

NSE4_FGT-6.4 Dumps

Fortinet NSE 4 - FortiOS 6.4

https://www.certleader.com/NSE4_FGT-6.4-dumps.html



NEW QUESTION 1

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: A

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

View the exhibit.

A user behind the FortiGate is trying to go to <http://www.addictinggames.com> (Addicting Games). Based on this configuration, which statement is true?

- A. Addicting.Games is allowed based on the Application Overrides configuration.
- B. Addicting.Games is blocked on the Filter Overrides configuration.
- C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
- D. Addcting.Games is allowed based on the Categories configuration.

Answer: A

NEW QUESTION 4

NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

- A. Web filtering
- B. Antivirus
- C. Web proxy
- D. Application control

Answer: B

NEW QUESTION 5

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 6

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 7

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 8

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 9

A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface. Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

- A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
- B. The two VLAN sub interfaces must have different VLAN IDs.
- C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
- D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

Answer: B

Explanation:

FortiGate_Infrastructure_6.0_Study_Guide_v2-Online.pdf → page 147

“Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID”

NEW QUESTION 10

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 10

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 12

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

Answer: A

NEW QUESTION 14

Which of statement is true about SSL VPN web mode?

- A. The tunnel is up while the client is connected.
- B. It supports a limited number of protocols.
- C. The external network application sends data through the VPN.
- D. It assigns a virtual IP address to the client.

Answer: C

NEW QUESTION 18

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 23

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 28

An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

- A. Policy lookup will be disabled.
- B. By Sequence view will be disabled.
- C. Search option will be disabled
- D. Interface Pair view will be disabled.

Answer: A

NEW QUESTION 31

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 36

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check.

Answer: D

NEW QUESTION 37

Examine the following web filtering log.

Which statement about the log message is true?

- A. The action for the category Games is set to block.
- B. The usage quota for the IP address 10.0.1.10 has expired
- C. The name of the applied web filter profile is default.
- D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

Answer: C

NEW QUESTION 41

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 function is used to track user logouts.

Answer: A

NEW QUESTION 45

If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

- A. The Services field prevents SNAT and DNAT from being combined in the same policy.
- B. The Services field is used when you need to bundle several VIPs into VIP groups.
- C. The Services field removes the requirement to create multiple VIPs for different services.
- D. The Services field prevents multiple sources of traffic from using multiple services to connect to a single computer.

Answer: C

NEW QUESTION 49

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 51

View the exhibit:

Which the FortiGate handle web proxy traffic rue? (Choose two.)

- A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
- B. port-VLAN1 is the native VLAN for the port1 physical interface.
- C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
- D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: AC

NEW QUESTION 53

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 57

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 61

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

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

Answer: D

NEW QUESTION 64

Examine this PAC file configuration.

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

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 67

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuaid update servers
- C. Operating mode
- D. NGFW mode

Answer: AD

NEW QUESTION 68

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 70

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 73

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 75

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.

E. Captive portal is enabled in the interface.

Answer: ABC

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

NEW QUESTION 80

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4_FGT-6.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT-6.4-dumps.html