



Vendor: Juniper

Exam Code: JN0-632

Exam Name: Security, Professional (JNCIP-SEC)

Version: DEMO

QUESTION 1

Which two configuration tasks should you use to implement filter-based forwarding? (Choose two.)

- A. Create a VRF routing instance.
- B. Create a firewall filter with an action of virtual-channel
- C. Create routing options with rib-groups.
- D. Create routing options with interface routes.

Answer: CD

QUESTION 2

Your corporate network consists of a central office and four branch offices. You are responsible for coming up with an effective solution to provide secure connectivity between the sites. Which solution meets the requirements?

- A. Implement firewall filters on each device.
- B. Implement an HTTPS-based mesh between all sites.
- C. Implement secure routing policies.
- D. Implement a hub-and-spoke VPN.

Answer: D

QUESTION 3

You have been asked to configure a signature to block an attack released by a security vulnerability reporting agency. Which two characteristics of the attack must you understand to configure the attack object? (Choose two)

- A. the source IP address of the attacker
- B. the protocol the attack is transported in
- C. a string or regular expression that occurs within the attack
- D. IPv4 routing header

Answer: BC

QUESTION 4

In a group VPN topology, you have three members A, B, and C. You want A to communicate with B using a different encryption key from the one it uses to communicate with C. How do you achieve this?

- A. You put A, B, and C in three different groups
- B. You put A, B, and C in the same group, but you define a different match-policy for communication between A and B and for communication between A and C
- C. You define a different SA and a different match-policy for communication between A and B and for communication between A and C.
- D. In a group VPN, all members of a group must use the same key to communicate with each other.

Answer: D

QUESTION 5

Click the Exhibit button. The client is downloading a file from the FTP server. The FTP control channel is established using a security policy named trust-to-untrust. Which statement is correct about the output in the exhibit regarding the data channel?



```
user@srx# run show security flow session extensive
""
Session ID: 8444, Status: Normal
Flag: 0x0001000
Policy name: trust-to-untrust/6
Source NAT pool: Null
Maximum timeout: 2, Current timeout: 2
Session State: Valid
Start time: 1559573, Duration: 0
Client: FTP ALG, Group: 1, Resource: 1
In: 11.1.1.10/20 --> 10.1.1.10/52304;tcp,
Interface: ge-0/0/2.0,
Session token: 0x7, Flag: 0x0x21
Route: 0x0010, Gateway: 11.1.1.10, Tunnel: 0
Port sequence: 0, FIN sequence: 0,
FIN state: 2,
Pkts: 5, Bytes: 330
Out: 10.1.1.10/52304 --> 11.1.1.10/20;tcp,
Interface: ge-0/0/1.0,
Session token: 0x6, Flag: 0x0x20
Route: 0x0010, Gateway: 10.1.1.10, Tunnel: 0
Port sequence: 0, FIN sequence: 0,
FIN state: 2,
Pkts: 4, Bytes: 208
Total sessions: 2
```

- A. Passive FTP is being used to establish the data channel.
- B. The pinhole has been opened by the FTP ALG for return traffic.
- C. The session requires a separate security policy for return traffic.
- D. The session is using NAT to translate IP addresses.

Answer: B

QUESTION 6

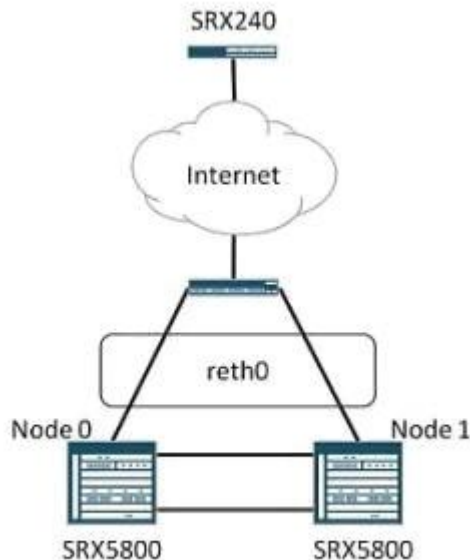
You are implementing a chassis cluster and adding the cluster to your multicast domain. Which two statements are valid considerations for this implementation scenario? (Choose two.)

- A. Multicast sessions are only maintained on the primary node in the cluster and will not be maintained during a failover scenario.
- B. Multicast sessions are synchronized on both nodes within the cluster and will be maintained during a failover scenario.
- C. The ppe and ppd interfaces are used to enable a cluster to act as a rendezvous point (RP) or first hop router in the multicast domain.
- D. The pe and pd interfaces are used to enable a cluster to act as a rendezvous point (RP) or first hop router in the multicast domain.

Answer: BC

QUESTION 7

Click the Exhibit button. In the exhibit, a site-to-site IPSec tunnel between the chassis cluster and the remote SRX240 device will not establish. The chassis cluster and the remote SRX240 device are using their loopback interfaces for IPSec tunnel termination. What is causing the problem?



- A. Site-to-site IPSec VPNs are not supported on a chassis cluster; a GRE tunnel must be used instead.
- B. Loopback interface IPSec tunnel termination is not supported on high-end SRX Series chassis clusters; use the reth0 interface instead.
- C. Site-to-site IPSec VPNs between high-end SRX Series chassis clusters and branch SRX devices are not supported. The SRX240 device must be replaced with a high-end SRX device
- D. Loopback interface IPSec tunnel termination within a chassis cluster must have PFS enabled Configure PFS on both ends of the IPSec tunnel.

Answer: B

QUESTION 8

In terms of application and protocol recognition, how does the IPS engine inspect the traffic?

- A. unidirectional on the incoming interface
- B. unidirectional on the outbound interface
- C. only traffic from and to well-known ports
- D. bidirectionally

Answer: D

QUESTION 9

Your company has installed a new transparent proxy server that it wants all employee traffic to traverse before taking the default route to the Internet. The proxy server is within two DMZ zones from the SRX Series device, which means your SRX device must now have two default routes:

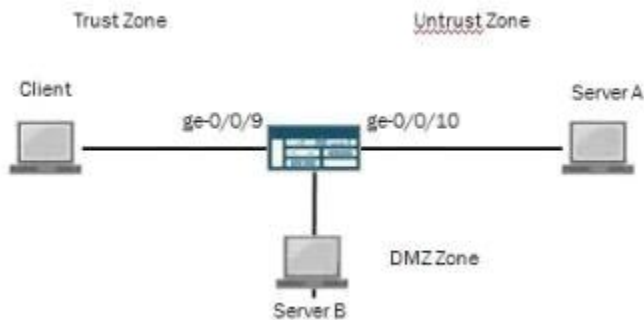
one to the proxy DMZ and one to the Internet from the proxy DMZ. What can you do to get the traffic to flow to the transparent proxy DMZ, and then from the proxy DMZ to the Internet, regardless of the destination or port?

- A. Configure two static default floating routes: one from the employee zone to the ingress proxy DMZ and a second from the egress proxy DMZ to the Internet.
- B. Configure two separate routing instances: one instance for the employee zone to the ingress proxy DMZ and the second for the egress proxy DMZ to the Internet.
- C. Configure security policies that will route all traffic to the ingress proxy DMZ then traffic will follow the default route to the Internet from the egress proxy DMZ.
- D. Configure a rib-group to handle the two default routes between the ingress and egress zones of the new proxy.

Answer: B

QUESTION 10

Click the Exhibit button. In the exhibit, traffic from the client is routed to Server A by default you have just implemented filter-based forwarding to redirect specific traffic from the client to Server B. Server B will then send that traffic to Server A. After finalizing this implementation, you notice reverse traffic from Server A back to the client is being dropped. Which statement describes why the reverse traffic is being dropped?



- A. The filter-based forwarding unidirectional-only option has been enabled.
- B. The MAC caching configuration option has not been enabled.
- C. The Junos OS performs a route lookup on the reverse traffic and drops the traffic due to a zone mismatch.
- D. The Junos OS performs a security policy check in the fast path packet flow on traffic matched by a stateless filter.

Answer: C

Thank You for Trying Our Product

PassLeader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



10% Discount Coupon Code: STNAR2014