Juniper

Exam JN0-696

Security Support, Professional (JNCSP-SEC)

Verson: Demo

[Total Questions: 10]

Question No : 1

You have deployed AppID on your SRX Series device. You want to block all HTTP connections. However, there is a packet-monitoring device that shows the SRX Series device is still allowing some packets through to the webservers on TCP port 80.

In this scenario, which statement is correct?

A. Traffic is hitting the default fall-back option.
B. The packet-monitoring device is allowing packets to TCP port 80.
C. After deploying AppID, this is a normal behavior.
D. There are new sessions matching the webservers on TCP port 80.

Answer: C

Explanation:

Note: The APPID (application identification) feature is a Junos OS feature that identifies applications as constituents of application groups in TCP/UDP/ICMP traffic.
References: http://www.juniper.net/techpubs/en_US/junos-mobility12.1/topics/concept/pcef-app-idoverview.html

Question No : 2

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

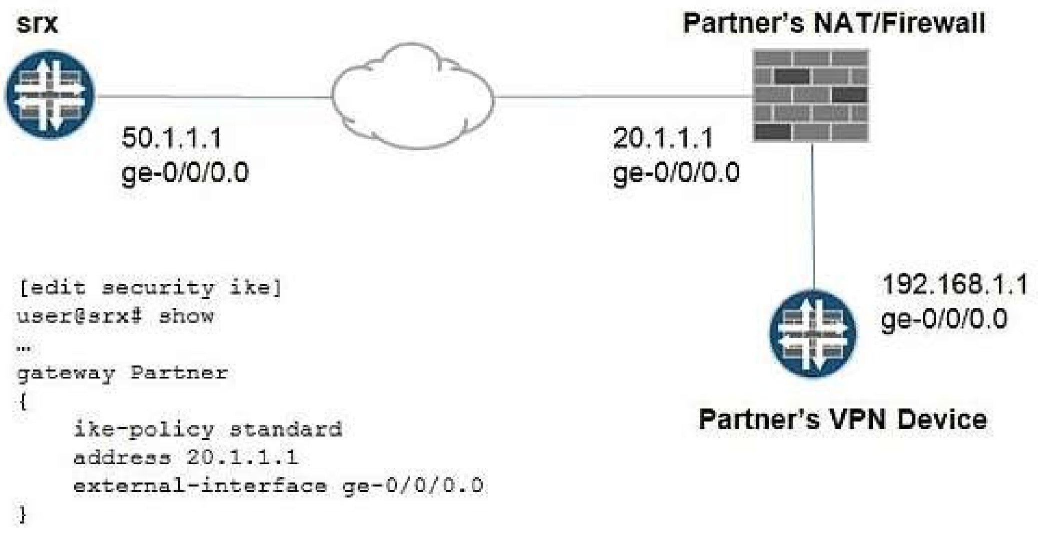
What are two explanations for this problem? (Choose two.)

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

Answer: A,C

Question No : 3

-- Exhibit –



```
[edit security ike]
user@srx# show
…
gateway Partner
{
    ike-policy standard
    address 20.1.1.1
    external-interface ge-0/0/0.0
}
```

-- Exhibit --

Click the Exhibit button.

You have created a new VPN tunnel to your partner's site but IKE Phase 1 is not coming up. You check the trace log and find the following log message:

Jun

[IKED 2] iked_pm_id_validate id NOT matched.

Considering the topology and the SRX Series device's configuration shown in the exhibit, which modification is needed under [edit security gateway Partner]?

A. rename address 20.1.1.1 to address 192.168.1.1
B. set remote-identity inet 192.168.1.1
C. set local-identity inet 20.1.1.1
D. set local-identity inet 50.1.1.1

Answer: B

Explanation:

You stablish the tunnel against a public IP of a firewall, which maps NAT to the private IP. The address is right, as you never been able to reach a private IP address through the internet.
You need to stablish the tunnel with the private IP, so the remote address command is the right choice.
References:
http://kb.juniper.net/InfoCenter/index?page=content&id=KB25462

Question No : 4

-- Exhibit –

-- Exhibit --

Click the Exhibit button.

There is an existing chassis cluster connected to the corporate network 192.168.1.0/24. You are asked to connect another department to this VLAN. To achieve this, you add a new chassis cluster to the network. After connecting to the network, the cluster experiences traffic problems. You have verified that the addresses and VLAN IDs are configured correctly.

Referring to the exhibit, which configuration would resolve this problem?

A. user@SRX-3> set chassis cluster cluster-id 1 node 0 rebootuser@SRX-4> set chassis cluster cluster-id 1 node 1 reboot
B. user@SRX-3# set chassis cluster redundancy-group 1 node 0 priority 100user@SRX-3# commit
C. user@SRX-3# set chassis cluster redundancy-group 1 preemptuser@SRX-3# commit
D. user@SRX-3> set chassis cluster cluster-id 2 node 0 rebootuser@SRX-4> set chassis cluster cluster-id 2 node 1 reboot

Answer: D
Explanation:

The reth MAC addresses are calculated based on the cluster IDs and two similar cluster IDs in the same network might cause a network impact due to overlapping virtual MAC entries.

Question No : 5

A customer downloaded and installed the IDP policy template. After copying the recommended templates and creating the needed policy, the customer deleted the templates. After the commit, the templates return.

Which command will prevent the templates from appearing again?

A. user@srx# deactivate security idp active-policy Recommended
B. user@srx# delete security idp idp-policy Recommended
C. user@srx# set security idp security-package automatic
D. user@srx# deactivate system scripts commit file templates.xsl

Answer: D

Explanation:

Delete or deactivate the commit script file. By deleting the commit script file, you avoid the risk of overwriting modifications to the template when you commit the configuration. Run one of the following commands:

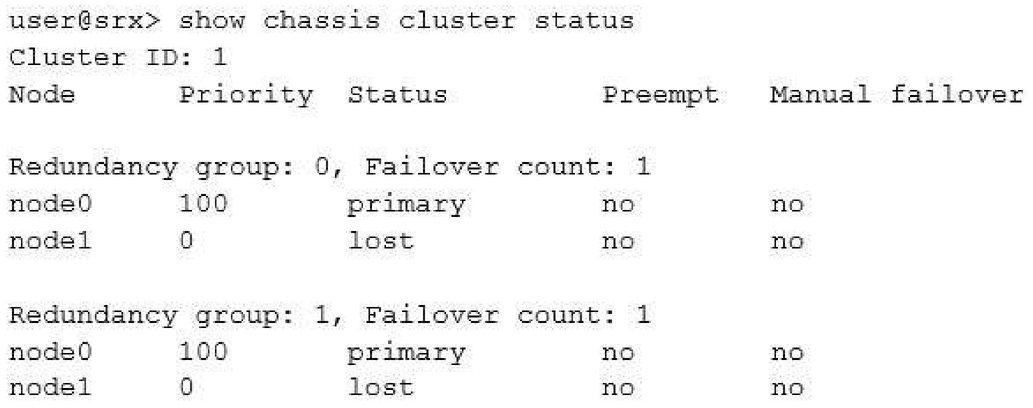
user@host# delete system scripts commit file templates.xsl user@host# deactivate system scripts commit file templates.xsl

References:

http://www.juniper.net/documentation/en_US/junos12.1x47/topics/task/configuration/idp-predefined-policytemplate-downloading-and-using-cli.html

Question No : 6

Click the Exhibit button.



```
user@srx> show chassis cluster status
Cluster ID: 1
Node       Priority  Status         Preempt   Manual failover

Redundancy group: 0, Failover count: 1
node0      100       primary        no        no
node1      0         lost           no        no

Redundancy group: 1, Failover count: 1
node0      100       primary        no        no
node1      0         lost           no        no
```

You recently configured a chassis cluster between two branch SRX Series devices and realize that the cluster is not functional, with node device status lost.

Referring to the exhibit, which two actions will correct this problem? (Choose two.)

A. Confirm both devices are synchronized with the local NTP.
B. Confirm that the software on both devices is the same Junos OS version.
C. Confirm both devices are running with the same security policies.
D. Confirm that the hardware on both devices is the same.

Answer: B,D

Explanation:

Chassis Cluster prerequisites include:

B: The SOFTWARE on both standalone devices must be the same Junos OS version.

Verify using this command on both devices:

root> show version

Model: srx220h

JUNOS Software Release [11.4R7.5]

D: Confirm that the HARDWARE on both devices is the same.

Verify using this command on both devices: root@srx220> show chassis hardware detail

References:

http://kb.juniper.net/InfoCenter/index?page=content&id=KB21312&actp=search

Question No : 7

You have an SRX branch device with two ISP connections. During analysis of the traffic, you notice that traffic from internal users to ISP 1 are replied to by ISP 2.

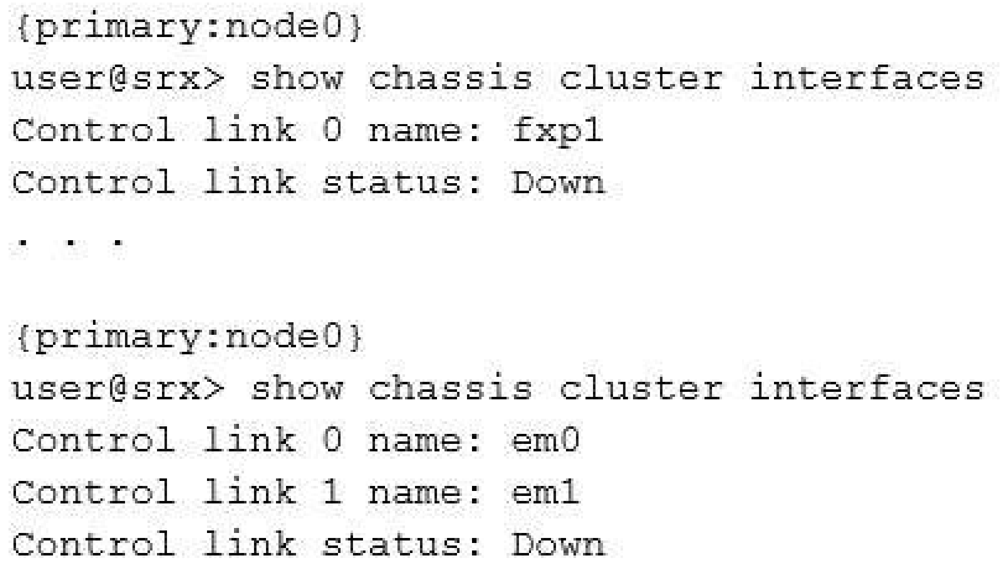
Which two configurations will correct the asymmetric problem? (Choose two.)

A. Create a security policy to allow traffic through ISP 1 only.
B. Create routing instances that include routes to ISP 1 and ISP 2.
C. Configure filter-based forwarding to provide load balancing.
D. Create an interface-specific firewall filter to forward the traffic to ISP 1.

Answer: A,B

Question No : 8

Click the Exhibit button.



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

{primary:node0}
user@srx> show chassis cluster interfaces
Control link 0 name: em0
Control link 1 name: em1
Control link status: Down
```

You are reviewing the status of a high-end SRX Series chassis cluster and notice that some interfaces have error messages.

Referring to the exhibit, which two steps would you use to troubleshoot the problem? (Choose two.)

A. Verify the security policies for incoming traffic.
B. Verify if there are Layer 1 or Layer 2 issues between the node devices.
C. Recognize the control link port to a different Services Processing Card (SPC), move the cable, and rebootboth nodes.
D. Reconfigure the firewall filters to allow traffic.

Answer: B,C

Explanation:

B: If the Control Link is SFP-type port, change the transceiver on both ends. Ensure that the transceivers are same type (LX, SX, etc.) and that they are Juniper-branded parts.
C: Change the cable that you are using for control link. Is the interface link light GREEN now?
Yes - Previous link cable was faulty. Recommend to now reboot both the nodes simultaneously.
References:
http://kb.juniper.net/InfoCenter/index?page=content&id=kb20698&actp=search

Question No : 9

You recently installed a new webserver which resides in the DMZ zone of an SRX Series device. However, the server is not accessible from any host in the Untrust zone.

Which two statements are true? (Choose two.)

A. A security policy must be configured to allow traffic from the Untrust zone destined to the DMZ zone.
B. The webserver and the SRX Series device must be configured to use the same NTP server.
C. The webserver's IP address must be represented in an address book entry on the SRX Series device.
D. The SRX Series device must be configured to allow SSH as host-inbound-traffic.

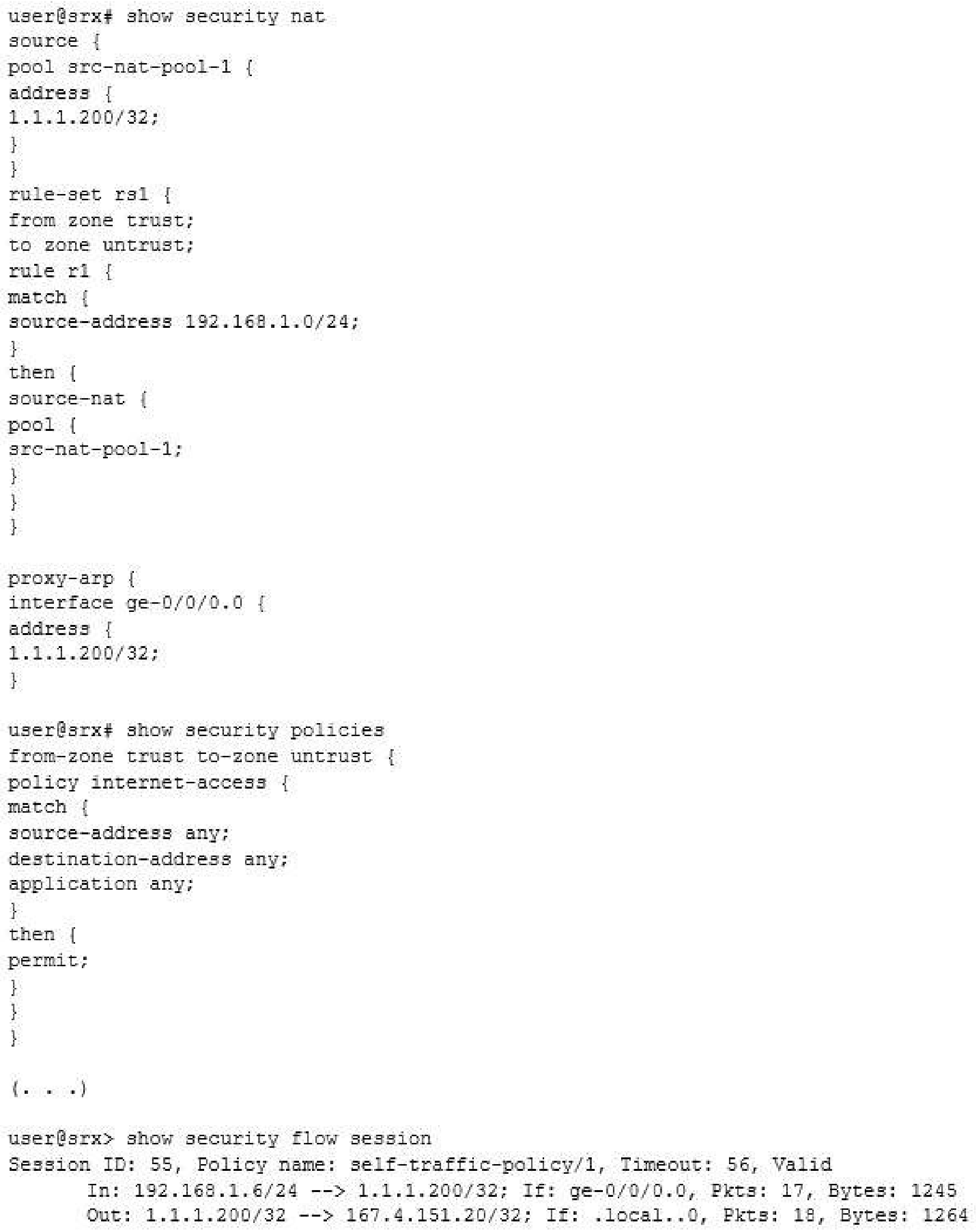
Answer: A,C

Explanation:

C: Example: set security zones security-zone dmz address-book address webserver 172.16.1.250/24 - Creates an address book entry for the webserver
References:
http://www.juniper.net/documentation/en_US/junos12.1x47/topics/example/security-srx-device-natconfiguring.html http://www.juniper.net/us/en/local/pdf/app-notes/3500153-en.pdf

Question No : 10

Click the Exhibit button.



```
user@srx# show security nat
source {
pool src-nat-pool-1 {
address {
1.1.1.200/32;
}
}
rule-set rs1 {
from zone trust;
to zone untrust;
rule r1 {
match {
source-address 192.168.1.0/24;
}
then {
source-nat {
pool {
src-nat-pool-1;
}
}
}

proxy-arp {
interface ge-0/0/0.0 {
address {
1.1.1.200/32;
}

user@srx# show security policies
from-zone trust to-zone untrust {
policy internet-access {
match {
source-address any;
destination-address any;
application any;
}
then {
permit;
}
}
}

(. . .)

user@srx> show security flow session
Session ID: 55, Policy name: self-traffic-policy/1, Timeout: 56, Valid
       In: 192.168.1.6/24 --> 1.1.1.200/32; If: ge-0/0/0.0, Pkts: 17, Bytes: 1245
       Out: 1.1.1.200/32 --> 167.4.151.20/32; If: .local..0, Pkts: 18, Bytes: 1264
```

You are asked to troubleshoot why users outside of the network cannot access internal resources. The network administrator says that NAT is configured on the SRX Series device and that it is working properly as shown in the exhibit. You realize that the current configuration is inadequate for this scenario.

Which two actions would resolve this problem? (Choose two.)

A. Configure destination NAT.
B. Configure the proxy ARP for 0.0.0.0/0.
C. Change the destination address in the security policy to 1.1.1.200.
D. Configure static one-to-one NAT.

Answer: A,C