Juniper.JN0-637.by.Mark.59q

Number: JN0-637
Passing Score: 800
Time Limit: 120
File Version: 3.0

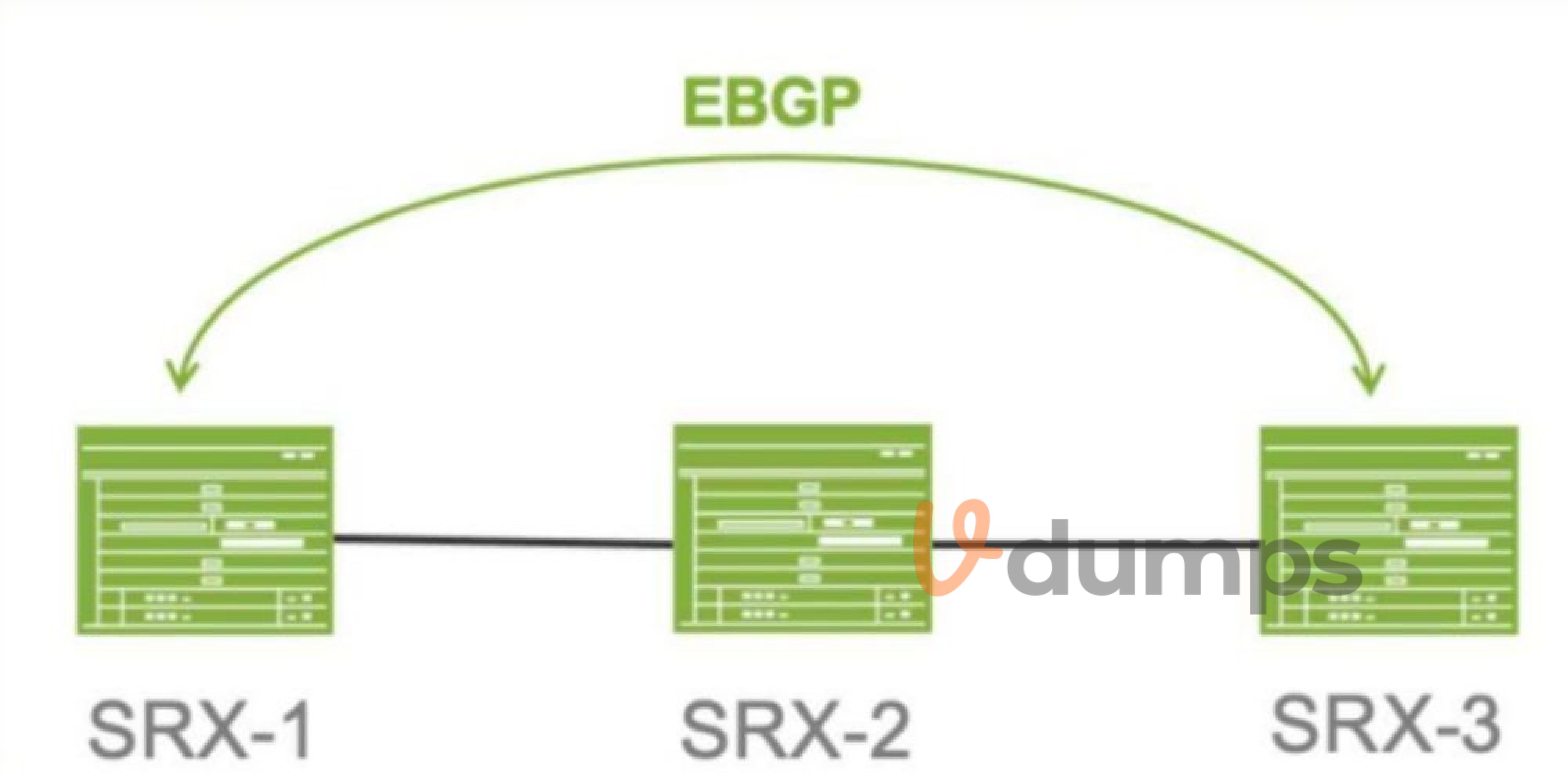
Exam Code: JN0-637

Exam Name: Security, Professional

Exam A

QUESTION 1

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.

Correct Answer: D
Section:
Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security Reference
Understanding the Scenario:
SRX-1 and SRX-3:
Need to establish an EBGP session through SRX-2.
Issue:
BGP session is not coming up despite correct configurations on SRX-1 and SRX-3.

Option D: The security policy to allow SRX-1 and SRX-3 to communicate on TCP port 179 should be configured.
BGP uses TCP port 179 for establishing sessions.
SRX-2 must have a security policy allowing traffic between SRX-1 and SRX-3 on TCP port 179.
'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.

QUESTION 2
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

Correct Answer: B
Section:

QUESTION 3
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.)

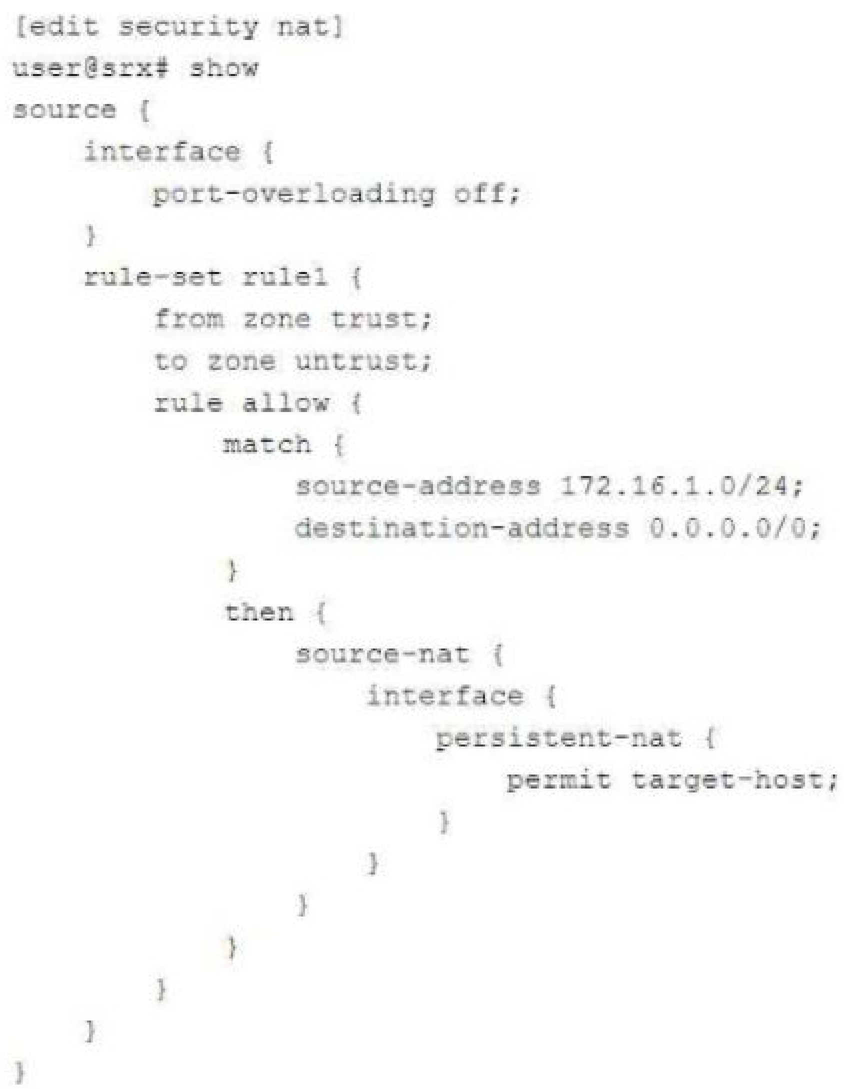
A. [edit security nat source] user@OfficeA# show rule-set OfficeBtoA { from zone OfficeB; to zone OfficeA; rule 1 { match { source-address 192.168.210.0/24; destination-address 192.168.200.0/24; } then { source-nat { interface; } } } }
B. [edit security nat static] user@OfficeA# show rule-set From-Office-B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

Correct Answer: A, D
Section:
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
Reference:

Juniper NAT Configuration Guide: Detailed instructions on how to configure source NAT and resolve address conflicts between networks.

QUESTION 4

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.

Correct Answer: A, B

Section:

QUESTION 5

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.

Correct Answer: A, B, C
Section:
Explanation:
A . The interface is not assigned to a security zone.
SRX Series devices rely heavily on security zones for traffic management. If an interface isn't assigned to a zone, the device won't know how to handle traffic arriving on that interface, including ping requests (ICMP echo requests).
B . The interface's host-inbound-traffic security zone configuration does not permit ping.
Even if an interface is in a zone, you must explicitly allow ICMP ping traffic within the zone's host-inbound-traffic settings. By default, most zones block ping for security reasons.
C . The ping traffic is matching a firewall filter.
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.
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.

QUESTION 6
You are deploying IPsec VPNs to securely connect several enterprise sites with ospf for dynamic routing. Some of these sites are secured by third-party devices not running Junos.
Which two statements are true for this deployment? (Choose two.)

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

B. Sites with overlapping address spaces can be supported.

C. OSPF over GRE over IPsec is required to enable intersite dynamic routing

D. Sites with overlapping address spaces cannot be supported.

Correct Answer: B, C
Section:
Explanation:
Understanding the Scenario:Objective: Deploy IPsec VPNs connecting multiple enterprise sites using OSPF for dynamic routing.Challenge: Some sites use third-party devices not running Junos OS.Considerations:Compatibility between Juniper and third-party devices.Support for dynamic routing protocols (OSPF) over IPsec VPNs.Handling overlapping IP address spaces.Option Analysis:Option A: OSPF over IPsec can be used for intersite dynamic routing.OSPF Characteristics:OSPF uses multicast addresses (224.0.0.5 and 224.0.0.6) for neighbor discovery and routing updates.IPsec Limitations:Standard IPsec tunnel mode does not support multicast traffic natively.Multicast traffic cannot traverse IPsec tunnels unless encapsulated.Juniper Solution:Juniper devices can use routed VPNs (route-based VPNs) with st0 interfaces, allowing OSPF over IPsec.However, this requires support from both ends of the VPN tunnel.Third-Party Devices:May not support OSPF over IPsec without additional configurations.Conclusion:Option A is not universally true in this scenario due to third-party device limitations.'OSPF can be run over IPsec VPNs using route-based VPNs, but interoperability with third-party devices must be verified.'Source: Juniper TechLibrary - OSPF over IPsec VPNsOption B: Sites with overlapping address spaces can be supported.Overlapping IP Address Spaces:Occurs when different sites use the same IP subnets.Can cause routing ambiguities and conflicts.Solution:NAT over VPN:Use Network Address Translation (NAT) to translate overlapping IP addresses to unique addresses.Juniper devices support NAT over IPsec VPNs.Third-Party Device Considerations:Need to ensure third-party devices support NAT over IPsec.Many enterprise-grade

devices provide this functionality.Conclusion:Option B is true; overlapping address spaces can be supported using NAT.'When sites have overlapping IP addresses, NAT can be used over IPsec VPNs to resolve address conflicts.'Source: Juniper TechLibrary - NAT with IPsec VPNsOption C: OSPF over GRE over IPsec is required to enable intersite dynamic routing.GRE Tunnels:Generic Routing Encapsulation (GRE) can encapsulate multicast and broadcast traffic.Allows OSPF packets to be transmitted over IPsec VPNs.IPsec Encryption:GRE tunnels can be encrypted using IPsec for secure communication.Interoperability:GRE over IPsec is a common method to support OSPF between devices from different vendors.Third-party devices are more likely to support GRE over IPsec than OSPF over IPsec directly.Conclusion:Option C is true; using OSPF over GRE over IPsec is required in this scenario.'To run OSPF between devices that do not support multicast over IPsec, GRE tunnels can be used over IPsec VPNs.'Source: Juniper TechLibrary - Configuring GRE over IPsecOption D: Sites with overlapping address spaces cannot be supported.Contradicts Option B.As established, overlapping address spaces can be supported using NAT over IPsec VPNs.Conclusion:Option D is false.Conclusion:Answer:s: B and COption B: Overlapping address spaces can be supported using NAT over IPsec VPNs.Option C: OSPF over GRE over IPsec is required to enable intersite dynamic routing, especially when third-party devices are involved.Additional DetailedWhy OSPF over IPsec May Not Be Feasible (Option A):Multicast Traffic:OSPF relies on multicast for neighbor discovery and updates.IPsec in tunnel mode does not natively support multicast traffic.Third-Party Devices:May not support proprietary extensions or configurations required to run OSPF directly over IPsec.Workaround:Encapsulate OSPF multicast packets within GRE tunnels, which can carry multicast traffic over unicast IPsec tunnels.Why OSPF over GRE over IPsec Is Necessary (Option C):GRE Tunnels:Encapsulate multicast/broadcast traffic into unicast packets.Allow routing protocols like OSPF to function over IPsec VPNs.Compatibility:GRE is a widely supported protocol across different vendors.Facilitates interoperability between Juniper and third-party devices.Supporting Overlapping Address Spaces (Option B):NAT over IPsec:Translates private IP addresses to unique addresses across the VPN.Prevents routing conflicts and allows communication between sites with overlapping subnets.Considerations:Requires proper configuration on both ends of the VPN tunnel.Third-party devices must support NAT over IPsec.Reference to Juniper Security Concepts:Route-Based VPNs:'Route-based VPNs use virtual tunnel interfaces (st0) and support dynamic routing protocols over IPsec.'Source: Juniper TechLibrary - Route-Based VPNsGRE over IPsec:'GRE over IPsec allows the transmission of multicast and non-IP protocols over IPsec tunnels.'Source: Juniper TechLibrary - GRE over IPsec OverviewNAT with IPsec VPNs:'NAT can be applied to IPsec VPN traffic to resolve overlapping address issues and facilitate communication between sites.'Source: Juniper TechLibrary - NAT with IPsecFinal Notes:Interoperability:When working with third-party devices, always verify compatibility for protocols and features.Best Practices:Use GRE over IPsec for dynamic routing protocols requiring multicast support across IPsec VPNs.Implement NAT over VPN when dealing with overlapping address spaces.

QUESTION 7
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,

Correct Answer: A, C, D
Section:
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.

QUESTION 8
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

Correct Answer: A, C, D

Section:
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.

QUESTION 9

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.

Correct Answer: A, C
Section:
Explanation:
Explanation of Answer A (Session Reclassification):
APBR (Advanced Policy-Based Routing) requires the session to be classified based on the specified rule, which can change midstream as additional packets are processed. If the session was already established before the APBR rule took effect, the traffic may not be correctly reclassified to match the new APBR rule, leading to IDP (Intrusion Detection and Prevention) processing instead of being bypassed. This can occur especially when the session

was already established before the rule change.

Explanation of Answer C (Application Services Bypass):

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

Example configuration for bypassing IDP services:

bash

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

Step-by-Step Resolution:

Reclassify the Session Midstream:

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

Command to clear the session:

bash

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

Configure Application Services Bypass:

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

Example configuration:

bash

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

Juniper Security

Reference:

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

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

QUESTION 10

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.

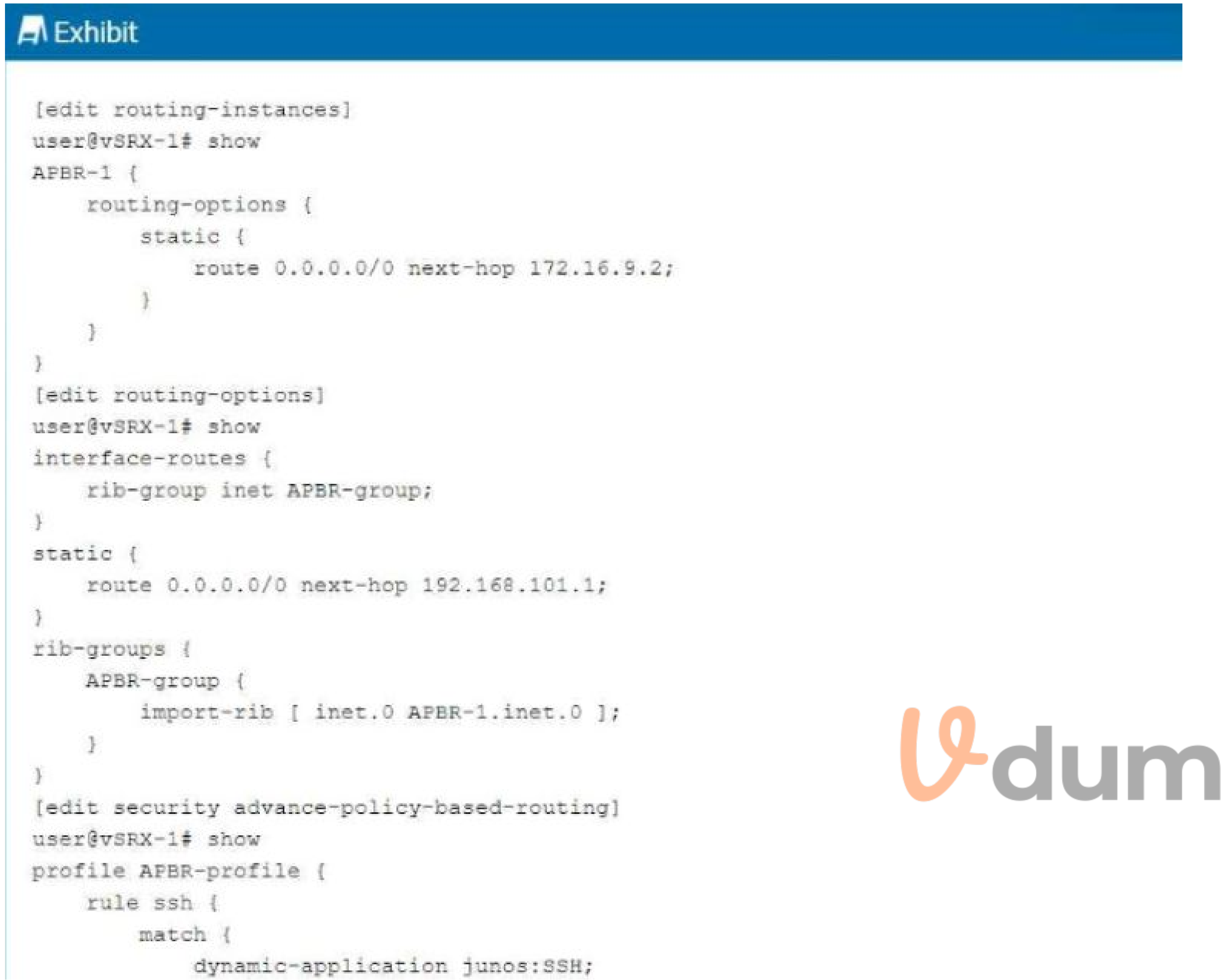
D. IRB interfaces cannot be used to route traffic.

Correct Answer: B, C

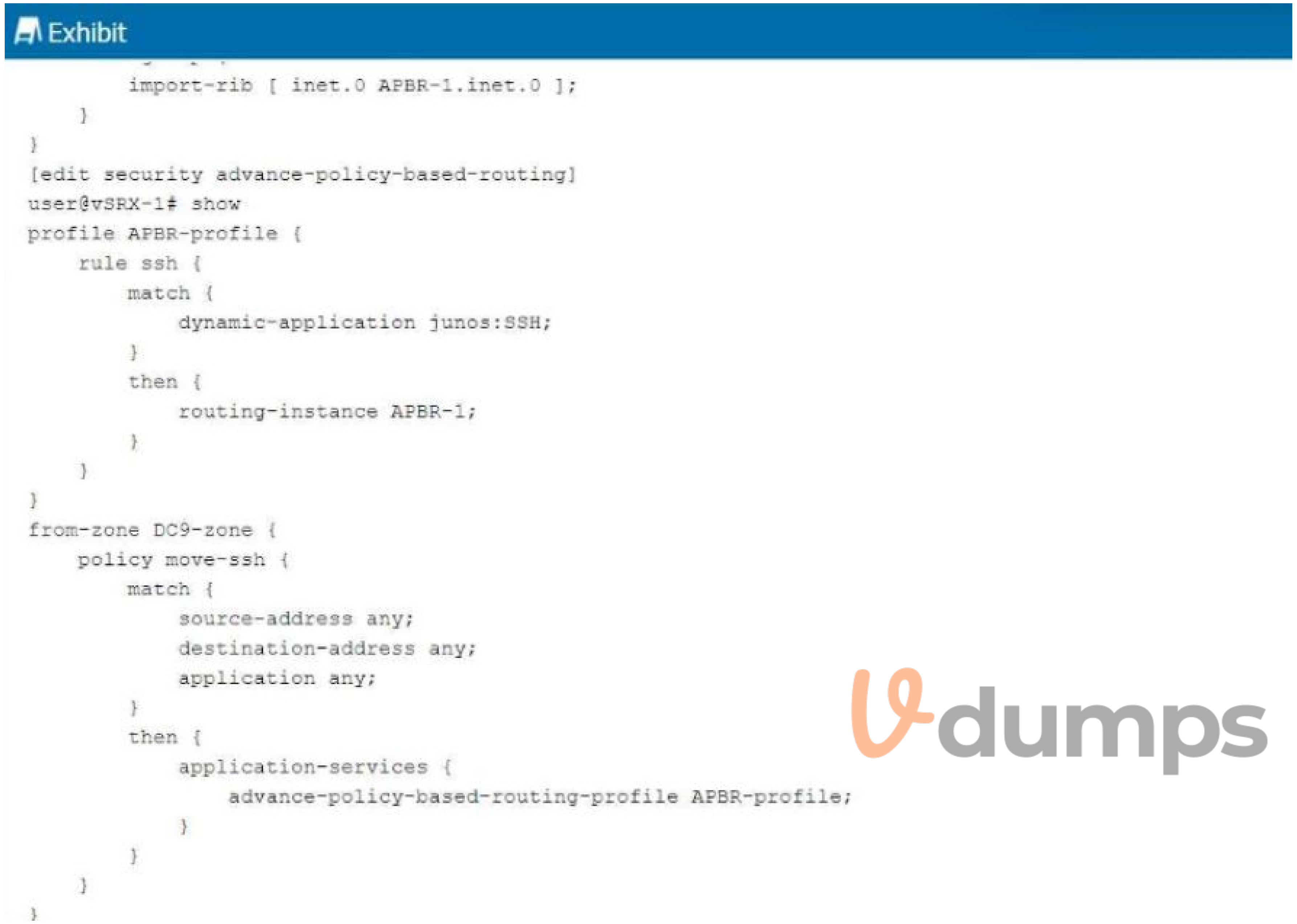
Section:

QUESTION 11

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.

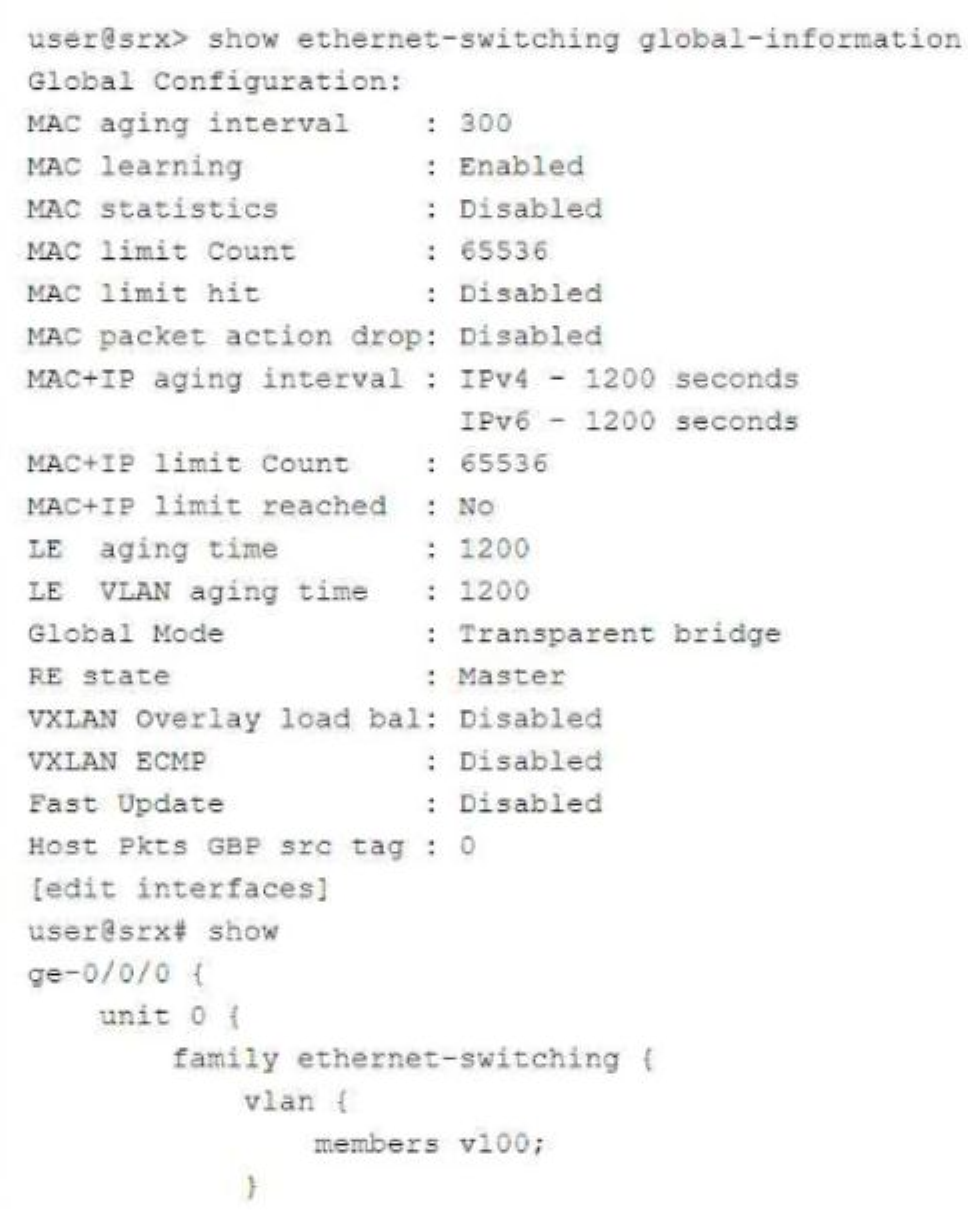
B. Change the routing instance to a forwarding instance.

C. Change the routing instance to a virtual router instance.

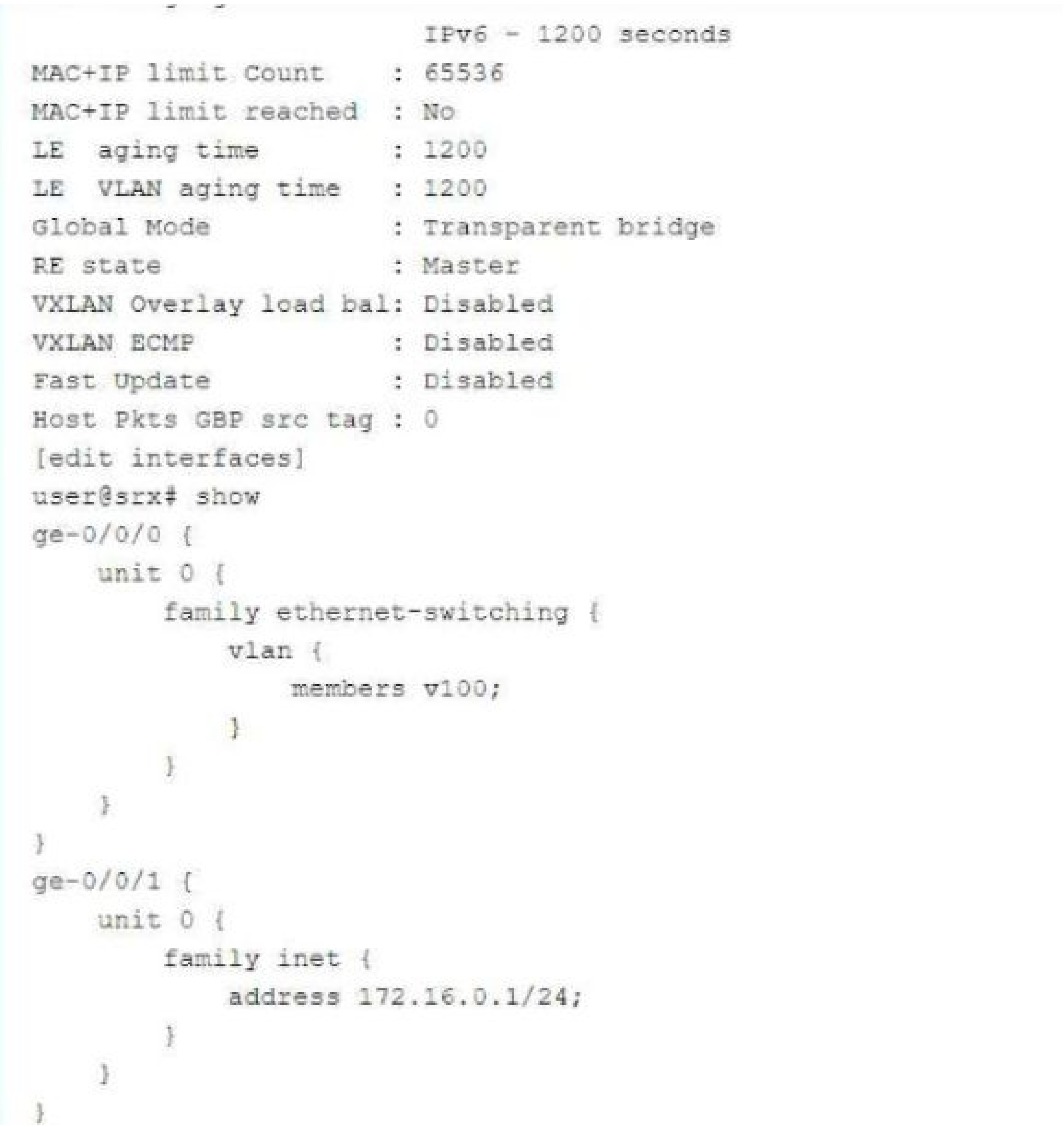
D. Remove the default static route from the main instance configuration.

Correct Answer: B
Section:

QUESTION 12
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

Correct Answer: C
Section:

QUESTION 13
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.

Correct Answer: A, C
Section:
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):
When two interfaces are configured as Layer 2 interfaces and belong to the same VLAN but are not assigned to any security zone, traffic switched between them is handled purely at Layer 2. Stateful security features, such as firewall policies, are applied at Layer 3, so traffic between these interfaces will not undergo any stateful inspection or firewalling by default.
Explanation of Answer C (Interfaces Will Not Forward Traffic):
In Junos, Layer 2 interfaces must be added to a security zone to allow traffic forwarding. Since the interfaces in this scenario are not part of a security zone, they will not forward traffic by default until assigned to a zone. This is a security measure to prevent unintended forwarding of 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.

QUESTION 14
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.

Correct Answer: B, C
Section:
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):
If the packet is destined for an interface other than the ingress interface, the SRX performs a security policy evaluation specifically for the junos-host zone. This ensures that management or host-bound traffic is evaluated according to the security policies defined for that zone.
Explanation of Answer C (Packet to the Ingress Interface):
If the packet is addressed to the ingress interface, the device first checks the host-inbound-traffic configuration for the ingress interface and zone. This configuration determines whether certain types of traffic (such as SSH, HTTP, etc.) are allowed to reach the device on that specific 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
```

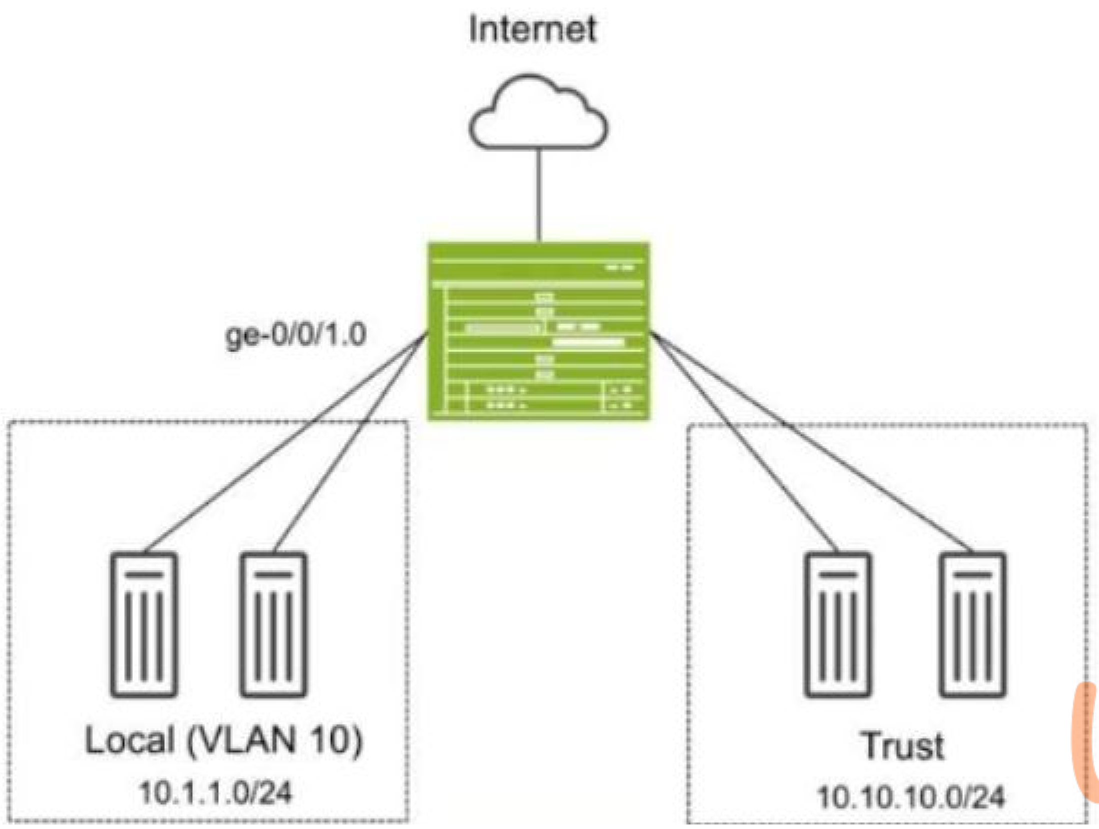
Security Policy for junos-host: Ensure policies are defined for managing traffic destined for the SRX device:
bash

```
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.

QUESTION 15
Exhibit:



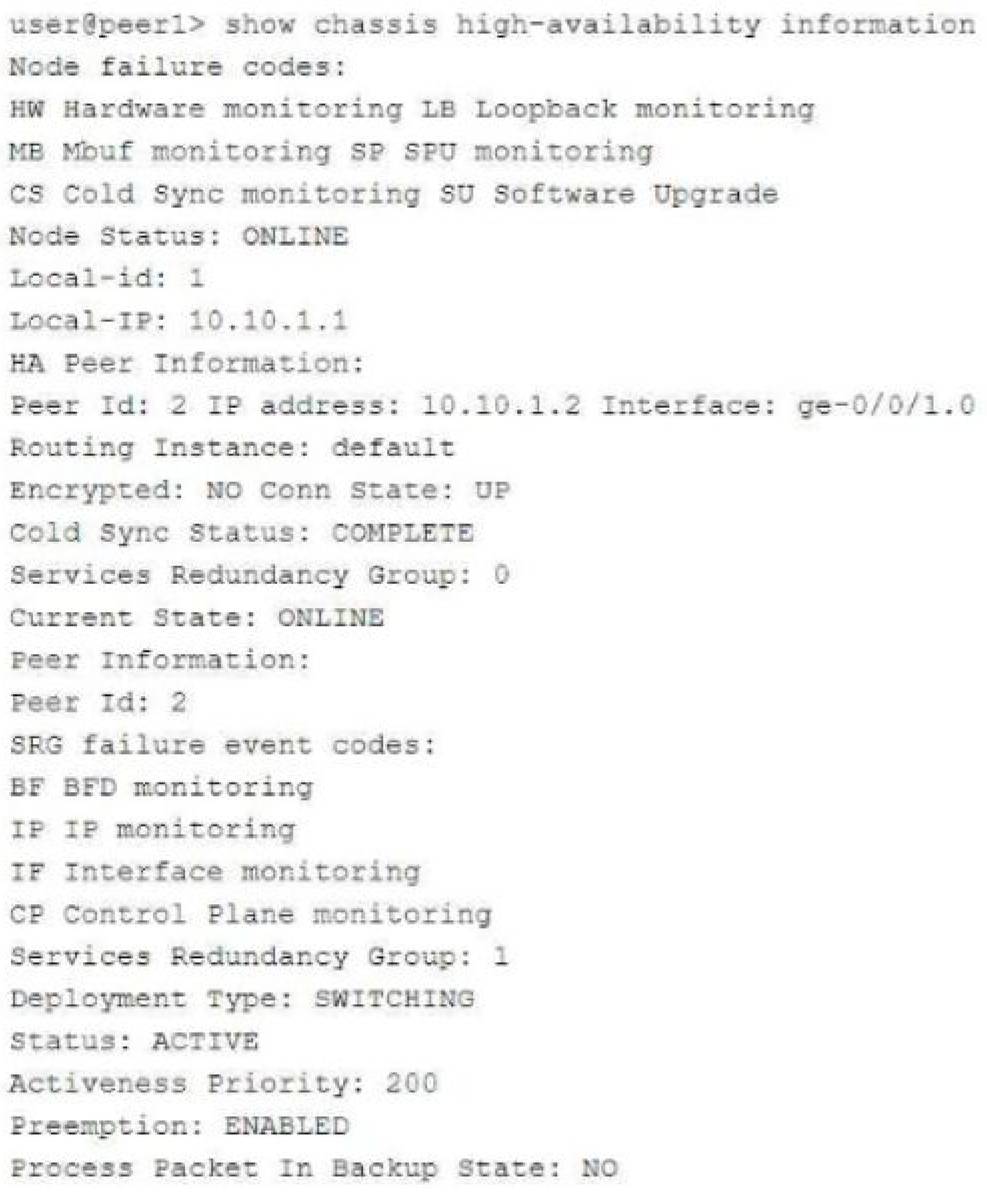
You have deployed an SRX Series device as shown in the exhibit. The devices in the Local zone have recently been added, but their SRX interfaces have not been configured. You must configure the SRX to meet the following requirements:
Devices in the 10.1.1.0/24 network can communicate with other devices in the same network but not with other networks or the SRX.
You must be able to apply security policies to traffic flows between devices in the Local zone.
Which three configuration elements will be required as part of your configuration? (Choose three.)

A. set security zones security-zone Local interfaces ge-0/0/1.0
B. set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan-members 10
C. set protocols l2-learning global-mode switching
D. set protocols l2-learning global-mode transparent-bridge
E. set security zones security-zone Local interfaces irb.10

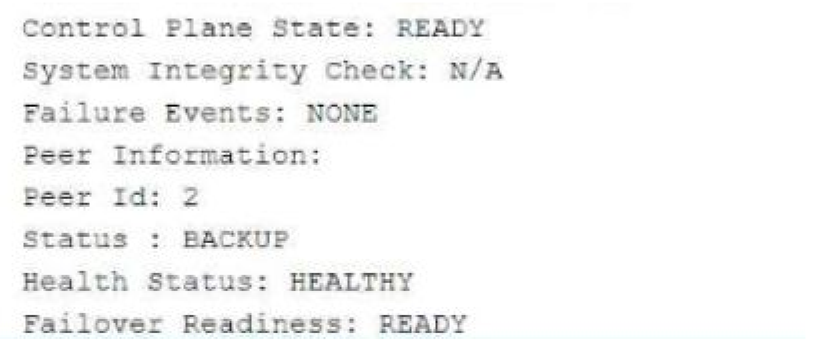
Correct Answer: A, B, D
Section:
Explanation:
In this scenario, we need to configure the SRX Series device so that devices in the Local zone (VLAN 10, 10.1.1.0/24 network) can communicate with each other but not with other networks or the SRX itself. Additionally, you must be able to apply security policies to traffic flows between the devices in the Local zone.
Explanation of Answer A (Assigning Interface to Security Zone):
You need to assign the interface ge-0/0/1.0 to the Local security zone. This is crucial because the SRX only applies security policies to interfaces assigned to security zones. Without this, traffic between devices in the Local zone won't be processed by security policies.
Configuration:
set security zones security-zone Local interfaces ge-0/0/1.0

Explanation of Answer B (Configuring Ethernet-Switching for VLAN 10):
Since we are using Layer 2 switching between devices in VLAN 10, we need to configure the interface to operate in Ethernet switching mode and assign it to VLAN 10.
Configuration:
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan-members 10
Explanation of Answer D (Transparent Bridging Mode for Layer 2):
The global mode for Layer 2 switching on the SRX device must be set to transparent-bridge. This ensures that the SRX operates in Layer 2 mode and can switch traffic between devices without routing.
Configuration:
set protocols l2-learning global-mode transparent-bridge
Summary:
Interface Assignment: Interface ge-0/0/1.0 is assigned to the Local zone to allow policy enforcement.
Ethernet-Switching: The interface is configured for Layer 2 Ethernet switching in VLAN 10.
Transparent Bridging: The SRX is configured in Layer 2 transparent-bridge mode for switching between devices.
Juniper Security
Reference:
Layer 2 Bridging and Switching Overview: This mode allows the SRX to act as a Layer 2 switch for forwarding traffic between VLAN members without routing. Reference: Juniper Transparent Bridging Documentation.

QUESTION 16
Exhibit:



```
user@peer1> show chassis high-availability information
Node failure codes:
HW Hardware monitoring LB Loopback monitoring
MB Mbuf monitoring SP SPU monitoring
CS Cold Sync monitoring SU Software Upgrade
Node Status: ONLINE
Local-id: 1
Local-IP: 10.10.1.1
HA Peer Information:
Peer Id: 2 IP address: 10.10.1.2 Interface: ge-0/0/1.0
Routing Instance: default
Encrypted: NO Conn State: UP
Cold Sync Status: COMPLETE
Services Redundancy Group: 0
Current State: ONLINE
Peer Information:
Peer Id: 2
SRG failure event codes:
BF BFD monitoring
IP IP monitoring
IF Interface monitoring
CP Control Plane monitoring
Services Redundancy Group: 1
Deployment Type: SWITCHING
Status: ACTIVE
Activeness Priority: 200
Preemption: ENABLED
Process Packet In Backup State: NO
```



```
Control Plane State: READY
System Integrity Check: N/A
Failure Events: NONE
Peer Information:
Peer Id: 2
Status : BACKUP
Health Status: HEALTHY
Failover Readiness: READY
```

Referring to the exhibit, which statement is true?

A. SRG1 is configured in hybrid mode.

B. The ICL is encrypted.

C. If SRG1 moves to peer 2, peer 1 will drop packets sent to the SRG1 interfaces.

D. If SRG1 moves to peer 2, peer 1 will forward packets sent to the SRG1 interfaces.

Correct Answer: D
Section:
Explanation:
The exhibit describes a Chassis Cluster configuration with high availability (HA) settings. The key information is related to Service Redundancy Group 1 (SRG1) and its failover behavior between the two peers.
Explanation of Answer D (Packet Forwarding after Failover):
In a typical SRX HA setup with active/backup configuration, if the SRG1 group moves to peer 2 (the backup), peer 1 (previously the active node) will forward packets to peer 2 instead of dropping them. This ensures smooth failover and seamless continuation of services without packet loss.
This behavior is part of the active/backup failover process in SRX chassis clusters, where the standby peer takes over traffic processing without disruption.
Juniper Security
Reference:
Chassis Cluster Failover Behavior: When a service redundancy group fails over to the backup peer, the previously active peer forwards traffic to the new active node. Reference: Juniper Chassis Cluster Documentation.

QUESTION 17
You are asked to create multiple virtual routers using a single SRX Series device. You must ensure that each virtual router maintains a unique copy of the routing protocol daemon (RPD) process.
Which solution will accomplish this task?

A. Secure wire

B. Tenant system

C. Transparent mode

D. Logical system

Correct Answer: D
Section:
Explanation:
Logical systems on SRX Series devices allow the creation of separate virtual routers, each with its unique RPD process. This segmentation ensures that routing and security policies are isolated across different logical systems, effectively acting like independent routers within a single SRX device. For further information, see Juniper Logical Systems Documentation.
To create multiple virtual routers on a single SRX Series device, each with its own unique copy of the routing protocol daemon (RPD) process, you need to use logical systems. Logical systems allow for the segmentation of an SRX device into multiple virtual routers, each with independent configurations, including routing instances, policies, and protocol daemons.
Explanation of Answer D (Logical System):
A logical system on an SRX device enables you to create multiple virtual instances of the SRX, each operating independently with its own control plane and routing processes. Each logical system gets a separate copy of the RPD process, ensuring complete isolation between virtual routers.
This is the correct solution when you need separate routing instances with their own RPD processes on the same physical device.
Configuration Example:

```
bash
set logical-systems <logical-system-name> interfaces ge-0/0/0 unit 0
set logical-systems <logical-system-name> routing-options static route 0.0.0.0/0 next-hop 192.168.1.1
```

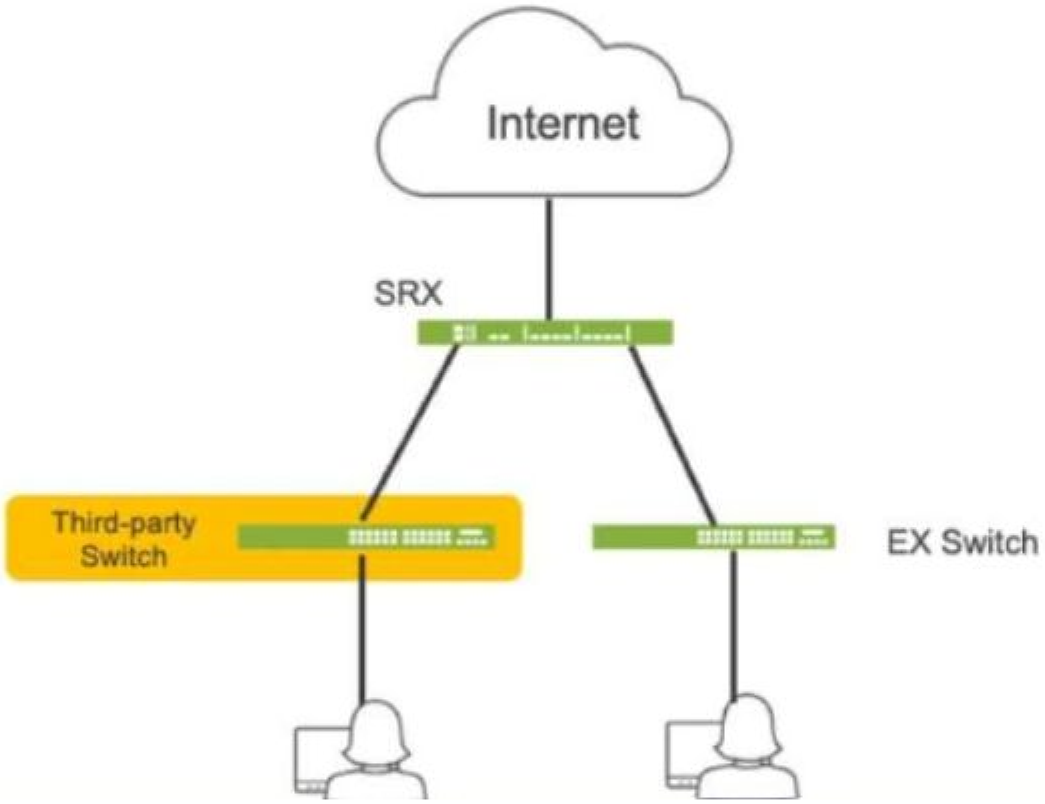
Juniper Security

Reference:

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

QUESTION 18

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.

Correct Answer: A, B, C

Section:

Explanation:

A. Enroll the SRX Series device with Juniper ATP Cloud. This is essential for the SRX to receive threat intelligence from ATP Cloud, enabling it to identify infected hosts and take action.

B. Use a third-party connector. In this specific scenario, a third-party connector is required to integrate the SRX with the third-party switch. While Juniper has native integration for its EX switches, a connector is necessary to communicate with and manage the third-party switch.

C. Deploy Security Director with Policy Enforcer. Security Director orchestrates the automated response, and Policy Enforcer translates the policies into device-specific commands for the SRX and the third-party switch (via the connector).

QUESTION 19

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

Correct Answer: C
Section:

QUESTION 20
You are asked to connect two hosts that are directly connected to an SRX Series device. The traffic should flow unchanged as it passes through the SRX, and routing or switch lookups should not be performed. However, the traffic should still be subjected to security policy checks.
What will provide this functionality?

A. MACsec
B. Mixed mode
C. Secure wire
D. Transparent mode

Correct Answer: C
Section:
Explanation:
Secure wire mode on SRX devices allows traffic to flow transparently through the firewall without being routed or switched, while still applying security policies. This is ideal for scenarios where traffic inspection is required without altering the traffic path or performing additional routing decisions. For further details on Secure Wire, refer to Juniper Secure Wire Documentation.
In this scenario, you want traffic to pass through the SRX unchanged (without routing or switching lookups) but still be subject to security policy checks. The best solution for this requirement is Secure Wire.
Explanation of Answer C (Secure Wire):
Secure Wire allows traffic to flow through the SRX without any Layer 3 routing or Layer 2 switching decisions. It effectively bridges two interfaces at Layer 2 while still applying security policies. This ensures that traffic remains unchanged, while security policies (such as firewall rules) can still be enforced.
This is an ideal solution when you need the SRX to act as a 'bump in the wire' for security enforcement without changing the traffic or performing complex network lookups.
Juniper Security
Reference:
Secure Wire Functionality: Provides transparent Layer 2 forwarding with security policy enforcement, making it perfect for scenarios where traffic needs to pass through unchanged. Reference: Juniper Secure Wire Documentation.

QUESTION 21
Which two statements are true when setting up an SRX Series device to operate in mixed mode? (Choose two.)

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

Correct Answer: C, D
Section:
Explanation:
In mixed mode, SRX devices can simultaneously handle Layer 2 switching and Layer 3 routing, but a reboot is required when configuring Layer 2 and Layer 3 interfaces to ensure the configuration takes effect. Layer 2 packets

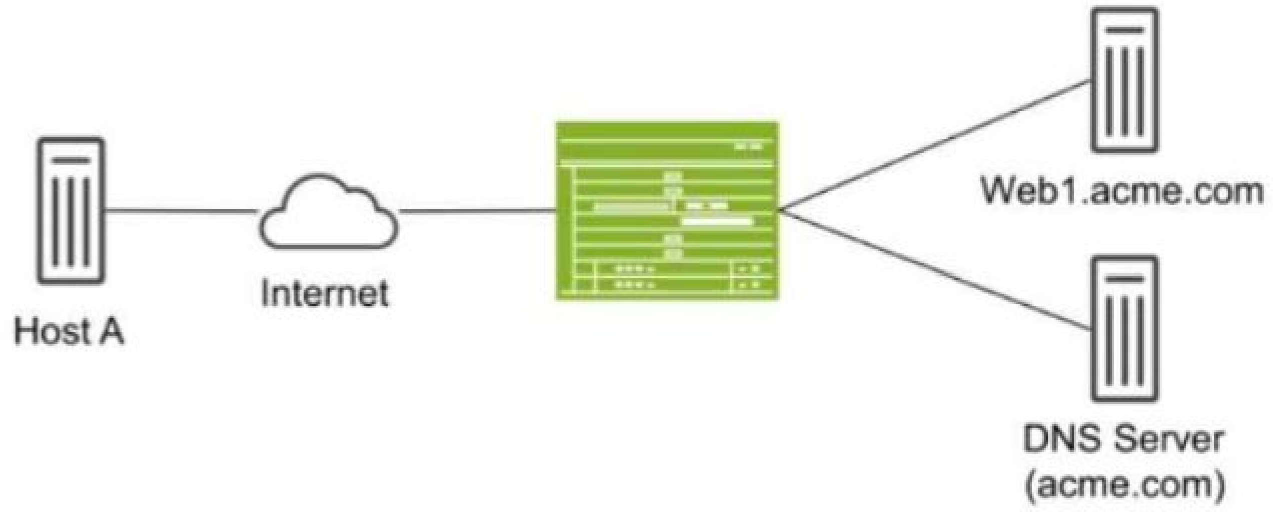
are switched within the defined bridge domain. Further guidance on SRX mixed mode can be found at Juniper Mixed Mode Documentation.
When an SRX Series device is configured in mixed mode, both Layer 2 switching and Layer 3 routing functionalities can be used on the same device. This enables the SRX to act as both a router and a switch for different interfaces. However, there are certain considerations:
Explanation of Answer C (Reboot Requirement):
After configuring the SRX to operate with at least one Layer 2 interface and one Layer 3 interface, the device needs to be rebooted. This is required to properly initialize the mixed mode configuration, as the SRX needs to switch between Layer 2 and Layer 3 processing modes.
Explanation of Answer D (Layer 2 Traffic Handling):
In mixed mode, traffic from Layer 2 interfaces is switched within the same bridge domain. A bridge domain defines a Layer 2 broadcast domain, and packets from Layer 2 interfaces are forwarded based on MAC addresses within that domain.
Juniper Security
Reference:
Mixed Mode Overview: Juniper SRX devices can operate in mixed mode to handle both Layer 2 and Layer 3 traffic simultaneously. Reference: Juniper Mixed Mode Documentation.

QUESTION 22
You have configured the backup signal route IP for your multinode HA deployment, and the ICL link fails.
Which two statements are correct in this scenario? (Choose two.)

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

Correct Answer: A, C
Section:

QUESTION 23
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?

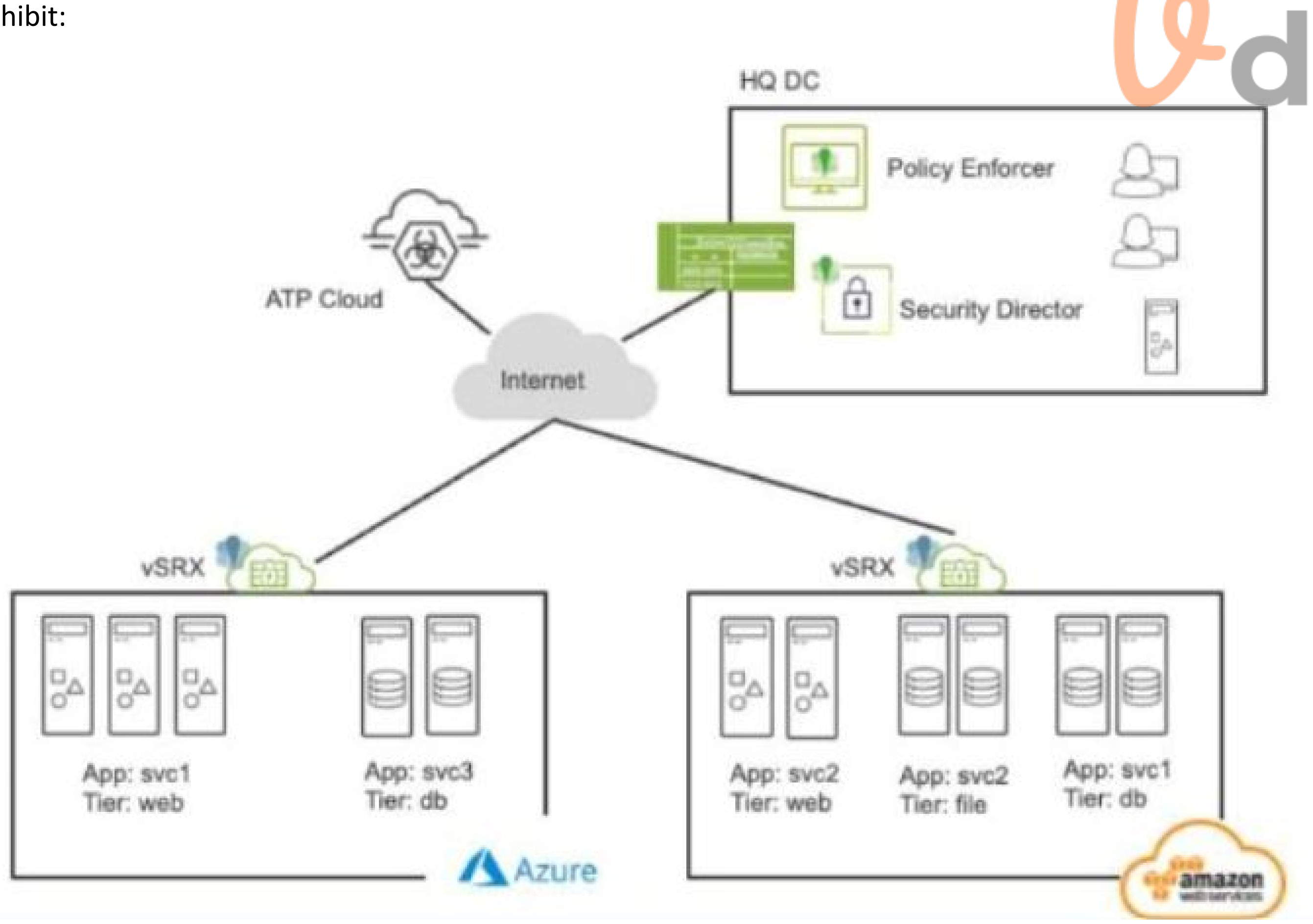
A. Persistent NAT
B. Double NAT
C. DNS doctoring
D. STUN protocol

Correct Answer: C
Section:
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):
DNS doctoring is a feature that modifies DNS replies as they pass through the SRX device. In this case, DNS doctoring can be used to replace the private IP address returned in the DNS response with the correct public IP address for Host A. This allows external clients to reach internal resources without being aware of their private IP addresses.
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.

QUESTION 24
Exhibit:

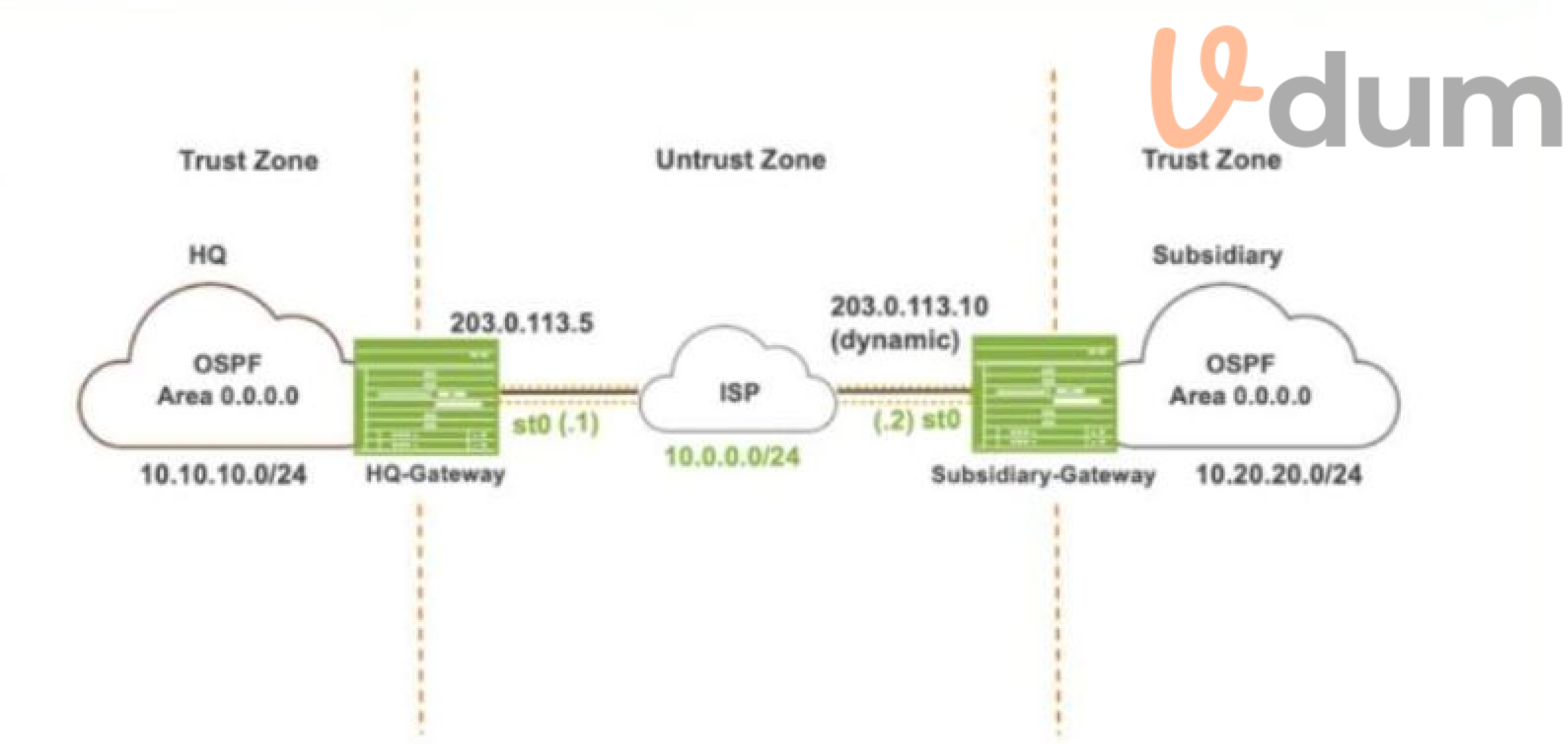


Referring to the exhibit, what do you use to dynamically secure traffic between the Azure and AWS clouds?

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.

Correct Answer: C
Section:
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):
Security tags allow dynamic enforcement of security policies based on metadata rather than static IP addresses or zones. This is crucial in cloud environments, where resources and IP addresses can change dynamically.
Using security tags in the security policies, you can associate traffic flows with specific applications, services, or virtual machines, regardless of their underlying IP addresses or network locations. This ensures that security policies are automatically updated as cloud resources change.
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.

QUESTION 25
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

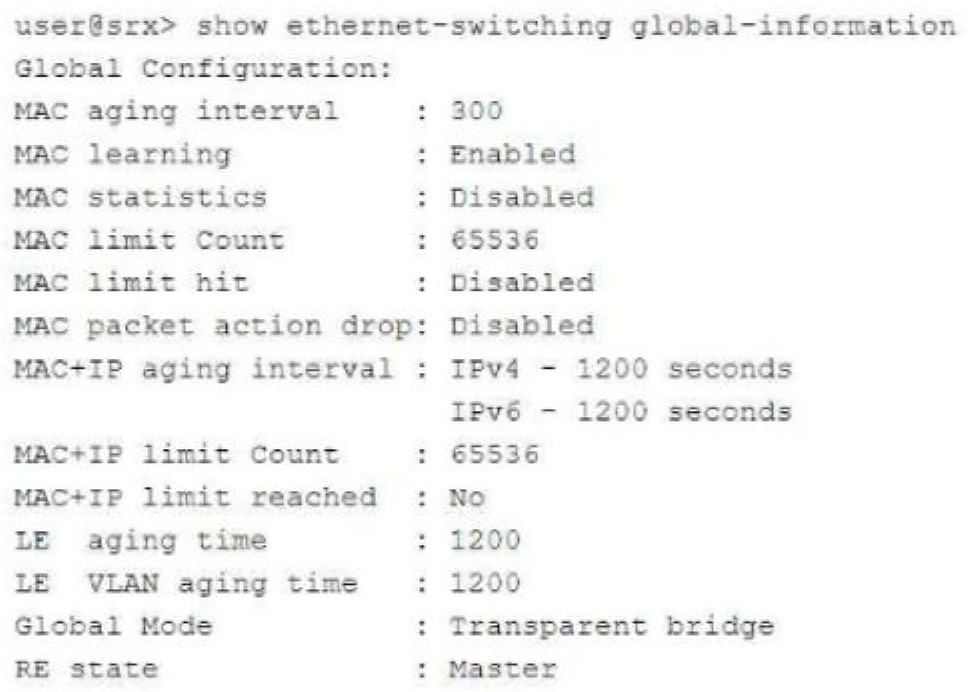
Correct Answer: B
Section:

QUESTION 26
You are deploying threat remediation to endpoints connected through third-party devices.
In this scenario, which three statements are correct? (Choose three.)

A. All third-party switches must support AAA/RADIUS and Dynamic Authorization Extensions to the RADIUS protocol.
B. The connector uses an API to gather endpoint MAC address information from the RADIUS server.
C. All third-party switches in the specified network are automatically mapped and registered with the RADIUS server.
D. The connector queries the RADIUS server for the infected host endpoint details and initiates a change of authorization (CoA) for the infected host.
E. The RADIUS server sends Status-Server messages to update infected host information to the connector.

Correct Answer: A, B, D
Section:
Explanation:
For threat remediation in a third-party network, the RADIUS protocol is necessary to communicate with the RADIUS server for details about infected hosts. CoA enables security measures to be enforced based on endpoint information provided by the RADIUS server. Details on this setup can be found in Juniper RADIUS and AAA Documentation.
When deploying threat remediation to endpoints connected through third-party devices, such as switches, the following conditions must be met for proper integration and functioning:
Explanation of Answer A (Support for AAA/RADIUS and Dynamic Authorization Extensions):
Third-party switches must support AAA (Authentication, Authorization, and Accounting) and RADIUS with Dynamic Authorization Extensions. These extensions allow dynamic updates to be made to a session's authorization parameters, which are essential for enforcing access control based on threat detection.
Explanation of Answer B (Connector Gathers MAC Information via API):
The connector uses an API to gather MAC address information from the RADIUS server. This MAC address data is necessary to identify and take action on infected hosts or endpoints.
Explanation of Answer D (Connector Initiates CoA):
The connector queries the RADIUS server for infected host details and triggers a Change of Authorization (CoA) for the infected host. The CoA allows the connector to dynamically alter the host's access permissions or isolate the infected host based on its threat status.
Juniper Security
Reference:
Threat Remediation via RADIUS: Dynamic remediation actions, such as CoA, can be taken based on information received from the RADIUS server regarding infected hosts. Reference: Juniper RADIUS and CoA Documentation.

QUESTION 27
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.

Correct Answer: B, C
Section:
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):
The SRX device can secure inter-VLAN traffic because it supports security policies for Layer 3 traffic between different VLANs. In this case, traffic moving between different VLANs (i.e., Layer 3 traffic) can be processed and controlled using security policies.
Explanation of Answer C (Pass Layer 2 and Layer 3 Traffic Simultaneously):
The SRX device can handle both Layer 2 and Layer 3 traffic simultaneously. In mixed mode, the device is capable of switching traffic at Layer 2 (intra-VLAN) while also routing traffic at Layer 3 (inter-VLAN). This is evident from the global configuration showing transparent bridge mode and Layer 3 interfaces.
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.

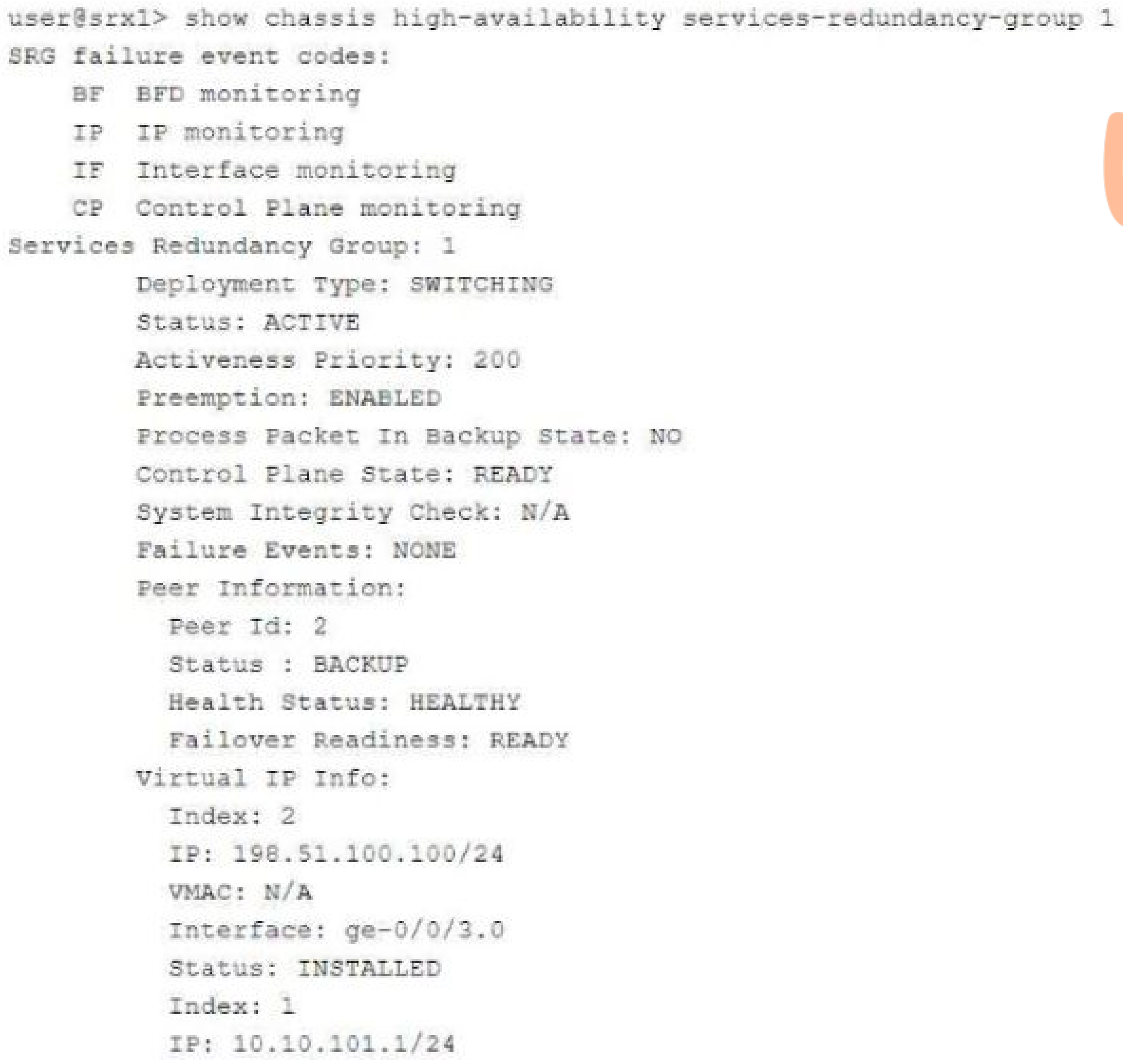
QUESTION 28
You want to test how the device handles a theoretical session without generating traffic on the Junos security device.
Which command is used in this scenario?

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

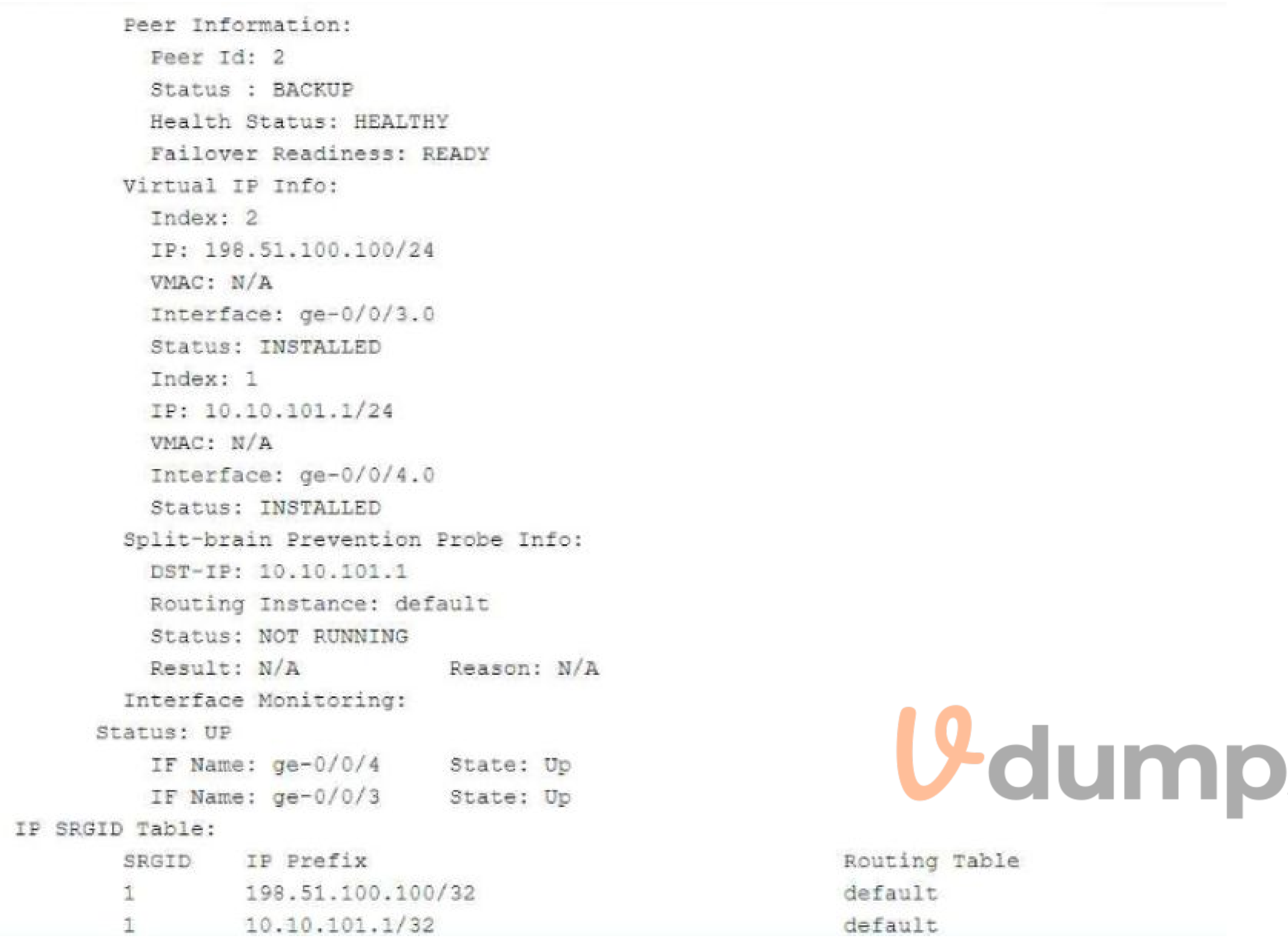
D. show security policies

Correct Answer: A
Section:
Explanation:
The request security policies check command allows you to simulate a session through the SRX device, checking the security policy action that would apply without needing to send real traffic. This helps in validating configurations before actual deployment. For more details, see Juniper Security Policies Testing.
The command request security policies check is used to test how a Junos security device handles a theoretical session without generating actual traffic. This command is useful for validating how security policies would be applied to a session based on various parameters like source and destination addresses, application type, and more.
Explanation of Answer A (request security policies check):
This command allows you to simulate a session and verify which security policies would be applied to the session. It's a proactive method to test security policy configurations without the need to generate real traffic.
Example usage:
bash
request security policies check from-zone trust to-zone untrust source 10.1.1.1 destination 192.168.1.1 protocol tcp application junos-https
Juniper Security
Reference:
Security Policies Check: This command provides a way to simulate and verify security policy behavior without actual traffic. Reference: Juniper Security Policy Documentation.

QUESTION 29
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.

Correct Answer: A, B
Section:
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):
The exhibit indicates that this SRX device is in the backup role for SRG1. The status: BACKUP field confirms that this device is currently in a standby role and is not the active node for the services redundancy group.
Explanation of Answer A (Interfaces Not Active):
Since the device is in the backup role, the interfaces ge-0/0/3.0 and ge-0/0/4.0 will not respond to ARP requests for the virtual IP's MAC address. Only the active node's interfaces respond to ARP requests in a chassis cluster configuration.

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.

QUESTION 30
Which role does an SRX Series device play in a DS-Lite deployment?

A. Softwire concentrator
B. STUN server
C. STUN client
D. Softwire initiator

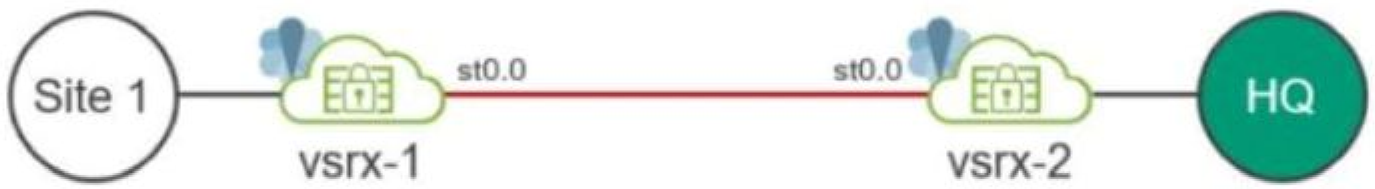
Correct Answer: A
Section:

QUESTION 31
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 HA peers.
C. The ICL traffic can be encrypted.
D. The ICL is the local device management interface in a multinode HA environment.

Correct Answer: B, C
Section:

QUESTION 32
Exhibit:

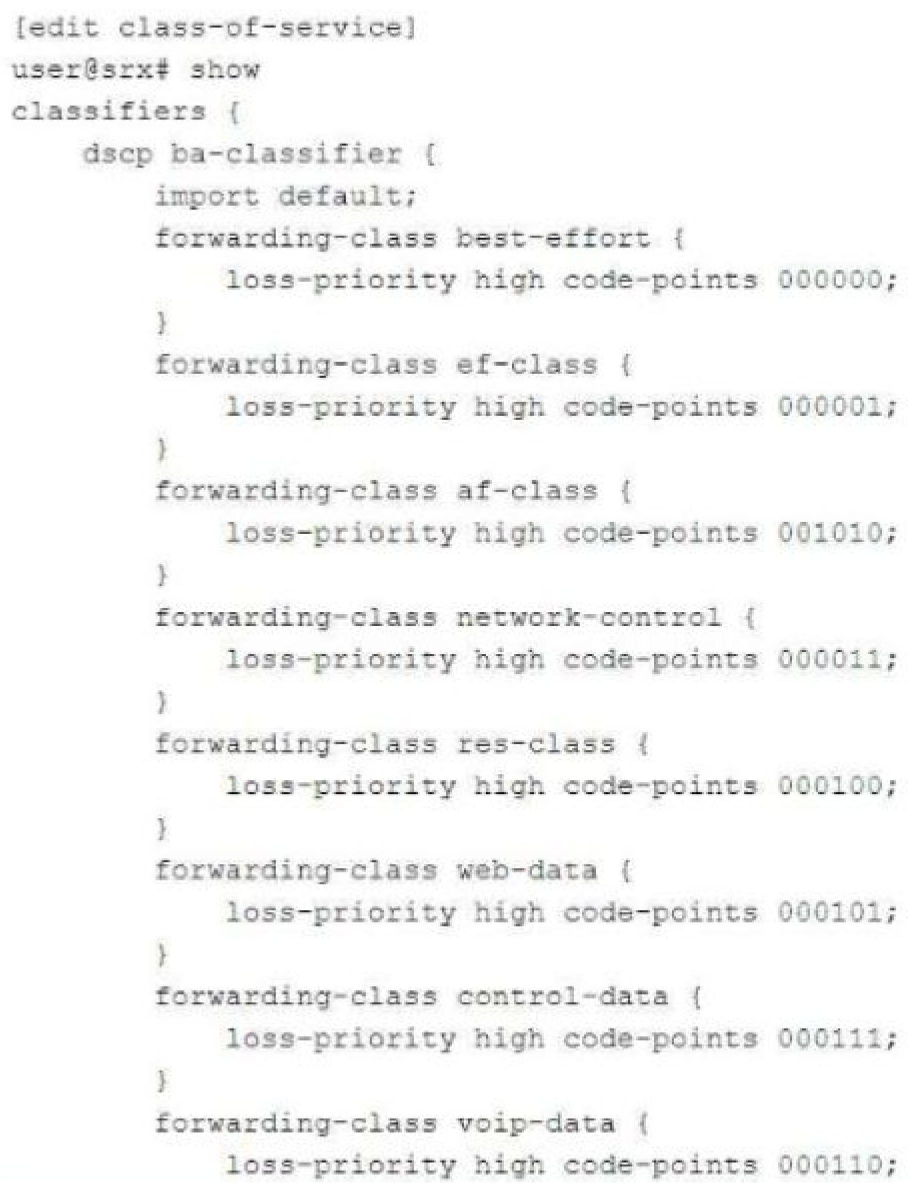


Your company uses SRX Series devices to establish an IPsec VPN that connects Site-1 and the HQ networks. You want VoIP traffic to receive priority over data traffic when it is forwarded across the VPN.
Which three actions should you perform in this scenario? (Choose three.)

A. Enable next-hop tunnel binding.
B. Create a firewall filter that identifies VoIP traffic and associates it with the correct forwarding class.
C. Configure CoS forwarding classes and scheduling parameters.
D. Enable the copy-outer-dscp parameter so that DSCP header values are copied to the tunneled packets.
E. Enable the multi-sa parameter to enable two separate IPsec SAs for the VoIP and data traffic.

Correct Answer: B, C, E
Section:

QUESTION 33
Exhibit:



```
[edit class-of-service]
user@srx# show
classifiers {
    dscp ba-classifier {
        import default;
        forwarding-class best-effort {
            loss-priority high code-points 000000;
        }
        forwarding-class ef-class {
            loss-priority high code-points 000001;
        }
        forwarding-class af-class {
            loss-priority high code-points 001010;
        }
        forwarding-class network-control {
            loss-priority high code-points 000011;
        }
        forwarding-class res-class {
            loss-priority high code-points 000100;
        }
        forwarding-class web-data {
            loss-priority high code-points 000101;
        }
        forwarding-class control-data {
            loss-priority high code-points 000111;
        }
        forwarding-class voip-data {
            loss-priority high code-points 000110;
```

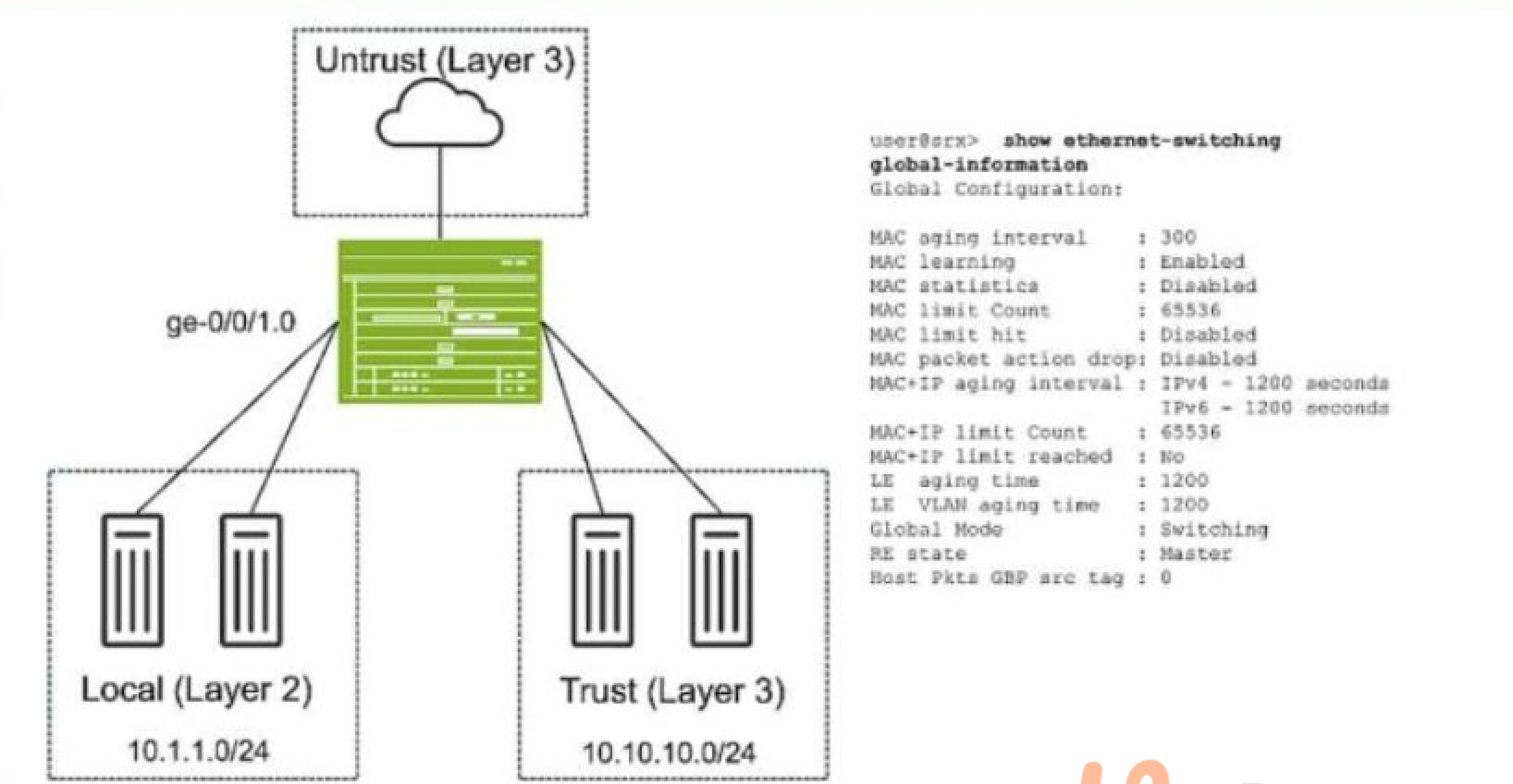
You have configured a CoS-based VPN that is not functioning correctly.
Referring to the exhibit, which action will solve the problem?

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

Correct Answer: A
Section:
Explanation:
In the exhibit, the CoS-based VPN configuration is not functioning correctly due to an issue with the number of forwarding classes. The maximum number of forwarding classes supported for CoS-based VPNs with multiple SAs (security associations) is typically four forwarding classes. In this case, more than four forwarding classes are defined.
To solve the issue, one forwarding class must be deleted to ensure that the total number of forwarding classes is reduced to four or fewer.

QUESTION 34

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            : Switching
RE state               : Master
Host Pkts GBP src tag : 0
```

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

A. Hosts in the Local zone can be enabled for control plane access to the SRX.

B. An IRB interface is required to enable communication between the Trust and the Untrust zones.

C. You can configure security policies for traffic flows between hosts in the Local zone.

D. Hosts in the Local zone can communicate with hosts in the Trust zone with a security policy.

Correct Answer: A, D

Section:

QUESTION 35

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.

Correct Answer: A, C

Section:

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.

QUESTION 36
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.

Correct Answer: B, D
Section:
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.

QUESTION 37
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.

Correct Answer: C, D
Section:
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.

QUESTION 38
You are deploying a large-scale VPN spanning six sites. You need to choose a VPN technology that satisfies the following requirements:
All sites must have secure reachability to all other sites.
New spoke sites can be added without explicit configuration on the hub site.

All spoke-to-spoke communication must traverse the hub site.
Which VPN technology will satisfy these requirements?

A. ADVPN
B. Group VPN
C. Secure Connect VPN
D. AutoVPN

Correct Answer: D
Section:
Explanation:
AutoVPN simplifies deployment by dynamically establishing tunnels from spokes to the hub. This architecture supports easy scaling with minimal configuration changes, ensuring spoke-to-spoke traffic flows through the hub.
For more information, see Juniper AutoVPN Overview.
In this scenario, you need a VPN solution that ensures secure, dynamic connectivity between multiple sites, with the following conditions:
All sites must have secure reachability.
New spoke sites can be added without explicit configuration on the hub site.
Spoke-to-spoke communication must traverse the hub.
The correct technology to meet these requirements is AutoVPN. It simplifies VPN configurations by automating the setup between hub and spoke sites. Additionally, AutoVPN automatically establishes secure tunnels for new spoke sites without requiring manual configuration at the hub, and all spoke-to-spoke traffic is routed through the hub.

QUESTION 39
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

Correct Answer: C
Section:
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.

QUESTION 40
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.

Correct Answer: A, C
Section:

QUESTION 41
You have deployed two SRX Series devices in an active/passive multimode HA scenario.
In this scenario, which two statements are correct? (Choose two.)

A. Services redundancy group 1 (SRG1) is used for services that do not have a control plane state.
B. Services redundancy group 0 (SRG0) is used for services that have a control plane state.
C. Services redundancy group 0 (SRG0) is used for services that do not have a control plane state.
D. Services redundancy group 1 (SRG1) is used for services that have a control plane state.

Correct Answer: C, D
Section:

QUESTION 42
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.

Correct Answer: B, C
Section:

QUESTION 43
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.

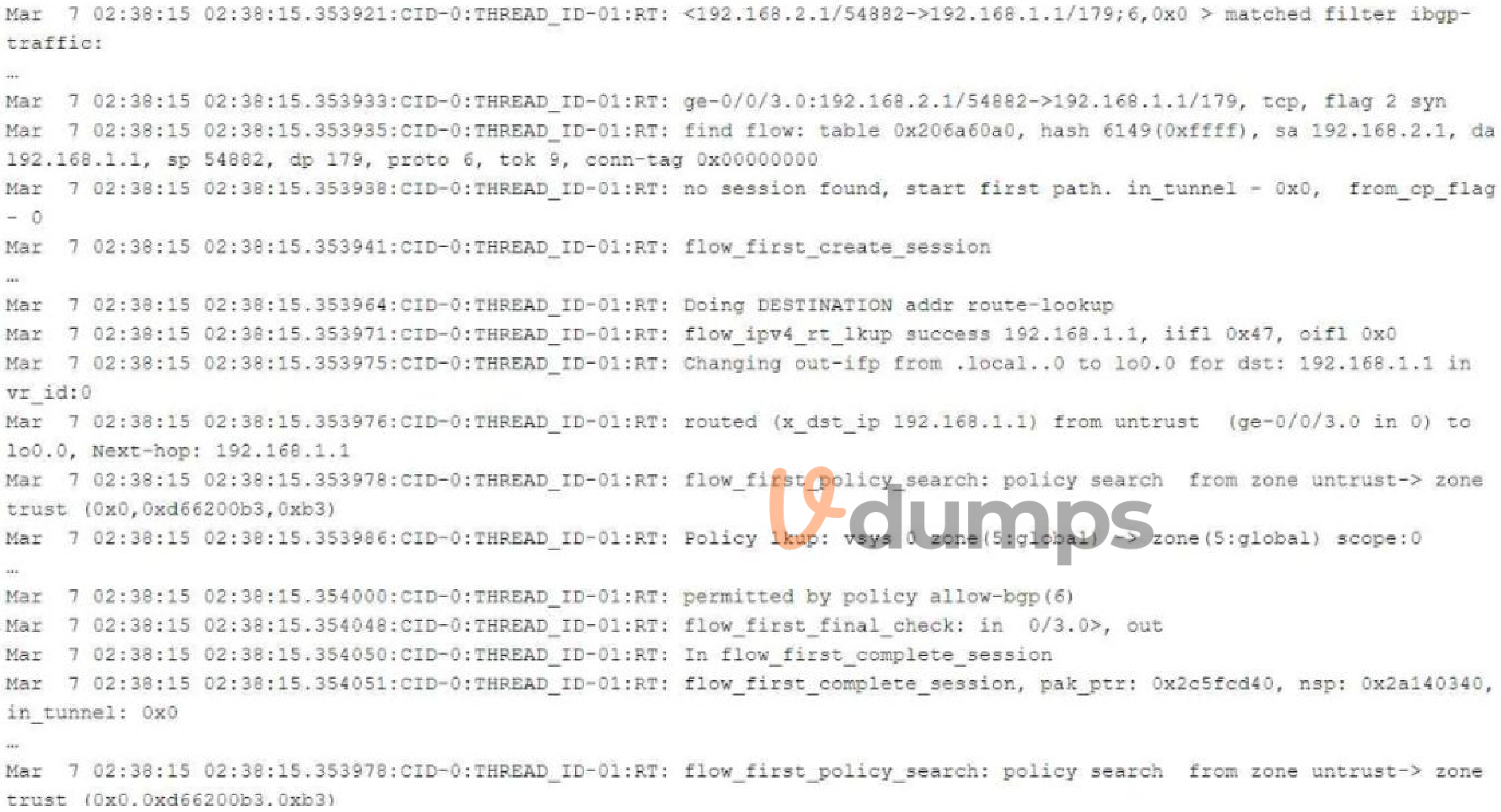
Correct Answer: D
Section:

QUESTION 44
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?

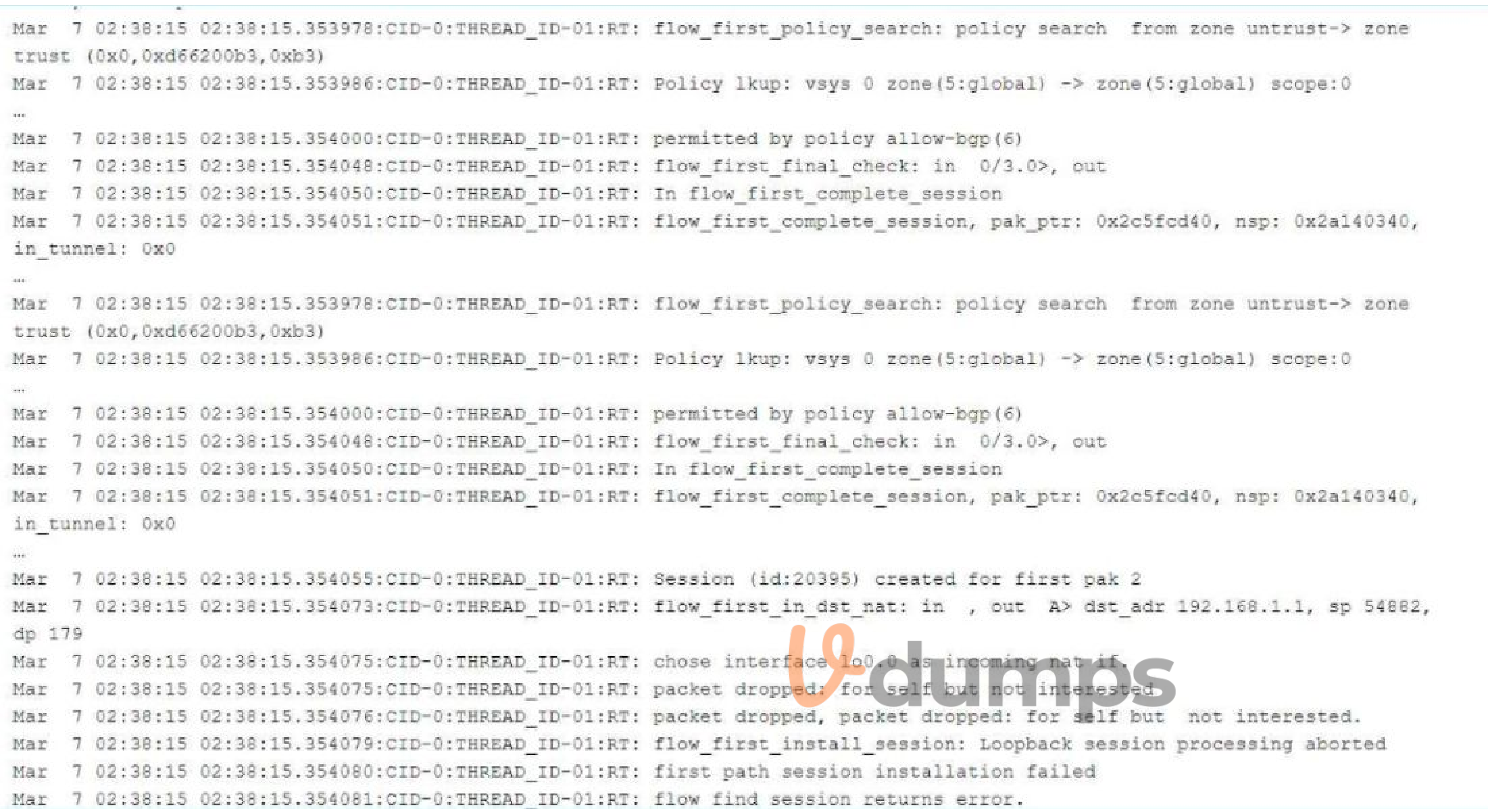
A. Security Director
B. Network Director
C. Mist
D. Security Director Insights

Correct Answer: C
Section:

QUESTION 45
You are asked to establish IBGP between two nodes, but the session is not established. To troubleshoot this problem, you configured trace options to monitor BGP protocol message exchanges.



```
Mar  7 02:38:15 02:38:15.353921:CID-0:THREAD_ID-01:RT: <192.168.2.1/54882->192.168.1.1/179;6,0x0 > matched filter ibgp-
traffic:
…
Mar  7 02:38:15 02:38:15.353933:CID-0:THREAD_ID-01:RT: ge-0/0/3.0:192.168.2.1/54882->192.168.1.1/179, tcp, flag 2 syn
Mar  7 02:38:15 02:38:15.353935:CID-0:THREAD_ID-01:RT: find flow: table 0x206a60a0, hash 6149(0xffff), sa 192.168.2.1, da
192.168.1.1, sp 54882, dp 179, proto 6, tok 9, conn-tag 0x00000000
Mar  7 02:38:15 02:38:15.353938:CID-0:THREAD_ID-01:RT: no session found, start first path. in_tunnel - 0x0,  from_cp_flag
- 0
Mar  7 02:38:15 02:38:15.353941:CID-0:THREAD_ID-01:RT: flow_first_create_session
…
Mar  7 02:38:15 02:38:15.353964:CID-0:THREAD_ID-01:RT: Doing DESTINATION addr route-lookup
Mar  7 02:38:15 02:38:15.353971:CID-0:THREAD_ID-01:RT: flow_ipv4_rt_lkup success 192.168.1.1, iifl 0x47, oifl 0x0
Mar  7 02:38:15 02:38:15.353975:CID-0:THREAD_ID-01:RT: Changing out-ifp from .local..0 to lo0.0 for dst: 192.168.1.1 in
vr_id:0
Mar  7 02:38:15 02:38:15.353976:CID-0:THREAD_ID-01:RT: routed (x_dst_ip 192.168.1.1) from untrust  (ge-0/0/3.0 in 0) to
lo0.0, Next-hop: 192.168.1.1
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0,0xd66200b3,0xb3)
Mar  7 02:38:15 02:38:15.353986:CID-0:THREAD_ID-01:RT: Policy lkup: vsys 0 zone(5:global) -> zone(5:global) scope:0
…
Mar  7 02:38:15 02:38:15.354000:CID-0:THREAD_ID-01:RT: permitted by policy allow-bgp(6)
Mar  7 02:38:15 02:38:15.354048:CID-0:THREAD_ID-01:RT: flow_first_final_check: in  0/3.0>, out
Mar  7 02:38:15 02:38:15.354050:CID-0:THREAD_ID-01:RT: In flow_first_complete_session
Mar  7 02:38:15 02:38:15.354051:CID-0:THREAD_ID-01:RT: flow_first_complete_session, pak_ptr: 0x2c5fcd40, nsp: 0x2a140340,
in_tunnel: 0x0
…
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0.0xd66200b3.0xb3)
```



```
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0,0xd66200b3,0xb3)
Mar  7 02:38:15 02:38:15.353986:CID-0:THREAD_ID-01:RT: Policy lkup: vsys 0 zone(5:global) -> zone(5:global) scope:0
…
Mar  7 02:38:15 02:38:15.354000:CID-0:THREAD_ID-01:RT: permitted by policy allow-bgp(6)
Mar  7 02:38:15 02:38:15.354048:CID-0:THREAD_ID-01:RT: flow_first_final_check: in  0/3.0>, out
Mar  7 02:38:15 02:38:15.354050:CID-0:THREAD_ID-01:RT: In flow_first_complete_session
Mar  7 02:38:15 02:38:15.354051:CID-0:THREAD_ID-01:RT: flow_first_complete_session, pak_ptr: 0x2c5fcd40, nsp: 0x2a140340,
in_tunnel: 0x0
…
Mar  7 02:38:15 02:38:15.353978:CID-0:THREAD_ID-01:RT: flow_first_policy_search: policy search  from zone untrust-> zone
trust (0x0,0xd66200b3,0xb3)
Mar  7 02:38:15 02:38:15.353986:CID-0:THREAD_ID-01:RT: Policy lkup: vsys 0 zone(5:global) -> zone(5:global) scope:0
…
Mar  7 02:38:15 02:38:15.354000:CID-0:THREAD_ID-01:RT: permitted by policy allow-bgp(6)
Mar  7 02:38:15 02:38:15.354048:CID-0:THREAD_ID-01:RT: flow_first_final_check: in  0/3.0>, out
Mar  7 02:38:15 02:38:15.354050:CID-0:THREAD_ID-01:RT: In flow_first_complete_session
Mar  7 02:38:15 02:38:15.354051:CID-0:THREAD_ID-01:RT: flow_first_complete_session, pak_ptr: 0x2c5fcd40, nsp: 0x2a140340,
in_tunnel: 0x0
…
Mar  7 02:38:15 02:38:15.354055:CID-0:THREAD_ID-01:RT: Session (id:20395) created for first pak 2
Mar  7 02:38:15 02:38:15.354073:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat: in  , out  A> dst_adr 192.168.1.1, sp 54882,
dp 179
Mar  7 02:38:15 02:38:15.354075:CID-0:THREAD_ID-01:RT: chose interface lo0.0 as incoming nat if.
Mar  7 02:38:15 02:38:15.354075:CID-0:THREAD_ID-01:RT: packet dropped: for self but not interested
Mar  7 02:38:15 02:38:15.354076:CID-0:THREAD_ID-01:RT: packet dropped, packet dropped: for self but  not interested.
Mar  7 02:38:15 02:38:15.354079:CID-0:THREAD_ID-01:RT: flow_first_install_session: Loopback session processing aborted
Mar  7 02:38:15 02:38:15.354080:CID-0:THREAD_ID-01:RT: first path session installation failed
Mar  7 02:38:15 02:38:15.354081:CID-0:THREAD_ID-01:RT: flow find session returns error.
```

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

A. Add the junos-host zone policy to permit the BGP packets.

B. Add a firewall filter to lo0 that permits the BGP packets.

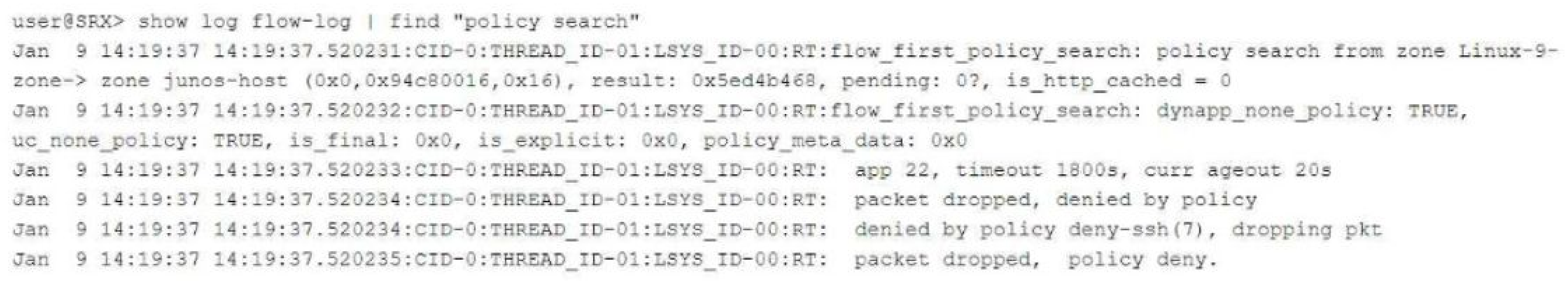
C. Modify the security policy to permit the BGP packets.

D. Add BGP to the lo0 host-inbound-traffic configuration.

Correct Answer: D
Section:

QUESTION 46

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.

Correct Answer: A, D
Section:

QUESTION 47
You have deployed automated threat mitigation using Security Director with Policy Enforcer, Juniper ATP Cloud, SRX Series devices, and EX Series switches.
In this scenario, which device is responsible for blocking the infected hosts?

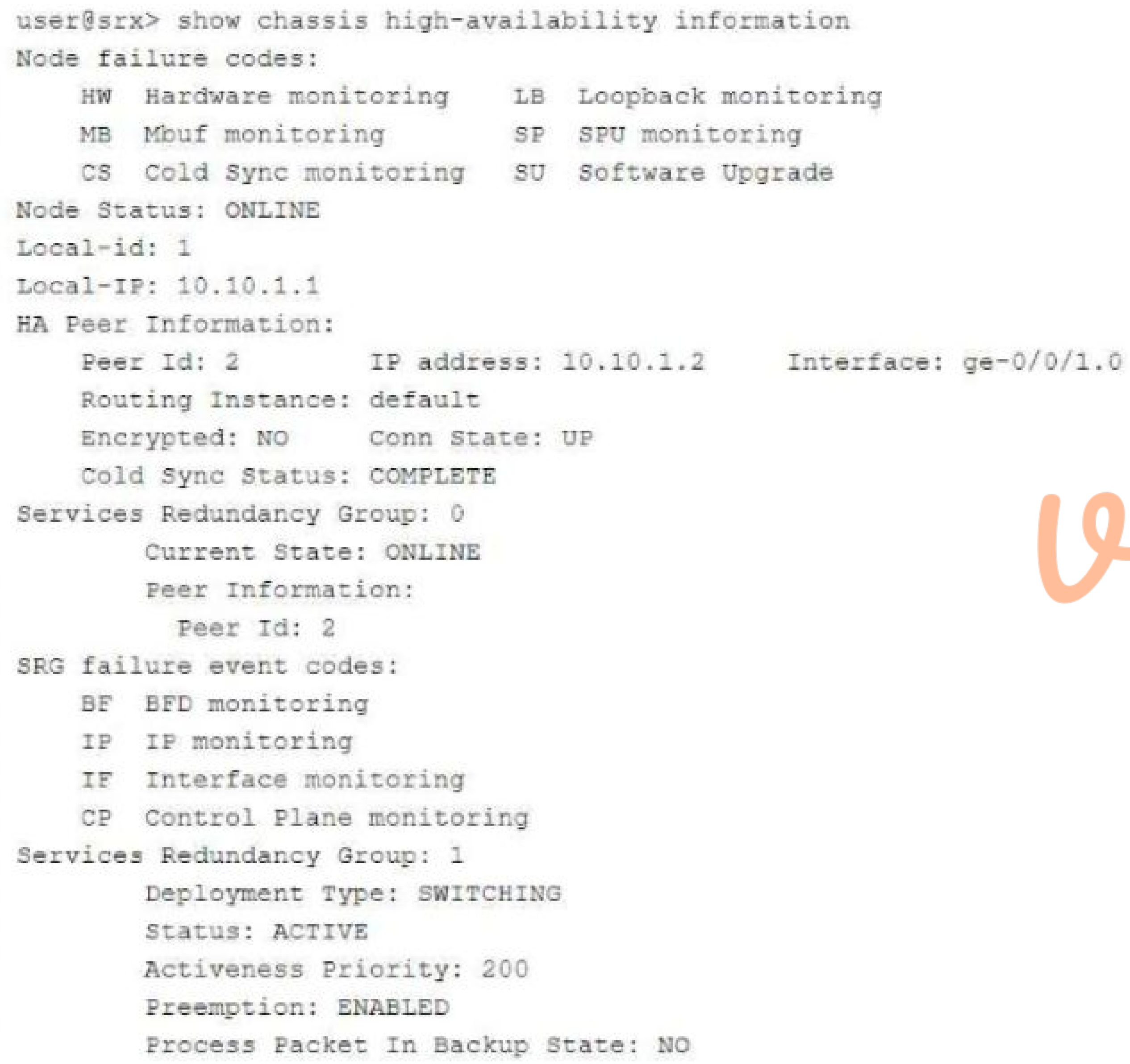
A. Policy Enforcer
B. Security Director
C. Juniper ATP Cloud
D. EX Series switch

Correct Answer: A
Section:
Explanation:
Policy Enforcer interacts with other network elements like EX switches to enforce blocking of infected hosts based on threat intelligence from ATP Cloud and other sources. For more information, refer to Juniper Policy Enforcer Documentation.
In a Juniper automated threat mitigation setup involving Security Director, Policy Enforcer, Juniper ATP Cloud, SRX Series, and EX Series switches, the Policy Enforcer is the component responsible for blocking infected hosts.
The role of each component is as follows:
Policy Enforcer (Correct: Option A):
Policy Enforcer receives threat intelligence from Juniper ATP Cloud and instructs SRX devices and EX Series switches to block or quarantine infected hosts. Policy Enforcer pushes policies to these devices to enforce the mitigation actions.
Security Director (Incorrect):
Security Director provides centralized management and visibility but does not directly enforce policies.
Juniper ATP Cloud (Incorrect):

Juniper ATP Cloud is responsible for analyzing threats and providing intelligence but does not take direct mitigation actions.
EX Series Switch (Incorrect):
EX Series switches can enforce the policy pushed by Policy Enforcer but are not responsible for deciding which hosts to block.
Juniper
Reference:
Juniper ATP Cloud and Policy Enforcer Documentation: Details the roles of each component in the automated threat mitigation architecture.

QUESTION 48

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.

Correct Answer: A, C, D

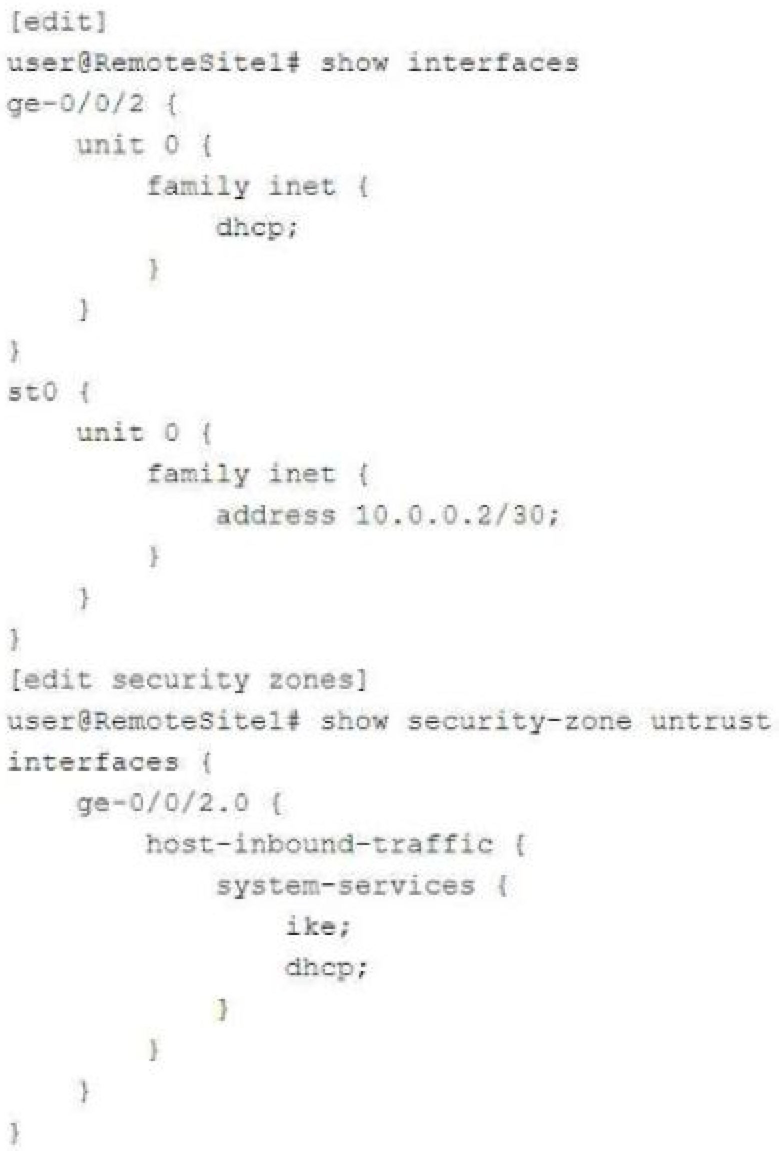
Section:
Explanation:
Referring to the exhibit for a multinode HA environment, we can conclude the following about the HA setup:
Two Services Redundancy Groups (Correct: Option A):
The output shows the status of SRG 0 and SRG 1, confirming that there are two services redundancy groups in the HA configuration.
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
Reference:
Juniper HA Documentation: Provides details on multinode HA setups, SRG configurations, and session synchronization.

QUESTION 49
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?

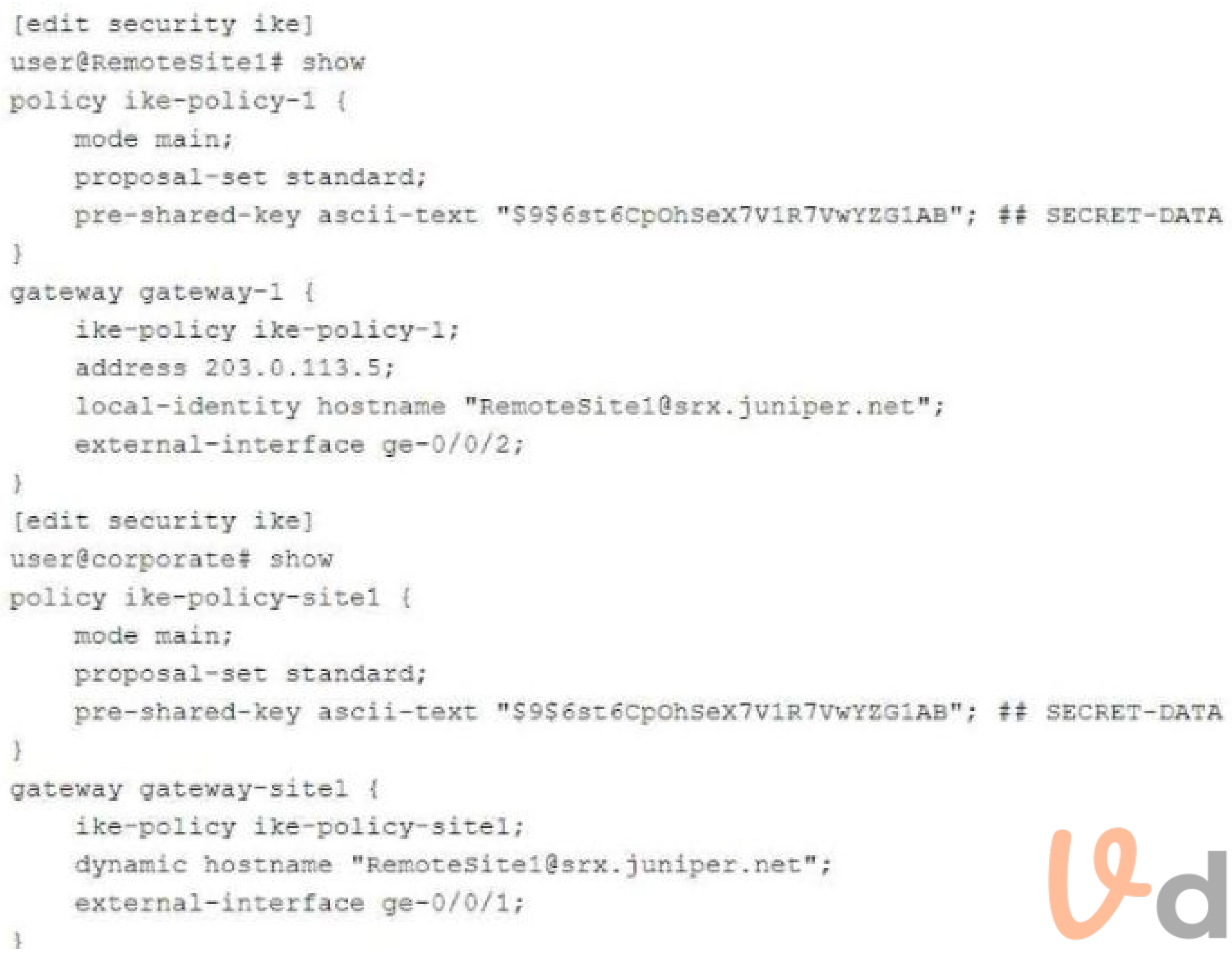
A. You must ensure that you are using aggressive mode when incorporating third-party devices as your spokes.
B. You must statically configure the next-hop tunnel binding table entries for each of the third-party spoke devices.
C. You must create a policy-based VPN on the hub device when peering with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

Correct Answer: B
Section:

QUESTION 50
Exhibit:



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



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

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

A. On the RemoteSite1 device, change the IKE gateway external interface to st0.0.

B. On both devices, change the IKE version to use version 2 only.

C. On both devices, change the IKE policy proposal set to basic.

D. On both devices, change the IKE policy mode to aggressive.

Correct Answer: D
Section:
Explanation:
Aggressive mode is required when an IP address is dynamically assigned, such as through DHCP, as it allows for faster establishment with less identity verification. More details are available in Juniper IKE and IPsec Configuration Guide.
The configuration shown in the exhibit highlights that the RemoteSite1 SRX Series device is using DHCP to obtain an IP address for its external interface (ge-0/0/2). This introduces a challenge in IPsec VPN configurations when the public IP address of the remote site is not static, as is the case here.
Aggressive mode in IKE (Internet Key Exchange) is designed for situations where one or both peers have dynamically assigned IP addresses. In this scenario, aggressive mode allows the devices to exchange identifying information, such as hostnames, rather than relying on static IP addresses, which is necessary when the remote peer (RemoteSite1) has a dynamic IP from DHCP.
Correct Action (D): Changing the IKE policy mode to aggressive will resolve the issue by allowing the two devices to establish the VPN even though one of them is using DHCP. In aggressive mode, the initiator can present its identity (hostname) during the initial handshake, enabling the VPN to be established successfully.
Incorrect Options:
Option A: Changing the external interface to st0.0 is incorrect because the st0 interface is used for the tunnel interface, not for the IKE negotiation.
Option B: Changing to IKE version 2 would not resolve the dynamic IP issue directly, and IKEv1 works in this scenario.

Option C: Changing the IKE proposal set to basic doesn't address the dynamic IP challenge in this scenario.
Juniper
Reference:
Juniper IKE and VPN Documentation: Provides details on when to use aggressive mode, especially when a dynamic IP address is involved.

QUESTION 51
You are asked to see if your persistent NAT binding table is exhausted.
Which show command would you use to accomplish this task?

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

Correct Answer: D
Section:
Explanation:
The command show security nat source persistent-nat-table all provides a comprehensive view of all entries in the persistent NAT table, enabling administrators to monitor and manage resource exhaustion. Refer to Juniper NAT Monitoring Guide for more.
In Junos OS, when persistent NAT is configured, a binding table is created to keep track of NAT sessions and ensure that specific hosts are allowed to initiate sessions back to internal hosts. To check if the persistent NAT binding table is full or exhausted, the correct command must display the entire table.
Correct Command (D):
The command show security nat source persistent-nat-table all will display the entire persistent NAT binding table. This allows you to check whether the table is exhausted or if there is space available for new persistent NAT sessions.
Incorrect Options:
Option A: The command show security nat source persistent-nat-table summary provides a summary view but does not give detailed insights into whether the table is exhausted.
Option B and Option C: These commands deal with general NAT source summaries or pools, which are not related specifically to persistent NAT bindings.
Juniper
Reference:
Juniper Persistent NAT Documentation: Describes the persistent NAT binding table and the commands used to monitor its status.

QUESTION 52
Which two statements are true regarding NAT64? (Choose two.)

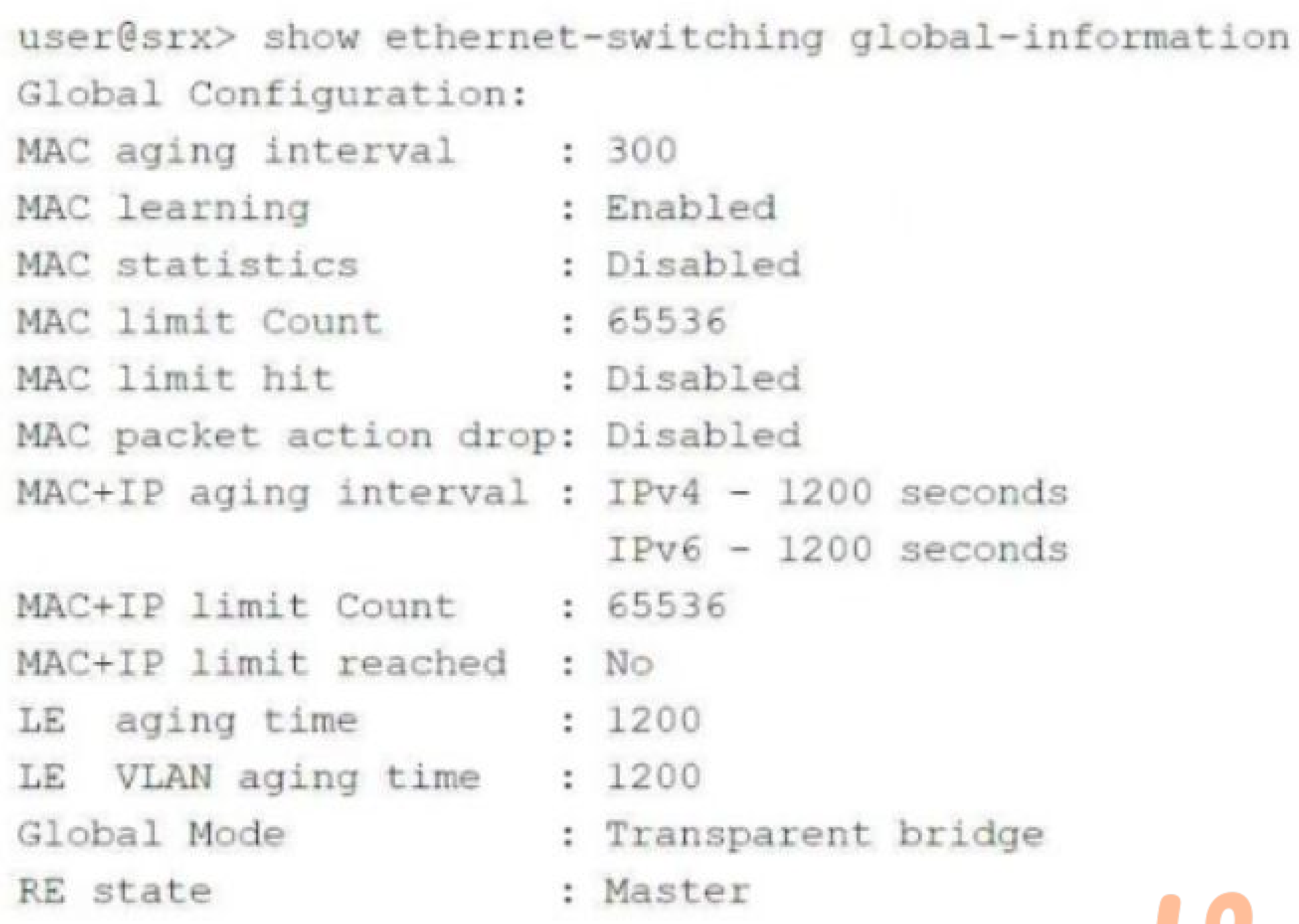
A. An SRX Series device should be in flow-based forwarding mode for IPv4.
B. An SRX Series device should be in packet-based forwarding mode for IPv4.
C. An SRX Series device should be in packet-based forwarding mode for IPv6.
D. An SRX Series device should be in flow-based forwarding mode for IPv6.

Correct Answer: A, D
Section:
Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security Reference
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:
The SRX device processes packets based on the session state.

Supports advanced services like NAT, IDP, and ALG.
Packet-Based Forwarding Mode:
The SRX device processes each packet individually without maintaining session state.
Limited support for advanced services.
Option A: An SRX Series device should be in flow-based forwarding mode for IPv4.
True.
NAT64 requires flow-based mode for IPv4 traffic to properly translate and maintain session states.
Option B: An SRX Series device should be in packet-based forwarding mode for IPv4.
False.
Packet-based mode does not support NAT features.
Option C: An SRX Series device should be in packet-based forwarding mode for IPv6.
False.
Similar to IPv4, NAT64 requires flow-based mode for IPv6 traffic.
Option D: An SRX Series device should be in flow-based forwarding mode for IPv6.
True.
Flow-based mode is necessary for NAT64 to handle IPv6 traffic correctly.
Key Points:
NAT64 Requires Flow-Based Mode:
Both IPv4 and IPv6 interfaces involved in NAT64 must be configured in flow-based mode.
This is because NAT64 relies on session information and stateful packet inspection.
Packet-Based Mode Limitations:
Does not support NAT, as it lacks session awareness.
Not suitable for NAT64 operations.
Juniper Security
Reference:
Juniper Networks Documentation:
'NAT64 is supported only in flow-based processing mode.'
Source: Configuring NAT64
Understanding Flow-Based and Packet-Based Modes:
'Flow-based mode is required for stateful services such as NAT.'
Source: Flow-Based and Packet-Based Processing
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.

QUESTION 53

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.

Correct Answer: A, D
Section:
Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security Reference
Understanding the Exhibit:
The SRX device is operating in Transparent Mode, as indicated by:
Global Mode : Transparent bridge
Transparent Mode on SRX Devices:
Transparent Mode (Layer 2 Mode):
The SRX device acts as a Layer 2 switch.
Does not perform routing functions.
Security policies can be applied to inter-VLAN (Layer 2) traffic but not intra-VLAN traffic.
Cannot handle Layer 3 traffic simultaneously.
Option A: You cannot secure intra-VLAN traffic with a security policy on this device.
True.
In Transparent Mode, intra-VLAN traffic is switched within the VLAN and does not pass through the SRX firewall processing engine.
Therefore, security policies cannot be applied to intra-VLAN traffic.

Option B: You can secure inter-VLAN traffic with a security policy on this device.
False.
In Transparent Mode, all interfaces are in the same VLAN (unless VLAN tagging is configured).
Inter-VLAN routing is not possible as the device does not perform Layer 3 functions.
Option C: The device can pass Layer 2 and Layer 3 traffic at the same time.
False.
In Transparent Mode, the SRX device operates exclusively at Layer 2.
It cannot process Layer 3 traffic simultaneously.
Option D: The device cannot pass Layer 2 and Layer 3 traffic at the same time.
True.
The SRX device in Transparent Mode cannot handle both Layer 2 and Layer 3 traffic concurrently.
Key Points:
Intra-VLAN Traffic:
Traffic within the same VLAN.
In Transparent Mode, this traffic is switched and does not go through the firewall's security policies.
Inter-VLAN Traffic:
Traffic between different VLANs.
Requires routing capabilities (Layer 3).
In Transparent Mode, the SRX cannot perform routing functions.
Juniper Security
Reference:
Juniper Networks Documentation:
'In transparent mode, the SRX Series device acts like a Layer 2 switch or bridge. Security policies cannot control intra-VLAN traffic because such traffic does not pass through the firewall.'
Source: Understanding Transparent Mode
'The device cannot perform both Layer 2 switching and Layer 3 routing simultaneously in transparent mode.'
Source: Transparent Mode Limitations
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.

QUESTION 54
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.

Correct Answer: A, D
Section:

QUESTION 55
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.

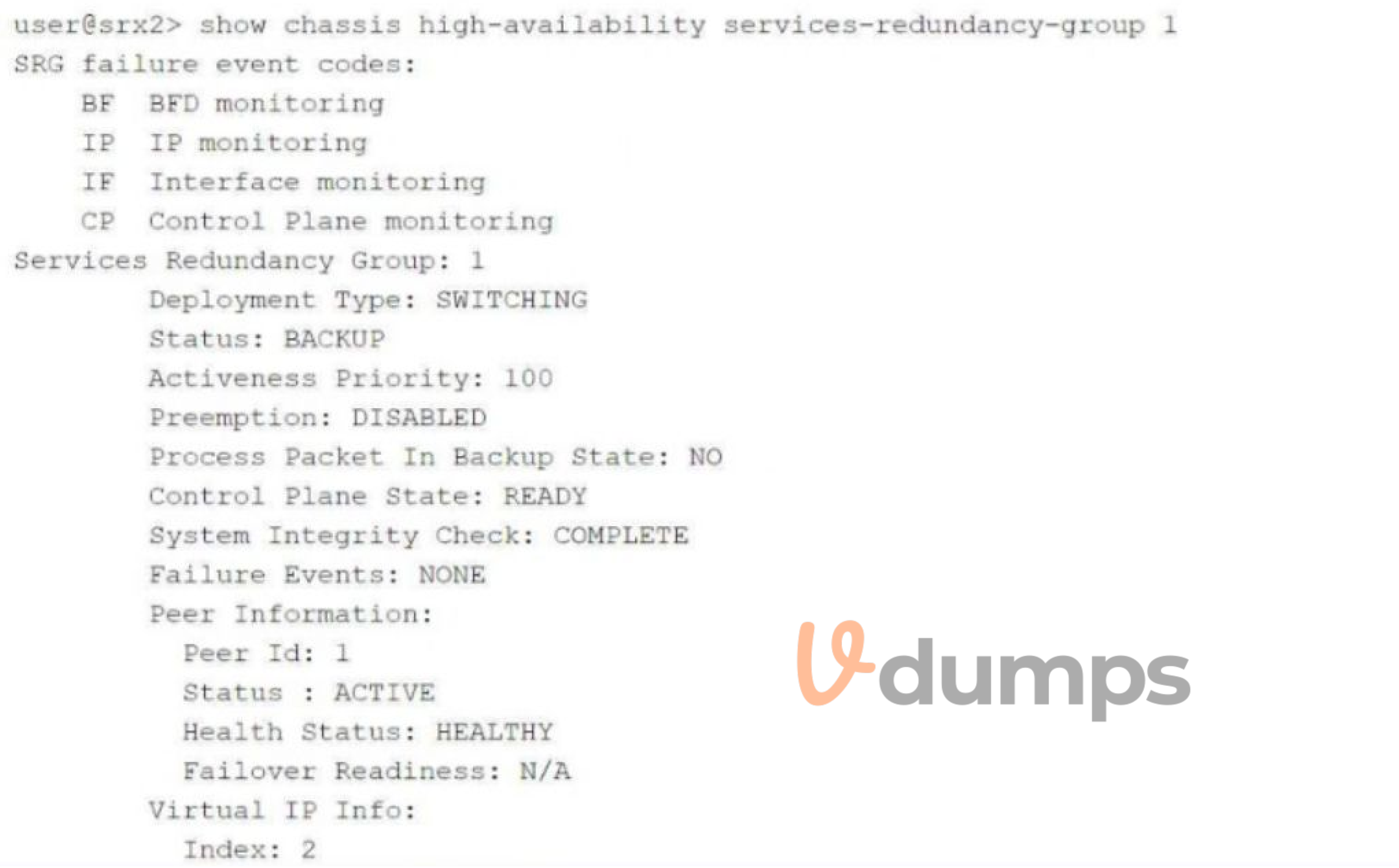
Correct Answer: A, D
Section:
Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security ReferenceUnderstanding the Scenario:Objective: Deploy OSPF over IPsec between an SRX Series device and a third-party device using GRE tunnels.Components Involved:GRE (Generic Routing Encapsulation): Encapsulates packets to allow routing protocols like OSPF to run over IPsec tunnels.IPsec: Provides security for the GRE tunnels.OSPF: Dynamic routing protocol used over the GRE tunnel.Option A: The GRE interface should use lo0 as endpoints.Using the loopback interface (lo0) as the source and destination endpoints for GRE tunnels is a common best practice.Advantages:Stability: Loopback interfaces are always up, ensuring the GRE tunnel remains operational even if physical interfaces fail.Reachability: Provides consistent endpoint IP addresses for GRE tunnels.Configuration:Assign IP addresses to lo0 interfaces on both devices.Configure GRE tunnels to use these lo0 IP addresses as source and destination.Juniper Networks Documentation:'Using loopback interfaces as GRE tunnel endpoints ensures stability and consistent reachability for routing protocols over GRE tunnels.'Source: Configuring GRE TunnelsOption D: The GRE interface must be configured under the OSPF protocol.To run OSPF over the GRE tunnel, the GRE interface must be included in the OSPF configuration.Configuration Steps:Create GRE Interface:Example: set interfaces gr-0/0/0 unit 0 tunnel source <source-ip> tunnel destination <destination-ip>Assign IP Address to GRE Interface:Example: set interfaces gr-0/0/0 unit 0 family inet address <ip-address>Include GRE Interface in OSPF:Example: set protocols ospf area interface gr-0/0/0.0Result:OSPF will establish adjacencies over the GRE interface and exchange routing information.Juniper Networks Documentation:'To enable OSPF over GRE tunnels, you must include the GRE interfaces in the OSPF configuration.'Source: OSPF over GRE ConfigurationWhy Options B and C are Incorrect:Option B: The OSPF protocol must be enabled under the VPN zone.Since OSPF is running over the GRE tunnel, which is encapsulated over IPsec, the OSPF packets are encapsulated within GRE and IPsec.The SRX device does not need to allow OSPF in the security policies or enable OSPF under the VPN zone for GRE-encapsulated traffic.Security Policies:The GRE traffic (IP protocol 47) must be permitted through the security policies.OSPF runs inside the GRE tunnel and does not require additional configuration under the VPN zone.Juniper Networks Documentation:'When using GRE over IPsec, routing protocols run over GRE and do not require separate security policies for their control traffic.'Source: Security Policies for GRE over IPsecOption C: Overlapping addresses are allowed between remote networks.Overlapping IP addresses can cause routing conflicts and are generally not recommended.In a GRE over IPsec scenario, overlapping addresses can lead to issues in routing protocol adjacency and data forwarding.Best Practice:Ensure unique IP addressing schemes between remote networks to prevent routing issues.Juniper Networks Documentation:'Overlapping IP address spaces can lead to routing ambiguities and should be avoided when configuring GRE tunnels.'Source: Avoiding Overlapping IP AddressesConclusion:Answer::s: A and DRationale:Option A is correct because using lo0 as endpoints for GRE provides stability and reliability.Option D is correct because the GRE interface must be included in the OSPF configuration to enable OSPF over the tunnel.

QUESTION 56
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

Correct Answer: A
Section:
Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security ReferenceUnderstanding 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:Used for features like filter-based forwarding (FBF) and APBR.Provides a separate forwarding table but shares the global routing table.Supports APBR.Virtual Router:Provides a separate routing table and forwarding table.Used for logical separation of routing domains.Does not support APBR directly.Virtual Switch:Operates at Layer 2.Used for VLAN separation and Layer 2 switching.Not applicable to routing or APBR.Non-Forwarding Instance:Used for management purposes.Does not forward transit traffic.Not suitable for APBR.Option A: forwardingCorrect.A forwarding routing instance is specifically designed to support advanced policy-based routing.It allows the SRX device to direct traffic based on policies to different forwarding instances.Rationale:A forwarding routing instance is the appropriate type to support advanced policy-based routing.Juniper Networks Documentation:'To configure advanced policy-based routing, you must create a forwarding-type routing instance.'Source: Configuring Advanced Policy-Based RoutingWhy Other Options Are Incorrect:Option B: virtual switchIncorrect.Virtual switch instances are for Layer 2 switching and VLAN separation.They do not support routing or APBR.Option C: virtual routerIncorrect.Virtual router instances are used for isolating routing tables.While they support routing, they are not designed for APBR.Option D: non-forwardingIncorrect.Non-forwarding instances do not handle transit traffic.They are used for management routing tables and cannot be used for APBR.Conclusion:Answer:: A. forwarding

QUESTION 57
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.

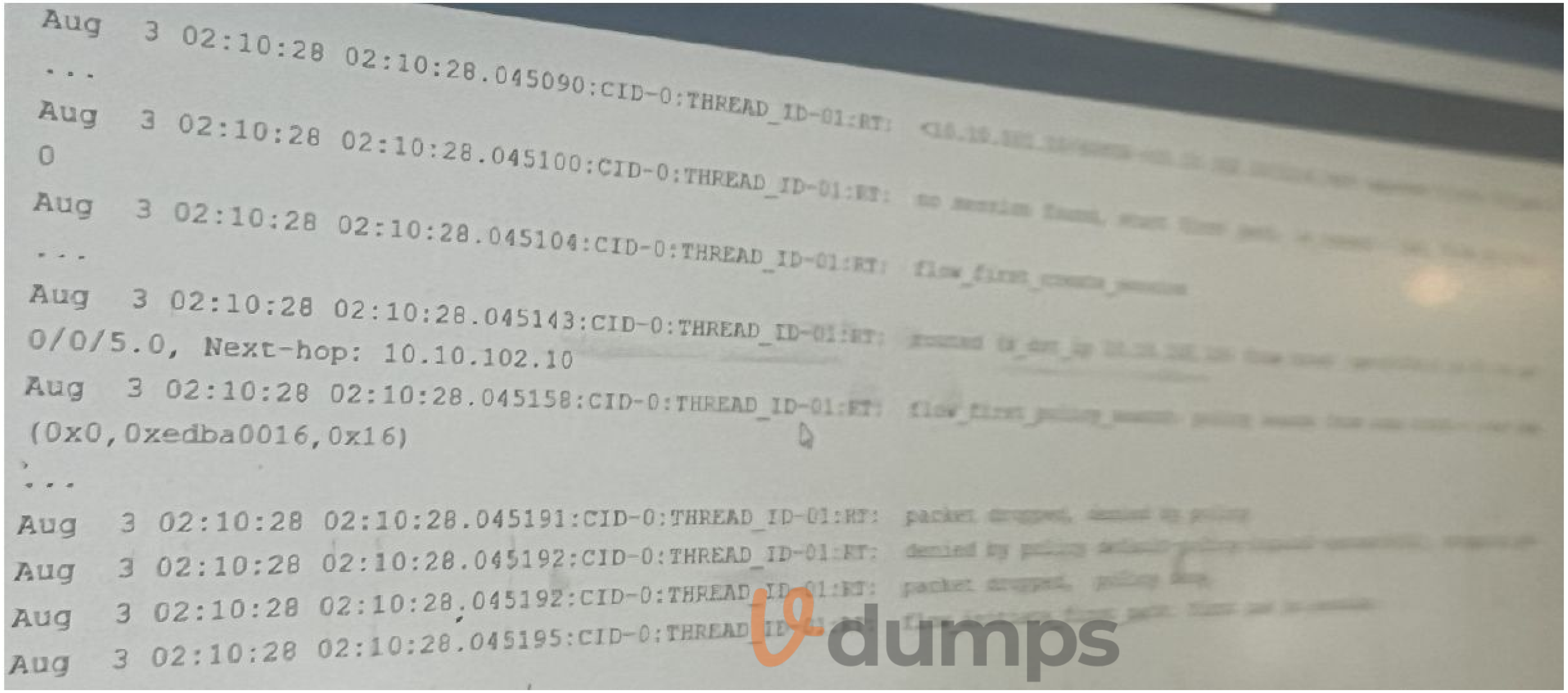
B. The ge-0/0/3.0 and ge-0/0/4.0 interfaces are not active and will not respond to ARP requests to the virtual IP MAC address.

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.

Correct Answer: C, D
Section:

QUESTION 58
Exhibit:



```
Aug  3 02:10:28 02:10:28.045090:CID-0:THREAD_ID-01:RT:  <10.10.101.10/[illegible]
...
Aug  3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT:  no session found, start first path. [illegible]
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) [illegible]
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 [illegible]
(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-[illegible]
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 [illegible] first path. [illegible]
```

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.

Correct Answer: A, C
Section:

QUESTION 59
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

E. RIB group: RIB groups are used for route management and are not directly involved in APBR rule configuration.

Correct Answer: B, C
Section:

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:

Applications: Match based on specific applications or application groups.

URL categories: Match based on URL categories provided by a web filtering service.

Other criteria: You can also match based on source/destination IP addresses, ports, protocols, etc.

C . Then action: This specifies the action to take when traffic matches the rule. The primary action in APBR is:

routing-instance: This redirects the matching traffic to a specific routing instance, allowing you to steer traffic through different paths based on the application or URL category.

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.