

Juniper

JN0-1331 Exam

Security Design, Specialist

Questions & Answers Demo

Version: 4.0

Question: 1

You are deploying Security Director with the logging and reporting functionality for VMs that use SSDs. You expect to have approximately 20,000 events per second of logging in your network. In this scenario, what is the minimum number of logging and reporting devices that should be used?

- A. 2
- B. 4
- C. 1
- D. 3

Answer: C

Reference: https://www.juniper.net/documentation/en_US/junos-space17.1/topics/task/multi-task/junos-space-sd-log-collector-installing.html

Question: 2

You are concerned about users attacking the publicly accessible servers in your data center through encrypted channels. You want to block these attacks using your SRX Series devices. In this scenario, which two features should you use? (Choose two.)

- A. Sky ATP
- B. IPS
- C. SSL forward proxy
- D. SSL reverse proxy

Answer: BC

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-ssl-tls.html

Question: 3

Your customer needs help designing a single solution to protect their combination of various Junos network devices from unauthorized management access. Which Junos OS feature will provide this protection?

- A. Use a firewall filter applied to the fxp0 interface
- B. Use a security policy with the destination of the junos-host zone
- C. Use the management zone host-inbound-traffic feature
- D. Use a firewall filter applied to the lo0 interface

Answer: A

Reference: https://www.juniper.net/documentation/en_US/junos/topics/concept/junos-software-router-security-supported-features.html

Question: 4

You must allow applications to connect to external servers. The session has embedded IP address information to enable the remote system to establish a return session. In your design, which function should be implemented?

- A. source NAT
- B. application layer gateway
- C. destination NAT
- D. HTTP redirect

Answer: A

Question: 5

You are using SRX Series devices to secure your network and you require sandboxing for malicious file detonation. However, per company policy, you cannot send potentially malicious files outside your network for sandboxing.

Which feature should you use in this situation?

- A. Sky ATP
- B. UTM antivirus
- C. IPS
- D. JATP

Answer: D

Explanation:

Juniper Advanced Threat Prevention Appliance

Reference: <https://www.juniper.net/us/en/products-services/security/srx-series/datasheets/1000654.page>

Question: 6

You are creating a security design proposal for an enterprise customer. As part of the design, you are implementing 802.1x authentication on your EX Series devices.

In this scenario, which two statements are correct? (Choose two.)

- A. The supplicant is the device that prevents the authenticator's access until it is authenticated
- B. The supplicant is the device that is being authenticated
- C. The authenticator is the device that is being authenticated
- D. The authenticator is the device that prevents the supplicant's access until it is authenticated

Answer: BD

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/802-1x-authentication-switching-devices.html