Juniper

Exam Questions JN0-637

Security - Professional (JNCIP-SEC)

NEW QUESTION 1
Exhibit:

```
user@srx1> show chassis high-availability services-redundancy-group 1
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
        Virtual IP Info:
          Index: 2
          IP: 198.51.100.100/24
          VMAC: N/A
          Interface: ge-0/0/3.0
          Status: INSTALLED
          Index: 1
          IP: 10.10.101.1/24
```

```
Peer Information:
  Peer Id: 2
  Status : BACKUP
  Health Status: HEALTHY
  Failover Readiness: READY
Virtual IP Info:
  Index: 2
  IP: 198.51.100.100/24
  VMAC: N/A
  Interface: ge-0/0/3.0
  Status: INSTALLED
  Index: 1
  IP: 10.10.101.1/24
  VMAC: N/A
  Interface: ge-0/0/4.0
  Status: INSTALLED
Split-brain Prevention Probe Info:
    DST-IP: 10.10.101.1
    Routing Instance: default
    Status: NOT RUNNING
    Result: N/A          Reason: N/A
  Interface Monitoring:
Status: UP
    IF Name: ge-0/0/4     State: Up
    IF Name: ge-0/0/3     State: Up
IP SRGID Table:
    SRGID    IP Prefix                              Routing Table
    1        198.51.100.100/32                      default
    1        10.10.101.1/32                         default
```

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

A. The ge-0/0/3.0 and ge-0/0/4.0 interfaces are not active and will not respond to ARP requests to the virtual IP MAC address.
B. This device is the backup node for SRG1.
C. The ge-0/0/3.0 and ge-0/0/4.0 interfaces are active and will respond to ARP requests to the virtual IP MAC address.
D. This device is the active node for SRG1.

Answer: AB

Explanation:
The interfaces are active and respond to ARP for virtual IP as long as the node is the primary or active node in the SRG group. This ensures high availability and proper traffic forwarding. For information, refer to Juniper SRX HA Documentation.
The exhibit shows information about a chassis cluster and its services redundancy group (SRG1). Let's analyze the relevant details:
? Explanation of Answer B (Backup Node for SRG1):
? Explanation of Answer A (Interfaces Not Active):
Juniper Security Reference:
? Chassis Cluster Redundancy Overview: In a chassis cluster, the backup node does not respond to ARP requests for the virtual IP. Only the active node handles such requests to ensure seamless traffic forwarding. Reference: Juniper Chassis Cluster Documentation.
==========

NEW QUESTION 2
Which encapsulation type must be configured on the lt-0/0/0 logical units for an interconnect logical systems VPLS switch?

A. encapsulation ethernet-bridge
B. encapsulation ethernet
C. encapsulation ethernet-vpls
D. encapsulation vlan-vpls

Answer: C

NEW QUESTION 3
Which two statements describe the behavior of logical systems? (Choose two.)

A. Each logical system shares the routing protocol process.
B. A default routing instance must be manually created for each logical system

C. Each logical system has a copy of the routing protocol process.
D. A default routing instance is automatically created for each logical system.

Answer: CD

NEW QUESTION 4
How does an SRX Series device examine exception traffic?

A. The device examines the host-inbound traffic for the ingress interface and zone.
B. The device examines the host-outbound traffic for the ingress interface and zone.
C. The device examines the host-inbound traffic for the egress interface and zone.
D. The device examines the host-outbound traffic for the egress interface and zone.

Answer: A

Explanation:
Exception traffic, including management and control plane traffic, is handled by examining host-inbound traffic configurations at the ingress interface and zone. It ensures traffic reaches necessary services like SSH and IKE securely. See Juniper Host Inbound Traffic Documentation for more.
SRX Series devices handle exception traffic (such as management traffic like SSH, Telnet, DNS queries, etc.) differently than regular transit traffic. Exception traffic is examined based
on host-inbound traffic for the ingress interface and zone. If traffic is destined for the device itself (e.g., management traffic or routing protocol messages), it must be allowed as host-inbound traffic on both the ingress interface and zone.
Example Command: bash
set security zones security-zone trust host-inbound-traffic system-services ssh
This ensures that traffic destined to the SRX device is inspected based on the ingress interface and zone.
: Juniper documentation on host-inbound traffic and exception handling.
==========

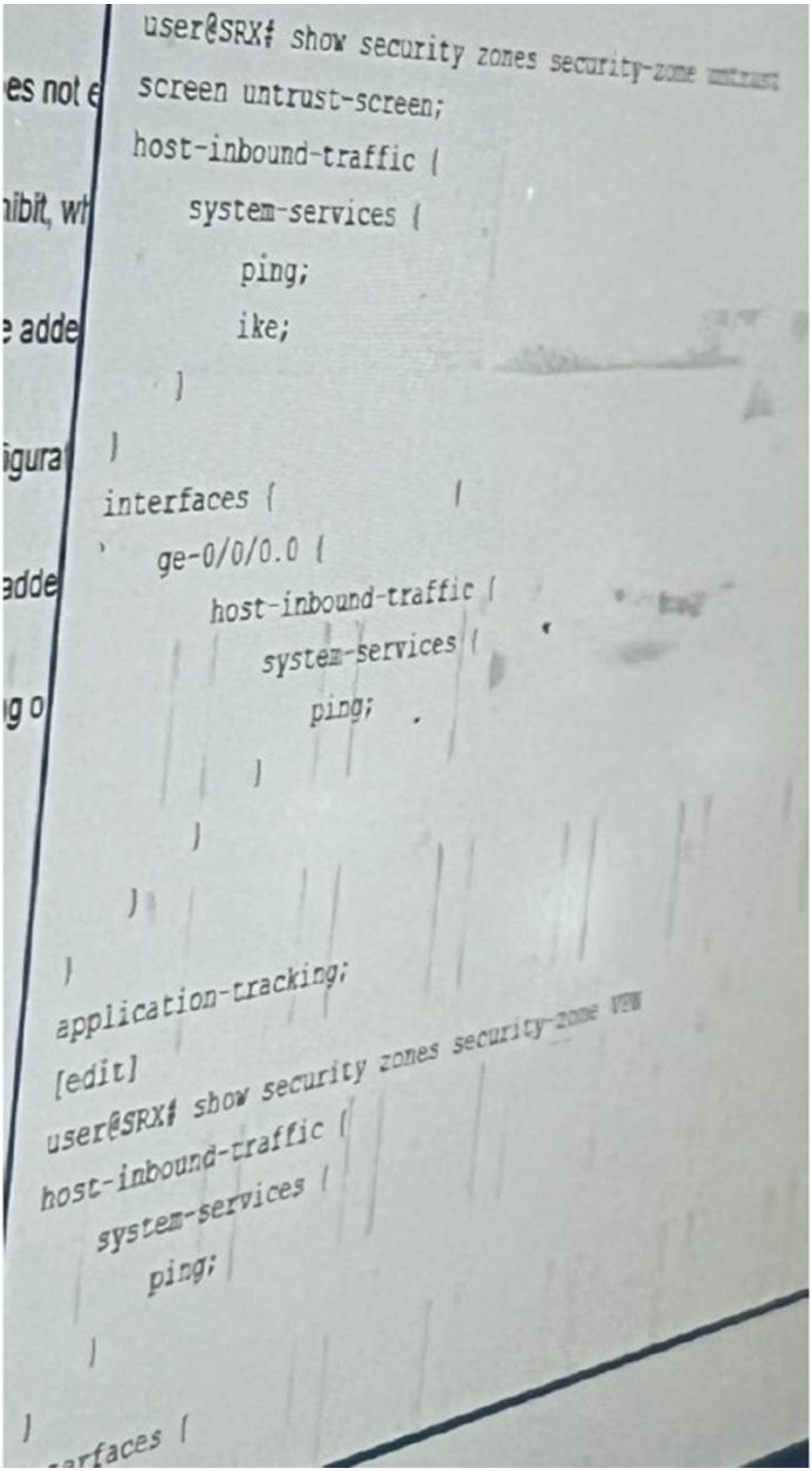
NEW QUESTION 5
You configure two Ethernet interfaces on your SRX Series device as Layer 2 interfaces and add them to the same VLAN. The SRX is using the default L2-learning setting. You do not add the interfaces to a security zone.
Which two statements are true in this scenario? (Choose two.)

A. You are unable to apply stateful security features to traffic that is switched between the two interfaces.
B. You are able to apply stateful security features to traffic that enters and exits the VLAN.
C. The interfaces will not forward traffic by default.
D. You cannot add Layer 2 interfaces to a security zone.

Answer: AC

Explanation:
When Ethernet interfaces are configured as Layer 2 and added to the same VLAN without being assigned to a security zone, they will not forward traffic by default. Additionally, because they are operating in a pure Layer 2 switching mode, they lack the capability to enforce stateful security policies. For further details, refer to Juniper Ethernet Switching Layer 2 Documentation.
? Explanation of Answer A (Unable to Apply Stateful Security Features):
? Explanation of Answer C (Interfaces Will Not Forward Traffic):
Juniper Security Reference:
? Layer 2 Interface Configuration: Layer 2 interfaces must be properly assigned to security zones to enable traffic forwarding and apply security policies.
Reference: Juniper Networks Layer 2 Interface Documentation.
==========

NEW QUESTION 6
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 7
Exhibit:

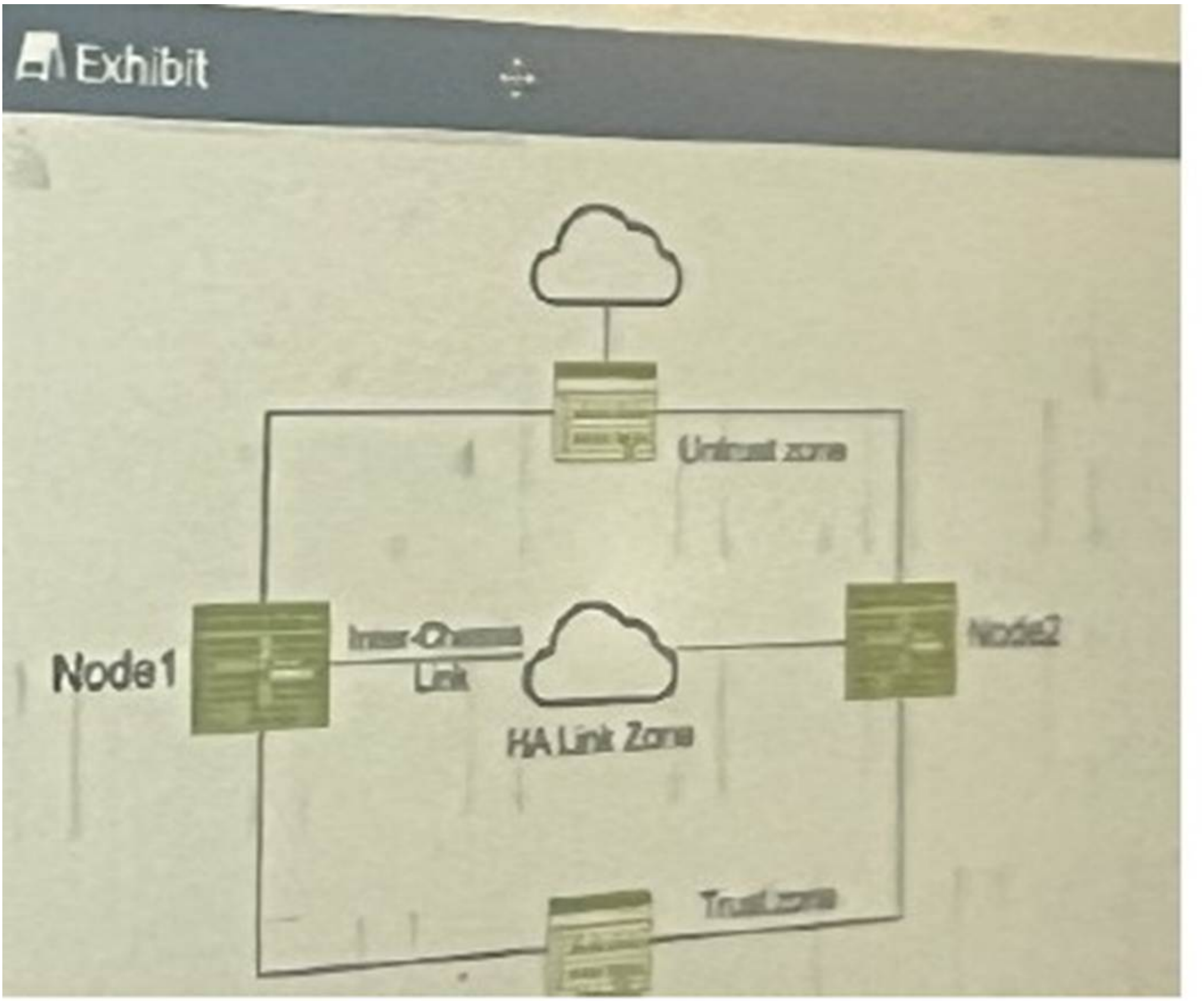
```
[edit]
user@srx# show security nat
source {
    pool ipv4-source-pool {
        address {
            10.10.101.10/32;
        }
    }
    rule-set ipv6-source {
        from zone trust;
        to zone untrust;
        rule ipv6-host-source {
            match {
                source-address 2001:db8::1/128;
                destination-address 10.10.201.10/32;
            }
            then {
                source-nat {
                    pool {
                        ipv4-source-pool;
                    }
                }
            }
        }
    }
}
```

You are configuring NAT64 on your SRX Series device. You have committed the configuration shown in the exhibit. Unfortunately, the communication with the 10.10.201.10 server is not working. You have verified that the interfaces, security zones, and security policies are all correctly configured.
In this scenario, which action will solve this issue?

A. Configure source NAT to translate return traffic from IPv4 address to the IPv6 address of your source device.
B. Configure proxy-ARP on the external IPv4 interface for the 10.10.201.10/32 address.
C. Configure proxy-NDP on the IPv6 interface for the 2001:db8::1/128 address.
D. Configure destination NAT to translate return traffic from the IPv4 address to the IPv6 address of your source device.

Answer: D

NEW QUESTION 8
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 9
You have cloud deployments in Azure, AWS, and your private cloud. You have deployed
multicloud using security director with policy enforcer to. Which three statements are true in this scenario? (Choose three.)

A. You can run Juniper ATP scans only on traffic from your private cloud.
B. You can run Juniper ATP scans for all three domains.
C. You must secure the policies individually by domain.
D. The Policy Enforcer is able to flag infected hosts in all three domains.
E. You can simultaneously manage the security policies in all three domains.

Answer: BDE

NEW QUESTION 10
Which two statements about the differences between chassis cluster and multinode HA on SRX series devices are true? (Choose Two)

A. Multinode HA member nodes require Layer 2 connectivity.
B. Multinode HA supports Layer 2 and Layer 3 connectivity between nodes.
C. Multinode HA requires Layer 3 connectivity between nodes.
D. Chassis cluster member nodes require Layer 2 connectivity.

Answer: BD

NEW QUESTION 10
Exhibit:

```
[edit]
user@RemoteSite1# show interfaces
ge-0/0/2 {
    unit 0 {
        family inet {
            dhcp;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.0.0.2/30;
        }
    }
}
[edit security zones]
user@RemoteSite1# show security-zone untrust
interfaces {
    ge-0/0/2.0 {
        host-inbound-traffic {
            system-services {
                ike;
                dhcp;
            }
        }
    }
}
```

```
[edit security ike]
user@RemoteSite1# show
policy ike-policy-1 {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$6st6CpOhSeX7V1R7VwYZG1AB"; ## SECRET-DATA
}
gateway gateway-1 {
    ike-policy ike-policy-1;
    address 203.0.113.5;
    local-identity hostname "RemoteSite1@srx.juniper.net";
    external-interface ge-0/0/2;
}
[edit security ike]
user@corporate# show
policy ike-policy-site1 {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$6st6CpOhSeX7V1R7VwYZG1AB"; ## SECRET-DATA
}
gateway gateway-site1 {
    ike-policy ike-policy-site1;
    dynamic hostname "RemoteSite1@srx.juniper.net";
    external-interface ge-0/0/1;
}
```

You are troubleshooting a new IPsec VPN that is configured between your corporate office and the RemoteSite1 SRX Series device. The VPN is not currently establishing. The RemoteSite1 device is being assigned an IP address on its gateway interface using DHCP.
Which action will solve this problem?

A. On the RemoteSite1 device, change the IKE gateway external interface to st0.0.
B. On both devices, change the IKE version to use version 2 only.
C. On both devices, change the IKE policy proposal set to basic.
D. On both devices, change the IKE policy mode to aggressive.

Answer: D

Explanation:
Aggressive mode is required when an IP address is dynamically assigned, such as through DHCP, as it allows for faster establishment with less identity verification. More details are available in Juniper IKE and IPsec Configuration Guide.
The configuration shown in the exhibit highlights that the RemoteSite1 SRX Series device is using DHCP to obtain an IP address for its external interface (ge-0/0/2). This introduces a challenge in IPsec VPN configurations when the public IP address of the remote site is not static, as is the case here.
Aggressive mode in IKE (Internet Key Exchange) is designed for situations where one or both peers have dynamically assigned IP addresses. In this scenario, aggressive mode allows the devices to exchange identifying information, such as hostnames, rather than relying on static IP addresses, which is necessary when the remote peer (RemoteSite1) has a dynamic IP from DHCP.
? Correct Action (D): Changing the IKE policy mode to aggressive will resolve the
issue by allowing the two devices to establish the VPN even though one of them is using DHCP. In aggressive mode, the initiator can present its identity (hostname) during the initial handshake, enabling the VPN to be established successfully.
? Incorrect Options:
Juniper References:
? Juniper IKE and VPN Documentation: Provides details on when to use aggressive mode, especially when a dynamic IP address is involved.
==========

NEW QUESTION 14
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

NEW QUESTION 15
You are deploying IPsec VPNs to securely connect several enterprise sites with ospf for dynamic routing. Some of these sites are secured by third-party devices not running Junos.
Which two statements are true for this deployment? (Choose two.)

A. OSPF over IPsec can be used for intersite dynamic routing.

B. Sites with overlapping address spaces can be supported.
C. OSPF over GRE over IPsec is required to enable intersite dynamic routing
D. Sites with overlapping address spaces cannot be supported.

Answer: BC

Explanation:
Understanding the Scenario:
? Objective: Deploy IPsec VPNs connecting multiple enterprise sites using OSPF for dynamic routing.
? Challenge: Some sites use third-party devices not running Junos OS.
? Considerations:
Option Analysis:
Option A: OSPF over IPsec can be used for intersite dynamic routing.
? Explanation:
Reference:
"OSPF can be run over IPsec VPNs using route-based VPNs, but interoperability with third- party devices must be verified."
Source: Juniper TechLibrary - OSPF over IPsec VPNs
Option B: Sites with overlapping address spaces can be supported.
* Explanation:
Overlapping IP Address Spaces:
Occurs when different sites use the same IP subnets. Can cause routing ambiguities and conflicts. Solution:
NAT over VPN:
Use Network Address Translation (NAT) to translate overlapping IP addresses to unique addresses.
Juniper devices support NAT over IPsec VPNs. Third-Party Device Considerations:
Need to ensure third-party devices support NAT over IPsec.
Many enterprise-grade devices provide this functionality.
Conclusion:
Option B is true; overlapping address spaces can be supported using NAT.
Reference:
"When sites have overlapping IP addresses, NAT can be used over IPsec VPNs to resolve address conflicts."
Source: Juniper TechLibrary - NAT with IPsec VPNs
Option C: OSPF over GRE over IPsec is required to enable intersite dynamic routing.
* Explanation: GRE Tunnels:
Generic Routing Encapsulation (GRE) can encapsulate multicast and broadcast traffic. Allows OSPF packets to be transmitted over IPsec VPNs.
IPsec Encryption:
GRE tunnels can be encrypted using IPsec for secure communication.
Interoperability:
GRE over IPsec is a common method to support OSPF between devices from different vendors.
Third-party devices are more likely to support GRE over IPsec than OSPF over IPsec directly.
Conclusion:
Option C is true; using OSPF over GRE over IPsec is required in this scenario.
Reference:
"To run OSPF between devices that do not support multicast over IPsec, GRE tunnels can be used over IPsec VPNs."
Source: Juniper TechLibrary - Configuring GRE over IPsec
Option D: Sites with overlapping address spaces cannot be supported.
* Explanation:
Contradicts Option B.
As established, overlapping address spaces can be supported using NAT over IPsec VPNs.
Conclusion: Option D is false.
Conclusion:
Correct Answers: B and C
Option B: Overlapping address spaces can be supported using NAT over IPsec VPNs.
Option C: OSPF over GRE over IPsec is required to enable intersite dynamic routing, especially when third-party devices are involved.
Additional Detailed Explanation:
Why OSPF over IPsec May Not Be Feasible (Option A): Multicast Traffic:
OSPF relies on multicast for neighbor discovery and updates. IPsec in tunnel mode does not natively support multicast traffic. Third-Party Devices:
May not support proprietary extensions or configurations required to run OSPF directly over IPsec.
Workaround:
Encapsulate OSPF multicast packets within GRE tunnels, which can carry multicast traffic over unicast IPsec tunnels.
Why OSPF over GRE over IPsec Is Necessary (Option C): GRE Tunnels:
Encapsulate multicast/broadcast traffic into unicast packets. Allow routing protocols like OSPF to function over IPsec VPNs. Compatibility:
GRE is a widely supported protocol across different vendors.
Facilitates interoperability between Juniper and third-party devices.
Supporting Overlapping Address Spaces (Option B): NAT over IPsec:
Translates private IP addresses to unique addresses across the VPN.
Prevents routing conflicts and allows communication between sites with overlapping subnets.
Considerations:
Requires proper configuration on both ends of the VPN tunnel. Third-party devices must support NAT over IPsec. References to Juniper Security Concepts:
Route-Based VPNs:
"Route-based VPNs use virtual tunnel interfaces (st0) and support dynamic routing protocols over IPsec."
Source: Juniper TechLibrary - Route-Based VPNs
GRE over IPsec:
"GRE over IPsec allows the transmission of multicast and non-IP protocols over IPsec tunnels."
Source: Juniper TechLibrary - GRE over IPsec Overview
NAT with IPsec VPNs:
"NAT can be applied to IPsec VPN traffic to resolve overlapping address issues and facilitate communication between sites."
Source: Juniper TechLibrary - NAT with IPsec
Final Notes: Interoperability:
When working with third-party devices, always verify compatibility for protocols and features.
Best Practices:
Use GRE over IPsec for dynamic routing protocols requiring multicast support across IPsec VPNs.
Implement NAT over VPN when dealing with overlapping address spaces.

NEW QUESTION 20
You have deployed a new site as shown in the exhibit. Hosts in the 10.10.10.0/24 network
must access the DB1 server. The DB1 server must also have internet access the DB1 server encrypted.
Which two configuration statements will be required as part of the configuration on SRX1 to satisfy this requirement? (Choose two)

A. set security macsec interfaces ge-0/0/1 connectivity association access-sw
B. set protocols 12-learning global mode transpårent-bridge
C. set security forwarding-options secure-wire access-sw interface ge-0/0/1.0
D. set security macsec connectivity-association access-sw security-mode static-cak

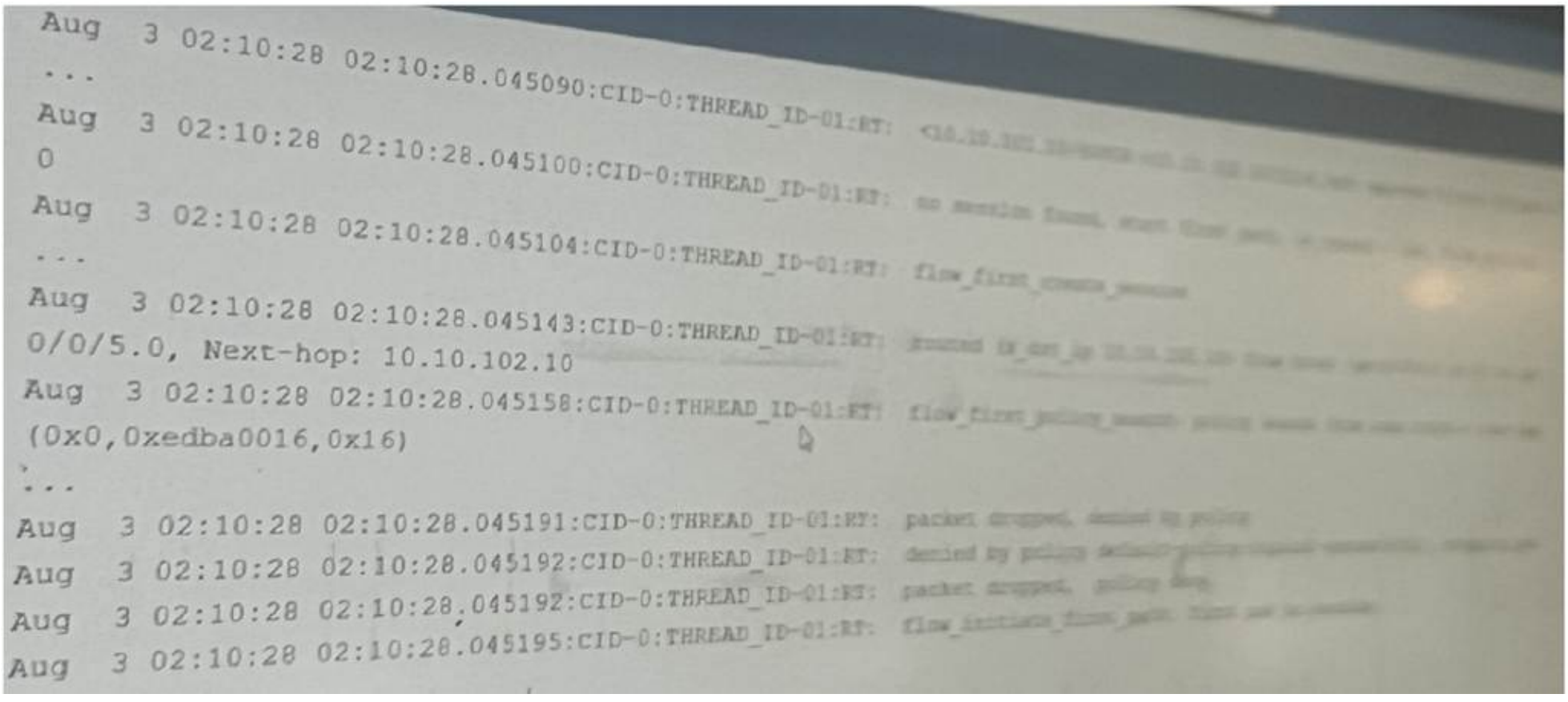
Answer: AD

NEW QUESTION 21
You are asked to select a product offered by Juniper Networks that can collect and assimilate data from all probes and determine the optimal links for different applications to maximize the full potential of AppQoE.
Which product provides this capability?

A. Security Director
B. Network Director
C. Mist
D. Security Director Insights

Answer: C

NEW QUESTION 25
Exhibit:



Which two statements are correct about the output shown in the exhibit. (Choose Two)

A. The data shown requires a traceoptions flag of basic-datapath.
B. The data shown requires a traceoptions flag of host-traffic.
C. The packet is dropped by the default security policy.
D. The packet is dropped by a configured security policy.

Answer: AC

NEW QUESTION 26
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.)

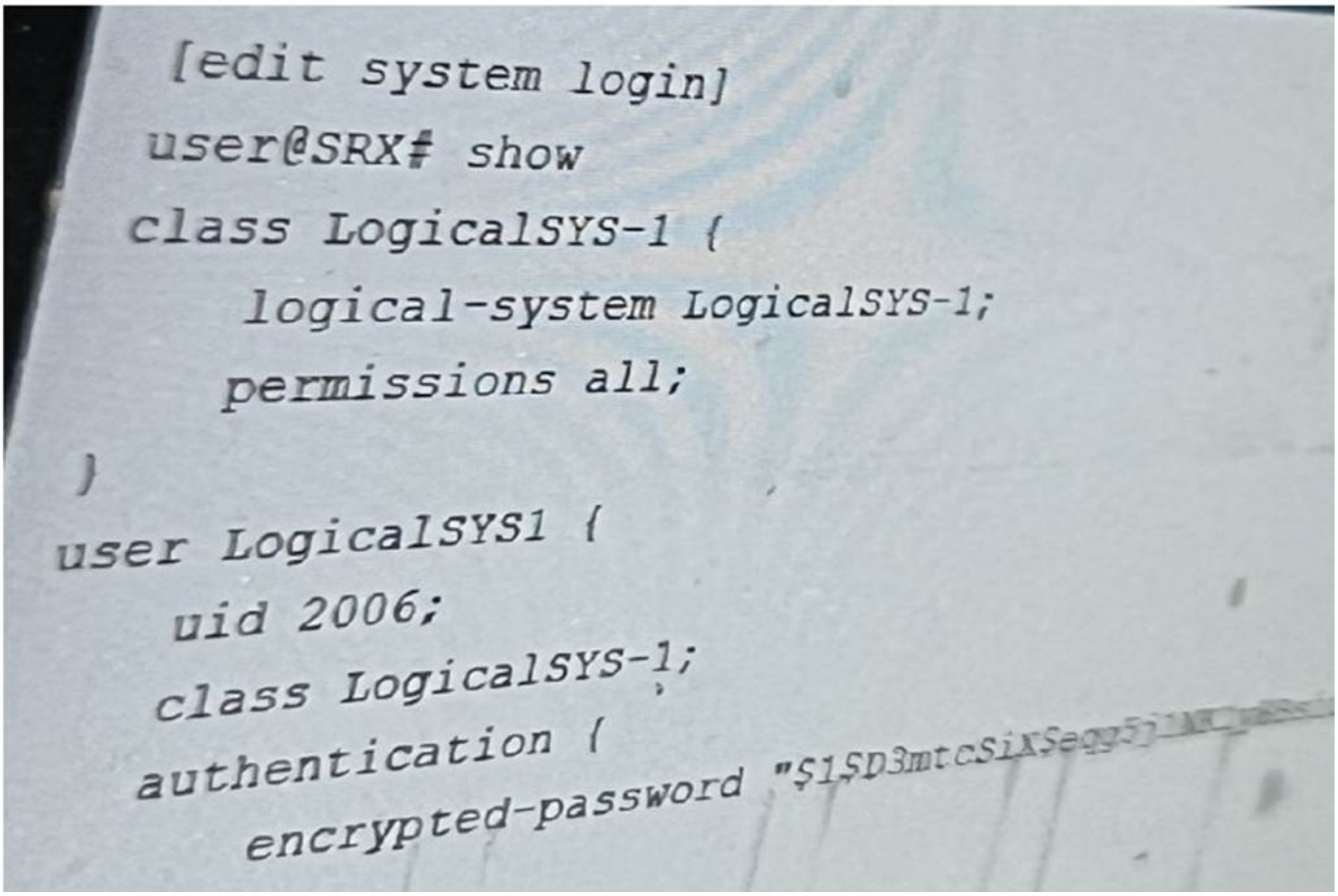
A. address persistence
B. STUN
C. persistent NAT
D. double NAT

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 29
Referring to the exhibit, you have been assigned the user LogicalSYS1 credentials shown in
the configuration.



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

A. When you log in to the device, you will be permitted to view all routing tables available on the SRX device
B. When you log in to the device, you will be permitted to view only the routing tables for Logic
C. When you log in to the device, you will be located at the operational mode of the Logic
D. When you log in to the device, you will be located at the operational mode of the main system

Answer: BC

NEW QUESTION 30
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 34
Which two statements are correct about mixed mode? (Choose two.)

A. Layer 2 and Layer 3 interfaces can use the same security zone.
B. IRB interfaces can be used to route traffic.
C. Layer 2 and Layer 3 interfaces can use separate security zones.
D. IRB interfaces cannot be used to route traffic.

Answer: BC

NEW QUESTION 35
What are three attributes that APBR queries from the application system cache module. (Choose Three)

A. TTL
B. destination port
C. service
D. DSCP
E. protocol type

Answer: BCE

NEW QUESTION 39
Exhibit:

```
Aug  3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT:  <10.10.101.10/60858->10.10.102.10/22;6,0x0> matched filter filter-1:
...
Aug  3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT:  no session found, start first path. in_tunnel - 0x0, from_cp_flag -
0
Aug  3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT:  flow_first_create_session
...
Aug  3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT:  routed (x_dst_ip 10.10.102.10) from trust (ge-0/0/4.0 in 0) to ge-
0/0/5.0, Next-hop: 10.10.102.10
Aug  3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT:  flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xedba0016,0x16)
...
Aug  3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT:  packet dropped, denied by policy
Aug  3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT:  denied by policy default-policy-logical-system-00(2), dropping pkt
Aug  3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT:  packet dropped,  policy deny.
Aug  3 02:10:28 02:10:28.045195:CID-0:THREAD_ID-01:RT:  flow_initiate_first_path: first pak no session
```

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

A. The packet is dropped by the default security policy.
B. The packet is dropped by a configured security policy.
C. The data shown requires a traceoptions flag of host-traffic.
D. The data shown requires a traceoptions flag of basic-datapath.

Answer: AD

Explanation:
? Understanding the Flow Log Output:
From the flow logs in the exhibit, we can observe the following key events:
? uk.co.certification.simulator.questionpool.PList@30863efa
? Explanation of Answer A (Dropped by the default security policy):
The log message clearly states that the packet was dropped by the default security policy (default-policy-logical-system-00). In Junos, when a session is attempted between two zones and no explicit policy exists to allow the traffic, the default policy is to deny the traffic. This is a common behavior in Junos OS when a security policy does not explicitly allow traffic between zones.
? Explanation of Answer D (Requires traceoptions flag of basic-datapath):
The information displayed in the log involves session creation, flow policy search, and packet dropping due to policy violations, which are all part of basic packet processing in the data path. This type of information is logged when the traceoptions flag is set to basic- datapath. The basic-datapath traceoption provides detailed information about the forwarding process, including policy lookups and packet drops, which is precisely what we see in the exhibit.
? uk.co.certification.simulator.questionpool.PList@2aaa48ae
Step-by-Step Configuration for Tracing (Basic-Datapath):
? Enable flow traceoptions:
To capture detailed information about how traffic is being processed, including policy lookups and flow session creation, enable traceoptions for the flow.
bash
set security flow traceoptions file flow-log
set security flow traceoptions flag basic-datapath
? Apply the configuration and commit:
bash
commit
? View the logs:
Once enabled, you can check the trace logs for packet flows, policy lookups, and session creation details:
bash
show log flow-log
This log will contain information similar to the exhibit, including session creation attempts and packet drops due to security policy.

Juniper Security Reference:
? Default Security Policies: Juniper SRX devices have a default security policy to deny all traffic that is not explicitly allowed by user-defined policies. This is essential for security best practices. Reference: Juniper Networks Documentation on Security Policies.
? Traceoptions for Debugging Flows: Using traceoptions is crucial for debugging and understanding how traffic is handled by the SRX, particularly when issues arise from policy misconfigurations or routing. Reference: Juniper Traceoptions.
By using the basic-datapath traceoptions, you can gain insights into how the device processes traffic, including policy lookups, route lookups, and packet drops, as demonstrated in the exhibit.
==========

NEW QUESTION 44
Which two statements are true regarding NAT64? (Choose two.)

A. An SRX Series device should be in flow-based forwarding mode for IPv4.
B. An SRX Series device should be in packet-based forwarding mode for IPv4.
C. An SRX Series device should be in packet-based forwarding mode for IPv6.
D. An SRX Series device should be in flow-based forwarding mode for IPv6.

Answer: AD

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding NAT64:
? NAT64 allows IPv6-only clients to communicate with IPv4 servers by translating IPv6 addresses to IPv4 addresses and vice versa.
? It is essential in environments where IPv6 clients need access to IPv4 resources.
Flow-Based vs. Packet-Based Forwarding Modes:
? Flow-Based Forwarding Mode:
? Packet-Based Forwarding Mode:
? Option A: An SRX Series device should be in flow-based forwarding mode for IPv4.
? Option B: An SRX Series device should be in packet-based forwarding mode for IPv4.
? Option C: An SRX Series device should be in packet-based forwarding mode for IPv6.
? Option D: An SRX Series device should be in flow-based forwarding mode for IPv6.
Key Points:
? NAT64 Requires Flow-Based Mode:
? Packet-Based Mode Limitations:
Juniper Security References:
? Juniper Networks Documentation:
? Understanding Flow-Based and Packet-Based Modes:
Conclusion:
? To implement NAT64 on an SRX Series device, both IPv4 and IPv6 traffic must be processed in flow-based forwarding mode.
? Therefore, Options A and D are the correct statements.

NEW QUESTION 48
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)
```

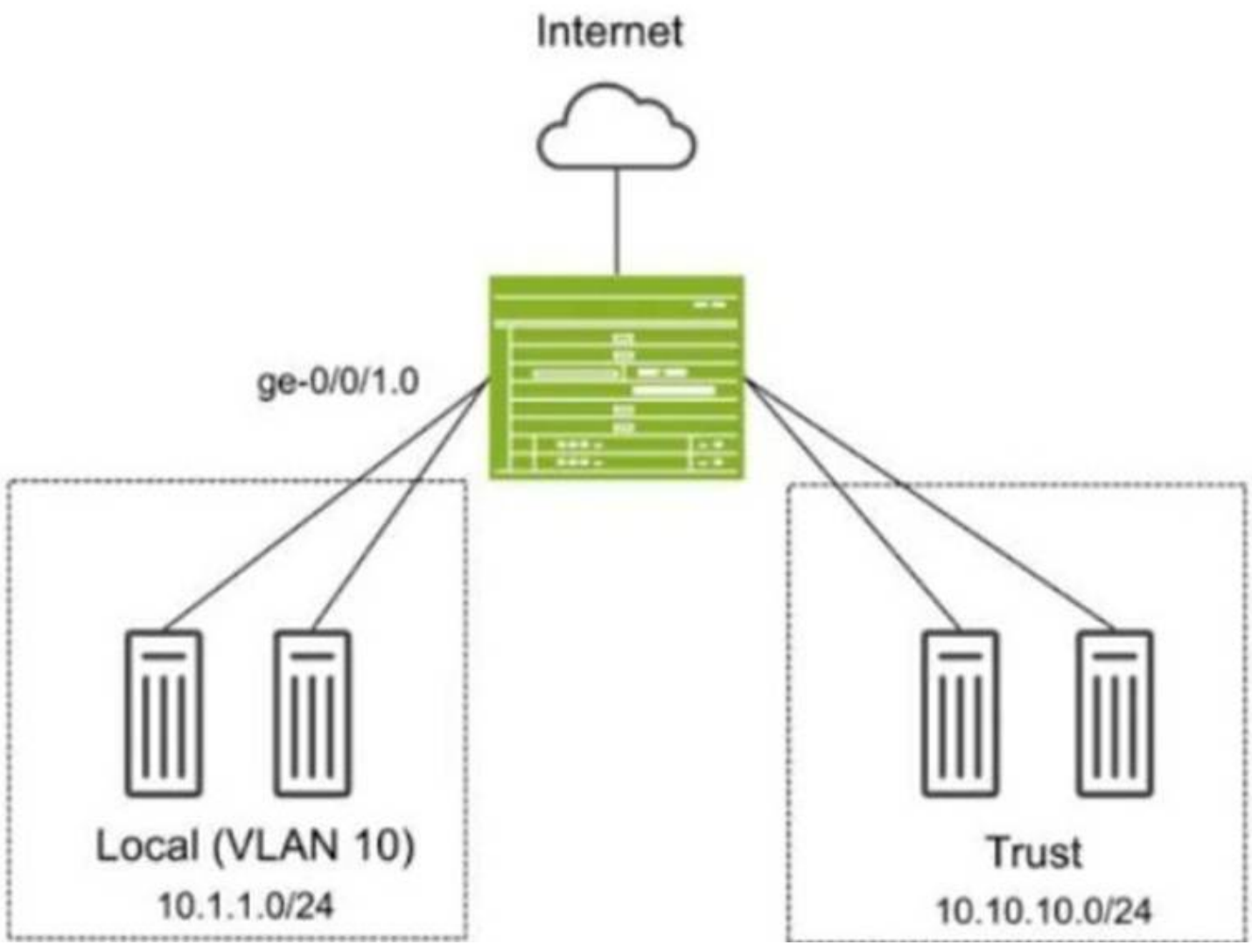
```
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0,0xd66200b3,0xb3)
Mar  7 02:38:15 02:38:15.353986:CID-0:THREAD_ID-01:RT: Policy lkup: vsys 0 zone(5:global) -> zone(5:global) scope:0
…
Mar  7 02:38:15 02:38:15.354000:CID-0:THREAD_ID-01:RT: 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 02:38:15.353978: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 53
Exhibit:



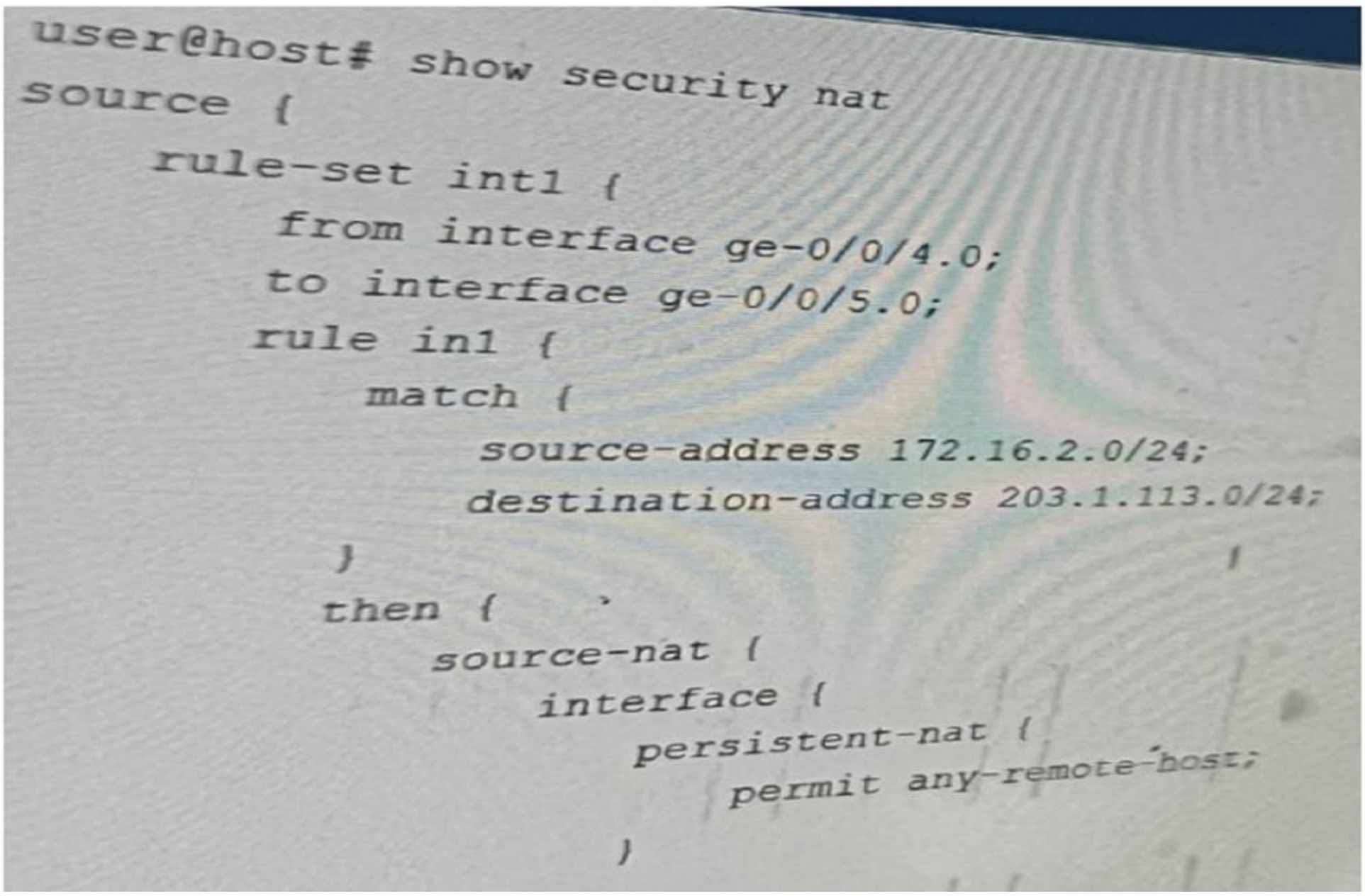
You have deployed an SRX Series device as shown in the exhibit. The devices in the Local zone have recently been added, but their SRX interfaces have not been configured. You must configure the SRX to meet the following requirements:
? Devices in the 10.1.1.0/24 network can communicate with other devices 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.
? Explanation of Answer A (Assigning Interface to Security Zone):
set security zones security-zone Local interfaces ge-0/0/1.0
? Explanation of Answer B (Configuring Ethernet-Switching for VLAN 10):
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan-members 10
? Explanation of Answer D (Transparent Bridging Mode for Layer 2):
set protocols l2-learning global-mode transparent-bridge
Summary:
? Interface Assignment: Interface ge-0/0/1.0 is assigned to the Local zone to allow policy enforcement.
? Ethernet-Switching: The interface is configured for Layer 2 Ethernet switching in VLAN 10.
? Transparent Bridging: The SRX is configured in Layer 2 transparent-bridge mode for switching between devices.
Juniper Security Reference:
? Layer 2 Bridging and Switching Overview: This mode allows the SRX to act as a Layer 2 switch for forwarding traffic between VLAN members without routing.
Reference: Juniper Transparent Bridging Documentation.
==========

NEW QUESTION 54
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 57
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 58
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;
                        }
                    }
                }
            }
        }
    }
}
```

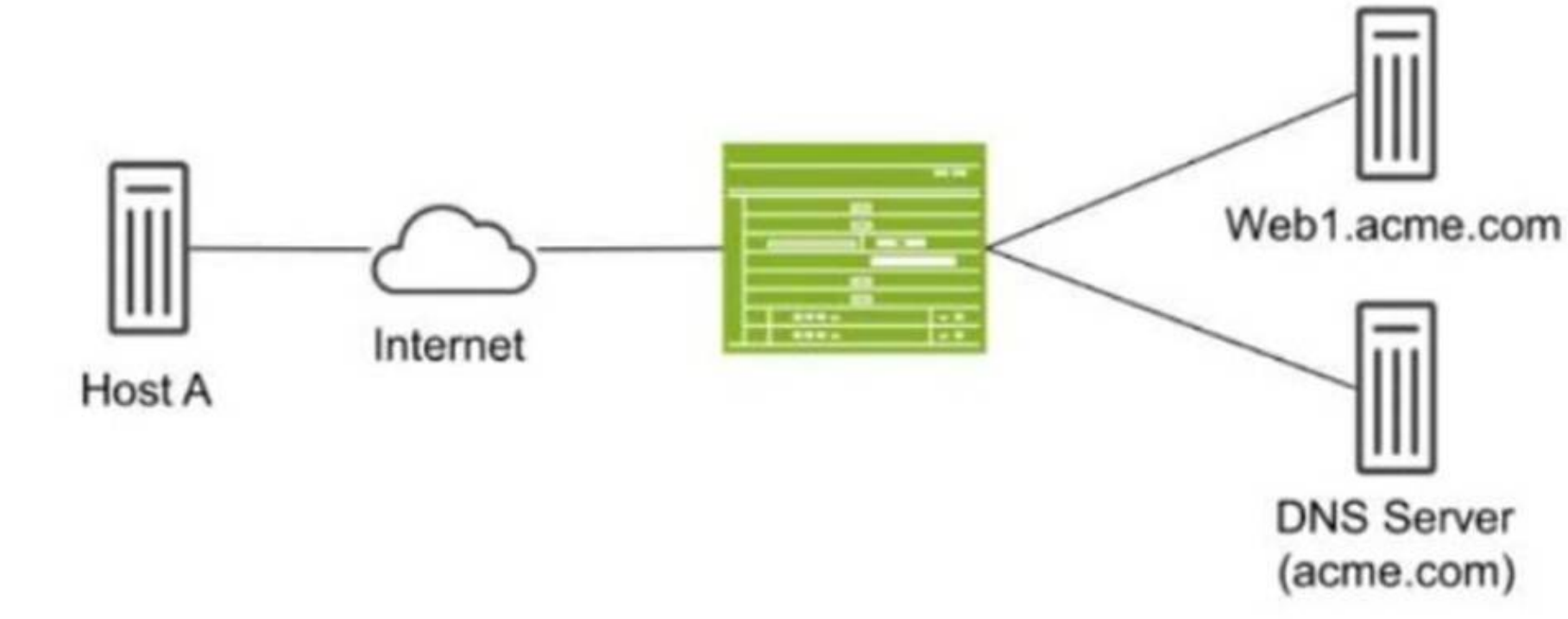
which two statements are correct about the NAT configuration? (Choose two.)

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 62
Exhibit:



Host A shown in the exhibit is attempting to reach the Web1 webserver, but the connection is failing. Troubleshooting reveals that when Host A attempts to resolve the domain name of the server (web.acme.com), the request is resolved to the private address of the server rather than its public IP.
Which feature would you configure on the SRX Series device to solve this issue?

A. Persistent NAT
B. Double NAT
C. DNS doctoring
D. STUN protocol

Answer: C

Explanation:
DNS doctoring modifies DNS responses for hosts behind NAT devices, allowing them to receive the correct public IP address for internal resources when queried from the public network. This prevents issues where private IPs are returned and are not reachable externally. For details, visit Juniper DNS Doctoring Documentation.
In this scenario, Host A is trying to resolve the domain name web.acme.com, but the DNS resolution returns the private IP address of the web server instead of its public IP. This is a common issue in networks where private addresses are used internally, but public addresses are required for external clients.
? Explanation of Answer C (DNS Doctoring):
Configuration Example:
bash
set security nat dns-doctoring from-zone untrust to-zone trust
Juniper Security Reference:
? DNS Doctoring Overview: DNS doctoring is used to modify DNS responses so that external clients can access internal resources using public IP addresses.
Reference: Juniper DNS Doctoring Documentation.
==========

NEW QUESTION 64
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 68
Referring to the exhibit,

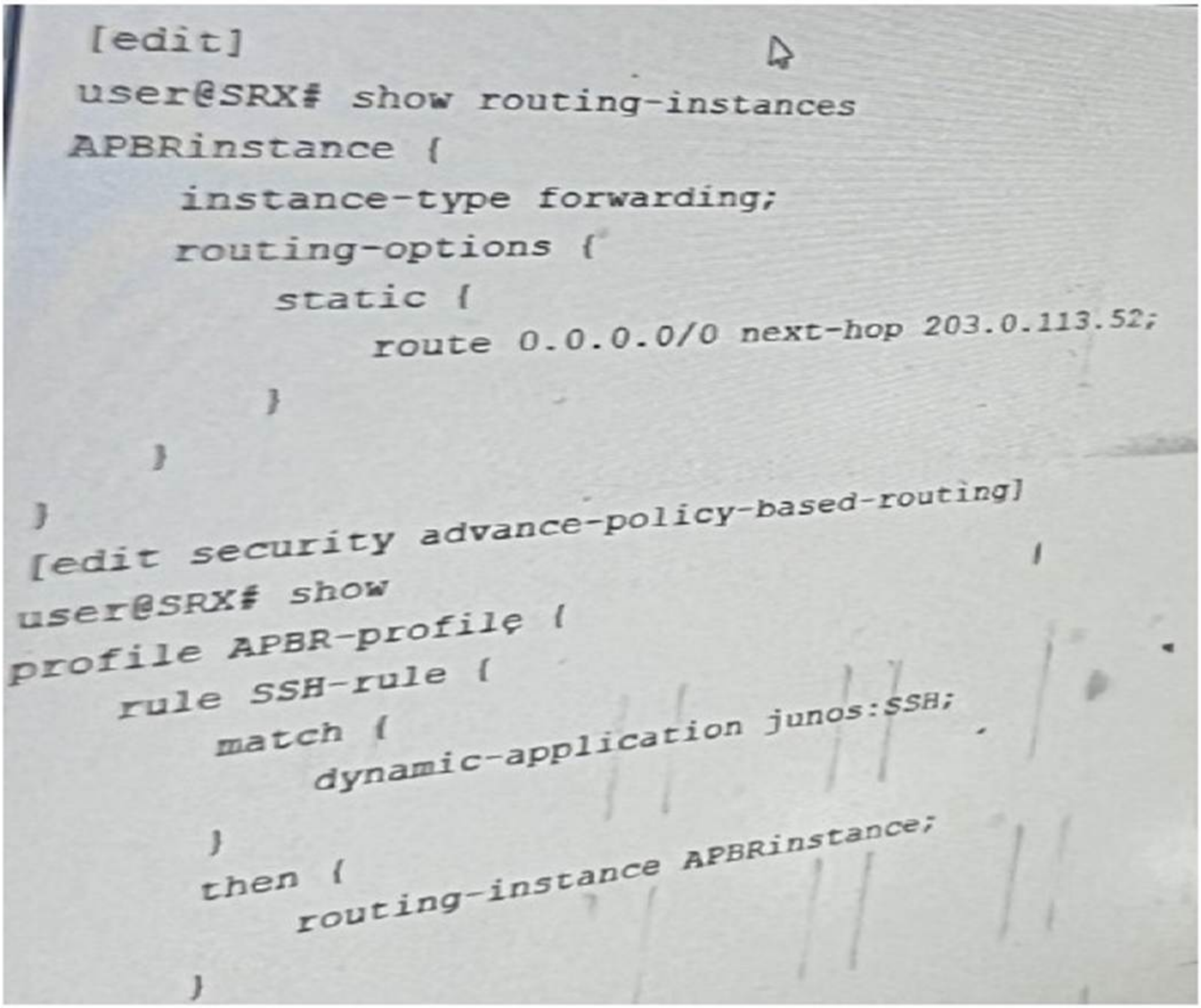
```
[edit security nat]
user@srx# show
source {
    interface {
        port-overloading off;
    }
    rule-set rule1 {
        from zone trust;
        to zone untrust;
        rule allow {
            match {
                source-address 172.16.1.0/24;
                destination-address 0.0.0.0/0;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

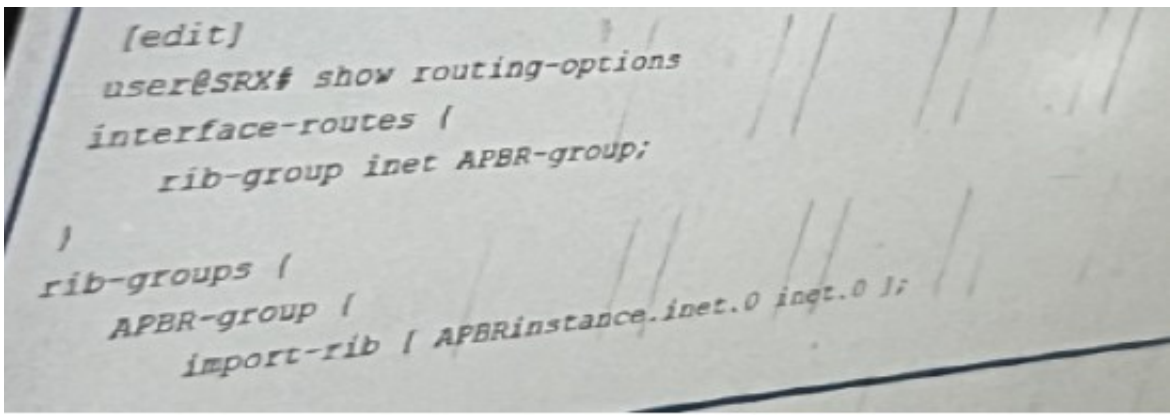
which two statements are correct about the NAT configuration? (Choose two.)

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: AB

NEW QUESTION 73
You are configuring advanced policy-based routing. You have created a static route with next hop of an interface in your inet.0 routing table





Referring to the exhibit, what should be changed to solve this issue?

A. You should change the routing instance type to virtual-router.
B. You should move the static route configuration to the main routing instance.
C. You should move the ine
D. o table before the routing instance table in your rib-groups configuration.
E. You should delete the interface-routes configuration under the routing-options hierarchy.

Answer: C

NEW QUESTION 78
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?

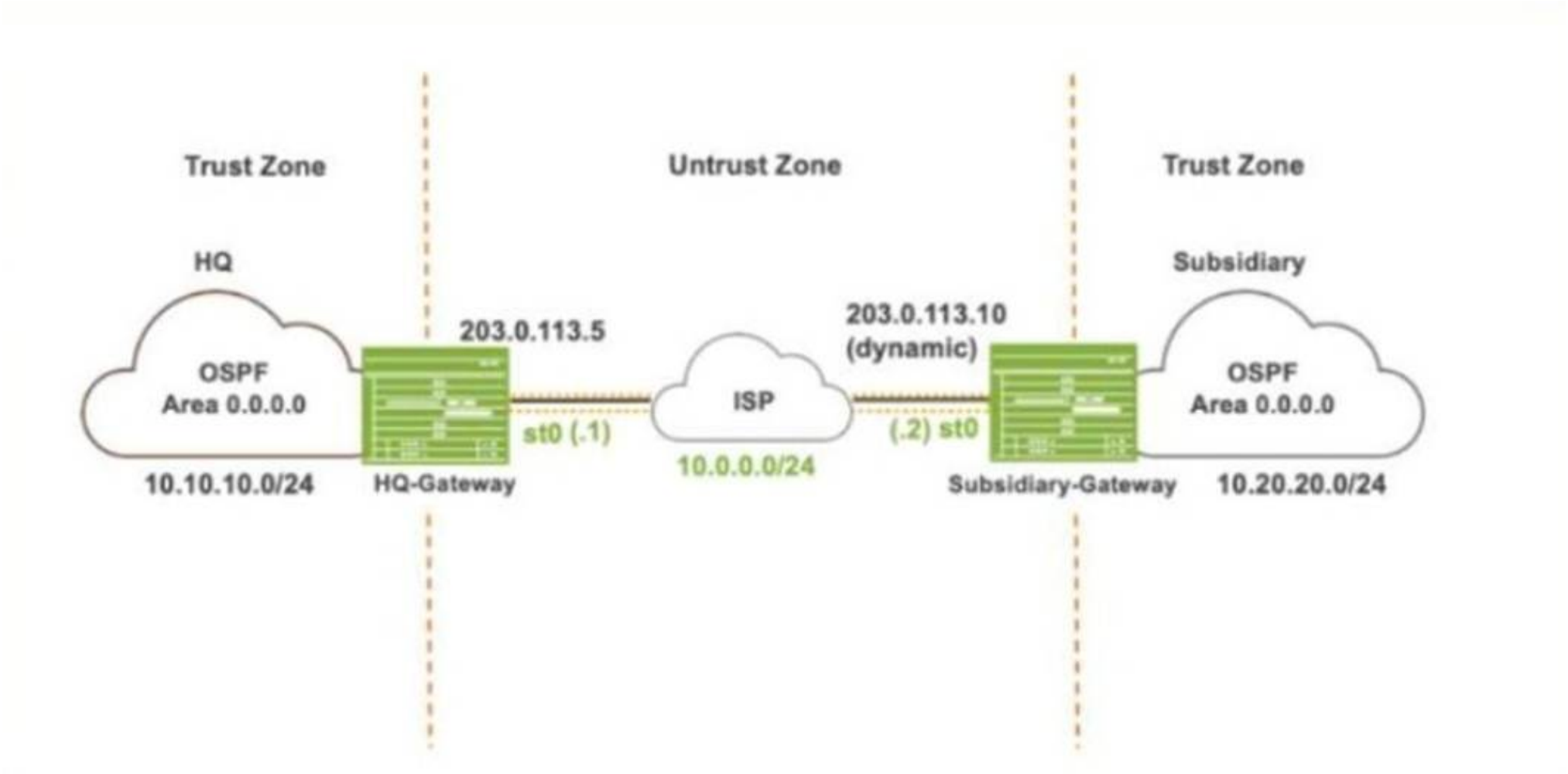
A. SRG1 is configured in hybrid mode.
B. The ICL is encrypted.
C. If SRG1 moves to peer 2, peer 1 will drop packets sent to the SRG1 interfaces.
D. If SRG1 moves to peer 2, peer 1 will forward packets sent to the SRG1 interfaces.

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.

? Explanation of Answer D (Packet Forwarding after Failover):
Juniper Security Reference:
? Chassis Cluster Failover Behavior: When a service redundancy group fails over to the backup peer, the previously active peer forwards traffic to the new active node. Reference: Juniper Chassis Cluster Documentation.
==========

NEW QUESTION 80
Exhibit:



Referring to the exhibit, which IKE mode will be configured on the HQ-Gateway and Subsidiary-Gateway?

A. Main mode on both the gateways
B. Aggressive mode on both the gateways
C. Main mode on the HQ-Gateway and aggressive mode on the Subsidiary-Gateway
D. Aggressive mode on the HQ-Gateway and main mode on the Subsidiary-Gateway

Answer: B

NEW QUESTION 83
A company has acquired a new branch office that has the same address space of one of its local networks, 192.168.100/24. 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: AD

Explanation:
The problem describes two offices needing to communicate, but both share the same IP address space, 192.168.100.0/24. To resolve this, NAT must be configured to translate the conflicting address spaces on each side. Here??s how each of the configurations works:
? Option A (Correct):This source NAT rule translates the source address of traffic
from Office B to Office A. By configuring source NAT, the source IP addresses from Office B (192.168.210.0/24) will be translated when communicating with Office A (192.168.200.0/24). This method ensures that there is no overlap in address space when packets are transmitted between the two offices.
? Option D (Correct):This is a source NAT rule configured on Office B, which
translates the source addresses from Office A to prevent address conflicts. It ensures that when traffic is initiated from Office A to Office B, the overlapping address range (192.168.100.0/24) is translated.
? Options B and C (Incorrect):These options involve static NAT rules that map address ranges between the two offices, but they do not resolve the overlapping IP address space issue effectively. Static NAT is not the optimal solution in this scenario since the problem involves address space conflict, which requires translation of source addresses during communication.
Juniper References:
? Juniper NAT Configuration Guide: Detailed instructions on how to configure source NAT and resolve address conflicts between networks.
==========

NEW QUESTION 86

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

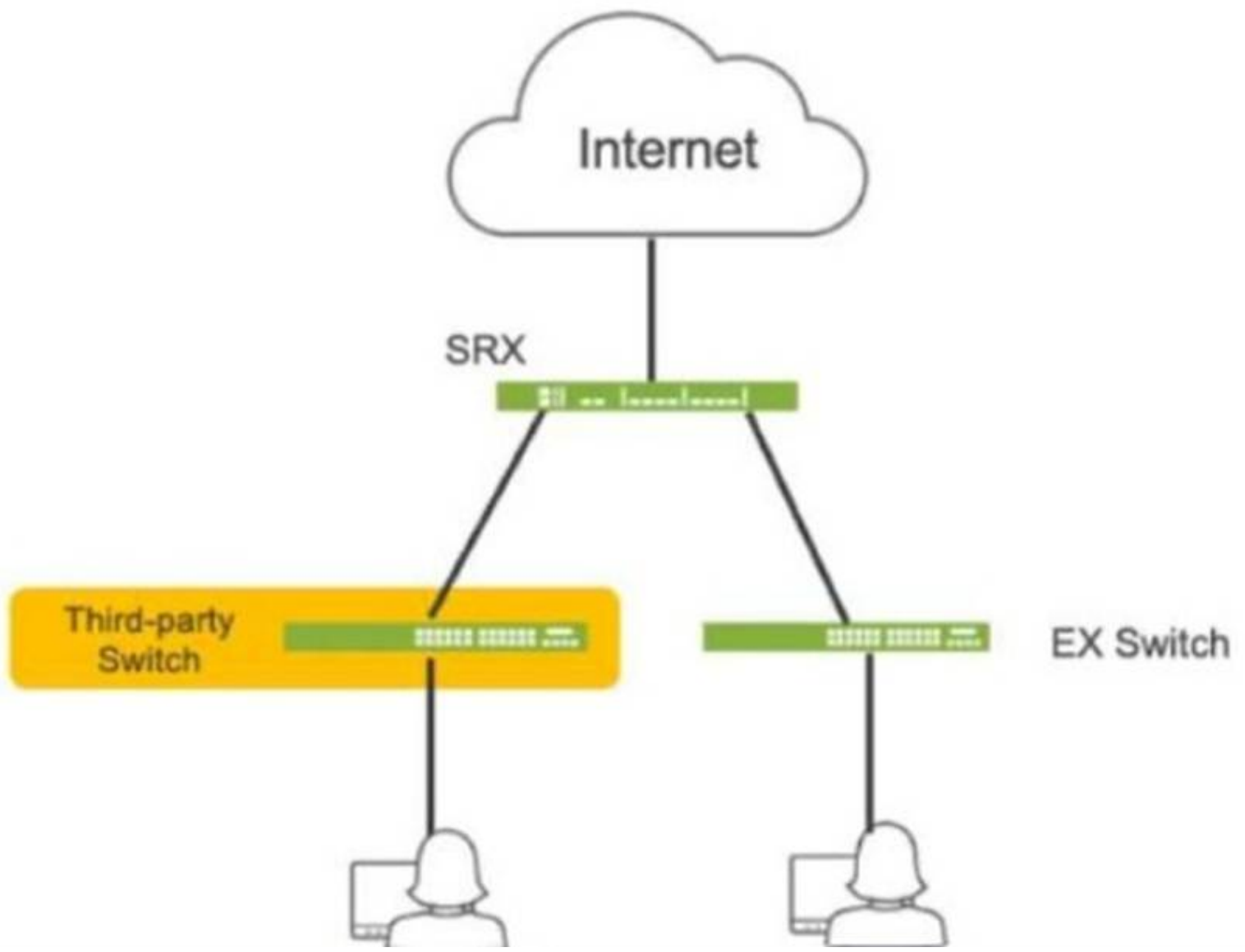
Explanation:
In mixed mode, SRX devices can simultaneously handle Layer 2 switching and Layer 3 routing, but a reboot is required when configuring Layer 2 and Layer 3 interfaces to ensure the configuration takes effect. Layer 2 packets are switched within the defined bridge domain. Further guidance on 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 89
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.)

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: AC

NEW QUESTION 92
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).
==========

NEW QUESTION 95
Click the Exhibit button.

```
[edit class-of-service]
user@srx# show
classifiers {
    dscp ba-classifier {
        import default;
        forwarding-class best-effort {
            loss-priority high code-points 000000;
        }
        forwarding-class ef-class {
            loss-priority high code-points 000001;
        }
        forwarding-class af-class {
            loss-priority high code-points 001010;
        }
        forwarding-class network-control {
            loss-priority high code-points 000011;
        }
        forwarding-class res-class {
            loss-priority high code-points 000100;
        }
        forwarding-class web-data {
            loss-priority high code-points 000101;
```

You have configured a CoS-based VPN that is not functioning correctly. Referring to the exhibit, which action will solve the problem?

A. You must change the loss priorities of the forwarding classes to low.
B. You must change the code point for the DB-data forwarding class to 10000.
C. You must use inet precedence instead of DSCP.
D. You must delete one forwarding class.

Answer: D

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding the Problem:
? A CoS-based VPN has been configured but is not functioning correctly.
? The exhibit shows that under the class-of-service configuration, six forwarding classes are defined.
Forwarding Classes in the Exhibit:
? best-effort
? ef-class
? af-class
? network-control
? res-class
? web-data
Juniper CoS-Based VPN Limitations:
? Maximum Number of Forwarding Classes: In CoS-based VPNs (Layer 3 VPNs), there is a limitation on the number of forwarding classes that can be used.
? Supported Forwarding Classes: Only up to four forwarding classes are supported in an L3VPN for CoS purposes.

Reference:
Juniper Networks Documentation:
"For Layer 3 VPNs, the maximum number of forwarding classes supported is four. If you configure more than four forwarding classes, CoS functionality might not work as expected."
Source: Juniper TechLibrary - Class of Service Limitations in VPNs
* Explanation:
Issue Identification:
The VPN is not functioning correctly because it exceeds the maximum number of supported forwarding classes for a CoS-based VPN.
Solution:
Option D: You must delete one forwarding class.
By reducing the number of forwarding classes to four or fewer, the CoS-based VPN will comply with the limitations and function correctly.
Why Other Options Are Incorrect:
Option A: You must change the loss priorities of the forwarding classes to low.
Changing loss priorities does not affect the limitation on the number of forwarding classes.
The issue is not related to loss priority settings but to the number of forwarding classes. Option B: You must change the code point for the DB-data forwarding class to 10000. There is no forwarding class named DB-data in the exhibit.
Changing a code point does not address the issue of exceeding the maximum number of forwarding classes.
Option C: You must use inet precedence instead of DSCP.
Switching from DSCP to IP Precedence does not resolve the issue of having too many forwarding classes.
The limitation on the number of forwarding classes remains the same regardless of the classification method used.
Conclusion:
To resolve the issue with the CoS-based VPN not functioning correctly due to exceeding the maximum number of forwarding classes, you must delete forwarding classes to reduce the total number to four or fewer.
* Answer: D. You must delete one forwarding class.
Additional References: Juniper TechLibrary:
"Configuring Class of Service for MPLS VPNs" - Discusses CoS considerations and limitations in MPLS L3VPN deployments.
Source: Juniper TechLibrary - CoS for VPNs
Juniper Networks Day One Book:
"Deploying MPLS Layer 3 VPNs" - Provides insights into CoS limitations and best practices for VPN deployments.

NEW QUESTION 96
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

JN0-637 Practice Exam Features:

* JN0-637 Questions and Answers Updated Frequently

* JN0-637 Practice Questions Verified by Expert Senior Certified Staff

* JN0-637 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* JN0-637 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year