

**100%** Money Back  
**Guarantee**

**Vendor:**Juniper

**Exam Code:**JN0-333

**Exam Name:**Security, Specialist (JNCIS-SEC)

**Version:**Demo

## QUESTION 1

Click the Exhibit button.

```
user@host> show security ike security-associations

user@host> show route 172.16.1.2

inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.1.0/24          *[Static/5] 00:04:21
                    > via st0.0

user@host> ping 172.16.1.2 source 172.16.1.1
PING 172.16.1.2 (172.16.1.2): 56 data bytes
64 bytes from 172.16.1.2: icmp_seq=0 ttl=64 time=3.428 ms
64 bytes from 172.16.1.2: icmp_seq=1 ttl=64 time=1.367 ms
64 bytes from 172.16.1.2: icmp_seq=2 ttl=64 time=1.911 ms
```

You have an IPsec tunnel between two devices. You clear the IKE security associations, but traffic continues to flow across the tunnel.

Referring to the exhibit, which statement is correct in this scenario?

- A. The IPsec security association is independent from the IKE security association
- B. The traffic is no longer encrypted
- C. The IKE security association immediately reestablishes
- D. The traffic is using an alternate path

Correct Answer: AB

---

## QUESTION 2

Click the Exhibit button.

```
user@host> show security ike active-peer detail
```

```
Peer address: 31.0.0.6, Port: 500,  
Peer IKE-ID: C=US, ST=California, L=Sunnyvale, O=Example, OU=sales, CN=SPOKE9061  
XAUTH username: not available  
Assigned network attributes:  
IP Address: 0.0.0.0, netmask : 0.0.0.0  
DNS Address : 0.0.0.0, DNS2 Address : 0.0.0.0  
WINS Address : 0.0.0.0, WINS2 Address : 0.0.0.0  
  
Previous Peer address : 0.0.0.0, Port : 0  
Active IKE SA indexes : 75203629  
IKE SA negotiated : 1  
IPSec tunnels active : 1, IPSec Tunnel IDs : 68157442  
  
DPD Config Info : Mode: always-send Interval: 60 Threshold: 5 plsa_index:75203629  
DPD Statistics : DPD-flags: REMOTE_ACCESS  
DPD Statistics : DPD TTL : 0 DPD seq-no : 0  
DPD Statistics : DPD Req Sent : 0 DPD Resp Rcvd : 0
```

A customer would like to monitor their VPN using dead peer detection.

Referring to the exhibit, for how many minutes was the peer down before the customer was notified?

- A. 5
- B. 3
- C. 4
- D. 2

Correct Answer: A

---

### QUESTION 3

What are two valid zones available on an SRX Series device? (Choose two.)

- A. security zones
- B. policy zones
- C. transit zones
- D. functional zones

Correct Answer: AD

---

### QUESTION 4

Click the Exhibit button.

```

user@host# show security nat
destination {
  pool dst-nat-pool-1 {
    address 192.168.1.200/32 port 80;
  }
  pool dst-nat-pool-2 {
    address 192.168.1.220/32 port 8000;
  }
  rule-set rsl {
    from zone untrust;
    rule r1 {
      match {
        destination-address 203.0.113.200/32;
        destination-port 80;
      }
      then {
        destination-nat pool dst-nat-pool-1;
      }
    }
    rule r2 {
      match {
        destination-address 203.0.113.200/32;
        destination-port 8000;
      }
      then {
        destination-nat pool dst-nat-pool-2;
      }
    }
  }
}

```

Which feature is enabled with destination NAT as shown in the exhibit?

- A. NAT overload
- B. block allocation
- C. port translation
- D. NAT hairpinning

Correct Answer: D

#### QUESTION 5

Which statement is true about Perfect Forward Secrecy (PFS)?

- A. PFS is used to resolve compatibility issues with third-party IPsec peers.
- B. PFS is implemented during Phase 1 of IKE negotiations and decreases the amount of time required for IKE negotiations to complete.
- C. PFS increases security by forcing the peers to perform a second DH exchange during Phase 2.

D. PFS increases the IPsec VPN encryption key length and uses RSA or DSA certificates.

Correct Answer: C

---

### QUESTION 6

Click to the Exhibit button.

```
user@host# show security nat
static {
    rule-set rsl {
        from zone untrust;
        rule rl {
            match {
                destination-address 1.1.1.200/32;
            }
            then {
                static-nat prefix 192.168.1.200/32;
            }
        }
    }
}
proxy-arp {
    interface ge-0/0/0.0 {
        address {
            1.1.1.200/32;
        }
    }
}
```

Referring to the exhibit, what does proxy ARP allow?

- A. the internal network to ARP for the internal address of the server
- B. the external network to ARP for the internal address of the server
- C. the internal network to ARP for the public address of the server
- D. the external network to ARP for the public address of the server

Correct Answer: A

---

### QUESTION 7

Click the Exhibit button.

```
security {
  nat {
    source {
      pool pool-1 {
        address {
          10.1.1.8/32;
        }
      }
      rule-set rs-1 {
        from zone untrust;
        to zone trust;
        rule rule-1 {
          match {
            source-address 2001:db8::8/128;
            destination-address 10.1.1.5/32;
          }
          then {
            source-nat {
              pool {
                pool-1;
                persistent-nat {
                  permit any-remote-host;
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Referring to the exhibit, which action will be taken for traffic coming from the untrust zone going to the trust zone?

- A. Source address 2001:db8::8 will be translated to 10.1.1.5.
- B. Source address 2001:db8::8 will be translated to 10.1.1.8.
- C. Source address 10.1.1.8 will be translated to 2001:db8::8.
- D. Source address 10.1.1.5 will be translated to 2001:db8::8.

Correct Answer: B

---

### QUESTION 8

Which process describes the implementation of screen options on an SRX Series device?

- A. Configured screen options are only applied when traffic does not match a valid route.
- B. Configured screen options are applied only to the first packet that is processed in a stateful session.
- C. Configured screen options are applied to all packets that are processed by the stateful session firewall processor.

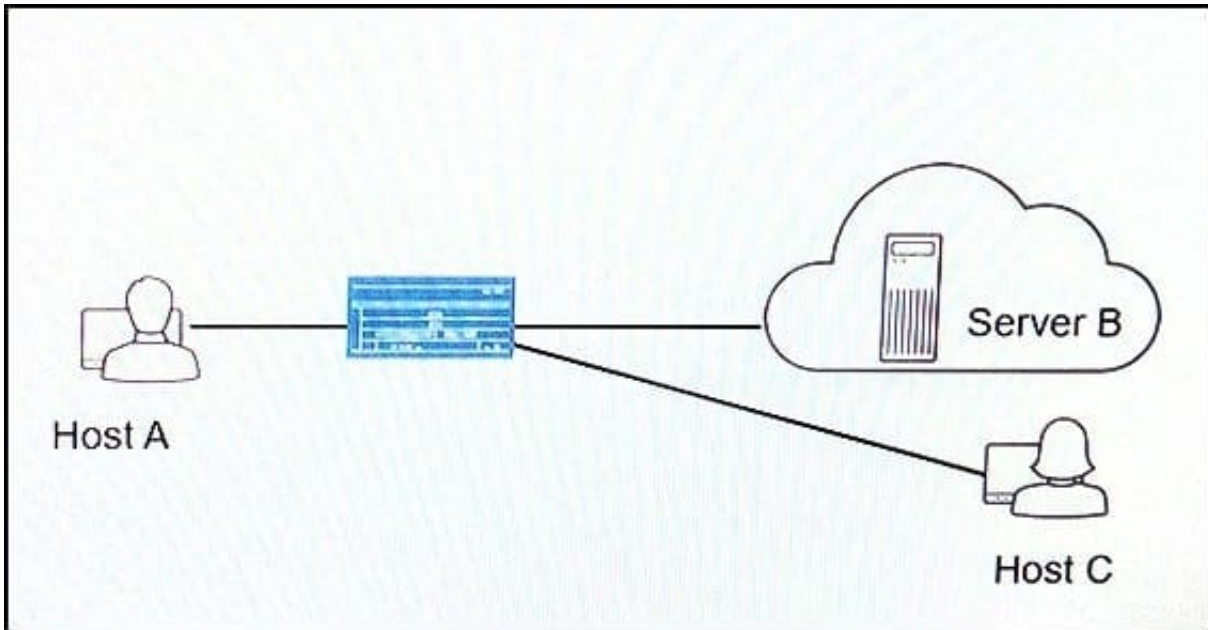
D. Configured screen options are only applied when traffic does not match a valid policy.

Correct Answer: C

---

### QUESTION 9

Click the Exhibit button.



You have configured NAT on your network so that Host A can communicate with Server B. You want to ensure that Host C can initiate communication with Host A using Host A's reflexive address.

Referring to the exhibit, which parameter should you configure on the SRX Series device to satisfy this requirement?

- A. Configure persistent NAT with the target-host parameter.
- B. Configure persistent NAT with the target-host-port parameter.
- C. Configure persistent NAT with the any-remote-host parameter.
- D. Configure persistent NAT with the port-overloading parameter.

Correct Answer: A

---

### QUESTION 10

A session token on an SRX Series device is derived from what information? (Choose two.)

- A. routing instance
- B. zone
- C. screen

D. MAC address

Correct Answer: AB

---

#### QUESTION 11

You have recently configured an IPsec tunnel between two SRX Series devices. One of the devices is assigned an IP address using DHCP with an IP address that changes frequently. Initial testing indicates that the IPsec tunnel is not working. Troubleshooting has revealed that Phase 1 negotiations are failing.

Which two actions would solve the problem? (Choose two.)

- A. Verify that the device with the IP address assigned by DHCP is the traffic initiator.
- B. Verify that VPN monitoring is enabled.
- C. Verify that the IKE policy is configured for aggressive mode.
- D. Verify that PKI is properly configured.

Correct Answer: AC

---

#### QUESTION 12

Your network includes IPsec tunnels. One IPsec tunnel transits an SRX Series device with NAT configured. You must ensure that the IPsec tunnels function properly.

Which statement is correct in this scenario?

- A. Persistent NAT should be enabled.
- B. NAT-T should be enabled.
- C. Destination NAT should be configured.
- D. A source address pool should be configured.

Correct Answer: B