HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **JN0-696**

Title : Security Support, Professional (JNCSP-SEC)

Version : DEMO

1.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

2.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: A,C

3.You recently configured the antivirus feature profile on your Junos device. The security policy is sending traffic for antivirus scanning. However, the traffic is being blocked and you repeatedly receive the system log message that the scan engine is not ready. You must not allow the traffic to be dropped when the scan engine is not ready.
Which action will resolve this problem?
A. Configure antivirus trickling to prevent the scan engine from timing out.
B. Configure an antivirus file scanning extension list to reduce the number of files for scanning.
C. Configure an antivirus fallback option to permit the traffic when the scan engine is not ready.
D. Configure an antivirus content size limit to minimize the scanning of large files.
Answer: C
Explanation:
Configure a fallback so that no traffic gets dropped when you are scanning a lot or big files for instance. The size of the files that can be scanned can also be configured. References:
http://www.juniper.net/documentation/en_US/junos12.1/topics/reference/configuration-statement/security-editengine-not-ready-sophos-engine.html

4.Click the Exhibit button.

```
{primary:node0}
user@srx> show chassis cluster interfaces
Control link 0 name: fxp1
Control link status: Up

Fabric interfaces:
     Name      Child-interface     Status
     fab0      ge-0/0/2            up
     fab0
     fab1      ge-9/0/2            up
     fab1
Fabric link status: Up

Redundant-ethernet Information:
     Name      Status              Redundancy-group
     reth0     Down                1
     reth1     Down                1
     reth2     Down                Not configured
     reth3     Down                Not configured

Interface Monitoring:
     Interface      Weight    Status    Redundancy-group
     ge-0/0/1       255       Down      1
     ge-9/0/1       255       Up        1
     ge-9/0/0       255       Down      1
     ge-0/0/0       255       Down      1

{primary:node0} user@srx> show chassis cluster status

Cluster ID: 3
     Node name Priority  Status    Preempt   Manual failover
Redundancy-group: 0, Failover count: 1
     node0     254       primary   no        no
     node1     2         secondary no        no
Redundancy-group: 1, Failover count: 1
     node0     254       primary   no        no
     node1     1         secondary no        no
```

You are implementing a high availability chassis cluster on an SRX Series device. You would like to manage both devices through the J-Web utility. However, when you try to log in to the second device using SSL HTTP, you receive a message from your Web browser indicating that the message has timed out.

Why you are receiving this message?

A. There is a firewall policy blocking traffic to the control plane.

B. HTTP is not configured as host inbound traffic.

C. The incoming traffic is not being allowed on the correct port.

D. The rdp daemon is on standby on the secondary device.

Answer: A

5.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.html