Juniper

JN0-696 Exam

Security Support, Professional (JNCSP-SEC)

Version: 10.0

Question: 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: AC

Question: 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: D

Explanation:
UDP port 500 is used by IKE.

Question: 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: B

Question: 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: D

Question: 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: B

Question: 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: A

Explanation:
Host inbound traffic configuration is ignored as this is not destined to the device (SRX) itself.

Question: 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.
B. You must configure a security policy to allow intrazone communication.
C. You must enable the allow-internal parameter under the Trust security zone.
D. You must enable the all parameter for host inbound traffic for the zone.

Answer: B

Explanation:
References:
http://www.juniper.net/documentation/en_US/junos12.1×46/topics/example/security-srx-device-zone-and-policyconfiguring

Question: 8

You have implemented AppTrack on your SRX Series device to track YouTube streaming video usage in your network. However, many of the YouTube videos that your users are watching are shorter than five minutes. You notice that the statistics for starting these short YouTube videos are not being recorded by AppTrack.
Which two actions would allow AppTrack to record the statistics for these sessions? (Choose two.)

A. Change AppTrack to collect session information during shorter intervals.
B. Change AppTrack to collect session information when the session is first created.
C. Change AppTrack to collect session information for nested applications only.
D. Change AppTrack to collect session information for applications only.

Answer: AB

Explanation:
You need to change the interval to be a smaller window and you need to log at session creation.
References:
http://www.juniper.net/documentation/en_US/junos12.1/topics/example/app-track-configuring-

cli

Question: 9

While attempting to set up IDP on an SRX Series device, the IDP attack database fails to download. What is one reason for this behavior?

A. The device's Untrust zone to Trust zone security policy does not allow this traffic.
B. The device's configuration does not include the URL from which to retrieve the attack database.
C. A firewall filter applied to the loopback interface is preventing the download of the attack database.
D. The host inbound traffic has not been configured correctly.

Answer: B

Explanation:
Note: The scenarios, which might cause the above error, can be broadly classified as follows:
The SRX device does not have Internet connectivity.
The DNS server is not configured on the SRX device.
The SRX device does not have access to the SIG DB server.
Storage space in the Compact Flash is full.
References: http://kb.juniper.net/InfoCenter/index?page=content&id=KB23359

Question: 10

When attempting to delete IDP policies and configurations from an SRX Series device, a user enters these configuration commands:
Delete security idp
Commit
However, after the commit has completed, the configuration is still present under the [edit security idp] hierarchy.
What should the user do to permanently remove the configuration?

A. Delete the /var/db/scripts/commit/templates.xsl file and reboot the device.
B. Delete the [edit security idp] hierarchy, commit the change, and immediately reboot the device.
C. Stop the idpd process using the set system processes idp-policy disable configuration command, committhe change, delete the [edit security idp] hierarchy, and then commit that change.
D. Delete the IDP templates commit script from the [edit system scripts commit] hierarchy, delete the [editsecurity idp] hierarchy, and then commit the change.

Answer: D

Explanation:
References: https://kb.juniper.net/InfoCenter/index?page=content&id=KB27182&actp=search

Thank You for trying JN0-696 PDF Demo

To Buy Latest JN0-696 Full Version Download visit link below

https://www.certkillers.net/Exam/JN0-696

Start Your JN0-696 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your JN0-696 preparation with actual exam questions.