Juniper JNCDS-SEC Certification JN0-1330 Exam

- **Vendor: Juniper**
- **Exam Code: JN0-1330**
- **Exam Name: Juniper Networks Certified Design Specialist, Security (JNCDS-SEC)**

QUESTION 1
Which security solution protects against zero-day attacks?

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

Answer: B

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.

Answer: ABC
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.
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

Answer: ABD
Explanation:
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

Answer: AD

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

Answer: AB

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

Answer: D

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

Answer: C
Explanation:
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.

Answer: ABE
Explanation:
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.

Answer: C

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

Answer: D

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

Answer: B
Explanation:
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. App Secure
B. Service Policy
C. Express Path
D. Virtual Network

Answer: BD
Explanation:
Service chaining requires the following configuration components to build the chain:
- Service template
- Virtual networks
- Service instance
- Network policy

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.

Answer: BC

QUESTION 14
What is the maximum number of SRX Series devices in a chassis cluster?

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

Answer: A

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.

Answer: B

QUESTION 16
Spotlight Secure provides which benefit?

A. log management
B. botnet protection
C. centralized management of security devices
D. IPsec encryption

Answer: C

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.

Answer: CDE
Explanation:

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.

Answer: D

Explanation:

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

Answer: A

Explanation:

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.

Answer: C

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.

Answer: ADE
Explanation:
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.

Answer: ABE

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

Answer: D
Explanation:
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 webservers 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.

Answer: AD

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

Answer: D

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 100ms.
C. Fabric links should share the transit traffic infrastructure.
D. Control and fabric link must use different VLAN IDs.

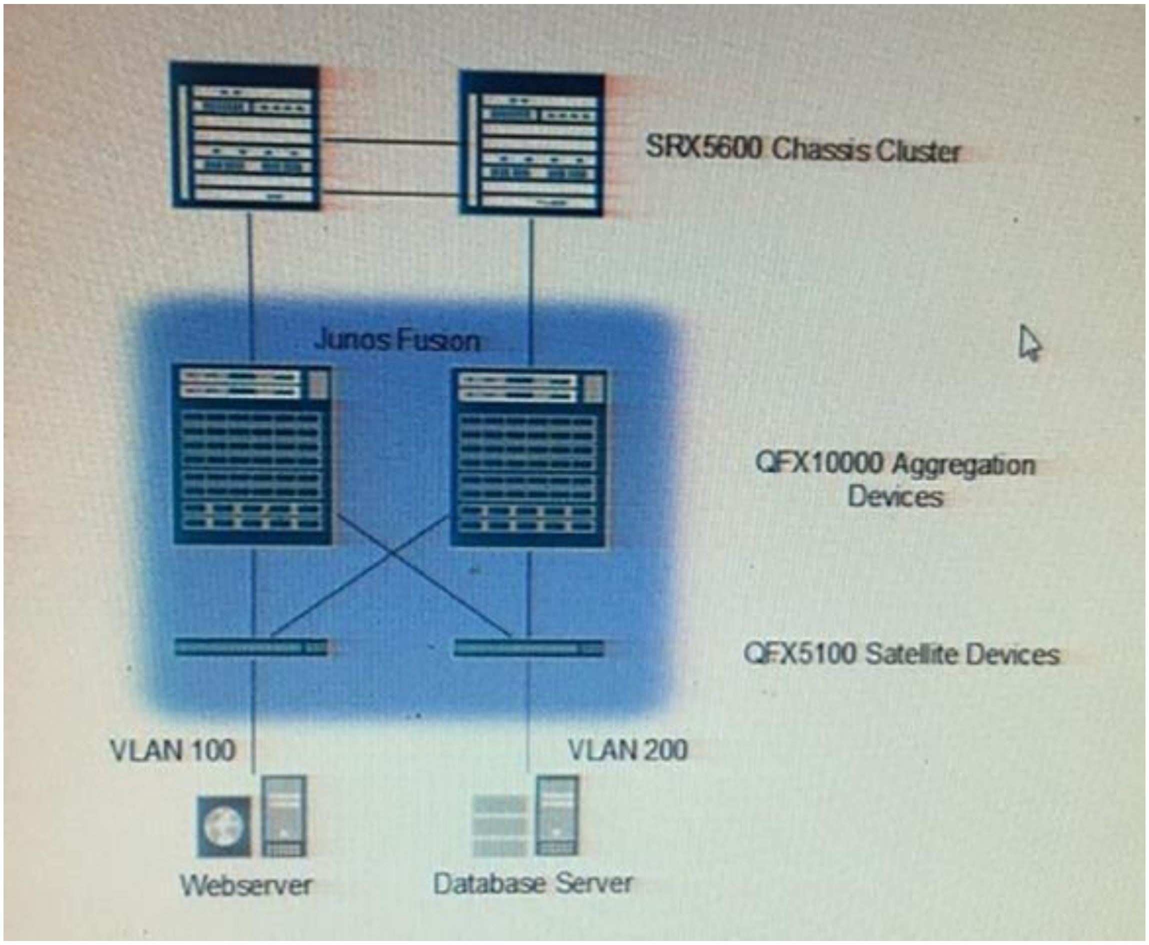
Answer: AB
Explanation:
https://forums.juniper.net/jnet/attachments/jnet/srx/1659/1/L2HAAppNotev2.pdf

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

Answer: BC

QUESTION 28
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.

Answer: CD

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

Answer: B

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

Answer: BCD

QUESTION 31
Your company must enable high-speed Layer 2 connectivity between two data centers connected by private fiber. Your security policy mandates that all company data is encrypted between sites. Which technology would you use to meet these requirements?

A. IPsec
B. MACsec
C. L2PT
D. VXLAN

Answer: B

QUESTION 32
Your customer is in the design stage for a new data center. They have historically used the SRX5600. To improve the security of the data center, you will be suggesting they deploy vSRXs and hardware-based firewalls. In this scenario, what are two reasons for deploying a virtual firewall? (Choose two.)

A. The SRX5600 does not support IPS.
B. The ability to secure traffic between VMs without leaving the physical server hardware.
C. vSRX can reside anywhere in the virtual environment.
D. A vSRX has greater throughput than an SRX5600.

Answer: BC

QUESTION 33
Which statements about IPsec tunnels is true?

A. They are used to provide in-depth packet inspection for traffic leaving your network.
B. They are used to prevent routing loops in a Layer 2 environment.
C. They are used to secure and encrypt traffic between tunnel endpoints.
D. They are used to combine multiple interfaces into a single bundle.

Answer: C

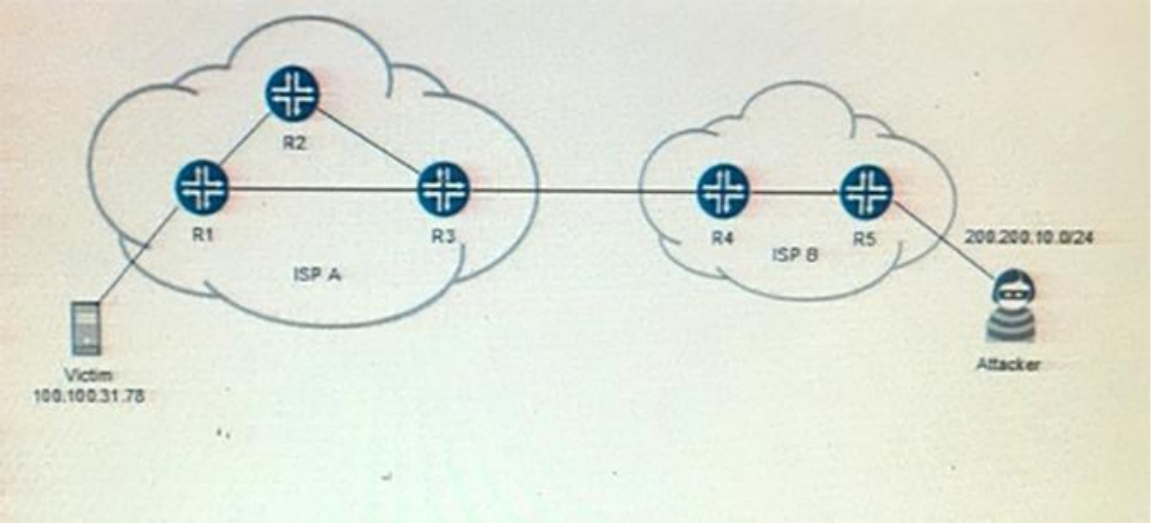
QUESTION 34
A client wants to deploy a vSRX chassis cluster across two existing ESXi hosts without changing the external switch configuration. Which two actions must you perform to meet this requirement? (Choose two.)

A. Use a distributed virtual switch.
B. Use an overlay network to transport cluster heartbeats over Layer 3.

C. Configure private VLANs on the virtual switch for the control and fabric links.
D. Use a standard virtual switch.

Answer: AC
Explanation:
http://www.juniper.net/techpubs/en_US/vsrx15.1x49/topics/task/configuration/security-vsrx-chassis-cluster-node-dswitch-deploying.html

QUESTION 35
Referring to the network shown in the exhibit, a SYN flood attacks is initiated by an attacker that has a public IP address from ISP B within the 200.200.10.0/24 prefix. The attacker is sending SYN packets to the victim, connected to ISP A, with destination address of 100.100.31.78 using spoofed source addresses at random from the 192.168.0.0/16 prefix. Which two design best practices would prevent this attack from working? (Choose two.)



A. ISP A should implement an ingress firewall filter on router R2 to discard traffic originating from the 200.200.10.0/24 prefix.
B. ISP A should implement an ingress firewall filter on router R3 to discard traffic originating from the 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 prefixes.
C. ISP A should implement an ingress firewall filter on router R3 to discard traffic originating from the 200.200.10.0/24 prefix.
D. ISP B should implement an ingress firewall filter on the router R5 interface connecting to the attacker that discards packets with a source address not matching the 200.200.10.0/24 prefix.

Answer: BD

QUESTION 36
You are asked to deploy user access to the Internet, and you want to determine which applications are passing through the firewall. Which feature accomplishes this task?

A. IPS
B. AppTrack
C. AppQoS
D. AppFW

Answer: B

QUESTION 37

A customer is globally expanding their retail stores exponentially. Their IT department is small. The effort to deploy new services is delaying the project. The customer's requirements are shown below:

```
- New stores must be activated with minimal effort.
- New stores must have IPsec connectivity back to the main data center.
- Some systems must be deployed locally and cannot be hosted in the data center.
- All systems deployed in remote stores must be upgraded at once when needed.
- The solution must allow new services to be included in the remote locations with minimal effort.
```

Which three Juniper solutions would you recommend in this scenario? (Choose three.)

A. Network Service Activator
B. Junos Space Network Director
C. NFX Network Services Platform
D. Contrail Service Orchestration
E. Junos Space Virtual Director

Answer: ABC

QUESTION 38

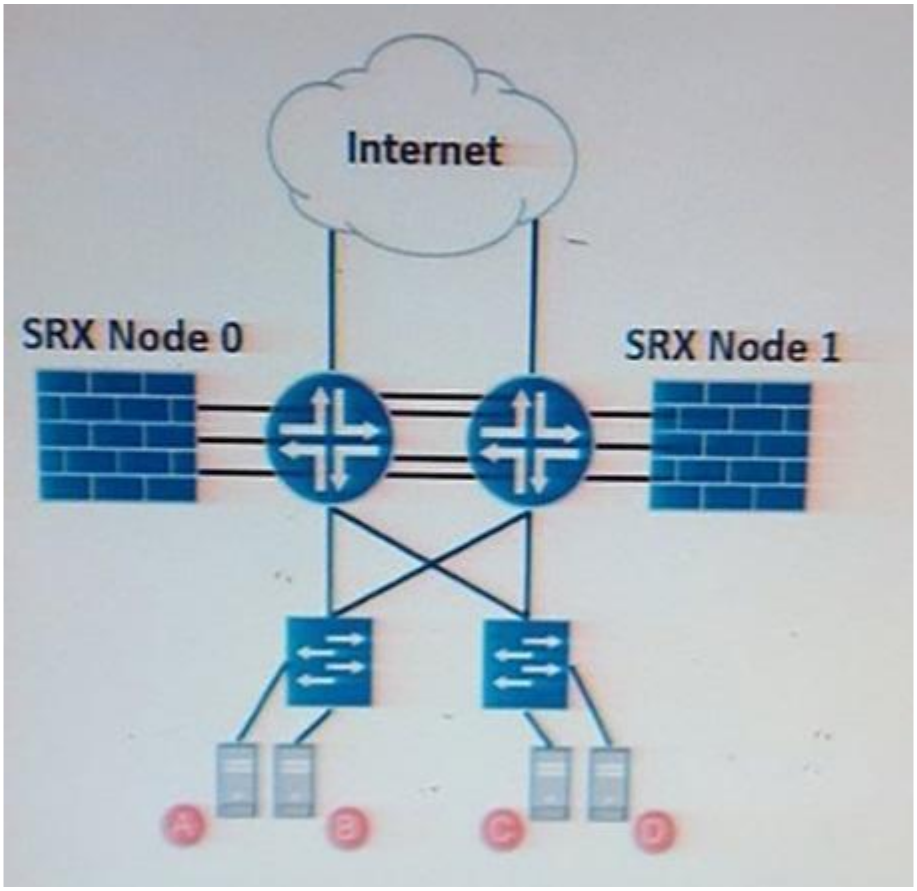
You are designing a network management solution for a customer's data center. Your design must include a solution that supports the collection of events from SRX Series devices, as well as events from various third-party devices. In this scenario, which solution should you recommend?

A. Secure Analytics
B. Cloud Analytics Engine
C. Log Director
D. NorthStar Controller

Answer: A

QUESTION 39

The data center shown in the exhibit is running an active/active SRX Series chassis cluster and an active/active network infrastructure. Customer A needs to communicate with customer D, and customer B needs to communicate with customer C. In this scenario, which two steps avoid Z-mode traffic? (Choose two.)



A. Associate customer A and customer D network segments in different redundancy groups.
B. Associate customer A and customer D network segments in the same redundancy groups.
C. Associate customer B and customer C network segments in the same redundancy groups.
D. Associate customer B and customer C network segments in different redundancy groups.

Answer: BC

QUESTION 40
Which solution centralizes the management of security devices in your data center?

A. Juniper Secure Analytics
B. J-Web
C. Junos Space Security Director
D. Junos CLI

Answer: C

QUESTION 41
Your company's IT policy restricts general access to recruitment websites from within the corporate network. However, the human resources department requires access to these sites. Which two features accomplish this goal? (Choose two.)

A. URL whitelist
B. Active Directory authentication
C. Web authentication

D. Enhanced Web filtering

Answer: AD

QUESTION 42

In the data center, what are two characteristics of access tier VLAN termination at the firewall? (Choose two.)

A. Inter-VLAN traffic can bypass firewall services.
B. Intra-VLAN traffic is secured through firewall services.
C. Inter-VLAN traffic is secured through firewall services.
D. Intra-VLAN traffic can bypass firewall services.

Answer: CD

QUESTION 43

Your company is migrating an existing enterprise application to use TLS. The application is written in PHP and must have IPS protection. Which two actions will ensure that the application is protected on an SRX5400? (Choose two.)

A. Use an IPS policy to protect all port 80 traffic.
B. Use the SSL reverse proxy feature.
C. Use the IPS policy that includes critical and major PHP signatures.
D. Use enhanced Web filtering.

Answer: CD

QUESTION 44

You are asked to deploy security in your data center with the criteria listed below:

```
- The deployment must allow for selective firewall redirect.
- The deployment must allow for selective firewall bypass.
```

Which deployment meets these requirements?

A. inline firewall
B. two-arm firewall
C. one-arm firewall
D. transparent firewall

Answer: C
Explanation:
http://www.juniper.net/us/en/local/pdf/implementation-guides/8010046-en.pdf

QUESTION 45

You are asked to implement network segmentation to increase security within your internal network. Which three statements are correct in this scenario? (Choose three.)

A. Analyze the compute resource and provisioning requirements.
B. Determine the appropriate routing protocols for traffic management.
C. Gain visibility of traffic, users, and assets.
D. Implement granular controls on traffic, users and assets.
E. Protect communications and resources on both inbound and outbound requests.

Answer: CDE
Explanation:
http://www.securityweek.com/using-network-segmentation-protect-modern-enterprise-network

QUESTION 46

You are designing a network for a customer who has given you specific requirements for the Internet gateway:

```
- The device must validate BGP peers
- Administrators must be able to verify that packet filters on the
loopback interfaces are working as expected
```

What are two features on the Internet gateway that address the customer's requirements? (Choose two.)

A. packet counting and logging
B. routing protocol authentication
C. source network address translation
D. intrusion prevention system

Answer: AB

QUESTION 47

You are preparing for the initial deployment of 100 SRX Series devices, and you want to leverage the autoinstallation feature. Which three prerequisites are required before you begin this task? (Choose three.)

A. Create a device-specific or default configuration file, and store it on a TFTP server in the network.
B. Confirm reachability to an active Contrail Controller within the same Layer 2 domain.
C. Log in to the SRX Series device as the root user and confirm the BASH shell connectivity.
D. Physically attach the SRX Series devices to the network using a valid interface.
E. Configure a DHCP server on your network to meet your network requirements.

Answer: ADE
Explanation:
https://www.juniper.net/techpubs/en_US/junos14.1/topics/task/configuration/ex-series-configuration-files-autoinstallation-cli.html

QUESTION 48

Which three functions are licensed UTM features? (Choose three.)

A. denial-of-service protection
B. antispam
C. enhanced Web filtering
D. intrusion prevention system
E. antivirus

Answer: BCE
Explanation:
http://www.juniper.net/documentation/en_US/junos12.3x48/topics/concept/security-branch-device-utm-understanding.html

QUESTION 49

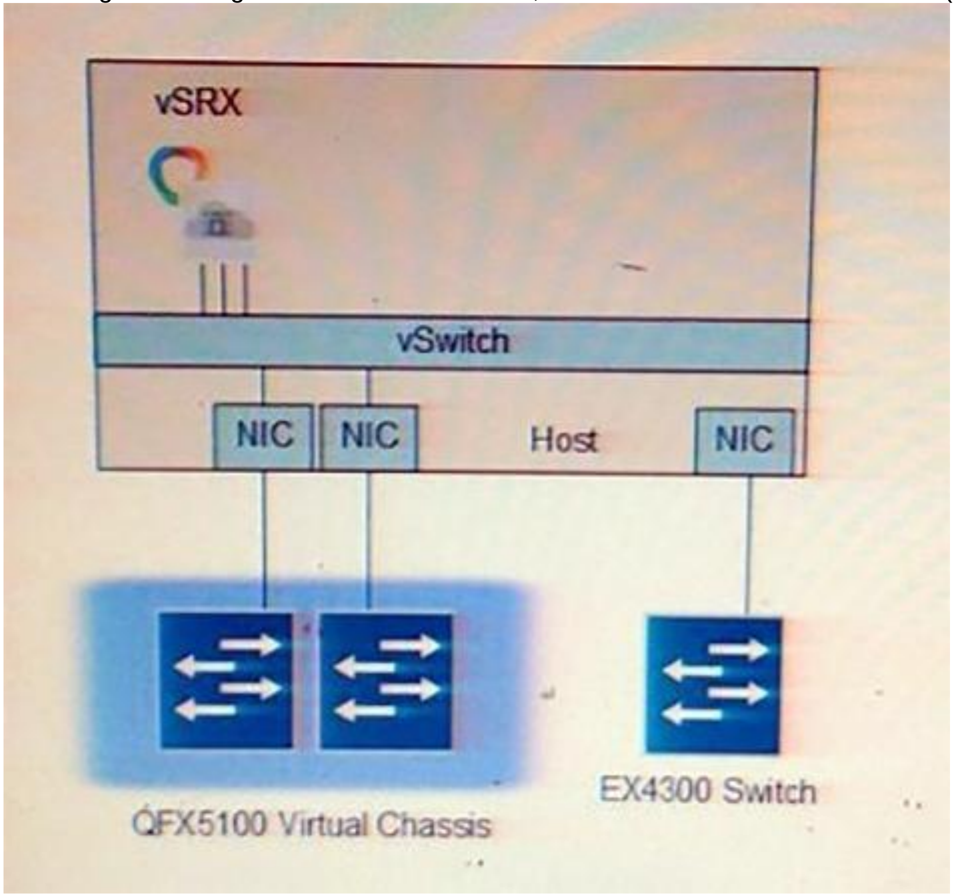
You are asked to design a high availability solution for a customer that wants to use a chassis cluster with two redundancy groups (RG0 and RG1). Their requirements dictate that the Routing Engine does not failover if RG1 fails. RG1 must failover automatically if there is an interface failure. How would you accomplish this task?

A. Monitor all interfaces in RG1 only.
B. Monitor all interfaces in RG0 only.

C. Do not monitor any interfaces in either redundancy group.
D. Monitor all interfaces in all redundancy groups.

Answer: A

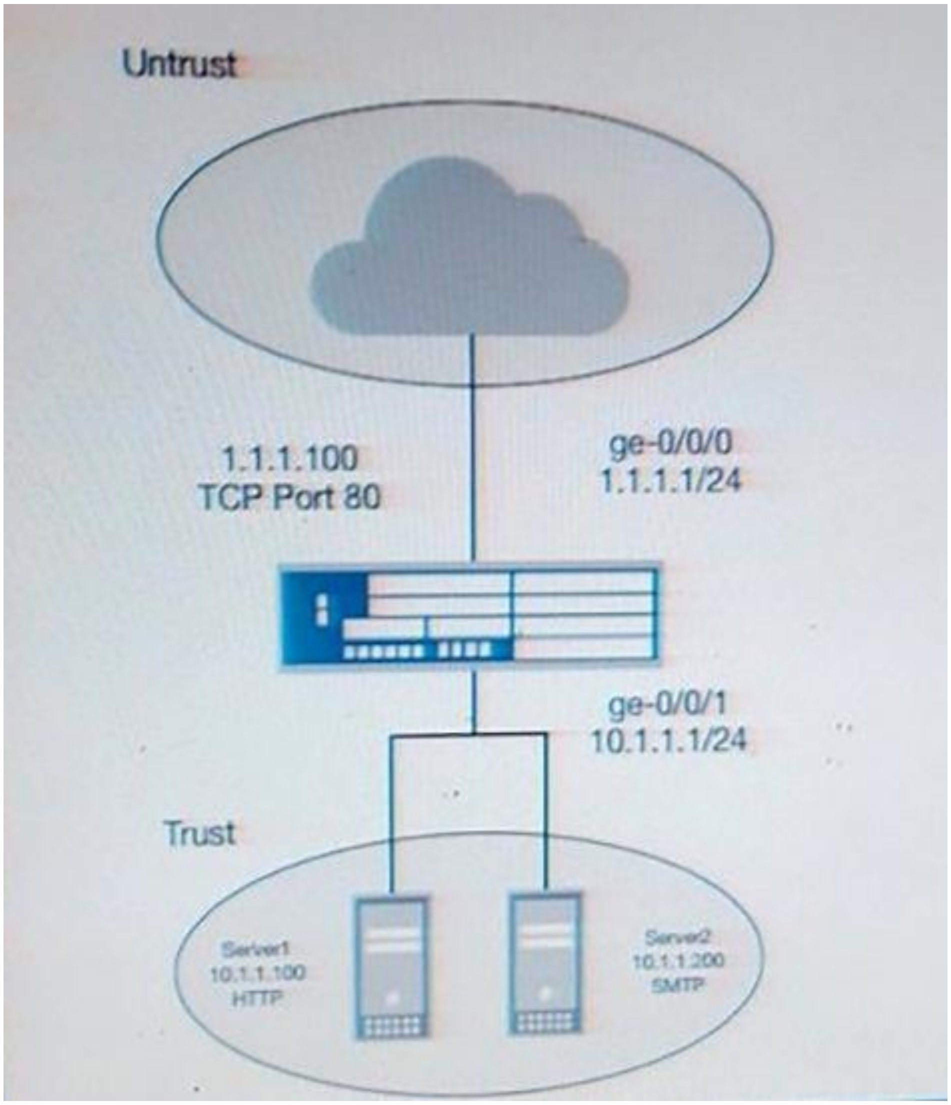
QUESTION 50
Referring to the diagram shown in the exhibit, which three statements are true? (Choose three.)



A. Layer 2 high availability can be enabled by configuring 802.3ad link aggregation between the vSRX and the vSwitch.
B. Layer 2 high availability can be enabled by configuring 802.3ad link aggregation between the vSwitch and the QFX5100 Virtual Chassis.
C. VMware and KVM are supported host hypervisors for vSRX.
D. The number of NICs on the vSRX must match the number of NICs on the host.
E. One NIC on the vSRX is reserved for management.

Answer: BCE

QUESTION 51
Your customer needs to make Server's HTTP service and Server2's SMTP service available to the Internet behind a single public IP address.



Referring to the exhibit, which type of NAT will satisfy the customer requirement?

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

Answer: B
Explanation:
https://www.juniper.net/techpubs/en_US/junos12.1/topics/example/nat-security-destination-address-port-translation-configuring.html

QUESTION 52
You are designing the security improvements needed to protect an application that your company is about to deploy. The only traffic that the application can receive is valid HTTP traffic on TCP port 8080 that was inspected for Application Layer attacks. Which three SRX Series device features will satisfy the requirements? (Choose three.)

A. intrusion prevention system

B. AppSecure
C. screens
D. security policy
E. antivirus

Answer: ABD

QUESTION 53
You are asked to design security policies for your corporate network where policy-based VPNs will be used. In this scenario, which three statements for a traffic match are true? (Choose three.)

A. The policy action is always permit.
B. A VPN tunnel is indirectly referenced by a route that points to a specific tunnel interface.
C. The security policy sets up the IPsec tunnel.
D. Tunnels are generated when traffic matches a policy.
E. The policy refers to the remote IKE gateway.

Answer: ABC
Explanation:
https://kb.juniper.net/InfoCenter/index?page=content&id=KB4124&actp=search

QUESTION 54
What are two reasons to add Routing Engine protection? (Choose two.)

A. to ensure that only permitted network nodes and hosts communicate with the WAN infrastructure.
B. to conceal routes by hiding them behind Internet gateways.
C. to ensure that all routing information is encrypted.
D. to protect the infrastructure from DDoS attacks.

Answer: AD

QUESTION 55
Which technology would you use to detect and analyze a denial-of service attack on a service provider network?

A. Sky Advanced Threat Prevention
B. route reflector
C. J-Flow
D. unified threat management

Answer: ......