JN0-633$^{\text{Q\&As}}$

Security, Professional (JNCIP-SEC)

Pass Juniper JN0-633 Exam with 100% Guarantee

QUESTION 1

You want to route traffic between two newly created virtual routers without the use of logical systems using the configuration options on the SRX5800.

Which two methods of forwarding, between virtual routers, would you recommend? (Choose two.)

A. Use a static route to forward traffic across virtual routers using the next-table option. Enable the return route by using a RIB group. next-table command.

B. Create static routes in each virtual router using the

C. Use a RIB group to share the internal routing protocol routes from the master routing instance.

D. Connect a direct cable between boo physical interfaces, one in each virtual router and use next-hop command. static routes with the

Correct Answer: BD

QUESTION 2

What are two configurable routing instance types? (Choose two.)

A. IPsec

B. VPLS

C. GRE

D. VRF

Correct Answer: BD

QUESTION 3

You are asked to establish a baseline for your company\\'s network traffic to determine the bandwidth usage per application. You want to undertake this task on the central SRX device that connects all segments together. What are two ways to accomplish this goal? (Choose two.)

A. Configure a mirror port on the SRX device to capture all traffic on a data collection server for further investigation.

B. Use interface packet counters for all permitted and denied traffic and calculate the values using Junos scripts.

C. Send SNMP traps with bandwidth usage to a central SNMP server.

D. Enable AppTrack on the SRX device and configure a remote syslog server to receive AppTrack messages.

Correct Answer: AD

QUESTION 4

You recently implemented application firewall rules on an SRX device to act upon encrypted traffic. However, the encrypted traffic is not being correctly identified. Which two actions will help the SRX device correctly identify the encrypted traffic? (Choose two.)

A. Enable heuristics to detect the encrypted traffic.

B. Disable the application system cache.

C. Use the junos:UNSPECIFIED-ENCRYPTED application signature.

D. Use the junos:SPECIFIED-ENCRYPTED application signature.

Correct Answer: AC

QUESTION 5

You have been asked to configure traffic to flow between two virtual routers (VRs) residing on two unique

logical systems (LSYSs) on the same SRX5800.

How would you accomplish this task?

A. Configure a security policy that contains the context from VR1 to VR2 to permit the relevant traffic.

B. Configure a security policy that contains the context from LSYS1 to LSYS2 and relevant match conditions in the rule set to allow traffic between the IP networks in VR1 and VR2.

C. Configure logical tunnel interfaces between VR1 and VR2 and security policies that allow relevant traffic between VR1 and VR2 over that link.

D. Configure an interconnect LSYS to facilitate a connection between LSYS1 and LSYS2 and relevant policies to allow the traffic.

Correct Answer: C

QUESTION 6

Click the Exhibit button.

```
user@host> monitor traffic interface ge-0/0/3

verbose output suppressed, use or for full protocol decode

Address resolution is ON. Use to avoid any reverse lookup delay.

Address resolution timeout is 4s.

Listening on ge-0/0/3, capture size 96 bytes

Reverse lookup for 172.168.3.254 failed (check DNS reachability). Other reverse lookup failures will not be
```

reported.

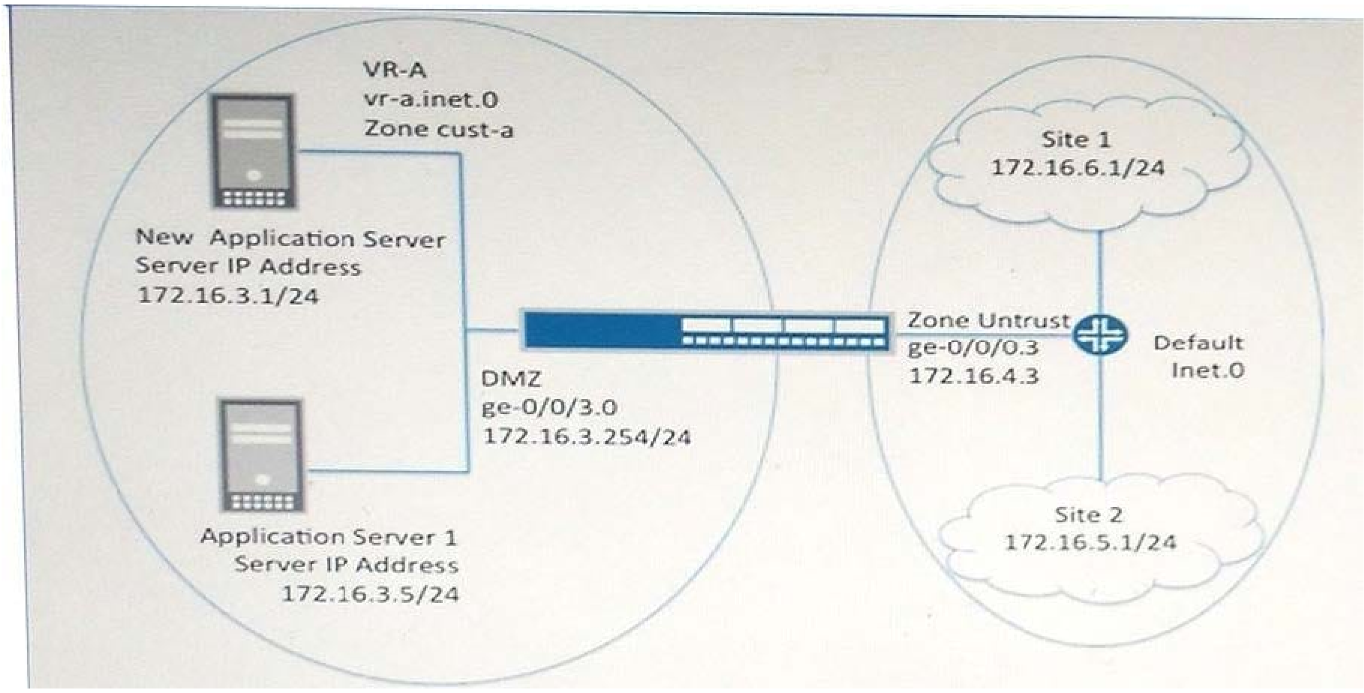
Use to avoid reverse lockups on IP addresses.

```
19:24:16.320907 In arp who-has 172.168.3.254 tell 172.168.3.1

19.24:17.322751 In arp who has 172.168.3.254 tell 172.168.3.1

19.24:18.328895 In arp who-has 172.168.3.254 tell 172.168.3.1

19.24:18.332956 In arn who has 172.168.3.254 tell 172.168.3.1
```

A new server has been set up in your environment. The administrator suspects that the firewall is blocking the traffic from the new server. Previously existing servers in the VLAN are working correctly. After reviewing the logs, you do not see any traffic for the new server.

Referring to the exhibit, what is the cause of the problem?

Exhibit:



A. The server is in the wrong VLAN.

B. The server has been misconfigured with the wrong IP address.

C. The firewall has been misconfigured with the incorrect routing-instance.

D. The firewall has a filter enabled to block traffic from the server.

Correct Answer: C

QUESTION 7

Click the Exhibit button.

```
[edit security application-firewall]
user@host# show
rule-sets web {
 rule one {
 match {
 dynamic-application junos:HTTP;
 }
 then {
permit;
 }
 }
 default-rule {
 reject; } }
```

What will happen to non-HTTP traffic that matches the application-firewall policy shown in the exhibit?

A. It will be denied because this is a blacklist policy.

B. It will be dropped and an error will be sent to the source.

C. It will be silently dropped.

D. It will be allowed because this is a whitelist policy.

Correct Answer: C

QUESTION 8

You must configure a central SRX device connected to two branch offices with overlapping IP address space. The branch office connections to the central SRX device must reside in separate routing instances. Which two components are required? (Choose two.)

A. virtual routing instance

B. forwarding instance

C. static NAT

D. persistent NAT

Correct Answer: AC

QUESTION 9

You are asked to configure your SRX Series device to support IDP SSL inspections for up to 6,000 concurrent HTTP sessions to a server within your network.

Which two statements are true in this scenario? (Choose two.)

A. You must add at least one PKI certificate.

B. Junos does not support more than 5000 sessions in this scenario.

C. You must enable SSL decoding.

D. You must enable SSL inspection.

Correct Answer: CD

QUESTION 10

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 is a chassis cluster formed from two SRX240s. Which two statements about this deployment are true? (Choose two.)

A. You must remove the SRX240s from the chassis cluster before enabling the dynamic VPNs.

B. The remote clients can run Windows XP, Windows Vista, Windows 7, or OS X operating systems.

C. If more than two dynamic VPN tunnels are required, you must purchase and install a new license.

D. The remote users can be authenticated by the SRX240s or a configured RADIUS server.

Correct Answer: CD

QUESTION 11

Click the Exhibit button.

```
user@host> show security ike security-associations Index State Initiator cookie Responder cookie Mode Remote
Address 3271043 UP 7f42284089404673 95fd8408940438d8 Main 172.31.50.2

user@host> show security ipsec security-associations Total active tunnels: 0

user@host> show log phase2

Feb 2 14:21:18 host kmd[1088]: IKE negotiation failed with error: TS unacceptable. IKE Version: 1, VPN:

vpn-1 Gateway: gate-1, Local: 172.31.50.1/500, Remote: 172.31.50.2/500, Local IKE-ID: 172.31.50.1,

Remote IKE-ID: 172.31.50.2, VR-ID: 0
```

```
Feb 2 14:21:18 host kmd[1088]: KMD_VPN_TS_MISMATCH: Traffic-selector mismatch, vpn name: vpn-1,

Peer Proposed traffic-selector local-ip: ipv4(2.2.2.2), Peer Proposed traffic-selector remote-ip: ipv4

(1.1.1.1)

Feb 2 14:21:54 host kmd[1088]: IKE negotiation failed with error: No proposal chosen. IKE Version: 1,

VPN: vpn-1 Gateway: gate-1, Local:

172.31.50.1/500, Remote: 172.31.50.2/500, Local IKE-ID: 172.31.50.1, Remote IKE-ID: 172.31.50.2, VRID: 0

Feb 2 14:22:19 host kmd[1088]: KMD_VPN_TS_MISMATCH: Traffic-selector mismatch, vpn name: vpn-1,

Peer Proposed traffic-selector local-ip:

ipv4 (2.2.

2.2), Peer Proposed traffic-selector remote-ip: ipv4(1.1.1.1)
```

You have recently configured an IPsec VPN between an SRX Series device and another non- Junos security device. The phase one tunnel is up but the phase two tunnel is not present.

Referring to the exhibit, what is the cause of this problem?

A. preshared key mismatch

B. mode mismatch

C. proposal mismatch

D. proxy-ID mismatch

Correct Answer: D

QUESTION 12

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 13

The IPsec VPN on your SRX Series device establishes both the Phase 1 and Phase 2 security associations. Users are able to pass traffic through the VPN. During peak VPN usage times, users complain about decreased performance. Network connections outside of the VPN are not seriously impacted.

Which two actions will resolve the problem? (Choose two.)

A. Lower the MTU size on the interface to reduce the likelihood of packet fragmentation.

B. Verify that NAT-T is not disabled in the properties of the phase 1 gateway.

C. Lower the MSS setting in the security flow stanza for IPsec VPNs.

D. Verify that the PKI certificate used to establish the VPN is being properly verified using either the CPL or OCSP.

Correct Answer: AC

QUESTION 14

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 15

You have installed a new IPS license on your SRX device and successfully downloaded the attack signature database. However, when you run the command to install the database, the database fails to install. What are two reasons for the failure? (Choose two.)

A. The file system on the SRX device has insufficient free space to install the database.

B. The downloaded signature database is corrupt.

C. The previous version of the database must be uninstalled first.

D. The SRX device does not have the high memory option installed.

Correct Answer: AB