Juniper Networks Certified Internet Specialist, JNCIS-SEC

1. Which two content-filtering features does FTP support? (Choose two.)

A. notifications-options

B. protocol command list

C. block MIME type

D. block extension list

Answer(s): B,D

---

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

A. from a zone to a different zone

B. from a zone to the device itself

C. from a zone to the same zone

D. from one interface to another interface

Answer(s): A,C

---

3. Which three algorithms are used by an SRX Series device to validate the integrity of the data exchanged through an IPsec VPN? (Choose three.)

A. SHA2

B. MD5

C. 3DES

D. NHTB

E. SHA1

Answer(s): A,B,E

---

4. Regarding secure tunnel (st) interfaces, which statement is true?

A. You cannot apply static NAT on an st interface logical unit.

B. You cannot assign st interfaces to a security zone.

C. A static route can reference the st interface logical unit as the next-hop.

D. st interfaces are optional when configuring a route-based VPN.

Answer(s): C

---

5. You want to create an out-of-band management zone and assign the ge-0/0/0.0 interface to that zone.

A. set security zones management interfaces ge-0/0/0.0

B. set zones functional-zone management interfaces ge-0/0/0.0

C. set security zones functional-zone management interfaces ge-0/0/0.0

D. set security zones functional-zone out-of-band interfaces ge-0/0/0.0

Answer(s): C

---

6. Which statement is true about a NAT rule action of off?

A. The NAT action of off is only supported for destination NAT rule-sets.

B. The NAT action of off is useful for detailed control of NAT.

C. The NAT action of off is useful for disabling NAT when a pool is exhausted.

D. The NAT action of off is only supported for source NAT rule-sets.

Answer(s): B

---

7. Which statement is true about SurfControl integrated Web filter solution?

A. The SurfControl server in the cloud provides the SRX device with only the reputation of the URL.

B. The SurfControl server in the cloud provides the SRX device with only the category of the URL.

C. The SurfControl server in the cloud provides the SRX device with the category of the URL as well as the reputation of the URL.

D. The SurfControl server in the cloud provides the SRX device with a decision to permit or deny the URL.

Answer(s): B

---

8. Which three actions can a branch SRX Series device perform on a spam e-mail message? (Choose three.)

A. It can drop the connection at the IP address level.

B. It can allow the e-mail and bypass all UTM inspection.

C. It can allow the e-mail to be forwarded, but change the intended recipient to a new e-mail address.

D. It can block the e-mail based upon the sender ID.

E. It can allow the e-mail to be forwarded to the destination, but tag it with a custom value in the subject line.

---

9. Which statement is true when express AV detects a virus in TCP session?

A. TCP traffic is allowed and an SNMP trap is sent.

B. AV scanning is restarted.

C. TCP RST is sent and a session is restarted.

D. TCP connection is closed gracefully and the data content is dropped.

Answer(s): D

---

10. A user wants to establish an HTTP session to a server behind an SRX device but is being pointed to Web page on the SRX device for additional authentication. Which type of user authentication is configured?

A. pass-through with Web redirect

B. WebAuth with HTTP redirect

C. WebAuth

D. pass-through

Answer(s): C

---

11. Which two statements are true regarding SRX Series devices? (Choose two)

A. Session setup and maintenance is performed in the data plane.

B. High-end SRX Series use IOCs, NPCs. and SPCs for control plane operations.

C. High-end SRX Series use IOCs, NPCs. and SPCs for data plane operations.

D. Session setup and maintenance is performed in the control plane.

Answer(s): C,D

---

12. Which two statements are true regarding built-in applications on Junos SRX Series devices? (Choose two.)

A. You can change the default timer values through configuration.

B. You cannot change the name of a built-in application through configuration.

C. You cannot change the default timer values through configuration.

D. You can change the name of a built-in application through configuration.

Answer(s): B,C

---

13. What are two valid match conditions for source NAT? (Choose two.)

A. port range

B. destination address

C. source address

D. source port

Answer(s): B,C

---

14. Which Junos security feature helps protect against spam, viruses, trojans, and malware?

A. session-based stateful firewall

B. IPsec VPNs

C. security policies

D. Unified Threat Management

Answer(s): D

---

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

A. an antispam license

B. a UTM profile with an antispam configuration in the appropriate security policy

C. antivirus (full or express)

D. DNS servers configured on the SRX Series device

E. SMTP services on SRX

Answer(s): A,B,D

---

16. You are troubleshooting a security policy. The operational command show security flow session does not show any sessions for this policy.

A. The security monitoring performance session command should be used to show sessions.

B. Logging on session closure has not been enabled in the policy.

C. Logging on session initialization has not been enabled in the policy.

D. The traffic is not being matched by the policy.

Answer(s): D

17. Which statement describes an ALG?

A. An ALG intercepts and analyzes all traffic, allocates resources, and defines dynamic policies to deny the traffic.

B. An ALG intercepts and analyzes all traffic, allocates resources, and defines dynamic policies to permit the traffic to pass.

C. An ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to deny the traffic.

D. An ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass.

Answer(s): D

---

18. Which three features are part of the branch SRX series UTM suite? (Choose three.)

A. application firewalling

B. antispam

C. antivirus

D. Web filtering

E. IPS

Answer(s): B,C,D

---

19. When an SRX series device receives an ESP packet, what happens?

A. If the destination address of the outer IP header of the ESP packet matches the IP address of the ingress interface, based on SPI match and route lookup of inner header, it will decrypt the packet.

B. If the destination IP address in the outer IP header of ESP does not match the IP address of the ingress interface, it will discard the packet.

C. If the destination address of the outer IP header of the ESP packet matches the IP address of the ingress interface, based on SPI match, it will decrypt the packet.

D. If the destination address of the outer IP header of the ESP packet matches the IP address of the ingress interface, it will immediately decrypt the packet.

Answer(s): C

---

20. What are three different integrated UTM components available on the branch SRX Series devices? (Choose three.)

A. antispam

B. firewall user authentication

C. Web filtering

D. antivirus (full AV, express AV)

E. antivirus (desktop AV)

Answer(s): A,C,D