Juniper

Exam Questions JN0-637

Security - Professional (JNCIP-SEC)

NEW QUESTION 1
How does an SRX Series device examine exception traffic?

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

Answer: A

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

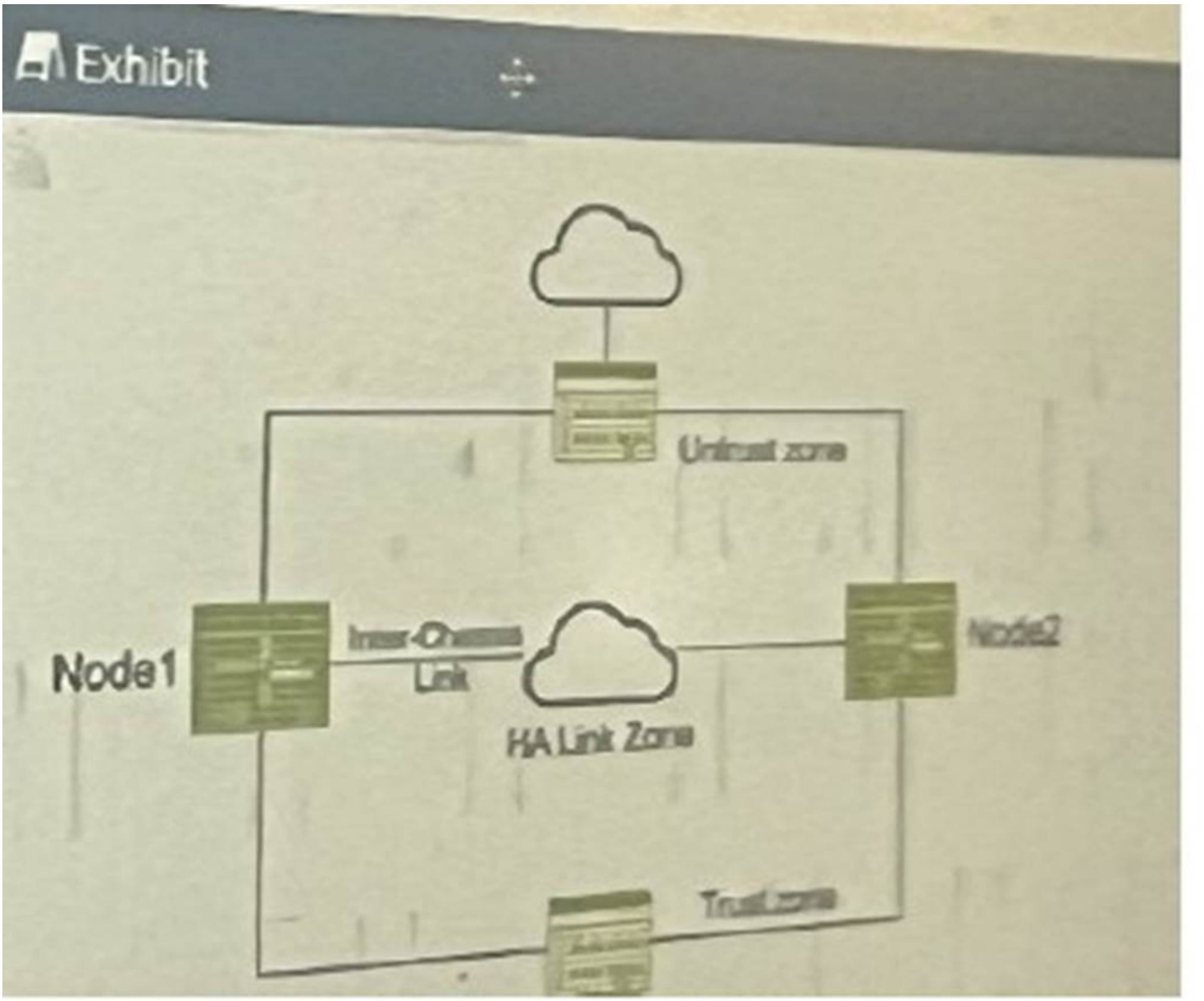
NEW QUESTION 2
You configure two Ethernet interfaces on your SRX Series device as Layer 2 interfaces and add them to the same VLAN. The SRX is using the default L2-learning setting. You do not add the interfaces to a security zone.
Which two statements are true in this scenario? (Choose two.)

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

Answer: AC

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

NEW QUESTION 3
Exhibit:



You have deployed a pair of SRX series devices in a multimode HA environment. You need to enable IPsec encryption on the interchassis link.
Referring to the exhibit, which three steps are required to enable ICL encryption? (Choose three.)

A. Install the Junos IKE package on both nodes.
B. Enable OSPF for both interchassis link interfaces and tum on the dynamic-neighbors parameter.
C. Configure a VPN profile for the HA traffic and apply to both nodes.
D. Enable HA link encryption in the IPsec profile on both nodes.
E. Enable HA link encryption in the IKE profile on both nodes,

Answer: ACD

Explanation:
? A. Install the Junos IKE package on both nodes. While I previously stated that IKE
is usually included in the base Junos OS image, it's essential to ensure that the necessary IKE package is indeed installed and enabled on both SRX nodes to support ICL encryption.
? C. Configure a VPN profile for the HA traffic and apply it to both nodes. This
dedicated VPN profile defines the security parameters (encryption algorithms, authentication, etc.) specifically for the ICL traffic.
? D. Enable HA link encryption in the IPsec profile on both nodes. Within the IPsec
profile, you must explicitly enable ICL encryption to ensure that all traffic traversing the interchassis link is protected.
Why E is incorrect:
? E. Enable HA link encryption in the IKE profile on both nodes. While securing IKE negotiations is important, it's typically handled within the IPsec profile itself when configuring ICL encryption on SRX devices.

NEW QUESTION 4
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
Which two statements are correct about the ICL in an active/active mode multinode HA environment? (Choose two.)

A. The ICL is strictly a Layer 2 interface.
B. The ICL uses a separate routing instance to communicate with remote multinode HApeers.
C. The ICL traffic can be encrypted.
D. The ICL is the local device management interface in a multinode HA environment.

Answer: BC

NEW QUESTION 7
In a multinode HA environment, which service must be configured to synchronize between nodes?

A. Advanced policy-based routing
B. PKI certificates
C. IPsec VPN
D. IDP

Answer: B

NEW QUESTION 8
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 9
A company has acquired a new branch office that has the same address space as one of its local networks, 192.168.100.0/24. The offices need to communicate with each other.
Which two NAT configurations will satisfy this requirement? (Choose two.)

A. [edit security nat source]user@OfficeA# show rule-set OfficeBtoA { from zone OfficeB;to zone OfficeA; rule 1 {match {source-address 192.168.210.0/24; destination-address 192.168.200.0/24;}then {source-nat { interface; }}}}
B. [edit security nat static]user@OfficeA# show rule-set From-Office-B { from interface ge-0/0/0.0;rule 1 { match {destination-address 192.168.200.0/24;}then { static-nat {prefix { 192.168.100.0/24; }}}}}
C. [edit security nat static]user@OfficeB# show rule-set From-Office-A { from interface ge-0/0/0.0;rule 1 { match {destination-address 192.168.210.0/24;}then { static-nat {prefix { 192.168.100.0/24; }}}}}
D. [edit security nat source]user@OfficeB# show rule-set OfficeAtoB { from zone OfficeA;to zone OfficeB; rule 1 {match {source-address 192.168.200.0/24; destination-address 192.168.210.0/24;}then {source-nat { interface; }}}}

Answer: BC

Explanation:
* 1. Static NAT Configuration at Office A (Option B):
? Configuration:
[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; }
}
}
}
}
? Explanation:
Reference:
Juniper Networks Documentation: "Configuring Static NAT"
* 2. Static NAT Configuration at Office B (Option C): Configuration:
[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; }
}
}
}
}
* Explanation:
from interface ge-0/0/0.0;: Specifies the interface through which the traffic is received.
Matching Traffic:
destination-address 192.168.210.0/24;: Matches packets destined for 192.168.210.0/24. Action:
static-nat { prefix { 192.168.100.0/24; } }: Translates the destination address to 192.168.100.0/24.
Result:
Office A sends packets to 192.168.210.0/24, which are translated to 192.168.100.0/24
upon arrival at Office B.
Reference:
Juniper Networks Documentation: "Configuring Static NAT"
Why Options A and D are Incorrect:
Option A and Option D use Source NAT, which is typically used for translating the source IP address of outgoing traffic.
Source NAT with interface-based translation may not resolve overlapping IP issues effectively because it doesn't provide a one-to-one mapping of the overlapping addresses.
In scenarios with overlapping networks, Static NAT is preferred as it allows for consistent and predictable address translation, essential for two-way communication.
Key Juniper Concepts: Static NAT:
Provides a one-to-one mapping between local and global addresses. Useful for scenarios where bidirectional communication is required. Reference: Juniper Networks Day One Book "Advanced NAT Concepts" Source NAT:
Typically used for translating private IP addresses to public IP addresses for outbound traffic.
Interface-based Source NAT translates the source IP to the IP address of the egress interface.
Not ideal for resolving overlapping IP spaces in bidirectional communication.
Additional References:
Juniper TechLibrary:
"Understanding NAT in SRX Series Devices" "Configuring NAT for Overlapping Networks" Juniper Forums and Knowledge Base Articles:
Discussions on resolving overlapping IP address spaces using Static NAT.
Conclusion:
By implementing Static NAT configurations as shown in Options B and C, both offices can effectively communicate despite having overlapping IP address spaces.
Static NAT ensures that IP addresses are uniquely translated, avoiding conflicts and enabling seamless connectivity between the two networks.

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

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

Answer: AD

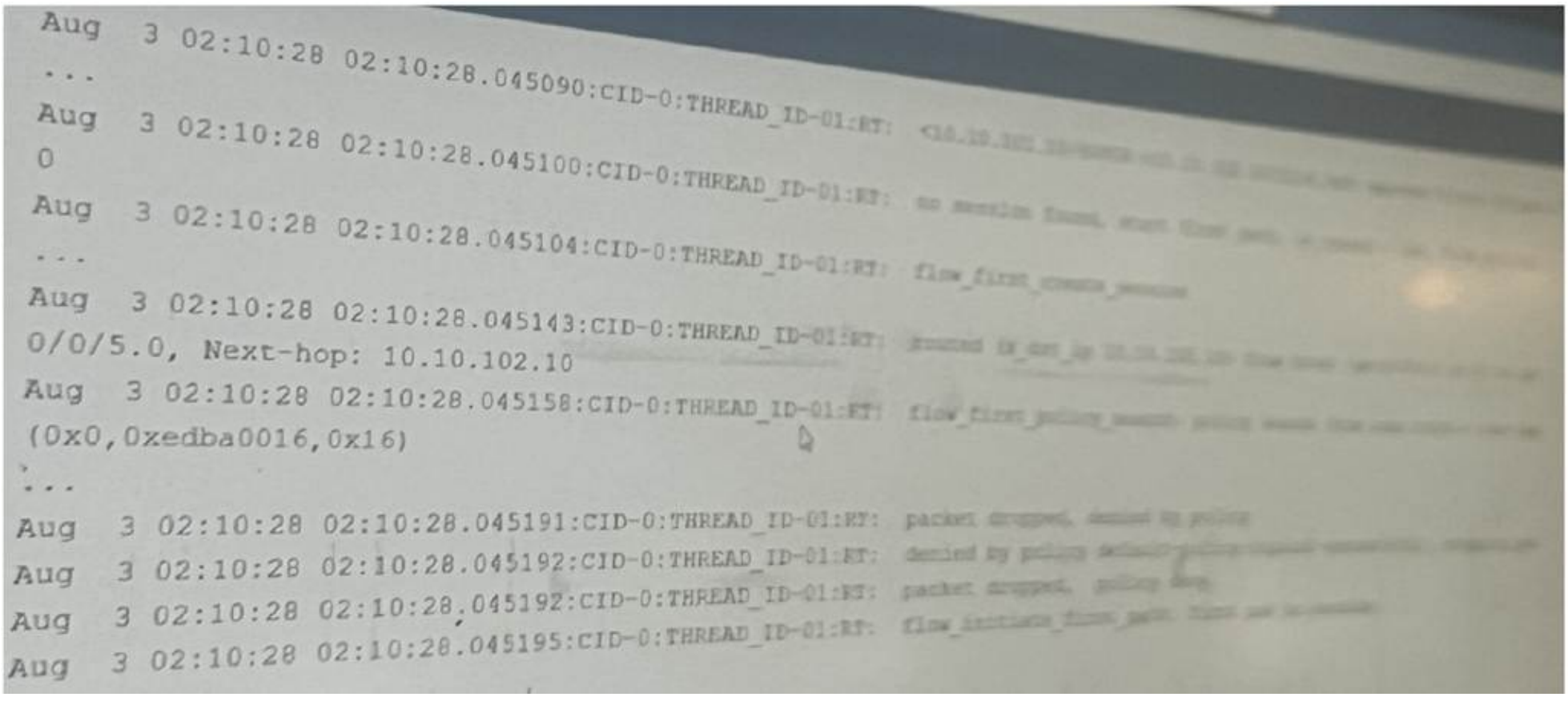
NEW QUESTION 15
You want to configure the SRX Series device to map two peer interfaces together and ensure that there is no switching or routing lookup to forward traffic.
Which feature on the SRX Series device is used to accomplish this task?

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

Answer: B

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security References
Understanding Secure Wire:
? Secure Wire Feature:
? Use Case:
Option B: Secure wire
? Explanation:
Reference:
"The secure wire feature allows traffic to pass between two interfaces without any security processing or route lookups."
Source: Juniper TechLibrary - Secure Wire Overview
Why Other Options Are Incorrect:
Option A: Transparent mode involves Layer 2 switching.
Option C: Mixed mode combines Layer 2 and Layer 3 but doesn't prevent switching/routing lookups.
Option D: Switching mode operates at Layer 2 and includes switching lookups.
Conclusion:
Secure wire is the correct feature to map two interfaces together without switching or routing lookups.

NEW QUESTION 18
Exhibit:



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

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

Answer: AC

NEW QUESTION 22
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 23
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

Answer: D

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):
? Incorrect Options:
Juniper References:
? Juniper Persistent NAT Documentation: Describes the persistent NAT binding table and the commands used to monitor its status.

NEW QUESTION 27
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_1kup success 192.168.1.1, iif1 0x47, oif1 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 1kup: 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 1kup: vsys 0 zone(5:global) -> zone(5:global) scope:0
…
Mar  7 02:38:15 02:38:15.354000:CID-0:THREAD_ID-01:RT: permitted by policy allow-bgp(6)
Mar  7 02:38:15 02:38:15.354048:CID-0:THREAD_ID-01:RT: flow_first_final_check: in  0/3.0>, out
Mar  7 02:38:15 02:38:15.354050:CID-0:THREAD_ID-01:RT: In flow_first_complete_session
Mar  7 02:38:15 02:38:15.354051:CID-0:THREAD_ID-01:RT: flow_first_complete_session, pak_ptr: 0x2c5fcd40, nsp: 0x2a140340,
in_tunnel: 0x0
…
Mar  7 02:38:15 02:38:15.354055:CID-0:THREAD_ID-01:RT: Session (id:20395) created for first pak 2
Mar  7 02:38:15 02:38:15.354073:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat: in  , out  A> dst_adr 192.168.1.1, sp 54882,
dp 179
Mar  7 02:38:15 02:38:15.354075:CID-0:THREAD_ID-01:RT: chose interface lo0.0 as incoming nat if.
Mar  7 02:38:15 02:38:15.354075:CID-0:THREAD_ID-01:RT: packet dropped: for self but not interested
Mar  7 02:38:15 02:38:15.354076:CID-0:THREAD_ID-01:RT: packet dropped, packet dropped: for self but  not interested.
Mar  7 02:38:15 02:38:15.354079:CID-0:THREAD_ID-01:RT: flow_first_install_session: Loopback session processing aborted
Mar  7 02:38:15 02:38:15.354080:CID-0:THREAD_ID-01:RT: first path session installation failed
Mar  7 02:38:15 02:38:15.354081:CID-0:THREAD_ID-01:RT: flow find session returns error.
```

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

A. Add the junos-host zone policy to permit the BGP packets.
B. Add a firewall filter to lo0 that permits the BGP packets.
C. Modify the security policy to permit the BGP packets.
D. Add BGP to the lo0 host-inbound-traffic configuration.

Answer: D

NEW QUESTION 29
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 32
You want to bypass IDP for traffic destined to social media sites using APBR, but it is not working and IDP is dropping the session.
What are two reasons for this problem? (Choose two.)

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

Answer: AC

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

NEW QUESTION 36
Which two statements are correct about automated threat mitigation with Security Director? (Choose two.)

A. Infected hosts are tracked by their IP address.
B. Infected hosts are tracked by their chassis serial number.
C. Infected hosts are tracked by their MAC address.
D. Infected hosts are tracked by their user identity.

Answer: AC

NEW QUESTION 39
An ADVPN configuration has been verified on both the hub and spoke devices and it seems fine. However, OSPF is not functioning as expected.

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

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

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

Answer: AB

Explanation:
For ADVPN with OSPF, using a point-to-multipoint (p2mp) interface type and
enabling dynamic-neighbors are crucial. This configuration allows dynamic discovery of neighbors and the establishment of tunnels. For more information, refer to Juniper ADVPN Configuration Guide.
In the ADVPN configuration, OSPF isn't functioning as expected due to the interface configuration on st0.0. Here are the adjustments needed:
? Interface Type p2mp (Answer A): OSPF requires that the tunnel interface be set to
p2mp (point-to-multipoint) to allow OSPF to communicate with multiple dynamic neighbors over the ADVPN tunnels.
Command Example: bash
set interfaces st0.0 family inet ospf interface-type p2mp
? Dynamic Neighbors (Answer B): The dynamic neighbors statement allows OSPF to discover and communicate with dynamically established spokes in an ADVPN environment. This is essential for ADVPN to function properly since the tunnel endpoints are not static.
Command Example: bash
set protocols ospf area 0.0.0.0 interface st0.0 dynamic-neighbors
These settings ensure OSPF properly functions over dynamically created ADVPN tunnels.
: Juniper ADVPN and OSPF configuration.
==========

NEW QUESTION 43
You are deploying OSPF over IPsec with an SRX Series device and third-party device using GRE.
Which two statements are correct? (Choose two.)

A. The GRE interface should use lo0 as endpoints.
B. The OSPF protocol must be enabled under the VPN zone.
C. Overlapping addresses are allowed between remote networks.
D. The GRE interface must be configured under the OSPF protocol.

Answer: AD

Explanation:
Comprehensive Detailed Step-by-Step Explanation with All Juniper Security
References
Understanding the Scenario:
? Objective: Deploy OSPF over IPsec between an SRX Series device and a third- party device using GRE tunnels.
? Components Involved:
Option A: The GRE interface should use lo0 as endpoints.
? Explanation:
Reference:
Juniper Networks Documentation:
"Using loopback interfaces as GRE tunnel endpoints ensures stability and consistent reachability for routing protocols over GRE tunnels."
Source: Configuring GRE Tunnels
Option D: The GRE interface must be configured under the OSPF protocol.
* Explanation:
To run OSPF over the GRE tunnel, the GRE interface must be included in the OSPF configuration.
Configuration Steps: Create GRE Interface:
Example: set interfaces gr-0/0/0 unit 0 tunnel source <source-ip> tunnel destination
<destination-ip>
Assign IP Address to GRE Interface:
Example: set interfaces gr-0/0/0 unit 0 family inet address <ip-address>
Include GRE Interface in OSPF:
Example: set protocols ospf area <area-id> interface gr-0/0/0.0
Result:
OSPF will establish adjacencies over the GRE interface and exchange routing information.
Reference:
Juniper Networks Documentation:
"To enable OSPF over GRE tunnels, you must include the GRE interfaces in the OSPF configuration."
Source: OSPF over GRE Configuration

Why Options B and C are Incorrect:
Option B: The OSPF protocol must be enabled under the VPN zone.
* Explanation:
Since OSPF is running over the GRE tunnel, which is encapsulated over IPsec, the OSPF packets are encapsulated within GRE and IPsec.
The SRX device does not need to allow OSPF in the security policies or enable OSPF under the VPN zone for GRE-encapsulated traffic.
Security Policies:
The GRE traffic (IP protocol 47) must be permitted through the security policies.
OSPF runs inside the GRE tunnel and does not require additional configuration under the VPN zone.
Reference:
Juniper Networks Documentation:
"When using GRE over IPsec, routing protocols run over GRE and do not require separate security policies for their control traffic."
Source: Security Policies for GRE over IPsec
Option C: Overlapping addresses are allowed between remote networks.
* Explanation:
Overlapping IP addresses can cause routing conflicts and are generally not recommended. In a GRE over IPsec scenario, overlapping addresses can lead to issues in routing protocol
adjacency and data forwarding.
Best Practice:
Ensure unique IP addressing schemes between remote networks to prevent routing issues.
Reference:
Juniper Networks Documentation:
"Overlapping IP address spaces can lead to routing ambiguities and should be avoided when configuring GRE tunnels."
Source: Avoiding Overlapping IP Addresses
Conclusion:
Correct Answers: A and D Rationale:
Option A is correct because using lo0 as endpoints for GRE provides stability and reliability.
Option D is correct because the GRE interface must be included in the OSPF configuration to enable OSPF over the tunnel.

NEW QUESTION 44
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

Answer: D

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):
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.
==========

NEW QUESTION 49
Exhibit:

```
user@peer1> show chassis high-availability information
Node failure codes:
HW Hardware monitoring LB Loopback monitoring
MB Mbuf monitoring SP SPU monitoring
CS Cold Sync monitoring SU Software Upgrade
Node Status: ONLINE
Local-id: 1
Local-IP: 10.10.1.1
HA Peer Information:
Peer Id: 2 IP address: 10.10.1.2 Interface: ge-0/0/1.0
Routing Instance: default
Encrypted: NO Conn State: UP
Cold Sync Status: COMPLETE
Services Redundancy Group: 0
Current State: ONLINE
Peer Information:
Peer Id: 2
SRG failure event codes:
BF BFD monitoring
IP IP monitoring
IF Interface monitoring
CP Control Plane monitoring
Services Redundancy Group: 1
Deployment Type: SWITCHING
Status: ACTIVE
Activeness Priority: 200
Preemption: ENABLED
Process Packet In Backup State: NO
Control Plane State: READY
System Integrity Check: N/A
Failure Events: NONE
Peer Information:
Peer Id: 2
Status : BACKUP
Health Status: HEALTHY
Failover Readiness: READY
```

Referring to the exhibit, which statement is true?

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

Answer: D

Explanation:
The exhibit describes a Chassis Cluster configuration with high availability (HA) settings. The key information is related to Service Redundancy Group 1 (SRG1) and its failover behavior between the two peers.

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

NEW QUESTION 50
A customer wants to be able to initiate a return connection to an internal host from a specific
Server.
Which NAT feature would you use in this scenario?

A. target-host
B. any-remote-host
C. port-overloading
D. target-server

Answer: A

NEW QUESTION 53
Which two statements about policy enforcer and the forescout integration are true? (Choose two)

A. 802.1X authenticated devices are supported.
B. 802.1X authenticated devices are not supported.
C. A Forescout CounterACT agent must be installed on third-party devices
D. A Forescout CounterACT agent is agentless and does not need to be installed on third- party device

Answer: AD

NEW QUESTION 58
Which two statements about transparent mode and Ethernet switching mode on an SRX series
device are correct.

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

Answer: BC

NEW QUESTION 62
You need to set up source NAT so that external hosts can initiate connections to an internal device, but only if a connection to the device was first initiated by the internal device.
Which type of NAT solution provides this functionality?

A. Address persistence
B. Persistent NAT with any remote host
C. Persistent NAT with target host
D. Static NAT

Answer: C

Explanation:
Persistent NAT with target host allows external hosts to establish
connections only when the internal device initiates a session first, ideal for specific interactive applications. Refer to Juniper Persistent NAT Documentation.
The scenario requires that external hosts be able to initiate a connection only if the internal device has already initiated a connection. The correct solution is Persistent NAT with target host, which ensures that a specific external host can initiate new connections back to the internal device, but only after the internal device has established a session first.
? Persistent NAT with Target Host (Answer C): This allows the internal device to
initiate a connection, and once established, the specified external host can also initiate new connections to the internal device on the same NAT mapping.
Example Configuration: bash
set security nat source persistent-nat permit target-host-port
This solution is appropriate when controlled bidirectional communication is required based on an internal-initiated connection.
: Juniper persistent NAT documentation.
==========

NEW QUESTION 67
Which two statements are true about the procedures the Junos security device uses when handling traffic destined for the device itself? (Choose two.)

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

Answer: BC

Explanation:

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

NEW QUESTION 71
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The JN0-637 Practice Test Here