

JN0-633^{Q&As}

Security, Professional (JNCIP-SEC)

Pass Juniper JN0-633 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.certbus.com/jn0-633.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers

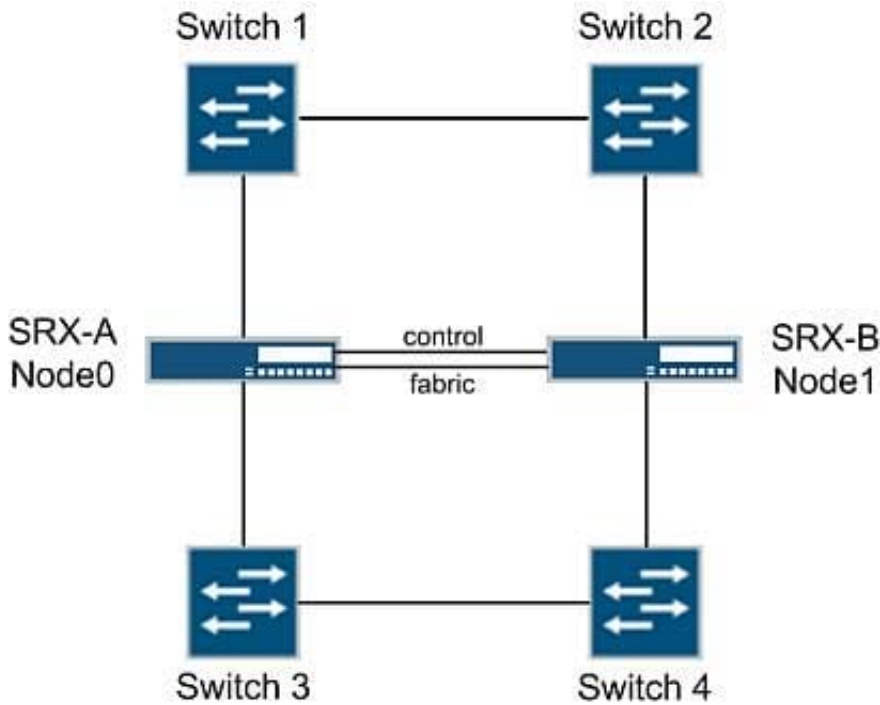


QUESTION 1

Click the Exhibit button.

Referring to the exhibit, a pair of SRX3600s is in an active/passive chassis cluster configured for transparent mode. Which type of traffic would traverse the secondary SRX3600 (node 1)?

Exhibit:



- A. all traffic including non-IP traffic
- B. any IP traffic
- C. only TCP and UDP traffic
- D. only BPDU traffic

Correct Answer: D

QUESTION 2

What is a benefit of using a dynamic VPN?

- A. It provides a layer of redundancy on top of a point-to-point VPN mesh architecture.
- B. It eliminates the need for point-to-point VPN tunnels.
- C. It provides a way to grant VPN access on a per-user-group basis.
- D. It simplifies IPsec access for remote clients.

Correct Answer: D

QUESTION 3

Your company's network has seen an increase in Facebook-related traffic. You have been asked to restrict the amount of Facebook-related traffic to less than 100 Mbps regardless of congestion. What are three components used to accomplish this task? (Choose three.)

- A. IDP policy
- B. application traffic control
- C. application firewall
- D. security policy
- E. application signature

Correct Answer: BDE

QUESTION 4

Click the Exhibit button.

```
Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:1.1.1.30/3389;6> matched filter MatchTraffic: Feb 2 09:00:02
09:00:00.1872004:CID-0:RT:packet [48] ipid = 5015, @423d7e9e Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:----
flow_process_pkt: (thd 1): flow_ctxt type 13, common flag Ox0, mbuf Ox423d7d00 Feb 2 09:00:02
09:00:00.1872004:CID-0:RT: flow process pak fast ifl 72 In_ifp fe-0/0/7.0 Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:
fe-0/0/7.0:1.1.1.100/51303->1.1.1.30/3389, top, flag 2 syn Feb 2 09:00:02 09:00:00.1872004:CID-0:RT: find flow: table
Ox5258d7b0, hash 17008(Oxffff), sa 1.1.1.100, da 1.1.1.30, sp 51303, dp 3389, proto 6, tok 448 Feb 2 09:00:02
09:00:00.1872004:CID-0:RT: no session found, start first path. in_tunnel - 0, from_cp_flag - 0 Feb 2 09:00:02
09:00:00.1872004:CID-0:RT: flow_first_create_session Feb 2 09:00:02 09:00:00.1872004:CID-0:RT: flow
first_in_dst_nat: in , out dst_adr 1.1.1.30, sp 51303, dp 3389 Feb 2 09:00:02 09:00:00.1872004:CID-0:RT: chose
interface fe-0/0/7.0 as incoming nat if. Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:flow_first_rule_dst_xlate: packet
1.1.1.100->1.1.1.30 nsp2 0.0.0.0->192.168.224.30. Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:flow_first_routing: call
flow_route_lookup() src_ip 1.1.1.100, x_dst_ip 192.168.224.30, in ifp fe-0/0/7.0, out ifp N/A sp 51303, dp 3389, ip_proto
6, tos 0 Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:Doing DESTINATION addr route-lookup Feb 2 09:00:02
09:00:00.1872004:CID-0:RT: routed (x_dst_ip 192.168.224.30) from untrust (fe-0/0/7.0 in 0) to ge-0/0/0.0, Next-hop:
192.168.224.30 Feb 2 09:00:02 09:00:00.1872004:CID-0:RT: policy search from zone untrust-> zone trust Feb 2
09:00:02 09:00:00.1872004:CID-0:RT: policy has timeout 900 Feb 2 09:00:02 09:00:00.1872004:CID-0:RT: app 0,
timeout 1800s, curr ageout 20s Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:flow_first_src_xlate: src nat 0.0.0.0(51303)
to 192.168.224.30 (3389) returns status 1, rule/pool id 1/2. Feb 2 09:00:02 09:00:00.1872004:CID-0:RT: dip id = 2/0,
1.1.1.100/51303->192.168.224.3/48810 Feb 2 09:00:02 09:00:00.1872004:CID-0:RT: choose interface ge-0/0/0.0 as
outgoing phy if Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:is_loop_pak: No loop: on ifp: ge-0/0/0.0, addr:
192.168.224.30, rtt_idx:0 Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:sm_flow_interest_check: app_id 0, policy 9,
app_svc_en 0, flags Ox2. not interested Feb 2 09:00:02 09:00:00.1872004:CID-0:RT:sm_flow_interest_check: app_id 1,
policy 9, app_svc_en 0, flags Ox2. not interested Feb 2 09:00:02
09:00:00.1872004:CID-0:RT:flow_first_service_lookup(): natp(Ox51ee4680): app_id, 0(0). Feb 2 09:00:02
09:00:00.1872004:CID-0:RT: service lookup identified service O.
```

Referring to the exhibit, which two statements are correct? (Choose two.)

- A. The packet being inspected is a UDP packet.

- B. The incoming interface is fe-0/0/7.
- C. This traffic matches an existing flow.
- D. Source NAT is being used.

Correct Answer: BC

QUESTION 5

You have recently deployed a dynamic VPN. Some remote users are complaining that they cannot authenticate through the SRX device at the corporate network. The SRX device serves as the tunnel endpoint for the dynamic VPN. What are two reasons for this problem? (Choose two.)

- A. The supported number of users has been exceeded for the applied license.
- B. The users are connecting to the portal using Windows Vista.
- C. The SRX device does not have the required user account definitions.
- D. The SRX device does not have the required access profile definitions.

Correct Answer: AD

QUESTION 6

A security administrator has configured an IPsec tunnel between two SRX devices. The devices are configured with OSPF on the st0 interface and an external interface destined to the IPsec endpoint. The administrator notes that the IPsec tunnel and OSPF adjacency keep going up and down. Which action would resolve this issue?

- A. Create a firewall filter on the st0 interface to permit IP protocol 89.
- B. Configure the IPsec tunnel to accept multicast traffic.
- C. Create a /32 static route to the IPsec endpoint through the external interface.
- D. Increase the OSPF metric of the external interface.

Correct Answer: C

QUESTION 7

Click the Exhibit button.

An attacker is using a nonstandard port for HTTP for reconnaissance into your network. Referring to the exhibit, which two statements are true? (Choose two.)

Exhibit:

```
[edit security]
user@srx# show
idp {
  idp-policy NewPolicy {
    rulebase-ips {
      rule 1 {
        match {
          application junos-http;
        }
        then {
          action {
            drop-packet;
          }
        }
      }
    }
  }
}
```

- A. The IPS engine will not detect the application due to the nonstandard port.
- B. The IPS engine will detect the application regardless of the nonstandard port.
- C. The IPS engine will perform application identification until the session is established.
- D. The IPS engine will perform application identification until it processes the first 256 bytes of the packet.

Correct Answer: BD

QUESTION 8

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.

Correct Answer: AC

QUESTION 9

How does the SRX5800, in transparent mode, signal failover to the connected switches?

- A. It initiates spanning-tree BPDUs.
- B. It sends out gratuitous ARPs.
- C. It flaps the impaired interfaces.
- D. It uses an IP address monitoring configuration.

Correct Answer: B

QUESTION 10

You are asked to apply individual upload and download bandwidth limits to YouTube traffic. Where in the configuration would you create the necessary bandwidth limits?

- A. under the [edit security application-firewall] hierarchy
- B. under the [edit security policies] hierarchy
- C. under the [edit class-of-service] hierarchy
- D. under the [edit firewall policer] hierarchy

Correct Answer: D

QUESTION 11

You want to implement a hub-and-spoke VPN topology using a single logical interface on the hub. Which st0 interface configuration is correct for the hub device?

- A. [edit interfaces] user@srx# show st0 { multipoint

```
unit 0 {  
  
family inet {  
  
address 10.10.10.1/24;  
  
}  
  
}  
  
}
```

- B. [edit interfaces] user@srx# show st0 {

```
unit 0 {  
  
family inet {  
  
address 10.10.10.1/24;
```

}

}

}

C. [edit interfaces] user@srx# show st0 {

unit 0 {

point-to-point;

family inet {

address 10.10.10.1/24;

}

}

}

D. [edit interfaces] user@srx# show st0 {

unit 0 {

multipoint;

family inet {

address 10.10.10.1/24;

}

}

}

Correct Answer: D

QUESTION 12

You are deploying a standalone SRX650 in transparent mode for evaluation purposes in a potential client's network. The client will need to access the device to modify security policies and perform other various configurations. Where would you configure a Layer 3 interface to meet this requirement?

A. fxp0.0

B. vlan.1

C. irb.1

D. ge-0/0/0.0

Correct Answer: C

QUESTION 13

Microsoft has altered the way their Web-based Hotmail application works. You want to update your application firewall policy to correctly identify the altered Hotmail application. Which two steps must you take to modify the application? (Choose two.)

- A. user@srx> request services application-identification application copy junos:HOTMAIL
- B. user@srx> request services application-identification application enable junos:HOTMAIL
- C. user@srx# edit services custom application-identification my:HOTMAIL
- D. user@srx# edit services application-identification my:HOTMAIL

Correct Answer: AD

QUESTION 14

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

Correct Answer: D

QUESTION 15

You recently implemented application firewall rules on an SRX device to act upon encrypted traffic. However, the encrypted traffic is not being correctly identified. Which two actions will help the SRX device correctly identify the encrypted traffic? (Choose two.)

- A. Enable heuristics to detect the encrypted traffic.
- B. Disable the application system cache.
- C. Use the junos:UNSPECIFIED-ENCRYPTED application signature.
- D. Use the junos:SPECIFIED-ENCRYPTED application signature.

Correct Answer: AC
