Juniper

Exam JN0-332

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

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 2: Volume B	2
Topic 3: Volume C	4
Topic 4: Volume D	3
Topic 5: Volume E	1

Topic 2, Volume B

Question No : 1 - (Topic 2)

Which three are necessary for antispam to function properly on a branch SRX Series device? (Choose three.)

A. an antispam license
B. DNS servers configured on the SRX Series device
C. SMTP services on SRX
D. a UTM profile with an antispam configuration in the appropriate security policy
E. antivirus (full or express)

Answer: A,B,D

Question No : 2 - (Topic 2)

Using a policy with the policy-rematch flag enabled, what happens to the existing and new sessions when you change the policyaction from permit to deny?

A. The new sessions matching the policy are denied. The existing sessions are dropped.
B. The new sessions matching the policy are denied. The existing sessions, not being allowed to carry any traffic, simply timeout.
C. The new sessions matching the policy might be allowed through if they match another policy. The existing sessions are dropped.
D. The new sessions matching the policy are denied. The existing sessions continue until they are completed or their timeout is reached.

Answer: A

Topic 3, Volume C

Question No : 3 - (Topic 3)

Which two configuration elements are required for a route-based VPN? (Choose two.)

A. secure tunnel interface
B. security policy to permit the IKE traffic

C. a route for the tunneled transit traffic
D. tunnel policy for transit traffic referencing the IPsec VPN

Answer: A,C

Question No : 4 - (Topic 3)

When the first packet in a new flow is received, which high-end SRX component is responsible for setting up the flow?

A. Routing Engine
B. I/O card
C. network processing card
D. services processing card

Answer: D

Question No : 5 - (Topic 3)

You are required to configure a SCREEN option that enables IP source route option detection.

Which two configurations meet this requirement? (Choose two.)

A. [edit security screen]
user@host# show
ids-option protectFromFlood {
ip {
loose-source-route-option;
strict-source-route-option;
}}
B. [edit security screen]
user@host# show
ids-option protectFromFlood {
ip {
source-route-option;
}}
C. [edit security screen]
user@host# show

```
ids-option protectFromFlood {
ip {
record-route-option;
security-option;
}}
```

D. [edit security screen]

```
user@host# show
ids-option protectFromFlood {
ip {
strict-source-route-option;
record-route-option;
}}
```

Answer: A,B

Question No : 6 - (Topic 3)

What do you use to group interfaces with similar security requirements?

A. zones
B. policies
C. address book
D. NAT configuration

Answer: A

Topic 4, Volume D

Question No : 7 - (Topic 4)

You are asked to establish a chassis cluster between two branch SRX Series devices. You must ensure that no single point of failure exists.

What would prevent a single point of failure?

A. dual data plane links
B. redundant routing tables
C. redundant cluster IDs
D. dual control plane links

Answer: A

Question No : 8 - (Topic 4)

You are asked to implement the hashing algorithm that uses the most bits in the calculation on your Junos security device.

Which algorithm should you use?

A. SHA-512
B. SHA-256
C. MD5-Plus
D. MD5

Answer: B

Question No : 9 - (Topic 4)

Click the Exhibit button.

```
user@host> show log kmd
Dec 12 08:22:11 jnp_ike_connect: Start, remote_name = 192.168.2.100:500, xchg = 2, flags = 00000000
Dec 12 08:22:11 ike_sa_allocate: Start, SA = { c543561b 08des114c - 00000000 00000000 }
Dec 12 08:22:11 ike_init_isakmp_sa: Start, remote = 192.168.2.100:500, initiator = 1
Dec 12 08:22:11 jnp_ike_connect: SA = { c543561b 08des114c - 00000000 00000000}, nego = -1
Dec 12 08:22:11 ike_st_o_sa_proposal: Start
Dec 12 08:22:11 ike_policy_reply_isakmp_vendor_ids: Start
Dec 12 08:22:11 ike_st_o_private: Start
Dec 12 08:22:11 ike_policy_reply_private_payload_out: Start
Dec 12 08:22:11 ike_encode_packet: Start, SA = { 0xc543561b 08des114c - 00000000 00000000 } / 00000000,
nego = -1
Dec 12 08:22:11 ike_send_packet: Start, send SA = { c543561b 08des114c - 00000000 00000000}, nego = -1,
src = 192.168.1.100:500, dst = 192.168.2.100:500, routing table id = 0
Dec 12 08:22:11 ike_get_sa: Start, SA = { c543561b 08des114c - 2b282cfa fb5b7e9e } / 00000000, remote =
192.168.2.100:500
Dec 12 08:22:11 ike_sa_find: Not found SA = { c543561b 08des114c - 2b282cfa fb5b7e9e }
Dec 12 08:22:11 ike_sa_find_half: Found half SA = { c543561b 08des114c - 00000000 00000000 }
Dec 12 08:22:11 ike_sa_upgrade: Start, SA = { c543561b 08des114c - 00000000 00000000 } -> { ... -
2b282cfa fb5b7e9e }
Dec 12 08:22:11 ike_alloc_negotiation: Start, SA = { c543561b 08des114c - 2b282cfa fb5b7e9e}
Dec 12 08:22:11 ike_decode_packet: Start
Dec 12 08:22:11 ike_decode_packet: Start, SA = { c543561b 08des114c - 2b282cfa fb5b7e9e} / 00000000, nego
= 0
```

You are troubleshooting an IPsec VPN connection between a local SRX Series device using IP address 192.168.1.100 and a remote SRX device using IP address 192.168.2.100. A VPN connection cannot be established. Referring to the exhibit, you examine the kmd log file.

What is the problem?

A. The Phase 2 proposal is invalid.
B. The Phase 1 proposal is invalid.
C. The Phase 1 gateway is invalid.
D. The Phase 2 gateway is invalid.

Answer: B

Topic 5, Volume E

Question No : 10 - (Topic 5)

Click the Exhibit button.

```
[edit security policies]
user@host# show
from-zone INTERNET to-zone INT-WEB {
    policy web-server-zone {
        match {
            source-address any;
            destination-address web-server;
            application junos-http;
        }
        then {
            deny;
        }
    }
}
global {
    policy web-server-global {
        match {
            source-address any;
            destination-address web-server;
            application any;
        }
        then {
            permit;
        }
    }
}
```

Hosts are attempting to communicate with the Web server. However, the traffic is failing to reach the Web server.

Referring to the exhibit, which two actions would you take to resolve the problem? (Choose two.)

A. Insert the global-based policy before the zone-based policy.
B. Remove the zone-based policy.
C. Change the zone-based policy's action topermit.
D. Change the application in the global-based policy tojunos-http.

Answer: B,C