SonicWall Network Security Administrator (SNSA) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Copyright © 2025 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

SAMPLE

Questions

SAMPLE

1. **What happens when the primary WAN link fails under the basic failover option?**

   A. Secondary WAN link takes over

   B. All traffic is blocked

   C. Only critical traffic is rerouted

   D. Automatic reset to factory settings

2. **True or False: SonicOS 7 features intelligent device dashboards with actionable alerts and simplified policy management.**

   A. True

   B. False

   C. Not applicable

   D. Depends on configuration

3. **What port does the syslog server use?**

   A. 8080

   B. 514

   C. 80

   D. 443

4. **Does SonicWall recommend enabling IPS for low priority attacks?**

   A. True

   B. False

   C. Only for critical attacks

   D. Only in testing environments

5. **Which solution protects against both file-based and fileless malware with 360-degree attack view?**

   A. Next Generation Firewall

   B. Continuous Behavioral Monitoring

   C. Threat Intelligence Service

   D. VPN Client

SAMPLE

6. What type of intermediate traffic is monitored by the packet monitor?

A. Unicast Traffic

B. SSL Decrypted Traffic

C. Multicast Traffic

D. Remote Mirrored Traffic

7. What does a metric of infinity indicate in routing protocols?

A. The route is highly stable

B. The route is unreachable

C. The metric is optimal

D. The routing table is full

8. Which of the following statements is true about TACAS+?

A. It is not widely used anymore

B. It only supports SSL encryption

C. It provides authentication and accounting services

D. It is limited to internal users only

9. True or False: Denying LAN to WAN will prevent the check network setting Test MySonicWall.com.

A. True

B. False

C. Depends on configuration

D. Only for certain devices

10. In NSM, how are features such as unified policy management classified?

A. Compliance standards

B. Usability enhancements

C. Network monitoring

D. Device management

SAMPLE

Answers

SAMPLE

1. A
2. A
3. B
4. A
5. B
6. B
7. B
8. C
9. A
10. B

SAMPLE

Explanations

SAMPLE

1. What happens when the primary WAN link fails under the basic failover option?

A. Secondary WAN link takes over

B. All traffic is blocked

C. Only critical traffic is rerouted

D. Automatic reset to factory settings

When the primary WAN link fails and the basic failover option is configured, the secondary WAN link takes over. This automatic switch to the secondary link ensures that the network remains operational without manual intervention. The primary purpose of implementing failover mechanisms is to enhance network reliability and continuity by providing a backup pathway for data traffic. In this scenario, the secondary WAN link is already established and configured to handle traffic when the primary link is no longer available. This process is designed to minimize downtime and maintain connectivity for users or applications relying on the network. Other options are not applicable in this context; blocking all traffic would disrupt connectivity entirely, while rerouting only critical traffic would not fulfill the purpose of failover which is to provide continuous service through the secondary link. The mention of a factory reset is irrelevant to the failover process, as it implies a complete reconfiguration of the device rather than ensuring uninterrupted service.

2. True or False: SonicOS 7 features intelligent device dashboards with actionable alerts and simplified policy management.

A. True

B. False

C. Not applicable

D. Depends on configuration

SonicOS 7 indeed includes intelligent device dashboards that provide users with a comprehensive view of their network environment. These dashboards are designed to present critical information in a clear and concise manner, enabling administrators to monitor network health and performance effectively. Additionally, SonicOS 7 introduces actionable alerts that help users quickly identify and respond to potential security threats and performance issues. By simplifying policy management, it allows for easier and more efficient configuration of security policies, making it more accessible for network administrators to implement security measures. The features of intelligent dashboards and actionable alerts contribute significantly to improved network management and security, which explains why the statement is true.

SAMPLE

3. What port does the syslog server use?

A. 8080

B. 514

C. 80

D. 443

The syslog server primarily uses port 514 for communication. This port is specified in the relevant standards for syslog, allowing devices and applications to send log messages to the syslog server for aggregation and analysis. Syslog operates over UDP by default, but can also be configured to use TCP, with port 514 serving as the designated communication channel for both protocols. Understanding this standard is critical for network administrators, as correct configuration ensures efficient logging and monitoring of network events, allowing for improved troubleshooting and security monitoring. Other ports listed, such as 8080 (commonly used for HTTP alternative services), 80 (standard HTTP traffic), and 443 (standard HTTPS traffic), are not defined for syslog and serve different purposes in network communication.

4. Does SonicWall recommend enabling IPS for low priority attacks?

A. True

B. False

C. Only for critical attacks

D. Only in testing environments

SonicWall recommends enabling Intrusion Prevention System (IPS) for both low priority and higher severity attacks to provide comprehensive network protection. Enabling IPS helps in detecting and preventing potential threats that could exploit vulnerabilities in the network. Even low-priority attacks can lead to significant issues, especially if they are part of a larger attack vector or if they exploit a previously unknown vulnerability. Using IPS allows organizations to maintain robust security posture and proactively block threats before they can inflict damage. Prioritizing IPS enables network administrators to minimize risks by maintaining visibility and control over all forms of attack, rather than selectively filtering them by severity level. It's also essential to recognize that the dynamics of network threats are constantly changing; what may be considered a low priority today could escalate into a significant threat tomorrow. Therefore, having IPS enabled provides a dual benefit – it offers real-time protection against known and emerging threats while ensuring the security of network assets against a broader attack surface.

SAMPLE

5. Which solution protects against both file-based and fileless malware with 360-degree attack view?

A. Next Generation Firewall

B. Continuous Behavioral Monitoring

C. Threat Intelligence Service

D. VPN Client

The choice of Continuous Behavioral Monitoring as the correct answer highlights its capability to provide a comprehensive defense strategy against both file-based and fileless malware threats. Continuous Behavioral Monitoring leverages machine learning and advanced analytics to observe and analyze the behavior of applications and processes in real-time, allowing it to detect anomalies that signify potential malware activity. This proactive approach enables the identification of not only traditional malware but also sophisticated fileless threats that often evade conventional detection methods. In contrast, solutions like the Next Generation Firewall primarily focus on network-level security and may employ signature-based detection, which can sometimes miss fileless malware since it doesn't rely on files. The Threat Intelligence Service, while valuable for staying ahead of evolving threats, operates as an informational resource and does not actively monitor behaviors. The VPN Client serves a different purpose primarily aimed at securing remote connections and does not directly address malware threats. Continuous Behavioral Monitoring stands out for its holistic attack view, enabling organizations to safeguard against a full spectrum of malware attacks effectively.

6. What type of intermediate traffic is monitored by the packet monitor?

A. Unicast Traffic

B. SSL Decrypted Traffic

C. Multicast Traffic

D. Remote Mirrored Traffic

The correct answer is SSL Decrypted Traffic. The packet monitor is designed to analyze and inspect traffic that has been decrypted, particularly traffic that uses Secure Sockets Layer (SSL) encryption. When SSL traffic is intercepted and decrypted, it provides a clear view of the data flows, enabling the monitoring of both the content and the connection itself. By focusing on SSL decrypted traffic, the packet monitor plays a crucial role in helping network administrators detect and mitigate potential security threats that may be hidden within encrypted sessions. This capability is essential for maintaining network security, as it allows for the identification of malicious activity that would otherwise remain concealed within encrypted data transmissions. In contrast, unicast traffic refers to one-to-one communications between devices, multicast traffic pertains to one-to-many delivery models, and remote mirrored traffic generally involves a method used to replicate data across locations for redundancy or backup purposes. While these traffic types may also be monitored in various contexts, they do not specifically focus on the analysis of decrypted SSL communications, which is the primary function of the packet monitor.

SAMPLE

7. What does a metric of infinity indicate in routing protocols?

A. The route is highly stable

B. The route is unreachable

C. The metric is optimal

D. The routing table is full

In routing protocols, a metric of infinity signifies that the route is unreachable. When a route's metric is set to infinity, it essentially means that there is no viable path to the destination; the network considers it inaccessible. This concept is often employed in distance-vector routing protocols like RIP, where a route that exceeds a certain distance (commonly 16 hops) is deemed unreachable and assigned an infinite metric. This mechanism helps routers make informed decisions about the best paths to forward packets. If a route to a destination has an infinite metric, the router will no longer include this route in its routing table, preventing it from attempting to direct traffic to an islanded or non-existent endpoint. In contrast, other metrics, such as those indicating stability or optimality, refer to the quality or efficiency of a route but do not indicate unreachability. Additionally, a full routing table pertains to different limitations within the router's memory or configuration and does not directly relate to a route's metric.

8. Which of the following statements is true about TACAS+?

A. It is not widely used anymore

B. It only supports SSL encryption

C. It provides authentication and accounting services

D. It is limited to internal users only

TACACS+ is a protocol developed by Cisco that serves primarily for remote authentication and is known for providing both authentication and accounting services. It allows for secure communication between the user and the server, which is crucial for maintaining the integrity and confidentiality of user credentials and session details. The authentication aspect means that TACACS+ can verify the identity of users trying to access a network or system. Meanwhile, the accounting services track the usage of network resources by those authenticated users, which is key for monitoring which users were active and what operations they performed. These dual capabilities make TACACS+ a valuable tool in network security management, supporting organizations in their compliance and auditing efforts. Addressing the other statements, it is still a widely used protocol in many enterprises, is not limited to SSL encryption, and is designed to authenticate users regardless of whether they are internal or external to an organization, thereby demonstrating its flexibility. Therefore, the statement regarding TACACS+ providing both authentication and accounting services stands out as accurate.

SAMPLE

9. True or False: Denying LAN to WAN will prevent the check network setting Test MySonicWall.com.

A. True

B. False

C. Depends on configuration

D. Only for certain devices

Denying LAN to WAN traffic effectively restricts communication from your internal network to the external network. When this type of traffic is denied, users on the LAN will not be able to access resources or services available on the WAN, which includes the check network setting feature of Test MySonicWall.com. This is crucial because Test MySonicWall.com requires connectivity to perform its functionality; if traffic is blocked, the tests and verifications it provides cannot be executed successfully. Thus, by denying LAN to WAN, you are indeed preventing any communication required for utilizing that feature, making the statement true. This aligns with principles of network management where appropriate access controls directly affect functionality related to external diagnostic tools or services.

10. In NSM, how are features such as unified policy management classified?

A. Compliance standards

B. Usability enhancements

C. Network monitoring

D. Device management

Unified policy management, as classified within Network Security Management (NSM), refers to the simplification and enhancement of how policies are created, deployed, and managed across the network. Usability enhancements focus on improving the interactions between users and systems, making processes more intuitive and effective. In the context of NSM, these enhancements streamline the management of security policies, ensuring they are easier to handle and enforce consistently across various devices and platforms. This is particularly important in environments where security policy needs to adapt to changing network conditions and threats, allowing administrators to respond intelligently without excessive overhead. By improving usability in policy management, administrators can better maintain compliance with security standards and respond to incidents more effectively. The other categories do not capture the essence of unified policy management. Compliance standards relate to regulatory requirements and validation, network monitoring focuses on tracking and analyzing network performance and security events, while device management pertains to the administration of hardware assets rather than the overarching policies governing security across those devices.

SAMPLE