



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.pass4itsure.com/jn0-636.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper
Official Exam Center

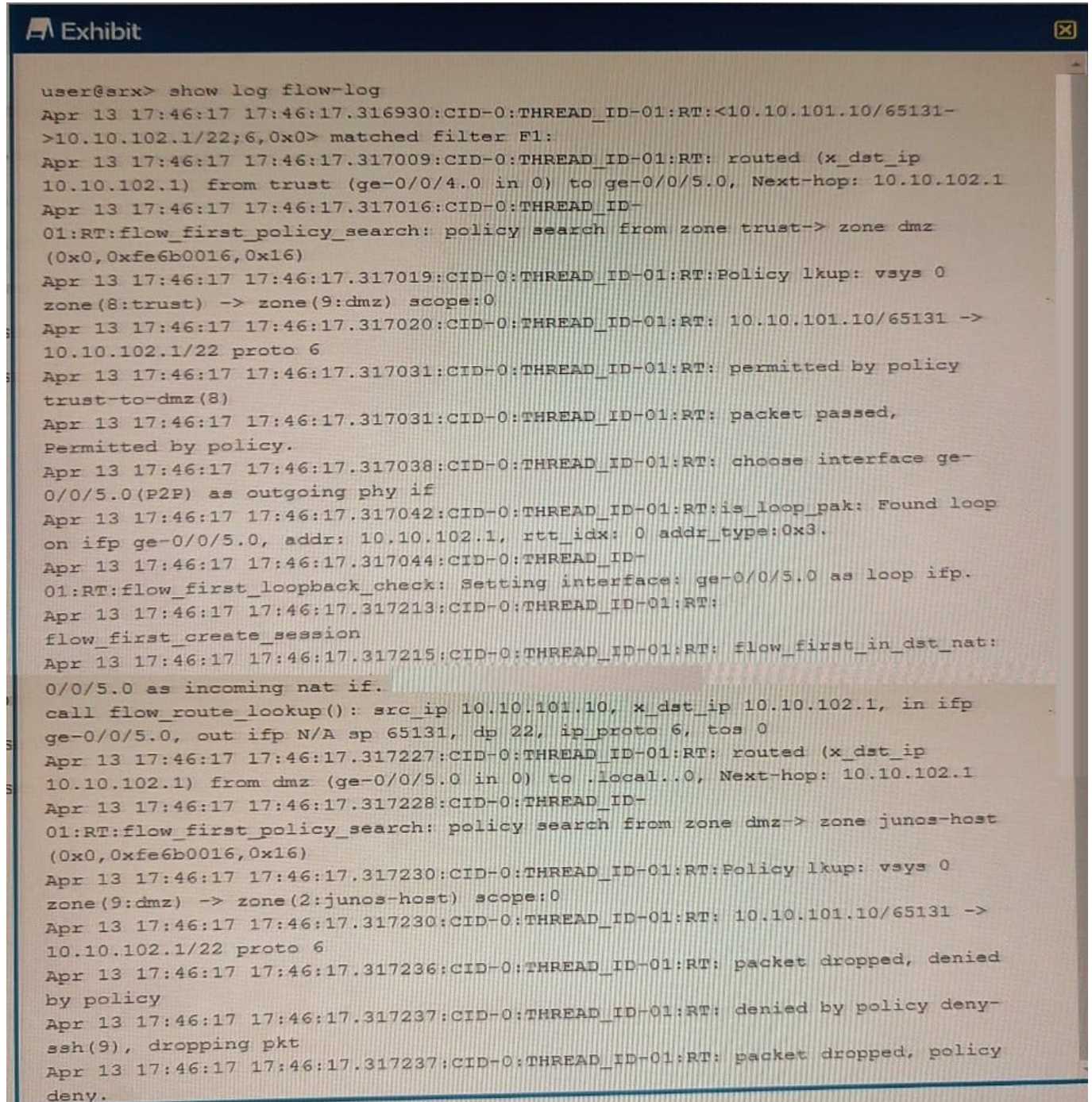
- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





QUESTION 1

Exhibit



```
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.
```

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 is the last packet in the session.
- B. The SRX Series device is performing both source and destination NAT on this session.



C. This is the first packet in the session.

D. The SRX Series device is performing only source NAT on this session.

Correct Answer: AB

QUESTION 2

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

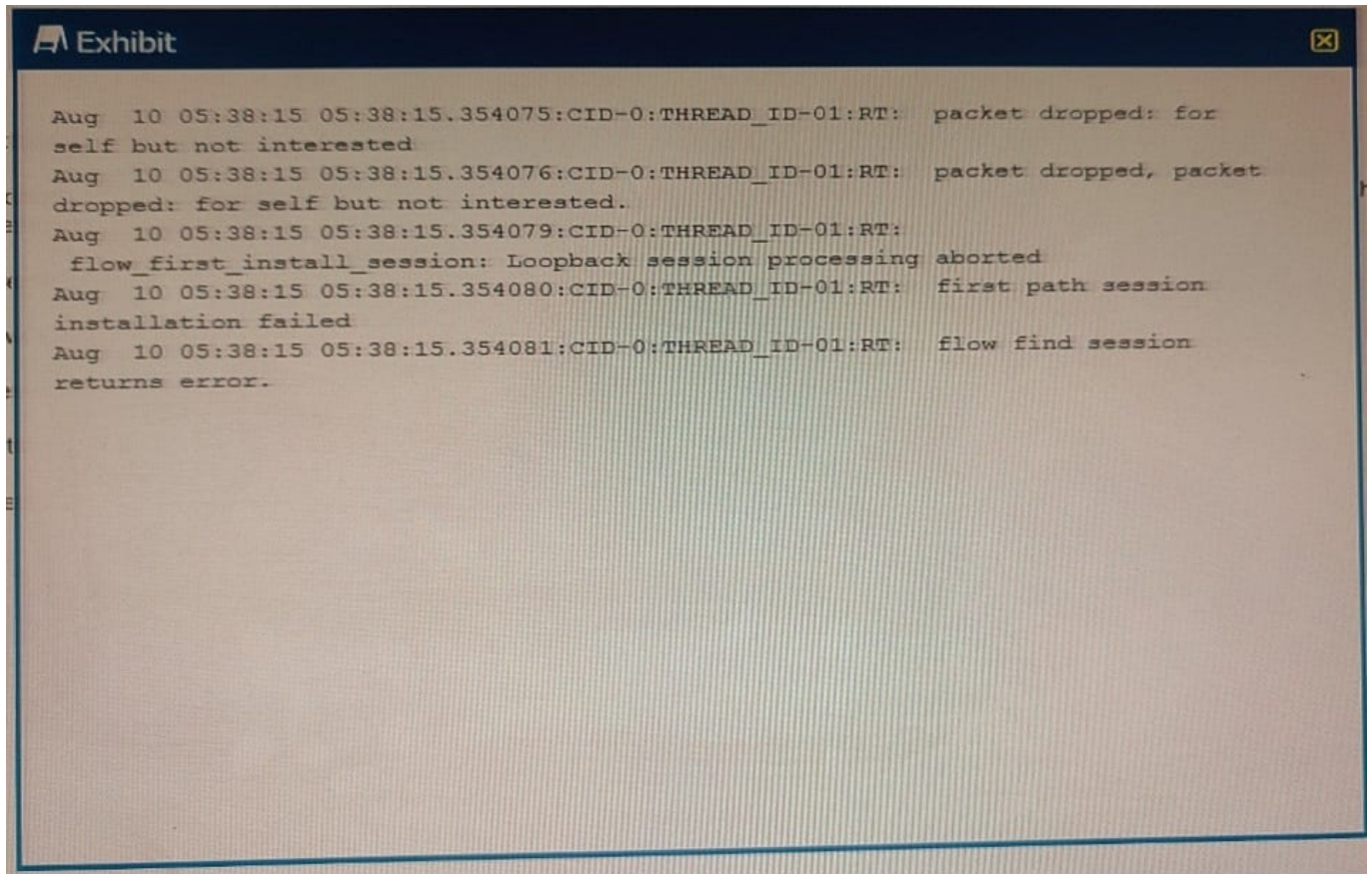
D. Incorrect peer address.

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 3

Exhibit



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.

Correct Answer: A

QUESTION 4

Exhibit.



```
[edit]
user@srx# show system security-profile
SP-1 {
    policy {
        maximum 100;
        reserved 50;
    }
    zone {
        maximum 100;
        reserved 50;
    }
    nat-nopat-address {
        maximum 115;
        reserved 100;
    }
    nat-static-rule {
        maximum 125;
        reserved 100;
    }
}

[edit]
user@srx# show tenants
C-1 {
    security-profile {
        SP-1;
```

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

Exhibit

```
user@host> show security mka sessions summary
Interface  Member-ID                               Type Status Tx Rx CAK Name
ge-0/0/1   E752CAFAE8DDFB82D4EA4BF7               preceding live 8887
           8951                               8888
ge-0/0/1   0F2D5171F38EAB16C2E0CB62               fallback active 8959
           8952                               FFFF
ge-0/0/1   6B49BD5CF7188F3CD9A29D30               primary in-progress 2439 0
           AAAA
```

Referring to the exhibit, which two statements are true about the CAK status for the CAK named "FFFF"? (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 6

You want to configure a threat prevention policy.

Which three profiles are configurable in this scenario? (Choose three.)

- A. device profile
- B. SSL proxy profile
- C. infected host profile
- D. CandC profile
- E. malware profile

Correct Answer: ACE

QUESTION 7



You issue the command shown in the exhibit.

Which policy will be active for the identified traffic?

- A. Policy p4
- B. Policy p7
- C. Policy p1
- D. Policy p12

Correct Answer: B

QUESTION 8

Your organization has multiple Active Directory domain to control user access. You must ensure that security policies are passing traffic based upon the user's access rights.

What would you use to assist your SRX series devices to accomplish this task?

- A. JIMS
- B. Junos Space
- C. JSA
- D. JATP Appliance

Correct Answer: A

Explanation: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-configure-jims.html

QUESTION 9

Exhibit An administrator wants to configure an SRX Series device to log binary security events for tenant systems. Referring to the exhibit, which statement would complete the configuration?



```
[edit tenants TSYS1 security]
user@srx# show
log {
mode stream;
stream TN1_s format binary host 10.3.54.22
source address 10.3.45.66
transport protocol tls
...
}
[edit system security-profile p1]
user@srx# show
security-log-stream-number reserved 1
security-log-stream-number maximum 2
```

- A. Configure the tenant as TSYS1 for the pi security profile.
- B. Configure the tenant as root for the pi security profile.
- C. Configure the tenant as master for the pi security profile.
- D. Configure the tenant as local for the pi security profile

Correct Answer: B

QUESTION 10

You are asked to determine if the 203.0.113.5 IP address has been added to the third-party security feed, DS hield, from Juniper SecInte1. You have an SRX Series device that is using SecInte1 feeds from Juniper ATP Cloud. Which command will return this information?

- A. show security dynamic--address category--name CC | match 203.0.113.5
- B. show security dynamic--address category--name Infected--Hosts | match 203.0.113.5
- C. show security dynamic-address category-name IP Filter | match 203.0.113.5
- D. show Security dynamic-address category-name JWAS | match 203.0.113.5

Correct Answer: A

Explanation: The command "show security dynamic-address category-name DS hield" will show the IP addresses that are part of the DS hield category. By filtering the output of this command with the "match 203.0.113.5" command, you can determine if the IP address 203.0.113.5 is part of the DS hield feed. This command will check the feeds that are configured on SRX Series device and are associated to juniper ATP Cloud.

**QUESTION 11**

Exhibit

```
user@srx> show security flow session family inet6
Flow Sessions on FPC10 PIC1:
Session ID: 410000066, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/3 > 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
  Bytes: 104, CP Session ID: 410000076
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8:5::2/323;icmp6, If: .local..0, Pkts: 1,
  Bytes: 104, CP Session ID: 410000076
Session ID: 410000068, Policy name: default-policy-00/2, Timeout: 2, Valid
  In: 2001:dbf8::6:2/4 --> 2001:dbf8:5::2/7214;icmp6, If: ge-7/1/0.0, Pkts: 1,
  Bytes: 104, CP Session ID: 410000077
  Out: 2001:dbf8:5::2/7214 --> 2001:dbf8::6:2/4;icmp6, If: .local..0, Pkts: 1,
  Bytes: 104, CP Session ID: 410000077
Total sessions: 2
```

Which statement is true about the output shown in the exhibit?

- A. The SRX Series device is configured with default security forwarding options.
- B. The SRX Series device is configured with packet-based IPv6 forwarding options.
- C. The SRX Series device is configured with flow-based IPv6 forwarding options.
- D. The SRX Series device is configured to disable IPv6 packet forwarding.

Correct Answer: A

QUESTION 12

You want to use selective stateless packet-based forwarding based on the source address.

In this scenario, which command will allow traffic to bypass the SRX Series device flow daemon?

- A. set firewall family inet filter bypaa3_flowd term t1 then skip--services accept
- B. set firewall family inet filter bypass_flowd term t1 then routing-instance stateless
- C. set firewall family inet filter bypas3_flowd term t1 then virtual-channel stateless
- D. set firewall family inet filter bypass__f lowd term t1 then packet--mode

Correct Answer: C

QUESTION 13

Exhibit.



```
[edit security nat]
user@host# show
source {
  pool servers {
    address {
      198.51.100.240/32 to 198.51.100.254/32;
    }
    address-persistent subscriber ipv6-prefix-length 64;
  }
}
rule-set RS1 {
  from zone trust;
  to zone untrust;
  rule R1 {
    match {
      source-address 2001:db8::/32;
      destination-address 198.51.100.198/32;
    }
    then {
      source-nat {
        pool {
          servers;
        }
      }
    }
  }
}
```

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

- A. The configured solution allows IPv6 to IPv4 translation.
- B. The configured solution allows IPv4 to IPv6 translation.
- C. The IPv6 address is invalid.
- D. External hosts cannot initiate contact.

Correct Answer: AC

QUESTION 14

You have a webserver and a DNS server residing in the same internal DMZ subnet. The public Static NAT addresses for the servers are in the same subnet as the SRX Series devices internet-facing interface.

You implement DNS doctoring to ensure remote users can access the webserver.

Which two statements are true in this scenario? (Choose two.)

- A. The DNS doctoring ALG is not enabled by default.
- B. The Proxy ARP feature must be configured.
- C. The DNS doctoring ALG is enabled by default.
- D. The DNS CNAME record is translated.

Correct Answer: BC



QUESTION 15

Exhibit

```
user@router> show security flow session
Session ID: 36, Policy name: pre-id-default-policy/n, Timeout: 2, Valid
  In: 10.10.10.2/61606 --> 203.0.113.100/179;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
  Pkts: 1, Bytes: 64,
  Out: 203.0.113.100/179 --> 203.0.113.1/61606;tcp, Conn Tag: 0x0, If:
  .local..0, Pkts: 1, Bytes: 40,
```

Referring to the exhibit, which type of NAT is being performed?

- A. Static NAT
- B. Destination NAT
- C. Persistent NAT
- D. Source NAT

Correct Answer: D

[JN0-636 Practice Test](#)

[JN0-636 Exam Questions](#)

[JN0-636 Braindumps](#)