# Juniper

## Exam Questions JN0-637

Security - Professional (JNCIP-SEC)

# About Exambible

## *Your Partner of IT Exam*

## Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

## Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**
You want to create a connection for communication between tenant systems without using physical revenue ports on the SRX Series device.
What are two ways to accomplish this task? (Choose two.)

A. Use an external router.
B. Use an interconnect VPLS switch.
C. Use a secure wire.
D. Use a point-to-point logical tunnel.

**Answer:** BD

**NEW QUESTION 2**
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 3**
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 4**
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 5**
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

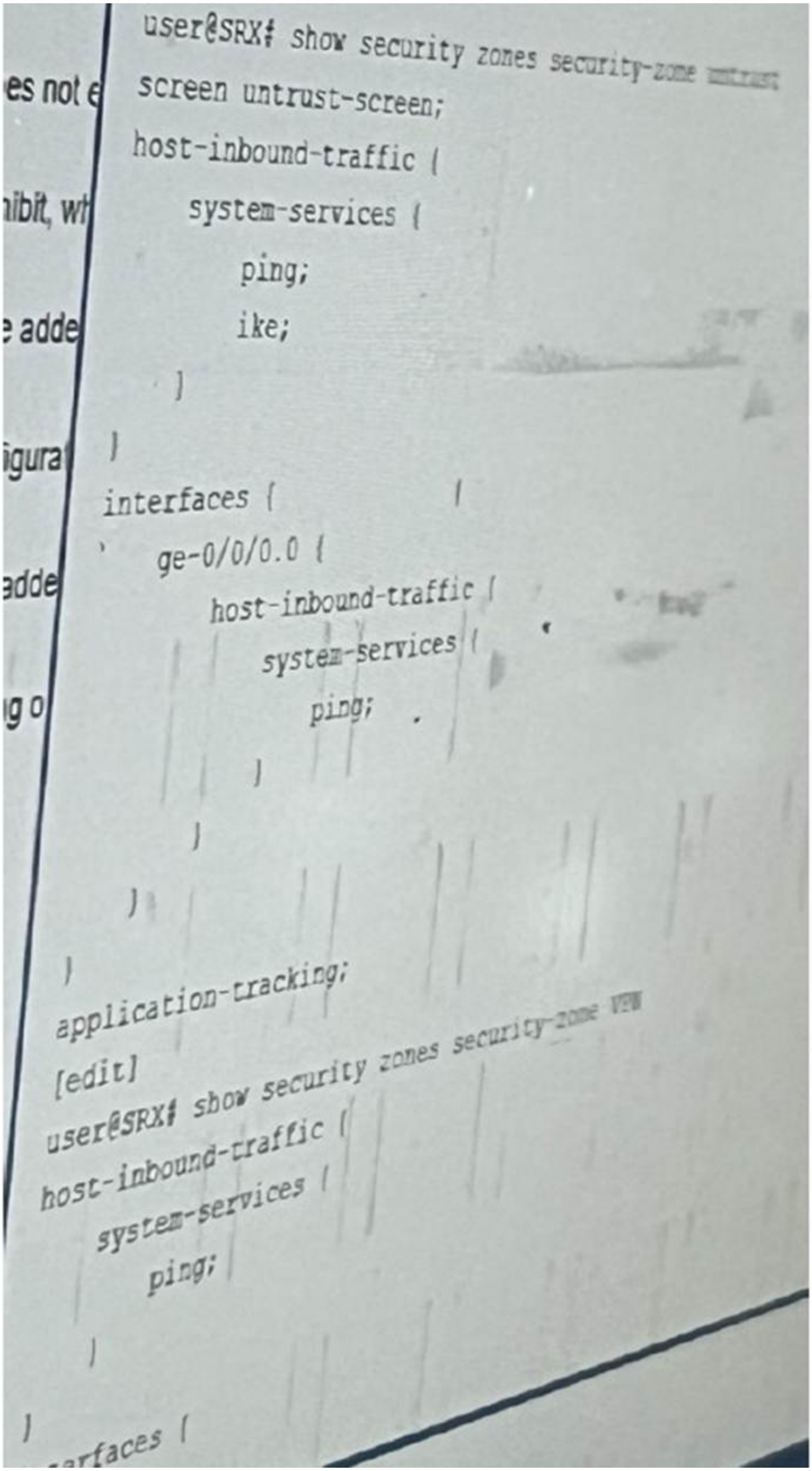
**NEW QUESTION 6**
You configure two Ethernet interfaces on your SRX Series device as Layer 2 interfaces and add them to the same VLAN. The SRX is using the default L2-learning setting. You do not add the interfaces to a security zone.
Which two statements are true in this scenario? (Choose two.)

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 7**
Exhibit:



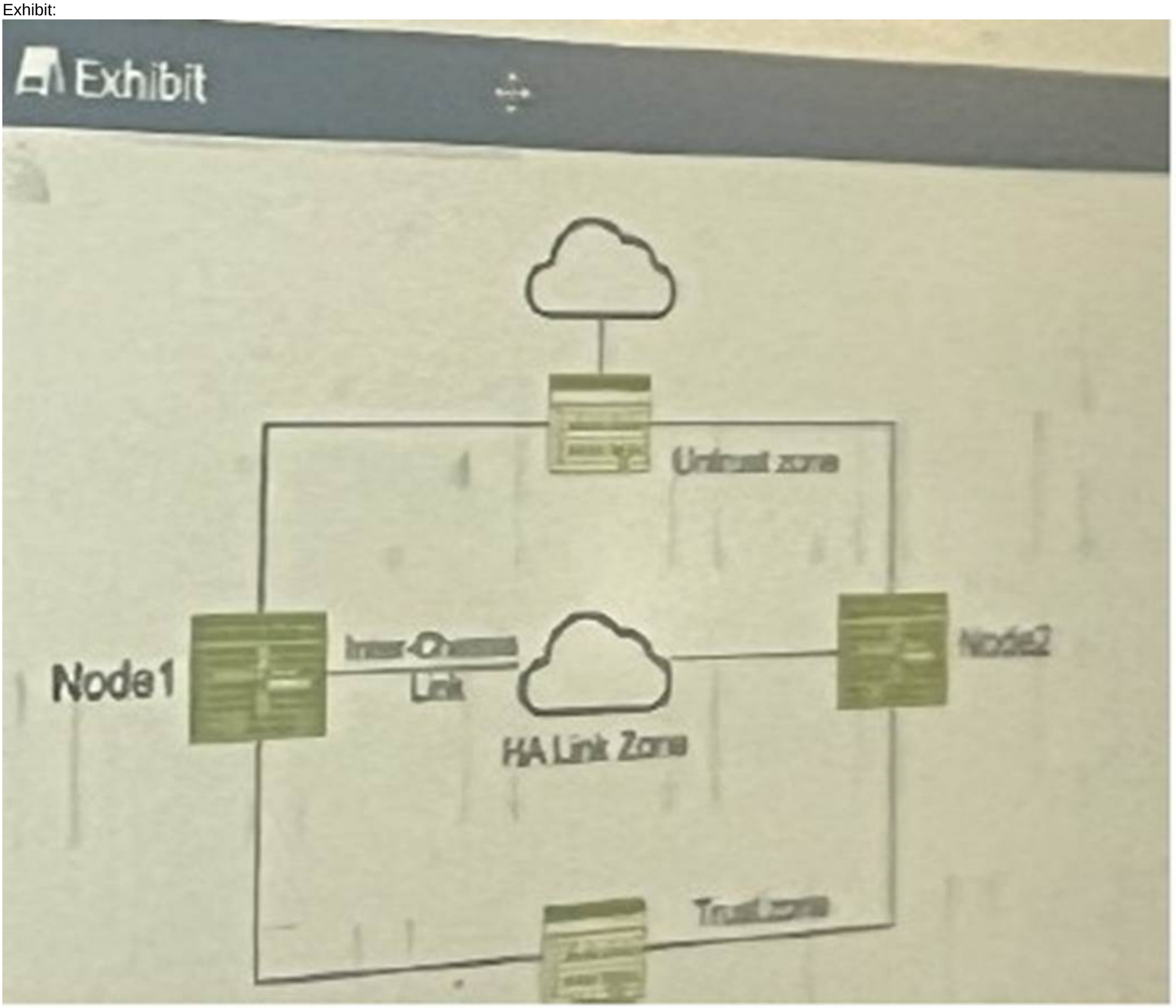

The Ipsec VPN does not establish when the peer initiates, but it does establish when the SRX series device initiates. Referring to the exhibit, what will solve this problem?

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 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 are asked to establish a hub-and-spoke IPsec VPN using an SRX Series device as the hub. All of the spoke devices are third-party devices.
Which statement is correct in this scenario?

A. You must ensure that you are using aggressive mode when incorporating third-party devices as your spokes.
B. You must statically configure the next-hop tunnel binding table entries for each of the third-party spoke devices.
C. You must create a policy-based VPN on the hub device when peering with third-party devices.
D. You must always peer using loopback addresses when using non-Junos devices as your spokes.

**Answer:** B

**NEW QUESTION 10**
What are three configurable monitor components for a service redundancy group? (Choose two)

A. Interface
B. BFD
C. hardware alarm
D. IP
E. ARP

**Answer:** ADE

**NEW QUESTION 10**
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 13**
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 17**
Which two elements are necessary to configure a rule under an APBR profile? (Choose Two)

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

**Answer:** BC

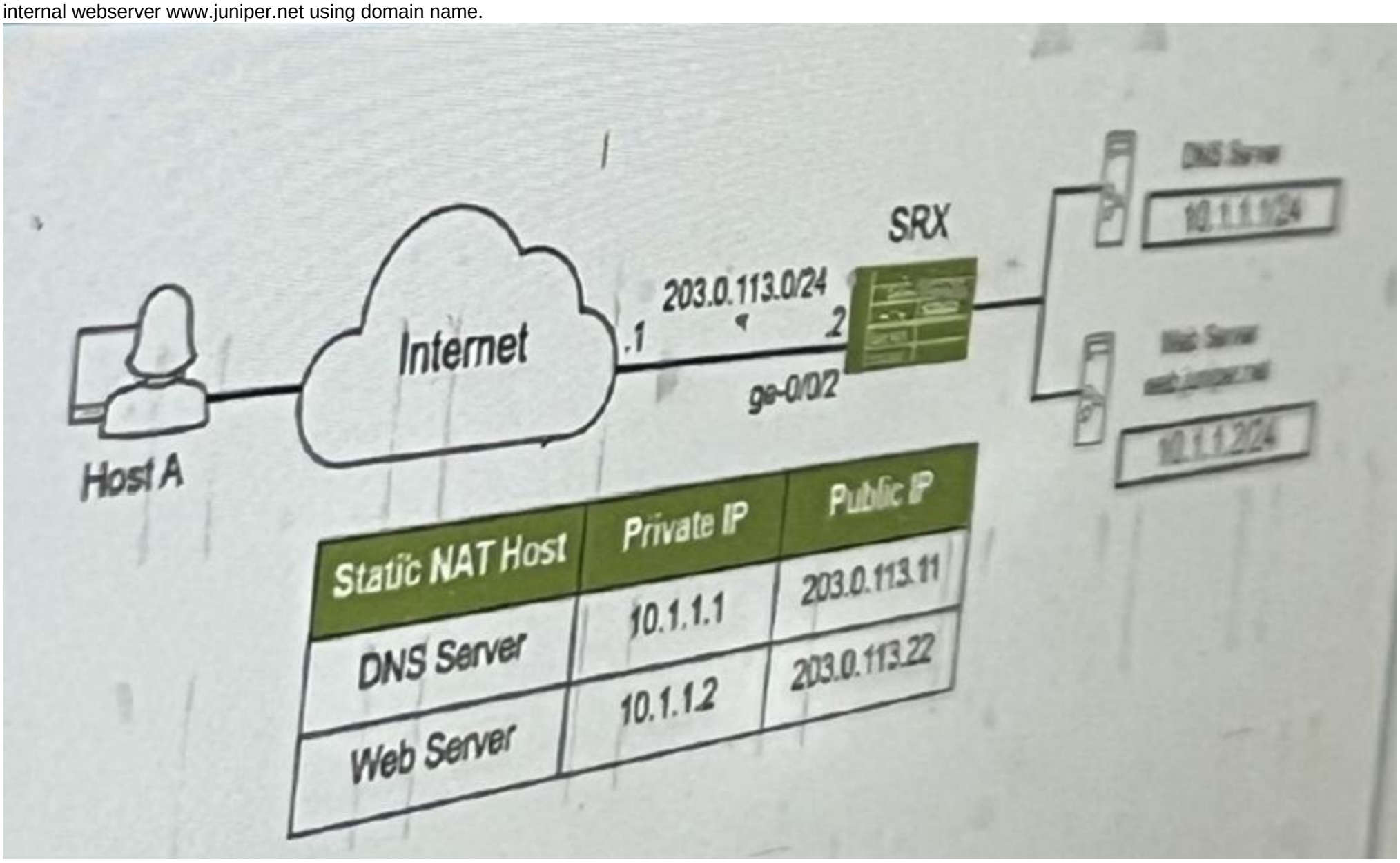
**Explanation:**
Here's why those elements are necessary for configuring a rule under an APBR profile:
? B. Match condition: This defines the criteria for matching traffic to the APBR rule. It can include:
? C. Then action: This specifies the action to take when traffic matches the rule. The primary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

**NEW QUESTION 18**
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 19**
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 24**
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 29**
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 34**
A user reports that a specific application is not working properly. This application makes
multiple connection to the server and must have the same address every time from a pool and this behavior needs to be changed.
What would solve this problem?

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

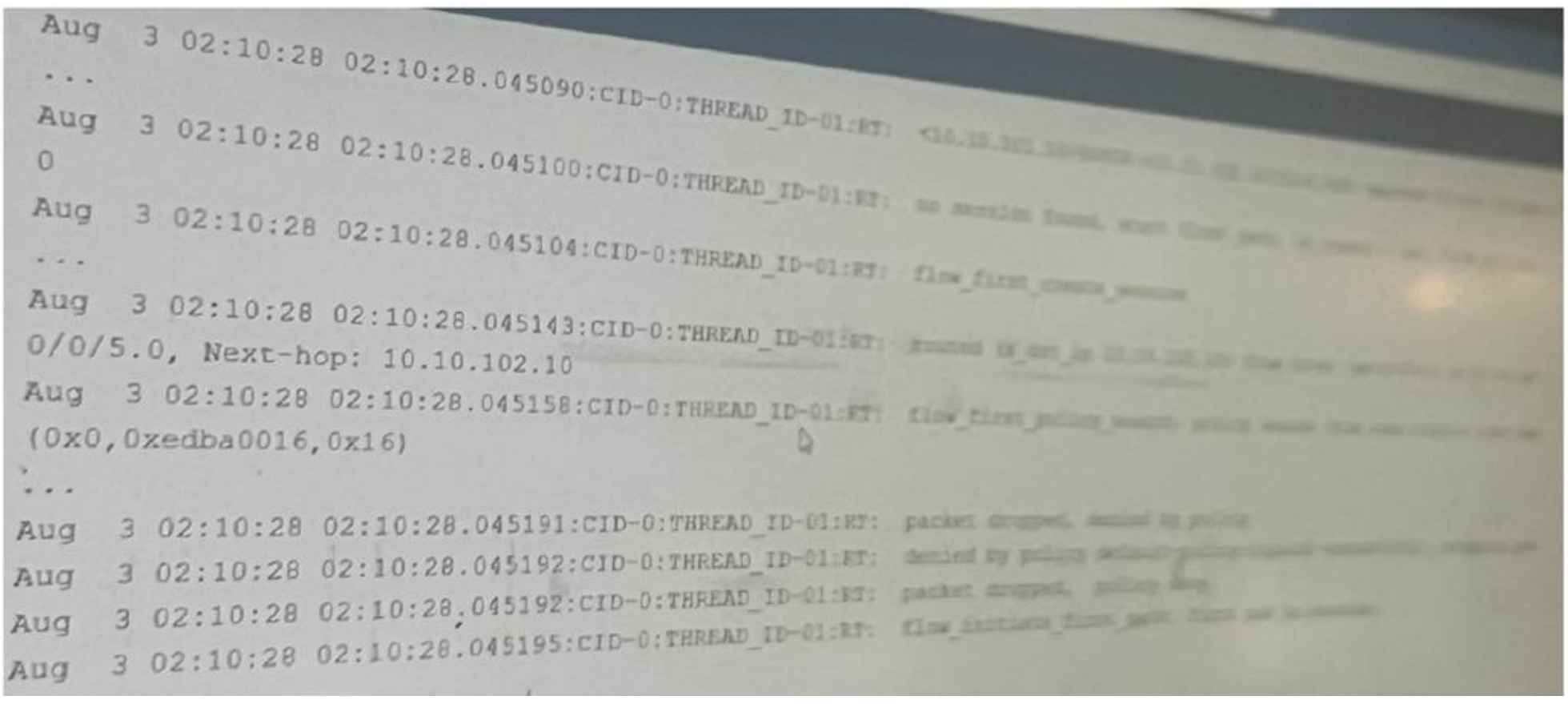
**Answer:** D

**NEW QUESTION 36**
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 37**
Exhibit:

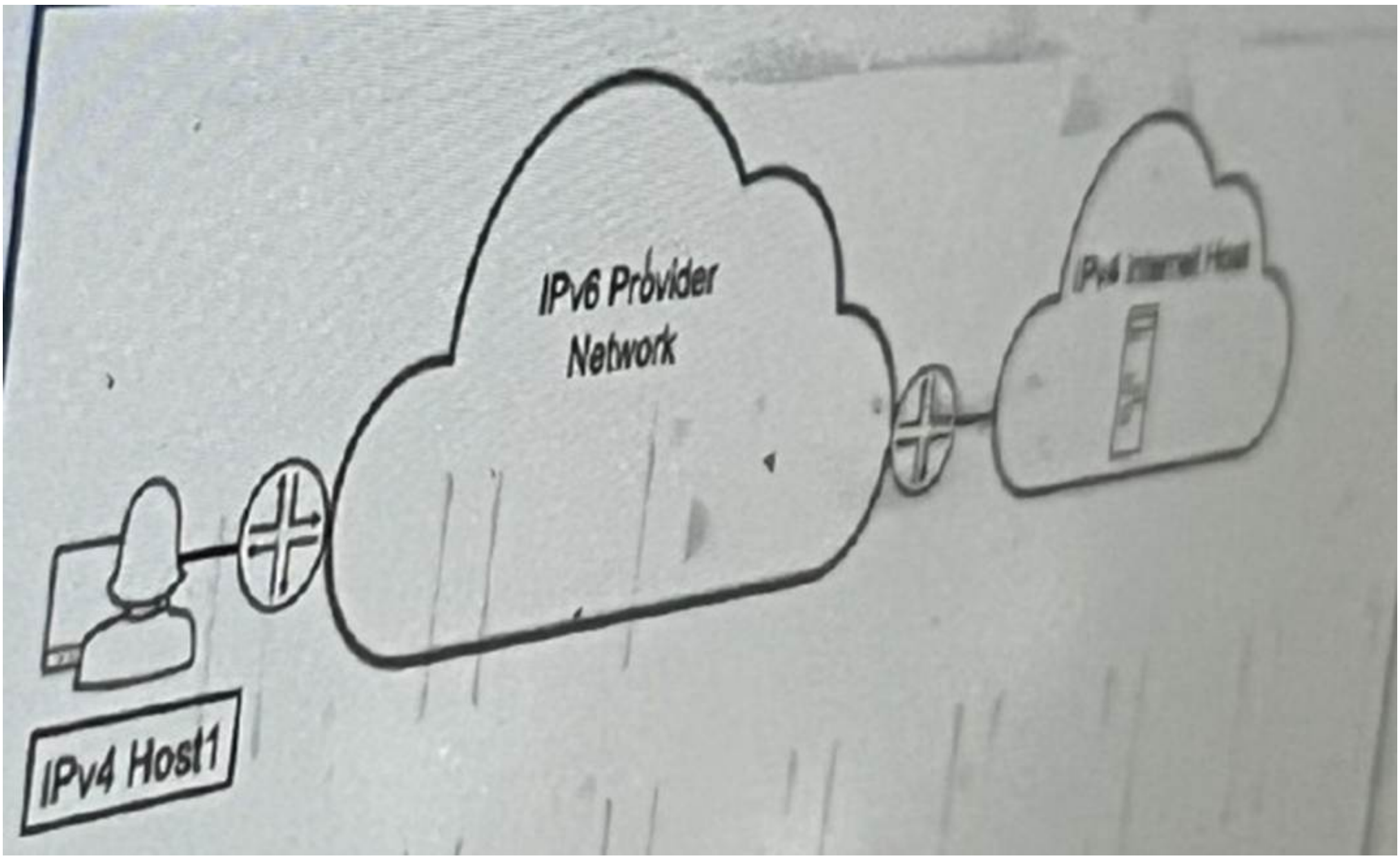



Which two statements are correct about the output shown in the exhibit. (Choose Two)

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 42**
Exhibit:




Referring to the exhibit, which technology would you use to provide communication between IPv4 host1 and ipv4 internal host

A. DS-Lite
B. NAT444
C. NAT46
D. full cone NAT

**Answer:** A

**NEW QUESTION 44**
What is the advantage of using separate st0 logical units for each spoke connection?

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

**Answer:** D

**NEW QUESTION 48**
You have a multinode HA default mode deployment and the ICL is down.
In this scenario, what are two ways that the SRX Series devices verify the activeness of their peers? (Choose two.)

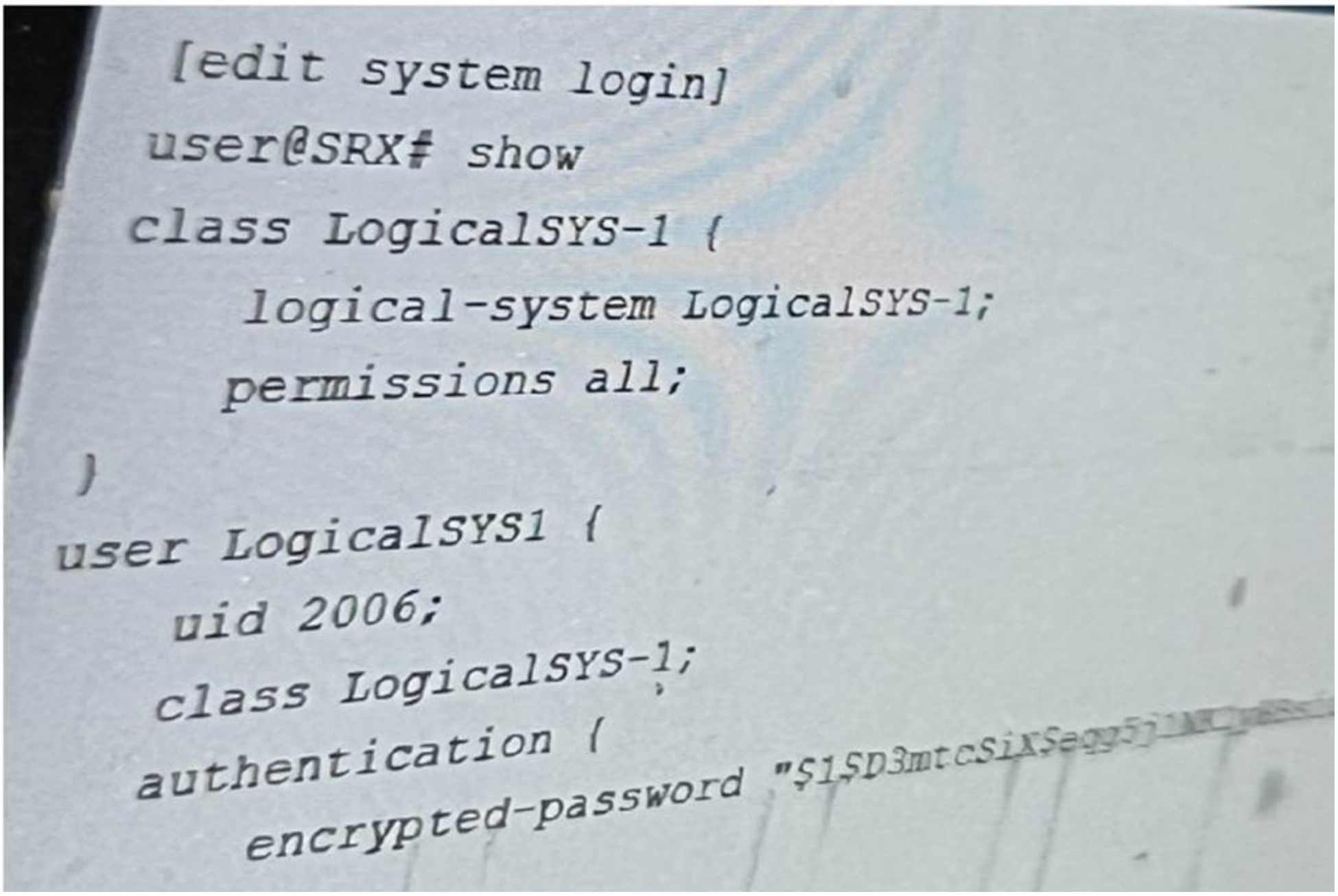
A. Custom IP addresses may be configured for the activeness probe.
B. Fabric link heartbeats are used to verify the activeness of the peers.
C. Each peer sends a probe with the virtual IP address as the destination IP address.
D. Each peer sends a probe with the virtual IP address as the source IP address and the upstream router as the destination IP address.

**Answer:** AD

**Explanation:**
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding the Scenario:
? Multinode HA Default Mode Deployment:
? ICL (Inter-Cluster Link) is Down:
? Objective:
Option A: Custom IP addresses may be configured for the activeness probe.
? Explanation:
Reference:
"You can configure the SRX Series device to send activeness probes to a configured IP address to verify the peer's state when the control link is down."
Source: Juniper Networks Documentation - Control Link Failure Detection
Option D: Each peer sends a probe with the virtual IP address as the source IP address and the upstream router as the destination IP address.
* Explanation:
The SRX devices send ICMP probes to an upstream device using the redundancy group's virtual IP address as the source.

This helps determine if the peer node is still active by verifying network reachability.
Reference:
"When the control link fails, each node sends ICMP pings to the configured probe addresses using the redundancy group's virtual IP address as the source."
Source: Juniper Networks Documentation - Chassis Cluster Control Link Failure
Why Options B and C are Incorrect:
Option B: Fabric link heartbeats cannot be used because the ICL (which includes the fabric link) is down.
Option C: Probes are sent to upstream devices, not using the virtual IP address as the destination.
Conclusion:
The correct options are A and D because they accurately describe how SRX devices verify activeness without the ICL.

**NEW QUESTION 51**
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 56**
Referring to the exhibit,

```
security {
    advance-policy-based-routing {
        profile profile1 {
            rule Web-Proxy {
                match {
                    dynamic-application [ junos:HTTP junos:HTTPS ];
                }
                then {
                    routing-instance R1;
                }
            }
            rule DNS {
                match {
                    dynamic-application-group junos:DNS;
                }
                then {
                    routing-instance R2;
                }
            }
        }
    }
}
routing-instances {
    R1 {
        instance-type forwarding;
        routing-options {
            static {
                route 192.168.0.0/16 next-hop 10.1.0.1;
```

which statement about TLS 1.2 traffic is correct?

A. TLS 1.2 traffic will be sent to routing instance R1 but not forwarded to the next hop.
B. TLS 1.2 traffic will be sent to routing instance R1 and forwarded to next hop 10.1.0.1.
C. TLS 1.2 traffic will be sent to routing instance R2 but not forwarded to the next hop.
D. TLS 1.2 traffic will be sent to routing instance R2 and forwarded to next hop 10.2.0.1.

**Answer:** A

**NEW QUESTION 60**
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 65**
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 67**
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 71**
Click the Exhibit button.

```
user@srx2> 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: BACKUP
        Activeness Priority: 100
        Preemption: DISABLED
        Process Packet In Backup State: NO
        Control Plane State: READY
        System Integrity Check: COMPLETE
        Failure Events: NONE
        Peer Information:
          Peer Id: 1
          Status : ACTIVE
          Health Status: HEALTHY
          Failover Readiness: N/A
        Virtual IP Info:
          Index: 2
```

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

A. This device is the backup node for SRG1.
B. 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.
C. This device is the active node for SRG1.
D. 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.

**Answer:** CD

**NEW QUESTION 72**
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 77**
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.
==========

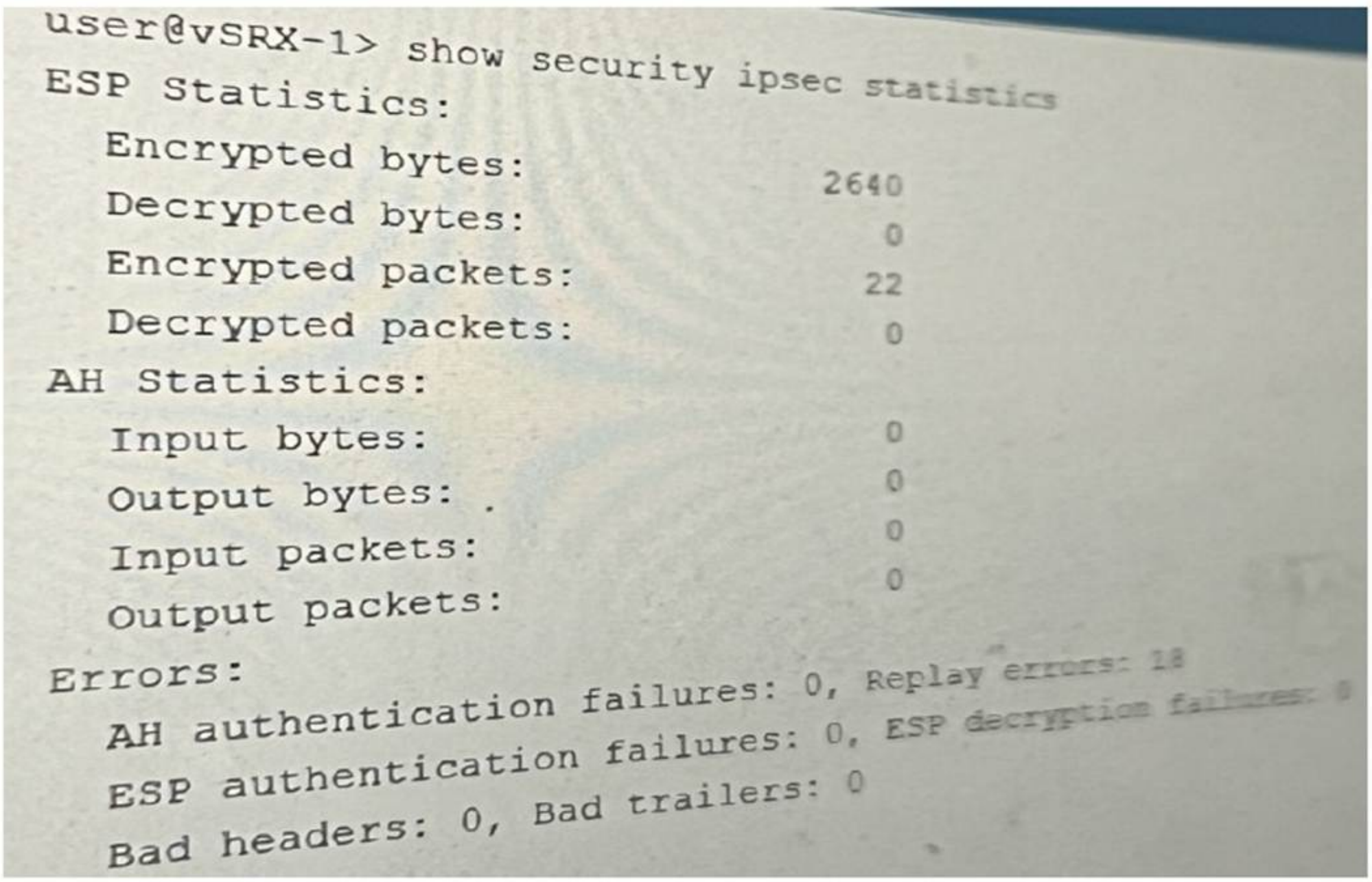
**NEW QUESTION 79**
Which two statements are true regarding NAT64? (Choose two.)

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 82**
Referring to the exhibit, which two statements are true ?



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

**Answer:** BD

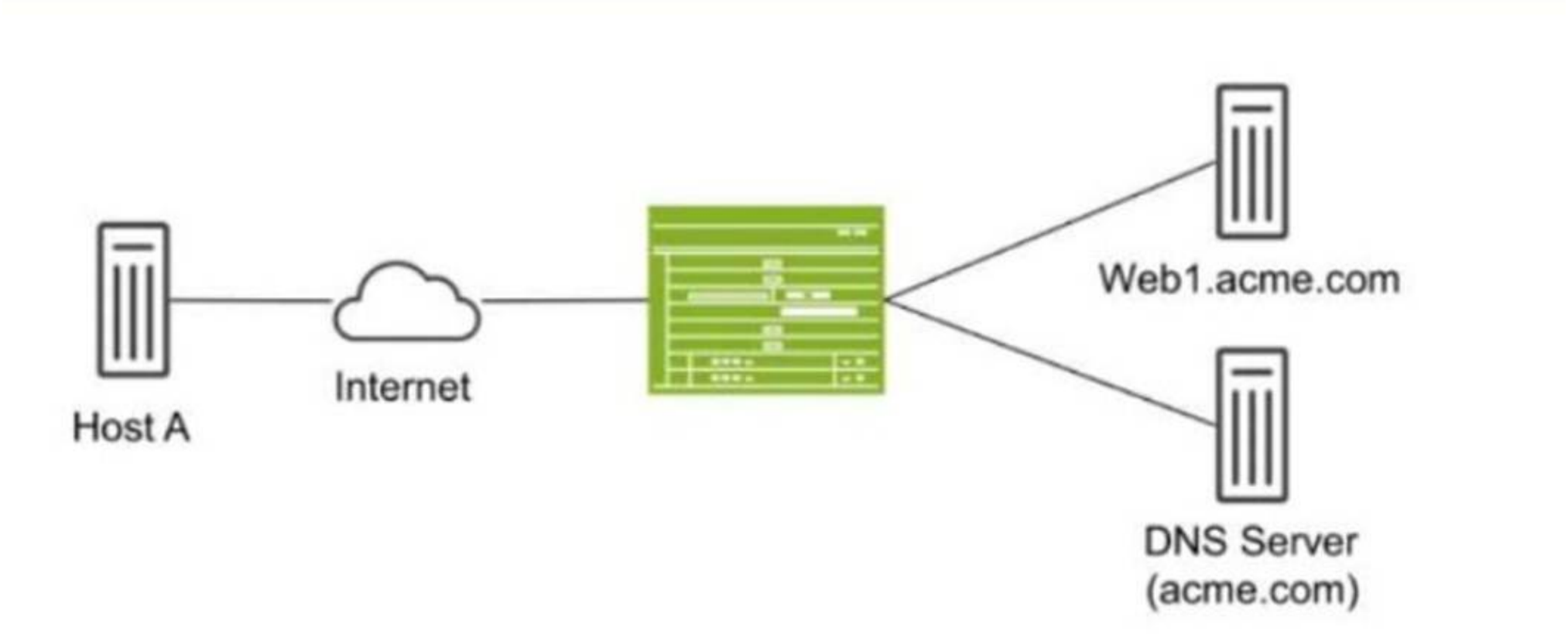
**NEW QUESTION 85**
You want to bypass IDP for traffic destined to social media sites using APBR, but it is not working and IDP is dropping the session.
What are two reasons for this problem? (Choose two.)

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

**Answer:** AC

**Explanation:**
? Explanation of Answer A (Session Reclassification):
? Explanation of Answer C (Application Services Bypass): Example configuration for bypassing IDP services:
bash
set security forwarding-options advanced-policy-based-routing profile <profile-name> application-services-bypass
Step-by-Step Resolution:
? Reclassify the Session Midstream: Command to clear the session:
bash
clear security flow session destination-prefix <ip-address>
? Configure Application Services Bypass: Example configuration:
bash
set security forwarding-options advanced-policy-based-routing profile <profile-name> application-services-bypass
Juniper Security Reference:
? Session Reclassification in APBR: APBR requires reclassification of sessions in real-time to ensure midstream packets are processed by the correct rule. This is crucial when policies change dynamically or new rules are added.
? Application Services Bypass in APBR: This feature ensures that security services such as IDP are bypassed for traffic that matches specific APBR rules. This is essential for applications where performance is a priority and security inspection is not necessary.
==========

**NEW QUESTION 90**
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.
==========

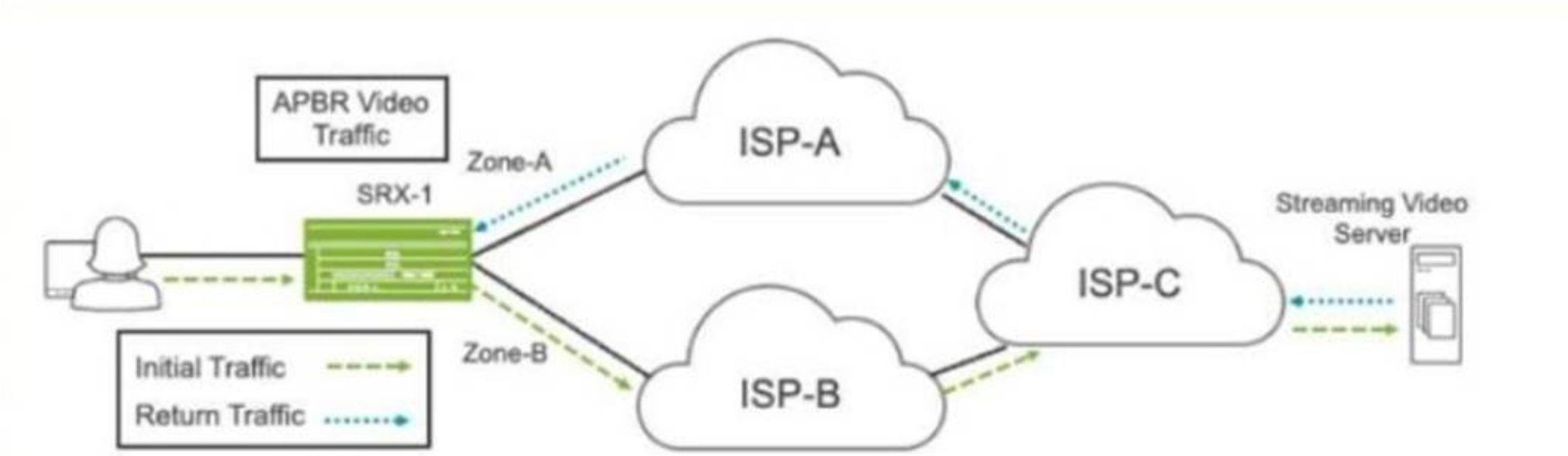
**NEW QUESTION 94**
Your customer needs embedded security in an EVPN-VXLAN solution.
What are two benefits of adding an SRX Series device in this scenario? (Choose two.)

A. It enhances tunnel inspection for VXLAN encapsulated traffic with Layer 4-7 security services.
B. It adds extra security with the capabilities of an enterprise-grade firewall in the EVPN- VXLAN underlay.
C. It adds extra security with the capabilities of an enterprise-grade firewall in the EVPN- VXLAN overlay.
D. It enhances tunnel inspection for VXLAN encapsulated traffic with only Layer 4 security services.

**Answer:** AC

**Explanation:**
The SRX Series can inspect traffic within VXLAN tunnels, providing in-depth security services across multiple layers. Adding SRX in the overlay network allows comprehensive control, leveraging advanced firewall capabilities. For more details, see Juniper EVPN-VXLAN Security.
When integrating an SRX Series device into an EVPN-VXLAN solution, it offers several security benefits:
? Layer 4-7 Security Services (Answer A): The SRX can provide deep packet
inspection for VXLAN encapsulated traffic, enhancing security by offering services such as intrusion prevention, application layer filtering, and antivirus scanning. This allows security monitoring of the encapsulated traffic at higher layers of the OSI model (Layers 4-7), which is essential for advanced threat detection.
? Security in the Overlay Network (Answer C): The SRX adds security by functioning
as an enterprise-grade firewall within the EVPN-VXLAN overlay. This means that traffic flowing between virtualized segments or networks can be inspected and filtered using SRX firewall rules, ensuring that the VXLAN overlay remains secure.
These features make the SRX a powerful addition for securing EVPN-VXLAN environments, providing comprehensive security for encapsulated traffic and ensuring that both the underlay and overlay networks are protected.
: Juniper documentation on SRX integration in EVPN-VXLAN solutions.
==========

**NEW QUESTION 96**
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 97**
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 98**
Click the Exhibit button.

```
user@SRX>show security flow session
Session ID: 100, Policy name: L1-to-L9/11, Timeout: 36, Session State: Valid
  In: 10.10.101.10/1 --> 10.10.102.10/1;icmp, Conn Tag: 0x0, If: ge-0/0/4.0, Pkts: 1, Bytes: 84,
  Out: 10.10.102.10/1 --> 10.10.101.10/1;icmp, Conn Tag: 0x0, If: ge-0/0/5.0, Pkts: 0, Bytes: 0,
```

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

A. The traffic is permitted.
B. The traffic was initiated by the 10.10.102.10 address.
C. The destination device is not responding.
D. The traffic is denied.

**Answer:** AC

**Explanation:**
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding the Session Output:
? Session State: Valid
? Policy Name: L1-to-L9/11
? In Direction:
? Out Direction:
Option A: The traffic is permitted.
? Explanation:
Reference:
"A session with a Valid state and an associated policy name indicates permitted traffic."
Source: Juniper TechLibrary - Understanding Security Flow Sessions
Option C: The destination device is not responding.
* Explanation:
The lack of packets in the Out direction suggests that the destination (10.10.102.10) is not responding.
Reference:
"If there are no packets in the reverse direction, it may indicate that the destination host is not responding."
Source: Juniper KB - Troubleshooting Traffic Flows
Why Options B and D are Incorrect:
Option B: The traffic was initiated by 10.10.101.10, not 10.10.102.10. Option D: The session is valid and permitted; the traffic is not denied. Conclusion:
The correct options are A and C because they accurately describe the state of the session.

**NEW QUESTION 102**
You are setting up multinode HA for redundancy.
Which two statements are correct in this scenario? (Choose two.)

A. Dynamic routing is active on one device at a time.
B. Dynamic routing is active on both devices.
C. Physical connections are used for the control and fabric links.
D. ICL links require Layer 3 connectivity between peers.

**Answer:** AC

**Explanation:**
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding Multinode HA:
? Chassis Cluster in Active/Passive Mode:
? Dynamic Routing Protocols:
Option A: Dynamic routing is active on one device at a time.
? Explanation:
Reference:
"In a chassis cluster, the primary node handles all control plane tasks, including dynamic routing."
Source: Juniper TechLibrary - Chassis Cluster Overview
Option C: Physical connections are used for the control and fabric links.
* Explanation:
Control and fabric links are direct physical connections between cluster nodes.
Reference:
"The control and fabric links must be connected using physical interfaces between the nodes."
Source: Juniper TechLibrary - Chassis Cluster Components
Why Options B and D are Incorrect:
Option B: Dynamic routing is not active on both devices simultaneously in active/passive mode.
Option D: The Inter-Cluster Link (ICL) uses Layer 2 connectivity, not Layer 3.
Conclusion:
The correct options are A and C.

**NEW QUESTION 106**
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 107**
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

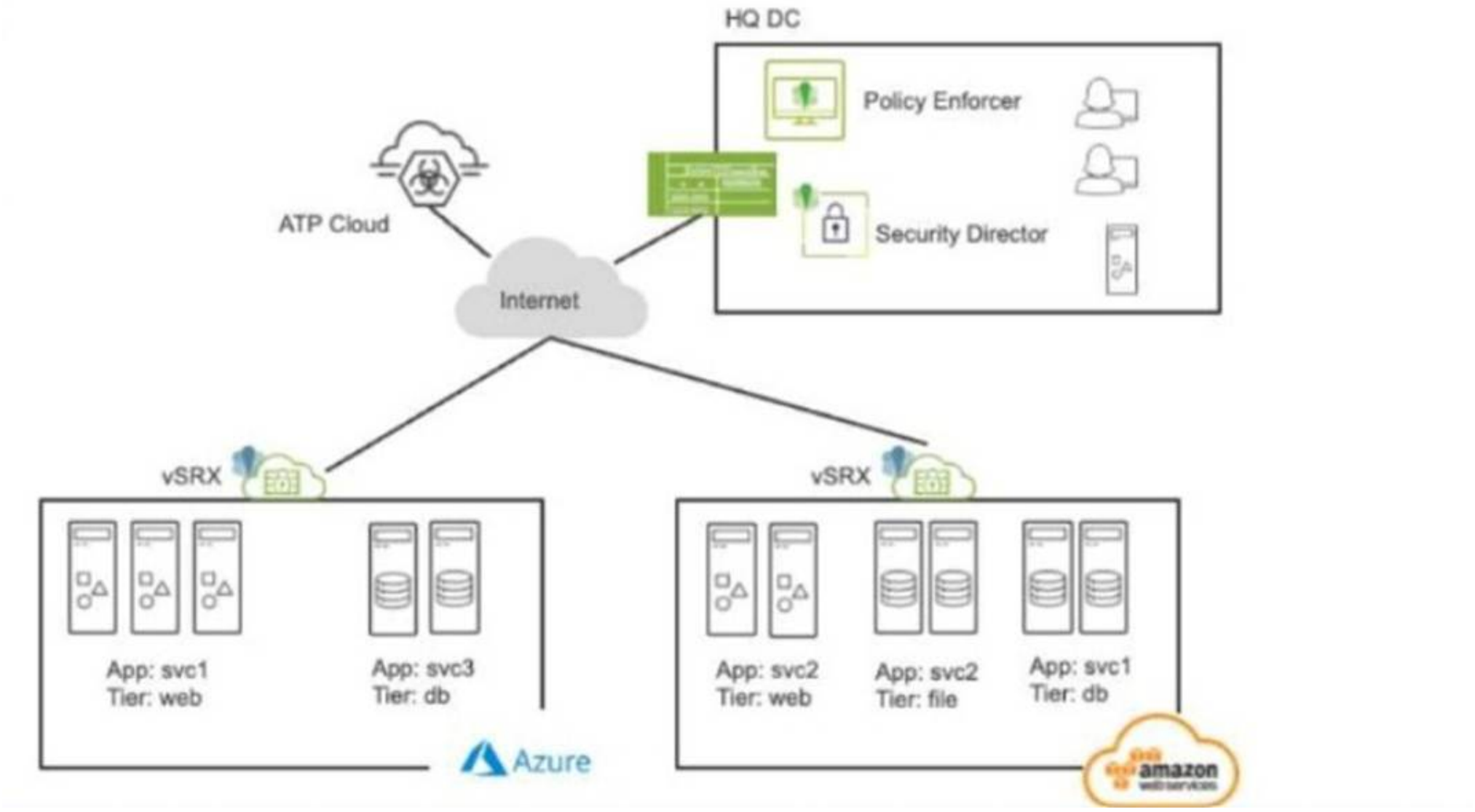
**NEW QUESTION 111**
You want to use a security profile to limit the system resources allocated to user logical systems.
In this scenario, which two statements are true? (Choose two.)

A. If nothing is specified for a resource, a default reserved resource is set for a specific logical system.
B. If you do not specify anything for a resource, no resource is reserved for a specific logical system, but the entire system can compete for resources up to the maximum available.
C. One security profile can only be applied to one logical system.
D. One security profile can be applied to multiple logical systems.

**Answer:** BD

**Explanation:**
When using security profiles to limit system resources in Juniper logical systems:
? No Resource Specification (Answer B): If a resource limit is not specified for a logical system, no specific amount of system resources is reserved for it. Instead, the logical system competes for resources along with others in the system, up to the maximum available. This allows flexible resource allocation, where logical systems can scale based on actual demand rather than predefined limits.
? Multiple Logical Systems per Security Profile (Answer D): A single security profile can be applied to multiple logical systems. This allows administrators to define resource limits once in a profile and apply it across several logical systems, simplifying management and ensuring consistency across different environments.
These principles ensure efficient and flexible use of system resources within a multi-tenant or multi-logical-system environment.
: Juniper security profiles and logical system documentation.
==========

**NEW QUESTION 116**
Exhibit:



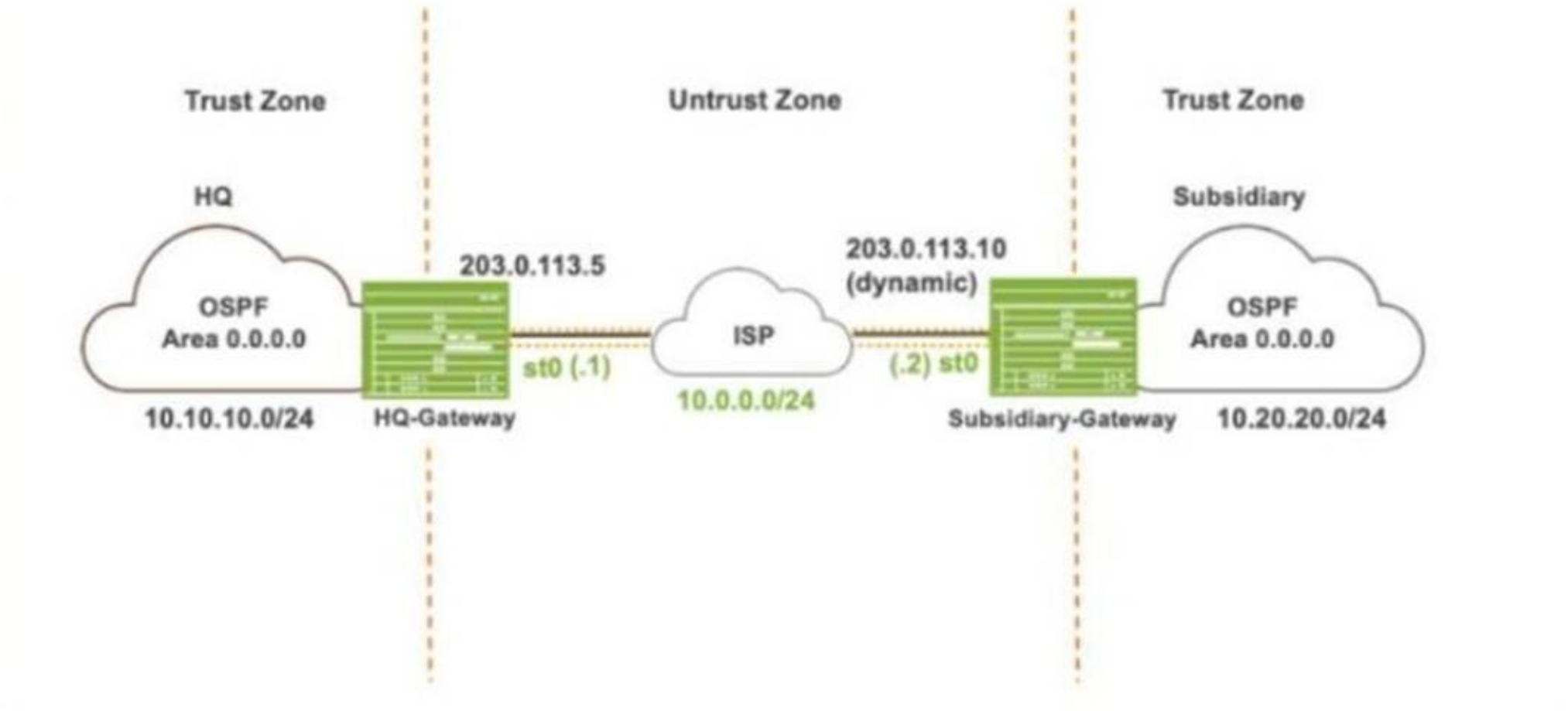

Referring to the exhibit, what do you use to dynamically secure traffic between the Azure and AWS clouds?

A. You can dynamically secure traffic between the clouds by using user identities in the security policies.
B. You can dynamically secure traffic between the clouds by using advanced connection tracking in the security policies.
C. You can dynamically secure traffic between the clouds by using security tags in the security policies.
D. You can dynamically secure traffic between the clouds by using URL filtering in the security policies.

**Answer:** C

**Explanation:**
Security tags facilitate dynamic traffic management between cloud environments like Azure and AWS. Tags allow flexible policies that respond to cloud-native events or resource changes, ensuring secure inter-cloud communication. For more information, see Juniper Cloud Security Tags.
In the scenario depicted in the exhibit, where traffic needs to be dynamically secured between Azure and AWS clouds, the best method to achieve dynamic security is by using
security tags in the security policies.
? Explanation of Answer C (Security Tags in Security Policies):
Juniper Security Reference:
? Dynamic Security with Security Tags: This feature allows you to dynamically secure cloud-based traffic using metadata and tags, ensuring that security policies remain effective even in dynamic environments. Reference: Juniper Security Tags Documentation.
==========

**NEW QUESTION 117**
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 121**
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 125**
Which two statements about transparent mode and Ethernet switching mode on an SRX series device are correct.

A. In Ethernet switching mode, Layer 2 interfaces must be placed in a security zone.
B. In Ethernet switching mode, IRB interfaces must be placed in a security zone.
C. In transparent mode, Layer 2 interfaces must be placed in a security zone.
D. In transparent mode, IRB interfaces must be placed in a security zone.

**Answer:** BC

**NEW QUESTION 127**
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 129**
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 131**
You need to generate a certificate for a PKI-based site-to-site VPN. The peer is expecting to
user your domain name vpn.juniper.net.
Which two configuration elements are required when you generate your certificate request? (Chose two,)

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

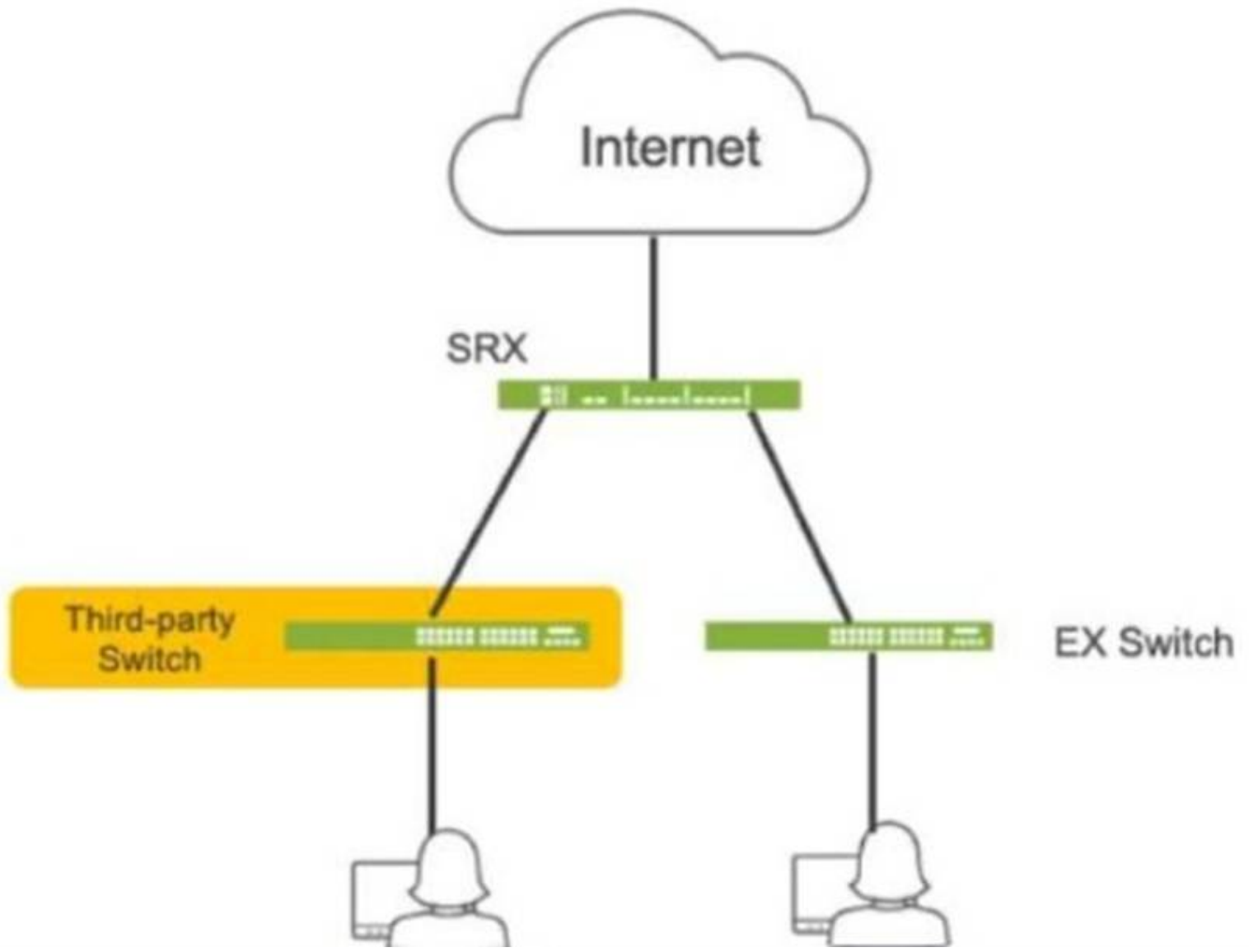
**Answer:** BD

**NEW QUESTION 132**
Which three statements about persistent NAT are correct? (Choose Three)

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

**Answer:** BCD

**NEW QUESTION 137**
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 138**
You are configuring an interconnect logical system that is configured as a VPLS switch to allow two logical systems to communicate.
Which two parameters are required when configuring the logical tunnel interfaces?
(Choose two.)

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

**Answer:** CD

**NEW QUESTION 141**
.....

# Relate Links

**100% Pass Your JN0-637 Exam with Exambible Prep Materials**

https://www.exambible.com/JN0-637-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/