JN0-696

Security Support, Professional (JNCSP-SEC)

DEMO

https://www.islever.com/jn0-696.html
https://www.islever.com/juniper.html

QUESTION NO: 1

You are having problems establishing an IPsec tunnel between two SRX Series devices.

What are two explanations for this problem? (Choose two.)

A. proposal mismatch
B. antivirus configuration
C. preshared key mismatch
D. TCP MSS clamping is disabled

Answer: B,D
Explanation:

QUESTION NO: 2

Two SRX Series devices are having problems establishing an IPsec VPN session. One of the devices has a firewall filter applied to its gateway interface that rejects UDP traffic.

What would resolve the problem?

A. Disable the IKE Phase 1 part of the session establishment.
B. Disable the IKE Phase 2 part of the session establishment.
C. Change the configuration so that session establishment uses TCP.
D. Edit the firewall filter to allow UDP port 500.

Answer: A
Explanation:

QUESTION NO: 3

Your SRX Series device has the following configuration:

user@host> show security policies

...

Policy: my-policy, State: enabled, Index: 5, Sequence number: 1

Source addresses: any

Destination addresses: any

Applications: snmp

Action: reject

From zone: trust, To zone: untrust

...

When traffic matches my-policy, you want the device to silently drop the traffic; however, you notice that the device is replying with ICMP unreachable messages instead.

What is causing this behavior?

A. the snmp application
B. the reject action
C. the trust zone
D. the untrust zone

Answer: C
Explanation:

QUESTION NO: 4

You want to allow remote users using PCs running Windows 7 to access the network using an IPsec VPN. You implement a route-based hub-and-spoke VPN; however, users report that they are not able to access the network.

What is causing this problem?

A. The remote clients do not have proper licensing.
B. Hub-and-spoke VPNs cannot be route-based; they must be policy-based.
C. The remote clients' OS is not supported.
D. Hub-and-spoke VPNs do not support remote client access; a dynamic VPN must be implemented instead.

Answer: B
Explanation:

QUESTION NO: 5

You notice that the secondary node of a chassis cluster has become disabled.

What caused this behavior?

A. The fxp0 interface on the secondary device failed.
B. The control link between the devices failed.
C. A reth on the secondary device failed.
D. An IPsec tunnel between the two devices failed.

Answer: D
Explanation:

QUESTION NO: 6

Users at a branch office report that they cannot reach an internal Web server. The users connect through a single SRX Series device to reach the Web server. A security policy has been configured on the device that allows traffic to flow between interfaces in the Trust zone.

What is causing this problem?

A. The interface on the device that connects to the Web server is not in the Trust zone.
B. The IPsec VPN connection between the users and the Web server is down.
C. There is a host inbound traffic configuration problem.
D. There is an antispam configuration problem.

Answer: C
Explanation:

QUESTION NO: 7

You are asked to troubleshoot a user communication problem. Users connected to the Trust zone cannot communicate with other devices connected to the same zone. These users are able to communicate with other devices in all other zones.

How should you resolve this problem?

A. You must put each device in a separate subzone to allow internal communication.