Vendor: Juniper

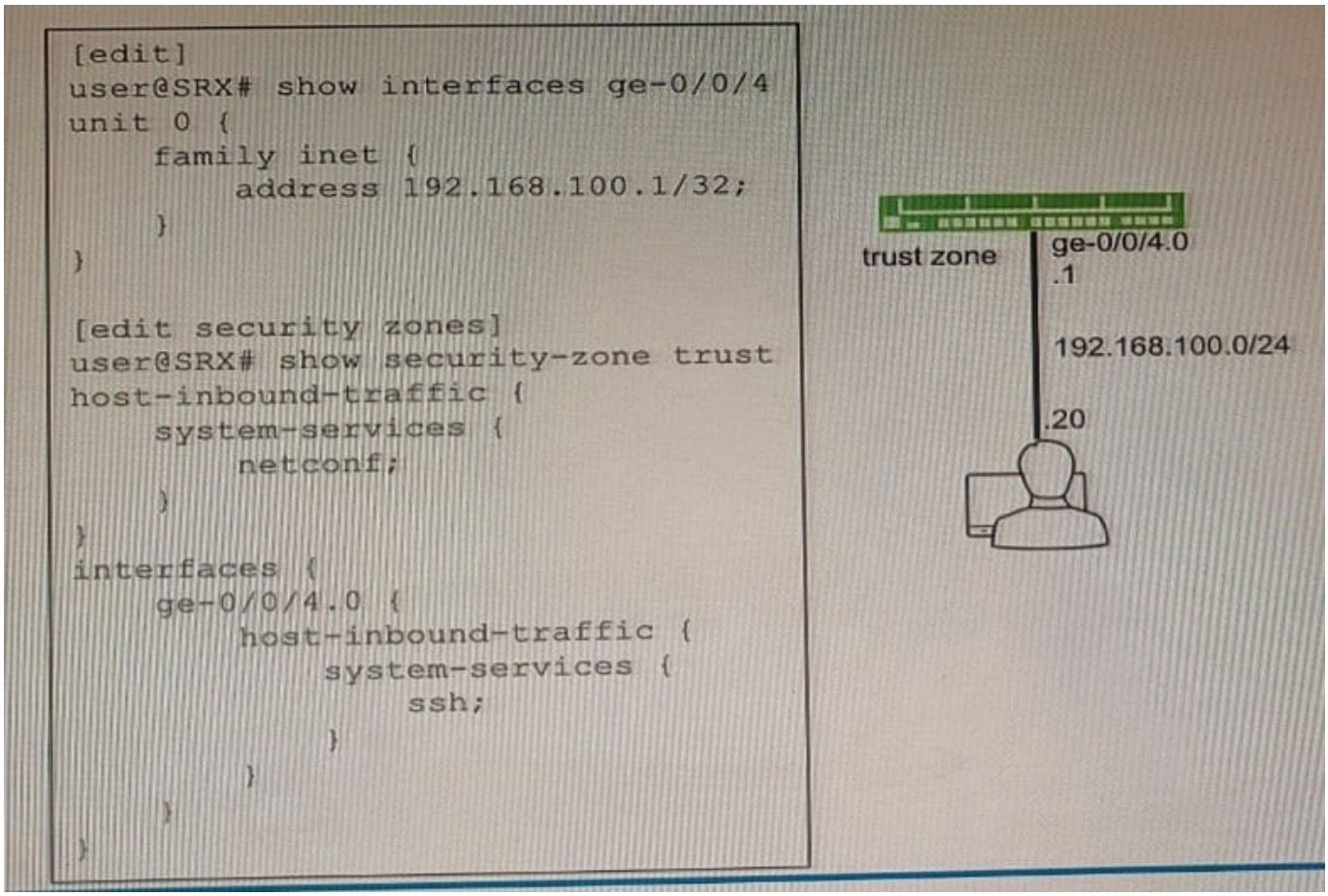
Exam Code:JN0-636

Exam Name: Service Provider Routing and Switching Professional (JNCIP-SP)

Version: Demo

QUESTION 1

Exhibit



You are not able to ping the default gateway of 192.168 100 1 (or your network that is located on your SRX Series firewall. Referring to the exhibit, which two commands would correct the configuration of your SRX Series device? (Choose two.)

A.
```
[edit security zones security-zone trust]
user@SRX# set interfaces ge-0/0/4.0 host-inbound-traffic system-services ping
```

B.
```
[edit interfaces ge-0/0/4]
user@SRX# replace pattern 32 with 24
```

C.
```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping
```

D.
```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping except
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 2

You configured a chassis cluster for high availability on an SRX Series device and enrolled this HA cluster with the Juniper ATP Cloud. Which two statements are correct in this scenario? (Choose two.)

A. You must use different license keys on both cluster nodes.

B. When enrolling your devices, you only need to enroll one node.

C. You must set up your HA cluster after enrolling your devices with Juniper ATP Cloud

D. You must use the same license key on both cluster nodes.

Correct Answer: BD

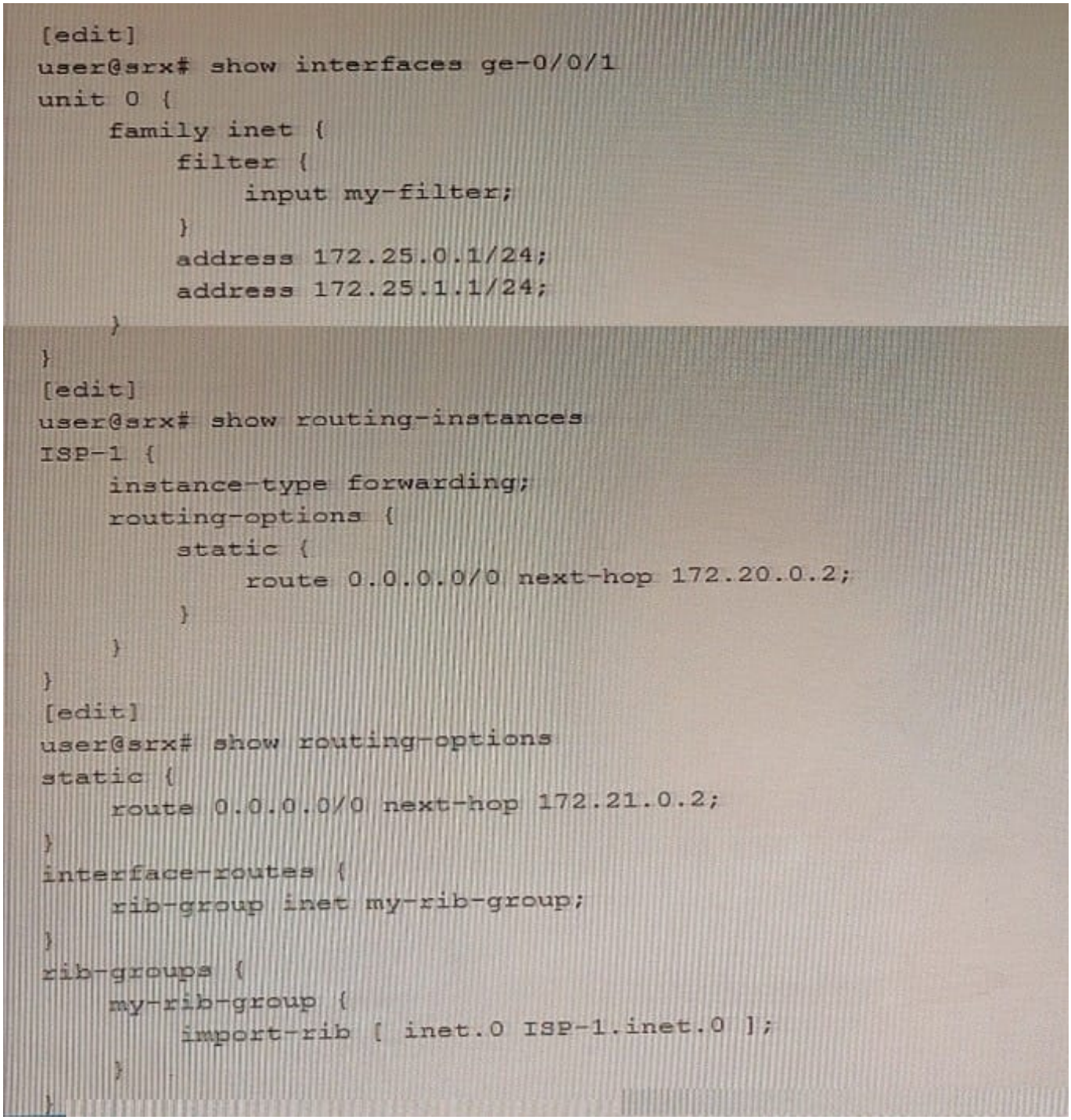
When enrolling your devices, you only need to enroll one node: The Juniper ATP Cloud automatically recognizes the HA configuration and applies the same license and configuration to both nodes of the cluster.

You must use the same license key on both cluster nodes: The HA cluster needs to share the same license key in order to be recognized as a single device by the Juniper ATP Cloud.

You must set up your HA cluster before enrolling your devices with Juniper ATP Cloud. And it is not necessary to use different license keys on both cluster nodes because the HA cluster shares the same license key.

QUESTION 3

Exhibit



```
[edit]
user@srx# show interfaces ge-0/0/1
unit 0 {
    family inet {
        filter {
            input my-filter;
        }
        address 172.25.0.1/24;
        address 172.25.1.1/24;
    }
}
[edit]
user@srx# show routing-instances
ISP-1 {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 172.20.0.2;
        }
    }
}
[edit]
user@srx# show routing-options
static {
    route 0.0.0.0/0 next-hop 172.21.0.2;
}
interface-routes {
    rib-group inet my-rib-group;
}
rib-groups {
    my-rib-group {
        import-rib [ inet.0 ISP-1.inet.0 ];
    }
}
```

You are implementing filter-based forwarding to send traffic from the 172.25.0.0/24 network through ISP-1 while sending all other traffic through your connection to ISP-2. Your ge- 0/0/1 interface connects to two networks, including the 172.25.0.0/24 network. You have implemented the configuration shown in the exhibit. The traffic from the 172.25.0.0/24 network is being forwarded as expected to 172.20.0.2, however traffic from the other network (172.25.1.0/24) is not being forwarded to the upstream 172.21.0.2 neighbor.

In this scenario, which action will solve this problem?

A. You must specify that the 172.25.1.1/24 IP address is the primary address on the ge- 0/0/1 interface.

B. You must apply the firewall filter to the lo0 interface when using filter-based forwarding.

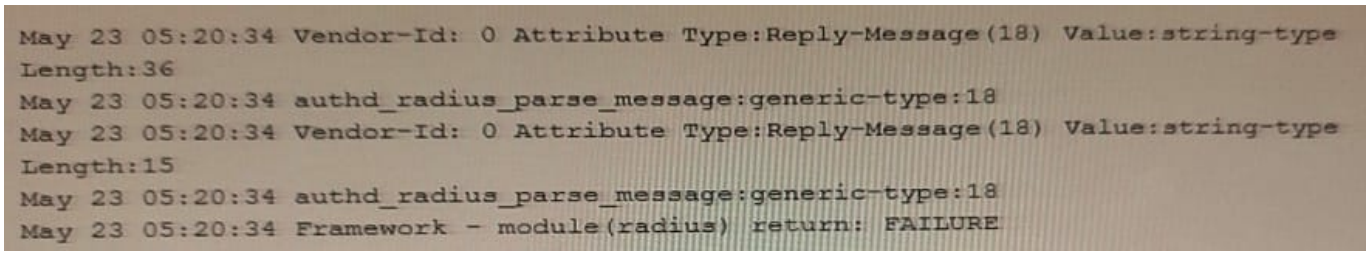
C. You must add another term to the firewall filter to accept the traffic from the 172.25.1.0/24 network.

D. You must create the static default route to neighbor 172.21 0.2 under the ISP-1 routing instance hierarchy.

Correct Answer: D

QUESTION 4

Exhibit



You configure a traceoptions file called radius on your returns the output shown in the exhibit What is the source of the problem?

A. An incorrect password is being used.

B. The authentication order is misconfigured.

C. The RADIUS server IP address is unreachable.

D. The RADIUS server suffered a hardware failure.

Correct Answer: D

QUESTION 5

According to the log shown in the exhibit, you notice the IPsec session is not establishing. What is the reason for this behavior?

A. Mismatched proxy ID

B. Mismatched peer ID

C. Mismatched preshared key

D. Incorrect peer address.

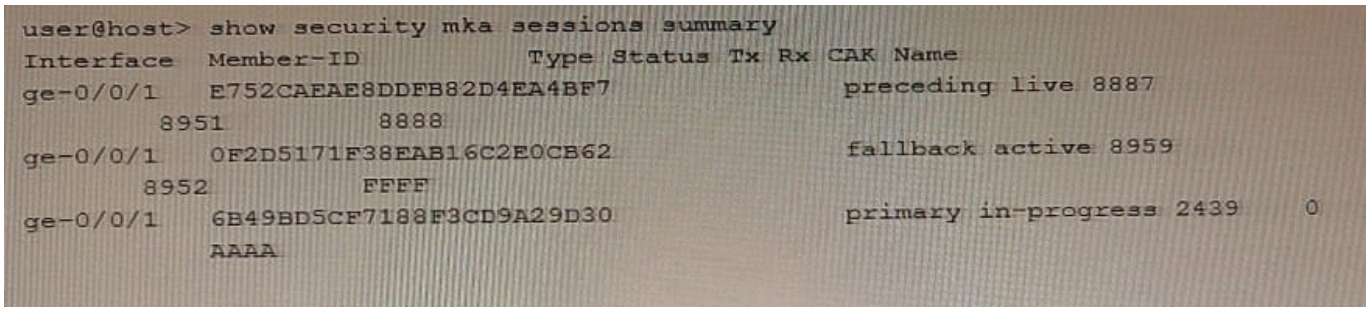
Correct Answer: B

Explanation: https://www.juniper.net/documentation/en_US/release- independent/nce/topics/example/policy-based-vpn-using-j-series-srxseries-device- configuring.html

---

QUESTION 6

Exhibit



Referring to the exhibit, which two statements are true about the CAK status for the CAK named "FFFP"? (Choose two.)

A. CAK is not used for encryption and decryption of the MACsec session.

B. SAK is successfully generated using this key.

C. CAK is used for encryption and decryption of the MACsec session.

D. SAK is not generated using this key.

Correct Answer: CD

QUESTION 7

Regarding IPsec CoS-based VPNs, what is the number of IPsec SAs associated with a peer based upon?

A. The number of traffic selectors configured for the VPN.

B. The number of CoS queues configured for the VPN.

C. The number of classifiers configured for the VPN.

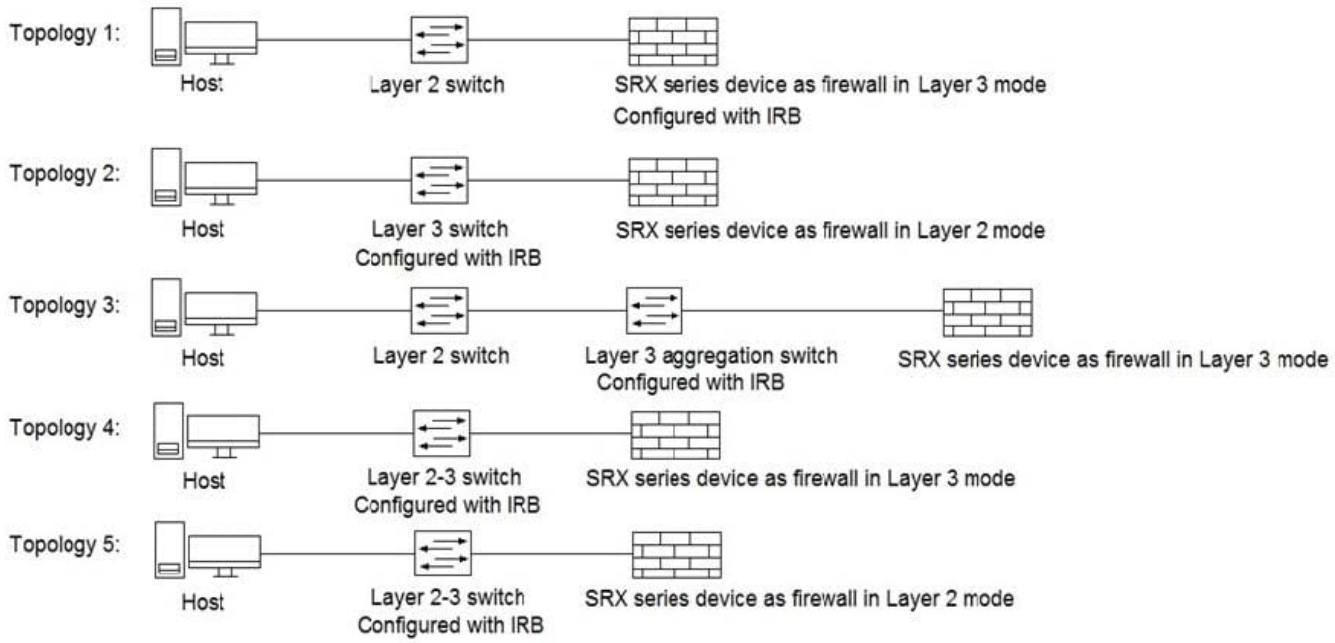
D. The number of forwarding classes configured for the VPN.

Correct Answer: D

Explanation: In IPsec CoS-based VPNs, the number of IPsec Security Associations (SAs) associated with a peer is based on the number of forwarding classes configured for the VPN. The forwarding classes are used to classify and prioritize different types of traffic, such as voice and data traffic. Each forwarding class requires a separate IPsec SA to be established between the peers, in order to provide the appropriate level of security and quality of service for each type of traffic.

QUESTION 8

Click the Exhibit button.



Referring to the exhibit, which three topologies are supported by Policy Enforcer? (Choose three.)

A. Topology 3

B. Topology 5

C. Topology 2

D. Topology 4

E. Topology 1

Correct Answer: ADE

Reference: https://www.juniper.net/documentation/en_US/junos-space17.2/policy- enforcer/topics/concept/ policy-enforcer-deployment-supported-topologies.html

---

QUESTION 9

Your company wants to use the Juniper SecIntel feeds to block access to known command and control servers, but they do not want to use Security Director to manage the feeds. Which two Juniper devices work in this situation? (Choose two)

A. EX Series devices

B. MX Series devices

C. SRX Series devices

D. QFX Series devices

Correct Answer: BC

Explanation: Juniper MX and SRX series devices support the integration of SecIntel feeds, which provide information about known command and control servers, for the purpose of blocking access to them. These devices can be configured to use the SecIntel feeds without the need for Security Director to manage the feeds. EX series and QFX series devices are not capable of working in this situation, as they do not support the integration of SecIntel feeds.

QUESTION 10

Which method does an SRX Series device in transparent mode use to learn about unknown devices in a network?

A. LLDP-MED

B. IGMP snooping

C. RSTP

D. packet flooding

Correct Answer: D

Explanation: The SRX Series device in transparent mode uses packet flooding to learn about unknown devices in a network. Packet flooding is a process wherein the device sends out packets to every device it knows about or suspects in the network. When the packets are returned, the device can identify and classify the unknown devices in the network.

QUESTION 11

What are two valid modes for the Juniper ATP Appliance? (Choose two.)

A. flow collector

B. event collector

C. all-in-one

D. core

Correct Answer: AC

Explanation: The Juniper ATP Appliance supports two valid modes of operation:

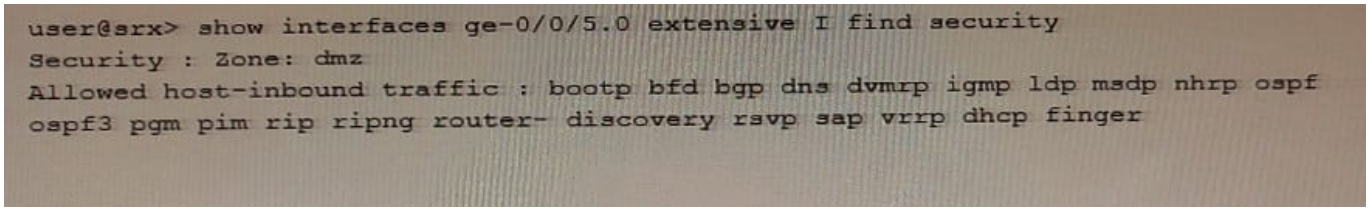
Flow Collector: This mode allows the Juniper ATP Appliance to collect and analyze network flow data to detect malicious activity.

All-in-One: This mode allows the Juniper ATP Appliance to perform both flow collection and event collection. It includes all the features of the Flow Collector and Event Collector mode.

Event collector and core are not valid modes for the Juniper ATP Appliance, the first one is focused on collecting events and the second one is a term that\\'s not related to the appliance.

QUESTION 12

Exhibit



Referring to the exhibit, which three protocols will be allowed on the ge-0/0/5.0 interface? (Choose three.)

A. IBGP

B. OSPF

C. IPsec

D. DHCP

E. NTP

Correct Answer: BDE

Explanation: The exhibit shows the output of the "show interfaces ge-0/0/5.0 extensive" command on an SRX Series device. The output includes a section called "Security" that lists the protocols that are allowed on the ge-0/0/5.0 interface.

The protocols that are allowed on the ge-0/0/5.0 interface are:

OSPF

DHCP

NTP

It\\'s important to notice that the output don\\'t have IBGP, IPsec, so these protocols are not allowed on the ge-0/0/5.0 interface.