NSE4-5.4 Q&As

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Pass Fortinet NSE4-5.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/nse4-5-4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which changes to IPS will reduce resource usage and improve performance? (Choose three)

A. In custom signature, remove unnecessary keywords to reduce how far into the signature tree that FortiGate must compare in order to determine whether the packet matches.

B. In IPS sensors, disable signatures and rate based statistics (anomaly detection) for protocols, applications and traffic directions that are not relevant.

C. In IPS filters, switch from \\'Advanced\\' to \\'Basic\\' to apply only the most essential signatures.

D. In firewall policies where IPS is not needed, disable IPS.

E. In firewall policies where IPS is used, enable session start logs.

Correct Answer: ABD

QUESTION 2

Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type. Which of the following are some of the available event types in Web Config? (Select all that apply.)

A. Intrusion detected.

B. Successful firewall authentication.

C. Oversized file detected.

D. DHCP address assigned.

E. FortiGuard Web Filtering rating error detected.

Correct Answer: A

QUESTION 3

If Open Shortest Path First (OSPF) has already been configured on a FortiGate unit, which of the following statements is correct if the routes learned through OSPF need to be announced by Border Gateway Protocol (BGP)?

A. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Autonomous System Boundary Router (ASBR).

B. The FortiGate unit will automatically announce all routes learned through OSPF to its BGP peers if the FortiGate unit is configured as an OSPF Area Border Router (ABR).

C. At a minimum, the network administrator needs to enable Redistribute OSPF in the BGP settings.

D. The BGP local AS number must be the same as the OSPF area number of the routes learned that need to be redistributed into BGP.

E. By design, BGP cannot redistribute routes learned through OSPF.

Correct Answer: C

QUESTION 4

Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

A. TCP SYN packets are always handled by the NP Processor

B. The initial packets go to the NP Processor, where a decision is taken on if the session can be offloaded or not.

C. Packets for a session termination are always handled by the CPU.

D. The initial packets go to the CPU, where a decision is taken on if the session can be offloaded or not.

Correct Answer: AD

QUESTION 5

Which define device identification? (Choose two.)

A. Device identification is enabled by default on all interfaces.

B. Enabling a source device in a firewall policy enables device identification on the source interfaces of that policy.

C. You cannot combine source user and source device in the same firewall policy.

D. FortiClient can be used as an agent based device identification technique.

E. Only agentless device identification techniques are supported.

Correct Answer: BD

QUESTION 6

What is the maximum number of FortiAnalyzer/FortiManager devices a FortiGate unit can be configured to send logs to?

A. 1

B. 2

C. 3

D. 4

Correct Answer: C

QUESTION 7

Which email filter is NOT available on a FortiGate device?

A. Sender IP reputation database.

B. URLs included in the body of known SPAM messages.

C. Email addresses included in the body of known SPAM messages.

D. Spam object checksums.

E. Spam grey listing.

Correct Answer: E

QUESTION 8

Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?

A. TCP connection

B. File attachments

C. Message headers

D. Message body

Correct Answer: A

QUESTION 9

Which of the following network protocols can be used to access a FortiGate unit as an administrator?

A. HTTPS, HTTP, SSH, TELNET, PING, SNMP

B. FTP, HTTPS, NNTP, TCP, WINS

C. HTTP, NNTP, SMTP, DHCP

D. Telnet, FTP, RLOGIN, HTTP, HTTPS, DDNS

E. Telnet, UDP, NNTP, SMTP

Correct Answer: A

QUESTION 10

In the Tunnel Mode widget of the web portal, the administrator has configured an IP Pool and enabled split tunneling. Which of the following statements is true about the IP address used by the SSL VPN client?

A. The IP pool specified in the SSL-VPN Tunnel Mode Widget Options will override the IP address range defined in the SSL-VPN Settings.

B. Because split tunneling is enabled, no IP address needs to be assigned for the SSL VPN tunnel to be established.

C. The IP address range specified in SSL-VPN Settings will override the IP address range in the SSL-VPN Tunnel Mode Widget Options.

Correct Answer: A

QUESTION 11

A DLP rule with an action of Exempt has been matched against traffic passing through the FortiGate unit. Which of the following statements is correct regarding how this transaction will be handled by the FortiGate unit?

A. Any other matched DLP rules will be ignored with the exception of Archiving.

B. Future files whose characteristics match this file will bypass DLP scanning.

C. The traffic matching the DLP rule will bypass antivirus scanning.

D. The client IP address will be added to a white list.

Correct Answer: A

QUESTION 12

You have created a new administrator account, and assign it the prof_admin profile. Which is false about that account\\'s permissions?

A. It cannot upgrade or downgrade firmware.

B. It can create and assign administrator accounts to parts of its own VDOM.

C. It can reset forgotten passwords for other administrator accounts such as "admin".

D. It has a smaller permissions scope than accounts with the "super_admin" profile.

Correct Answer: A

QUESTION 13

Which statement best describes the objective of the SYN proxy feature available in SP processors?

A. Accelerate the TCP 3-way handshake

B. Collect statistics regarding traffic sessions

C. Analyze the SYN packet to decide if the new session can be offloaded to the SP processor

D. Protect against SYN flood attacks.

Correct Answer: D

QUESTION 14

Which of the following is true regarding Switch Port Mode?

A. Allows all internal ports to share the same subnet.

B. Provides separate routable interfaces for each internal port.

C. An administrator can select ports to be used as a switch.

D. Configures ports to be part of the same broadcast domain.

Correct Answer: A

QUESTION 15

Which of the following statements correctly describes how a FortiGate unit functions in Transparent mode?

A. To manage the FortiGate unit, one of the interfaces must be designated as the management interface. This interface may not be used for forwarding data.

B. An IP address is used to manage the FortiGate unit but this IP address is not associated with a specific interface.

C. The FortiGate unit must use public IP addresses on the internal and external networks.

D. The FortiGate unit uses private IP addresses on the internal network but hides them using address translation.

Correct Answer: B

QUESTION 16

Review the IPsec phase 1 configuration in the exhibit; then answer the question below.

Which statements are correct regarding this configuration? (Choose two.)

A. The remote gateway address on 10.200.3.1.

B. The local IPsec interface address is 10.200.3.1.

C. The local gateway IP is the address assigned to port1.

D. The local gateway IP address is 10.200.3.1.

Correct Answer: AC

QUESTION 17

Under the System Information widget on the dashboard, which of the following actions are available for the system configuration? (Select all that apply.)

A. Backup

B. Restore

C. Revisions

D. Export

Correct Answer: ABC

QUESTION 18

What inspections are executed by the IPS engine? (Choose three.)

A. Application control

B. Flow-based data leak prevention

C. Proxy-based antispam

D. Flow-based web filtering

E. Proxy-based antivirus

Correct Answer: ABD

QUESTION 19

Which statement concerning IPS is false?

A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.

B. One-arm topology with sniffer mode improves performance of IPS blocking.

C. IPS can detect zero-day attacks.

D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from \\'diag autoupdate version\\'

Correct Answer: D

QUESTION 20

Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The available actions for URL Filtering are Allow and Block.

B. Multiple URL Filter lists can be added to a single Web filter profile.

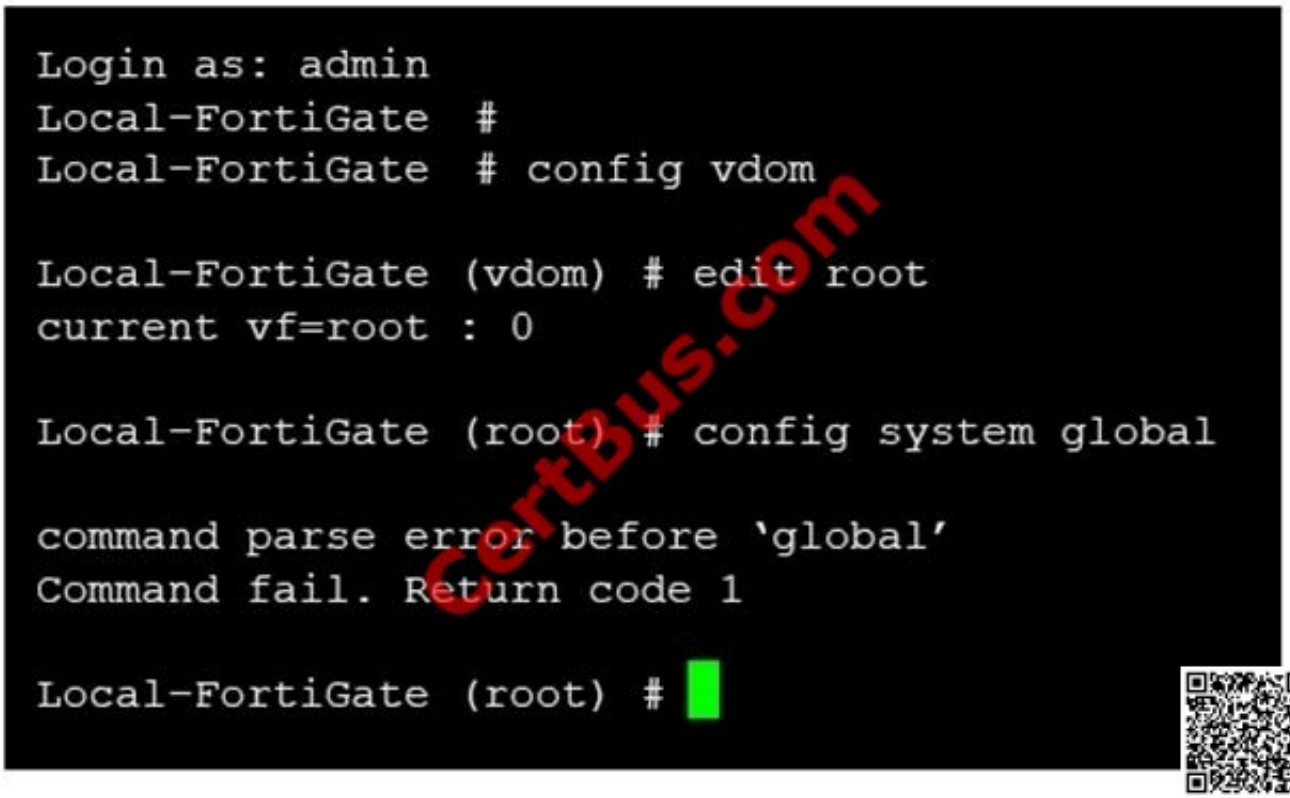
C. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.

D. The available actions for URL Filtering are Allow, Block and Exempt.

Correct Answer: D

QUESTION 21

View the exhibit.



Why is the administrator getting the error shown in the exhibit?

A. The administrator admin does not have the privileges required to configure global settings.

B. The global settings cannot be configured from the root VDOM context.

C. The command config system global does not exist in FortiGate.

D. The administrator must first enter the command edit global.

Correct Answer: A

QUESTION 22

Review the static route configuration for IPsec shown in the exhibit; then answer the question below.

Which statements are correct regarding this configuration? (Choose two.)

A. Interface remote is an IPsec interface.

B. A gateway address is not required because the interface is a point-to-point connection.

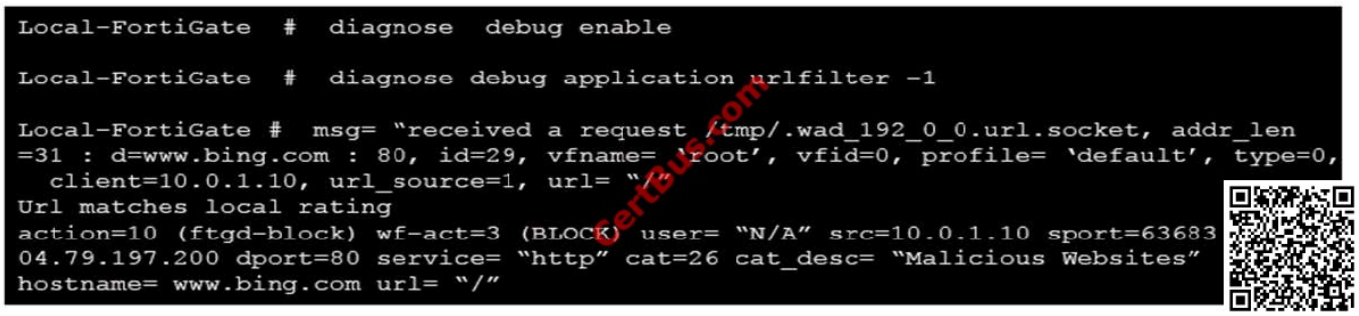
C. A gateway address is not required because the default route is used.

D. Interface remote is a zone.

Correct Answer: AB

QUESTION 23

Examine the exhibit, which shows the output of a web filtering real time debug.



Why is the site www.bing.com being blocked?

A. The web server IP address 204.79.197.200 is categorized by FortiGuard as Malicious Websites.

B. The rating for the web site www.bing.com has been locally overridden to a category that is being blocked.

C. The web site www.bing.com is categorized by FortiGuard as Malicious Websites.

D. The user has not authenticated with the FortiGate yet.

Correct Answer: A

QUESTION 24

Which statement best describes what the FortiGate hardware acceleration processors main task is?

A. Offload traffic processing tasks from the main CPU.

B. Offload management tasks from the main CPU.

C. Compress and optimize the network traffic.

D. Increase maximum bandwidth available in a FortiGate interface.

Correct Answer: A

QUESTION 25

An administrator needs to offload logging to FortiAnalyzer from a FortiGate with an internal hard drive. Which statements are true? (Choose two.)

A. Logs must be stored on FortiGate first, before transmitting to FortiAnalyzer

B. FortiGate uses port 8080 for log transmission

C. Log messages are transmitted as plain text in LZ4 compressed format (store-and-upload method).

D. FortiGate can encrypt communications using SSL encrypted OFTP traffic.

Correct Answer: AC

QUESTION 26

Which statements about an IPv6-over-IPv4 IPsec configuration are correct? (Choose two.)

A. The remote gateway IP must be an IPv6 address.

B. The source quick mode selector must be an IPv4 address.

C. The local gateway IP must an IPv4 address.

D. The destination quick mode selector must be an IPv6 address.

Correct Answer: CD

QUESTION 27

Examine the following log message attributes and select two correct statements from the list below. (Choose two.)

hostname=www.youtube.com profiletype="Webfilter_Profile" profile="default" status="passthrough" msg="URL belongs to a category with warnings enabled"

A. The traffic was blocked.

B. The user failed authentication.

C. The category action was set to warning.

D. The website was allowed

Correct Answer: CD

QUESTION 28

Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT.

B. Central NAT can be enabled or disabled from the CLI only.

C. Source NAT, using central NAT, requires at least one central SNAT policy.

D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall policy.

Correct Answer: AB

QUESTION 29

Identify the statement which correctly describes the output of the following command:

diagnose ips anomaly list

A. Lists the configured DoS policy.

B. List the real-time counters for the configured DoS policy.

C. Lists the errors captured when compiling the DoS policy.

D. Lists the IPS signature matches.

Correct Answer: B

QUESTION 30

What is longest length of time allowed on a FortiGate device for the virus scan to complete?

A. 20 seconds

B. 30 seconds

C. 45 seconds

D. 10 seconds

Correct Answer: B

QUESTION 31

Which of the following features could be used by an administrator to block FTP uploads while still allowing FTP downloads?

A. Anti-Virus File-Type Blocking

B. Data Leak Prevention

C. Network Admission Control

D. FortiClient Check

Correct Answer: B

QUESTION 32

Which of the following are operating mode supported in FortiGate devices? (Choose two)

A. Proxy

B. Transparent

C. NAT/route

D. Offline inspection

Correct Answer: BC

QUESTION 33

Which of the following settings can be configured per VDOM? (Choose three.)

A. Operating mode (NAT/route or transparent)

B. Static routes

C. Hostname

D. System time

E. Firewall Policies

Correct Answer: ABE

QUESTION 34

Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user\\'s source IP.

B. It is a hard timeout. The FortiGate removes the temporary policy for a user\\'s source IP address after this timer has expired.

C. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user\\'s source MAC.

D. It is a hard timeout. The FortiGate removes the temporary policy for a user\\'s source MAC address after this timer has expired.

Correct Answer: A

QUESTION 35

Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

A. Proxy-based

B. DNS-based

C. Flow-based

D. Man-in-the-middle.

Correct Answer: C

QUESTION 36

In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.

Which statements are correct regarding this setting? (Choose two.)

A. Interface settings on port7 will not be synchronized with other cluster members.

B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.

C. When connecting to port7 you always connect to the master device.

D. A gateway address may be configured for port7.

Correct Answer: AD

QUESTION 37

Which of the following statements correctly describes how a push update from the FortiGuard Distribution Network (FDN) works?

A. The FDN sends push updates only once.

B. The FDN sends package updates automatically to the FortiGate unit without requiring an update request.

C. The FDN continues to send push updates until the FortiGate unit sends an acknowledgement.

D. The FDN sends a message to the FortiGate unit that there is an update available and that the FortiGate unit should download the update.

Correct Answer: D

QUESTION 38

What actions are possible with Application Control? (Choose three.)

A. Warn

B. Allow

C. Block

D. Traffic Shaping

E. Quarantine

Correct Answer: BCD

QUESTION 39

Which is true about incoming and outgoing interfaces in firewall policies?

A. A physical interface may not be used.

B. A zone may not be used.

C. Multiple interfaces may not be used for both incoming and outgoing.

D. Source and destination interfaces are mandatory.

Correct Answer: D

QUESTION 40

Which of the following actions can be used with the FortiGuard quota feature? (Choose three.)

A. Allow

B. Block

C. Monitor

D. Warning

E. Authenticate

Correct Answer: CDE

NSE4-5.4 PDF Dumps NSE4-5.4 Practice Test NSE4-5.4 Study Guide

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

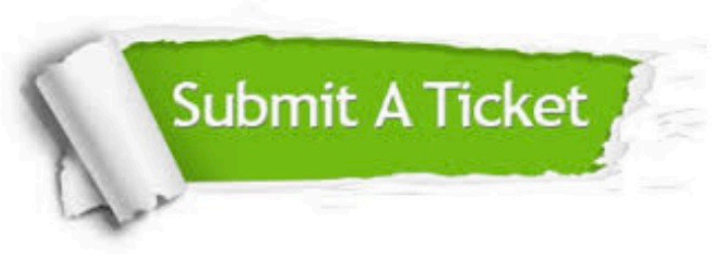
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © certbus, All Rights Reserved.