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

KILL EXAMS

JN0-231 MCQs
JN0-231 TestPrep
JN0-231 Study Guide
JN0-231 Practice Test
JN0-231 Exam Questions

killexams.com

Juniper

JN0-231

Security - Associate (JNCIA-SEC)

ORDER FULL VERSION

Question: 674

When configuring a VPN on a Juniper SRX device, which protocol is primarily responsible for ensuring the authenticity and integrity of data packets during transmission between two endpoints?

A. GRE
B. L2TP
C. IPsec
D. SSL

Answer: C

Explanation: IPsec (Internet Protocol Security) is specifically designed to provide authentication, integrity, and confidentiality for data packets transmitted over an IP network, making it essential for securing VPN connections.

Question: 675

Which two statements regarding the use of security policies on Juniper SRX devices are important for ensuring effective traffic control? (Choose two.)

A. Security policies must explicitly define both source and destination zones for effective traffic management.
B. The order of security policies is irrelevant; they are applied in a random manner.
C. Policies can be configured to log all traffic, allowing for detailed monitoring and analysis.
D. All traffic is allowed by default unless explicitly denied by a security policy.

Answer: A, C

Explanation: Effective traffic control requires security policies to explicitly define source and destination zones, and configuring policies to log all traffic is crucial for detailed monitoring and analysis of security events.

Question: 676

When configuring a Site-to-Site VPN in Junos, which of the following is a critical step that must be performed to ensure both ends of the tunnel can communicate securely?

A. Configure the same static routes on both devices to ensure proper traffic flow.

B. Implement a default permit rule for all traffic in the security policies to allow VPN traffic.
C. Set up a dynamic routing protocol to automatically manage tunnel traffic.
D. Ensure both devices have matching IKE and IPsec settings, including encryption algorithms and lifetimes.

Answer: D

Explanation: Ensuring that both devices have matching IKE and IPsec settings, including encryption algorithms and lifetimes, is critical for establishing a secure and functional Site-to-Site VPN.

Question: 677

Which authentication method provides the highest level of security for user access control in a Juniper firewall setup?

A. Password-based authentication
B. Machine-based authentication
C. Single sign-on (SSO)
D. Two-factor authentication

Answer: D

Explanation: Two-factor authentication (2FA) adds an additional layer of security by requiring not only a password but also a second factor, such as a mobile device or token, making it significantly harder for unauthorized access.

Question: 678

When configuring NAT on a Juniper SRX device, which two statements regarding source NAT and destination NAT are accurate? (Choose two.)

A. Source NAT is used primarily for internal hosts to communicate with external networks.
B. Destination NAT is used to allow external hosts to initiate connections to internal services.
C. Both source and destination NAT can be configured simultaneously for the same traffic flow.
D. Source NAT modifies the destination address of packets leaving the network.

Answer: A, B

Explanation: Source NAT is primarily used for allowing internal hosts to communicate with external networks, while destination NAT enables external hosts to connect to services hosted internally, facilitating bidirectional communication.

Question: 679

In the context of an application firewall, why is it important to implement application-layer filtering in addition to traditional network-layer filtering?

A. Traditional filtering is sufficient to protect against all types of attacks.
B. Application-layer filtering addresses threats that exploit vulnerabilities specific to applications, which network-layer filtering cannot adequately mitigate.
C. Application-layer filtering is only necessary for web traffic.
D. It simplifies the configuration of firewall rules.

Answer: B

Explanation: Application-layer filtering is crucial because it addresses threats that target specific application vulnerabilities, which traditional network-layer filtering alone cannot adequately mitigate, thus providing a more comprehensive security approach.

Question: 680

In a Juniper SRX environment, what is the primary function of the "log" action within a security policy?

A. To deny all traffic that does not match the specified criteria
B. To automatically block malicious users from accessing the network
C. To generate logs for traffic that matches the policy for future analysis
D. To redirect traffic to a different interface for monitoring

Answer: C

Explanation: The "log" action within a security policy generates logs for traffic that matches the policy, providing valuable information for future analysis and helping to identify patterns or potential security incidents.

Question: 681

Which two aspects of the vSRX deployment make it suitable for cloud environments? (Choose two.)

A. It requires dedicated physical hardware for optimal performance.

B. It can scale vertically by increasing resources on a single instance.
C. The vSRX can be deployed on various hypervisors, enhancing flexibility.
D. It is limited to specific cloud providers for deployment.

Answer: B, C

Explanation: The vSRX can scale vertically by increasing resources on a single instance, making it adaptable to varying loads. It also supports deployment on various hypervisors, providing flexibility in cloud environments.

Question: 682

In the context of Juniper's advanced threat prevention capabilities, which two features are critical for detecting and mitigating malware and zero-day threats? (Choose two.)

A. Application Layer Gateways (ALGs) that modify application traffic in real-time.
B. Integrated intrusion detection and prevention systems (IDPS) that analyze traffic patterns.
C. Static signature databases that exclusively rely on known malware definitions.
D. Behavioral analysis tools that monitor for anomalous activities across the network.

Answer: B, D

Explanation: Advanced threat prevention mechanisms rely on integrated intrusion detection and prevention systems (IDPS) to analyze traffic patterns and behavioral analysis tools to identify anomalous activities, thus effectively detecting and mitigating malware and zero-day threats.

Question: 683

Which two functionalities of Juniper's IDPS are vital for detecting and responding to threats? (Choose two.)

A. Signature-based detection of known threats.
B. Passive monitoring without any response capabilities.
C. Real-time alerts for suspicious activities.
D. Capability to learn and adapt to new threats automatically.

Answer: A, C

Explanation: The IDPS in Juniper devices utilizes signature-based detection to identify known threats and generates real-time alerts for suspicious activities. This proactive approach allows for timely responses to potential security incidents.

Question: 684

Which command would you use to verify the active security policies applied to an interface on a Juniper

SRX device, ensuring that you are examining the correct zone configuration?

A. show interfaces security
B. show configuration security policies
C. show security policies from-zone to-zone
D. show security zones

Answer: C

Explanation: The command show security policies from-zone to-zone allows you to check the specific security policies applied between defined zones, providing clarity on how traffic is managed based on the security configuration.

Question: 685

Which two statements about Juniper's device hardening techniques are essential for mitigating potential vulnerabilities and securing the SRX devices? (Choose two.)

A. Disabling unnecessary services and protocols to reduce the attack surface.
B. Keeping the default administrative credentials to simplify future access.
C. Regularly updating the device firmware and software to patch known vulnerabilities.
D. Allowing unrestricted access to management interfaces from any IP address.

Answer: A, C

Explanation: Device hardening techniques include disabling unnecessary services and protocols to minimize the attack surface, as well as regularly updating firmware and software to patch known vulnerabilities, ensuring the security of SRX devices.

Question: 686

During an analysis of security incidents, you want to correlate information from multiple log sources in Junos Space® Security Director. Which feature facilitates this correlation?

A. The "Event Correlation" engine that analyzes related events in context.
B. The "Log Aggregation" tool that combines logs from various sources.
C. The "Traffic Overview" that summarizes general traffic patterns.
D. The "Device Health" monitoring that focuses on device performance.

Answer: A

Explanation: The "Event Correlation" engine in Junos Space® Security Director facilitates the correlation of information from multiple log sources, analyzing related events in context to provide deeper insights into security incidents.

Question: 687

During a penetration test, it was discovered that certain application traffic was bypassing the Juniper SRX firewall. Which feature should be configured to ensure that all application traffic is inspected and controlled?

A. Basic NAT configurations
B. Network Address Translation (NAT)
C. Static routing
D. Application Layer Gateway

Answer: D

Explanation: Configuring an Application Layer Gateway ensures that all application traffic is inspected and controlled, preventing unauthorized bypassing of the firewall and enhancing overall security.

Question: 688

When configuring security policies, which statements about the role of application firewalls are correct? (Choose two.)

A. Application firewalls inspect traffic at the application layer to identify specific protocol misuse.
B. Application firewalls can only protect against network layer attacks.
C. Application firewalls are designed to manage traffic for well-defined applications.
D. Application firewalls operate independently of other security policies in place.

Answer: A, C

Explanation: Application firewalls provide deep packet inspection at the application layer, allowing them to detect and mitigate specific application-level attacks while managing traffic for designated applications effectively.

Question: 689

What is the role of "User Identity" in Juniper's security policies, and how can it be leveraged? (Choose three.)

A. It allows policies to be tied to user roles and identities.
B. It simplifies the configuration of network access controls.
C. It requires additional hardware to function effectively.
D. It can enhance security by enabling user-based logging.
E. It is only applicable in VPN configurations.

Answer: A, B, D

Explanation: User Identity allows for policies linked to user roles, simplifies access control configurations, and enhances security through detailed user-based logging, improving overall visibility.

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.