Vendor: Juniper

Exam Code:JN0-633

Exam Name: Security, Professional (JNCIP-SEC)

Version: Demo

QUESTION 1

You are troubleshooting an IPsec session and see the following IPsec security associations: ID Gateway Port Algorithm SPI Life:sec/kb Mon vsys

 192.168.224.1 500 ESP:aes-256/sha1 153ec235 26/ unlim - 0

 192.168.224.1 500 ESP:aes-256/sha1 153ec236 3011/ unlim - 0

What are two reasons for this behavior? (Choose two.)

A. Both peers are trying to establish IKE Phase 1 but are not successful.

B. Both peers have established SAs with one another, resulting in two IPsec tunnels.

C. The lifetime of the Phase 2 negotiation is close to expiration.

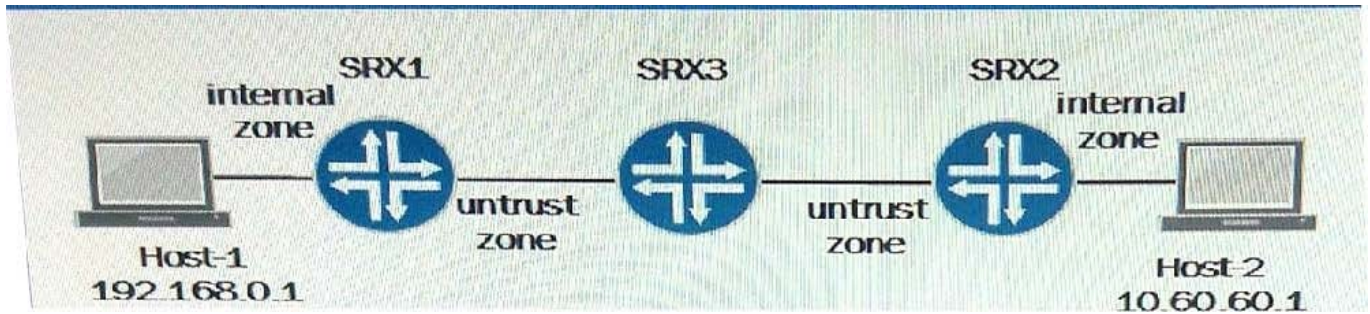D. Both peers have establish-tunnels immediately configured.

Correct Answer: CD

QUESTION 2

Click the Exhibit button.

[edit security nat static rule-set 12] user@SRX2# show from zone untrust; rule 1 {

match {

destination-address 192.168.1.1/32;

}

then {

static-nat {

prefix {

10.60.60.1/32;

}

}

}

}

Host-2 initiates communication with Host-1. All other routing and policies are in place to allow the traffic. What is the result of the communication?

Exhibit:

SRX1
internal
zone

SRX3

SRX2
internal
zone

untrust
zone

untrust
zone

Host-1
192.168.0.1

Host-2
10.60.60.1

A. The 192.168.0.1 address is translated to the 10.60.60.1 address.

B. The 10.60.60.1 address is translated to the 192.168.1.1 address.

C. No translation occurs.

D. The 192.168.0.1 address is translated to the 192.168.1.1 address.

Correct Answer: B

QUESTION 3

You are asked to deploy dynamic VPNs between the corporate office and remote employees that work from home. The gateway device at the corporate office consists of a pair of SRX650s in a chassis cluster. Which two statements about the deployment are true? (Choose two.)

A. The SRX650s must be separated as standalone devices to support the dynamic VPNs.

B. The remote clients must install client software to establish a tunnel with the corporate network.

C. The remote clients must reside behind an SRX device configured as the local tunnel endpoint.

D. The SRX650 must have HTTP or HTTPS enabled to aid in the client software distribution process.

Correct Answer: BD

QUESTION 4

Which problem is introduced by setting the terminal parameter on an IPS rule?

A. The SRX device will stop IDP processing for future sessions.

B. The SRX device might detect more false positives.

C. The SRX device will terminate the session in which the terminal rule detected the attack.
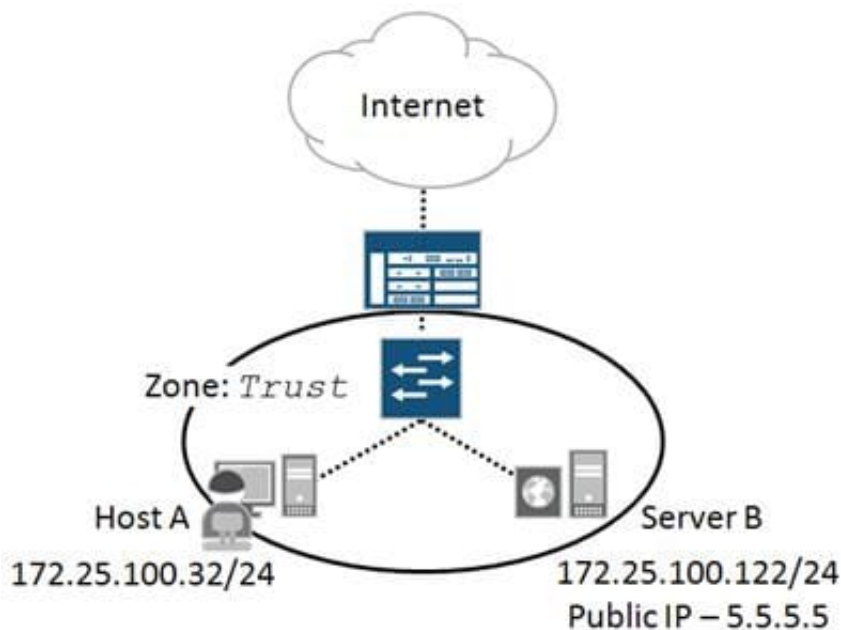
D. The SRX device might miss attacks.

Correct Answer: D

QUESTION 5

Click the Exhibit button.

Referring to the topology shown in the exhibit, which two configuration tasks will allow Host A to telnet to the public IP address associated with Server B? (Choose two.)

Exhibit:

A. Configure transparent mode to bypass the NAT processing of Server B\\'s public IP address.

B. Configure a stateless filter redirecting local traffic destined to Server B\\'s public IP address.

C. Configure a destination NAT rule that matches local traffic destined to Server B\\'s public IP address.

D. Configure a source NAT rule that matches local traffic destined to Server B\\'s public IP address.

Correct Answer: CD

QUESTION 6

When configuring AutoVPN, which two actions are required for an administrator to establish communication from the hub site to the spoke sites? (Choose two.)

A. Configure the next hop tunnel binding (NHTB).

B. Configure static routes from the hub to the spoke.

C. Configure a dynamic routing protocol such as BGP, OSPF, or RIP on the tunnel interfaces.

D. Create a multipoint secure tunnel interface on the hub device.

Correct Answer: CD

QUESTION 7

You are deploying a standalone SRX650 in transparent mode for evaluation purposes in a potential client\\'s network. The client will need to access the device to modify security policies and perform other various configurations. Where would you configure a Layer 3 interface to meet this requirement?

A. fxp0.0

B. vlan.1

C. irb.1

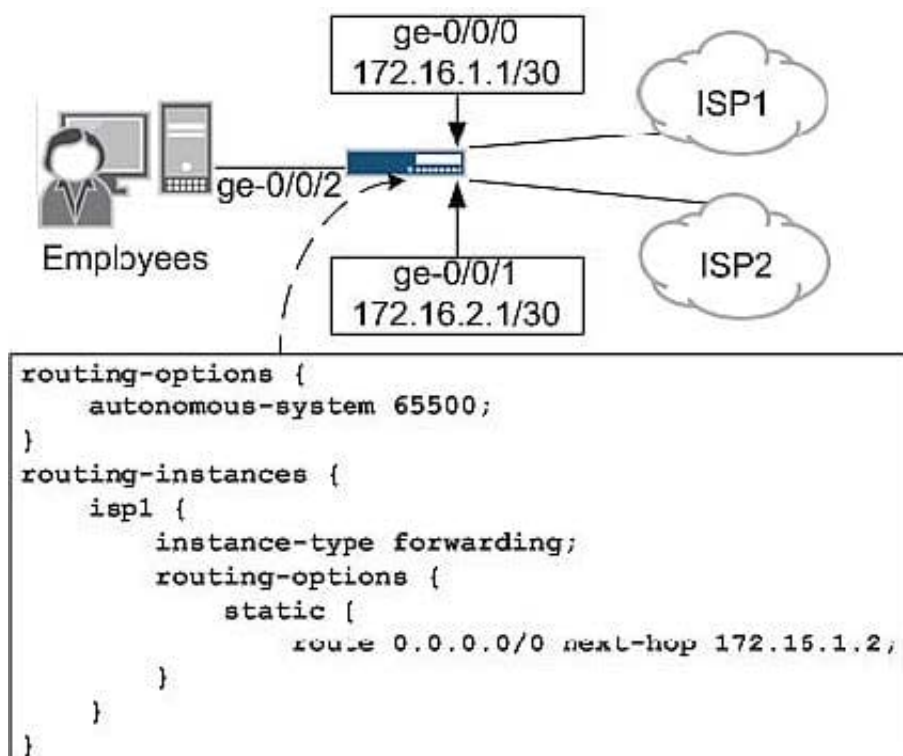D. ge-0/0/0.0

Correct Answer: C

QUESTION 8

Click the Exhibit button.

In the network shown in the exhibit, you want to forward traffic from the employees to ISP1 and ISP2. You want to forward all Web traffic to ISP1 and all other traffic to ISP2. However, your configuration is not producing the expected results. Part of the configuration is shown in the exhibit. When you run the show route table isp1 command, you do not see the default route listed.

What is causing this behavior?

Exhibit:


```
routing-options {
    autonomous-system 65500;
}
routing-instances {
    isp1 {
        instance-type forwarding;
        routing-options {
            static [
                route 0.0.0.0/0 next-hop 172.15.1.2;
            }
        }
    }
}
```

A. The autonomous system number is incorrect, which is preventing the device from receiving a default route from ISP1.

B. The device is not able to resolve the next-hop.

C. The isp1 routing instance is configured with an incorrect instance-type.

D. The show route table isp1 command does not display the default route unless you add the exact 0.0.0.0/0 option.
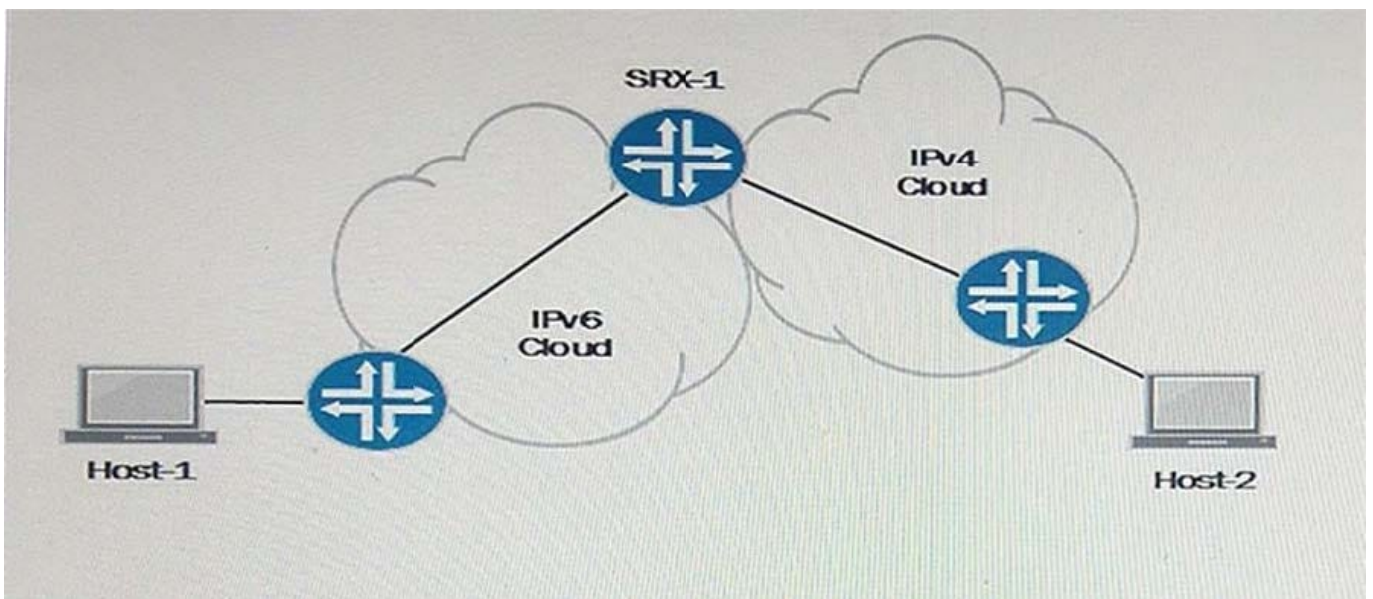
Correct Answer: B

QUESTION 9

Click the Exhibit button.

Referring to the exhibit, you must send traffic from Host-1 to Host-2. These two hosts can only

communicate with IPv4.

Which feature would you use to permit communication between Host-1 and Host-2?

Exhibit:

A. 6rd

B. DS-Lite

C. NAT46

D. NAT444

Correct Answer: B

QUESTION 10

You want requests from the same internal transport address to be mapped to the same external transport address. Only internal hosts can initialize the session. Which Junos configuration setting supports the requirements?

A. any-remote-host

B. target-host

C. source-host

D. address-persistent

Correct Answer: D

QUESTION 11

Click the Exhibit button.

user @host> show bgp summary logical-system LSYS1 Groups : 11 Peers : 10 Down peers: 1 Table Tot. Paths Act Paths Suppressed History Damp State

Pending inet.0 141 129 0 0 0 Peer AS InPkt OutPkt OutQ Flaps Last Up/Dwn State|#Active/Received/Accepted/Damped...

192.168.64.12 65008 11153 11459 0 26 3d

3:10:43 9/10/10/0 0/0/0/0

192.168.72.12 65009 11171 11457 0 26 3d

3:10:39 11/12/12/0 0/0/0/0

192.168.80.12 65010 9480 9729 0 27 3d

3:10:42 11/12/12/0 0/0/0/0

192.168.88.12 65011 11171 11457 0 25 3d

3:10:31 12/13/13/0 0/0/0/0

192.168.96.12 65012 9479 9729 0 26 3d

3:10:34 12/13/13/0 0/0/0/0

192.168.10.12 65013 111689 11460 0 27 3d

3:10:46 9/10/10/0 0/0/0/0

192.168.11.12 65014 111688 11458 0 25 3d

3:10:42 9/10/10/0 0/0/0/0

192.168.12.12 65015 111687 11457 0 25 3d

3:10:38 9/10/10/0 0/0/0/0

192.68.11.12 650168 9478 9729 0 25 3d

3:10:42 9/10/10/0 0/0/0/0

192.168.13.12 65017 111687 11457 0 27 3d

3:10:30 9/10/10/0 0/0/0/0

192.168.16.12 65017 111687 11457 0 27 1w3d2h Connect

user@host> show interfaces ge-0/0/7.0 extensive Logical interface ge-0/0/7.0 (Index 76) (SNMP ifIndex 548) (Generation 141)

... Security: Zone: log Allowed host-inbound traffic : bootp dns dhcp finger ftp tftp ident-reset http https ike netconf ping

reverse-telnet reverse-ssh rloqin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text xnm-ssl lsping ntp sip

r2cp Flow Statistics: Flow Input statistics:

Self packets: 0

ICMP packets: 0

VPN packets: 0

Multicast packets: 0

Bytes permitted by policy: 0

Connections established: 0

Flow Output statistics:

Multicast packets: 0

Bytes permitted by policy: 0

Flow error statistics (Packets dropped due to):

Address spoofing: 0

Authentication failed: 0

Incoming NAT errors: 0

Invalid zone received packet: 0

Multiple user authentications: 0

Multiple incoming NAT: 0

No parent for a gate: 0

No one interested in self pakets: 0

No minor session: 0

No more sessions: 589723

No NAT gate: 0

No route present: 0

No SA for incoming SPI: 0

No tunnel found: 0

No session for a gate: 0

No zone or NULL zone binding 0

Policy denied: 0

Security association not active: 0

TCP sequence number out of window: 0

Syn-attack protection: 0

User authentication errors: 0

Protocol inet, MTU: 1500, Generation: 1685, Route table: 0

Flags: Sendbcast-pkt-to-re

Addresses, F1ags: Is-Preferred Is-Primary

Destination: 10.5.123/24, Local: 10.5.123.3, Broadcast: 10.5.123.255, Generation: 156 Protocol multiservice, MTU: Unlimited, Generation: 1686, Route table: 0 Policer: Input: __default_arp_policer__ ...

...

An SRX Series device has been configured with a logical system LSYS1. One of the BGP peers is down.

Referring to the exhibit, which statement explains this problem?

A. The LSYS license only allows up to ten BGP peerings.

B. The maximum number of allowed flows is set to low.

C. The allocated memory is not sufficient for this LSYS.

D. The minimum number of flows is set to high.

Correct Answer: B

QUESTION 12

Click the Exhibit button.

According to the log shown in the exhibit, you notice that the IPsec session is not establishing. What are two reasons for this behavior? (Choose two.)

Exhibit:

```
Feb 8 10:39:40 Unable to find phase-1 policy as remote peer:2.2.2.2 is not recognized.
Feb 8 10:39:40 KMD_PM_P1_POLICY_LOOKUP_FAILURE: Policy lookup for Phase-1 [responder] failed for
p1_local=ipv4(any:0,[0..3]=1.1.1.2) p1_remote=ipv4(any:0,[0..3]=2.2.2.2)
Feb 8 10:39:40 1.1.1.2:500 (Responder) <-> 2.2.2.2:500 { 18983055 dbe1c0af - a4d6d829 f9ed3bba [-1] /
0x00000000 } IP; Error = No proposal chosen (14)
```

A. mismatched preshared key

B. mismatched proxy ID

C. incorrect peer address

D. mismatched peer ID

Correct Answer: CD