JN0-636 Q&As

Service Provider Routing and Switching Professional (JNCIP-SP)

Pass Juniper JN0-636 Exam with 100% Guarantee

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

https://www.geekcert.com/jn0-636.html

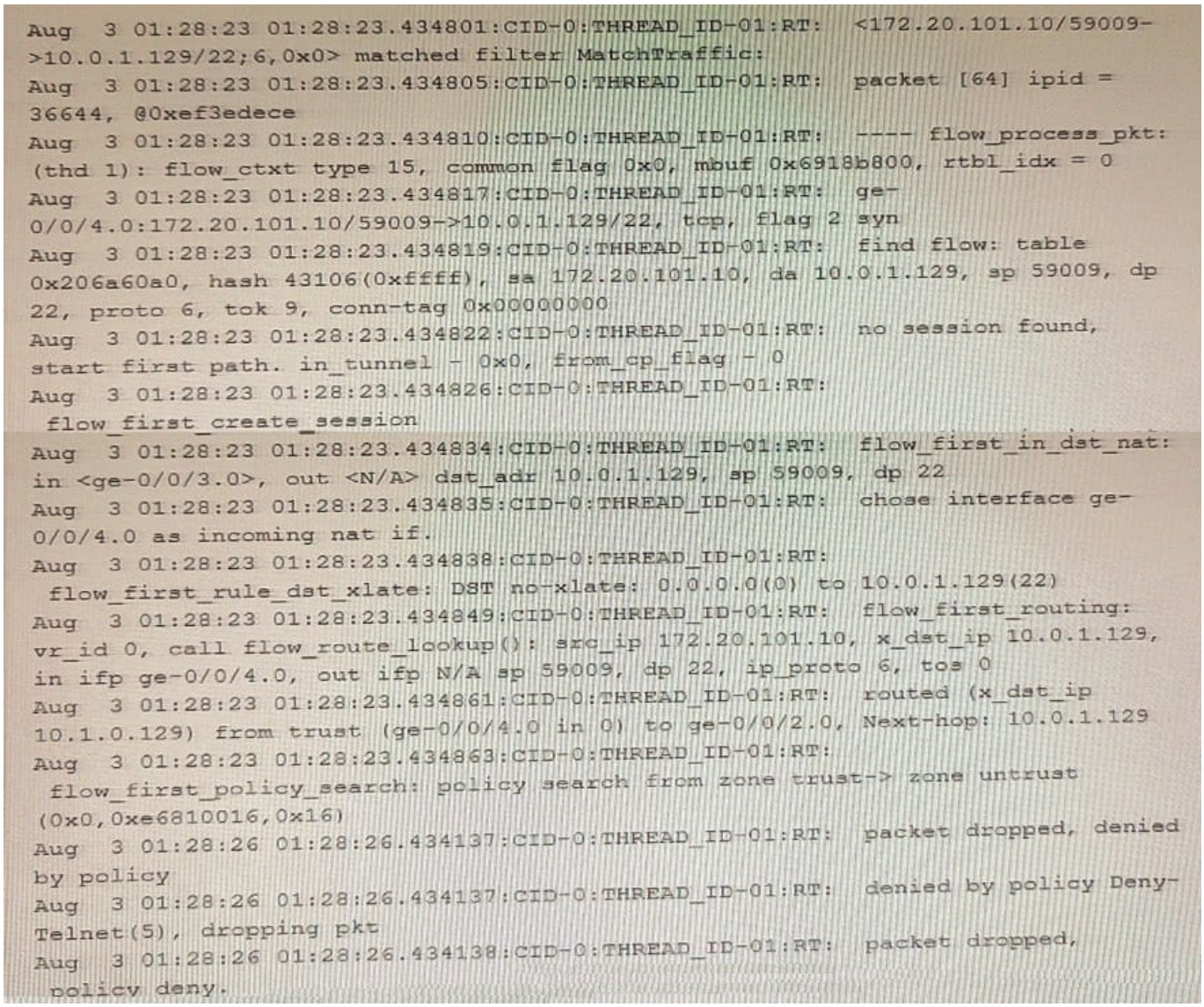
100% Passing Guarantee
100% Money Back Assurance

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

Exhibit



Referring to the exhibit, which statement is true?

A. This custom block list feed will be used before the Juniper SecIntel

B. This custom block list feed cannot be saved if the Juniper SecIntel block list feed is configured.

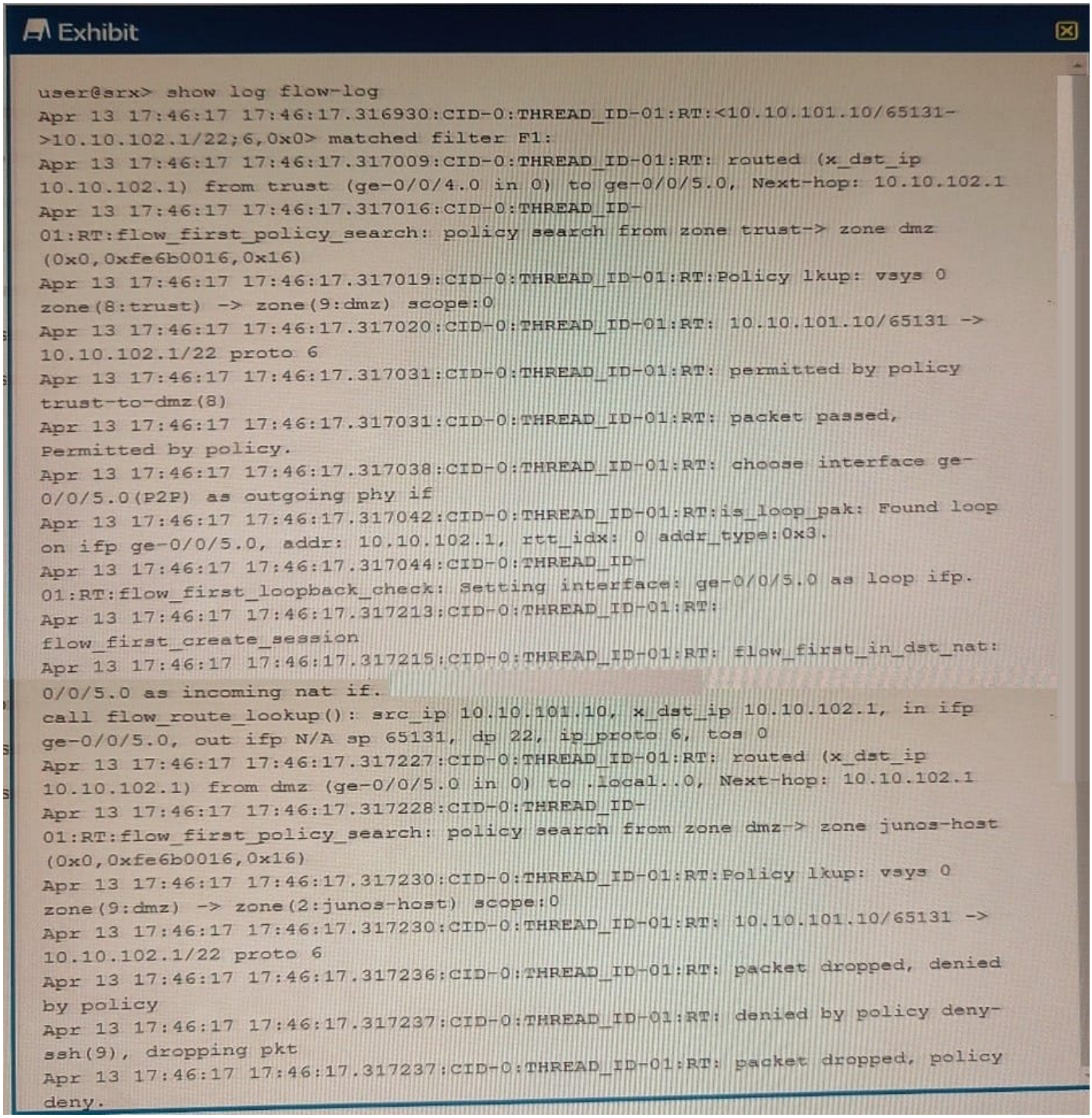
C. This custom block list feed will be used instead of the Juniper SecIntel block list feed

D. This custom block list feed will be used after the Juniper SecIntel block list feed.

Correct Answer: D

QUESTION 2

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



Exhibit

```
user@srx> show log flow-log
Apr 13 17:46:17 17:46:17.316930:CID-0:THREAD_ID-01:RT:<10.10.101.10/65131-
>10.10.102.1/22;6,0x0> matched filter F1:
Apr 13 17:46:17 17:46:17.317009:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317016:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317019:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(8:trust) -> zone(9:dmz) scope:0
Apr 13 17:46:17 17:46:17.317020:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: permitted by policy
trust-to-dmz(8)
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: packet passed,
Permitted by policy.
Apr 13 17:46:17 17:46:17.317038:CID-0:THREAD_ID-01:RT: choose interface ge-
0/0/5.0(P2P) as outgoing phy if
Apr 13 17:46:17 17:46:17.317042:CID-0:THREAD_ID-01:RT:is_loop_pak: Found loop
on ifp ge-0/0/5.0, addr: 10.10.102.1, rtt_idx: 0 addr_type:0x3.
Apr 13 17:46:17 17:46:17.317044:CID-0:THREAD_ID-
01:RT:flow_first_loopback_check: Setting interface: ge-0/0/5.0 as loop ifp.
Apr 13 17:46:17 17:46:17.317213:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Apr 13 17:46:17 17:46:17.317215:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
0/0/5.0 as incoming nat if.
call flow_route_lookup(): src_ip 10.10.101.10, x_dst_ip 10.10.102.1, in ifp
ge-0/0/5.0, out ifp N/A sp 65131, dp 22, ip_proto 6, tos 0
Apr 13 17:46:17 17:46:17.317227:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from dmz (ge-0/0/5.0 in 0) to .local..0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317228:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone dmz-> zone junos-host
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(9:dmz) -> zone(2:junos-host) scope:0
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317236:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: denied by policy deny-
ssh(9), dropping pkt
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
```

A. The packet\\'s destination is to an interface on the SRX Series device.

B. The packet\\'s destination is to a server in the DMZ zone.

C. The packet originated within the Trust zone.

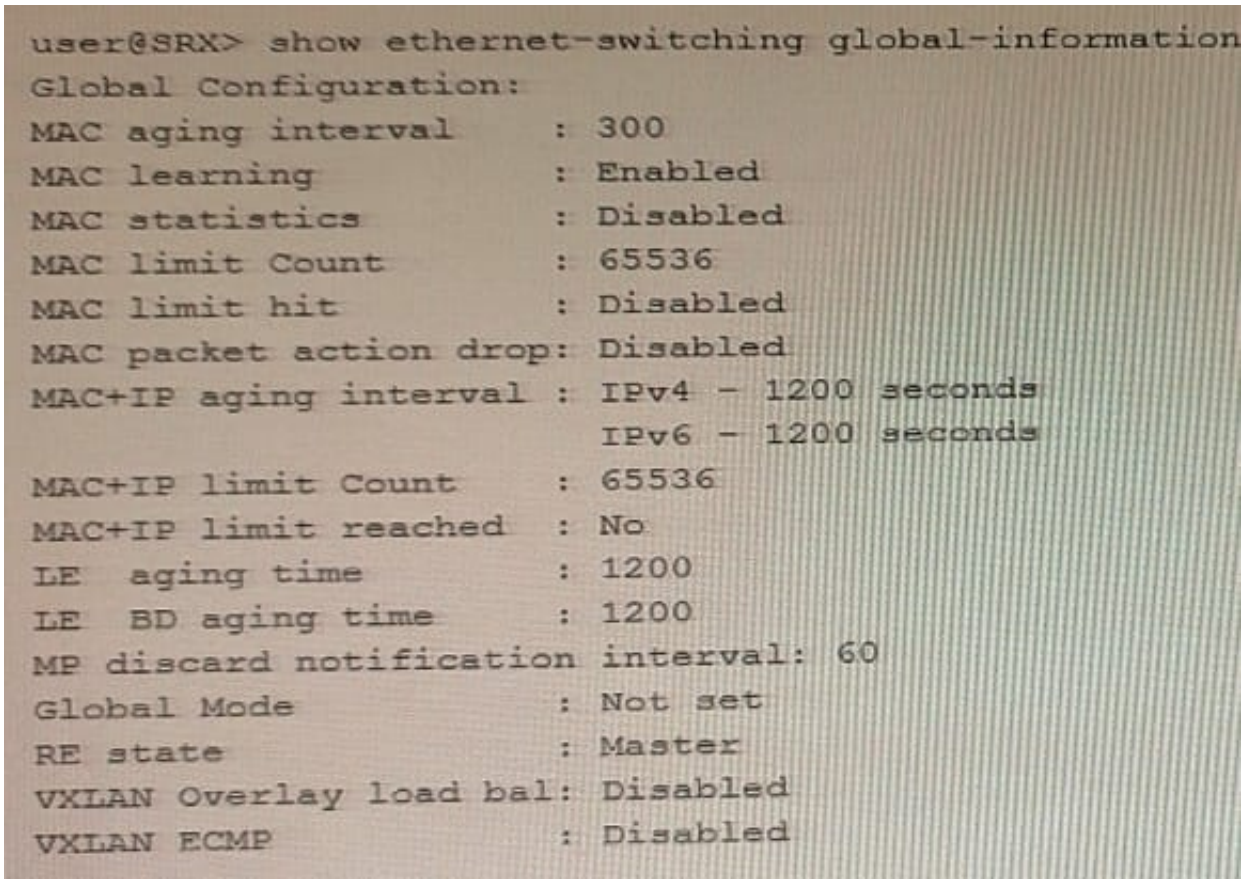
D. The packet is dropped before making an SSH connection.

E. The packet is allowed to make an SSH connection.

Correct Answer: ACD

QUESTION 3

Exhibit You have configured the SRX Series device to switch packets for multiple directly connected hosts that are within the same broadcast domain However, the traffic between two hosts in the same broadcast domain are not matching any security policies



```
user@SRX> show ethernet-switching global-information
Global Configuration:
MAC aging interval      : 300
MAC learning            : Enabled
MAC statistics          : Disabled
MAC limit Count         : 65536
MAC limit hit           : Disabled
MAC packet action drop: Disabled
MAC+IP aging interval : IPv4 - 1200 seconds
                        IPv6 - 1200 seconds
MAC+IP limit Count      : 65536
MAC+IP limit reached    : No
LE  aging time          : 1200
LE  BD aging time       : 1200
MP discard notification interval: 60
Global Mode             : Not set
RE state                : Master
VXLAN Overlay load bal: Disabled
VXLAN ECMP              : Disabled
```

Referring to the exhibit, what should you do to solve this problem?

A. You must change the global mode to security switching mode.

B. You must change the global mode to security bridging mode

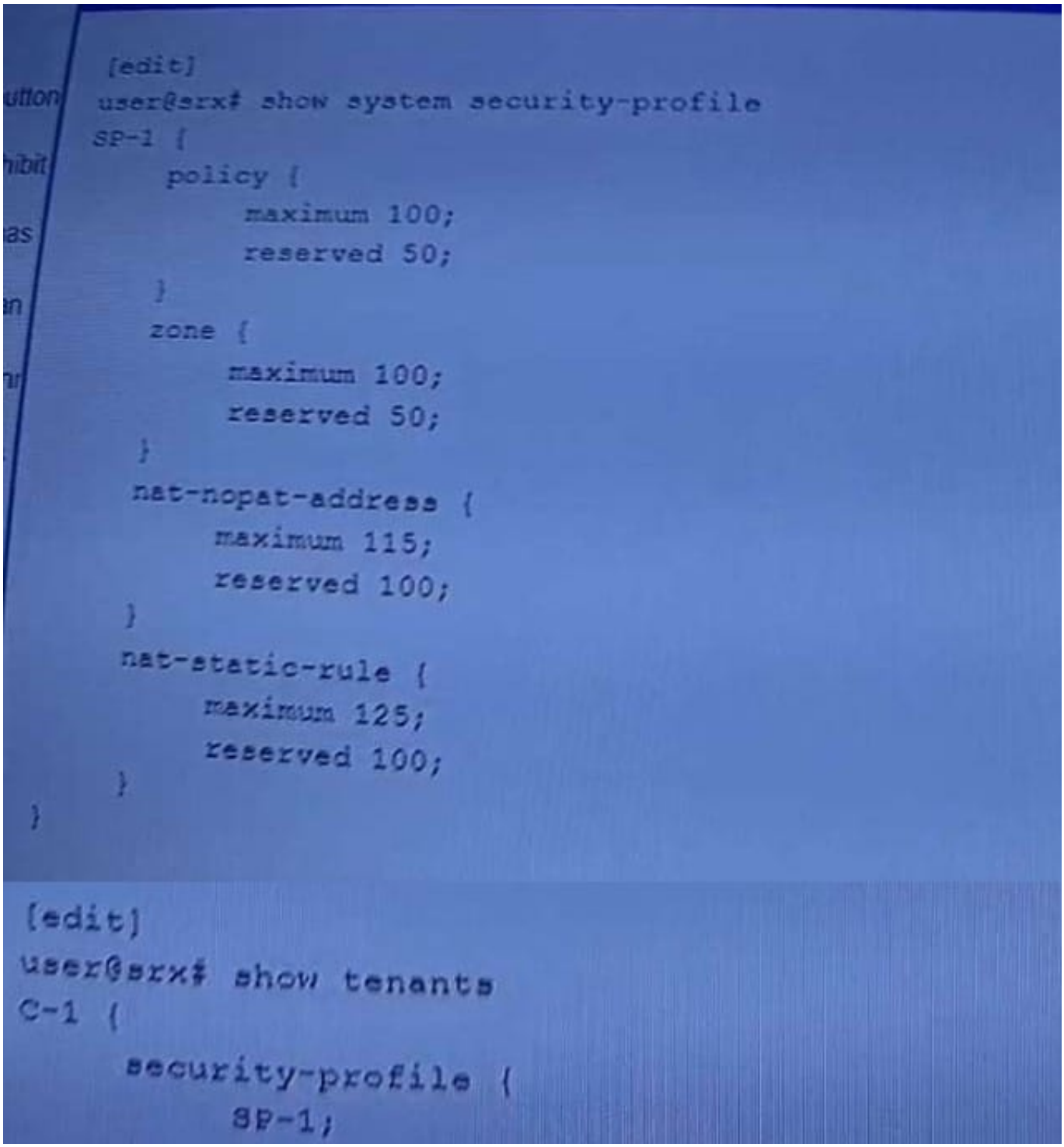
C. You must change the global mode to transparent bridge mode.

D. You must change the global mode to switching mode.

Correct Answer: B

QUESTION 4

Exhibit.



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

A. The c-1 TSYS has a reservation for the security flow resource.

B. The c-1 TSYS can use security flow resources up to the system maximum.

C. The c-1 TSYS cannot use any security flow resources.

D. The c-1 TSYS has no reservation for the security flow resource.

Correct Answer: CD

Explanation: https://www.juniper.net/documentation/en_US/junos/topics/topic- map/security-profile-logical-system.html

QUESTION 5

Your IPsec VPN configuration uses two CoS forwarding classes to separate voice and data traffic. How many IKE security associations are required between the IPsec peers in this scenario?

B. 3

C. 4

D. 2

Correct Answer: A

Explanation: An IKE security association (SA) is a set of parameters that define how the Internet Key Exchange (IKE) protocol will authenticate and establish the secure channel between the IPsec VPN peers. When you configure an IPsec

VPN, one IKE SA is created between the peers, regardless of how many CoS forwarding classes are used to separate the traffic. The SA will be used to negotiate the IPsec SA parameters, such as encryption algorithms and keys.

In this scenario, only 1 IKE security association is required between the IPsec peers, no matter how many CoS forwarding classes are used to separate the voice and data traffic.