

Exam Questions NSE4_FGT-6.4

Fortinet NSE 4 - FortiOS 6.4

https://www.2passeasy.com/dumps/NSE4_FGT-6.4/



NEW QUESTION 1

What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

- A. Traffic to botnetservers
- B. Traffic to inappropriate web sites
- C. Server information disclosure attacks
- D. Credit card data leaks
- E. SQL injection attacks

Answer: ACE

NEW QUESTION 2

Which statement about the IP authentication header (AH) used by IPsec is true?

- A. AH does not provide any data integrity or encryption.
- B. AH does not support perfect forward secrecy.
- C. AH provides data integrity but no encryption.
- D. AH provides strong data integrity but weak encryption.

Answer: C

NEW QUESTION 3

If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

- A. A CRL
- B. A person
- C. A subordinate CA
- D. A root CA

Answer: D

NEW QUESTION 4

Examine this FortiGate configuration:

Examine the output of the following debug command:

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

- A. It is allowed, but with no inspection
- B. It is allowed and inspected as long as the inspection is flow based
- C. It is dropped.
- D. It is allowed and inspected, as long as the only inspection required is antivirus.

Answer: C

NEW QUESTION 5

Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

- A. Lookup is done on the first packet from the session originator
- B. Lookup is done on the last packet sent from the responder
- C. Lookup is done on every packet, regardless of direction
- D. Lookup is done on the trust reply packet from the responder

Answer: AD

NEW QUESTION 6

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 7

Refer to the exhibit.

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

- A. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs
- B. port1 is a native VLAN.
- C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- D. Traffic between port2 and port2-vlan1 is allowed by default.

Answer: CD

NEW QUESTION 8

Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

- A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
- B. To finish any inspection operations
- C. To remove the NAT operation
- D. To generate logs

Answer: B

NEW QUESTION 9

Refer to the exhibit.

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check. Which interface will be selected as an outgoing interface?

- A. port2
- B. port4
- C. port3
- D. port1

Answer: B

NEW QUESTION 10

Refer to the exhibit.

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses. How does FortiGate process the traffic sent to <http://www.fortinet.com>?

- A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
- B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
- C. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 1.
- D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Answer: D

NEW QUESTION 10

Examine the exhibit, which contains a virtual IP and firewall policy configuration.

The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port2) interface has the IP address 10.0.1.254/24. The first firewall policy has NAT enabled on the outgoing interface address. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0.1.10/24?

- A. 10.200.1.10
- B. Any available IP address in the WAN (port1) subnet 10.200.1.0/24
- C. 10.200.1.1
- D. 10.0.1.254

Answer: B

Explanation:

<https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs>.

NEW QUESTION 11

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- A. FortiCache
- B. FortiSIEM
- C. FortiAnalyzer
- D. FortiSandbox
- E. FortiCloud

Answer: BCD

NEW QUESTION 16

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 server certificate 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 18

Which two statements are true about the FGCP protocol? (Choose two.)

- A. Not used when FortiGate is in Transparent mode
- B. Elects the primary FortiGate device
- C. Runs only over the heartbeat links
- D. Is used to discover FortiGate devices in different HA groups

Answer: CD

NEW QUESTION 22

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic, in addition, the remote peer does not support a dynamic DNS update service. What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Static IP Address
- B. Dialup User
- C. Dynamic DNS
- D. Pre-shared Key

Answer: C

NEW QUESTION 25

Refer to the exhibit.

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

- A. The session is in SYN_SEXT state.
- B. The session is in FIN_ACK state.
- C. The session is in FTN_WAIT state.
- D. The session is in ESTABLISHED state.

Answer: D

NEW QUESTION 30

Refer to the exhibit.

The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode. The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem. Which two statements are true? (Choose two.)

- A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
- B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
- C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
- D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: AD

NEW QUESTION 34

An administrator has configured the following settings:

What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. A session for denied traffic is created.
- D. The number of logs generated by denied traffic is reduced.

Answer: CD

NEW QUESTION 36

Refer to the exhibits.

Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

- A. Administrators can access FortiGate only through the console port.
- B. FortiGate has entered conserve mode.
- C. FortiGate will start sending all files to FortiSandbox for inspection.
- D. Administrators cannot change the configuration.

Answer: CD

NEW QUESTION 38

Refer to the exhibit.

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

- A. Destination NAT is disabled in the firewall policy.
- B. One-to-one NAT IP pool is used in the firewall policy.
- C. Overload NAT IP pool is used in the firewall policy.
- D. Port block allocation IP pool is used in the firewall policy.

Answer: A

NEW QUESTION 41

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Answer: AC

NEW QUESTION 42

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.

Answer: AB

NEW QUESTION 43

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeou
- B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
- C. It is a hard timeou
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeou
- F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
- G. It is a hard timeou
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

Answer: A

NEW QUESTION 47

Refer to the exhibit.

Which contains a network diagram and routing table output. The Student is unable to access Webserver.
What is the cause of the problem and what is the solution for the problem?

- A. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- B. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
- C. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
- D. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

Answer: C

NEW QUESTION 51

Refer to the exhibit.

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up. but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, what configuration change will bring phase 2 up?

- A. On HQ-FortiGate,enable Auto-negotiate.
- B. On Remote-FortiGate, set Seconds to 43200.
- C. On HQ-FortiGate,enable Diffie-Hellman Group 2.
- D. On HQ-FortiGate, set Encryption to AES256.

Answer: D

NEW QUESTION 55

Refer to the web filter raw logs.

Based on the raw logs shown in the exhibit, which statement is correct?

- A. Social networking web filter category is configured with the action set to authenticate.
- B. The action on firewall policy ID 1 is set to warning.
- C. Access to the social networking web filter category was explicitly blocked to all users.
- D. The name of the firewall policy is all_users_web.

Answer: D

NEW QUESTION 59

Examine this FortiGate configuration:

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:

“What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting”

NEW QUESTION 61

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 Interface
- C. Outgoing Interface
- D. Schedule, and Service fields can be shared with both IPv4 and 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 64

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 67

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4_FGT-6.4 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT-6.4/

Money Back Guarantee

NSE4_FGT-6.4 Practice Exam Features:

- * NSE4_FGT-6.4 Questions and Answers Updated Frequently
- * NSE4_FGT-6.4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year