Juniper

Exam JN0-332

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

Version: 25.0

[Total Questions: 517]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	98
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	100
Topic 5: Volume E	119

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which two statements about staticNAT are true? (Choose two.)

A. Static NAT can only be used with destination NAT.
B. Static NAT rules take precedence over overlapping dynamic NAT rules.
C. NAT rules take precedence over overlapping static NAT rules.
D. A reverse mapping is automatically created.

Answer: B,D

Question No : 2 - (Topic 1)

A network administrator has configured source NAT, translating to an address that is on a locally connected subnet. The administrator sees the translation working, but traffic does not appear to come back. What is causing the problem?

A. The host needs to open the telnet port.
B. The host needs a route for the translated address.
C. The administrator must use a proxy-arp policy for the translated address.
D. The administrator must use a security policy, which will allow communication between the zones.

Answer: C

Question No : 3 - (Topic 1)

The Junos OS blocks an HTTP request due to the category of the URL. Which form of Web filtering is being used?

A. redirect Web filtering
B. integrated Web filtering
C. categorized Web filtering
D. local Web filtering

Answer: B

Question No : 4 - (Topic 1)

A system administrator detects thousands of open idle connections from the same source.Which problem can arise from this type of attack?

A. It enables an attacker to perform an IP sweep of devices.
B. It enables a hacker to know which operating system the system is running.
C. It can overflow the session table to its limit, which can result in rejection of legitimate traffic.
D. It creates a ping of death and can cause the entire network to be infected with a virus.

Answer: C

Question No : 5 - (Topic 1)

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 : 6 - (Topic 1)

Which URL database do branch SRX Series devices use when leveraging local Web filtering?

A. The SRX Series device will download the database from an online repository to locally inspect HTTP traffic for Web filtering.
B. The SRX Series device will use an offline database to locally inspect HTTP traffic for Web filtering.
C. The SRX Series device will redirect local HTTP traffic to an external Websense server

for Web filtering.
D. The SRX Series administrator will define the URLs and their associated action in the local database to inspect the HTTP traffic for Web filtering.

Answer: D

Question No : 7 - (Topic 1)

Which two statements about the use of SCREEN optionsare correct? (Choose two.)

A. SCREEN options are deployed at the ingress and egress sides of a packet flow.
B. Although SCREEN options are very useful, their use can result in more session creation.
C. SCREEN options offer protection against various attacks at the ingress zone of a packet flow.
D. SCREEN options examine traffic prior to policy processing, thereby resulting in fewer resources used for malicious packet processing.

Answer: C,D

Question No : 8 - (Topic 1)

Click the Exhibit button.

```
[edit security policies from-zone HR to-zone trust]
user@host# show
policy one {
    match {
        source-address any;
        destination-address any;
        application [ junos-http junos-ftp ];
    }
    then {
        permit;
    }
}
policy two {
    match {
        source-address host_a;
        destination-address host_b;
        application [ junos-http junos-smtp ];
    }
    then {
        deny;
    }
}
```

Assume the default-policy has not been configured. Given the configuration shown in the exhibit, which two statements about traffic from host_a in the HR zone to host_b in the trust zone are true? (Choose two.)

A. DNS traffic is denied.
B. HTTP traffic is denied.
C. FTP traffic is permitted.
D. SMTP traffic is permitted.

Answer: A,C

Question No : 9 - (Topic 1)

Which two statements about the use of SCREEN optionsare correct? (Choose two.)

A. SCREEN options offer protection against various attacks.
B. SCREEN options are deployed prior to route and policy processing in first path packet processing.
C. SCREEN options are deployed at the ingress and egress sides of a packet flow.
D. When you deploy SCREEN options, you must take special care to protect OSPF.

Answer: A,B

Question No : 10 - (Topic 1)

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 No : 11 - (Topic 1)

By default, how is traffic evaluated when the antivirus database update is in progress?

A. Traffic is scanned against the old database.
B. Traffic is scanned against the existing portion of the currently downloaded database.
C. All traffic that requires antivirus inspection is dropped and a log message generated displaying the traffic endpoints.
D. All traffic that requires antivirus inspection is forwarded with no antivirus inspection and a log message generated displaying the traffic endpoints.

Answer: D

Question No : 12 - (Topic 1)

Which zone type can be specified in a policy?

A. security
B. functional
C. user
D. system

Answer: A

Explanation:

QUESTIONNO: 41
Which two statements about Junos software packet handlingare correct? (Choose two.)

A. The Junos OS applies service ALGs only for the first packet of a flow.
B. The Junos OS uses fast-path processing only for the first packet of a flow.
C. The Junos OS performs policy lookup only for the first packet of a flow.
D. The Junos OS applies SCREEN options for both first and consecutive packets of a flow.

Answer: C, D

Question No : 13 - (Topic 1)

If both nodes in a chassis cluster initialize at different times, which configuration example will allow you to ensure that the node with the higher priority will become primary for your RGs other than RG0?

A. [edit chassis cluster]
user@host# show
redundancy-group 1 {
node 0 priority 200;
node 1 priority 150;
preempt;
}
B. [edit chassis cluster]
user@host# show
redundancy-group 1 {
node 0 priority 200;
node 1 priority 150;
monitoring;
}
C. [edit chassis cluster]
user@host# show
redundancy-group 1 {
node 0 priority 200;
node 1 priority 150;
control-link-recovery;

}
D. [edit chassis cluster]
user@host# show
redundancy-group 1 {
node 0 priority 200;
node 1 priority 150;
strict-priority;
}

Answer: A

Question No : 14 - (Topic 1)

Under which Junos hierarchy level are security policies configured?

A. [edit security]
B. [edit protocols]
C. [edit firewall]
D. [edit policy-options]

Answer: A

Question No : 15 - (Topic 1)

How many IDP policies can be active at one time on an SRX Series device by means of the set security idp active-policyconfiguration statement?

A. 1
B. 2
C. 4
D. 8

Answer: A

Question No : 16 - (Topic 1)

Click the Exhibit button.

```
[edit security zones security-zone trust]
user@host# show
host-inbound-traffic {
    protocols {
        all;
        ospf {
            except;
        }
    }
}
interfaces {
    ge-0/0/0.0 {
        host-inbound-traffic {
            protocols {
                rip;
            }
        }
    }
}
```

Given the configuration shown in the exhibit, which protocol(s) are allowed to communicate with the device on ge-0/0/0.0?

A. RIP
B. OSPF
C. BGP and RIP
D. RIP and PIM

Answer: A

Question No : 17 - (Topic 1)

What are three configuration objects used to build JunosIDP rules? (Choose three.)

A. zone objects
B. policy objects
C. attack objects
D. alert and notify objects
E. network and address objects

Answer: A,C,E