Vendor: Juniper

Exam Code: JN0-332

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

Version: DEMO

QUESTION 1
Which configuration keyword ensures that all in-progress sessions are re-evaluated upon committing a security policy change?

A. policy-rematch
B. policy-evaluate
C. rematch-policy
D. evaluate-policy

Answer: A

QUESTION 2
Click the Exhibit button. You need to alter the security policy shown in the exhibit to send matching traffic to an IPsec VPN tunnel. Which command causes traffic to be sent through an IPsec VPN named remote-vpn?

```
[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;
    }
}
```


A.
```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy tunnel-traffic then tunnel remote-vpn
```
B.
```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy tunnel-traffic then tunnel ipsec-vpn remote-vpn
```
C.
```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy tunnel-traffic then permit ipsec-vpn remote-vpn
```
D.
```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy tunnel-traffic then permit tunnel ipsec-vpn remote-vpn
```

Answer: D

QUESTION 3
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

Answer: ACE

QUESTION 4
You must configure a SCREEN option that would protect your router from a session table flood.Which configuration meets this requirement?

A.
```
[edit security screen]
user@host# show
ids-option protectFromFlood {
icmp {
ip-sweep threshold 5000;
flood threshold 2000;
}
}
```
B.
```
[edit security screen]
user@host# show
ids-option protectFromFlood {
tcp {
syn-flood {
attack-threshold 2000;
destination-threshold 2000;
}
}
}
```
C.
```
[edit security screen]
user@host# show
ids-option protectFromFlood {
udp {
flood threshold 5000;
}
}
```
D.
```
[edit security screen]
user@host# show
ids-option protectFromFlood {
limit-session {
source-ip-based 1200;
destination-ip-based 1200;
}
}
```

Answer: D

QUESTION 5
Which type of Web filtering by default builds a cache of server actions associated with each URL it has checked?

A. Websense Redirect Web filtering
B. integrated Web filtering
C. local Web filtering
D. enhanced Web filtering

Answer: B

QUESTION 6
Which security or functional zone name has special significance to the Junos OS?

A. self
B. trust
C. untrust
D. junos-global

Answer: D

QUESTION 7
Which command do you use to display the status of an antivirus database update?

A. show security utm anti-virus status
B. show security anti-virus database status
C. show security utm anti-virus database
D. show security utm anti-virus update

Answer: A

QUESTION 8
Which statement contains the correct parameters for a route-based IPsec VPN?

A.
```
[edit security ipsec]
user@host# show
proposal ike1-proposal {
protocol esp;
authentication-algorithm hmac-md5-96;
encryption-algorithm 3des-cbc;
lifetime-seconds 3200;
}
policy ipsec1-policy {
perfect-forward-secrecy {
keys group2;
}
proposals ike1-proposal;
}
vpn VpnTunnel {
interface ge-0/0/1.0;
ike {
gateway ike1-gateway;
ipsec-policy ipsec1-policy;
}
establish-tunnels immediately;
}
```

B.
```
[edit security ipsec]
user@host# show
proposal ike1-proposal {
protocol esp;
authentication-algorithm hmac-md5-96;
encryption-algorithm 3des-cbc;
lifetime-seconds 3200;
}
policy ipsec1-policy {
perfect-forward-secrecy {
```

```
keys group2;
}
proposals ike1-proposal;
}
vpn VpnTunnel {
interface st0.0;
ike {
gateway ike1-gateway;
ipsec-policy ipsec1-policy;
}
establish-tunnels immediately;
}
```

C.
```
[edit security ipsec]
user@host# show
proposal ike1-proposal {
protocol esp;
authentication-algorithm hmac-md5-96;
encryption-algorithm 3des-cbc;
lifetime-seconds 3200;
}
policy ipsec1-policy {
perfect-forward-secrecy {
keys group2;
}
proposals ike1-proposal;
}
vpn VpnTunnel {
bind-interface ge-0/0/1.0;
ike {
gateway ike1-gateway;
ipsec-policy ipsec1-policy;
}
establish-tunnels immediately;
}
```

D.
```
[edit security ipsec]
user@host# show
proposal ike1-proposal {
protocol esp;
authentication-algorithm hmac-md5-96;
encryption-algorithm 3des-cbc;
lifetime-seconds 3200;
}policy ipsec1-policy {
perfect-forward-secrecy {
keys group2;
}
proposals ike1-proposal;
}
vpn VpnTunnel {
bind-interface st0.0;
ike {
gateway ike1-gateway;
ipsec-policy ipsec1-policy;
}
establish-tunnels immediately;
}
```

Answer: D

QUESTION 9
Which zone is system-defined?

A. security
B. functional
C. junos-global
D. management

Answer: C

QUESTION 10
You want to allow your device to establish OSPF adjacencies with a neighboring device connected to interface ge-0/0/3.0. Interface ge-0/0/3.0 is a member of the HR zone. Under which configuration hierarchy must you permit OSPF traffic?

A. `[edit security policies from-zone HR to-zone HR]`
B. `[edit security zones functional-zone management protocols]`
C. `[edit security zones protocol-zone HR host-inbound-traffic]`
D. `[edit security zones security-zone HR host-inbound-traffic protocols]`

Answer: D

QUESTION 11
Click the Exhibit button. Your IKE SAs are up, but the IPsec SAs are not up.Referring to the exhibit, what is the problem?

```
Oct 8 10:56:00 Phase-1 [responder] done for local=ipv4(udp:500,[0..3]=1.1.1.2)
remote=ipv4(udp:500,[0..3]=2.2.2.2)

Oct 8 10:56:00 Failed to match the peer proxy ids p2_remote=ipv4_subnet(a
ny:0,[0..7]=192.168.168.0/24) p2_local=ipv4_subnet(any:0,[0..7]=10.10.20.0/24) for the
remote peer:ipv4(udp:500,[0..3]=2.2.2.2)

Oct 8 10:56:00 KMD_PM_P2_POLICY_LOOKUP_FAILURE: Policy lookup for Phase-2 [responder]
failed for p1_local=ipv4(udp:500,[0..3]=1.1.1.2) p1_remote=ipv4( udp:500,[0..3]=2.2.2.2)
p2_local=ipv4_subnet(any:0,[0..7]=10.10.20.0/24) p2_
remote=ipv4_subnet(any:0,[0..7]=192.168.168.0/24)

Oct 8 10:56:00 1.1.1.2:500 (Responder) <-> 2.2.2.2:500 ( 41f638eb cc22bbfe - 43fd0e85
b4f619d5 [0] / 0xc77fafcf \) QM; Error = No proposal chosen (14)
```

A. One or more of the phase 2 proposals such as authentication algorithm, encryption algorithm do not match.
B. The tunnel interface is down.
C. The proxy IDs do not match.
D. The IKE proposals do not match the IPsec proposals.

Answer: C

QUESTION 12
Which three statements are true regarding IDP? (Choose three.)

A. IDP cannot be used in conjunction with other Junos security features such as SCREEN options, zones, and security policy.
B. IDP inspects traffic up to the Application Layer.
C. IDP searches the data stream for specific attack patterns.
D. IDP inspects traffic up to the Presentation Layer.
E. IDP can drop packets, close sessions, prevent future sessions, and log attacks for review by network administrators when an attack is detected.

Answer: BCE

QUESTION 13
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

Answer: E

QUESTION 14
Referring to the exhibit, you have just committed the UTM antivirus configuration. You notice that the SRX Series device shows that Kaspersky scanning is being used instead of express scanning. What must you do to resolve this problem?

A. You must configure the antivirus type to use express scanning
B. You must configure the antivirus type to disable Kaspersky
C. You must update the antivirus signatures
D. You must wait until the next pattern update

Answer: A

QUESTION 15
Which statement is true about a logical interface?

A. A logical interface can belong to multiple zones
B. A logical interface can belong to multiple routing instances
C. A logical interface can belong to only one routing instance
D. All logical interfaces in a routing instance must belong to a single zone

Answer: C

Thank You for Trying Our Product

PassLeader Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **STNAR2014**