Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

JN0-335 MCQs
JN0-335 TestPrep
JN0-335 Study Guide
JN0-335 Practice Test
JN0-335 Exam Questions

PASS

killexams.com

Juniper

JN0-335

Security, Specialist (JNCIS-SEC)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/JN0-335

Question: 626

You are tasked with enhancing the visibility of network traffic through your Juniper SRX device. Which two features should you implement to achieve better monitoring and analysis capabilities? (Choose two.)

A. Enabling packet capture on specific interfaces for detailed traffic analysis.
B. Configuring flow monitoring to track traffic statistics and patterns.
C. Implementing endpoint security solutions to monitor device behavior.
D. Utilizing SNMP traps to alert on network anomalies.

Answer: A, B

Explanation: Packet capture provides detailed insights into traffic flows, while flow monitoring allows for the collection of statistics and patterns, enhancing visibility and facilitating analysis of network behavior.

Question: 627

What are the implications of enabling "Jumbo Frames" on a Juniper switch, and which two considerations must be taken into account? (Choose two.)

A. Jumbo Frames can significantly increase throughput by reducing CPU overhead associated with processing smaller packets.
B. All devices within the network must support Jumbo Frames to avoid fragmentation and potential packet loss.
C. Enabling Jumbo Frames may require reconfiguration of QoS policies to accommodate the larger frame size.
D. The use of Jumbo Frames can lead to increased latency in network traffic due to larger packet sizes.

Answer: B, C

Explanation: For Jumbo Frames to be effective, all network devices must support them to prevent fragmentation. Additionally, QoS policies may need adjustments to handle the larger frame sizes appropriately, ensuring optimal performance.

Question: 628

What is the primary function of a Juniper IDP (Intrusion Detection and Prevention) system in a network security architecture, and how does it differ from traditional firewall capabilities?

A. To analyze and block malicious traffic based on signatures
B. To provide antivirus protection for network traffic
C. To encrypt sensitive data in transit
D. To facilitate secure remote access for users

Answer: A

Explanation: The primary function of a Juniper IDP system is to analyze and block malicious traffic based on signatures and behavior, differentiating it from traditional firewalls that primarily focus on allowing or denying traffic based on predefined rules.

Question: 629

Which three configurations are necessary to secure Juniper firewall filters? (Choose three.)

A. Defining filter action precedence
B. Enabling logging within the filter
C. Configuring global firewall policies
D. Setting interface-specific filters
E. Implementing IPsec encapsulation

Answer: A, B, D

Explanation: To secure Juniper firewall filters, it is crucial to define the precedence of filter actions to ensure the correct application order, enable logging for monitoring and auditing purposes, and set interface-specific filters to apply different rules based on traffic direction and type.

Question: 630

When configuring a Juniper SRX Series device for intrusion prevention, which two components are critical in defining the behavior of the intrusion detection system (IDS) and intrusion prevention system (IPS)? (Choose two.)

A. Security policies
B. Threat intelligence feeds

C. Packet capture settings
D. Application layer gateways

Answer: A, B

Explanation: Security policies are essential for defining what constitutes malicious behavior within the network and how the IDS/IPS should respond. Threat intelligence feeds enhance the system's ability to identify and block known threats, making them critical components of effective intrusion prevention.

Question: 631

A network administrator is tasked with implementing a firewall policy that restricts access to sensitive data based on user roles. What method should the administrator prioritize to ensure that only authorized users can access this data while maintaining compliance with organizational security standards?

A. Implementing static IP address filtering
B. Configuring a DMZ for data access
C. Enforcing network segmentation
D. Utilizing role-based access control (RBAC)
Answer: D

Explanation: Role-based access control (RBAC) allows organizations to assign permissions based on user roles, ensuring that only authorized users can access sensitive data. This method aligns with compliance standards by limiting access based on job functions.

Question: 632

You are conducting a security assessment of your network and need to identify potential vulnerabilities. Which tool on your Juniper device would be most useful for this task?

A. Network Scanner
B. Vulnerability Assessment Tool
C. Log Analyzer
D. Configuration Management Tool

Answer: B

Explanation: A Vulnerability Assessment Tool helps identify weaknesses within your network

infrastructure, which is crucial for maintaining security.

Question: 633

While reviewing the configuration of a Juniper SRX device, you come across multiple security policies with overlapping match conditions. What is the recommended approach to resolve this issue?

A. Consolidate policies to eliminate redundancy and ensure clarity.
B. Maintain the overlapping policies to allow for flexibility in traffic handling.
C. Prioritize policies based on the order they appear in the configuration.
D. Document each policy's purpose to justify their coexistence.

Answer: A, C

Explanation: Consolidating policies reduces complexity and redundancy, while prioritization based on configuration order ensures that the most relevant policies are applied first.

Question: 634

What is the most significant challenge an organization faces when transitioning to a hybrid cloud environment in terms of security management?

A. Increased costs associated with cloud services
B. Lack of user adoption for cloud applications
C. Complexity of managing security across multiple environments
D. Difficulty in integrating legacy systems

Answer: C

Explanation: The complexity of managing security across multiple environments is the most significant challenge when transitioning to a hybrid cloud environment, as it requires consistent policies and visibility across both on-premises and cloud infrastructures.

Question: 635

Which of the following strategies is essential for maintaining the effectiveness of Juniper Advanced Threat Prevention systems in the face of rapidly evolving cyber threats?

A. Continuous learning and adaptation through AI and machine learning
B. Relying solely on historical data for decision-making
C. Limiting access to security logs
D. Reducing the frequency of system updates

Answer: A

Explanation: Continuous learning and adaptation through AI and machine learning are essential strategies for maintaining the effectiveness of Juniper Advanced Threat Prevention systems, enabling them to respond dynamically to new threats.

Question: 636

In a multi-layered security architecture, which two elements are crucial for ensuring effective application security?

A. Isolating application servers from the rest of the network
B. Implementing a comprehensive set of security policies that span all layers
C. Relying solely on perimeter defenses to secure applications
D. Regularly updating application components to the latest versions

Answer: B, D

Explanation: A comprehensive set of security policies across all layers ensures holistic protection, and regularly updating application components mitigates vulnerabilities that could be exploited by attackers.

Question: 637

While configuring your security infrastructure, you realize the need for automated policy enforcement based on user behavior. Which technology would best address this requirement?

A. Firewall rule sets
B. Network segmentation
C. User Behavior Analytics (UBA)

D. Static ACLs

Answer: C

Explanation: User Behavior Analytics (UBA) provides insights into user activity patterns and can automate policy enforcement based on detected anomalies, enhancing security.

Question: 638

Which three statements regarding the SRX Series firewall's application security features are true? (Choose three.)

A. Application security features can identify and control specific applications traversing the network.
B. The firewall can only block applications but cannot allow them based on policies.
C. Application signatures must be manually updated to recognize new threats.
D. The application security capabilities can integrate with user identity information for policy enforcement.
E. Policies can be defined to restrict access to specific applications during certain times.

Answer: A, D, E

Explanation: SRX firewalls can identify and control applications, integrate with user identity for policy enforcement, and allow time-based restrictions on application access.

Question: 639

When implementing IPSec VPNs on Juniper devices, which of the following statements correctly describes the purpose and function of the IKE phase in establishing a secure tunnel?

A. IKE phase establishes the security association and negotiates the encryption and authentication methods used for the VPN.
B. IKE phase is responsible for encrypting the data payload between the peers.
C. IKE phase is only used for key management and does not impact the actual data traffic.
D. IKE phase ensures that only authenticated users can establish a VPN connection, but does not handle key exchanges.

Answer: A

Explanation: The IKE (Internet Key Exchange) phase is crucial in establishing a secure tunnel for IPSec VPNs as it negotiates the security association parameters, including encryption and authentication methods. This negotiation is essential for ensuring that both peers agree on the cryptographic standards before any secured data transmission occurs.

Question: 640

Your organization requires that all email traffic be inspected for malware before it is delivered to users. As part of the firewall configuration on a Juniper SRX device, which feature should you enable to achieve this?

A. Enable application awareness for all email protocols.
B. Implement a dedicated email security gateway before the firewall.
C. Use the threat prevention settings to inspect email traffic.
D. Configure logging to monitor email traffic without inspection.

Answer: C

Explanation: Enabling threat prevention settings on the SRX device allows for malware inspection of email traffic, ensuring that threats are mitigated before reaching users.

Question: 641

Which of the following is a key requirement for deploying Juniper's vSRX in cloud environments to ensure optimal performance and scalability?

A. Sufficient physical resources
B. Static IP addressing
C. Limited network segmentation
D. No external firewall integration

Answer: A

Explanation: Sufficient physical resources are necessary to ensure that the vSRX can handle the expected traffic load and provide the required performance in cloud environments.

Question: 642

Which two configurations should be prioritized when deploying a Juniper SRX device in a multi-tenant environment? (Choose two.)

A. Implement virtual routers for traffic isolation.
B. Disable all logging features to save storage.
C. Utilize security zones for segmentation.
D. Use a single IP address for all tenants.

Answer: A, C

Explanation: Implementing virtual routers and security zones is critical for isolating tenants and managing traffic effectively in a multi-tenant environment, enhancing both security and performance.

Question: 643

You are tasked with configuring a security policy that restricts access to a specific web application based on user roles. Which of the following configurations would best achieve this goal?

A. Define user roles in the security policy and apply them directly to security zones.
B. Implement role-based access control (RBAC) within the security policy configuration.
C. Use a dynamic address book to group users based on their roles and apply it in the policy.
D. Configure application firewall rules that specify user roles in the match criteria.

Answer: B, C

Explanation: Role-based access control allows for fine-grained control over user access, while dynamic address books can help group users by roles, making policy application more efficient.

Question: 644

A company is implementing a new security policy that requires all remote access to corporate resources to be encrypted. What type of VPN should the network administrator configure to meet this requirement while allowing users to connect securely from various locations?

A. Site-to-site VPN
B. SSL VPN

C. Remote access VPN
D. IPsec VPN

Answer: B

Explanation: An SSL VPN allows for secure remote access to corporate resources over the internet, providing encryption for connections while being user-friendly and compatible with various devices and locations.

Question: 645

What is the significance of certificate revocation lists (CRLs) in SSL proxy environments?

A. CRLs are unnecessary as SSL proxies do not require any form of certificate validation.
B. They provide a mechanism for SSL proxies to verify that certificates presented by clients or servers have not been revoked.
C. CRLs are only used in non-SSL environments and have no relevance in secure communications.
D. CRLs should be ignored to streamline the SSL handshake process.

Answer: B

Explanation: Certificate revocation lists (CRLs) are essential for SSL proxies to verify that the certificates presented during the SSL handshake have not been revoked, ensuring the trustworthiness of the communication.

Question: 646

Which three types of malware can be effectively mitigated using Juniper's advanced malware detection features? (Choose three.)

A. Ransomware
B. Adware
C. Rootkits
D. Keyloggers
E. Worms

Answer: A, C, D

Explanation: Advanced malware detection features can effectively mitigate ransomware, which encrypts files for ransom, rootkits that hide malicious activities from detection, and keyloggers that capture keystrokes for credential theft.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.