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.pass4itsure.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

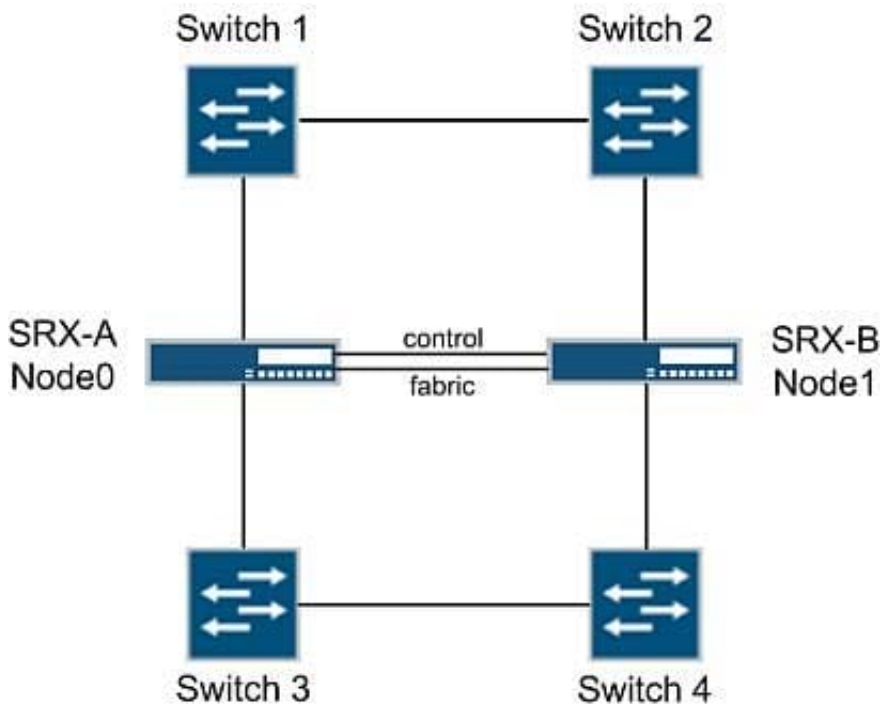**365 Days** Free Update

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

When configuring AutoVPN, which two actions are required for an administrator to establish communication from the hub site to the spoke sites? (Choose two.)

A. Configure the next hop tunnel binding (NHTB).

B. Configure static routes from the hub to the spoke.

C. Configure a dynamic routing protocol such as BGP, OSPF, or RIP on the tunnel interfaces.

D. Create a multipoint secure tunnel interface on the hub device.

Correct Answer: CD

QUESTION 3

A local user complains that they cannot connect to an FTP server on the DMZ network. You investigate and confirm that the security policy allows FTP traffic from the trust zone to the DMZ zone.

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

A. The FTP server has no route back to the local network.

B. No route is configured to the DMZ network.

C. No security policy exists for traffic from the DMZ zone to the trust zone.

D. The FTP ALG is disabled.

Correct Answer: AD

QUESTION 4

Which two configuration statements are used to share interface routes between routing instances? (Choose two.)

A. export-rib

B. static rib-group

C. interface-routes rib-group

D. import-rib

Correct Answer: CD

QUESTION 5

Click the Exhibit button.

root@host# show system login

user user { uid 2000; class operator; authentication {

encrypted-password "$1$4s7ePrk5$9S.MZTwmXTV7sovJZFFsw1"; ## SECRET-DATA] }

An SRX Series device has been configured for multiple certificate-based VPNs. The IPsec security association used for data replication is currently down . The administrator is a contractor and has the permissions on the SPX Series device as shown in the exhibit

Which command set would allow the administrator to troubleshoot the cause for the VPN being down?

A. set security ipsec traceoptions file ipsec set security ipsec traceoptions flag security-associations

B. set security ike traceoptions file ike set security ike traceoptions flag ike

C. request security pki verify-integrity-status

D. request security ike debug-enable local remote show security flow session Session ID. 7724, Policy namE. default-permit/4, Timeout: 2

 In: 1.1.70.6/17 --> 100.0.0.1/2326;icmp, IF. ge-0/0/3

 Out: 10.1.10.5/2326 --> 1.1.70.6/17;icmp, IF. ge-0/0/2

Session ID. 18408, Policy namE. default-permit/4, Timeout: 2 In: 10.1.10.5/64513 --> 1.1.70.6/512;icmp, IF. ge-0/0/2.0 Out: 1.1.70.6/512 --> 100.0.0.1/64513;icmp, IF. ge-0/0/3.10

-- Exhibit -

A user has reported a traffic drop issue between a host with the 10.1.10.5 internal IP address and a host with the 1.1.70.6 IP address. The traffic transits an SRX240 acting as a NAT translator. You are investigating the issue on the SRX240 using the output shown in the exhibit. Regarding this scenario, which two statements are true? (Choose two.)

A. The sessions shown indicate interface-based NAT processing.

B. The sessions shown indicate static NAT processing.

C. ICMP traffic is passing in both directions.

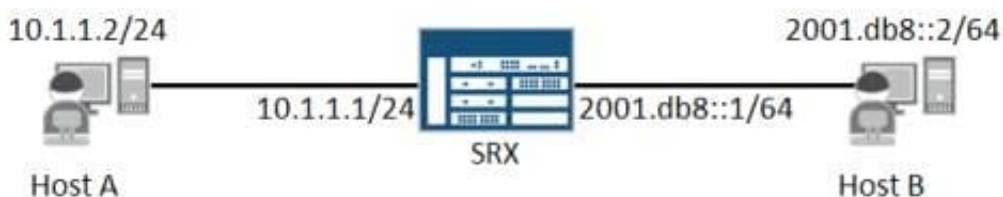D. ICMP traffic is passing in one direction.

Correct Answer: BC

QUESTION 9

Click the Exhibit button.

You are asked to implement NAT to translate addresses between the IPv4 and IPv6 networks shown in the

exhibit.

What are three configuration requirements? (Choose three.)

Exhibit:

A. Disable SYN checking.

B. Enable IPv6 flow mode.

C. Configure proxy ARP.

D. Configure stateless filtering.

E. Configure proxy NDP.

Correct Answer: BCE

QUESTION 10

An external host is attacking your network. The host sends an HTTP request to a Web server, but does not

include the version of HTTP in the request.

Which type of attack is being performed?

A. signature-based attack

B. application identification

C. anomaly

D. fingerprinting

Correct Answer: C

QUESTION 11

Click the Exhibit button.

You receive complaints from users that their Web browsing sessions keep dropping prematurely. Upon investigation, you find that the IDP policy shown in the exhibit is detecting the users\\' sessions as HTTP:WIN-CMD:WIN-CMD-EXE attacks, even though their sessions are not actual attacks. You must allow these sessions but still inspect for all other relevant attacks.

How would you configure your SRX device to meet this goal?

Exhibit:

```
[edit security idp]
user@srx# show
idp-policy basic {
    rulebase-ips {
        rule 1 {
            match {
                from-zone trust;
                source-address any;
                to-zone untrust;
                destination-address any;
                application default;
                attacks {
                    predefined-attack-groups "HTTP - All";
                }
            }
            then {
                action {
                    recommended;
                }
                notification {
                    log-attacks;
                }
            }
        }
    }
}
active-policy basic;
```

A. Create a new security policy that allows HTTP for all users and does not apply IDP.

B. Modify the security policy to add an application exception.

C. Modify the IDP policy to delete this particular attack from the IDP rulebase.

D. Modify the IDP policy to add an exempt rulebase rule to not inspect for this attack.

Correct Answer: D

QUESTION 12

You configured a custom signature attack object to match specific components of an attack:

HTTP-request Pattern .*\x90 90 90 ... 90 Direction: client-to-server

Which client traffic would be identified as an attack?

A. HTTP GET .*\x90 90 90 ... 90

B. HTTP POST .*\x90 90 90 ... 90

C. HTTP GET .*x909090 ... 90

D. HTTP POST .*x909090 ... 90

Correct Answer: A

QUESTION 13

[edit] useu@host# run show log debug Feb 3 22:04:32 22:04:31.983991:CID-0:RT:
ge-0/0/1.0:5.0.0.25/59028->25.0.0.25/23, tcp, flag 18

Feb 3 22:04:32 22:04:31.983997:CID-0:RT: find flow: table 0x582738c0, hash

53561(0xffff), sa 5.0.0.25, da 5.0.0.25, sp 59028, dp 23, proto 6, tok 20489 Feb 3 22:04:32
22:04:31.984004:CID-0:RT:Found: session id 0x14f98. sess tok 20489

Feb 3 22:04:32 22:04:31.984005:CID-0:RT: flow got session.

Feb 3 22:04:32 22:04:31.984006:CID-0:RT: flow session id 85912

Feb 3 22:04:32 22:04:31.984009:CID-0:RT: vector bits 0x2 vector 0x53a949e8

Feb 3 22:04:32 22:04:31.984012:CID-0:RT: tcp sec check.

Feb 3 22:04:32 22:04:31.984015:CID-0:RT:mbuf 0x4a82cd80, exit nh 0xa0010

Which two statements are true regarding the output shown in the exhibit? (Choose two.)

A. The outgoing interface is ge-0/0/1.0.

B. The packet is subject to fast-path packet processing.

C. The packet is part of the first-packet path processing.

D. TCP sequence checking is enabled.

Correct Answer: CD

QUESTION 14

You are asked to merge the corporate network with the network from a recently acquired company. Both networks use
the same private IPv4 address space (172.25.126.0/24). An SRX device serves as the gateway for each network. Which
solution allows you to merge the two networks without adjusting the current address assignments?

A. source NAT

B. persistent NAT

C. double NAT

D. NAT444

Correct Answer: C

QUESTION 15

Which QoS function is supported in transparent mode?

A. 802.1p

B. DSCP

C. IP precedence

D. MPLS EXP

Correct Answer: A