

# **Juniper**

## **JN0-636 Exam**

**Security, Professional  
Questions & Answers  
Demo**

# Version: 4.2

---

## Question: 1

---

Exhibit

```

Aug 1 21:04:18 21:04:18.706917:CID-0:RT: <10.0.1.129/22->10.0.1.1/61673;6,0x0>
matched filter MatchTrafficReverse:
Aug 1 21:04:18 21:04:18.706919:CID-0:RT: packet [88] ipid = 18817, 80x9e5a9cce
Aug 1 21:04:18 21:04:18.706919:CID-0:RT: ---- flow_process_pkt: (thd 1):
flow_ctxt type 15, common flag 0x0, mbuf 0x7122ae00, rtbl_idx = 0
Aug 1 21:04:18 21:04:18.706920:CID-0:RT: flow process pak fast ifl 80 in_ifp
ge-0/0/1.0
Aug 1 21:04:18 21:04:18.706921:CID-0:RT: ge-0/0/1.0:10.0.1.129/22-
>10.0.1.1/21755, tcp, flag 18
Aug 1 21:04:18 21:04:18.706925:CID-0:RT: find flow: table 0x2b5a7ec0, hash
282613(0x7fffff), sa 10.0.1.129, da 10.0.1.1, sp 22, dp 19066, proto 6, tok 10,
conn-tag 0x00000000, vrf-grp-id 0
Aug 1 21:04:18 21:04:18.706928:CID-0:RT: Found: session id 0x5aaf7. sess tok
10
Aug 1 21:04:18 21:04:18.706929:CID-0:RT: flow got session.
Aug 1 21:04:18 21:04:18.706929:CID-0:RT: flow session id 371447
Aug 1 21:04:18 21:04:18.706931:CID-0:RT: post addr xlation: 10.0.1.129-
>172.20.101.10.
Aug 1 21:04:18 21:04:18.706933:CID-0:RT: post addr xlation: 10.0.1.129-
>172.20.101.10.
Aug 1 21:04:18 21:04:18.706935:CID-0:RT: mbuf 0x7122ae00, exit nh 0x140010
  
```

You are using traceoptions to verify NAT session information on your SRX Series device. Referring to the exhibit, which two statements are correct? (Choose two.)

- A. This packet is part of an existing session.
- B. The SRX device is changing the source address on this packet from
- C. This is the first packet in the session
- D. The SRX device is changing the destination address on this packet 10.0.1.1 to 172.20.101.10.

---

**Answer: CD**

---

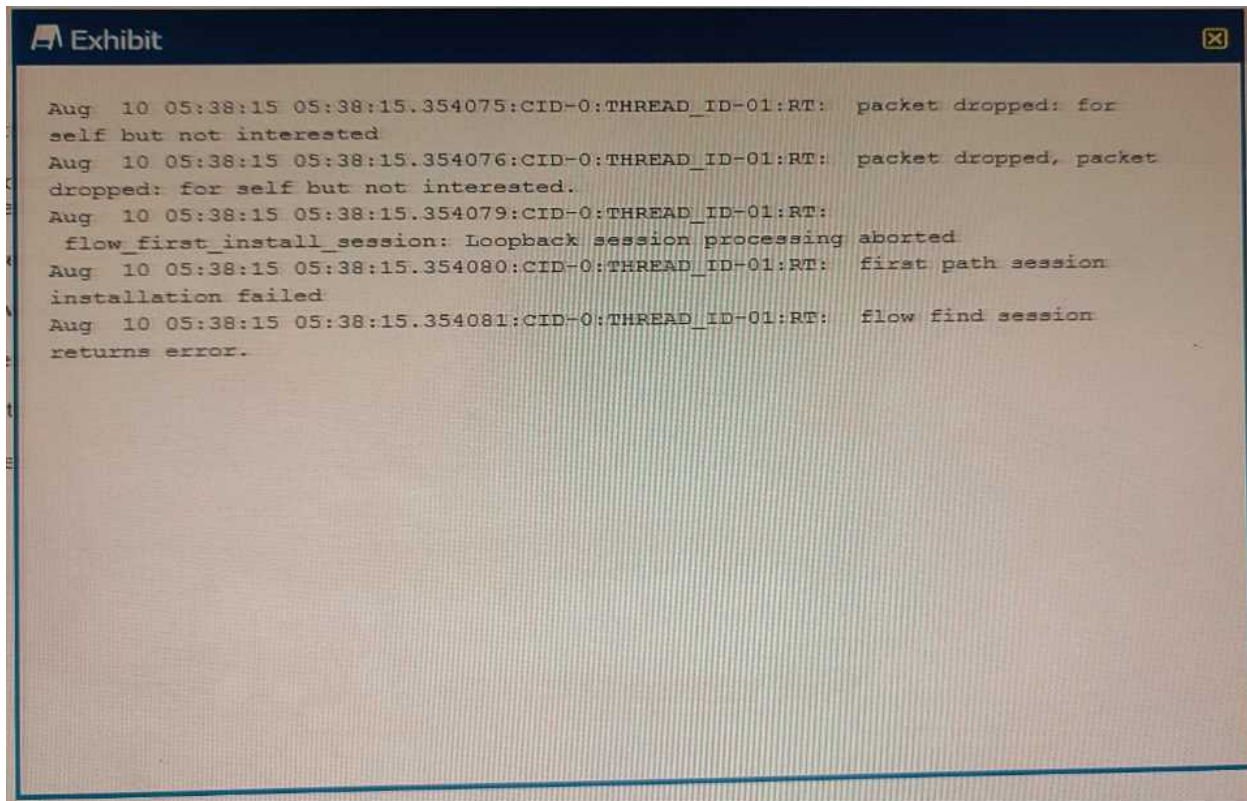


---

## Question: 2

---

Exhibit



```
Aug 10 05:38:15 05:38:15.354075:CID-0:THREAD_ID-01:RT: packet dropped: for
self but not interested
Aug 10 05:38:15 05:38:15.354076:CID-0:THREAD_ID-01:RT: packet dropped, packet
dropped: for self but not interested.
Aug 10 05:38:15 05:38:15.354079:CID-0:THREAD_ID-01:RT:
flow_first_install_session: Loopback session processing aborted
Aug 10 05:38:15 05:38:15.354080:CID-0:THREAD_ID-01:RT: first path session
installation failed
Aug 10 05:38:15 05:38:15.354081:CID-0:THREAD_ID-01:RT: flow find session
returns error.
```

You are asked to establish an IBGP peering between the SRX Series device and the router, but the session is not being established. In the security flow trace on the SRX device, packet drops are observed as shown in the exhibit.

What is the correct action to solve the problem on the SRX device?

- A. Create a firewall filter to accept the BGP traffic
- B. Configure destination NAT for BGP traffic.
- C. Add BGP to the Allowed host-inbound-traffic for the interface
- D. Modify the security policy to allow the BGP traffic.

---

**Answer: A**

---

---

### Question: 3

---

SRX Series device enrollment with Policy Enforcer fails To debug further, the user issues the following command `show configuration services security—intelligence url https://cloudfeeds.argon.juniperasecurity.net/api/manifeat.xml` and receives the following output:

What is the problem in this scenario?

- A. The device is directly enrolled with Juniper ATP Cloud.
- B. The device is already enrolled with Policy Enforcer.
- C. The SRX Series device does not have a valid license.
- D. Junos Space does not have matching schema based on the

---

**Answer: C**

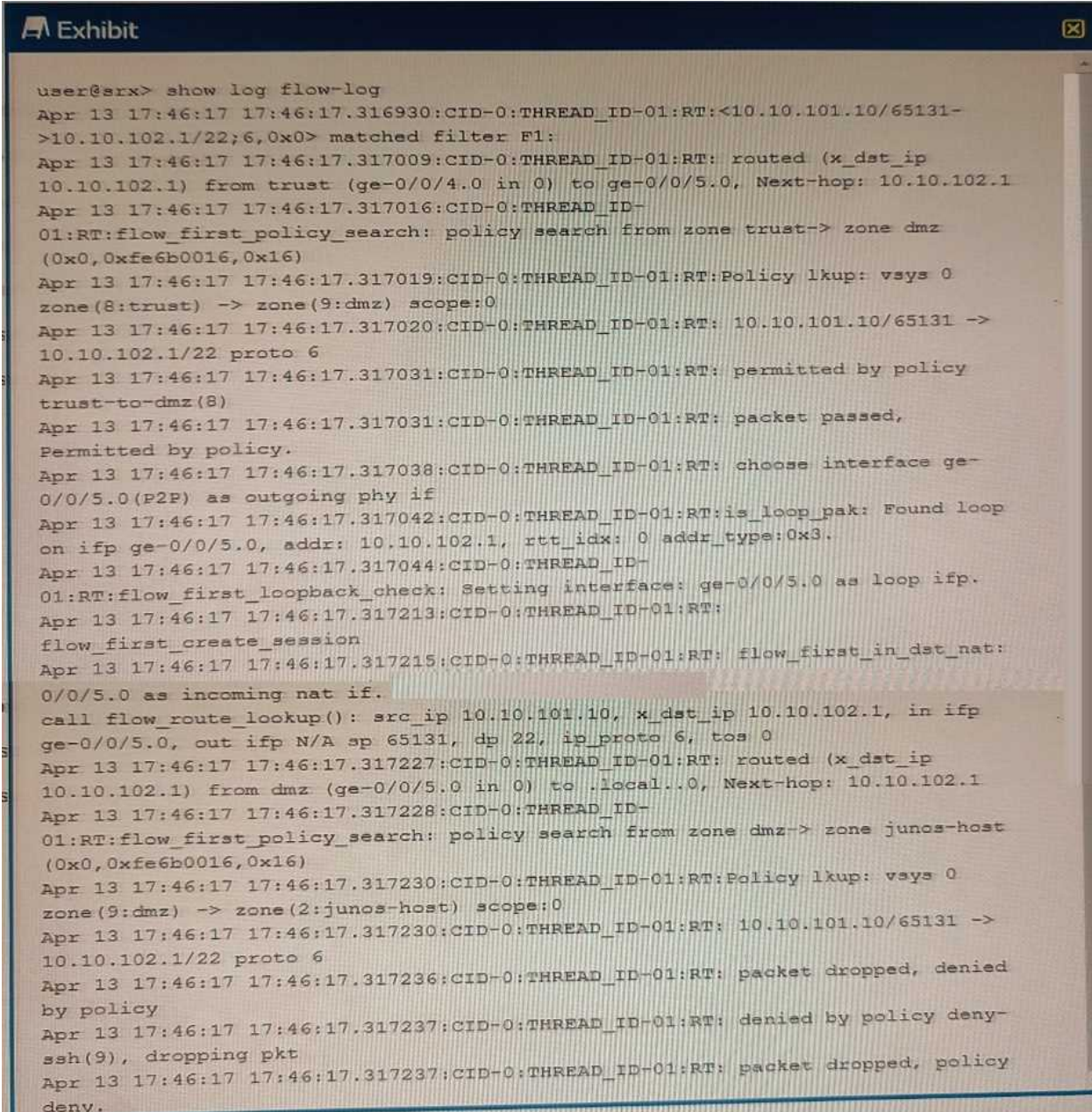
---

---

**Question: 4**

---

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.
```

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

- 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.

---

**Answer: ACD**

---

---

**Question: 5**

---

Exhibit

```
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:36
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Vendor-Id: 0 Attribute Type:Reply-Message(18) Value:string-type
Length:15
May 23 05:20:34 authd_radius_parse_message:generic-type:18
May 23 05:20:34 Framework - module(radius) return: FAILURE
```

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.

---

**Answer: D**

---