Juniper

Exam Questions JN0-637

Security - Professional (JNCIP-SEC)

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

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

Answer: BD

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

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

Answer: C

NEW QUESTION 3
You are using ADVPN to deploy a hub-and-spoke VPN to connect your enterprise sites. Which two statements are true in this scenario? (Choose two.)

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

Answer: CD

NEW QUESTION 4
What are three configurable monitor components for a service redundancy group? (Choose two)

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

Answer: ADE

NEW QUESTION 5
You are enabling advanced policy-based routing. You have configured a static route that
has a next hop from the inet.0 routing table. Unfortunately, this static route is not active in your routing instance.
In this scenario, which solution is needed to use this next hop?

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

Answer: A

Explanation:
To enable advanced policy-based routing in Junos OS and activate a static route with a next-hop address in the inet.0 table within your routing instance, you should utilize RIB groups. RIB groups allow you to import routes from one routing table to another. In this scenario, the static route within the routing instance needs access to the inet.0 routes, which is facilitated by configuring a RIB group. Juniper??s documentation outlines RIB groups as a necessary component for handling instances where routes need to be shared across routing tables, thereby ensuring seamless traffic flow through specified routes. For more details, refer to the Juniper Networks Documentation on RIB Groups.
In Junos OS for SRX Series devices, when enabling advanced policy-based routing and configuring a static route with a next-hop from the inet.0 routing table, the issue arises because the static route is not being used in the routing instance. This is a common scenario when the next-hop belongs to a different routing table or instance, and the routing instance is not aware of that next-hop.
To resolve this, RIB (Routing Information Base) groups are used. RIB groups allow routes from one routing table (RIB) to be shared or imported into another routing table. This means that the routing instance can import the necessary routes from inet.0 and make them available for the routing instance where the policy-based routing is applied.
Detailed Steps:
? Configure the Static Route: First, configure the static route pointing to the next-hop in inet.0. Here??s an example:
bash
set routing-options static route 10.1.1.0/24 next-hop 192.168.1.1 This static route will be placed in the inet.0 routing table by default.
? Create and Apply a RIB Group: To import routes from inet.0 into the routing
instance, create a RIB group configuration. This will allow the static route from inet.0 to be visible within the routing instance.
Example configuration for the RIB group: bash
set routing-options rib-groups RIB-GROUP import-rib inet.0
set routing-options rib-groups RIB-GROUP import-rib <routing-instance-name>.inet.0
This configuration ensures that routes from inet.0 are imported into the specified routing instance.

? Apply the RIB Group to the Routing Instance: Once the RIB group is configured,
apply it to the appropriate routing instance:
bash
set routing-instances <routing-instance-name> routing-options rib-group RIB-GROUP
? Verify Configuration: Use the following command to verify that the static route has been imported into the routing instance:
bash
show route table <routing-instance-name>.inet.0
The output should now display the static route imported from inet.0.
Juniper Security Reference:
? RIB Groups Overview: Juniper's documentation provides detailed information on how RIB groups function and how to use them to share routes between different routing tables. This is essential for scenarios involving policy-based routing where routes from one instance (like inet.0) need to be available in another instance.
Reference: Juniper Networks Documentation on RIB Groups.
By using RIB groups, you ensure that the static route from inet.0 is available in the appropriate routing instance for policy-based routing to function correctly. This avoids the need for other methods like filter-based forwarding or transparent mode, which do not address the specific issue of static route visibility across routing instances.
==========

NEW QUESTION 6
Referring to the exhibit,

which two statements about User1 are true? (Choose two.)

A. User1 has access to the configuration specific to their assigned logical system.
B. User1 is logged in to logical system LSYS-1.
C. User1 can add logical units to an interface that a primary administrator has not previously assigned.
D. User1 can view outputs from other user logical systems.

Answer: AB

Explanation:
In this configuration, User1 is logged into logical system LSYS-1, which restricts access and visibility to that particular system. This ensures isolation between logical systems on the same physical device. Only a system administrator can assign additional permissions. For more details, see Juniper Logical Systems Guide.
From the exhibit, we see that User1 is logged into logical system LSYS-1:
? Access to Assigned Logical System (Answer A): User1, being logged into the logical system LSYS-1, only has access to the configuration and interfaces within that logical system. This is a key feature of logical systems in Junos, ensuring users are restricted to their respective environments.
? Logged into LSYS-1 (Answer B): The prompt shows that User1 is currently operating in LSYS-1, as indicated by the User1@SRX:LSYS-1> command line.
: Juniper logical systems configuration and user permissions.
==========

NEW QUESTION 7
Which two elements are necessary to configure a rule under an APBR profile? (Choose Two)

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

Answer: BC

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

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

A. It works with third-party switches.
B. It provides endpoint protection by running a Juniper ATP Cloud agent on the servers.

C. It provides endpoint protection by running a Juniper ATP Cloud agent on EX Series devices.
D. It works with SRX Series devices.

Answer: AD

NEW QUESTION 9
You configured two SRX series devices in an active/passive multimode HA setup. In this scenario, which statement is correct?

A. Both devices are in the passive state until the activeness determination process is completed.
B. Both devices start in a hold state until the activeness determination process is completed.
C. Both devices start in the undiscovered state until the activeness determination process is completed.
D. Both devices are in the active state until the activeness determine determination process is completed.

Answer: D

NEW QUESTION 10
Exhibit:

```
user@srx> show ethernet-switching global-information
Global Configuration:
MAC aging interval      : 300
MAC learning            : Enabled
MAC statistics          : Disabled
MAC limit Count         : 65536
MAC limit hit           : Disabled
MAC packet action drop: Disabled
MAC+IP aging interval : IPv4 - 1200 seconds
                        IPv6 - 1200 seconds
MAC+IP limit Count      : 65536
MAC+IP limit reached    : No
LE  aging time          : 1200
LE  VLAN aging time     : 1200
Global Mode             : Transparent bridge
RE state                : Master
VXLAN Overlay load bal: Disabled
VXLAN ECMP              : Disabled
Fast Update             : Disabled
Host Pkts GBP src tag : 0
[edit interfaces]
user@srx# show
ge-0/0/0 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members v100;
            }
```

```
                                IPv6 - 1200 seconds
MAC+IP limit Count      : 65536
MAC+IP limit reached    : No
LE  aging time          : 1200
LE  VLAN aging time     : 1200
Global Mode             : Transparent bridge
RE state                : Master
VXLAN Overlay load bal: Disabled
VXLAN ECMP              : Disabled
Fast Update             : Disabled
Host Pkts GBP src tag : 0
[edit interfaces]
user@srx# show
ge-0/0/0 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members v100;
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 172.16.0.1/24;
        }
    }
}
```

In which mode is the SRX Series device?

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

Answer: C

NEW QUESTION 10
You are asked to select a product offered by Juniper Networks that can collect and assimilate data from all probes and determine the optimal links for different applications to maximize the full potential of AppQoE.
Which product provides this capability?

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

Answer: C

NEW QUESTION 11
Referring to the exhibit,

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

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

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

Answer: ACD

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

NEW QUESTION 14
You are attempting to ping the IP address that is assigned to the loopback interface on the SRX series device shown in the exhibit.

```
user@SRX> show interfaces lo0.0
  Logical interface lo0.0 (Index 86) (SNMP ifIndex 16)
    Flags: SNMP-Traps Encapsulation: Unspecified
   Input packets : 0
   Output packets: 0
  Security: Zone: Null
 Protocol inet, MTU: Unlimited
Max nh cache: 0, New hold nh limit: 0, Curr nh cnt: 0, Curr new hold cnt
NH drop cnt: 0
  Flags: Sendbcast-pkt-to-re
  Addresses, Flags: Is-Default Is-Primary
    Local: 192.168.1.1
```

What is causing this problem?

A. The loopback interface requires encapsulation.
B. The loopback interface is not assigned to a security zone.
C. The incorrect interface index ID is assigned to the loopback interface.
D. The IP address on the loopback interface is a private address.

Answer: C

NEW QUESTION 15
Click the Exhibit button.

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

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

Answer: D

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

NEW QUESTION 16
You want to enable transparent mode on your SRX series device.
In this scenario, which three actions should you perform? (Choose three.)

A. Enable the ethernet-switching family on your Layer 2 interfaces
B. Install a Layer 2 feature license.
C. Reboot the SRX device.
D. Ensure that no IRB interfaces are configured on the device.
E. Add your Layer 2 interfaces to a security zone.

Answer: ACE

NEW QUESTION 18
Which two statements are correct about mixed mode? (Choose two.)

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

Answer: BC

NEW QUESTION 19
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.

Answer: BCE

NEW QUESTION 20
Click the Exhibit button.

```
user@srx2> show chassis high-availability services-redundancy-group 1
SRG failure event codes:
    BF  BFD monitoring
    IP  IP monitoring
    IF  Interface monitoring
    CP  Control Plane monitoring
Services Redundancy Group: 1
        Deployment Type: SWITCHING
        Status: BACKUP
        Activeness Priority: 100
        Preemption: DISABLED
        Process Packet In Backup State: NO
        Control Plane State: READY
        System Integrity Check: COMPLETE
        Failure Events: NONE
        Peer Information:
          Peer Id: 1
          Status : ACTIVE
          Health Status: HEALTHY
          Failover Readiness: N/A
      Virtual IP Info:
          Index: 2
```

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

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

Answer: CD

NEW QUESTION 23
Exhibit:

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

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

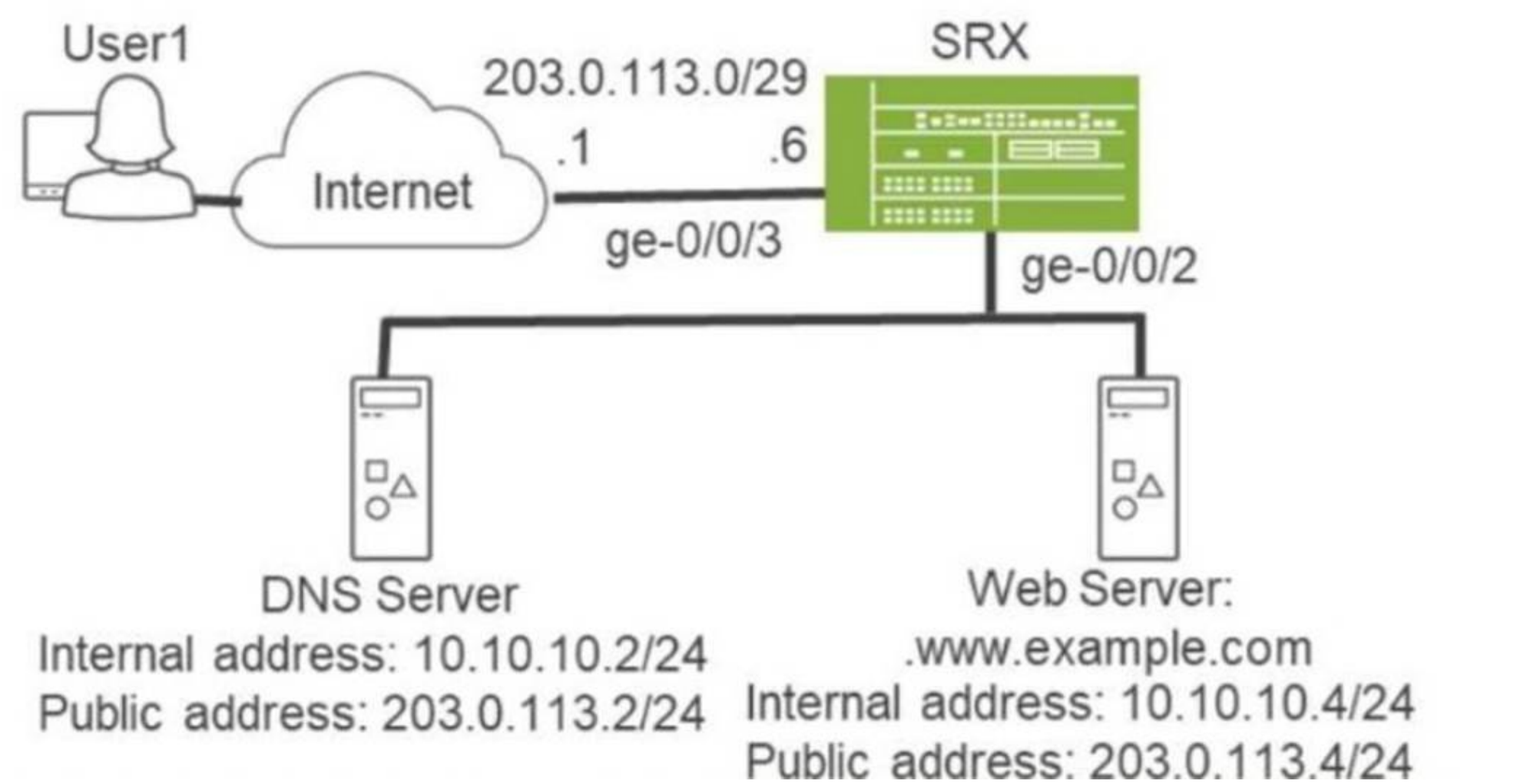
A. The packet is dropped by the default security policy.
B. The packet is dropped by a configured security policy.
C. The data shown requires a traceoptions flag of host-traffic.
D. The data shown requires a traceoptions flag of basic-datapath.

Answer: AD

Explanation:
? Understanding the Flow Log Output:
From the flow logs in the exhibit, we can observe the following key events:
? uk.co.certification.simulator.questionpool.PList@30863efa
? Explanation of Answer A (Dropped by the default security policy):
The log message clearly states that the packet was dropped by the default security policy (default-policy-logical-system-00). In Junos, when a session is attempted

between two zones and no explicit policy exists to allow the traffic, the default policy is to deny the traffic. This is a common behavior in Junos OS when a security policy does not explicitly allow traffic between zones.
? Explanation of Answer D (Requires traceoptions flag of basic-datapath):
The information displayed in the log involves session creation, flow policy search, and packet dropping due to policy violations, which are all part of basic packet processing in the data path. This type of information is logged when the traceoptions flag is set to basic- datapath. The basic-datapath traceoption provides detailed information about the forwarding process, including policy lookups and packet drops, which is precisely what we see in the exhibit.
? uk.co.certification.simulator.questionpool.PList@2aaa48ae
Step-by-Step Configuration for Tracing (Basic-Datapath):
? Enable flow traceoptions:
To capture detailed information about how traffic is being processed, including policy lookups and flow session creation, enable traceoptions for the flow.
bash
set security flow traceoptions file flow-log
set security flow traceoptions flag basic-datapath
? Apply the configuration and commit:
bash
commit
? View the logs:
Once enabled, you can check the trace logs for packet flows, policy lookups, and session creation details:
bash
show log flow-log
This log will contain information similar to the exhibit, including session creation attempts and packet drops due to security policy.
Juniper Security Reference:
? Default Security Policies: Juniper SRX devices have a default security policy to deny all traffic that is not explicitly allowed by user-defined policies. This is essential for security best practices. Reference: Juniper Networks Documentation on Security Policies.
? Traceoptions for Debugging Flows: Using traceoptions is crucial for debugging and understanding how traffic is handled by the SRX, particularly when issues arise from policy misconfigurations or routing. Reference: Juniper Traceoptions.
By using the basic-datapath traceoptions, you can gain insights into how the device processes traffic, including policy lookups, route lookups, and packet drops, as demonstrated in the exhibit.
==========

NEW QUESTION 28
Exhibit:



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

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

Answer: BD

Explanation:
In the scenario where internal users are trying to access the company's web server via its FQDN but the DNS server resolves to a private IP, two key actions are needed:
? Static NAT (Answer B): Since the internal DNS server resolves the web server to
its private IP address (10.10.10.4/24), you need to configure static NAT for both the DNS server and the webserver. This will ensure that requests coming from the internet will be translated to the web server's public IP (203.0.113.4) and the DNS server??s public IP (203.0.113.2).
Example Command: bash
set security nat static rule-set public-to-private from zone untrust

set security nat static rule-set public-to-private rule dns-server match destination-address 203.0.113.2/32
set security nat static rule-set public-to-private rule dns-server then static-nat-prefix 10.10.10.2/32
set security nat static rule-set public-to-private rule web-server match destination-address 203.0.113.4/32
set security nat static rule-set public-to-private rule web-server then static-nat-prefix 10.10.10.4/32
? Proxy ARP (Answer D): The SRX needs to respond to ARP requests for the public
IP addresses of both the DNS and webserver on the interface facing the internet (ge-0/0/3). This allows the SRX to handle requests directed at the public IPs.
Example Command:
set interfaces ge-0/0/3 unit 0 family inet proxy-arp interface-address 203.0.113.2/32 set interfaces ge-0/0/3 unit 0 family inet proxy-arp interface-address 203.0.113.4/32 These two configurations allow external users to access the internal web server via its public IP, as resolved by the DNS server.
: Juniper NAT and proxy ARP documentation.
==========

NEW QUESTION 30
You have configured the backup signal route IP for your multinode HA deployment, and the ICL link fails.
Which two statements are correct in this scenario? (Choose two.)

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

Answer: AC

NEW QUESTION 32
Your IPsec tunnel is configured with multiple security associations (SAs). Your SRX Series device supports the CoS-based IPsec VPNs with multiple IPsec SAs feature. You are asked to configure CoS for this tunnel.
Which two statements are true in this scenario? (Choose two.)

A. The local and remote gateways do not need the forwarding classes to be defined in the same order.
B. A maximum of four forwarding classes can be configured for a VPN with the multi-sa forwarding-classes statement.
C. The local and remote gateways must have the forwarding classes defined in the same order.
D. A maximum of eight forwarding classes can be configured for a VPN with the multi-sa forwarding-classes statement.

Answer: AD

NEW QUESTION 36
Referring to the exhibit,

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

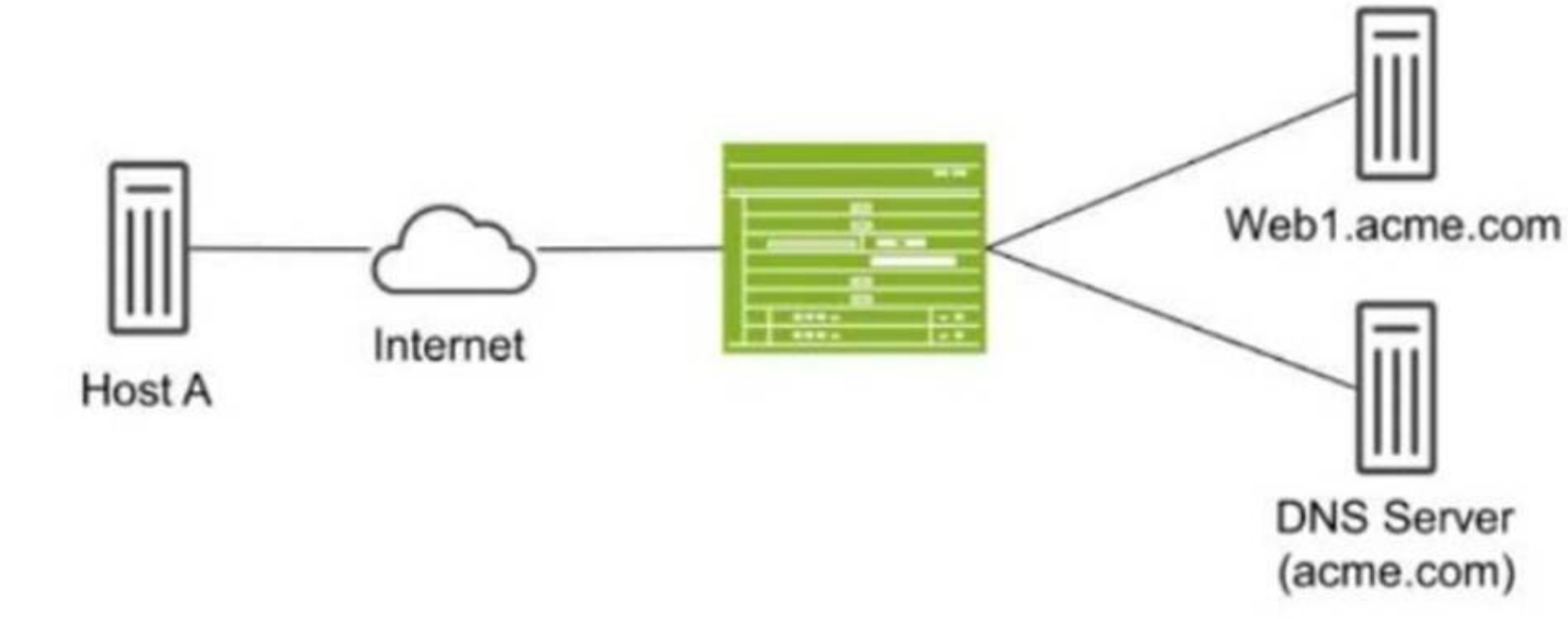
which two statements are correct about the NAT configuration? (Choose two.)

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

Answer: BD

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

NEW QUESTION 39
Exhibit:



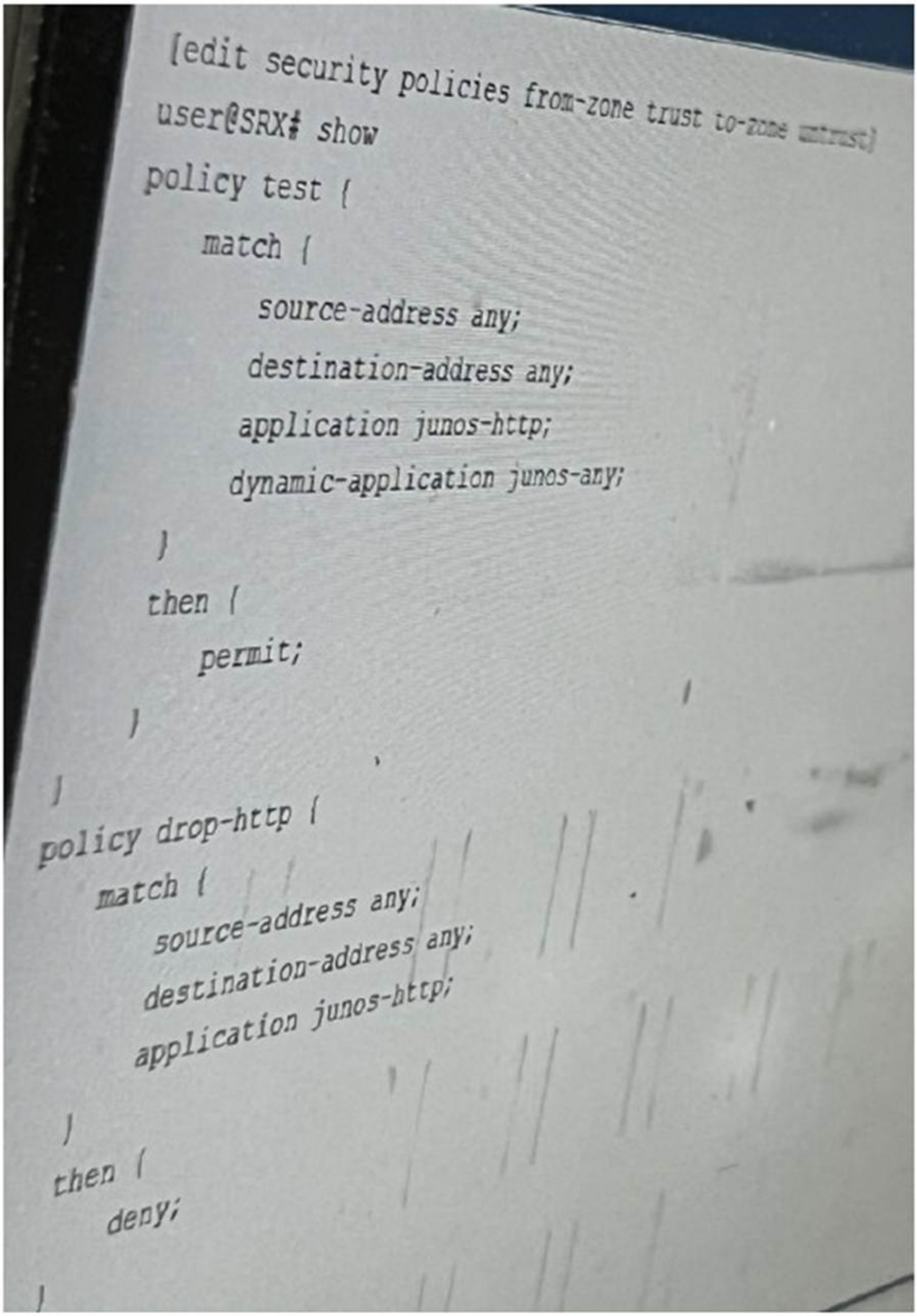
Host A shown in the exhibit is attempting to reach the Web1 webserver, but the connection is failing. Troubleshooting reveals that when Host A attempts to resolve the domain name of the server (web.acme.com), the request is resolved to the private address of the server rather than its public IP.
Which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

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

Answer: C

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

NEW QUESTION 41
Exhibit:



You created a Unified security policy called test on the network edge srx series firewall. According to the firewall, this new security policy is not passing traffic. Which two statements are correct in this scenario? (Choose two.)

A. The test policy should be the last policy.
B. A match exists on the test policy, but the dynamic application is waiting to be discovered
C. The source address cannot be any when a dynamic application is configured.
D. The drop-http policy is a terminating rule and will drop the traffic.

Answer: BD

NEW QUESTION 45
You want to use a security profile to limit the system resources allocated to user logical

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

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

Answer: BD

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

NEW QUESTION 48
Which two statements are true when setting up an SRX Series device to operate in mixed mode? (Choose two.)

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

Answer: CD

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

NEW QUESTION 50
Which three statements about persistent NAT are correct? (Choose Three)

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

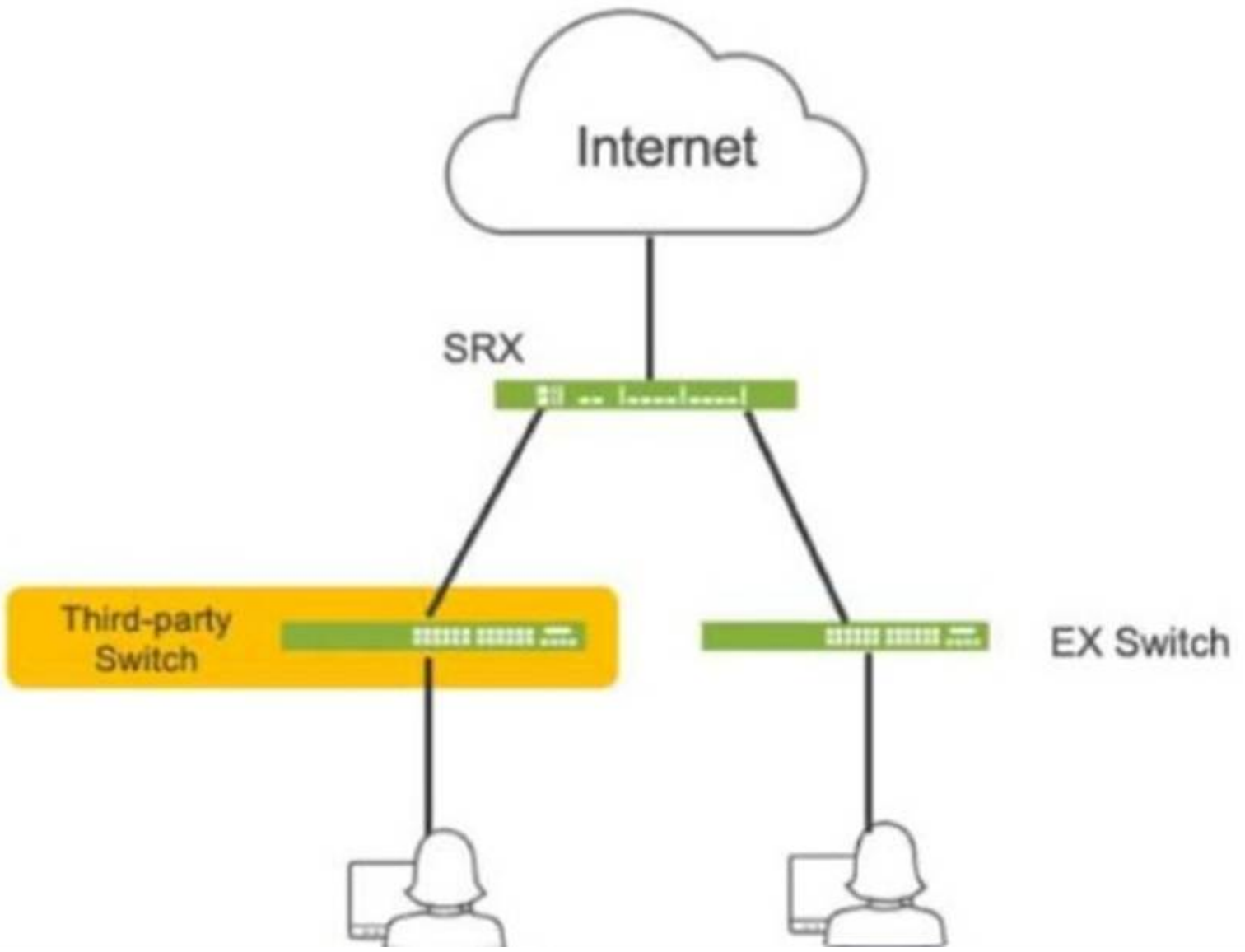
Answer: BCD

NEW QUESTION 55
You are using AutoVPN to deploy a hub-and-spoke VPN to connect your enterprise sites. In this scenario, which two statements are true? (Choose two.)

A. New spoke sites can be added without explicit configuration on the hub.
B. Direct spoke-to-spoke tunnels can be established automatically.
C. All spoke-to-spoke IPsec communication will pass through the hub.
D. AutoVPN requires OSPF over IPsec to discover and add new spokes.

Answer: AC

NEW QUESTION 57
Click the Exhibit button.



Referring to the exhibit, which three actions do you need to take to isolate the hosts at the switch port level if they become infected with malware? (Choose three.)

A. Enroll the SRX Series device with Juniper ATP Cloud.
B. Use a third-party connector.
C. Deploy Security Director with Policy Enforcer.
D. Configure AppTrack on the SRX Series device.
E. Deploy Juniper Secure Analytics.

Answer: ABC

Explanation:
? A. Enroll the SRX Series device with Juniper ATP Cloud. This is essential for the SRX to receive threat intelligence from ATP Cloud, enabling it to identify infected hosts and take action.
? B. Use a third-party connector. In this specific scenario, a third-party connector is required to integrate the SRX with the third-party switch. While Juniper has native integration for its EX switches, a connector is necessary to communicate with and manage the third-party switch.
? C. Deploy Security Director with Policy Enforcer. Security Director orchestrates the automated response, and Policy Enforcer translates the policies into device-specific commands for the SRX and the third-party switch (via the connector).
==========

NEW QUESTION 62
Click the Exhibit button.

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

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

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

Answer: D

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding the Problem:
? A CoS-based VPN has been configured but is not functioning correctly.
? The exhibit shows that under the class-of-service configuration, six forwarding classes are defined.
Forwarding Classes in the Exhibit:
? best-effort
? ef-class
? af-class
? network-control
? res-class
? web-data
Juniper CoS-Based VPN Limitations:
? Maximum Number of Forwarding Classes: In CoS-based VPNs (Layer 3 VPNs), there is a limitation on the number of forwarding classes that can be used.
? Supported Forwarding Classes: Only up to four forwarding classes are supported in an L3VPN for CoS purposes.
Reference:
Juniper Networks Documentation:
"For Layer 3 VPNs, the maximum number of forwarding classes supported is four. If you configure more than four forwarding classes, CoS functionality might not work as expected."
Source: Juniper TechLibrary - Class of Service Limitations in VPNs
* Explanation:
Issue Identification:
The VPN is not functioning correctly because it exceeds the maximum number of supported forwarding classes for a CoS-based VPN.
Solution:
Option D: You must delete one forwarding class.
By reducing the number of forwarding classes to four or fewer, the CoS-based VPN will comply with the limitations and function correctly.

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

NEW QUESTION 66
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

JN0-637 Practice Exam Features:

* JN0-637 Questions and Answers Updated Frequently

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

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

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