



# JN0-636<sup>Q&As</sup>

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.

```
[edit security ike gateway advpn-gateway]
user@srx# show
ike-policy advpn-policy;
address 192.168.3.1;
local-identity distinguished-name;
remote-identity distinguished-name container O=Juniper;
external-interface ge-0/0/3.0;
advpn {
  partner {
    disable;
  }
}
version v2-only;

[edit interfaces]
user@srx# show st0
unit 0 {
  multipoint;
  family inet {
    address 10.100.100.1/24;
  }
}
```

Referring to the exhibit, a spoke member of an ADVPN is not functioning correctly.

Which two commands will solve this problem? (Choose two.)

- A. [edit interfaces] user@srx# delete st0.0 multipoint
- B. [edit security ike gateway advpn-gateway] user@srx# delete advpn partner
- C. [edit security ike gateway advpn-gateway] user@srx# set version v1-only
- D. [edit security ike gateway advpn-gateway] user@srx# set advpn suggester disable

Correct Answer: BD

Explanation: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-auto-discovery-vpns.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discovery-vpns.html)

## QUESTION 2

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 3

Exhibit

```
Aug 1 11:28:23 11:28:23.434801:CID-0:THREAD_ID-01:RT:<172.20.101.10/59009->
>10.0.1.129/22;6,0x0> matched filter TestFilter:
Aug 1 11:28:23 11:28:23.434805:CID-0:THREAD_ID-01:RT:packet [64] ipid = 36644,
@0xef3edece
Aug 1 11:28:23 11:28:23.434810:CID-0:THREAD_ID-01:RT:---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug 1 11:28:23 11:28:23.434817:CID-0:THREAD_ID-01:RT:ge-0/0/4.0:
172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug 1 11:28:23 11:28:23.434819:CID-0:THREAD_ID-01:RT:find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug 1 11:28:23 11:28:23.434822:CID-0:THREAD_ID-01:RT:no session found, start
first path. in_tunnel - 0x0, from_cp_flag - 0
Aug 1 11:28:23 11:28:23.434826:CID-0:THREAD_ID-01:RT:flow_first_create_session
Aug 1 11:28:23 11:28:23.434834:CID-0:THREAD_ID-01:RT:flow_first_in_dst_nat: in
<ge-0/0/4.0>, out <N/A> dst_adr 10.0.1.129, sp 59009, dp 22
Aug 1 11:28:23 11:28:23.434835:CID-0:THREAD_ID-01:RT:chose interface ge-0/0/4.0
as incoming nat if.
Aug 1 11:28:23 11:28:23.434838:CID-0:THREAD_ID-01:RT:flow_first_rule_dst_xlate:
DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
```

The exhibit shows a snippet of a security flow trace.

In this scenario, which two statements are correct? (Choose two.)

- A. This packet arrived on interface ge-0/0/4.0.
- B. Destination NAT occurs.
- C. The capture is a packet from the source address 172.20.101.10 destined to 10.0.1.129.
- D. An existing session is found in the table.

Correct Answer: CD

### QUESTION 4

You are deploying a virtualization solution with the security devices in your network Each SRX Series device must support at least 100 virtualized instances and each virtualized instance must have its own discrete administrative domain. In this scenario, which solution would you choose?

- A. VRF instances



B. virtual router instances

C. logical systems

D. tenant systems

Correct Answer: C

Explanation: A logical system is a virtualization feature in SRX Series devices that allows you to create multiple, isolated virtual routers within a single physical device. Each logical system has its own routing table, firewall policies, and interfaces, and it can be managed and configured independently of the other logical systems. Logical systems are an effective way to isolate different administrative domains and to support a large number of virtualized instances.

## QUESTION 5

Exhibit

```
Aug 3 01:28:23 01:28:23.434801:CID-0:THREAD_ID-01:RT: <172.20.101.10/59009->
>10.0.1.129/22;6,0x0> matched filter MatchTraffic:
Aug 3 01:28:23 01:28:23.434805:CID-0:THREAD_ID-01:RT: packet [64] ipid =
36644, @0xef3edece
Aug 3 01:28:23 01:28:23.434810:CID-0:THREAD_ID-01:RT: ---- flow_process_pkt:
(thd 1): flow_ctxt type 15, common flag 0x0, mbuf 0x6918b800, rtbl_idx = 0
Aug 3 01:28:23 01:28:23.434817:CID-0:THREAD_ID-01:RT: ge-
0/0/4.0:172.20.101.10/59009->10.0.1.129/22, tcp, flag 2 syn
Aug 3 01:28:23 01:28:23.434819:CID-0:THREAD_ID-01:RT: find flow: table
0x206a60a0, hash 43106(0xffff), sa 172.20.101.10, da 10.0.1.129, sp 59009, dp
22, proto 6, tok 9, conn-tag 0x00000000
Aug 3 01:28:23 01:28:23.434822:CID-0:THREAD_ID-01:RT: no session found,
start first path. in_tunnel - 0x0, from_cp_flag - 0
Aug 3 01:28:23 01:28:23.434826:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Aug 3 01:28:23 01:28:23.434834:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
in <ge-0/0/3.0>, out <N/A> dst_addr 10.0.1.129, sp 59009, dp 22
Aug 3 01:28:23 01:28:23.434835:CID-0:THREAD_ID-01:RT: chose interface ge-
0/0/4.0 as incoming nat if.
Aug 3 01:28:23 01:28:23.434838:CID-0:THREAD_ID-01:RT:
flow_first_rule_dst_xlate: DST no-xlate: 0.0.0.0(0) to 10.0.1.129(22)
Aug 3 01:28:23 01:28:23.434849:CID-0:THREAD_ID-01:RT: flow_first_routing:
vr_id 0, call flow_route_lookup(): src_ip 172.20.101.10, x_dst_ip 10.0.1.129,
in ifp ge-0/0/4.0, out ifp N/A sp 59009, dp 22, ip_proto 6, tos 0
Aug 3 01:28:23 01:28:23.434861:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.1.0.129) from trust (ge-0/0/4.0 in 0) to ge-0/0/2.0, Next-hop: 10.0.1.129
Aug 3 01:28:23 01:28:23.434863:CID-0:THREAD_ID-01:RT:
flow_first_policy_search: policy search from zone trust-> zone untrust
(0x0,0xe6810016,0x16)
Aug 3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Aug 3 01:28:26 01:28:26.434137:CID-0:THREAD_ID-01:RT: denied by policy Deny-
Telnet(5), dropping pkt
Aug 3 01:28:26 01:28:26.434138:CID-0:THREAD_ID-01:RT: packet dropped,
policy deny.
```

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

[JN0-636 PDF Dumps](#)

[JN0-636 Study Guide](#)

[JN0-636 Exam Questions](#)