DUMPSBOSS.COM

Security-Professional (JNCIP-SEC)

Juniper JN0-635

Version Demo

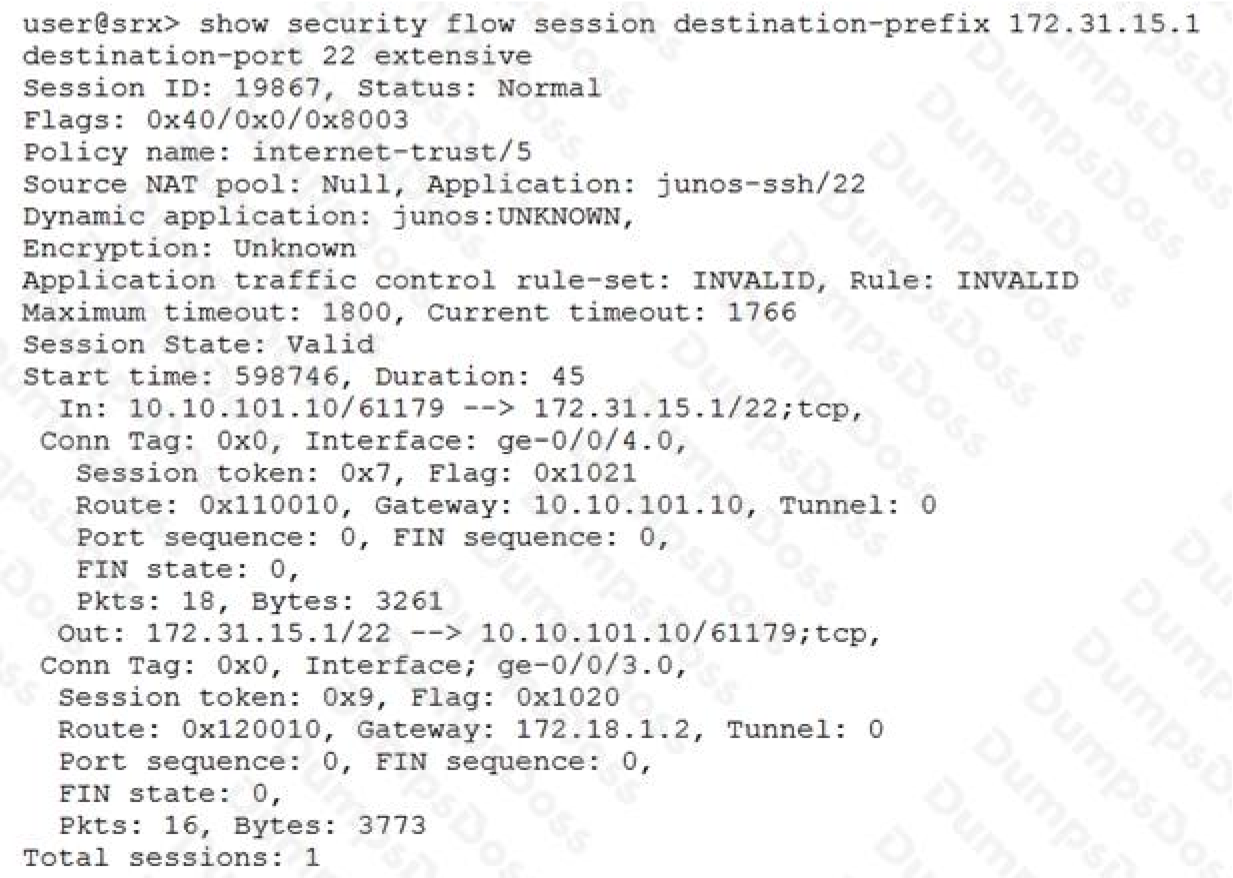
Total Demo Questions: 10

Total Premium Questions: 67

Buy Premium PDF

QUESTION NO: 1

Click the Exhibit button.



```
user@srx> show security flow session destination-prefix 172.31.15.1
destination-port 22 extensive
Session ID: 19867, Status: Normal
Flags: 0x40/0x0/0x8003
Policy name: internet-trust/5
Source NAT pool: Null, Application: junos-ssh/22
Dynamic application: junos:UNKNOWN,
Encryption: Unknown
Application traffic control rule-set: INVALID, Rule: INVALID
Maximum timeout: 1800, Current timeout: 1766
Session State: Valid
Start time: 598746, Duration: 45
  In: 10.10.101.10/61179 --> 172.31.15.1/22;tcp,
 Conn Tag: 0x0, Interface: ge-0/0/4.0,
   Session token: 0x7, Flag: 0x1021
   Route: 0x110010, Gateway: 10.10.101.10, Tunnel: 0
   Port sequence: 0, FIN sequence: 0,
   FIN state: 0,
   Pkts: 18, Bytes: 3261
  Out: 172.31.15.1/22 --> 10.10.101.10/61179;tcp,
 Conn Tag: 0x0, Interface; ge-0/0/3.0,
  Session token: 0x9, Flag: 0x1020
  Route: 0x120010, Gateway: 172.18.1.2, Tunnel: 0
  Port sequence: 0, FIN sequence: 0,
  FIN state: 0,
  Pkts: 16, Bytes: 3773
Total sessions: 1
```

Given the command output shown in the exhibit, which two statements are true? (Choose two.)

A. The host 172.31.15.1 is directly connected to interface ge-0/0/3.0

B. Traffic matching this session has been received since the session was established

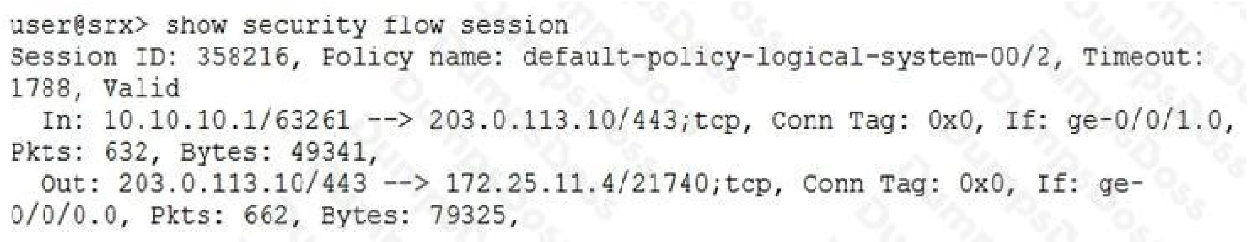
C. The host 10.10.101.10 is directly connected to interface ge-0/0/4.0

D. Network Address Translation is applied to this session

ANSWER: B C

QUESTION NO: 2

Click the Exhibit button.



```
user@srx> show security flow session
Session ID: 358216, Policy name: default-policy-logical-system-00/2, Timeout:
1788, Valid
  In: 10.10.10.1/63261 --> 203.0.113.10/443;tcp, Conn Tag: 0x0, If: ge-0/0/1.0,
Pkts: 632, Bytes: 49341,
  Out: 203.0.113.10/443 --> 172.25.11.4/21740;tcp, Conn Tag: 0x0, If: ge-
0/0/0.0, Pkts: 662, Bytes: 79325,
```

Referring to the exhibit, which statement is true?

A. Source NAT with PAT is occurring

B. Destination NAT is occurring

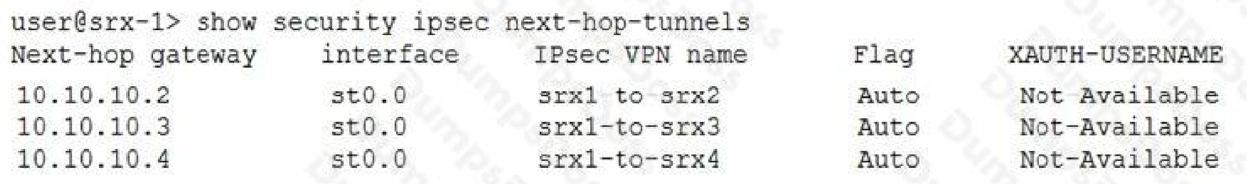
C. Static NAT without PAT is occurring

D. Source NAT without PAT is occurring

ANSWER: A

QUESTION NO: 3

Click the Exhibit button.



```
user@srx-1> show security ipsec next-hop-tunnels
Next-hop gateway    interface    IPsec VPN name      Flag     XAUTH-USERNAME
 10.10.10.2          st0.0        srx1 to srx2        Auto      Not Available
 10.10.10.3          st0.0        srx1-to-srx3        Auto      Not-Available
 10.10.10.4          st0.0        srx1-to-srx4        Auto      Not-Available
```

Which statement is correct regarding the information show in the exhibit?

A. The tunnel binding was discovered automatically

B. The output is for an ADVPN

C. The tunnel gateway address was automatically discovered

D. The tunnel is not encrypting the traffic

ANSWER: C

QUESTION NO: 4

You are asked to configure a new SRX Series CPE device at a remote office. The device must participate in forwarding MPLS and IPsec traffic.

Which two statements are true regarding this implementation? (Choose two.)

A. Host inbound traffic must not be processed by the flow module

B. Host inbound traffic must be processed by the flow module

C. The SRX Series device can process both MPLS and IPsec with default traffic handling

D. A firewall filter must be configured to enable packet mode forwarding

ANSWER: A D

QUESTION NO: 5

You correctly configured a security policy to deny certain traffic, but logs reveal that traffic is still allowed.

Which specific traceoption flag will help you troubleshoot this problem?

A. lookup

B. configuration

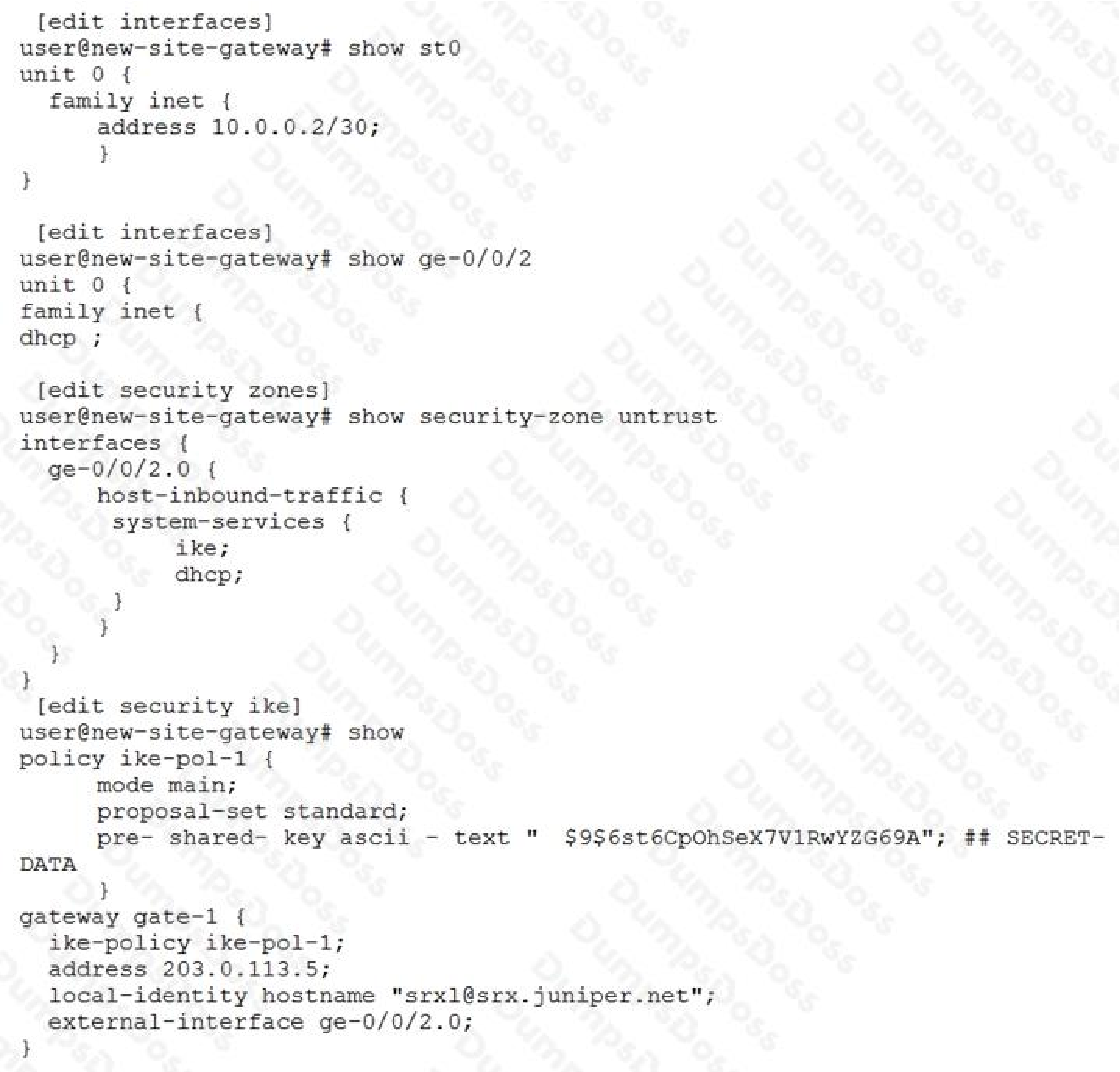
C. routing-socket

D. rules

ANSWER: D

QUESTION NO: 6

Click the Exhibit button.



```
 [edit interfaces]
user@new-site-gateway# show st0
unit 0 {
  family inet {
      address 10.0.0.2/30;
      }
}

 [edit interfaces]
user@new-site-gateway# show ge-0/0/2
unit 0 {
family inet {
dhcp ;

 [edit security zones]
user@new-site-gateway# show security-zone untrust
interfaces {
  ge-0/0/2.0 {
      host-inbound-traffic {
       system-services {
            ike;
            dhcp;
       }
      }
  }
}
 [edit security ike]
user@new-site-gateway# show
policy ike-pol-1 {
      mode main;
      proposal-set standard;
      pre- shared- key ascii - text "  $9$6st6CpOhSeX7V1RwYZG69A"; ## SECRET-
DATA
      }
gateway gate-1 {
  ike-policy ike-pol-1;
  address 203.0.113.5;
  local-identity hostname "srxl@srx.juniper.net";
  external-interface ge-0/0/2.0;
}
```

Your company has purchased a competitor and now must connect the new network to the existing one. The competitor's gateway device is receiving its ISP address using DHCP. Communication between the two sites must be secured; however, obtaining a static public IP address for the new site gateway is not an option at this time. The company has several requirements for this solution:

> A site-to-site IPsec VPN must be used to secure traffic between the two sites;

> The IKE identity on the new site gateway device must use the hostname option; and > Internet traffic from each site should exit through its local Internet connection.

The configuration shown in the exhibit has been applied to the new site's SRX, but the secure tunnel is not

working.

In this scenario, what configuration change is needed for the tunnel to come up?

A. Remove the quotes around the hostname

B. Bind interface st0 to the gateway

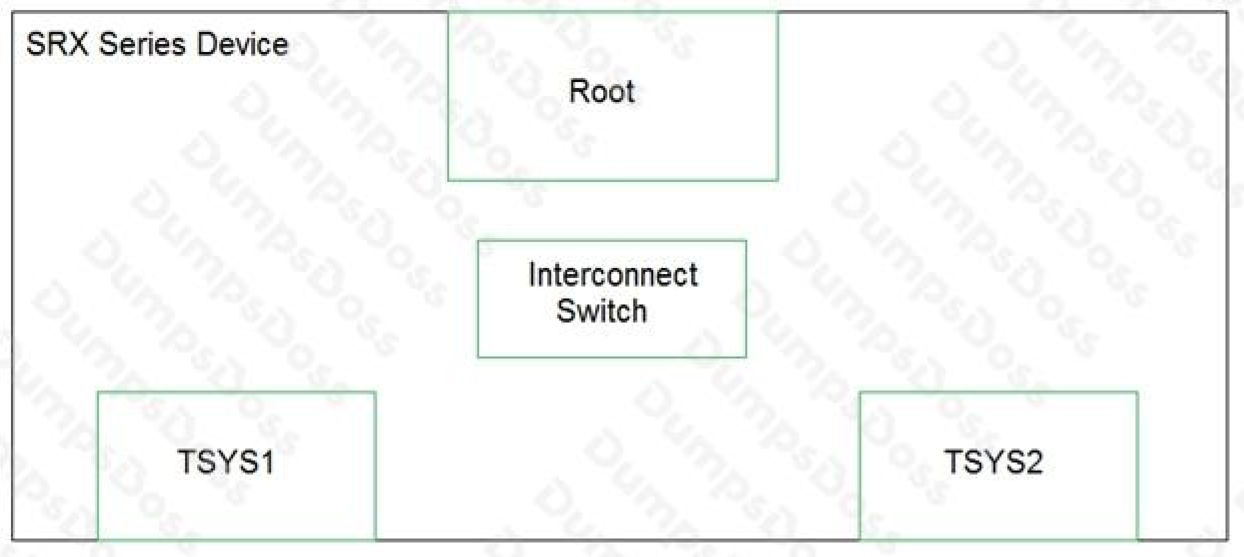
C. Change the IKE policy mode to aggressive

D. Apply a static address to ge-0/0/2

ANSWER: A

QUESTION NO: 7

Click the Exhibit button.



You have configured tenant systems on your SRX Series device.

Referring to the exhibit, which two actions should you take to facilitate inter-TSYS communication? (Choose two.)

A. Place the logical tunnel interfaces in a virtual router routing instance in the interconnect switch

B. Place the logical tunnel interfaces in a VPLS routing instance in the interconnect switch

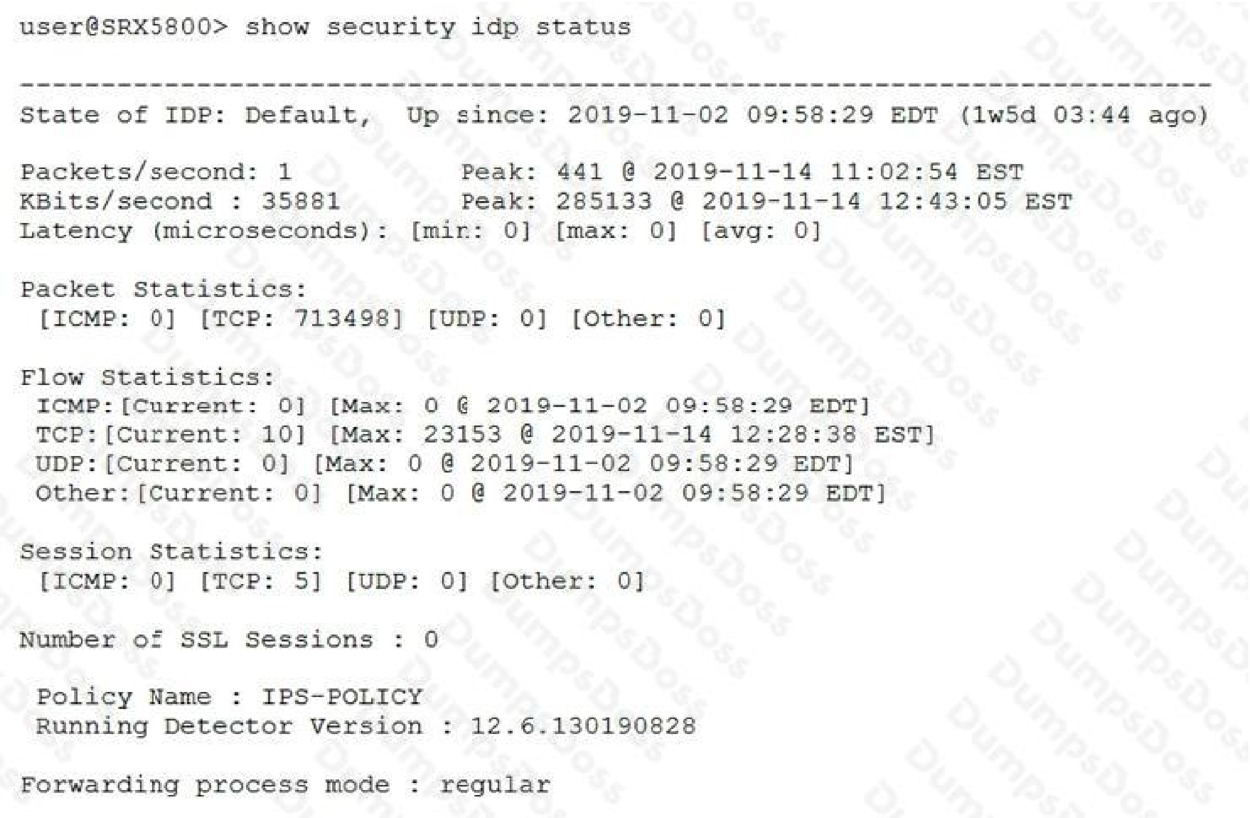
C. Connect each TSYS with the interconnect switch by configuring INET configured logical tunnel interfaces in the interconnect switch

D. Connect each TSYS with the interconnect switch by configuring Ethernet VPLS configured logical tunnel interfaces in the interconnect switch

ANSWER: A C

QUESTION NO: 8

Click the Exhibit button.



```
user@SRX5800> show security idp status

--------------------------------------------------------------------------
State of IDP: Default,  Up since: 2019-11-02 09:58:29 EDT (1w5d 03:44 ago)

Packets/second: 1            Peak: 441 @ 2019-11-14 11:02:54 EST
KBits/second : 35881         Peak: 285133 @ 2019-11-14 12:43:05 EST
Latency (microseconds): [min: 0] [max: 0] [avg: 0]

Packet Statistics:
 [ICMP: 0] [TCP: 713498] [UDP: 0] [Other: 0]

Flow Statistics:
 ICMP:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]
 TCP:[Current: 10] [Max: 23153 @ 2019-11-14 12:28:38 EST]
 UDP:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]
 Other:[Current: 0] [Max: 0 @ 2019-11-02 09:58:29 EDT]

Session Statistics:
 [ICMP: 0] [TCP: 5] [UDP: 0] [Other: 0]

Number of SSL Sessions : 0

 Policy Name : IPS-POLICY
 Running Detector Version : 12.6.130190828

Forwarding process mode : regular
```

Referring to the exhibit, which IPS deployment mode is running on the SRX5800 device?

A. sniffer mode

B. integrated mode

C. monitor mode

D. in-line tap mode

ANSWER: B

QUESTION NO: 9

You are asked to set up notifications if one of your collector traffic feeds drops below 100 kbps.

Which two configuration parameters must be set to accomplish this task? (Choose two.)

A. Set a traffic SNMP trap on the JATP appliance

B. Set a logging notification on the JATP appliance

C. Set a general triggered notification on the JATP appliance

D. Set a traffic system alert on the JATP appliance

ANSWER: B D

QUESTION NO: 10

You have a remote access VPN where the remote users are using the NCP client. The remote users can access

the internal corporate resources as intended; however, traffic that is destined to all other Internet sites is going through the remote access VPN. You want to ensure that only traffic that is destined to the internal corporate resources use the remote access VPN.

Which two actions should you take to accomplish this task? (Choose two.)

A. Enable the split tunneling feature within the VPN configuration on the SRX Series device

B. Enable IKEv2 within the VPN configuration on the SRX Series device

C. Configure the necessary traffic selectors within the VPN configuration on the SRX Series device

D. Configure split tunneling on the NCP profile on the remote client

ANSWER: C D