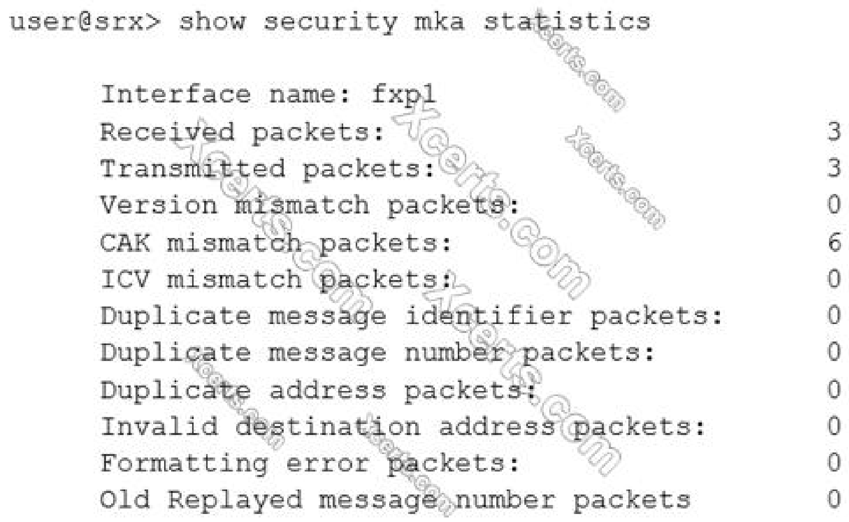
Security, Professional

1. Click the Exhibit button.



```
user@srx> show security mka statistics

    Interface name: fxp1
    Received packets:                              3
    Transmitted packets:                           3
    Version mismatch packets:                      0
    CAK mismatch packets:                          6
    ICV mismatch packets:                          0
    Duplicate message identifier packets:          0
    Duplicate message number packets:              0
    Duplicate address packets:                     0
    Invalid destination address packets:           0
    Formatting error packets:                      0
    Old Replayed message number packets            0
```

While configuring the SRX345, you review the MACsec connection between devices and note that it is not working.

Referring to the exhibit, which action would you use to identify problem?

A. Verify that the formatting settings are correct between the devices and that the software supports the version of MACsec in use

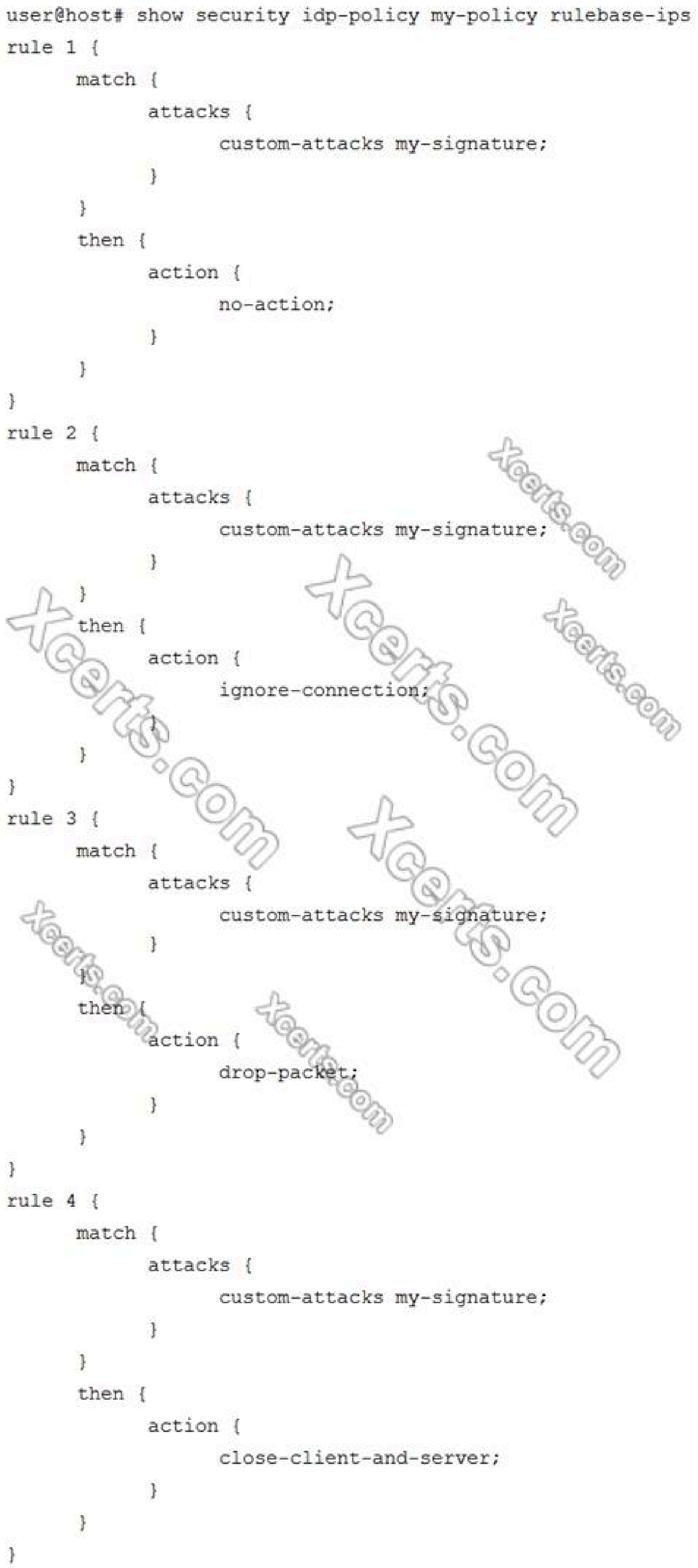
B. Verify that the connectivity association key and the connectivity association key name match on both devices

C. Verify that the transmission path is not replicating packets or correcting frame check sequence error packets

D. Verify that the interface between the two devices is up and not experiencing errors

Answer(s): B

2. Click the Exhibit button.



```
user@host# show security idp-policy my-policy rulebase-ips
rule 1 {
       match {
             attacks {
                   custom-attacks my-signature;
             }
       }
       then {
             action {
                   no-action;
             }
       }
}
rule 2 {
       match {
             attacks {
                   custom-attacks my-signature;
             }
       }
       then {
             action {
                   ignore-connection;
             }
       }
}
rule 3 {
       match {
             attacks {
                   custom-attacks my-signature;
             }
       }
       then {
             action {
                   drop-packet;
             }
       }
}
rule 4 {
       match {
             attacks {
                   custom-attacks my-signature;
             }
       }
       then {
             action {
                   close-client-and-server;
             }
       }
}
```

You have recently committed the IPS policy shown in the exhibit. When evaluating the expected behavior, you notice that you have a session that matches all the rules in your IPS policy.

In this scenario, which action would be taken?

A. drop packet

B. no-action

C. close-client-and-server

D. ignore-connection

Answer(s): B

---

3. Your organization has multiple Active Directory domains to control user access. You must ensure that security policies are passing traffic based upon the users' access rights.
What would you use to assist your SRX Series devices to accomplish this task?

A. JATP Appliance

B. JIMS

C. JSA

D. Junos Space

Answer(s): B

---

4. 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(s): B D

---

5. You have configured static NAT for a webserver in your DMZ. Both internal and external users can reach the webserver using the webserver's IP address. However, only internal users can reach the webserver using the webserver's DNS name. When external users attempt to reach the webserver using the webserver's DNS name, an error message is received.
Which action would solve this problem?

A. Disable Web filtering

B. Use DNS doctoring

C. Modify the security policy

D. Use destination NAT instead of static NAT

Answer(s): B

---

6. Which interface family is required for Layer 2 transparent mode on SRX Series devices?

A. LLDP

B. Ethernet switching

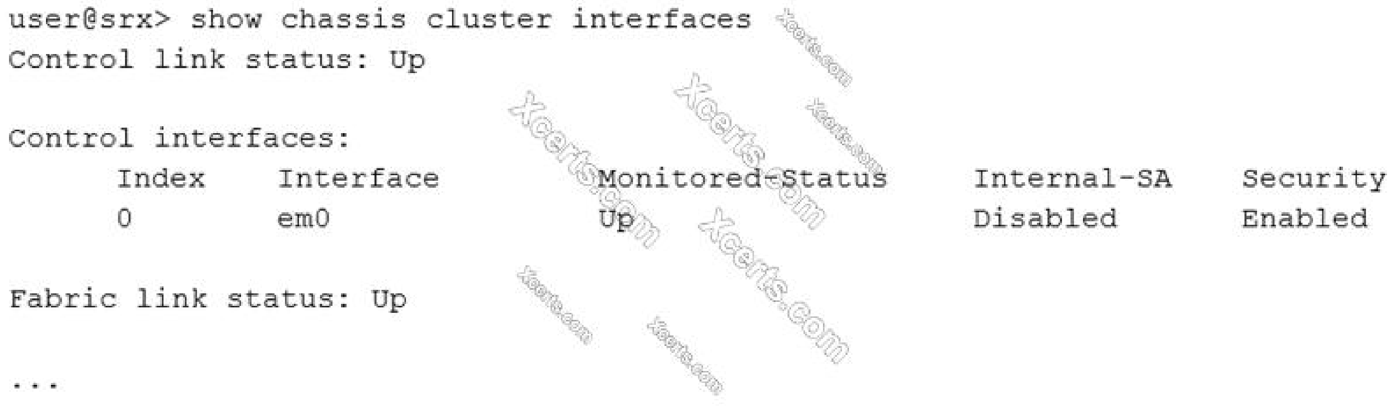
C. inet

D. VPLS

Answer(s): B

---

7. Click the Exhibit button.



```
user@srx> show chassis cluster interfaces
Control link status: Up

Control interfaces:
      Index    Interface        Monitored-Status    Internal-SA    Security
      0        em0              Up                  Disabled       Enabled

Fabric link status: Up

...
```

Referring to the exhibit, which statement is true?

A. ARP security is securing data across the control interface

B. IPsec is securing data across the control interface

C. SSH is securing data across the control interface

D. MACsec is securing data across the control interface

Answer(s): D

---

8. You have configured three logical tunnel interfaces in a tenant system on an SRX1500 device. When committing the configuration, the commit fails.
In this scenario, what would cause this problem?

A. There is no GRE tunnel between the tenant system and master system allowing SSH traffic

B. There is no VPLS switch on the tenant system containing a peer It-0/0/0 interface

C. The SRX1500 device does not support more than two logical interfaces per tenant system

D. The SRX1500 device requires a tunnel PIC to allow for logical tunnel interfaces

Answer(s): B

---

9. You are asked to merge to 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 Series device servers as the gateway for each network.
Which solution allows you to merge the two networks without modifying the current address assignments?

A. persistent NAT

B. NAT46

C. source NAT

D. double NAT

Answer(s): D

---

10. You have set up Security Director with Policy Enforcer and have configured 12 third-party feeds and a Sky ATP feed. You are also injecting 16 feeds using the available open API. You want to add another compatible feed using the available open API, but Policy Enforcer is not receiving the new feed.
What is the problem in this scenario?

A. You must wait 48 hours for the feed to update

B. You cannot add more than 16 feeds through the available open API

C. You have reached the maximum limit of 29 total feeds

D. You cannot add more than 16 feeds with the available open API

Answer(s): C

---

11. Which three types of peer devices are supported for CoS-based IPsec VPNs? (Choose three.)

□ A. branch SRX Series device

□ B. third-party device

□ C. cSRX

□ D. high-end SRX Series device

□ E. vSRX

Answer(s): A D E

---

12. 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(s): A D

---

13. Which three roles or protocols are required when configuring an ADVPN? (Choose three.)

□ A. OSPF

□ B. shortcut partner

□ C. shortcut suggester

□ D. IKEv1

□ E. BGP

Answer(s): A B C

---

14. You must troubleshoot ongoing problems with IPsec tunnels and security policy processing. Your network consists of SRX340s and SRX5600s.
In this scenario, which two statements are true? (Choose two.)

□ A. IPsec logs are written to the kmd log file by default

□ B. IKE logs are written to the messages log file by default

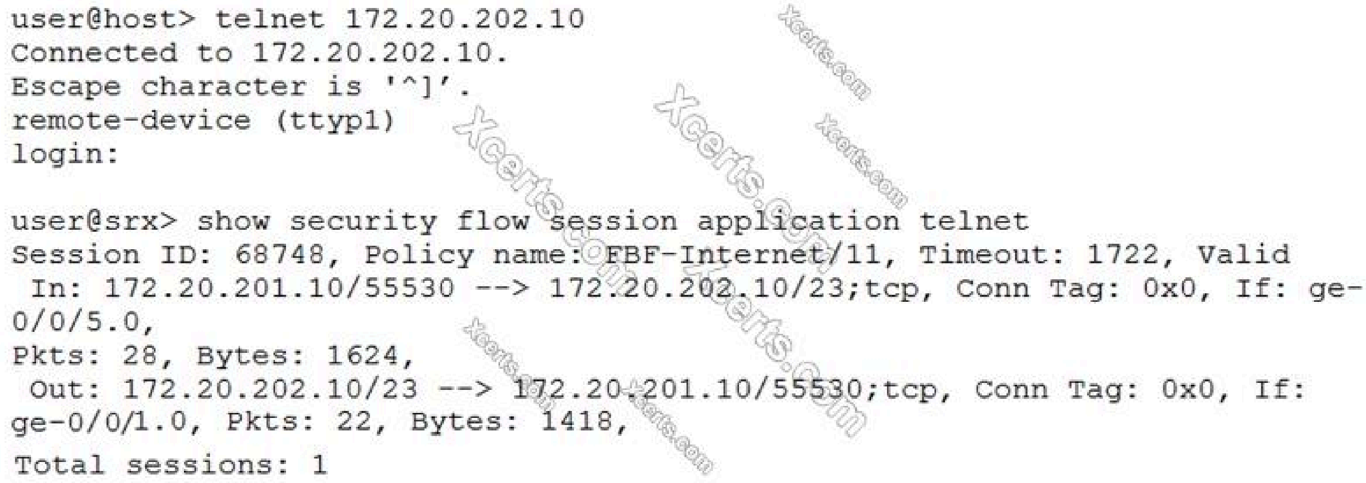
□ C. You must enable data plane logging on the SRX340 devices to generate security policy logs

□ D. You must enable data plane logging on the SRX5600 devices to generate security policy logs

Answer(s): A D

---

15. Click the Exhibit button.



```
user@host> telnet 172.20.202.10
Connected to 172.20.202.10.
Escape character is '^]'.
remote-device (ttyp1)
login:

user@srx> show security flow session application telnet
Session ID: 68748, Policy name: FBF-Internet/11, Timeout: 1722, Valid
 In: 172.20.201.10/55530 --> 172.20.202.10/23;tcp, Conn Tag: 0x0, If: ge-
0/0/5.0,
Pkts: 28, Bytes: 1624,
 Out: 172.20.202.10/23 --> 172.20.201.10/55530;tcp, Conn Tag: 0x0, If:
ge-0/0/1.0, Pkts: 22, Bytes: 1418,
 Total sessions: 1
```

You are implementing a new branch site and want to ensure Internet traffic is sent directly to your ISP and other traffic is sent to your company headquarters. You have configured filter-based forwarding to accomplish this objective. You verify proper functionality using the outputs shown in the exhibit.
Which two statements are true in this scenario? (Choose two.)

□ A. The session utilizes one routing instance

□ B. The ge-0/0/5 and ge-0/0/1 interfaces must reside in a single security zone

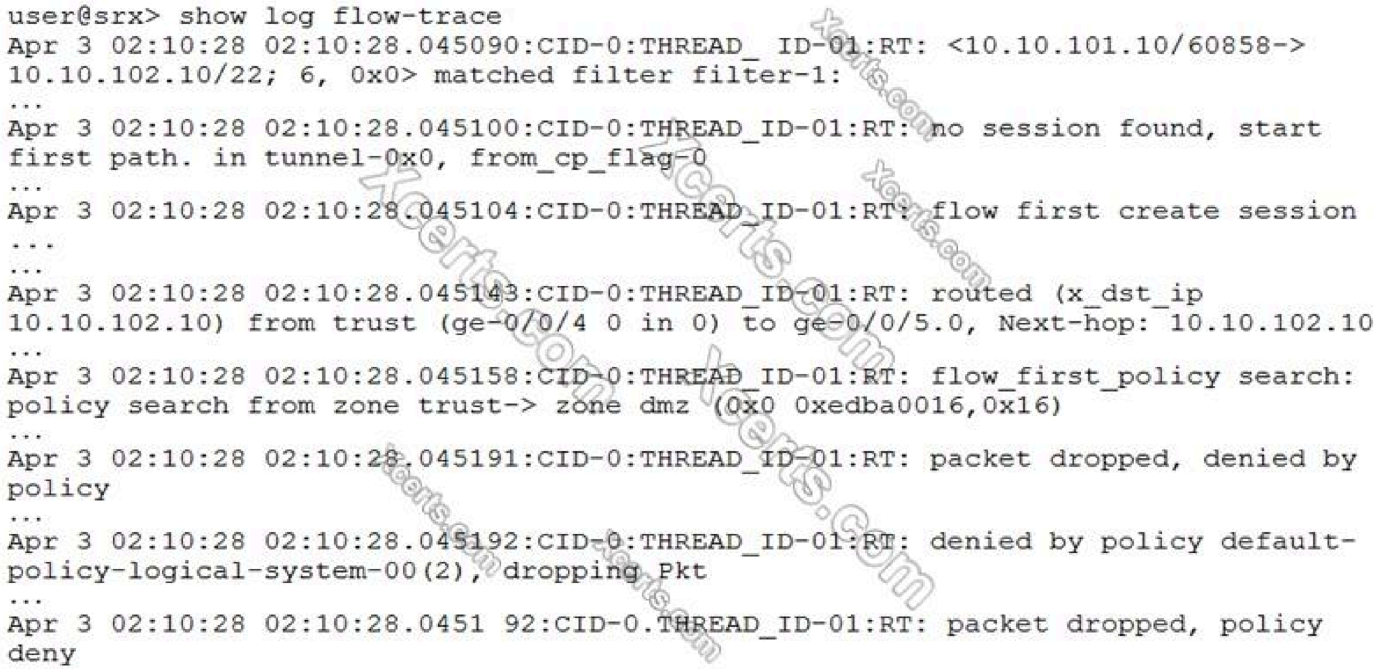
□ C. The ge-0/0/5 and ge-0/0/1 interfaces can reside in different security zones

□ D. The session utilizes two routing instances

Answer(s): A C

---

16. Click the Exhibit button.



```
user@srx> show log flow-trace
Apr 3 02:10:28 02:10:28.045090:CID-0:THREAD_ ID-01:RT: <10.10.101.10/60858->
10.10.102.10/22; 6, 0x0> matched filter filter-1:
...
Apr 3 02:10:28 02:10:28.045100:CID-0:THREAD_ID-01:RT: no session found, start
first path. in tunnel-0x0, from_cp_flag-0
...
Apr 3 02:10:28 02:10:28.045104:CID-0:THREAD_ID-01:RT: flow first create session
...
...
Apr 3 02:10:28 02:10:28.045143:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.10) from trust (ge-0/0/4 0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.10
...
Apr 3 02:10:28 02:10:28.045158:CID-0:THREAD_ID-01:RT: flow_first_policy search:
policy search from zone trust-> zone dmz (0x0 0xedba0016,0x16)
...
Apr 3 02:10:28 02:10:28.045191:CID-0:THREAD_ID-01:RT: packet dropped, denied by
policy
...
Apr 3 02:10:28 02:10:28.045192:CID-0:THREAD_ID-01:RT: denied by policy default-
policy-logical-system-00(2), dropping Pkt
...
Apr 3 02:10:28 02:10:28.0451 92:CID-0.THREAD_ID-01:RT: packet dropped, policy
deny
```

The exhibit shows a snippet of a security flow trace. A user cannot open an SSH session to a server. Which action will solve the problem?

A. Create a security policy that matches the traffic parameters

B. Edit the source NAT to correct the translated address

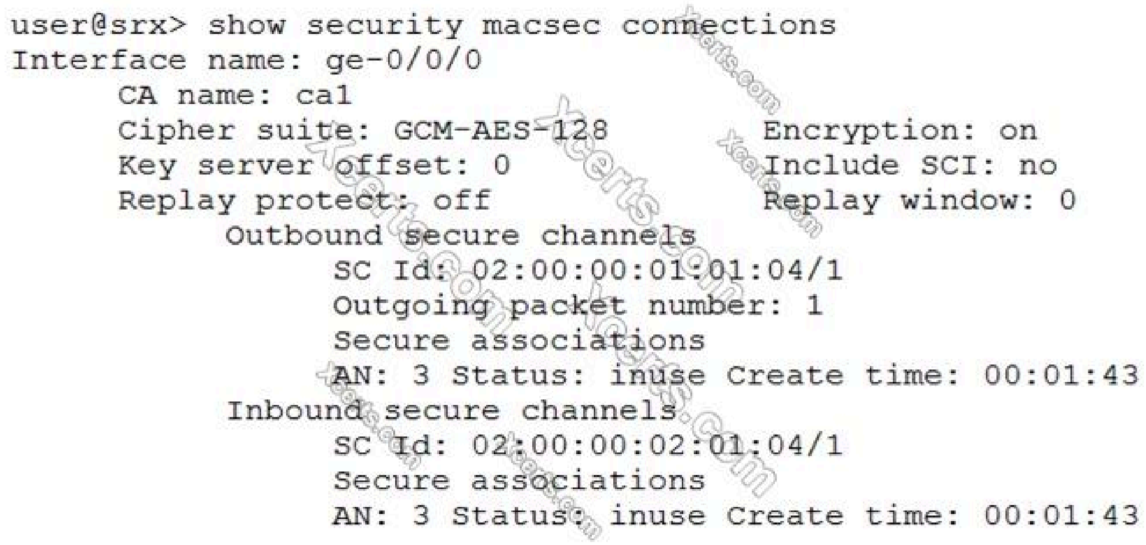
C. Create a route entry to direct traffic into the configured tunnel

D. Create a route to the desired server

Answer(s): A

---

17. Click the Exhibit button.



```
user@srx> show security macsec connections
Interface name: ge-0/0/0
      CA name: ca1
      Cipher suite: GCM-AES-128        Encryption: on
      Key server offset: 0             Include SCI: no
      Replay protect: off              Replay window: 0
            Outbound secure channels
                  SC Id: 02:00:00:01:01:04/1
                  Outgoing packet number: 1
                  Secure associations
                  AN: 3 Status: inuse Create time: 00:01:43
            Inbound secure channels
                  SC Id: 02:00:00:02:01:04/1
                  Secure associations
                  AN: 3 Status: inuse Create time: 00:01:43
```

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

□ A. Data is transmitted across the link in plaintext

□ B. The link is not protected against man-in-the-middle attacks

□ C. The link is protected against man-in-the-middle attacks

□ D. Data is transmitted across the link in cyphertext

Answer(s): B D

---

18. You are asked to secure your network against TOR network traffic. Which two Juniper products would accomplish this task? (Choose two.)

□ A. Contrail Edge

□ B. Contrail Insights

□ C. Juniper Sky ATP

□ D. Juniper ATP Appliance

Answer(s): C D

---

19. You are asked to implement the session cache feature on an SRX5400.
In this scenario, what information does a session cache entry record? (Choose two.)

□ A. The type of processing to do for ingress traffic

□ B. The type of processing to do for egress traffic

□ C. To which SPU the traffic of the session should be forwarded

□ D. To which NPU the traffic of the session should be forwarded

Answer(s): B C

---

20. Which feature of Sky ATP is deployed with Policy Enforcer?

A. zero-day threat mitigation

B. software image snapshot support

C. device inventory management

D. service redundancy daemon configuration support

Answer(s): A
