Juniper

Exam Questions JN0-637

Security - Professional (JNCIP-SEC)

NEW QUESTION 1
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.

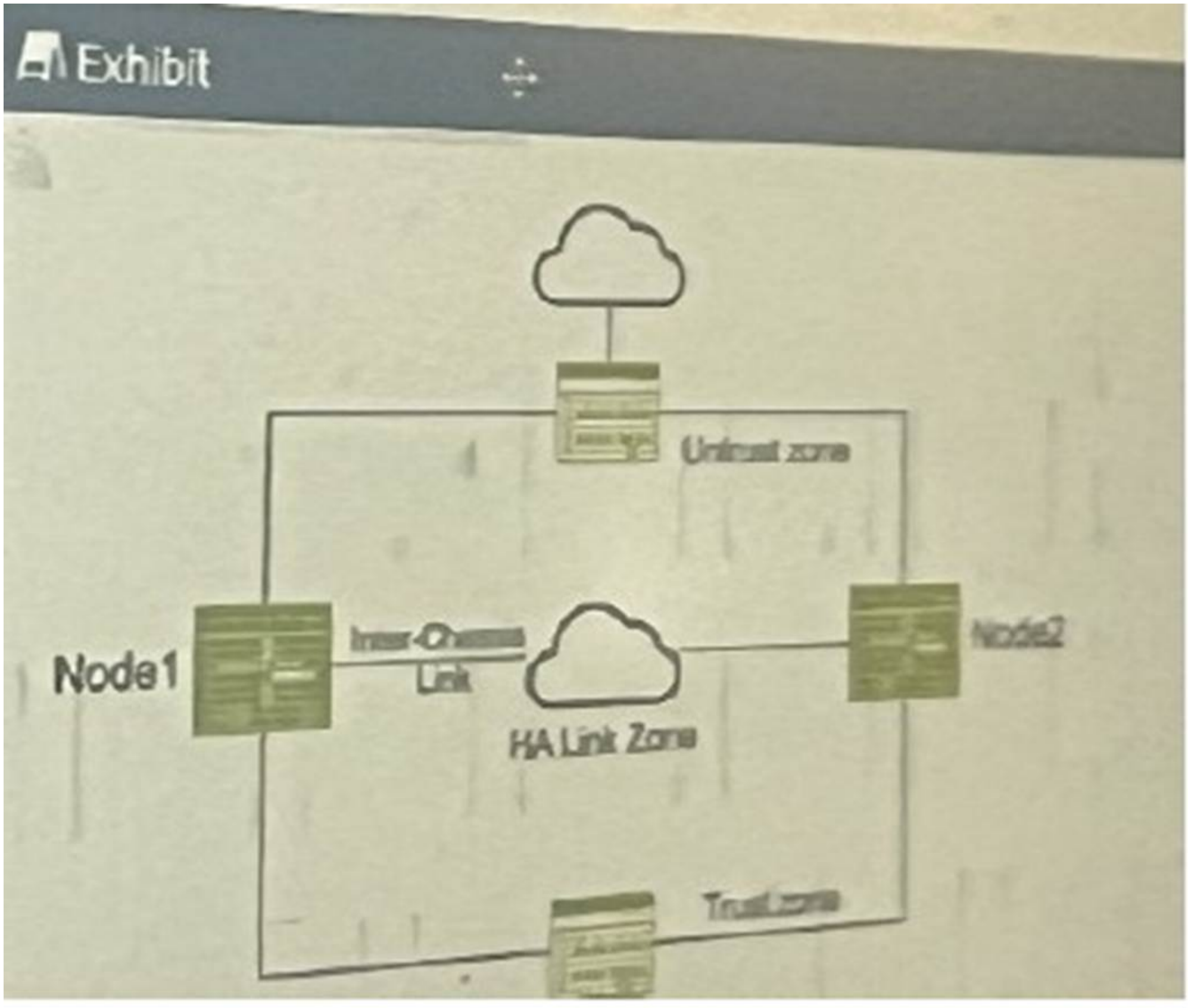
Answer: CD

NEW QUESTION 2
You are using ADVPN to deploy a hub-and-spoke VPN to connect your enterprise sites. Which two statements are true in this scenario? (Choose two.)

A. ADVPN creates a full-mesh topology.
B. IBGP routing is required.
C. OSPF routing is required.
D. Certificate-based authentication is required.

Answer: CD

NEW QUESTION 3
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 4
You are enabling advanced policy-based routing. You have configured a static route that
has a next hop from the inet.0 routing table. Unfortunately, this static route is not active in your routing instance.
In this scenario, which solution is needed to use this next hop?

A. Use RIB groups.
B. Use filter-based forwarding.
C. Use transparent mode.
D. Use policies.

Answer: A

Explanation:
To enable advanced policy-based routing in Junos OS and activate a static route with a next-hop address in the inet.0 table within your routing instance, you should utilize RIB groups. RIB groups allow you to import routes from one routing table to another. In this scenario, the static route within the routing instance needs access to the inet.0 routes, which is facilitated by configuring a RIB group. Juniper??s documentation outlines RIB groups as a necessary component for handling instances where routes need to be shared across routing tables, thereby ensuring seamless traffic flow through specified routes. For more details, refer to the Juniper Networks Documentation on RIB Groups.
In Junos OS for SRX Series devices, when enabling advanced policy-based routing and configuring a static route with a next-hop from the inet.0 routing table, the issue arises because the static route is not being used in the routing instance. This is a common scenario when the next-hop belongs to a different routing table or instance, and the routing instance is not aware of that next-hop.
To resolve this, RIB (Routing Information Base) groups are used. RIB groups allow routes from one routing table (RIB) to be shared or imported into another routing table. This means that the routing instance can import the necessary routes from inet.0 and make them available for the routing instance where the policy-based routing is applied.
Detailed Steps:
? Configure the Static Route: First, configure the static route pointing to the next-hop in inet.0. Here??s an example:
bash
set routing-options static route 10.1.1.0/24 next-hop 192.168.1.1 This static route will be placed in the inet.0 routing table by default.
? Create and Apply a RIB Group: To import routes from inet.0 into the routing
instance, create a RIB group configuration. This will allow the static route from inet.0 to be visible within the routing instance.
Example configuration for the RIB group: bash
set routing-options rib-groups RIB-GROUP import-rib inet.0
set routing-options rib-groups RIB-GROUP import-rib <routing-instance-name>.inet.0
This configuration ensures that routes from inet.0 are imported into the specified routing instance.
? Apply the RIB Group to the Routing Instance: Once the RIB group is configured,
apply it to the appropriate routing instance:
bash
set routing-instances <routing-instance-name> routing-options rib-group RIB-GROUP
? Verify Configuration: Use the following command to verify that the static route has been imported into the routing instance:
bash
show route table <routing-instance-name>.inet.0
The output should now display the static route imported from inet.0.
Juniper Security Reference:
? RIB Groups Overview: Juniper's documentation provides detailed information on how RIB groups function and how to use them to share routes between different routing tables. This is essential for scenarios involving policy-based routing where routes from one instance (like inet.0) need to be available in another instance.
Reference: Juniper Networks Documentation on RIB Groups.
By using RIB groups, you ensure that the static route from inet.0 is available in the appropriate routing instance for policy-based routing to function correctly. This avoids the need for other methods like filter-based forwarding or transparent mode, which do not address the specific issue of static route visibility across routing instances.
==========

NEW QUESTION 5
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 6
You are experiencing problem with your ADVPN tunnels getting established. The tunnel and egress interface are located in different zone. What are two reasons for these problems? (Choose two.)

A. IKE is not an allowed protocol in the external interfaces' security zone.
B. IKE is not an allowed protocol in the tunnel endpoints' security zone.
C. OSPF is not an allowed protocol in the tunnel endpoints' security zone.
D. BGP is not an allowed protocol in the tunnel endpoints' security zone.

Answer: AB

NEW QUESTION 7
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.

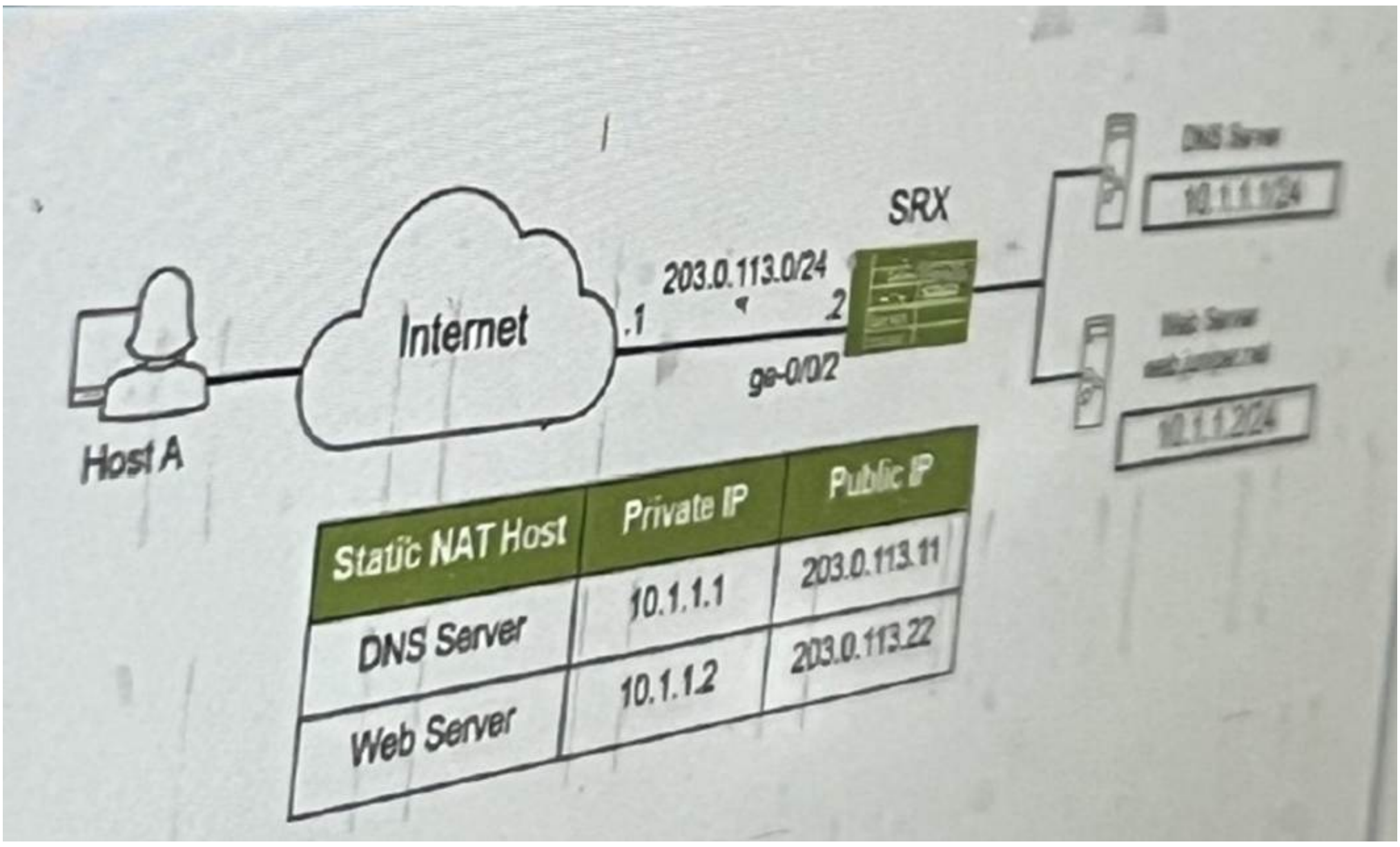
Answer: BC

NEW QUESTION 8
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 9
The SRX series device is performing static NAT. you want to ensure that host A can reach the internal webserver www.juniper.net using domain name.



Referring to the exhibit, which two Junos features are required to accomplish this task? (Choose two.)

A. DNS doctoring
B. proxy ARP
C. persistent NAT
D. STUN

Answer: AB

NEW QUESTION 10
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 10
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 14
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 18
You configured two SRX series devices in an active/passive multimode HA setup. In this scenario, which statement is correct?

A. Both devices are in the passive state until the activeness determination process is completed.
B. Both devices start in a hold state until the activeness determination process is completed.

C. Both devices start in the undiscovered state until the activeness determination process is completed.
D. Both devices are in the active state until the activeness determine determination process is completed.

Answer: D

NEW QUESTION 22
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
VXLAN Overlay load bal: Disabled
VXLAN ECMP             : Disabled
Fast Update            : Disabled
Host Pkts GBP src tag : 0
[edit interfaces]
user@srx# show
ge-0/0/0 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members v100;
            }
```

```
                                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
VXLAN Overlay load bal: Disabled
VXLAN ECMP              : Disabled
Fast Update             : Disabled
Host Pkts GBP src tag : 0
[edit interfaces]
user@srx# show
ge-0/0/0 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members v100;
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 172.16.0.1/24;
        }
    }
}
```

In which mode is the SRX Series device?

A. Packet
B. Ethernet switching
C. Mixed
D. Transparent

Answer: C

NEW QUESTION 23
Click the Exhibit button.

```
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: AD

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding the Exhibit:
? The SRX device is operating in Transparent Mode, as indicated by:
Transparent Mode on SRX Devices:
? Transparent Mode (Layer 2 Mode):
? Option A: You cannot secure intra-VLAN traffic with a security policy on this device.
? Option B: You can secure inter-VLAN traffic with a security policy on this device.
? Option C: The device can pass Layer 2 and Layer 3 traffic at the same time.
? Option D: The device cannot pass Layer 2 and Layer 3 traffic at the same time.
Key Points:
? Intra-VLAN Traffic:
? Inter-VLAN Traffic:
Juniper Security References:
? Juniper Networks Documentation:
Conclusion:
? Option A is correct because intra-VLAN traffic cannot be secured with security policies in Transparent Mode.
? Option D is correct because the device cannot pass both Layer 2 and Layer 3 traffic at the same time when operating in Transparent Mode.

NEW QUESTION 24
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 25
Referring to the exhibit,

```
user@srx> 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
```

which three statements about the multinode HA environment are true? (Choose three.)

A. Two services redundancy groups are available.
B. IP monitoring has failed for the services redundancy group.
C. Node 1 will host services redundancy group 1 unless it is unavailable.
D. Session state is synchronized on both nodes.
E. Node 2 will process transit traffic that it receives for services redundancy group 1.

Answer: ACD

Explanation:
Referring to the exhibit for a multinode HA environment, we can conclude the following about the HA setup:
? Two Services Redundancy Groups (Correct: Option A):The output shows the
status of SRG 0 and SRG 1, confirming that there are two services redundancy groups in the HA configuration.
? Node 1 Hosting SRG 1 (Correct: Option C):The exhibit indicates that Node 1 is
currently active for SRG 1. According to the configuration, Node 1 will continue to host SRG 1 unless it becomes unavailable.
? Session State Synchronization (Correct: Option D):In this HA setup, session state
synchronization is enabled between the two nodes. This ensures that sessions remain active and seamless failover can occur if one node fails.
Juniper References:
? Juniper HA Documentation: Provides details on multinode HA setups, SRG configurations, and session synchronization.
==========

NEW QUESTION 27
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 28
Click the Exhibit button.

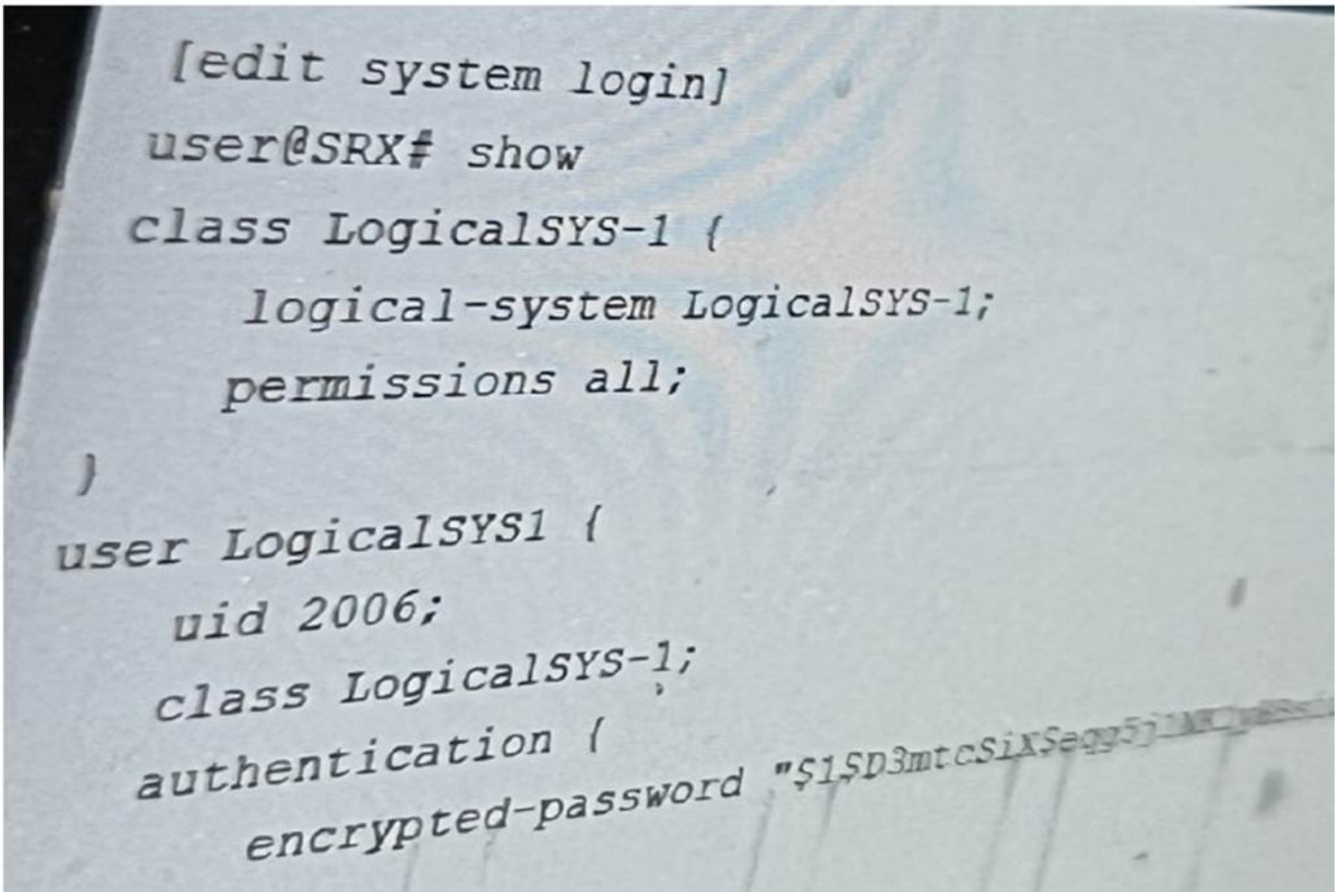
Referring to the exhibit. SRX-1 and SRX-3 have to be connected using EBGP. The BGP configuration on SRX-1 and SRX-3 is verified and correct.
Which configuration on SRX-2 would establish an EBGP connection successfully between SRX-1 and SRX-3?

A. The host-inbound-traffic statements do not allow EBGP traffic to traverse SRX-2.
B. The security policy to allow SRX-1 and SRX-3 to communicate on TCP port 79 should be configured.
C. The security policy to allow SRX-1 and SRX-3 to communicate on TCP port 169 should be configured.
D. The security policy to allow SRX-1 and SRX-3 to communicate on TCP port 179 should be configured.

Answer: D

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding the Scenario:
? SRX-1 and SRX-3:
? Issue:
Option D: The security policy to allow SRX-1 and SRX-3 to communicate on TCP port 179 should be configured.
? Explanation:
Reference:
"Security policies must permit BGP traffic (TCP port 179) to allow BGP sessions through the SRX device."
Source: Juniper TechLibrary - Configuring Security Policies for Transit Traffic
Why Other Options Are Incorrect:
Option A: Host-inbound-traffic affects traffic destined to SRX-2, not transit traffic.
Option B and C: TCP ports 79 and 169 are unrelated to BGP.
Conclusion:
The correct option is D, configuring a security policy to allow TCP port 179.

NEW QUESTION 31
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 36
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 37
Referring to the exhibit, you are assigned the tenantSYS1 user credentials on an SRX series device.
In this scenario, which two statements are correct? (Choose two.)

A. When you log in to the device, you will be located at the operational mode of the main system hierarchy.
B. When you log in to the device, you will be located at the operational mode of the Tenant.SY51 logical system hierarchy.
C. When you log in to the device, you will be permitted to view only the routing tables for the Tenant SYS1 logical system.
D. When you log in to the device, you will be permitted to view all routing tables available on the on an SYS1 Series device.

Answer: BC

NEW QUESTION 42
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 45
You are asked to set up advanced policy-based routing.
Which type of routing instance is designed to support this scenario?

A. forwarding
B. virtual switch
C. virtual router
D. non-forwarding

Answer: A

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding Advanced Policy-Based Routing (APBR):
? APBR: Allows routing decisions based on application-level information and policies.
? Objective: Direct specific application traffic through different paths based on policies.
Routing Instances in Junos OS:
? Forwarding Instance:
? Virtual Router:
? Virtual Switch:
? Non-Forwarding Instance:
? Option A: forwarding
Reference:
Juniper Networks Documentation:
"To configure advanced policy-based routing, you must create a forwarding-type routing instance."
Source: Configuring Advanced Policy-Based Routing
Why Other Options Are Incorrect: Option B: virtual switch
Incorrect.
Virtual switch instances are for Layer 2 switching and VLAN separation. They do not support routing or APBR.
Option C: virtual router
Incorrect.
Virtual router instances are used for isolating routing tables. While they support routing, they are not designed for APBR. Option D: non-forwarding
Incorrect.
Non-forwarding instances do not handle transit traffic.
They are used for management routing tables and cannot be used for APBR.
Conclusion:
Correct Answer: A. forwarding Rationale:
A forwarding routing instance is the appropriate type to support advanced policy-based routing.

NEW QUESTION 49
What are three core components for enabling advanced policy-based routing? (Choose three.)

A. Filter-based forwarding
B. Routing options
C. Routing instance
D. APBR profile
E. Policies

Answer: ACD

Explanation:
To enable Advanced Policy-Based Routing (APBR) on SRX Series devices, three key components are necessary: filter-based forwarding, routing instances, and APBR profiles. Filter-based forwarding is utilized to direct specific traffic flows to a routing instance based on criteria set by a policy. Routing instances allow the traffic to be managed independently of the main routing table, and APBR profiles define how and when traffic should be forwarded. These elements ensure that APBR is flexible and tailored to the network??s requirements. Refer to Juniper's APBR Documentation for more details.
Advanced policy-based routing (APBR) in Juniper's SRX devices allows the selection of different paths for traffic based on policies, rather than relying purely on routing tables. To enable APBR, the following core components are required:
? Filter-based Forwarding (Answer A): Filter-based forwarding (FBF) is a technique
used to forward traffic based on policies rather than the default routing table. It is essential for enabling APBR, as it helps match traffic based on filters and directs it to specific routes.
Configuration Example: bash
set firewall family inet filter FBF match-term source-address 192.168.1.0/24
set firewall family inet filter FBF then routing-instance custom-routing-instance
? Routing Instance (Answer C): A routing instance is required to define the separate routing table used by APBR. You can create multiple routing instances and assign traffic to these instances based on policies. The traffic will then use the routes defined within the specific routing instance.
Configuration Example: bash
set routing-instances custom-routing-instance instance-type forwarding
set routing-instances custom-routing-instance routing-options static route 0.0.0.0/0 next- hop 10.10.10.1
? APBR Profile (Answer D): The APBR profile defines the rules and policies for
advanced policy-based routing. It allows you to set up conditions such as traffic type, source/destination address, and port, and then assign actions such as

redirecting traffic to specific routing instances.
Configuration Example: bash
set security forwarding-options advanced-policy-based-routing profile apbr-profile match application http
set security forwarding-options advanced-policy-based-routing profile apbr-profile then routing-instance custom-routing-instance
Other Components:
? Routing Options (Answer B) are not a core component of APBR, as routing options define the general behavior of the routing table and protocols. However, APBR works by overriding these default routing behaviors using policies.
? Policies (Answer E) are crucial in many network configurations but are not a core component of enabling APBR. APBR specifically relies on profiles rather than standard security policies.
Juniper Security Reference:
? Advanced Policy-Based Routing (APBR): Juniper??s APBR is a powerful tool that allows routing based on specific traffic characteristics rather than relying on static routing tables. APBR ensures that specific types of traffic can take alternate paths based on business or network needs. Reference: Juniper Networks APBR Documentation.
==========

NEW QUESTION 53
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 57
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;
                        }
                    }
                }
            }
        }
    }
}
```

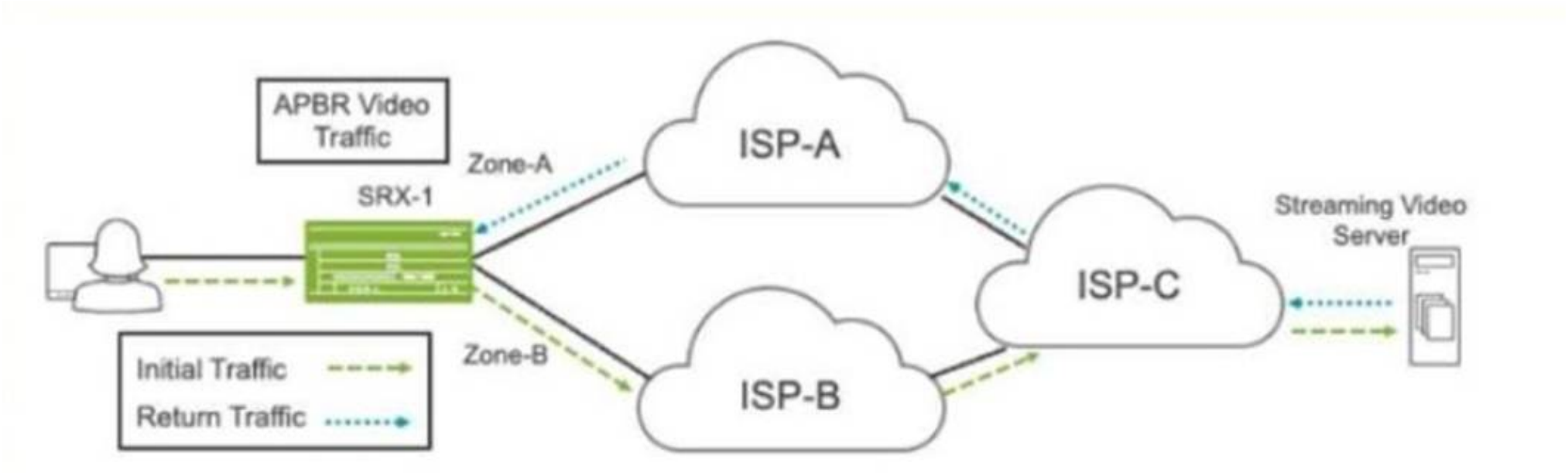
which two statements are correct about the NAT configuration? (Choose two.)

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:



Referring to the exhibit, a default static route on SRX-1 sends all traffic to ISP-A. You have configured APBR to send all requests for streaming video traffic to ISP-B. However, the return traffic from the streaming video server is coming through ISP-A, and the traffic is being dropped by SRX-1. You can only make changes on SRX-1.
How do you solve this problem?

A. Place both ISP-facing interfaces in the same zone.
B. Change the APBR routing instance from a forwarding instance to a virtual router instance.
C. Enable AppTrack to keep track of the sessions and zones for the streaming video traffic.
D. Configure BGP to control the return path of the streaming video traffic.

Answer: D

NEW QUESTION 64
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 67
An ADVPN configuration has been verified on both the hub and spoke devices and it seems fine. However, OSPF is not functioning as expected.

```
[edit protocols ospf]
user@ADVPN-HUB# show
area 0.0.0.0 {
    interface st0.0 {
        demand-circuit;
    }
    interface ge-0/0/3.0 {
        passive;
    }
}
```

Referring to the exhibit, which two statements under interface st0.0 on both the hub and spoke devices would solve this problem? (Choose two.)

A. interface-type p2mp
B. dynamic-neighbors
C. passive
D. interface-type p2p

Answer: AB

Explanation:
For ADVPN with OSPF, using a point-to-multipoint (p2mp) interface type and
enabling dynamic-neighbors are crucial. This configuration allows dynamic discovery of neighbors and the establishment of tunnels. For more information, refer to Juniper ADVPN Configuration Guide.
In the ADVPN configuration, OSPF isn't functioning as expected due to the interface configuration on st0.0. Here are the adjustments needed:
? Interface Type p2mp (Answer A): OSPF requires that the tunnel interface be set to
p2mp (point-to-multipoint) to allow OSPF to communicate with multiple dynamic neighbors over the ADVPN tunnels.
Command Example: bash
set interfaces st0.0 family inet ospf interface-type p2mp
? Dynamic Neighbors (Answer B): The dynamic neighbors statement allows OSPF to discover and communicate with dynamically established spokes in an

ADVPN environment. This is essential for ADVPN to function properly since the tunnel endpoints are not static.
Command Example: bash
set protocols ospf area 0.0.0.0 interface st0.0 dynamic-neighbors
These settings ensure OSPF properly functions over dynamically created ADVPN tunnels.
: Juniper ADVPN and OSPF configuration.
==========

NEW QUESTION 69
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 71
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 75
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

```
[edit]
user@SRX# show routing-instances
APBRinstance {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 203.0.113.52;
        }
    }
}
[edit security advance-policy-based-routing]
user@SRX# show
profile APBR-profile {
    rule SSH-rule {
        match {
            dynamic-application junos:SSH;
        }
        then {
            routing-instance APBRinstance;
        }
```

```
[edit]
user@SRX# show routing-options
interface-routes {
    rib-group inet APBR-group;
}
rib-groups {
    APBR-group {
        import-rib [ APBRinstance.inet.0 inet.0 ];
```

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 76
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 77
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 81
You are using trace options to troubleshoot a security policy on your SRX Series device.

```
user@SRX> show log flow-log | find "policy search"
Jan  9 14:19:37 14:19:37.520231:CID-0:THREAD_ID-01:LSYS_ID-00:RT:flow_first_policy_search: policy search from zone Linux-9-
zone-> zone junos-host (0x0,0x94c80016,0x16), result: 0x5ed4b468, pending: 0?, is_http_cached = 0
Jan  9 14:19:37 14:19:37.520232:CID-0:THREAD_ID-01:LSYS_ID-00:RT:flow_first_policy_search: dynapp_none_policy: TRUE,
uc_none_policy: TRUE, is_final: 0x0, is_explicit: 0x0, policy_meta_data: 0x0
Jan  9 14:19:37 14:19:37.520233:CID-0:THREAD_ID-01:LSYS_ID-00:RT:  app 22, timeout 1800s, curr ageout 20s
Jan  9 14:19:37 14:19:37.520234:CID-0:THREAD_ID-01:LSYS_ID-00:RT:  packet dropped, denied by policy
Jan  9 14:19:37 14:19:37.520234:CID-0:THREAD_ID-01:LSYS_ID-00:RT:  denied by policy deny-ssh(7), dropping pkt
Jan  9 14:19:37 14:19:37.520235:CID-0:THREAD_ID-01:LSYS_ID-00:RT:  packet dropped,  policy deny.
```

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

A. The SSH traffic matches an existing session.
B. No entries are created in the SRX session table.
C. The traffic is not destined for the root logical system.
D. The security policy controls traffic destined to the SRX device.

Answer: AD

NEW QUESTION 82
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 83
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 85
You have an initial setup of ADVPN with two spokes and a hub. A host at partner Spoke-1 is sending traffic to a host at partner Spoke-2.
In this scenario, which statement is true?

A. Spoke-1 will establish a VPN to Spoke-2 when this is first deployed, so traffic will be sent immediately to Spoke-2.
B. Spoke-1 will send the traffic through the hub and not use a direct VPN to Spoke-2.
C. Spoke-1 will establish the tunnel to Spoke-2 before sending any of the host traffic.
D. Spoke-1 will send the traffic destined to Spoke-2 through the hub until the VPN is established between the spokes.

Answer: A

NEW QUESTION 90
Which two statements are true about the procedures the Junos security device uses when handling traffic destined for the device itself? (Choose two.)

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

Answer: BC

Explanation:
When handling traffic that is destined for itself, the SRX examines the host- inbound-traffic configuration for the ingress interface and the associated security zone.

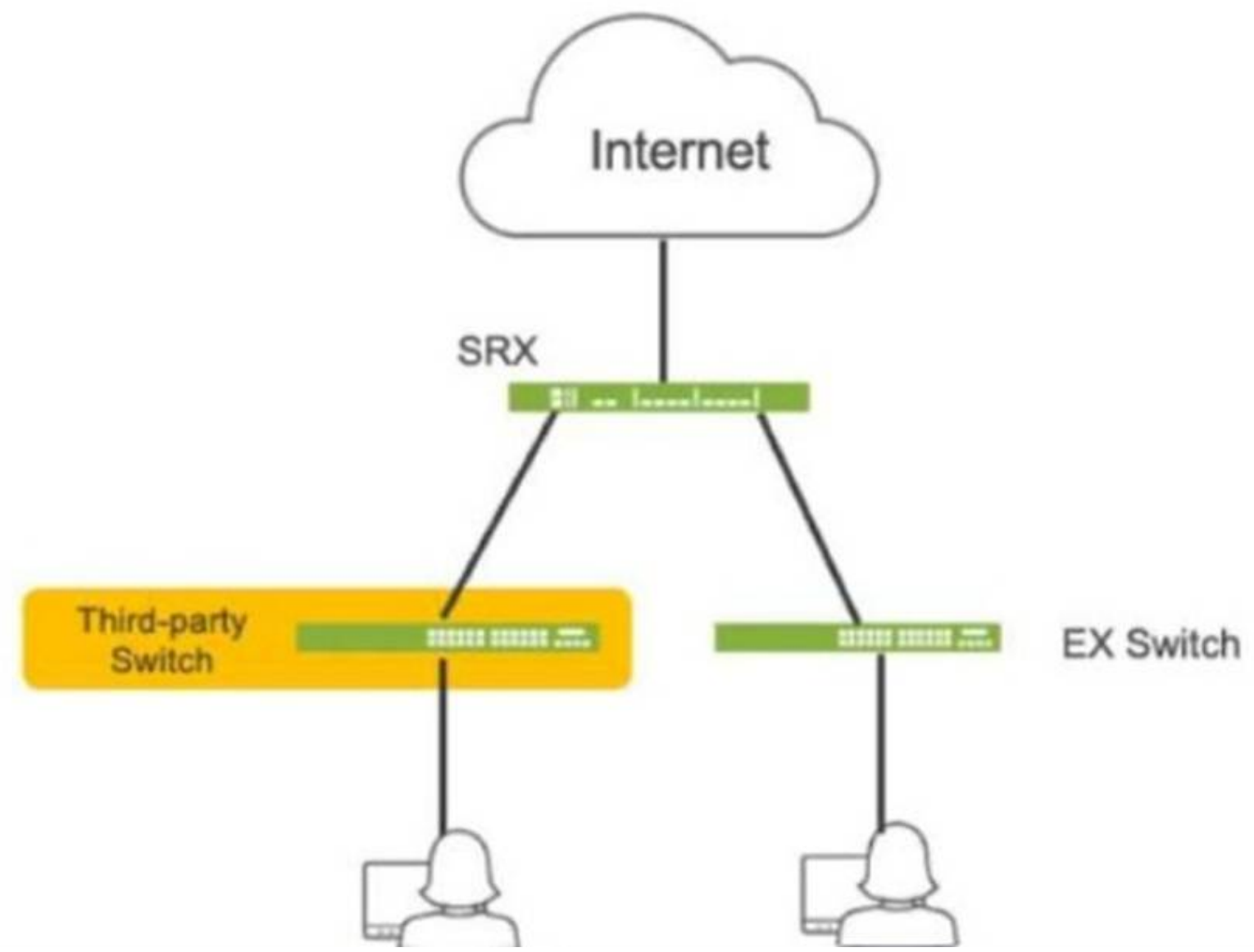
It evaluates whether the traffic should be allowed based on this configuration. Traffic not addressed to the ingress interface is handled based on security policies within the junos- host zone, which applies to traffic directed to the SRX itself. For more details, refer to Juniper Host Inbound Traffic Documentation.
When handling traffic that is destined for the SRX device itself (also known as host-bound traffic), the SRX follows a specific process to evaluate the traffic and apply the appropriate
security policies. The junos-host zone is a special security zone used for managing traffic destined for the device itself, such as management traffic (SSH, SNMP, etc.).
? Explanation of Answer B (Packet to a Different Interface):
? Explanation of Answer C (Packet to the Ingress Interface):
Step-by-Step Handling of Host-Bound Traffic:
? Host-Inbound Traffic: Define which services are allowed to the SRX device itself:
bash
set security zones security-zone <zone-name> host-inbound-traffic system-services ssh
? Security Policy for junos-host: Ensure policies are defined for managing traffic destined for the SRX device:
bash
set security policies from-zone <zone-name> to-zone junos-host policy allow-ssh match source-address any
set security policies from-zone <zone-name> to-zone junos-host policy allow-ssh match destination-address any
Juniper Security Reference:
? Junos-Host Zone: This special zone handles traffic destined for the SRX device, including management traffic. Security policies must be configured to allow this traffic. Reference: Juniper Networks Host-Inbound Traffic Documentation.
==========

NEW QUESTION 92
Which two statements are true regarding NAT64? (Choose two.)

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

Answer: BC

NEW QUESTION 94
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 97
.....

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