

Vendor: Juniper

Exam Code: JN0-633

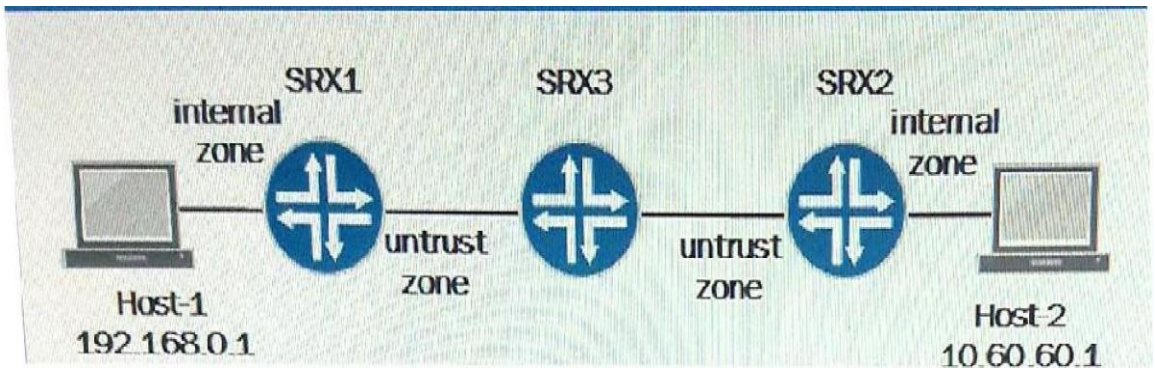
Exam Name: Security, Professional (JNCIP-SEC)

Version: DEMO

QUESTION 1
Click the Exhibit button.

```
[edit security nat static rule-set 12]
user@SRX2# show
from zone untrust;
rule 1 {
match {
destination-address 192.168.1.1/32;
}
then {
static-nat {
prefix {
10.60.60.1/32;
}
}
}
}
```

Host-2 initiates communication with Host-1.
All other routing and policies are in place to allow the traffic.
What is the result of the communication?



A. The 192.168.0.1 address is translated to the 10.60.60.1 address.
B. The 10.60.60.1 address is translated to the 192.168.1.1 address.
C. No translation occurs.
D. The 192.168.0.1 address is translated to the 192.168.1.1 address.

Answer: B

QUESTION 2
You have configured an IPsec VPN with traffic selectors; however, your IPsec tunnel does not appear to be working properly.
What are two reasons for the problem? (Choose two.)

A. You are configured a remote address value of 0.0.0.0/0.
B. You are trying to use traffic selectors with policy-based VPNs.
C. You have configured 15 traffic selectors on each SRX Series device.
D. You are trying to use traffic selectors with route-based VPNs.

Answer: AB

QUESTION 3
Click the Exhibit button.

```
user@host> show services application-identification application-system-
-cache
Application System Cache Configurations:
Application-cache: off
nested-application-cache: on
cache-unknown-result: on
cache-entry-timeout: 3600 seconds
```

You are using the application identification feature on your SRX Series device.
The help desk reports that users are complaining about slow Internet connectivity.
You issue the command shown in the exhibit.
What must you do to correct the problem?

A. Modify the configuration with thedelete services application-identification no-application- system-cachecommand and commit the change.
B. Modify the configuration with thedelete services application-identification no-clear- application-system-cachecommand and commit the change.
C. Reboot the SRX Series device.
D. Modify the configuration with thedelete services application-identification no-application - identification command and commit the change.

Answer: B

QUESTION 4
Click the Exhibit button.

```
user@host# run show security flow session
...
Session ID: 28, Policy name: allow/5, Timeout: 2, Valid
In: 172.168.1.2/24800 --> 66.168.100.100/8001; tcp, If: ge-0/0/3.0,
Pkts: 1, Bytes: 64
Out: 10.168.100.1/8001 --> 172.168.1.2/24800; tcp, If: ge-0/0/6.0,
Pkts: 1, Bytes: 40
```

Your customer is unable to reach your HTTP server that is connected to the ge-0/0/6 interface.
The HTTP server has an address of 10.168.100.1 on port 80 internally, but is accessed publicly using interface ge-0/0/3 with the address 66.168.100.100 on port 8001.
Referring to the exhibit, what is causing this problem?

A. The traffic is originated with incorrect IP address from the customer.
B. The traffic is translated with the incorrect IP address for the HTTP server.
C. The traffic is translated with the incorrect port number for the HTTP server.
D. The traffic is originated with the incorrect port number from the customer.

Answer: C

QUESTION 5
Click the Exhibit button.

```
user@host> monitor traffic interface ge-0/0/3
verbose output suppressed, use <detail> or <extensive> for full
protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup
delay.
Address resolution timeout is 4s.
Listening on ge-0/0/3, capture size 96 bytes
Reverse lookup for 172.168.3.254 failed (check DNS reachability).
Other reverse lookup
failures will not be reported.
Use <no-resolve> to avoid reverse lockups on IP addresses.
19:24:16.320907 In arp who-has 172.168.3.254 tell 172.168.3.1
19.24:17.322751 In arp
who has 172.168.3.254 tell 172.168.3.1 19.24:18.328895 In arp who-has
172.168.3.254 tell
172.168.3.1
19.24:18.332956 In arn who has 172.168.3.254 tell 172.168.3.1
```

A new server has been set up in your environment. The administrator suspects that the firewall is blocking the traffic from the new server. Previously existing servers in the VLAN are working correctly. After reviewing the logs, you do not see any traffic for the new server. Referring to the exhibit, what is the cause of the problem?

A. The server is in the wrong VLAN.
B. The server has been misconfigured with the wrong IP address.
C. The firewall has been misconfigured with the incorrect routing-instance.
D. The firewall has a filter enabled to blocktrafficfrom the server.

Answer: C

QUESTION 6
Which configuration statement would allow the SRX Series device to match a signature only on the first match, and not subsequent signature matches in a connection?

A. user@host# set security idp idp-policy test rulebase-ips rule 1 then action recommended
B. user@host# set security idp idp-policy test rulebase-ips rule 1 then action ignore- connection
C. user@host# set security idp idp-policy test rulebase-ips rule 1 then action no-action
D. user@host# set security idp idp-policy test rulebase-ips rule 1 then action drop-connection

Answer: B

QUESTION 7
The IPsec VPN on your SRX Series device establishes both the Phase 1 and Phase 2 security associations. Users are able to pass traffic through the VPN. During peak VPN usage times, users complain about decreased performance. Network connections outside of the VPN are not seriously impacted.
Which two actions will resolve the problem? (Choose two.)

A. Lower the MTU size on the interface to reduce the likelihood of packet fragmentation.
B. Verify that NAT-T is not disabled in the properties of the phase 1 gateway.
C. Lower the MSS setting in the security flow stanza for IPsec VPNs.

D. Verify that the PKI certificate used to establish the VPN is being properly verified using either the CPL or OCSP.

Answer: AC

QUESTION 8
You have initiated the download of the IPS signature database on your SRX Series device.
Which command would you use to confirm the download has completed?

A. request security idp security-package install
B. request security idp security-package download
C. request security idp security-package install status
D. request security idp security-package download status

Answer: D

QUESTION 9
You are asked to implement a Dynamic IPsec VPN on your new SRX240.
You are required to facilitate up to 5 simultaneous users.
Which two statements must be considered when accomplishing the task?

A. You must acquire at least three additional licenses.
B. Your devices must be in a chassis cluster.
C. You must be a policy-based VPN.
D. You must use main mode for your IKE phase 1 policy.

Answer: AC

QUESTION 10
You are using destination NAT to translate the address of your HTTPS server to a private address on your SRX Series device. You have decided to implement IDP SSL decryption.
Upon enabling the decryption, you notice sessions are not decrypted.
Which action resolves the problem?

A. Replace the server SSL certificate to use the public address.
B. Reboot the SRX Series device.
C. Increase the SSLsession-id-cache-timeoutvalue to any value greater than 5000 seconds.
D. Enable the IDPsensor-configurationdetector to detect address translation.

Answer: D

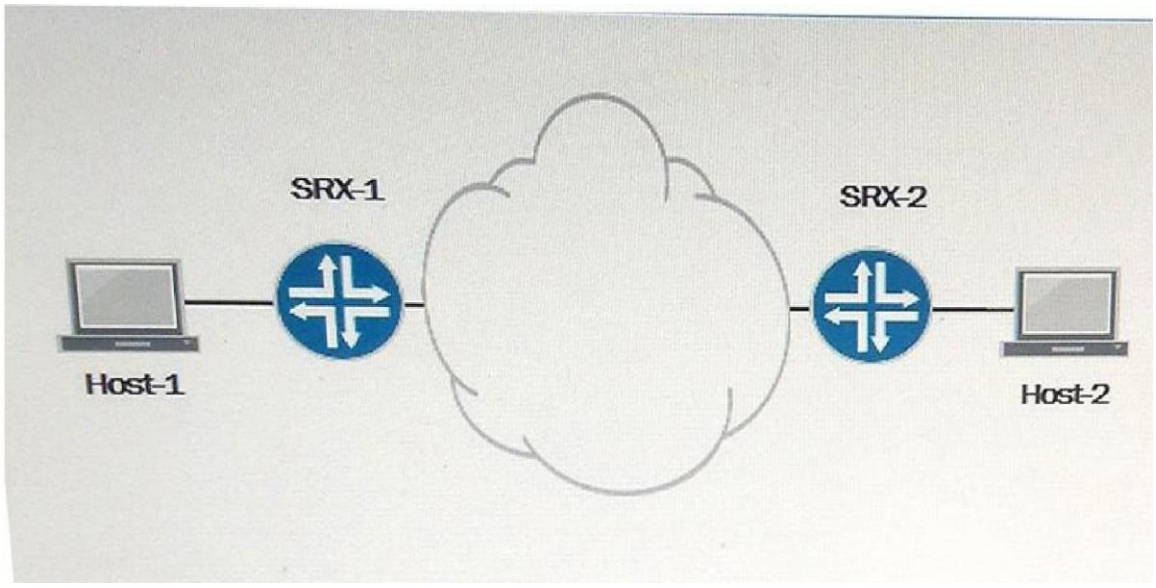
QUESTION 11
You are asked to ensure that your IPS engine blocks attacks. You must ensure that your system continues to drop additional malicious traffic without additional IPS processing for up to 30 minutes. You must ensure that the SRX Series device does send a notification packet when the traffic is dropped.
Which statement is correct?

A. Use the IP-Block action.

B. Use the Drop Packet action.
C. Use the Drop Connection action.
D. Use the IP-Close action.

Answer: D

QUESTION 12
Click the Exhibit button.Traffic is being sent from Host-1 to Host-2 through an IPsec VPN.
In this process, SRX-2 is using NAT to change the destination address of Host-2 from 192.168.1.1 to 10.60.60.1 SRX-1 uses the 172.31.50.1 address for its tunnel endpoint and SRX-2 uses the 10.10.50.1 address for its tunnel endpoint.



Referring to the exhibit, which statement is true?

A. The security policy on SRX-2 must permit traffic from the 172.31.50.1 destination address.
B. The security policy on SRX-2 must permit traffic from the 10.10.50.1destination address.
C. The security policy on SRX-2 must permit traffic from the 10.60.60.1 destination address.
D. The security policy on SRX-2 must permit traffic from the 192.168.1.1destination address.

Answer: C

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**