



# 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.passapply.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

You want to implement persistent NAT for an internal resource so that external hosts are able to initiate communications to the resource, without the internal resource having previously sent packets to the external hosts. Which configuration setting will accomplish this goal?

- A. persistent-nat permit target-host
- B. persistent-nat permit any-remote-host
- C. persistent-nat permit target-host-port
- D. address-persistent

Correct Answer: B

---

### QUESTION 2

-- Exhibit -[edit security idp]

user@srx# show | no-more

idp-policy basic {

rulebase-ips {

rule 1 {

match {

from-zone untrust;

source-address any;

to-zone trust;

destination-address any;

application default;

attacks {

custom-attacks data-inject;

}

}

then {

action {

recommended;



```
}  
  
notification {  
  
log-attacks; } } } }  
  
active-policy basic;  
  
custom-attack data-inject { recommended-action close; severity critical; attack-type {  
  
signature {  
  
context mssql-query;  
  
pattern "SELECT * FROM accounts";  
  
direction client-to-server;  
  
}  
  
} } -- Exhibit -
```

You have configured the custom attack signature shown in the exhibit. This configuration is valid, but you want to improve the efficiency and performance of your IDP.

Which two commands should you use? (Choose two.)

- A. set custom attack data-inject recommended-action drop
- B. set custom-attack data-inject attack-type signature protocol-binding tcp
- C. set idp-policy basic rulebase-ips rule 1 match destination-address webserver
- D. set idp-policy basic rulebase-ips rule 1 match application any

Correct Answer: BC

---

### QUESTION 3

Which AppSecure module provides Quality of Service?

- A. AppTrack
- B. AppFW
- C. AppID
- D. AppQoS

Correct Answer: D

---

### QUESTION 4



You have a group IPsec VPN established with a single key server and five client devices. Regarding this scenario, which statement is correct?

- A. There is one unique Phase 1 security association and five unique Phase 2 security associations used for this group.
- B. There is one unique Phase 1 security association and one unique Phase 2 security association used for this group.
- C. There are five unique Phase 1 security associations and five unique Phase 2 security associations used for this group.
- D. There are five unique Phase 1 security associations and one unique Phase 2 security association used for this group.

Correct Answer: D

---

#### QUESTION 5

You are working as a security administrator and must configure a solution to protect against distributed botnet attacks on your company's central SRX cluster.

How would you accomplish this goal?

- A. Configure AppTrack to inspect and drop traffic from the malicious hosts.
- B. Configure AppQoS to block the malicious hosts.
- C. Configure AppDoS to rate limit connections from the malicious hosts.
- D. Configure AppID with a custom application to block traffic from the malicious hosts.

Correct Answer: C

---

#### QUESTION 6

What is a benefit of using a dynamic VPN?

- A. It provides a layer of redundancy on top of a point-to-point VPN mesh architecture.
- B. It eliminates the need for point-to-point VPN tunnels.
- C. It provides a way to grant VPN access on a per-user-group basis.
- D. It simplifies IPsec access for remote clients.

Correct Answer: D

---

#### QUESTION 7

Click the Exhibit button.



You have configured an IDP policy as shown in the exhibit. The configuration commits successfully. Which traffic will be examined for attacks?

Exhibit:

```
[edit security idp]
user@srx# show
idp-policy basic {
    rulebase-ips {
        rule 1 {
            match {
                from-zone Trust;
                source-address any;
                to-zone Untrust;
                destination-address any;
                application default;
                attacks {
                    predefined-attack-groups "APP - All";
                }
            }
            then {
                action {
                    recommended;
                }
                notification {
                    log-attacks;
                }
            }
        }
    }
}
active-policy basic;
```

- A. only originating traffic from source to destination in a session
- B. only reply traffic from destination to source in a session
- C. both originating and reply traffic between hosts in a session
- D. recommended traffic between the source and destination hosts

Correct Answer: C

---

## QUESTION 8

Click the Exhibit button.

Based on the output shown in the exhibit, what are two results? (Choose two.)

Exhibit:



```
user@srx> show security flow session
Session ID: 136, Policy name: Trust-Web-Server-Int/4, Timeout: 1794, Valid
  In: 192.168.1.10/60246 --> 172.16.1.7/80;tcp, If: ge-0/0/8.0, Pkts: 3, Bytes: 176
  Out: 192.168.10.100/80 --> 192.168.1.10/60246;tcp, If: ge-0/0/9.0, Pkts: 2, Bytes: 120
Total sessions: 1
```

- A. The output shows source NAT.
- B. The output shows destination NAT.
- C. The port information is changed.
- D. The port information is unchanged.

Correct Answer: BD

---

### QUESTION 9

You must configure a central SRX device connected to two branch offices with overlapping IP address space. The branch office connections to the central SRX device must reside in separate routing instances. Which two components are required? (Choose two.)

- A. virtual routing instance
- B. forwarding instance
- C. static NAT
- D. persistent NAT

Correct Answer: AC

---

### QUESTION 10

What is a secure key management protocol used by IPsec?

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

Correct Answer: D

---

### QUESTION 11

You are asked to configure class of service (CoS) on an SRX device running in transparent mode. Which command would you use?



- A. set interfaces ge-0/0/0 unit 0 classifiers dscp priority-app
- B. set class-of-service interfaces ge-0/0/0 unit 0 classifiers dscp priority-app
- C. set class-of-service interfaces ge-0/0/0 unit 0 classifiers ieee-802.1 priority-app
- D. set interfaces ge-0/0/0 unit 0 classifiers inet-precedence priority-app

Correct Answer: C

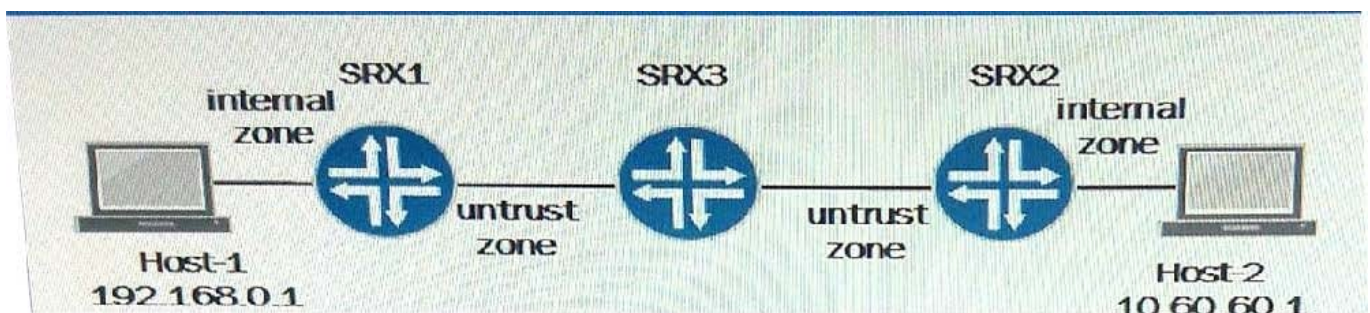
## QUESTION 12

Click the Exhibit button.

```
[edit security nat static rule-set 12] user@SRX2# show from zone untrust; rule 1 {  
  match {  
    destination-address 192.168.1.1/32;  
  }  
  then {  
    static-nat {  
      prefix {  
        10.60.60.1/32;  
      }  
    }  
  }  
}
```

Host-2 initiates communication with Host-1. All other routing and policies are in place to allow the traffic. What is the result of the communication?

Exhibit:



- A. The 192.168.0.1 address is translated to the 10.60.60.1 address.



- B. The 10.60.60.1 address is translated to the 192.168.1.1 address.
- C. No translation occurs.
- D. The 192.168.0.1 address is translated to the 192.168.1.1 address.

Correct Answer: B

---

### QUESTION 13

You must ensure that your Layer 2 traffic is secured on your SRX Series device in transparent mode.

What must be considered when accomplishing this task?

- A. Layer 2 interfaces must use the ethernet-switchingprotocol family.
- B. Security policies are not supported when operating in transparent mode.
- C. Screens are not supported in your security zones with transparent mode.
- D. You must reboot your device after configuring transparent mode.

Correct Answer: D

---

### QUESTION 14

Which configurable SRX Series device feature allows you to capture transit traffic?

- A. syslog
- B. traceoptions
- C. packet-capture
- D. archival

Correct Answer: B

---

### QUESTION 15

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

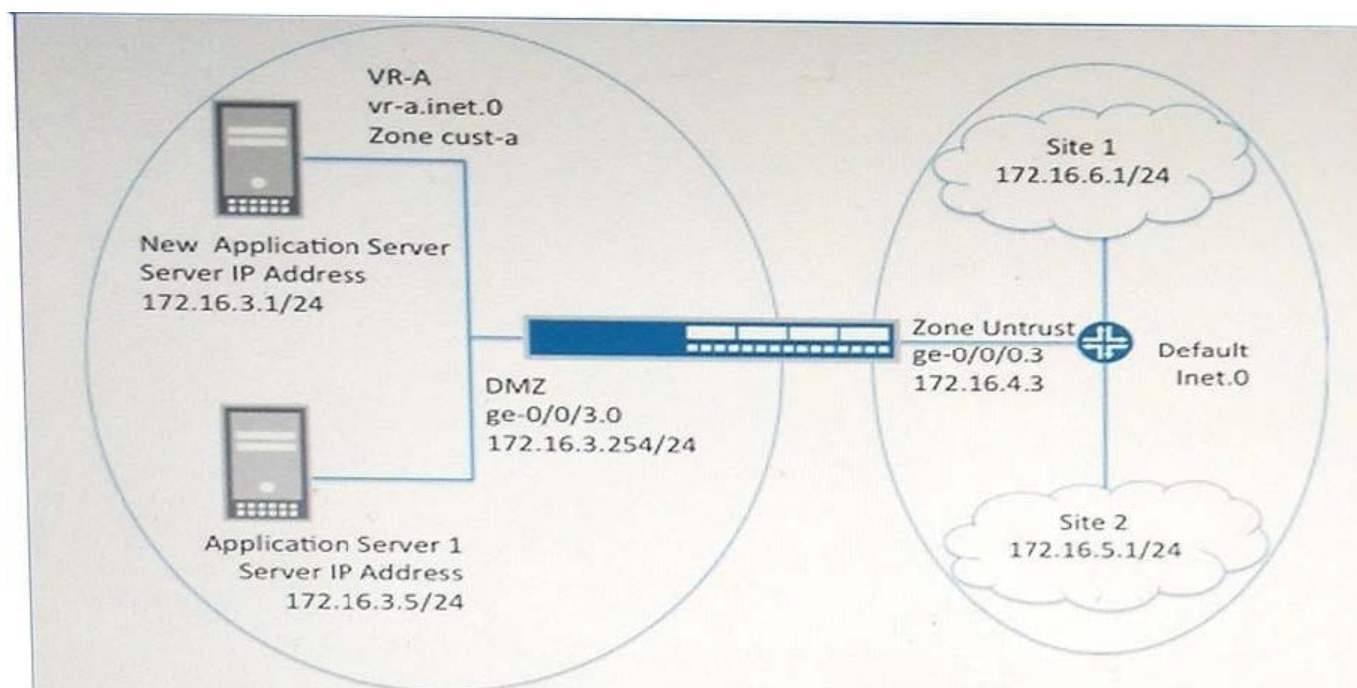
19:24:18.328895 In arp who-has 172.168.3.254 tell 172.168.3.1

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



VCE & PDF

PassApply.com

<https://www.passapply.com/jn0-633.html>

2024 Latest passapply JN0-633 PDF and VCE dumps Download

---

[JN0-633 PDF Dumps](#)

[JN0-633 Exam Questions](#)

[JN0-633 Braindumps](#)