

# JN0-1332<sup>Q&As</sup>

Security Design Specialist (JNCDS-SEC)

**Pass Juniper JN0-1332 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/jn0-1332.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



### QUESTION 1

You are working with a customer to create a design proposal using SRX Series devices. As part of the design, you must consider the requirements shown below:

1.

You must ensure that every packet entering your device is independently inspected against a set of rules.

2.

You must provide a way to protect the device from undesired access attempts.

3.

You must ensure that you can apply a different set of rules for traffic leaving the device than are in use for traffic entering the device.

In this scenario, what do you recommend using to accomplish these requirements?

- A. firewall filters
- B. intrusion prevention system
- C. unified threat management
- D. screens

Correct Answer: A

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/example/firewall-filter-statelessexample-trusted-source-block-telnet-and-ssh-access.html](https://www.juniper.net/documentation/en_US/junos/topics/example/firewall-filter-statelessexample-trusted-source-block-telnet-and-ssh-access.html)

---

### QUESTION 2

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

Correct Answer: D

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

---

**QUESTION 3**

You will be managing 1000 SRX Series devices. Each SRX Series device requires basic source NAT to access the Internet.

Which product should you use to manage these NAT rules on the SRX Series devices?

- A. Security Director
- B. CSO
- C. Contrail
- D. JSA

Correct Answer: A

---

**QUESTION 4**

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 log receiver devices that you should use?

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

Correct Answer: D

Reference: [https://www.juniper.net/documentation/en\\_US/junos-space17.1/topics/task/multi-task/junos-space-sd-log-collector-installing.html](https://www.juniper.net/documentation/en_US/junos-space17.1/topics/task/multi-task/junos-space-sd-log-collector-installing.html)

---

**QUESTION 5**

You are designing an SDN security solution for a new campus network. The network will consist of Juniper Networks Policy Enforcer, Juniper Networks switches, third-party switches, and SRX Series devices. The switches and the SRX Series devices will be used as security enforcement points. The design must be able to change the VLAN mapping of the switch port of a user that is already authenticated to the network in the event that the end user device becomes compromised.

Which component satisfies this requirement?

- A. certificate server
- B. RADIUS server

- C. Security Director
- D. DHCP server

Correct Answer: C

---

#### QUESTION 6

You work for an ISP that wants to implement remote-triggered black hole (RTBH) filters. What are three considerations in this scenario? (Choose three.)

- A. Source RTBH can block legitimate traffic on the network
- B. BGP FlowSpec improves the RTBH model by implementing dynamic firewall filters
- C. Source RTBH requires uRPF to be implemented on the service provider's network core
- D. Destination RTBH requires uRPF to be implemented on the service provider's network edge
- E. Destination RTBH essentially completes the attack on the victim's IP

Correct Answer: ABC

---

#### QUESTION 7

You are asked to design a secure enterprise WAN where all payload data is encrypted and branch sites communicate directly without routing all traffic through a central hub.

Which two technologies would accomplish this task? (Choose two.)

- A. group VPN
- B. AutoVPN
- C. MPLS Layer 3 VPN
- D. Auto Discovery VPN

Correct Answer: CD

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-auto-discoveryvpns.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discoveryvpns.html)

---

#### QUESTION 8

You are designing a network management solution that provides automation for Junos devices. Your customer wants to know which solutions would require additional software to be deployed to existing Junos devices.

Which two solutions satisfy this scenario? (Choose two.)

- A. SaltStack

- B. Ansible
- C. Puppet
- D. Chef

Correct Answer: AD

---

#### QUESTION 9

You are creating a security design proposal for a customer who is connecting their headquarters to a remote branch site over an unsecured Internet connection. As part of your design, you must recommend a solution to connect these sites together and ensure that the communication is secured and encrypted.

In this scenario, which solution do you recommend?

- A. GRE
- B. XMPP
- C. IPsec
- D. MPLS

Correct Answer: C

---

#### QUESTION 10

You have a campus location with multiple WAN links. You want to specify the primary link used for your VoIP traffic.

In this scenario, which type of WAN load balancing would you use?

- A. BGP
- B. OSPF
- C. FBF
- D. ECMP

Correct Answer: C

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-applicationadvanced-policy-based-routing.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-applicationadvanced-policy-based-routing.html)

---

#### QUESTION 11

You are designing a data center security architecture. The design requires automated scaling of security services according to real-time traffic flows.

Which two design components will accomplish this task? (Choose two.)

- A. telemetry with an SDN controller
- B. JFlow traffic monitoring with event scripts
- C. VNF security devices deployed on x86 servers
- D. VRF segmentation on high-capacity physical security appliances

Correct Answer: BC

Reference: [https://www.juniper.net/documentation/en\\_US/learn-about/LearnAbout\\_NFV.pdf](https://www.juniper.net/documentation/en_US/learn-about/LearnAbout_NFV.pdf)

---

#### QUESTION 12

A hosting company is migrating to cloud-based solutions. Their customers share a physical firewall cluster, subdivided into individual logical firewalls for each customer. Projection data shows that the cloud service will soon deplete all the resources within the physical firewall. As a consultant, you must propose a scalable solution that continues to protect all the cloud customers while still securing the existing physical network.

In this scenario, which solution would you propose?

- A. Deploy a vSRX cluster in front of each customer's servers while keeping the physical firewall cluster
- B. Deploy a software-defined networking solution
- C. Remove the physical firewall cluster and deploy vSRX clusters dedicated to each customer's servers
- D. Replace the physical firewall cluster with a higher-performance firewall

Correct Answer: C

---

#### QUESTION 13

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

Correct Answer: A

---

#### QUESTION 14

You are deploying a data center Clos architecture and require secure data transfers within the switching fabric.

In this scenario, what will accomplish this task?

- A. MACsec encryption
- B. LAG Layer 2 hashing
- C. IRB VLAN routing between hosts
- D. stacked VLAN tagging on the core switches

Correct Answer: C

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/example/private-vlans-irbinterfaces-mx-series-l2ng-configuring.html](https://www.juniper.net/documentation/en_US/junos/topics/example/private-vlans-irbinterfaces-mx-series-l2ng-configuring.html)

---

#### QUESTION 15

Your company has outgrown its existing secure enterprise WAN that is configured to use OSPF, AutoVPN, and IKE version 1. You are asked if it is possible to make a design change to improve the WAN performance without purchasing new hardware.

Which two design changes satisfy these requirements? (Choose two.)

- A. Modify the IPsec proposal from AES-128 to AES-256
- B. Change the IGP from OSPF to IS-IS
- C. Migrate to IKE version 2
- D. Implement Auto Discovery VPN

Correct Answer: BD

Reference: [https://www.juniper.net/documentation/en\\_US/junos/topics/topic-map/security-auto-discoveryvpns.html](https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discoveryvpns.html)

[Latest JN0-1332 Dumps](#)

[JN0-1332 PDF Dumps](#)

[JN0-1332 Practice Test](#)