Fortinet

Exam Questions NSE4_FGT-6.4

Fortinet NSE 4 - FortiOS 6.4

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Refer to the exhibit.

The exhibits show a network diagram and the explicit web proxy configuration.
In the commanddiagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

A. 'host 192.168.0.2 and port 8080'
B. 'host 10.0.0.50 and port 80'
C. 'host 192.168.0.1 and port 80'
D. 'host 10.0.0.50 and port 8080'

Answer: A

NEW QUESTION 2
To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. FortiManager
B. Root FortiGate
C. FortiAnalyzer
D. Downstream FortiGate

Answer: B

NEW QUESTION 3
Examine the network diagram shown in the exhibit, then answer the following question:

Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

A. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
B. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
C. 10.4.200.0/30 is directly connected, port2
D. 172.16.32.0/24 is directly connected, port1

Answer: D

NEW QUESTION 4
Which three statements about a flow-based antivirus profile are correct? (Choose three.)

A. IPS engine handles the process as a standalone.
B. FortiGate buffers the whole file but transmits to the client simultaneously.
C. If the virus is detected, the last packet is delivered to the client.
D. Optimized performance compared to proxy-based inspection.
E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

Answer: CDE

NEW QUESTION 5
Refer to the exhibit.

Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. This security fabric topology is a logical topology view.
B. There are 19 security recommendations for the security fabric.
C. There are five devices that are part of the security fabric.
D. Device detection is disabled on all FortiGate devices.

Answer: AD

NEW QUESTION 6
Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

A. FortiGate points the collector agent to use a remote LDAP server.
B. FortiGate uses the AD server as the collector agent.
C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.

D. FortiGate queries AD by using the LDAP to retrieve user group information.

Answer: CD

NEW QUESTION 7
Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
B. In flow-based inspection mod
C. FortiGate buffers the file, but also simultaneously transmits it to the client.
D. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
E. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: CD

NEW QUESTION 8
By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which two CLI commands will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering? (Choose two.)

A. set fortiguard anycast disable
B. set protocol udp
C. set webfilter-force-off disable
D. set webfilter-cache disable

Answer: AC

NEW QUESTION 9
Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

A. The public key of the web servercertificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The CA certificate that signed the web-server certificate must be installed on the browser.
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Answer: C

NEW QUESTION 10
Which type of logs on FortiGate record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs
B. Forward traffic logs
C. Local traffic logs
D. Security logs

Answer: A

NEW QUESTION 10
An administrator is running the following sniffer command:

Which three pieces of Information will be Includedin me sniffer output? {Choose three.)

A. Interface name
B. Packetpayload
C. Ethernet header
D. IP header
E. Application header

Answer: BCE

NEW QUESTION 13
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent must search security event logs.
D. The NetSessionEnum functionis user] to track user logouts.

Answer: A

NEW QUESTION 17
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
*All traffic must be routed through the primary tunnel when both tunnels are up
*The secondary tunnel must be used only if the primary tunnel goes down
*In addition, FortiGate should be able to detect a dead tunnel to speed up tunnelfailover
Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Enable Dead Peer Detection.
B. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
C. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the state route for the secondary tunnel.

Answer: A

NEW QUESTION 22
How do you format the FortiGate flash disk?

A. Load a debug FortiOS image.
B. Load the hardware test (HQIP) image.
C. Execute the CLI command execute formatlogdisk.
D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 23
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.
B. By default, the SSL VPN portal requires the installation of a client's certificate.
C. By default, split tunneling is enabled.
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 26
Refer to the exhibits.

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.
B. Change the Server IP address.
C. Change the idle-timeout.
D. Change the SSL VPN portal to the tunnel.

Answer: D

NEW QUESTION 30
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. hard-timeout
B. auth-on-demand
C. soft-timeout
D. new-session
E. Idle-timeout

Answer: ADE

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

NEW QUESTION 35
In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.
B. The Incoming Interfac
C. Outgoing Interfac
D. Schedule, and Service fields can be shared with both IPv4and IPv6.
E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
F. The IP version of the sources and destinations in a policy must match.
G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: ACE

NEW QUESTION 38
Refer to the exhibit.

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. The signature setting uses a custom rating threshold.
B. The signature setting includes a group of other signatures.
C. Traffic matching the signature will be allowed and logged.

D. Traffic matching the signature will be silently dropped and logged.

Answer: B

NEW QUESTION 42
Examine the two static routes shown in the exhibit, then answer the following question.

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.
B. FortiGate will use the port1 route as the primary candidate.
C. FortiGate will route twice as much traffic to the port2 route
D. FortiGate will only actuate the port1 route in the routing table

Answer: B

Explanation:
"If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path."

NEW QUESTION 47
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view
B. Log backups from the CLI cannot be restored to another FortiGate.
C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

NEW QUESTION 49
......

Relate Links

100% Pass Your NSE4_FGT-6.4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-6.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/