

## JN0-633<sup>Q&As</sup>

Security, Professional (JNCIP-SEC)

### Pass Juniper JN0-633 Exam with 100% Guarantee

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

<https://www.leads4pass.com/jn0-633.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

Click the Exhibit button.

```
user@key-server> show security group-vpn server ike security-associations Index State Initiator cookie Responder  
cookie Mode Remote Address 97 UP bb224408940cc5d 435b9404284083c2 Main 192.168.11.1 98 UP  
242c840089404d15 ab19284089408ba8 Main 192.168.11.2
```

```
user@key-server> show security group-vpn server ipsec security-associations Group: group-1, Group Id:
```

```
1 Total IPsec SAs: 1 IPsec SA Algorithm SPI Lifetime group-1-sa ESP:3des/shal 1343991c 2736
```

```
Group: group-2, Group id: 2 Total IPsec SAs: 1 IPsec SA Algorithm SPI Lifetime group-2-sa ESP:3des/shal 13be9e9  
2741
```

```
Group: group-3, Group Id: 3 Total IPsec SAs: 1 IPsec SA Algorithm SPI Lifetime group-3-sa ESP:3des/shal 20709057  
2741
```

```
Group: group-4, Group Id: 4 Total IPsec SAs: 1 IPsec SA Algorithm SPI Lifetime group-4-sa ESP:3des/shal 5111c2e1  
2741
```

Which statement is correct regarding the outputs shown in the exhibit?

Which statement is correct regarding the outputs shown in the exhibit?

- A. Two established peers are in the group VPNs.
- B. One established peer is in the group VPNs.
- C. No established peer is in the group VPNs.
- D. Four established peers are in the group VPNs.

Correct Answer: A

---

## QUESTION 2

What is a secure key management protocol used by IPsec?

- A. AH
- B. ESP
- C. TCP
- D. IKE

Correct Answer: D

---

## QUESTION 3

Click the Exhibit button.

```
user@host> monitor traffic interface ge-0/0/3
```

verbose output suppressed, use or for full protocol decode

Address resolution is ON. Use to avoid any reverse lookup delay.

Address resolution timeout is 4s.

Listening on ge-0/0/3, capture size 96 bytes

Reverse lookup for 172.168.3.254 failed (check DNS reachability). Other reverse lookup failures will not be reported.

Use to avoid reverse lookups on IP addresses.

```
19:24:16.320907 In arp who-has 172.168.3.254 tell 172.168.3.1
```

```
19:24:17.322751 In arp who has 172.168.3.254 tell 172.168.3.1
```

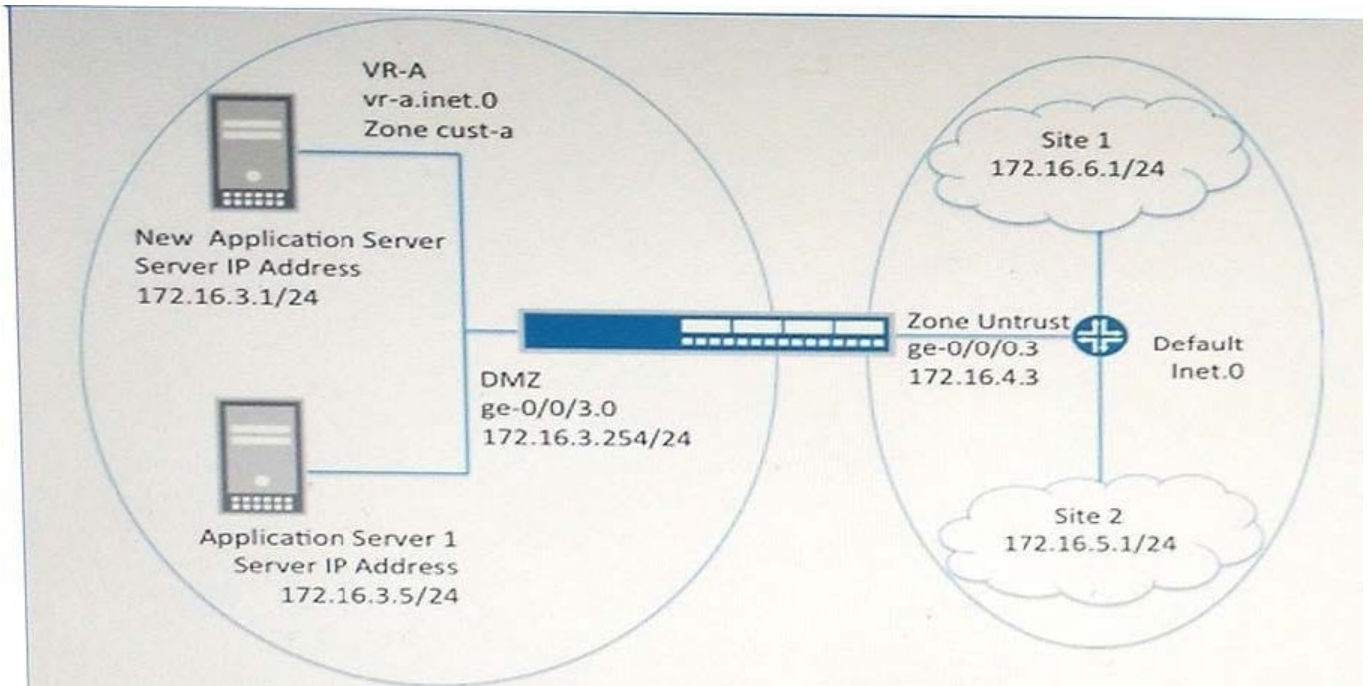
```
19:24:18.328895 In arp who-has 172.168.3.254 tell 172.168.3.1
```

```
19:24:18.332956 In arn who has 172.168.3.254 tell 172.168.3.1
```

A new server has been set up in your environment. The administrator suspects that the firewall is blocking the traffic from the new server. Previously existing servers in the VLAN are working correctly. After reviewing the logs, you do not see any traffic for the new server.

Referring to the exhibit, what is the cause of the problem?

Exhibit:



- A. The server is in the wrong VLAN.
- B. The server has been misconfigured with the wrong IP address.
- C. The firewall has been misconfigured with the incorrect routing-instance.
- D. The firewall has a filter enabled to block traffic from the server.

Correct Answer: C

**QUESTION 4**

A security administrator has configured an IPsec tunnel between two SRX devices. The devices are configured with OSPF on the st0 interface and an external interface destined to the IPsec endpoint. The administrator notes that the IPsec tunnel and OSPF adjacency keep going up and down. Which action would resolve this issue?

- A. Create a firewall filter on the st0 interface to permit IP protocol 89.
- B. Configure the IPsec tunnel to accept multicast traffic.
- C. Create a /32 static route to the IPsec endpoint through the external interface.
- D. Increase the OSPF metric of the external interface.

Correct Answer: C

**QUESTION 5**

-- Exhibit -[edit forwarding-options] user@srx240# show packet-capture {

```
file filename my-packet-capture;
```

```
maximum-capture-size 1500; } -- Exhibit -
```

Referring to the exhibit, you are attempting to perform a packet capture on an SRX240 to troubleshoot an SSH issue in your network. However, no information appears in the packet capture file.

Which firewall filter must you apply to the necessary interface to collect data for the packet capture?

A. user@srx240# show filter pkt-capture { term pkt-capture-term {

```
from {
```

```
protocol tcp;
```

```
port ssh;
```

```
}
```

```
then packet-mode;
```

```
}
```

```
term allow-all {
```

```
then accept;
```

```
}
```

```
}
```

```
[edit firewall family inet]
```

B. user@srx240# show filter pkt-capture { term pkt-capture-term {

```
from {
```

```
protocol tcp;
```

```
port ssh;
```

```
}
```

```
then {
```

```
count packet-capture;
```

```
}
```

```
}
```

```
term allow-all {
```

```
then accept;
```

```
}
```

```
}
```

```
[edit firewall family inet]
```

```
C. user@srx240# show filter pkt-capture { term pkt-capture-term {
```

```
from {
```

```
protocol tcp;
```

```
port ssh;
```

```
}
```

```
then {
```

```
routing-instance packet-capture;
```

```
}
```

```
}
```

```
term allow-all {
```

```
then accept;
```

```
}
```

```
}
```

```
[edit firewall family inet]
```

```
D. user@srx240# show
```

```
filter pkt-capture {
```

```
term pkt-capture-term {
```

```
from {
```

```
protocol tcp;
```

```
port ssh;
```

```
}
```

```
then {
```

```
sample;
```

```
accept;
```

```
}
```

```
}
```

```
term allow-all {
```

then accept;

}

}

[edit firewall family inet]

Correct Answer: D

[JN0-633 PDF Dumps](#)

[JN0-633 Practice Test](#)

[JN0-633 Study Guide](#)