

Exam Number : FCNSP

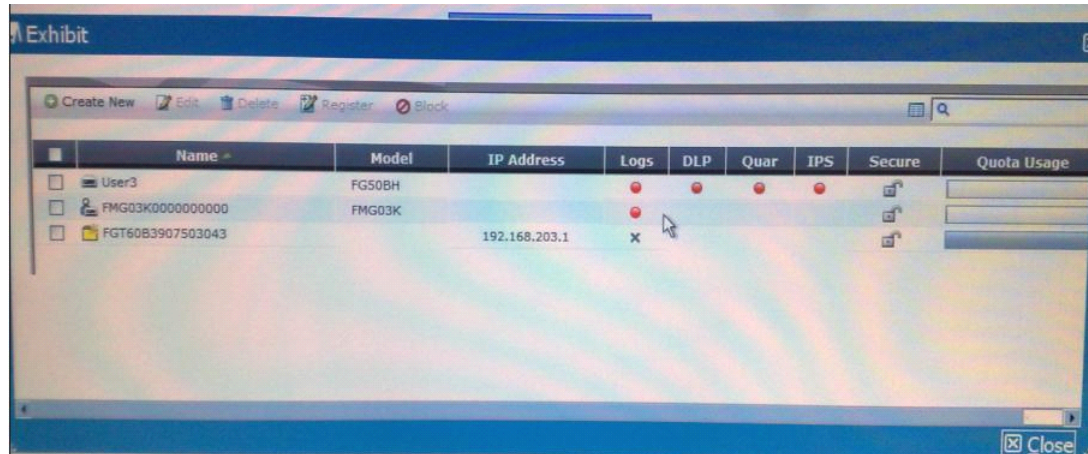
Exam Name : FortiOS 4.0 GA,
FortiAnalyzer 4.0
GA(FCNSP v4.0)

Version : Demo

<http://www.it-exams.com>

QUESTION NO: 1

A portion of the device listing for a Forti Analyzer unit is displayed in the exhibit.



Name	Model	IP Address	Logs	DLP	Quar	IPS	Secure	Quota Usage
User3	FG50BH							
FMG03K0000000000	FMG03K							
FGT60B3907503043		192.168.203.1	x					

Which of the following statements best describes the reason why the FortiGate 60B unit is unable to archive data to the Fortianalyzer unit?

- A. the FortiGate unit is considered an unregistered device.
- B. the Forti gate unit has been blocked from sending archive data to the Fortianalyzer device by the administrator.
- C. the Fortigate unit has insufficient privileges. The administrator should edit the device entry in the fortianalyzer and modify the privileges.
- D. the Fortigate unit is being treated as a syslog device and is only permitted to send log data.

Answer: A

QUESTION NO: 2

Which of the following describes the difference between the ban and quarantine actions?

- A. A ban action prevents future transactions using the same protocol which triggered the ban. A quarantine action blocks all future transactions, regardless of the protocol.
- B. A ban action blocks the transaction. A quarantine action archives the data.

C. A ban action has a finite duration. A quarantine action must be removed by an administrator,

D. A ban action is used for known users. A quarantine action is used for unknown users.

Answer: A

QUESTION NO: 3

Which of the following is an advantage of using SNMP v3 Instead of SNMP v1/v2 when querying the FortiGate unit?

A. Packet encryption

B. MIB-based report uploads

C. SNMP access limits through access lists

D. Running SNMP service on a non-standard port is possible

Answer: A

QUESTION NO: 4

An administrator has formed a High Availability cluster involving two FortiGate 310B units.

[Multiple ipstream Layer 2 switches] - [FortiGate HA Cluster] - [Multiple downstream Layer 2 switches]

The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this duster.

Which of the following options describes the best step the administrator can take?

The administrator should...

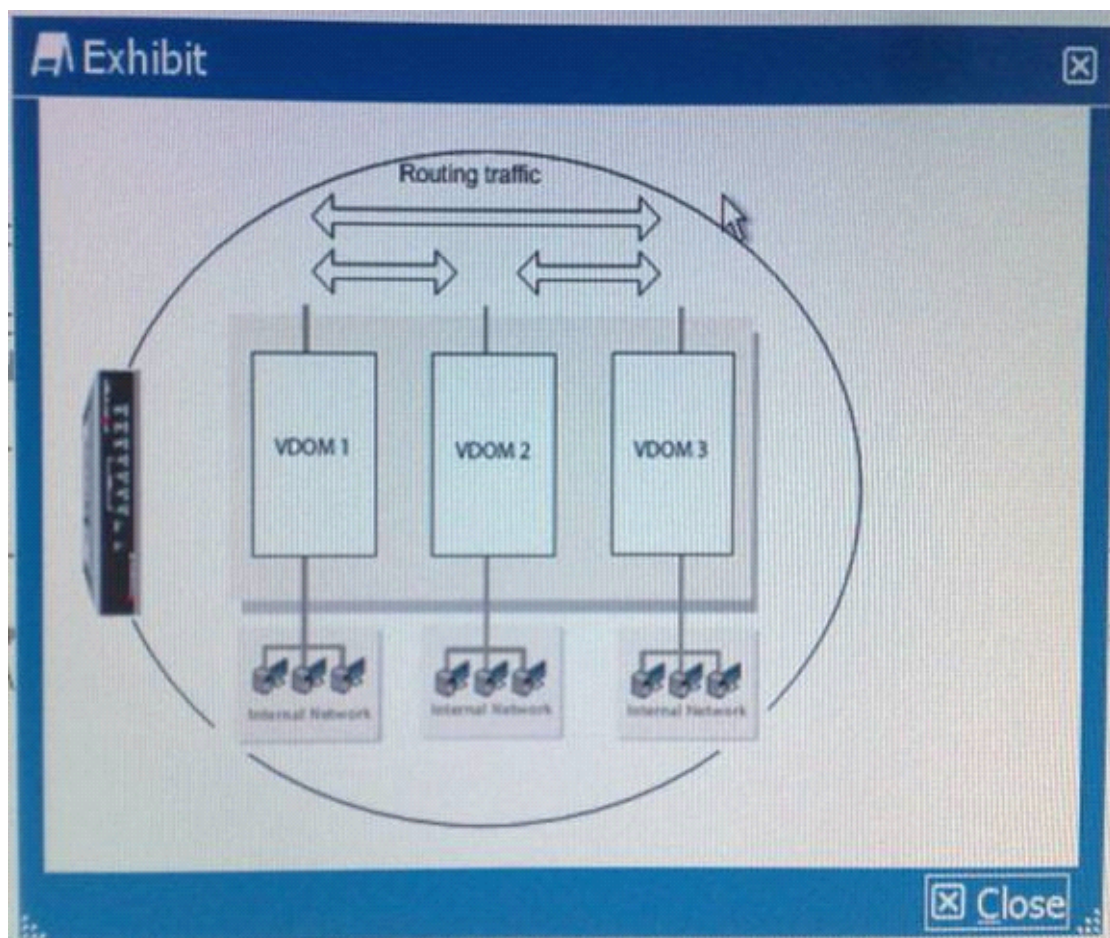
A. setup a full-mesh design which uses redundant interfaces.

- B. increase the number of FortiGate units in the cluster and configure HA in Active-Active mode.
- C. enables monitoring of all active interfaces.
- D. configure the HA ping server feature to allow for HA failover in the event that a path is Disrupted.

Answer: D

QUESTION NO: 5

FortiGate unit is configured with three Virtual Domains (VDMs) as illustrated in the exhibit.



Which of the following statements are true if the network administrator wants to route traffic between all the VDMs? (Select all that apply.)

- A. The administrator should configure inter-VDOM links to avoid using external interfaces and routers.
- B. As with all FortiGate unit interfaces, firewall policies must be in place for traffic to be allowed to pass through any interface, including inter-VDOM links. This provides the same level of security internally as externally.
- C. This configuration requires the use of an external router.
- D. Inter-VDOM routing is automatically provided if all the subnets that need to be routed are locally attached. As each VDOM has an independent routing table, routing rules need to be set (for example, static routing, OSPF) in each VDOM to route traffic between VDOMs.

Answer: A,B

QUESTION NO: 6

The `diag sys session list` command is executed in the CLI. The output of this command is shown in the exhibit.

```
Exhibit
session info: proto=6 proto_state=11 duration=539 expire=3571 timeout=3600
flags=00000000 sockflag=00000000 sockport=80 av_idx=0 use=5
origin-shaper=guarantee-100kbps prio=1 guarantee 12288/sec max 134217728/sec
traffic 123/sec
reply-shaper=low-priority prio=3 guarantee 0/sec max 134217728/sec traffic 115/sec
per_ip_shaper=
ha_id=0 hakey=1335
policy_dir=0 tunnel=/
state=redir local may_dirty ndr os rs rem
statistic(bytes/packets/allow_err): org=3201/59/1 reply=2672/58/1 tuples=3
origin->sink: org pre->post, reply pre->post dev=9->3/3->9
gwy=76.27.192.1/192.168.203.2
hook=post dir=org act=snat 192.168.203.2:3196-
>128.100.58.53:80(76.27.195.147:58618)
hook=pre dir=reply act=dnat 128.100.58.53:80-
>76.27.195.147:58618(192.168.203.2:3196)
hook=post dir=reply act=noop 128.100.58.53:80->192.168.203.2:3196(0.0.0.0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=10 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00115cae tos=ffff app_list=2000 app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=192.168.203.2, bps=1351
```

Based on the output from this command, which of the following statements is correct?

- A. This is a UDP session.
- B. Traffic shaping is being applied to this session.
- C. This is an ICMP session.
- D. This traffic has been authenticated
- E. This session matches a firewall policy with ID 5.

Answer: B

QUESTION NO: 7

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 EXP 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.

Answer: A

QUESTION NO: 8

Which of the following statements are correct regarding the configuration of a FortiGate unit as an SSL VPN gateway? (Select all that apply.)

- A. Tunnel mode can only be used if the SSL VPN user groups have at least one Host Check option enabled.
- B. The specific routes needed to access internal resources through an SSL VPN connection in tunnel mode from the client computer are defined in the routing widget associated with the SSL VPN portal.
- C. In order to apply a portal to a user, that user must belong to an SSL VPN user group.
- D. The portal settings specify whether the connection will operate in web-only or tunnel mode.

Answer: C,D

QUESTION NO: 9

Which of the following items are considered to be advantages of using the application control features on the FortiGate unit?

Implication control allows an administrator to:

- A. set a unique session-ttl for select applications.
- B. customizes application types in a similar way to adding custom IPS

signatures.

C. check, which applications are installed on workstations attempting to access the network.

D. enables AV seaming per application rather than per policy.

Answer: A

QUESTION NO: 10

Which of the following statements is not correct regarding virtual domains (VDMs)?

A. VDMs divide a single FortiGate unit two or more virtual units that function as multiple, independent units.

B. A management VDM handles SNMP, logging, alert email, and FDN-based updates.

C. A backup management VDM will synchronize the configuration from an active management VDM.

D. VDMs share firmware versions, as well as antivirus and IPS databases.

E. Only administrative users with a super_admin profile will be able to enter all VDMs to make configuration changes.

Answer: C

QUESTION NO: 11

A FortiGate unit is operating in NAT/Route mode and is configured with two Virtual LAN (VLAN) sub-interfaces added to the same physical interface.

Which of the following statements is correct regarding the VLAN IDs in this scenario?

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 if they are connected to different L2 IEEE 802.1Q compliant switches.

Answer: B

QUESTION NO: 12

A FortiClient fails to establish a VPN tunnel with a FortiGate unit.

The following information is displayed in the FortiGate unit logs:

```
msg="Initiator: sent 192.168.11.101 main mode message #1 (OK)"
```

```
msg="Initiator: sent 192.168.11.101 main mode message #2 (OK)"
```

```
msg="Initiator: sent 192.168.11.101 main mode message #3 (OK)"
```

```
msg="Initiator: parsed 192.168.11.101 main mode message #3 (DONE)"
```

```
msg="Initiator: sent 192.168.11.101 quick mode message #1 (OK)"
```

```
msg="Initiator: tunnel 192.168.1.1/192.168.11.101 install ipsec sa"
```

```
msg="Initiator: sent 192.168.11.101 quick mode message #2 (DONE)"
```

```
msg="Initiator: tunnel 192.168.11.101, transform=ESP_3DES, HMAC_MD5"
```

```
msg="Failed to acquire an IP address"
```

Which of the following statements is a possible cause for the failure to establish the VPN tunnel?

A. an IPsec DHCP server is not enabled on the external interface of the FortiGate unit.

B. There is no IPsec firewall policy configured for the policy-based VPN.

C. There is a mismatch between the FortiGate unit and the FortiClient IP addresses in the phase 2 settings.

D. The phase 1 configuration on the FortiGate unit uses Aggressive mode

while FortiClient uses Main mode.

Answer: C

QUESTION NO: 13

The Host Check feature can be enabled on the FortiGate unit for SSL VPN connections. When this feature is enabled, the FortiGate unit probes the remote host compute" to verify that it is "safe" before access is granted.

Which of the following items is NOT an option as part of the Host Check feature?

- A. FortiClient Antivirus software
- B. Microsoft Windows Firewall software
- C. FortiClient Firewall software
- D. Third-party Antivirus software

Answer: B

QUESTION NO: 14

A static route is configured for a FortiGate unit from the CLI using the following commands:

```
config router static
edit 1
set device "wanl"
set distance 20
set gateway 192.168.100.1
next
end
```

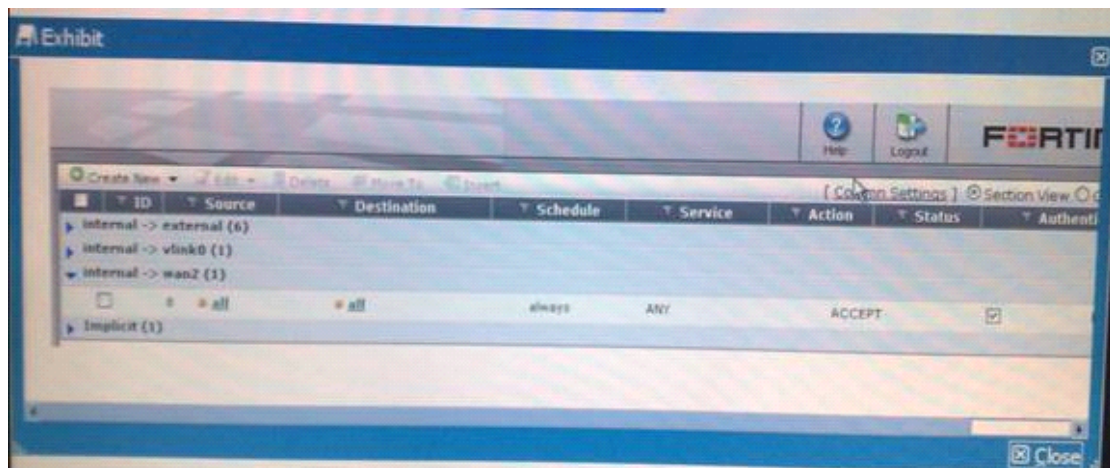
Which of the following conditions is NOT required for this static default route to be displayed in the FortiGate unit's routing table?

- A. The Administrative Status of the wan1 interface is displayed as up.
- B. the Link Status of the wan1 Interface is displayed as up.
- C. All other default routes should have an equal or higher distance.
- D. You must disable DHCP client on that interface.

Answer: D

QUESTION NO: 15

Refer to the Exhibit:



Which of the following statements is correct based on the firewall configuration illustrated in the exhibit?

- A. A user can access the Internet using only the protocols that are supported by user authentication.
- B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.

These require authentication before the user will be allowed access.

- C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.¹
- D. A user cannot access the Internet using any protocols unless the user has passed firewall Authentication.

Answer: D

QUESTION NO: 16

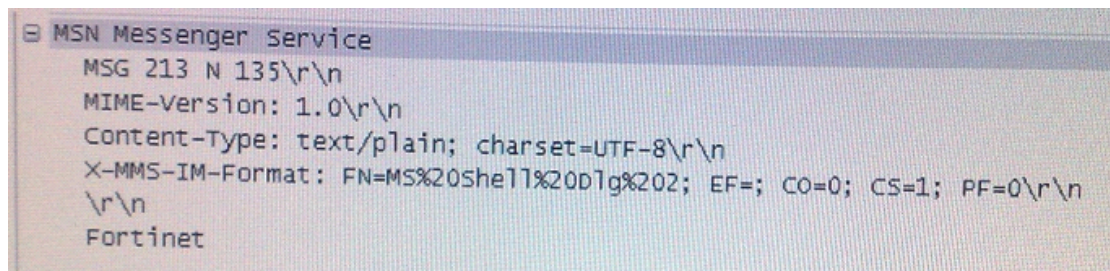
Which of the following features could be used by an administrator to block FTP uploads while still allowing FTP downloads?

- A. Anti-Virus File-Type Blocking
- B. Data Leak Prevention
- C. Network Admission Control
- D. FortiClient Check

Answer: B

QUESTION NO: 17

Which of the following describes the best custom signature for detecting the use of the word 'Fortinet' in chat applications?



```
MSN Messenger Service
MSG 213 N 135\r\n
MIME-Version: 1.0\r\n
Content-Type: text/plain; charset=UTF-8\r\n
X-MMS-IM-Format: FN=MS%20Shell%20Dlg%20; EF=; CO=0; CS=1; PF=0\r\n
\r\n
Fortinet
```

The sample packet trace illustrated in the exhibit provides detail on the packet that requires detection.

- A. F-SBID(-protocol top; -flow from .client; -pattern "X-MMS-IM-Format"; -pattern "fortinet; - no_case;)
- B. F-SB1D(--protocol tcp; --flow from_client; --pattern "fortinet"; --no.case;)
- C. F-SBID "Protocol tcp; -flow from.client; -pattern "X-MMS-IM-Format"; -pattern "fartinet"; -within 20; --no.case;)
- D. F-SBID(--protocol tcp; -flow from.client; -pattern "X-MMS-IM-Format";

-pattern "fortinet"; within 20;)

Answer: A

QUESTION NO: 18

An administrator sets up a new FTP server on TCP port 2121. A FortiGate unit is located between the FTP clients and the server, the administrator has created a policy for TCP port 2121.

Users have been complaining that when downloading data they receive a 200 Port command successful message followed by a 425 cannot build data connection message.

Which of the following statements represents the best solution to this problem?

- A. Create a new session helper for the FTP service monitoring port 2121.
- B. Enable the ANY service in the firewall policies for both incoming and outgoing traffic.
- C. Place the client and server interface in the same zone and enable intra-zone traffic.
- D. Disable any protection profiles being applied to FTP traffic.

Answer: A

QUESTION NO: 19

Which of the following represents the method used on a FortiGate unit running FortiOS version 4.2 to apply traffic shaping to P2P traffic, such as BitTorrent?

- A. Apply a Traffic Shaper to a BitTorrent entry in an Application Control List.
- B. enable the Shape option in a Firewall policy with a Service set to BitTorrent.
- C. Define a DLP Rule to match against BitTorrent traffic and include the rule in a DLP Sensor with Traffic Shaping enabled.

D. Specify the amount of Rate Limiting to be applied to BitTorrent traffic through the P2P settings of the Firewall Policy Protocol Options.

Answer: A

QUESTION NO: 20

Which of the following DLP actions will always be performed if it is selected?

- A. Archive
- B. Quarantine Interface
- C. Ban Sender
- D. Block
- E. None
- F. Ban
- G. Quarantine IP Address

Answer: A