NSE7 Enterprise Firewall Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which command provides a quick view of traffic on the device, including blocked attacks?

A. get session info

B. get system performance status

C. watch traffic flow

D. system traffic overview

2. For which task is the process name 'authd' responsible?

A. User authentication

B. IPsec connections

C. File scanning

D. FortiGuard updates

3. What command is employed to display the amount of shared memory by processes?

A. diagnose hardware sysinfo share

B. diagnose hardware sysinfo shm

C. diagnose processes shminfo

D. diagnose hardware shared-memory

4. What is the primary purpose of the process name 'scanunitd'?

A. IPsec management

B. File scanning

C. WAN optimization

D. User authentication

5. What is the state representation for UDP traffic in both directions?

A. proto_state=00

B. proto_state=01

C. proto_state=10

D. proto_state=11

6. Which command is used to display the HA virtual MAC address?

A. get sys ha status

B. diagnose hardware deviceinfo nic <port_name>

C. execute ha manage <HA_unit_index> <Admin_Username>

D. diagnose sys ha dump-by vlcuster

7. What ports does IKE traffic primarily use?

A. TCP 80 and 443

B. UDP 500 and UDP 4500

C. UDP 9999 and TCP 22

D. TCP 23 and 53

8. How does FortiGate determine the site rating when processing SNI?

A. By analyzing traffic patterns

B. By retrieving the FQDN

C. By performing a DNS lookup

D. By checking user history

9. What command summarizes the statuses of all the OSPF neighbors?

A. get router info ospf database self-originate

B. get router info ospf status

C. get router info ospf neighbor

D. get router info ospf interface

10. Which command displays the current statistics on a HA pair?

A. get router info ospf database brief

B. diagnose sys ha status

C. diagnose sys ha dump-by vlcuster

D. get router info ospf interface

Answers

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

Explanations

1. Which command provides a quick view of traffic on the device, including blocked attacks?

A. get session info

B. get system performance status

C. watch traffic flow

D. system traffic overview

The command that offers a quick view of traffic on the device, including blocked attacks, is related to system performance. This command provides valuable insights into the current state of network traffic and system metrics, making it easier for administrators to monitor live conditions and identify any abnormal activities such as blocked attacks. By analyzing performance statistics, users can ascertain traffic loads, identify trends, and receive alerts about potential issues, all of which are critical for maintaining network health and security. The other commands serve different purposes: some may focus on session information or specific traffic flows, while others might provide a more holistic view of traffic but do not encapsulate both traffic and blocked threats as efficiently as the performance status command. Understanding the specific function of each command allows network administrators to utilize the most relevant tools for their immediate needs.

2. For which task is the process name 'authd' responsible?

A. User authentication

B. IPsec connections

C. File scanning

D. FortiGuard updates

The process name 'authd' is responsible for user authentication. This process plays a critical role in managing authentication requests from users trying to access resources through the firewall. It handles both local and remote authentication methods, ensuring that only authorized users can gain access based on defined policies. The functionality of 'authd' includes processing login events and validating user credentials against authentication servers, like RADIUS or LDAP, as well as handling single sign-on scenarios. While the other options describe important processes and functionalities within the firewall, they do not pertain to the 'authd' process. IPsec connections involve secure network communications, file scanning pertains to inspecting files for malware, and FortiGuard updates are related to receiving security updates and threat intelligence. Each of these operates independently of the user authentication processes managed by 'authd'.

3. What command is employed to display the amount of shared memory by processes?

A. diagnose hardware sysinfo share

B. diagnose hardware sysinfo shm

C. diagnose processes shminfo

D. diagnose hardware shared-memory

The command used to display the amount of shared memory by processes in Fortinet devices is "diagnose hardware sysinfo shm." This command specifically targets shared memory information, providing a clear and concise output regarding the shared memory segment utilized by different processes on the device. The use of "sysinfo" indicates that you are querying system-level information, and "shm" is the abbreviation for shared memory. This combination is designed to provide insights into how much shared memory is allocated and utilized, which is crucial for performance tuning and troubleshooting in an enterprise firewall environment. While the other options may appear relevant, they do not specifically focus on shared memory in the same way. For example, the first choice includes "share," which may not precisely align with the terminology used in the firewall's command set, creating ambiguity in its intended function. Similarly, "diagnose processes shminfo" pertains to process-specific shared memory information but is not the standard command for broad system shared memory display. Lastly, "diagnose hardware shared-memory" lacks the specificity provided by "shm" to clearly address the shared memory output. By using the correct command, network professionals can effectively monitor and manage resources, which is a vital part of maintaining optimal firewall performance and ensuring security in

4. What is the primary purpose of the process name 'scanunitd'?

A. IPsec management

B. File scanning

C. WAN optimization

D. User authentication

The process name 'scanunitd' is primarily associated with file scanning functions within a system. This service is integral to the security architecture of devices, as it monitors and scans files for malware, viruses, and other malicious threats. By actively checking content that passes through the network, 'scanunitd' ensures that harmful files do not compromise device integrity or the overall security posture of the firewall. File scanning involves the examination of data as it is transmitted or stored to detect and neutralize threats before they can cause damage. The efficient operation of this process is crucial for maintaining a secure environment, as it aids in the prevention of data breaches and the spread of malware across the network. In contrast, while other processes or functionalities are related to different aspects of network management and security—such as IPsec management for secure communications or user authentication for validating users—'scanunitd' specifically targets the vital task of scanning files. This distinct focus underscores its importance in proactive threat management and network security practices.

5. What is the state representation for UDP traffic in both directions?

A. proto_state=00

B. proto_state=01

C. proto_state=10

D. proto_state=11

The representation for UDP traffic in both directions is indicated as proto_state=01. In network protocols, the state representation often indicates whether the traffic is considered established or not. For UDP, which is a connectionless protocol, the state representation signifies the presence of bidirectional traffic without requiring a session establishment like TCP. The "01" state specifically indicates traffic is flowing in both the incoming and outgoing directions. This is important for firewall configurations, as it allows for the proper handling of UDP packets that may not maintain a session state, yet still need to be processed for valid communication between endpoints. Understanding this state representation is crucial in configurations that rely on stateful inspection methods, particularly in environments that leverage firewalls to monitor and filter network traffic. In contrast, other state representations like "00", "10", and "11" do not apply to the condition of bidirectional UDP traffic, as these would either denote different states of traffic (like one-directional or inactive states).

6. Which command is used to display the HA virtual MAC address?

A. get sys ha status

B. diagnose hardware deviceinfo nic <port_name>

C. execute ha manage <HA_unit_index> <Admin_Username>

D. diagnose sys ha dump-by vlcuster

The command that displays the HA (High Availability) virtual MAC address is accurately identified. When using the command "diagnose hardware deviceinfo nic <port_name>", you can retrieve detailed information about the network interface, including the virtual MAC address assigned to it in an HA setup. This is vital for troubleshooting and verifying the correct operation of the HA configuration, as the virtual MAC address is utilized by the active unit to ensure consistent network communication through failover processes. By specifying the network interface name in the command, the system provides granular information about that specific interface, allowing administrators to confirm the virtual MAC address being used, which is critical in high-availability scenarios where seamless service continuity is necessary. This ensures that even during a failover, the MAC address remains consistent for connected devices, preventing disruptions in network connectivity.

7. What ports does IKE traffic primarily use?

A. TCP 80 and 443

B. UDP 500 and UDP 4500

C. UDP 9999 and TCP 22

D. TCP 23 and 53

IKE (Internet Key Exchange) is an essential component of establishing secure communication through VPNs. It is primarily responsible for setting up the security associations and exchanging keys, which are vital for initiating a Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) tunnel. The primary ports used by IKE traffic are UDP 500 and UDP 4500. UDP 500 is specifically used for IKE phase 1, where the initial negotiation and establishment of the security parameters take place. Once the IKE negotiation is complete, and if NAT (Network Address Translation) is involved, UDP 4500 may also be used for encapsulating IKE packets to ensure they can traverse NAT devices without issues. This utilization of UDP is crucial since it is a connectionless protocol, which is ideal for the quick exchanges required for session setup, unlike TCP that requires a connection establishment handshake. Thus, understanding the specific ports used by IKE is important for configuring firewalls and ensuring proper traffic can flow for successful VPN establishment.

8. How does FortiGate determine the site rating when processing SNI?

A. By analyzing traffic patterns

B. By retrieving the FQDN

C. By performing a DNS lookup

D. By checking user history

FortiGate determines the site rating when processing Server Name Indication (SNI) primarily by retrieving the Fully Qualified Domain Name (FQDN) from the client's SSL handshake. This information is crucial because the SNI allows the client to specify the hostname it is attempting to connect to during the SSL handshake. By accessing the FQDN, FortiGate can assess the associated site rating, which helps in making informed decisions about how to manage or filter that traffic. Retrieving the FQDN is essential as it not only identifies the specific website being accessed but also allows FortiGate to apply its security policies appropriately based on the reputation and type of site. This site rating influences the actions FortiGate takes, such as whether to allow or block the traffic or enforce certain security protocols. The other options do not accurately describe the method FortiGate uses to determine the site rating in this context. Analyzing traffic patterns and checking user history can provide insights into user behavior and security risk but do not directly relate to the site rating determination. Performing a DNS lookup could be part of the broader context of understanding a domain's IP, but it is not the primary method for assessing the site rating based on SNI. Thus, retrieving the

9. What command summarizes the statuses of all the OSPF neighbors?

A. get router info ospf database self-originate

B. get router info ospf status

C. get router info ospf neighbor

D. get router info ospf interface

The command that summarizes the statuses of all the OSPF (Open Shortest Path First) neighbors is specifically designed to provide detailed information about the OSPF neighbors configured on the device. By using this command, network administrators can view the status of each OSPF neighbor, including their current state (such as FULL, 2WAY, etc.), the interfaces used for OSPF, and other critical information that helps in network troubleshooting and monitoring. This command specifically focuses on the neighbor relationships, which are crucial for OSPF operation, as the protocol relies on these adjacencies for route exchange and network topology updates. Understanding the state of OSPF neighbors is essential for ensuring optimal routing and performance across a network. The other commands listed serve different purposes and do not provide a summary of OSPF neighbor statuses. For instance, commands that deal with OSPF database or interfaces may provide information about OSPF routes or the performance of OSPF over specific interfaces but do not summarize the neighbor relationships directly.

10. Which command displays the current statistics on a HA pair?

A. get router info ospf database brief

B. diagnose sys ha status

C. diagnose sys ha dump-by vlcuster

D. get router info ospf interface

The command that displays the current statistics on a High Availability (HA) pair is "diagnose sys ha status." This command provides detailed information about the HA configuration, including the roles of the devices in the pair, their operational status, synchronization information, and other relevant statistics that help administrators monitor the health and performance of the HA setup. Using this command is crucial in a maintenance or troubleshooting scenario because it aids in understanding how well the HA devices are functioning together and if there are any issues that need to be addressed. Information obtained from this command can help in assessing whether the primary and secondary devices are synchronized, which is a critical aspect of ensuring high availability. The other commands focus on different aspects of the network: - The command that retrieves OSPF database information provides insight into OSPF routing information, which is unrelated to the HA status. - A command that dumps HA information by cluster also provides HA information but may not summarize the current operational state as directly as the "diagnose sys ha status." - The command that displays OSPF interface information is more geared towards understanding the status of OSPF-enabled interfaces rather than HA settings. Therefore, "diagnose sys ha status" is specifically designed for reviewing the current HA statistics, making it