:
…
Mar  7 02:38:15 02:38:15.353933:CID-0:THREAD_ID-01:RT: ge-0/0/3.0:192.168.2.1/54882->192.168.1.1/179, tcp, flag 2 syn
Mar  7 02:38:15 02:38:15.353935:CID-0:THREAD_ID-01:RT: find flow: table 0x206a60a0, hash 6149(0xffff), sa 192.168.2.1, da
192.168.1.1, sp 54882, dp 179, proto 6, tok 9, conn-tag 0x00000000
Mar  7 02:38:15 02:38:15.353938:CID-0:THREAD_ID-01:RT: no session found, start first path. in_tunnel - 0x0,  from_cp_flag
- 0
Mar  7 02:38:15 02:38:15.353941:CID-0:THREAD_ID-01:RT: flow_first_create_session
…
Mar  7 02:38:15 02:38:15.353964:CID-0:THREAD_ID-01:RT: Doing DESTINATION addr route-lookup
Mar  7 02:38:15 02:38:15.353971:CID-0:THREAD_ID-01:RT: flow_ipv4_rt_lkup success 192.168.1.1, iifl 0x47, oifl 0x0
Mar  7 02:38:15 02:38:15.353975:CID-0:THREAD_ID-01:RT: Changing out-ifp from .local..0 to lo0.0 for dst: 192.168.1.1 in
vr_id:0
Mar  7 02:38:15 02:38:15.353976:CID-0:THREAD_ID-01:RT: routed (x_dst_ip 192.168.1.1) from untrust  (ge-0/0/3.0 in 0) to
lo0.0, Next-hop: 192.168.1.1
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0,0xd66200b3,0xb3)
Mar  7 02:38:15 02:38:15.353986:CID-0:THREAD_ID-01:RT: Policy lkup: vsys 0 zone(5:global) -> zone(5:global) scope:0
…
Mar  7 02:38:15 02:38:15.354000:CID-0:THREAD_ID-01:RT: permitted by policy allow-bgp(6)
Mar  7 02:38:15 02:38:15.354048:CID-0:THREAD_ID-01:RT: flow_first_final_check: in  0/3.0>, out
Mar  7 02:38:15 02:38:15.354050:CID-0:THREAD_ID-01:RT: In flow_first_complete_session
Mar  7 02:38:15 02:38:15.354051:CID-0:THREAD_ID-01:RT: flow_first_complete_session, pak_ptr: 0x2c5fcd40, nsp: 0x2a140340,
in_tunnel: 0x0
…
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0.0xd66200b3.0xb3)
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0,0xd66200b3,0xb3)
Mar  7 02:38:15 02:38:15.353986:CID-0:THREAD_ID-01:RT: Policy lkup: vsys 0 zone(5:global) -> zone(5:global) scope:0
…
Mar  7 02:38:15 02:38:15.354000:CID-0:THREAD_ID-01:RT: permitted by policy allow-bgp(6)
Mar  7 02:38:15 02:38:15.354048:CID-0:THREAD_ID-01:RT: flow_first_final_check: in  0/3.0>, out
Mar  7 02:38:15 02:38:15.354050:CID-0:THREAD_ID-01:RT: In flow_first_complete_session
Mar  7 02:38:15 02:38:15.354051:CID-0:THREAD_ID-01:RT: flow_first_complete_session, pak_ptr: 0x2c5fcd40, nsp: 0x2a140340,
in_tunnel: 0x0
…
Mar  7 02:38:15 02:38:15.354055:CID-0:THREAD_ID-01:RT: Session (id:20395) created for first pak 2
Mar  7 02:38:15 02:38:15.354073:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat: in  , out  A> dst_adr 192.168.1.1, sp 54882,
dp 179
Mar  7 02:38:15 02:38:15.354075:CID-0:THREAD_ID-01:RT: chose interface lo0.0 as incoming nat if.
Mar  7 02:38:15 02:38:15.354075:CID-0:THREAD_ID-01:RT: packet dropped: for self but not interested
Mar  7 02:38:15 02:38:15.354076:CID-0:THREAD_ID-01:RT: packet dropped, packet dropped: for self but  not interested.
Mar  7 02:38:15 02:38:15.354079:CID-0:THREAD_ID-01:RT: flow_first_install_session: Loopback session processing aborted
Mar  7 02:38:15 02:38:15.354080:CID-0:THREAD_ID-01:RT: first path session installation failed
Mar  7 02:38:15 02:38:15.354081:CID-0:THREAD_ID-01:RT: flow find session returns error.
```

Referring to the exhibit, which action would solve the problem?

A. Add the junos-host zone policy to permit the BGP packets.
B. Add a firewall filter to lo0 that permits the BGP packets.
C. Modify the security policy to permit the BGP packets.
D. Add BGP to the lo0 host-inbound-traffic configuration.

Answer: D

NEW QUESTION 35
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?

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

NEW QUESTION 40
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

NEW QUESTION 43
Referring to the exhibit,

```
[edit security nat]
user@srx# show
source {
    interface {
        port-overloading off;
    }
    rule-set rule1 {
        from zone trust;
        to zone untrust;
        rule allow {
            match {
                source-address 172.16.1.0/24;
                destination-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    interface {
                        persistent-nat {
                            permit target-host-port;
                        }
                    }
                }
            }
        }
    }
}
```

which two statements are correct about the NAT configuration? (Choose two.)

A. Both the internal and the external host can initiate a session after the initial translation.
B. Only a specific host can initiate a session to the reflexive address after the initial session.
C. Any external host will be able to initiate a session to the reflexive address.
D. The original destination port is used for the source port for the session.

Answer: BD

Explanation:
Persistent NAT with target-host restricts session initiation to specific addresses, enhancing security. Reflexive NAT supports multiple connections by preserving the original port. Refer to Juniper NAT Configuration Documentation.
Referring to the NAT configuration shown in the exhibit:
? Specific Host Can Initiate a Session (Answer B): The configuration uses persistent NAT with the permit target-host-port statement. This allows a specific external host (based on the target host and port used in the initial session) to initiate a session back to the internal host after the initial session has been established.
* Explanation: Persistent NAT ensures that the translation state is maintained, allowing external hosts to connect back only under specific conditions (e.g., the same target host and port as used in the original connection).
? Original Destination Port (Answer D): The original destination port used by the
internal host is retained as the source port when the session is established from outside to inside. This behavior is a result of how persistent NAT binds the internal and external sessions, ensuring that communication occurs over the same port used for the initial session.
: Juniper NAT and Persistent NAT configuration documentation.
==========

NEW QUESTION 45
Which two statements are correct about automated threat mitigation with Security Director? (Choose two.)

A. Infected hosts are tracked by their IP address.
B. Infected hosts are tracked by their chassis serial number.
C. Infected hosts are tracked by their MAC address.
D. Infected hosts are tracked by their user identity.

Answer: AC

NEW QUESTION 49
You are attempting to ping an interface on your SRX Series device, but the ping is unsuccessful.
What are three reasons for this behavior? (Choose three.)

A. The interface is not assigned to a security zone.
B. The interface's host-inbound-traffic security zone configuration does not permit ping
C. The ping traffic is matching a firewall filter.
D. The device has J-Web enabled.
E. The interface has multiple logical units configured.

Answer: ABC

Explanation:
Firewall filters (configured using the security policies hierarchy) can block specific traffic types, including ICMP. If a filter is applied to the interface or zone, and it doesn't have a rule to permit ping, the ping will be unsuccessful.
Reference: Firewall Filters [invalid URL removed]
Why other options are incorrect:
* D. The device has J-Web enabled. J-Web is a web-based management interface and has no direct impact on the device's ability to respond to pings.
* E. The interface has multiple logical units configured. Logical units divide a physical interface into multiple virtual interfaces. While this can affect routing and traffic flow, it doesn't inherently prevent ping responses as long as the relevant zones and policies are correctly configured.
Troubleshooting Steps:
If you're unable to ping an SRX interface, here's a systematic approach to troubleshoot:
Verify Interface Status: Ensure the interface is up and operational using show interfaces terse.
Check Zone Assignment: Confirm the interface belongs to a security zone using show security zones.
Examine host-inbound-traffic: Verify that the zone's host-inbound-traffic settings allow ping (e.g., set security zones security-zone trust host-inbound-traffic system-services ping).
Analyze Firewall Filters: Review any firewall filters applied to the interface or zone to
ensure they allow ICMP ping traffic. Use show security policies and monitor traffic to diagnose filter behavior.
Test from Different Zones: Try pinging the interface from devices in different zones to isolate potential policy issues.
By systematically checking these aspects, you can identify the root cause and resolve the ping issue on your SRX Series device.

NEW QUESTION 52
You are deploying OSPF over IPsec with an SRX Series device and third-party device using GRE.
Which two statements are correct? (Choose two.)

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: AD

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security
References
Understanding the Scenario:
? Objective: Deploy OSPF over IPsec between an SRX Series device and a third- party device using GRE tunnels.
? Components Involved:
Option A: The GRE interface should use lo0 as endpoints.
? Explanation:
Reference:
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.
* Explanation:
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 <area-id> interface gr-0/0/0.0
Result:
OSPF will establish adjacencies over the GRE interface and exchange routing information.
Reference:
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.
* Explanation:
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.
Reference:
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.
* Explanation:
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.
Reference:
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.

NEW QUESTION 53
Which two statements about policy enforcer and the forescout integration are true? (Choose two)

A. 802.1X authenticated devices are supported.
B. 802.1X authenticated devices are not supported.
C. A Forescout CounterACT agent must be installed on third-party devices
D. A Forescout CounterACT agent is agentless and does not need to be installed on third- party device

Answer: AD

NEW QUESTION 54
Exhibit:

Exhibit

```
[edit routing-instances]
user@vSRX-1# show
APBR-1 {
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 172.16.9.2;
        }
    }
}
[edit routing-options]
user@vSRX-1# show
interface-routes {
    rib-group inet APBR-group;
}
static {
    route 0.0.0.0/0 next-hop 192.168.101.1;
}
rib-groups {
    APBR-group {
        import-rib [ inet.0 APBR-1.inet.0 ];
    }
}
[edit security advance-policy-based-routing]
user@vSRX-1# show
profile APBR-profile {
    rule ssh {
        match {
            dynamic-application junos:SSH;
```

Exhibit

```
        import-rib [ inet.0 APBR-1.inet.0 ];
    }
}
[edit security advance-policy-based-routing]
user@vSRX-1# show
profile APBR-profile {
    rule ssh {
        match {
            dynamic-application junos:SSH;
        }
        then {
            routing-instance APBR-1;
        }
    }
}
from-zone DC9-zone {
    policy move-ssh {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            application-services {
                advance-policy-based-routing-profile APBR-profile;
            }
        }
    }
}
```

You are having problems configuring advanced policy-based routing. What should you do to solve the problem?

A. Apply a policy to the APBR RIB group to only allow the exact routes you need.
B. Change the routing instance to a forwarding instance.
C. Change the routing instance to a virtual router instance.
D. Remove the default static route from the main instance configuration.

Answer: B

NEW QUESTION 56
You need to set up source NAT so that external hosts can initiate connections to an internal device, but only if a connection to the device was first initiated by the internal device.
Which type of NAT solution provides this functionality?

A. Address persistence
B. Persistent NAT with any remote host
C. Persistent NAT with target host
D. Static NAT

Answer: C

Explanation:
Persistent NAT with target host allows external hosts to establish
connections only when the internal device initiates a session first, ideal for specific interactive applications. Refer to Juniper Persistent NAT Documentation.
The scenario requires that external hosts be able to initiate a connection only if the internal device has already initiated a connection. The correct solution is Persistent NAT with target host, which ensures that a specific external host can initiate new connections back to the internal device, but only after the internal device has established a session first.
? Persistent NAT with Target Host (Answer C): This allows the internal device to
initiate a connection, and once established, the specified external host can also initiate new connections to the internal device on the same NAT mapping.
Example Configuration: bash
set security nat source persistent-nat permit target-host-port
This solution is appropriate when controlled bidirectional communication is required based on an internal-initiated connection.
: Juniper persistent NAT documentation.
==========

NEW QUESTION 59
You need to generate a certificate for a PKI-based site-to-site VPN. The peer is expecting to
user your domain name vpn.juniper.net.
Which two configuration elements are required when you generate your certificate request? (Chose two,)

A. ip-address 10.100.0.5
B. subject CN=vpn.juniper.net
C. email admin@juniper.net
D. domain-name vpn.juniper.net

Answer: BD

NEW QUESTION 61
Which two statements are true when setting up an SRX Series device to operate in mixed mode? (Choose two.)

A. A physical interface can be configured to be both a Layer 2 and a Layer 3 interface at the same time.
B. User logical systems support Layer 2 traffic processing.
C. The SRX must be rebooted after configuring at least one Layer 3 and one Layer 2 interface.
D. Packets from Layer 2 interfaces are switched within the same bridge domain.

Answer: CD

Explanation:
In mixed mode, SRX devices can simultaneously handle Layer 2 switching and Layer 3 routing, but a reboot is required when configuring Layer 2 and Layer 3 interfaces to ensure the configuration takes effect. Layer 2 packets are switched within the defined bridge domain. Further guidance on SRX mixed mode can be found at Juniper Mixed Mode Documentation.
When an SRX Series device is configured in mixed mode, both Layer 2 switching and Layer 3 routing functionalities can be used on the same device. This enables the SRX to act as both a router and a switch for different interfaces. However, there are certain considerations:
? Explanation of Answer C (Reboot Requirement):
? Explanation of Answer D (Layer 2 Traffic Handling):
Juniper Security Reference:
? Mixed Mode Overview: Juniper SRX devices can operate in mixed mode to handle both Layer 2 and Layer 3 traffic simultaneously. Reference: Juniper Mixed Mode Documentation.
==========

NEW QUESTION 66
You are configuring an interconnect logical system that is configured as a VPLS switch to allow two logical systems to communicate.
Which two parameters are required when configuring the logical tunnel interfaces?
(Choose two.)

A. Encapsulation ethernet must be used.
B. The virtual tunnel interfaces should only be configured with two logical unit pairs per logical system interconnect.
C. The logical tunnel interfaces should be configured with two logical unit pairs per logical system interconnect.
D. Encapsulation ethernet-vpls must be used.

Answer: CD

NEW QUESTION 67
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your JN0-637 Exam with Our Prep Materials Via below:

https://www.certleader.com/JN0-637-dumps.html