

JN0-332^{Q&As}

Juniper Networks Certified Internet Specialist, SEC (JNCIS-SEC)





Pass Juniper JN0-332 Exam with 100% Guarantee

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

<https://www.leads4pass.com/jn0-332.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.

```
admin@SRX210> show security utm web-filtering status
UTM web-filtering status:
  Server status: SC-CPA server down
```

What are two valid reasons for the output shown in the exhibit? (Choose two.)

- A. The local Web-filtering daemon is not enabled or is not running.
- B. The integrated Web-filtering policy server is not reachable.
- C. No DNS is configured on the SRX Series device.
- D. No security policy is configured to use Web filtering.

Correct Answer: BC

QUESTION 2

Click the Exhibit button.

[edit security]

user@host# show

```
ike {
  policy ike-policy1 {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$GFjm5OBEclM5QCuO1yrYgo"; ## SECRET-DATA }
  gateway remote-ike {
    ike-policy ike-policy1;
    address 172.19.51.170;
    external-interface ge-0/0/3.0;
  }
  ipsec {
    policy vpn-policy1 {
```

```
proposal-set standard;  
  
}  
  
vpn remote-vpn {  
  
ike {  
  
gateway remote-ike;  
  
ipsec-policy vpn-policy1;  
  
}}}
```

Assuming you want to configure a route-based VPN, which command is required to bind the VPN to secure tunnel interface st0.0?

- A. set ipsec vpn remote-vpn bind-interface st0.0
- B. set ike gateway remote-ike bind-interface st0.0
- C. set ike policy ike-policy1 bind-interface st0.0
- D. set ipsec policy vpn-policy1 bind-interface st0.0

Correct Answer: A

QUESTION 3

-- Exhibit -

```
user@host# show chassis cluster
```

```
reth-count 2;  
  
redundancy-group 1 {  
  
node 0 priority 200;  
  
node 1 priority 100;  
  
interface-monitor {  
  
ge-0/0/5 weight 85;  
  
ge-0/0/6 weight 85;  
  
ge-0/0/7 weight 85;  
  
ge-0/0/8 weight 85;  
  
ge-5/0/5 weight 85;  
  
ge-5/0/6 weight 85;
```

```
ge-5/0/7 weight 85;
```

```
ge-5/0/8 weight 85;
```

```
}
```

```
}
```

-- Exhibit -

Click the Exhibit button.

Referring to the exhibit, you have two SRX Series devices in a chassis cluster, and Node 0 is currently the primary node. You want to ensure that traffic, using those interfaces, fails over to Node 1 when all interfaces go down.

Which configuration change should be made to ensure failover to Node 1?

- A. Decrease the weight of the interfaces to 1.
- B. Increase the weight of the interfaces to 255.
- C. Increase the weight of the interfaces to between 86 and 128.
- D. Decrease the weight of the interfaces to between 64 and 84.

Correct Answer: D

QUESTION 4

Click the Exhibit button.

```
Oct 8 10:39:40 RMD_PM_P1_POLICY_LOOKUP_FAILURE: Policy lookup for Phase-1 [response failed for p1_local=ipv4 (any: 3, [0..3]=1.1.1.2) p1_remote=ipv4 (any: 0, [0..3]=2.2.2.2)
```

You are the responder for an IPsec tunnel and you see the error messages shown in the exhibit. What is the problem?

- A. One or more of the phase 1 proposals such as authentication algorithm, encryption algorithm, or preshared key does not match.
- B. There is no route for 2.2.2.2.
- C. There is no IKE definition in the configuration for peer 2.2.2.2.
- D. system services ike is not enabled on the interface with IP 1.1.1.2.

Correct Answer: C

QUESTION 5

Click the Exhibit button.

```
[edit security policies from-zone trust to-zone untrust]
user@host# show
policy tunnel-traffic {
    match {
        source-address local-net;
        destination-address remote-net;
        application any;
    }
    then {
        permit;
    }
}
```

Which command is needed to change this policy to a tunnel policy for a policy-based VPN?

- A. set policy tunnel-traffic then tunnel remote-vpn
- B. set policy tunnel-traffic then permit tunnel remote-vpn
- C. set policy tunnel-traffic then tunnel ipsec-vpn remote-vpn permit
- D. set policy tunnel-traffic then permit tunnel ipsec-vpn remote-vpn

Correct Answer: D

QUESTION 6

Referring to the exhibit, you see that Node 0 is currently primary for redundancy Group 0. You have not yet configured any chassis cluster parameters. You want to ensure that Node 1 is always the primary node for this redundancy group if both nodes reboot at same time.

Which configuration step would accomplish this task?

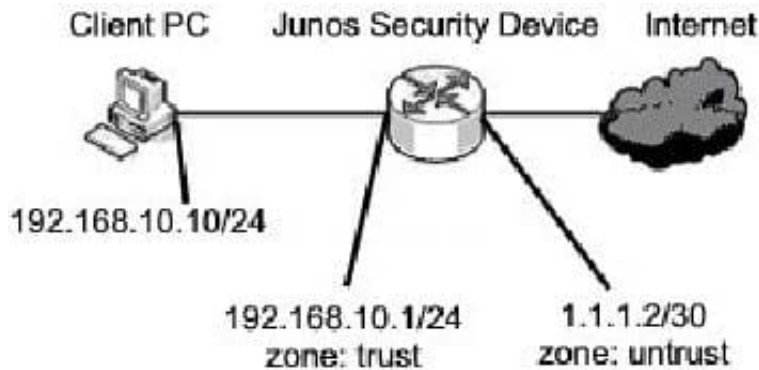
```
user@host>show chassis cluster status cluster ID: 1 Node Priority Status Preempt Manual Failover Redundancy group:
0 ,Failover count: 1 Node0 1 primary no no Node1 1 secondary no no
```

- A. user@host# set chassis cluster redundancy-group 0 node 1 priority 1
- B. user@host# set chassis cluster redundancy-group 0 node 1
- C. user@host# set chassis cluster redundancy-group 0 preempt
- D. user@host# set chassis cluster redundancy-group 0 node 0 priority 255
- E. user@host# set chassis cluster redundancy-group 0 node 1 priority 254

Correct Answer: E

QUESTION 7

Click the Exhibit button.



Which type of source NAT is configured in the exhibit?

- A. interface-based source NAT
- B. static source NAT
- C. pool-based source NAT with PAT
- D. pool-based source NAT without PAT

Correct Answer: A

QUESTION 8

Which two statements are correct about security policy schedulers on an SRX Series device? (Choose two.)

- A. A scheduler can be applied in multiple policies.
- B. You can only apply one scheduler per device.
- C. You can only apply one scheduler per policy.
- D. A scheduler can only be applied to a single policy.

Correct Answer: AC

QUESTION 9

Click the Exhibit button.

```
user@host> show configuration security nat
pool TO_INTERNET {
    address {
        3.3.3.100/32 to 3.3.3.110/32;
    }
    host-address-base 10.200.104.21/32;
}
rule-set TO_INTERNET-1 {
    from interface ge-0/0/4.104;
    to zone UNTRUST;
    rule 1 {
        match {
            destination-address 0.0.0.0/0;
        }
        then {
            source-nat {
                pool {
                    TO_INTERNET;
                }
            }
        }
    }
}
rule-set TO_INTERNET-2 {
    from zone TRUST;
    to zone UNTRUST;
    rule 2 {
        match {
            source-address 10.200.104.0/24;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
```

Users are able to access hosts on the Internet, however, they are using the TO_INTERNET pool instead of the IP address associated with the external interface for the translations.

Referring to the exhibit, why is the traffic using the source NAT pool instead of the IP address that is associated with the external interface for translations on the SRX Series device?

- A. The INTERNET-1 rule set is listed before the INTERNET-2 rule set in the configuration hierarchy.
- B. The INTERNET-2 rule set is not configured with a destination address of 0.0.0.0/0 in the match criterion.
- C. The INTERNET -1 rule set is configured with the more specific from criterion.
- D. The INTERNET -2 rule set is configured with the more specific from criterion.

Correct Answer: A

QUESTION 10

You have just changed a NAT rule and committed the change. Which statement is true?

- A. Affected sessions remain active and are not updated until the sessions restart.
- B. Affected sessions are torn down and are re-initiated as soon as the SRX device receives matching traffic.
- C. Affected sessions are torn down and are immediately re-initiated.
- D. Affected sessions are dynamically updated with the configuration change.

Correct Answer: B

QUESTION 11

Which three security concerns can be addressed by a tunnel mode IPsec VPN secured by AH? (Choose three.)

- A. data integrity
- B. data confidentiality
- C. data authentication
- D. outer IP header confidentiality
- E. outer IP header authentication

Correct Answer: ACE

QUESTION 12

When an SRX series device receives an ESP packet, what happens?

- A. If the destination address of the outer IP header of the ESP packet matches the IP address of the ingress interface, it

will immediately decrypt the packet.

B. If the destination IP address in the outer IP header of ESP does not match the IP address of the ingress interface, it will discard the packet.

C. If the destination address of the outer IP header of the ESP packet matches the IP address of the ingress interface, based on SPI match, it will decrypt the packet.

D. If the destination address of the outer IP header of the ESP packet matches the IP address of the ingress interface, based on SPI match and route lookup of inner header, it will decrypt the packet.

Correct Answer: C

QUESTION 13

-- Exhibit -

```
user@host> show security ipsec security-associations Total active tunnels: 1 ID Algorithm SPI Life:sec/kb Mon vsys
Port Gateway 131073 ESP:3des/sha1 cbc9281a 2532/ unlim - root 4500 1.1.1.1
```

```
user@host> show security ipsec security-associations detail Virtual-system: root Local Gateway: 1.0.0.1, Remote
Gateway: 1.1.1.1 Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0) Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv1 DF-bit: clear Direction: inbound, SPI: ac23df79, AUX-SPI: 0 , VPN Monitoring: Hard lifetime. Expires in
3186 seconds Lifesize Remaining: Unlimited Soft lifetime. Expires in 2578 seconds Mode. Tunnel, Type. dynamic,
State. installed Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc Anti-replay service. counter-based
enabled, Replay window size. 64 Direction: outbound, SPI: cbc9281a, AUX-SPI: 0 , VPN Monitoring: Hard lifetime.
Expires in 3186 seconds Lifesize Remaining: Unlimited Soft lifetime. Expires in 2578 seconds Mode. Tunnel, Type.
dynamic, State. installed Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc Anti-replay service.
counter-based enabled, Replay window size. 64 -- Exhibit -
```

Click the Exhibit button.

The exhibit shows output from two show commands.

What are two conclusions about the VPN tunnel from the output? (Choose two.)

- A. VPN monitoring is enabled.
- B. There is a device performing NAT between the two VPN endpoints.
- C. 3DES is the encryption protocol.
- D. Traffic with the DF-bit set that exceeds the MTU will be dropped.

Correct Answer: BC

QUESTION 14

An engineer has just created a single policy allowing ping traffic from a host in the Users zone to a server in the Servers zone.

When the host pings the server, what will happen to the return traffic?

- A. The return traffic will match the session and will be permitted.
- B. The return traffic will match the new policy and will be permitted.
- C. The return traffic will not be permitted; it will need a separate policy.
- D. The return traffic will not be permitted; it will match the system default policy.

Correct Answer: A

QUESTION 15

An attacker sends a low rate of TCP SYN segments to hosts, hoping that at least one port replies. Which type of an attack does this scenario describe?

- A. DoS
- B. SYN flood
- C. port scanning
- D. IP address sweep

Correct Answer: C

[Latest JN0-332 Dumps](#)

[JN0-332 PDF Dumps](#)

[JN0-332 Braindumps](#)