QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Fortinet

NSE4-5-4

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

QUESTION: 102
Examine the following web filtering log.

```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

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: D

QUESTION: 103
View the exhibit.

```
#diagnose hardware sysinfo shm

SHM COUNTER:           10316
SHM allocated:     617643792
SHM total:        1572380672
conserve mode:    on-mem
system last entered: Fri Jun 3 10:16:39    2016
sys fd last entered:   n/a
SHM FS total:     1607806976
SHM FS free:       990134272
SHM FS avail:      990134272
SHM FS alloc:      617672704
```

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

A. FortiGate generated an event log for system conserve mode.
B. FortiGate has entered in to system conserve mode.
C. By default, the FortiGate blocks new sessions.
D. FortiGate changed the global av-failopen settings to idledrop.

Answer: B, C

QUESTION: 104
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
```

Which statements are correct, based on this output? (Choose two.)

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

Answer: A, C

QUESTION: 105
View the example routing table.

```
S*    0.0.0.0/0 [10/0] via 172.20.121.2, port1
C     172.20.121.0/24 is directly connected, port1
C     172.20.168.0/24 is directly connected, port2
C     172.20.167.0/24 is directly connected, port3
S     10.20.30.0/26 [10/0] via 172.20.168.254, port2
S     10.20.30.0/24 [10/0] via 172.20.167.254, port3
```

Which route will be selected when trying to reach 10.20.30.254?

A. 10.20.30.0/26 [10/0] via 172.20.168.254, port2
B. The traffic will be dropped because it cannot be routed.
C. 10.20.30.0/24 [10/0] via 172.20.167.254, port3
D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1

Answer: C

QUESTION: 106
Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
 if (shExpMatch (url, "*.fortinet.com/*")) {
    return "DIRECT";}
 if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
    return "PROXY" altproxy.corp.com: 8060";}
 return "PROXY proxy.corp.com: 8090";
}
```

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: A, D

QUESTION: 107
An administrator wants to configure a FortiGate as a DNS server.
The FortiGate must use its DNS database first, and then relay all irresolvable queries to an external DNS server. Which of the following DNS method must you use?

A. Non-recursive
B. Recursive
C. Forward to primary and secondary DNS
D. Forward to system DNS

Answer: B

QUESTION: 108
You are tasked to architect a new IPsec deployment with the following criteria:
- There are two HQ sites that all satellite offices must connect to.
- The satellite offices do not need to communicate directly with other satellite offices.
- No dynamic routing will be used.
- The design should minimize the number of tunnels being configured. Which topology should be used to satisfy all of the requirements?

A. Redundant
B. Hub-and-spoke
C. Partial mesh
D. Fully meshed

Answer: B

QUESTION: 109
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.

D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: A, C

QUESTION: 110
An administrator has disabled Accept push updates under Antivirus & IPS Updates. Which statements is true when this setting is disabled?

A. The extreme database is disabled.
B. New AV definitions are not added to FortiGate as soon as they are releases by FortiGuard.
C. Administrators cannot manually upload new AV definitions to the FortiGate.
D. FortiGate does not send files to FortiSandbox for inspection.

Answer: B

QUESTION: 111
An administrator wants to create a policy-based IPsec VPN tunnel between two FortiGate devices. Which configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Define the phase 2 parameters.
B. Set the phase 2 encapsulation method to transport mode.
C. Define at least one firewall policy, with the action set to IPsec.
D. Define a route to the remote network over the IPsec tunnel.
E. Define the phase 1 parameters, without enabling IPsec interface mode.

Answer: A, C, E

QUESTION: 112
An administrator has blocked Netflix login in a cloud access security inspection (CASI) profile. The administrator has also applied the CASI profile to a firewall policy. What else is required for the CASI profile to work properly?

A. You must enable logging for security events on the firewall policy.
B. You must activate a FortiCloud account.
C. You must apply an application control profile to the firewall policy.
D. You must enable SSL inspection on the firewall policy.

Answer: D

For More exams visit https://killexams.com

Kill your exam at First Attempt....Guaranteed!