JN0-333 Q&As

Security, Specialist (JNCIS-SEC)

Pass Juniper JN0-333 Exam with 100% Guarantee

QUESTION 1

You want to ensure that any certificates used in your IPsec implementation do not expire while in use by your SRX Series devices.

In this scenario, what must be enabled on your devices?

A. RSA

B. TLS

C. SCEP

D. CRL

Correct Answer: C

QUESTION 2

Which SRX5400 component is responsible for performing first pass security policy inspection?

A. Routing Engine

B. Switch Control Board

C. Services Processing Unit

D. Modular Port Concentrator

Correct Answer: C

QUESTION 3

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

QUESTION 4

Which three elements does AH provide in an IPsec implementation? (Choose three.)

A. confidentiality

B. authentication

C. integrity

D. availability

E. replay attack protection

Correct Answer: BCE

QUESTION 5

You want to protect your SRX Series device from the ping-of-death attack coming from the untrust security zone.

How would you accomplish this task?

A. Configure the host-inbound-traffic system-services ping except parameter in the untrust security zone.

B. Configure the application tracking parameter in the untrust security zone.

C. Configure a from-zone untrust to-zone trust security policy that blocks ICMP traffic.

D. Configure the appropriate screen and apply it to the [edit security zone security-zone untrust] hierarchy.

Correct Answer: D

QUESTION 6

What are three characteristics of session-based forwarding, compared to packet-based forwarding, on an SRX Series device? (Choose three.)

A. Session-based forwarding uses stateful packet processing.

B. Session-based forwarding requires less memory.

C. Session-based forwarding performs faster processing of existing session.

D. Session-based forwarding uses stateless packet processing,

E. Session-based forwarding uses six tuples of information.

Correct Answer: ACE

QUESTION 7

You want to trigger failover of redundancy group 1 currently running on node 0 and make node 1 the primary node the redundancy group 1.

Which command would be used accomplish this task?

A. user@host# set chassis cluster redundancy-group 1 node 1

B. user@host> request chassis cluster failover redundancy-group 1 node 1

C. user@host# set chassis cluster redundancy-group 1 preempt

D. user@host> request chassis cluster failover reset redundancy-group 1

Correct Answer: B

QUESTION 8

You are asked to support source NAT for an application that requires that its original source port not be changed.

Which configuration would satisfy the requirement?

A. Configure a source NAT rule that references an IP address pool with interface proxy ARP enabled.

B. Configure the egress interface to source NAT fixed-port status.

C. Configure a source NAT rule that references an IP address pool with the port no-translation parameter enabled.

D. Configure a source NAT rule that sets the egress interface to the overload status.

Correct Answer: C

QUESTION 9

Which UDP port is used in Ipsec tunneling when NAT-T is in use?

A. 50

B. 4500

C. 500

D. 51

Correct Answer: B

QUESTION 10

You are changing the default vCPU allocation on a vSRX. How are the additional vCPUs allocated in this scenario?

A. The vCPU are allocated equally across the Junos control plane and packet forwarding engine.

B. One dedicated vCPU is allocated for the Junos control plane and the remaining vCPUs for the packet forwarding engine.

C. One dedicated vCPU is allocated for the packet forwarding engine, one for the Junos control plane, and the remaining vCPUs are equally balanced.

D. One dedicated vCPU is allocated for the packet forwarding engine and the remaining vCPUs for the Junos plane.

Correct Answer: B

QUESTION 11

Which two statements are true about global security policies? (Choose two.)

A. Global security policies are evaluated before regular security policies.

B. Global security policies can be configured to match addresses across multiple zones.

C. Global security policies can match traffic regardless of security zones.

D. Global security policies do not support IPv6 traffic.

Correct Answer: BC

QUESTION 12

Which feature is used when you want to permit traffic on an SRX Series device only at specific times?

A. scheduler

B. pass-through authentication

C. ALGs

D. counters

Correct Answer: A

QUESTION 13

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 14

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.

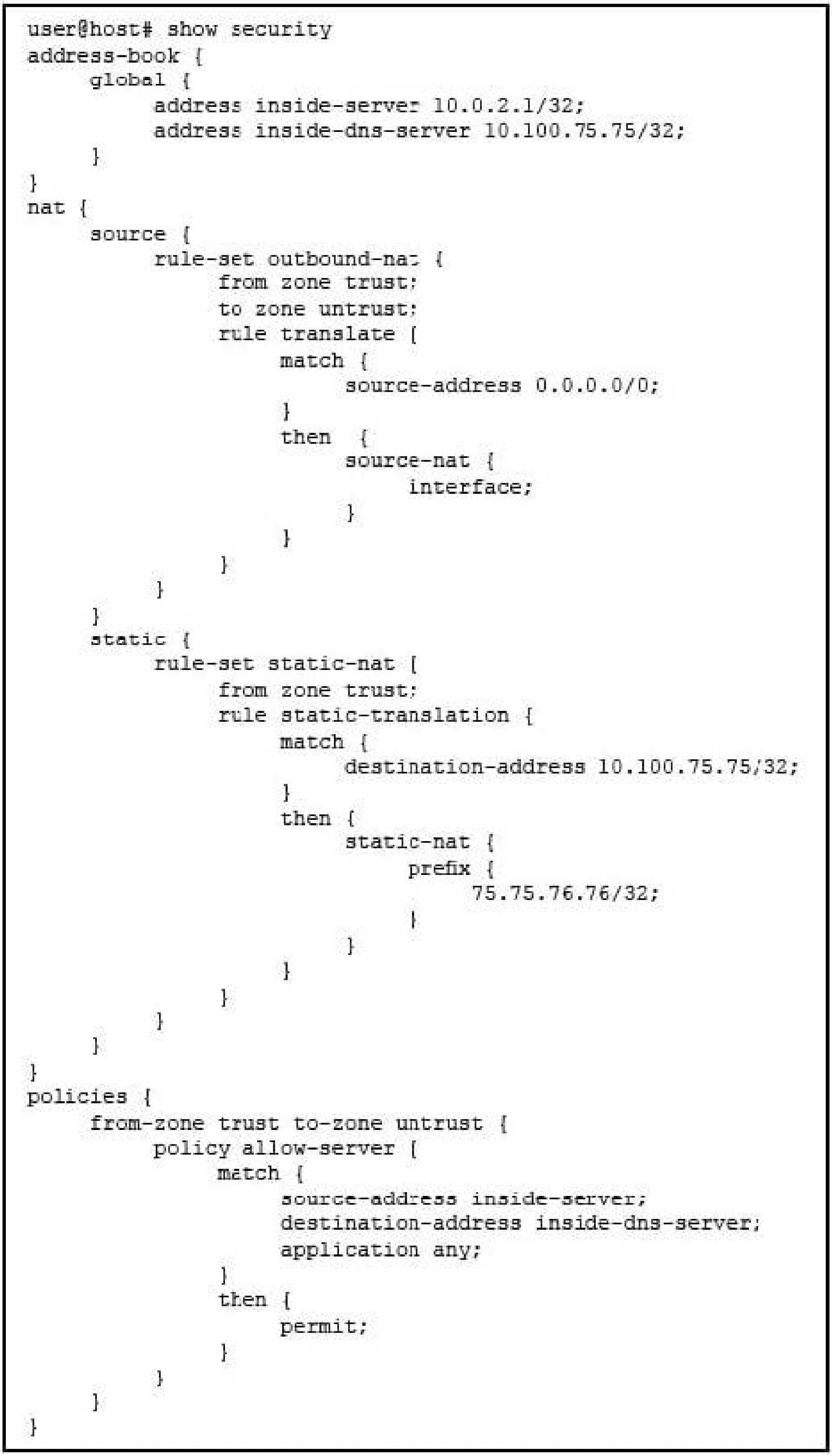
C. Verify that the IKE policy is configured for aggressive mode.

D. Verify that PKI is properly configured.

Correct Answer: AC

QUESTION 15

Click the Exhibit button.



```
user@host# show security
address-book {
    global {
        address inside-server 10.0.2.1/32;
        address inside-dns-server 10.100.75.75/32;
    }
}
nat {
    source {
        rule-set outbound-nat {
            from zone trust;
            to zone untrust;
            rule translate {
                match {
                    source-address 0.0.0.0/0;
                }
                then  {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
    static {
        rule-set static-nat {
            from zone trust;
            rule static-translation {
                match {
                    destination-address 10.100.75.75/32;
                }
                then {
                    static-nat {
                        prefix {
                            75.75.76.76/32;
                        }
                    }
                }
            }
        }
    }
}
policies {
    from-zone trust to-zone untrust {
        policy allow-server {
            match {
                source-address inside-server;
                destination-address inside-dns-server;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
```

The inside server must communicate with the external DNS server. The internal DNS server address is

10.100.75.75. The external DNS server address is 75.75.76.76. Traffic from the inside server to the DNS server fails.

Referring to the exhibit, what is causing the problem?

A. The security policy must match the translated destination address.

B. Source and static NAT cannot be configured at the same time.

C. The static NAT rule must use the global address book entry name for the DNS server.

D. The security policy must match the translated source and translated destination address.

Correct Answer: A