

T estpassport Q&A



La meilleure qualité le meilleur service

<http://www.testpassport.fr>

Service de mise à jour gratuit pendant un an

Exam : JN0-331

Title : SEC,Specialist(JNCIS-SEC)

Version : Demo

1. Regarding zone types, which statement is true?

- A. You cannot assign an interface to a functional zone.
- B. You can specify a functional zone in a security policy.
- C. Security zones must have a scheduler applied.
- D. You can use a security zone for traffic destined for the device itself.

Answer: D

2. Regarding attacks, which statement is correct?

- A. Both DoS and propagation attacks exploit and take control of all unprotected network devices.
- B. Propagation attacks focus on suspicious packet formation using the DoS SYN-ACK-ACK proxy flood.
- C. DoS attacks are directed at the network protection devices, while propagation attacks are directed at the servers.
- D. DoS attacks are exploits in nature, while propagation attacks use trust relationships to take control of the devices.

Answer: D

3. Click the Exhibit button.

[edit schedulers]

user@host# show

```
scheduler now {  
    monday all-day;  
    tuesday exclude;  
    wednesday {  
        start-time 07:00:00 stop-time 18:00:00;  
    }  
    thursday {  
        start-time 07:00:00 stop-time 18:00:00;  
    }  
}
```

[edit security policies from-zone Private to-zone External]

```
user@host# show
policy allowTransit {
    match {
        source-address PrivateHosts;
        destination-address ExtServers;
        application ExtApps;
    }
    then {
        permit {
            tunnel {
                ipsec-vpn myTunnel;
            }
        }
    }
    scheduler-name now;
```

Based on the configuration shown in the exhibit, what are the actions of the security policy?

- A. The policy will always permit transit packets and use the IPsec VPN myTunnel.
- B. The policy will permit transit packets only on Monday, and use the IPsec VPN Mytunnel.
- C. The policy will permit transit packets and use the IPsec VPN myTunnel all day Monday and Wednesday 7am to 6pm, and Thursday 7am to 6pm.
- D. The policy will always permit transit packets, but will only use the IPsec VPN myTunnel all day Monday and Wednesday 7am to 6pm, and Thursday 7am to 6pm.

Answer: C

4. Which two statements are true regarding proxy ARP? (Choose two.)

- A. Proxy ARP is enabled by default.
- B. Proxy ARP is not enabled by default.
- C. JUNOS security devices can forward ARP requests to a remote device when proxy ARP is enabled.
- D. JUNOS security devices can reply to ARP requests intended for a remote device when proxy ARP is enabled.

Answer: BD

5. For IKE phase 1 negotiations, when is aggressive mode typically used?

- A. when one of the tunnel peers has a dynamic IP address
- B. when one of the tunnel peers wants to force main mode to be used
- C. when fragmentation of the IKE packet is required between the two peers
- D. when one of the tunnel peers wants to specify a different phase 1 proposal

Answer: A

6. Click the Exhibit button.

[edit groups]

user@host# show

```
node0 {
    system {
        host-name NODE0;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 1.1.1.1/24;
                }
            }
        }
    }
}

node1 {
    system {
        host-name NODE1;
    }
}
```

```
interfaces {  
    fxp0 {  
        unit 0 {  
            family inet {  
                address 1.1.1.2/24;  
            }  
        }  
    }  
}
```

In the exhibit, what is the function of the configuration statements?

- A. This section is where you define all chassis clustering configuration.
- B. This configuration is required for members of a chassis cluster to talk to each other.
- C. You can apply this configuration in the chassis cluster to make configuration easier.
- D. This section is where unique node configuration is applied.

Answer: D

7. Which two statements describe the difference between JUNOS Software for security platforms and a traditional router? (Choose two.)

- A. JUNOS Software for security platforms supports NAT and PAT; a traditional router does not support NAT or PAT.
- B. JUNOS Software for security platforms does not forward traffic by default; a traditional router forwards traffic by default.
- C. JUNOS Software for security platforms uses session-based forwarding; a traditional router uses packet-based forwarding.
- D. JUNOS Software for security platforms performs route lookup for every packet; a traditional router performs route lookup only for the first packet.

Answer: BC

8. Which two statements describe the difference between JUNOS Software for security platforms and a

traditional router? (Choose two.)

- A. JUNOS Software for security platforms supports NAT and PAT; a traditional router does not support NAT or PAT.
- B. JUNOS Software for security platforms secures traffic by default; a traditional router does not secure traffic by default.
- C. JUNOS Software for security platforms allows for session-based forwarding; a traditional router uses packet-based forwarding.
- D. JUNOS Software for security platforms separates broadcast domains; a traditional router does not separate broadcast domains.

Answer: BC

9. A traditional router is better suited than a firewall device for which function?

- A. VPN establishment
- B. packet-based forwarding
- C. stateful packet processing
- D. Network Address Translation

Answer: B

10. Which three functions are provided by JUNOS Software for security platforms? (Choose three.)

- A. VPN establishment
- B. stateful ARP lookups
- C. Dynamic ARP inspection
- D. Network Address Translation
- E. inspection of packets at higher levels (Layer 4 and above)

Answer: ADE

11. What are two components of the JUNOS Software architecture? (Choose two.)

- A. Linux kernel
- B. routing protocol daemon
- C. session-based forwarding module

D. separate routing and security planes

Answer: BC

12. Which two functions of JUNOS Software are handled by the data plane? (Choose two.)

A. NAT

B. OSPF

C. SNMP

D. SCREEN options

Answer: AD

13. Host A opens a Telnet connection to Host B. Host A then opens another Telnet connection to Host B. These connections are the only communication between Host A and Host B. The security policy configuration permits both connections.

How many flows exist between Host A and Host B?

A. 1

B. 2

C. 3

D. 4

Answer: D

14. Which two statements about JUNOS Software packet handling are correct? (Choose two.)

A. JUNOS Software applies service ALGs only for the first packet of a flow.

B. JUNOS Software uses fast-path processing only for the first packet of a flow.

C. JUNOS Software performs route and policy lookup only for the first packet of a flow.

D. JUNOS Software applies SCREEN options for both first and consecutive packets of a flow.

Answer: CD

15. In JUNOS Software, which three packet elements can be inspected to determine if a session already exists? (Choose three.)

A. IP protocol

- B. IP time-to-live
- C. source and destination IP address
- D. source and destination MAC address
- E. source and destination TCP/UDP port

Answer: ACE

16. By default, which condition would cause a session to be removed from the session table?

- A. Route entry for the session changed.
- B. Security policy for the session changed.
- C. The ARP table entry for the source IP address timed out.
- D. No traffic matched the session during the timeout period.

Answer: D

17. What is the default session timeout for UDP sessions?

- A. 30 seconds
- B. 1 minute
- C. 5 minutes
- D. 30 minutes

Answer: C

18. What is the purpose of a zone in JUNOS Software?

- A. A zone defines a group of security devices with a common management.
- B. A zone defines the geographic region in which the security device is deployed.
- C. A zone defines a group of network segments with similar security requirements.
- D. A zone defines a group of network segments with similar class-of-service requirements.

Answer: C

19. Users can define policy to control traffic flow between which two components? (Choose two.)

- A. from a zone to the device itself
- B. from a zone to the same zone

- C. from a zone to a different zone
- D. from one interface to another interface

Answer: BC

20. Which two configurations are valid? (Choose two.)

A. [edit security zones]

```
user@host# show
```

```
security-zone red {
```

```
    interfaces {
```

```
        ge-0/0/1.0;
```

```
        ge-0/0/3.0;
```

```
    }
```

```
}
```

```
security-zone blue {
```

```
    interfaces {
```

```
        ge-0/0/2.0;
```

```
        ge-0/0/3.102;
```

```
    }
```

```
}
```

B. [edit security zones]

```
user@host# show
```

```
security-zone red {
```

```
    interfaces {
```

```
        ge-0/0/1.0;
```

```
        ge-0/0/2.0;
```

```
    }
```

```
}
```

```
security-zone blue {
```

```
    interfaces {
```

```
        ge-0/0/1.0;
```

```
        ge-0/0/3.0;
    }
}
C. [edit routing-instances]
user@host# show
red {
    interface ge-0/0/3.0;
    interface ge-0/0/2.102;
}
blue {
    interface ge-0/0/0.0;
    interface ge-0/0/3.0;
}
```

```
D. [edit routing-instances]
user@host# show
red {
    interface ge-0/0/3.0;
    interface ge-0/0/3.102;
}
blue {
    interface ge-0/0/0.0;
    interface ge-0/0/2.0;
}
```

Answer: AD