

Juniper.Premium.JN0-1330.by.VCEplus.65q

Number: JN0-1330 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.2



Exam Code: JN0-1330

Exam Name: Security Design, Specialist (JNCDS-SEC)

Certification Provider: Juniper

Corresponding Certification: JNCDS-SEC

Website: www.vceplus.com

Free Exam: <https://vceplus.com/exam-jn0-1330/>

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in JN0-1330 exam products and you get latest questions. We strive to deliver the best JN0-1330 exam product for top grades in your first attempt.

VCE to PDF Converter : <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

Google+ : <https://plus.google.com/+Vcepluscom>

LinkedIn : <https://www.linkedin.com/company/vceplus>



QUESTION 1

Which security solution protects against zero-day attacks?

- A. DDoS protection
- B. advanced anti-malware
- C. content filtering
- D. Application Layer Gateways

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

Which three statements about Sky Advanced Threat Prevention are true? (Choose three.)

- A. Dynamic analysis involves unique deception techniques.
- B. Machine-learning algorithms are enabled to adapt to and identify new malware.
- C. Rapid cache lookups are used to quickly identify known files.
- D. Files are flagged for next-day analysis for certain malware types.
- E. It uses a single, best-in-class antivirus engine.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Sky Advanced Threat Prevention's identification technology uses a variety of techniques to quickly identify a threat and prevent an impending attack. These methods include:

- Rapid cache lookups to identify known files.
- Dynamic analysis that involves unique deception techniques applied in a sandbox to trick malware into activating and self-identifying.

Additionally, machine-learning algorithms enable Sky Advanced Threat Prevention to adapt to and identify new malware in an ever-changing threat landscape

Reference: http://www.juniper.net/techpubs/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-release-notes-d50.pdf

QUESTION 3

Your client modifies an event script and needs to update 100 SRX Series devices with this new script. They want to use the refresh-from parameter to refresh the script from a centralized location.

In this scenario, which three protocols would you use to accomplish this task? (Choose three.)

- A. HTTP
- B. SCP
- C. TFTP
- D. FTP
- E. CIFS

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Reference: http://www.juniper.net/documentation/en_US/junos14.1/topics/reference/command-summary/request-system-scripts-refresh-from.html

QUESTION 4

You are asked to implement a new application to share documents with trusted external organizations while minimizing the risk of an attack that would enable access to other enterprise systems.

In this scenario, which two locations would you recommend to deploy the application? (Choose two.)

- A. public cloud
- B. management VLAN
- C. enterprise LAN
- D. enterprise DMZ

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

You are designing a WAN solution for a small service provider. The service provider has asked you to include ways to mitigate potential DDoS attacks against their customers. Which two solutions should you include in your proposal? (Choose two.)

- A. BGP flowspec
- B. remote triggered back hole
- C. intrusion prevention system
- D. unified threat management

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Your customer is purchasing another company. They must establish communication between the two corporate networks, which use an overlapping IPv4 address space. The customer knows they must deploy some of Network Address Translation (NAT).

Which type of NAT should you use?

- A. destination
- B. source
- C. persistent
- D. static



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Which component of the Juniper NFV solution architecture acts as the VNF manager?

- A. MetaFabric
- B. Service Control Gateway
- C. Contrail
- D. vSRX

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Section: (none)

Explanation

Reference: <https://www.juniper.net/assets/us/en/local/pdf/whitepapers/2000633-en.pdf>

QUESTION 8

In the ever-changing threat landscape, you are seeking to deploy a dynamic anti-malware solution.

What are three characteristics of the Sky Advanced Threat Prevention public cloud infrastructure? (Choose three.)

- A. Machine-learning algorithms adapt to and identify new malware.
- B. It provides rapid cache lookups to identify known files.
- C. Known malicious files are quickly identified and replicated to the firewall.
- D. It processes all known file types.
- E. It uses dynamic analysis including unique deception techniques.

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Sky Advanced Threat Prevention's identification technology uses a variety of techniques to quickly identify a threat and prevent an impending attack. These methods include:

- Rapid cache lookups to identify known files.
- Dynamic analysis that involves unique deception techniques applied in a sandbox to trick malware into activating and self-identifying.

Additionally, machine-learning algorithms enable Sky Advanced Threat Prevention to adapt to and identify new malware in an ever-changing threat landscape

Reference: http://www.juniper.net/techpubs/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-release-notes-d50.pdf

QUESTION 9

You need to provide wireless access to the user community without reducing security.

Which action accomplishes this task?

- A. Provide all users with the pre-shared key to the SSID to validate their access.
- B. Record the users' MAC addresses.

- C. Require users to authenticate with EAP-TLS.
- D. Hide the broadcast of the SSID.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Where are the security policies enforced for next-generation firewalls?

- A. at the Presentation Layer
- B. at the Session Layer
- C. at the Data Link Layer
- D. at the Application Layer

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 11

You are designing a Log Director deployment that must be able to handle 6,500 sustained events per second. What is the minimum deployment scenario?

- A. three Log Collector VMs and one Log Concentrator VM
- B. two Log Collector VMs and one Log Concentrator VM
- C. one Log Collector VM
- D. four Log Collector VMs and one Log Concentrator VM

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference:

https://www.juniper.net/techpubs/en_US/junos-space15.2/topics/concept/junos-space-log-collector-understanding.html**QUESTION 12**

Which two components are required to implement a Contrail service chain? (Choose two.)

- A. AppSecure
- B. service policy
- C. Express Path
- D. virtual network

Correct Answer: BD**Section:** (none)**Explanation****Explanation/Reference:**

Explanation:

Service chaining requires the following configuration components to build the chain:

- Service template
- Virtual networks
- Service instance
- Network policy

Reference: http://www.juniper.net/techpubs/en_US/vsrx15.1x49/information-products/pathway-pages/security-vsrx-contrail-quickstart-pwp.pdf**QUESTION 13**

You must implement access control lists to protect the control plane of a service provider's core devices.

What are two ways to accomplish this task? (Choose two.)

- A. Implement access control lists to filter RFC 1918 IP addresses from reaching the control plane.
- B. Implement access control lists to permit only internal management networks to reach the control plane.
- C. Implement access control lists to drop all IP packets that are fragments.
- D. Implement access control lists to protect the control plane against unauthorized user credentials.

Correct Answer: BC**Section:** (none)**Explanation****Explanation/Reference:**

QUESTION 14

What is the maximum number of SRX Series devices in a chassis cluster?

- A. 2
- B. 3
- C. 4
- D. 5

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

Due to changes in security requirements you must place a firewall between an existing Web server farm and a database server farm residing in the same subnet. In this scenario, why would you choose transparent mode as your operating mode?

- A. Transparent mode does not require zones to be configured.
- B. Transparent mode can be implemented with no changes to the current IP addresses.
- C. Transparent mode policies can be enforced based on MAC address ranges.
- D. Transparent mode allows only IP packets to pass through the security policies.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Spotlight Secure provides which benefit?

- A. log management
- B. botnet protection

- C. centralized management of security devices
- D. IPsec encryption

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

What are three characteristics of the integrated user firewall feature? (Choose three.)

- A. RADIUS user authentication is performed.
- B. Enforcement is performed at access.
- C. Best-effort user authentication is performed.
- D. Passive authentication is performed.
- E. Enforcement is performed at the firewall.

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

Reference: http://www.juniper.net/documentation/en_US/junos15.1x49/topics/concept/security-user-firewall-3-tier-understanding.html

QUESTION 18

You must design a solution to collect logs from a group of SRX Series devices using Junos Space Log Director. You will deploy this solution on virtual machines that will support traffic peaks up to 7,500 events per second. How would you accomplish this task?

- A. Implement one centralized log collector and continue the SRX Series clusters to forward logs to it.
- B. Implement one centralized log concentrator and configure the SRX Series clusters to forward logs to it.
- C. Implement one log concentrator, two log collectors, and a load balancer in front of them, configuring SRX Series devices to forward the logs to the Load Balancer VIP interface.
- D. Implement one log concentrator, three log collectors, and configure the SRX Series clusters to distribute the logs among the log collectors.

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:**

Reference: http://www.juniper.net/techpubs/en_US/junos-space14.1/logging-reporting/information-products/topic-collections/junos-space-security-director-logging-reporting-getting-started-guide.pdf

QUESTION 19

You are asked to implement port-based authentication on your access switches. Security and ease of access are the two primary requirements. Which authentication solution satisfies these requirements?

- A. MAC RADIUS
- B. network access control
- C. firewall authentication
- D. IPsec tunnel

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:**

Reference: https://www.juniper.net/documentation/en_US/junos12.1x46/topics/concept/layer-2-8021x-port-network-authentication-security-understanding.html

QUESTION 20

What is one way to increase the security of a site-to-site IPsec VPN tunnel?

- A. Implement a stronger Diffie-Hellman group.
- B. Change IKE Phase 1 from main mode to aggressive mode.
- C. Implement traffic selectors.
- D. Implement a policy-based VPN.

Correct Answer: C

Section: (none)

Explanation**Explanation/Reference:****QUESTION 21**

Your customer is planning the deployment of a new hub-and-spoke WAN architecture that must support dual stack. They have decided against using a dynamic

routing protocol. They are concerned about the difficulty of managing configurations and operations at the hub location as they deploy branch routers. In this scenario, what are three reasons for selecting route-based VPNs with traffic selectors? (Choose three.)

- A. Traffic selectors support IPv4 and IPv6.
- B. Traffic selectors reduce the number of Phase 2 IPsec security associations.
- C. Traffic selectors reduce latency because they bypass UTM.
- D. Traffic selectors support auto route insertion.
- E. You can define multiple traffic selectors within a single route-based VPN.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Reference: http://www.juniper.net/documentation/en_US/junos15.1x49/topics/concept/ipsec-vpn-traffic-selector-understanding.html

QUESTION 22

What are the three activities in the reconnaissance phase of an attack? (Choose three.)

- A. Determine the device OS.
- B. Scan for devices and ports to exploit.
- C. Install malware.
- D. Propagate the virus to servers and workstations.
- E. Map the network.

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Your customer is assessing their network incident response plan. They need to improve their recovery time when a networking issue occurs, especially when involves JTAC support. They have limited internal support staff and little automation experience to develop their own tools.

Which Juniper solution meets these requirements?

- A. Juniper Secure Analytics

- B. Network Director
- C. Service Insight
- D. Service Now

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: <http://www.juniper.net/us/en/products-services/network-management/junos-space-applications/service-now/>

QUESTION 24

Your customer is planning to secure a data center with web servers reachable through two ISP connections terminating on each node of an active/passive SRX Series chassis cluster. ISP-1 is the preferred connection because it provides higher bandwidth than ISP-2. Which two must you include in your design proposal to meet this requirement? (Choose two.)

- A. Use conditional BGP advertisements and use interface monitoring for both ISP interfaces.
- B. Use static routing and use interface monitoring for both ISP interfaces.
- C. Ensure that both ISP interfaces are in the same zone and use interface monitoring.
- D. Ensure that both the ISP interfaces are in different zones and use interface monitoring.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

You are asked to provide user-based network access through an SRX Series device. The implementation must use Active Directory credentials for user account validation. Which two solutions satisfy these requirements? (Choose two.)

- A. TACACS+ authentication
- B. Unified Access Control
- C. firewall authentication
- D. integrated user firewall

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

What are two design requirements for deploying a chassis cluster across a Layer 2 network? (Choose two.)

- A. VLAN tags from high availability traffic should be preserved.
- B. Latency between the two nodes must be less than 100 ms.
- C. Fabric links should share the transit traffic infrastructure.
- D. Control and fabric link must use different VLAN IDs.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://forums.juniper.net/jnet/attachments/jnet/srx/1659/1/L2HAApNotev2.pdf>

QUESTION 27

Your company is establishing a BYOD policy and you are asked to create the appropriate security infrastructure. In the policy, Internet access should only be provided to the BYOD wired and wireless devices. Which two security features meet these requirements? (Choose two.)

- A. 802.11g
- B. 802.1X
- C. guest VLAN
- D. C-VLAN

Correct Answer: BC

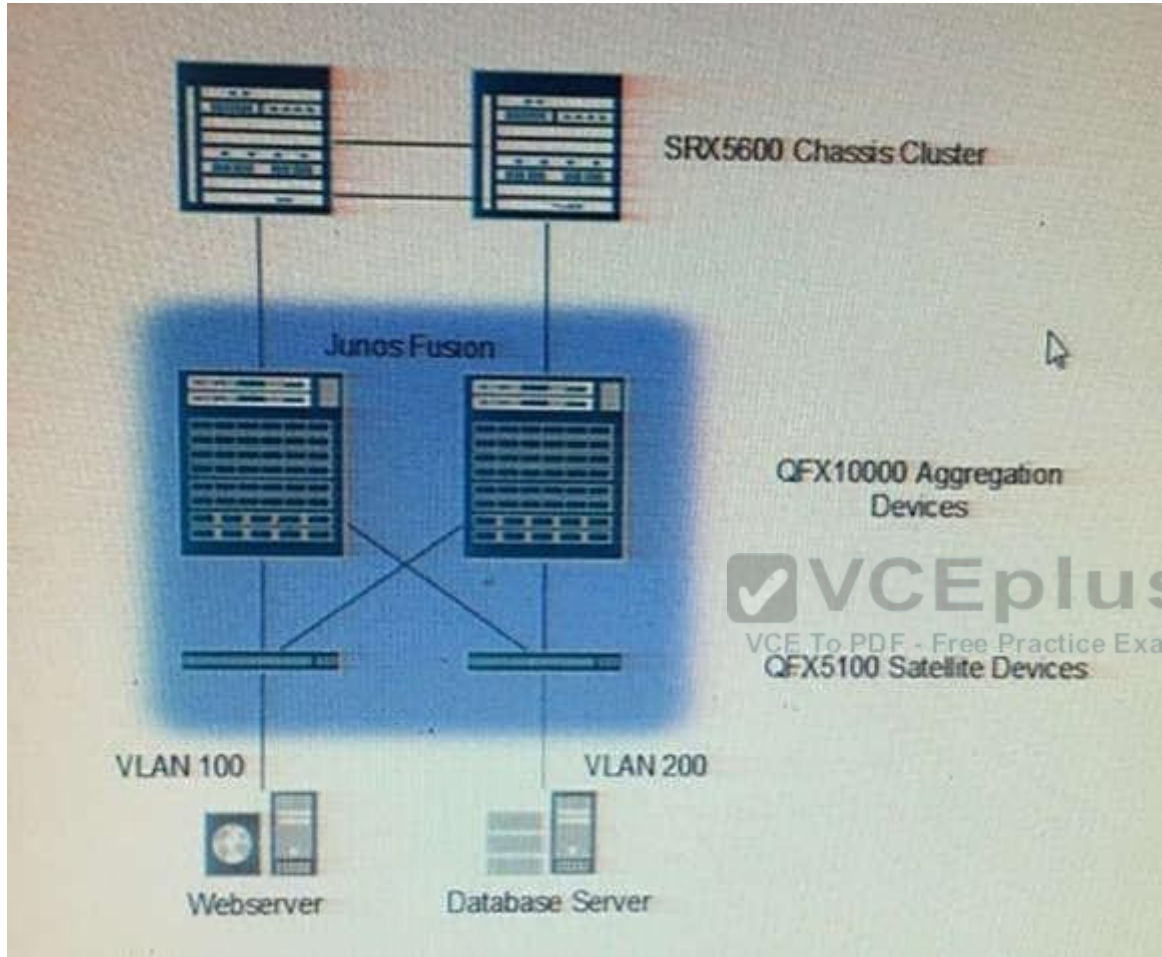
Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

Click the Exhibit button.



Given the data center topology shown in the exhibit, what are two designs that enable the SRX Series devices to inspect all traffic between the webserver and database server? (Choose two.)

- A. Place the Layer 3 gateways for VLAN 100 and VLAN 200 in the same virtual router in the Junos Fusion configuration. Connect this virtual router to a security zone on the SRX5600.
- B. Change the Junos Fusion configuration so that the webserver and database server are in the same VLAN.
- C. Place the Layer 3 gateways for VLAN 100 and VLAN 200 on redundant Ethernet interfaces of the SRX5600 and assign these interfaces to different security zones.

D. Place the Layer 3 gateways for VLAN 100 and VLAN 200 in different virtual routers in the Junos Fusion configuration. Connect the virtual routers to different security zones on the SRX5600.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

You are asked to provide a design proposal for a campus network. As part of the design, the customer requires that all end user devices must be authenticated before being granted access to their Layer 2 network. Which feature meets this requirement?

- A. IPsec
- B. 802.1X
- C. NAT
- D. ALGs

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Section: (none)

Explanation

QUESTION 30

Which three actions are part of an in-depth network defense strategy? (Choose three.)

- A. providing data modeling
- B. auditing for suspicious events
- C. providing security awareness training
- D. providing least privileged network access
- E. installing multiple antivirus solutions on desktop computers

Correct Answer: BCD

Section: (none)