Fortinet

NSE4_FGT-6.0 Exam

Fortinet NSE 4 - FortiOS 6.0 Exam

Questions & Answers
Demo

Version: 11.0

Question: 1

What files are sent to FortiSandbox for inspection in flow-based inspection mode?

A. All suspicious files that do not have their hash value in the FortiGuard antivirus signature database.
B. All suspicious files that are above the defined oversize limit value in the protocol options.
C. All suspicious files that match patterns defined in the antivirus profile.
D. All suspicious files that are allowed to be submitted to FortiSandbox in the antivirus profile.

Answer: C

Question: 2

Which statements about a One-to-One IP pool are true? (Choose two.)

A. It is used for destination NAT.
B. It allows the fixed mapping of an internal address range to an external address range.
C. It does not use port address translation.
D. It allows the configuration of ARP replies.

Answer: C,D

Question: 3

Which of the following FortiGate configuration tasks will create a route in the policy route table? (Choose two.)

A. Static route created with a Named Address object
B. Static route created with an Internet Services object
C. SD-WAN route created for individual member interfaces
D. SD-WAN rule created to route traffic based on link latency

Answer: B,D

Question: 4

A company needs to provide SSL VPN access to two user groups. The company also needs to display different welcome messages on the SSL VPN login screen for both user groups.
What is required in the SSL VPN configuration to meet these requirements?

A. Different SSL VPN realms for each group.
B. Two separate SSL VPNs in different interfaces mapping the same ssl.root.
C. Two firewall policies with different captive portals.
D. Different virtual SSL VPN IP addresses for each group.

Answer: A

Question: 5

An administrator is investigating a report of users having intermittent issues with browsing the web. The administrator ran diagnostics and received the output shown in the exhibit.

```
# diagnose sys session stat
misc info: session_count=16 setup_rate=0 exp_count=0 clash=889
memory_tension_drop=0 ephemeral=1/16384 removeable=3
delete=0, flush=0, dev_down=16/69
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=0005e722
ids_recv=000fdc94
url_recv=00000000
av_recv=001fee47
fqdn_count=00000000
tcp reset stat: syncqf=119 acceptqf=0 no-listener=3995 data=0 ses=2 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

Examine the diagnostic output shown exhibit. Which of the following options is the most likely cause of this issue?

A. NAT port exhaustion
B. High CPU usage
C. High memory usage
D. High session timeout value

Answer: A

Question: 6

An administrator has configured central DNAT and virtual IPs. Which of the following can be selected in the firewall policy Destination field?

A. A VIP group

B. The mapped IP address object of the VIP object
C. A VIP object
D. An IP pool

Answer: C

Question: 7

An administrator needs to strengthen the security for SSL VPN access. Which of the following statements are best practices to do so? (Choose three.)

A. Configure split tunneling for content inspection.
B. Configure host restrictions by IP or MAC address.
C. Configure two-factor authentication using security certificates.
D. Configure SSL offloading to a content processor (FortiASIC).
E. Configure a client integrity check (host-check).

Answer: C,D,E

Question: 8

Which statement about FortiGuard services for FortiGate is true?

A. The web filtering database is downloaded locally on FortiGate.
B. Antivirus signatures are downloaded locally on FortiGate.
C. FortiGate downloads IPS updates using UDP port 53 or 8888.
D. FortiAnalyzer can be configured as a local FDN to provide antivirus and IPS updates.

Answer: B

Question: 9

Which of the following route attributes must be equal for static routes to be eligible for equal cost multipath (ECMP) routing? (Choose two.)

A. Priority
B. Metric
C. Distance
D. Cost

Answer: A,C

Question: 10

View the exhibit.

```
Local-FortiGate # diagnose sys ha checksum cluster

================== FGVM010000058290 ==================

is_manage_master()=1, is_root_master()=1
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 42 a9 7d
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 13 c1 35

================== FGVM010000058289 ==================

is_manage_master()=0, is_root_master()=0
debugzone
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43

checksum
global: 85 26 52 f2 f9 6e 3c c9 f5 21 1a 78 69 b6 20 bd
root: 30 51 63 1b 2d ef 77 aa f7 50 00 25 4d 8a 55 8b
all: 38 28 3d e4 24 8f 5b 10 8a 64 30 f2 34 dc 9a 43
```

Based on this output, which statements are correct? (Choose two.)

A. The all VDOM is not synchronized between the primary and secondary FortiGate devices.
B. The root VDOM is not synchronized between the primary and secondary FortiGate devices.
C. The global configuration is synchronized between the primary and secondary FortiGate devices.
D. The FortiGate devices have three VDOMs.

Answer: B,C

Question: 11

Which statement is true regarding the policy ID number of a firewall policy?

A. Defines the order in which rules are processed.
B. Represents the number of objects used in the firewall policy.
C. Required to modify a firewall policy using the CLI.
D. Changes when firewall policies are reordered.

Answer: C

Question: 12

An administrator wants to block HTTP uploads. Examine the exhibit, which contains the proxy address created for that purpose.

Edit Address

Category	Address	Proxy Address

Name: Training

Color: Change

Type: HTTP Method

Host: all

Request Method:
GET
HEAD
OPTIONS
POST

Show in Address List: ⬤

Comments: 0/255

Tags

⊕ Add Tag Category

OK   Cancel

Where must the proxy address be used?

A. As the source in a firewall policy.
B. As the source in a proxy policy.
C. As the destination in a firewall policy.
D. As the destination in a proxy policy.

Answer: B