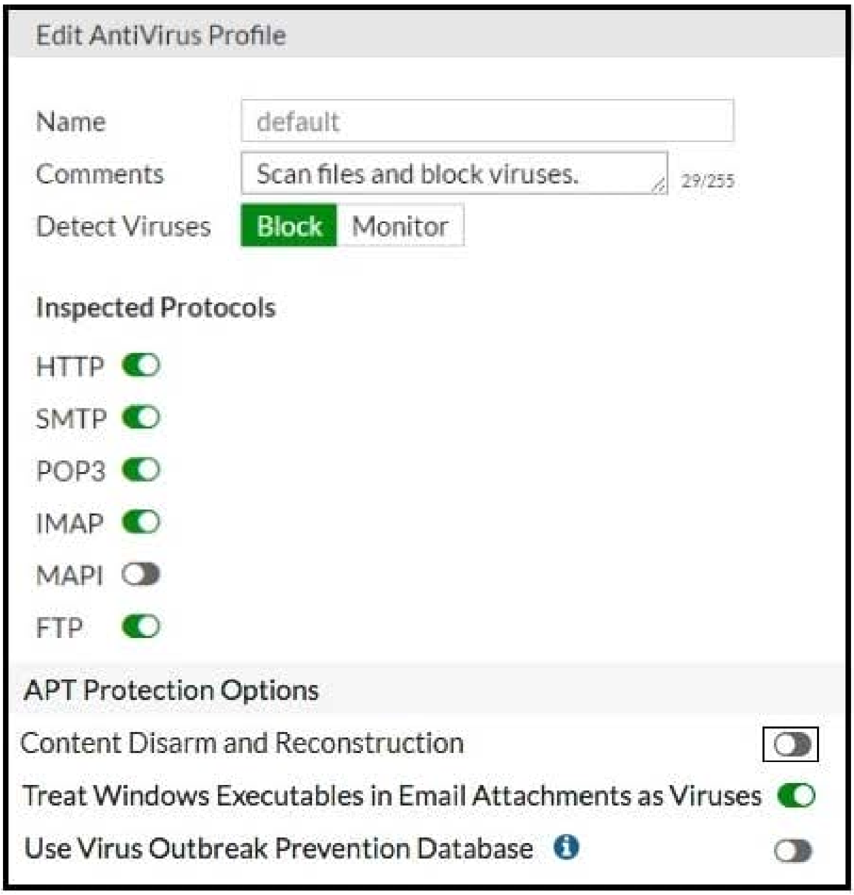
NSE4_FGT-6.2 Q&As

Fortinet NSE 4 - FortiOS 6.2

QUESTION 1

Refer to the following exhibit.



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

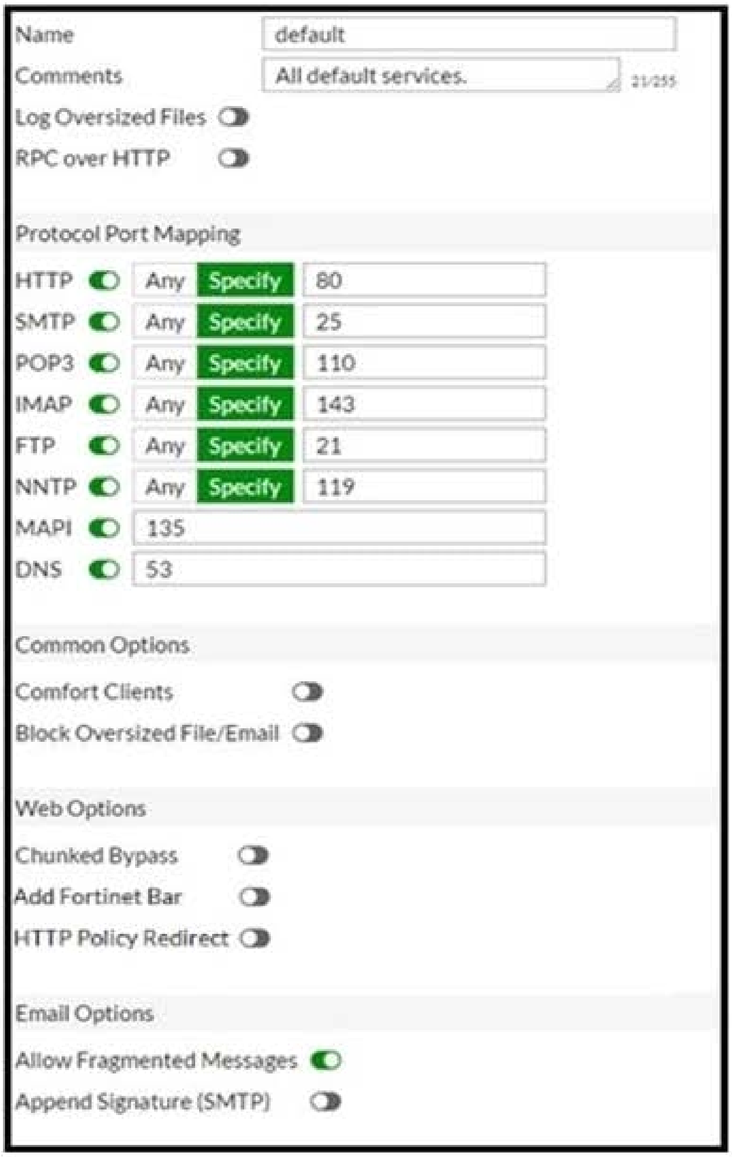
Detect Viruses: [✓ Block] Monitor

Inspected Protocols

- HTTP: on
- SMTP: on
- POP3: on
- IMAP: on
- MAPI: off
- FTP: on

APT Protection Options

- Content Disarm and Reconstruction: off
- Treat Windows Executables in Email Attachments as Viruses: on
- Use Virus Outbreak Prevention Database: off



Name	default
Comments	All default services. 21/255
Log Oversized Files	○
RPC over HTTP	○

Protocol Port Mapping

HTTP	●	Any [✓ Specify]	80
SMTP	●	Any [✓ Specify]	25
POP3	●	Any [✓ Specify]	110
IMAP	●	Any [✓ Specify]	143
FTP	●	Any [✓ Specify]	21
NNTP	●	Any [✓ Specify]	119
MAPI	●	135	
DNS	●	53	

Common Options

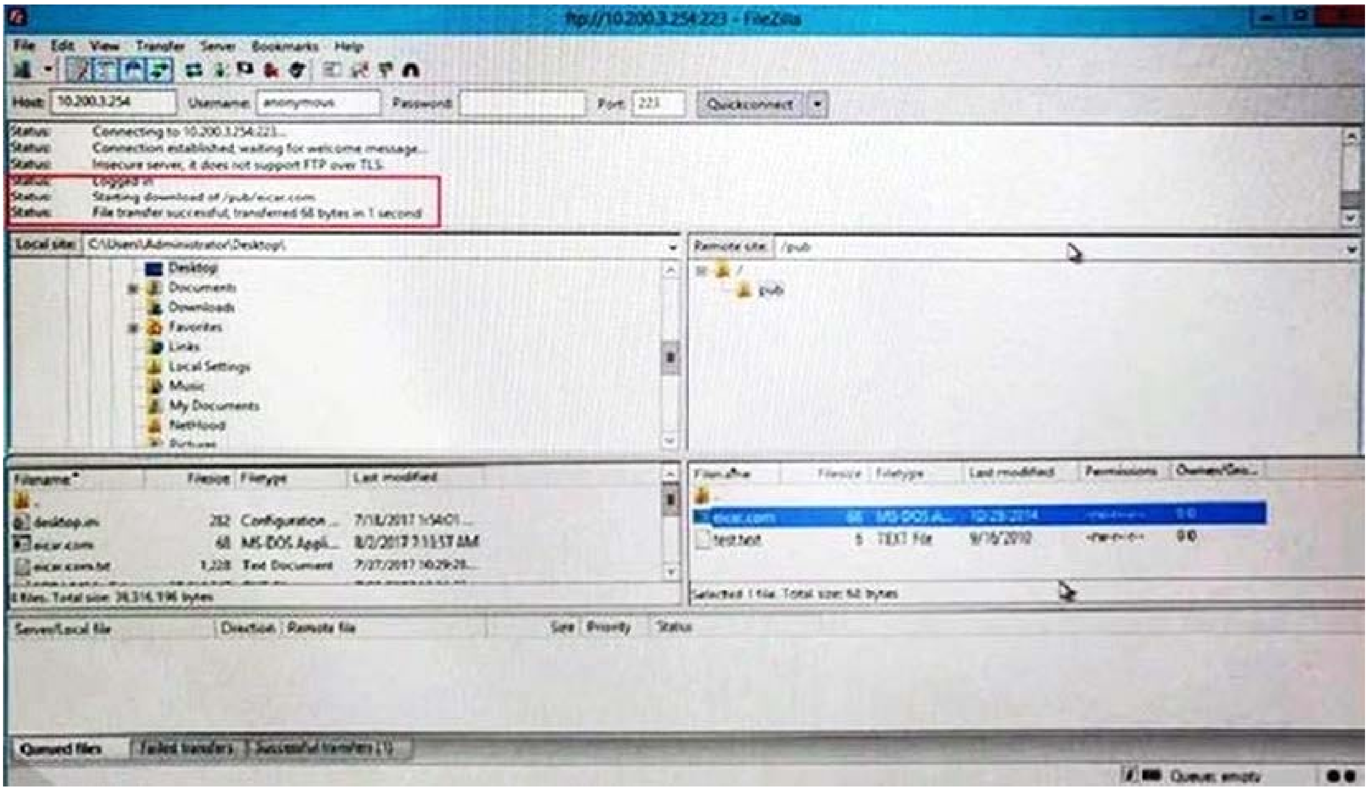
Comfort Clients	○
Block Oversized File/Email	○

Web Options

Chunked Bypass	○
Add Fortinet Bar	○
HTTP Policy Redirect	○

Email Options

Allow Fragmented Messages	●
Append Signature (SMTP)	○



Host: 10.200.3.254 Username: anonymous Password: Port: 223

```
Status:    Connecting to 10.200.3.254:223...
Status:    Connection established, waiting for welcome message...
Status:    Insecure server, it does not support FTP over TLS.
Status:    Logged in
Status:    Starting download of /pub/eicar.com
Status:    File transfer successful, transferred 68 bytes in 1 second
```

Local site: C:\Users\Administrator\Desktop\

Remote site: /pub

Filename	Filesize	Filetype	Last modified
..			
desktop.ini	282	Configuration ...	7/18/2017 1:54:01...
eicar.com	68	MS-DOS Appli...	8/2/2017 7:13:57 AM
eicar.com.txt	1,228	Text Document	7/27/2017 10:29:28...

8 files. Total size: 38,316,196 bytes

Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gro...
..					
eicar.com	68	MS-DOS A...	10/29/2014	-rw-r--r--	0 0
test.txt	5	TEXT File	9/16/2010	-rw-r--r--	0 0

Selected 1 file. Total size: 68 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status

Why is FortiGate not blocking the test file over FTP download?

A. Deep-inspection must be enabled for FortiGate to fully scan FTP traffic.

B. FortiGate needs to be operating in flow-based inspection mode in order to scan FTP traffic.

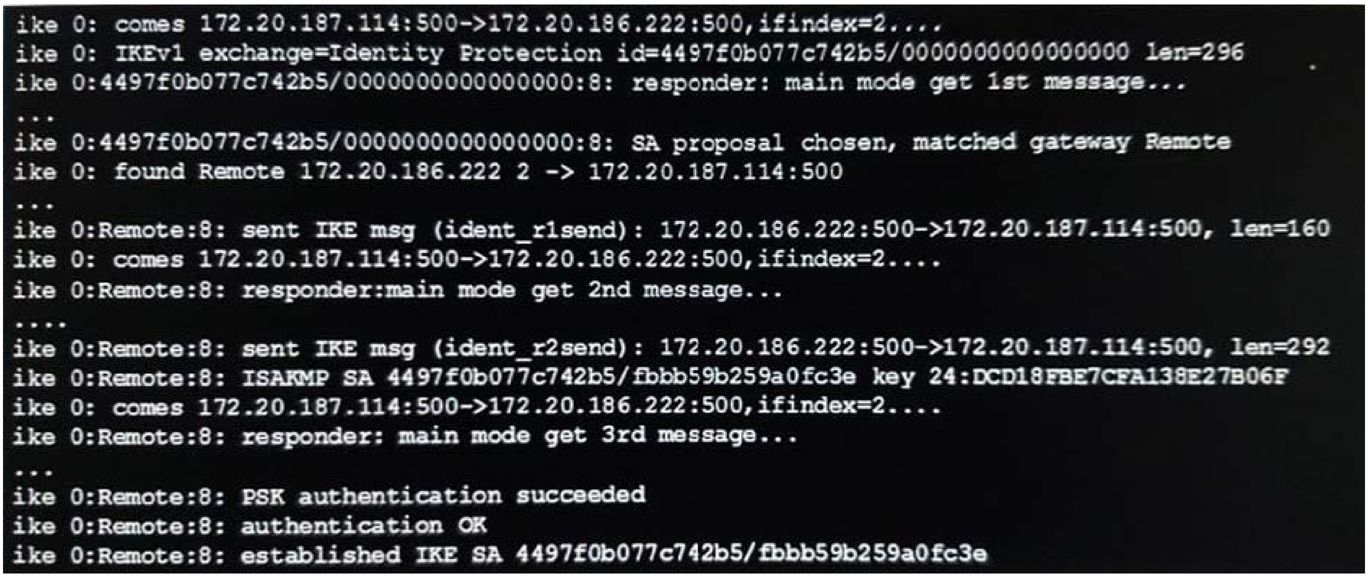
C. The FortiSandbox signature database is required to successfully scan FTP traffic.

D. The proxy options profile needs to scan FTP traffic on a non-standard port.

Correct Answer: D

QUESTION 2

Examine the exhibit, which shows the partial output of an IKE real-time debug.



```
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=4497f0b077c742b5/0000000000000000 len=296
ike 0:4497f0b077c742b5/0000000000000000:8: responder: main mode get 1st message...
...
ike 0:4497f0b077c742b5/0000000000000000:8: SA proposal chosen, matched gateway Remote
ike 0: found Remote 172.20.186.222 2 -> 172.20.187.114:500
...
ike 0:Remote:8: sent IKE msg (ident_r1send): 172.20.186.222:500->172.20.187.114:500, len=160
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder:main mode get 2nd message...
....
ike 0:Remote:8: sent IKE msg (ident_r2send): 172.20.186.222:500->172.20.187.114:500, len=292
ike 0:Remote:8: ISAKMP SA 4497f0b077c742b5/fbbb59b259a0fc3e key 24:DCD18FBE7CFA138E27B06F
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder: main mode get 3rd message...
...
ike 0:Remote:8: PSK authentication succeeded
ike 0:Remote:8: authentication OK
ike 0:Remote:8: established IKE SA 4497f0b077c742b5/fbbb59b259a0fc3e
```

Which of the following statement about the output is true?

A. The VPN is configured to use pre-shared key authentication.

B. Extended authentication (XAuth) was successful.

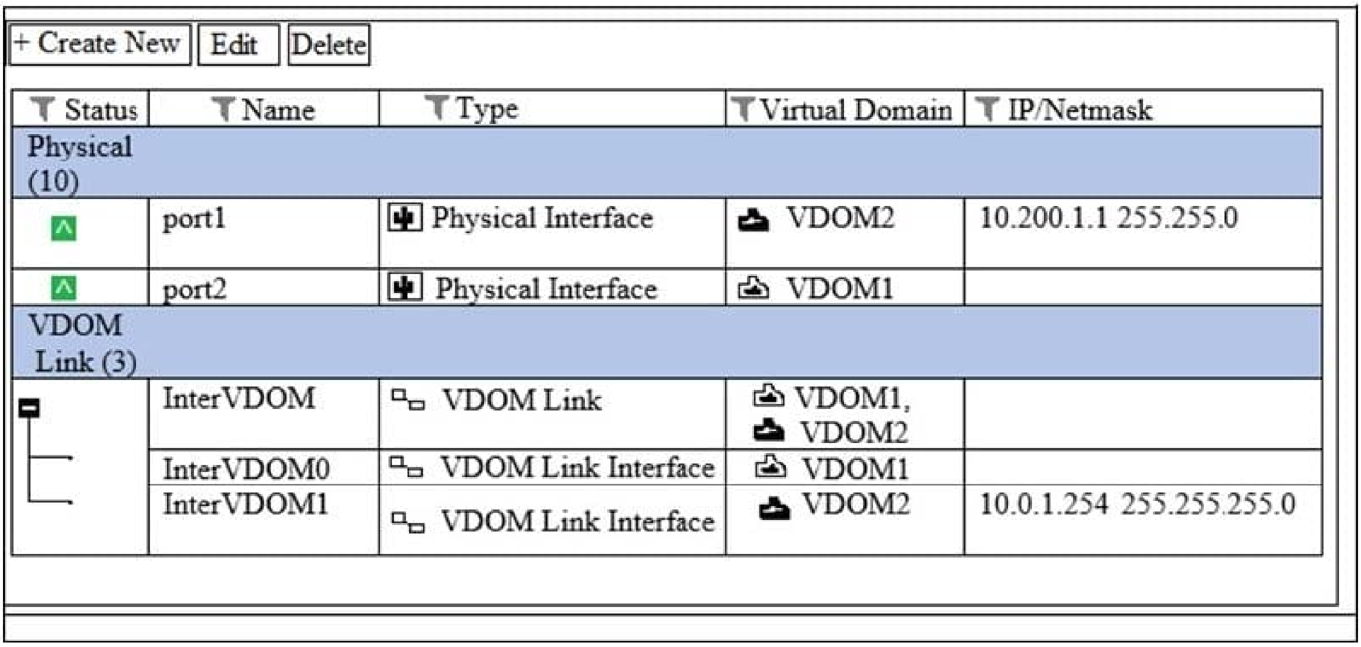
C. Remote is the host name of the remote IPsec peer.

D. Phase 1 went down.

Correct Answer: A

QUESTION 3

View the exhibit.



Status	Name	Type	Virtual Domain	IP/Netmask
Physical (10)				
🟩	port1	Physical Interface	VDOM2	10.200.1.1 255.255.0
🟩	port2	Physical Interface	VDOM1	
VDOM Link (3)				
⊟	InterVDOM	VDOM Link	VDOM1, VDOM2	
	InterVDOM0	VDOM Link Interface	VDOM1	
	InterVDOM1	VDOM Link Interface	VDOM2	10.0.1.254 255.255.255.0

VDOM1 is operating in transparent mode VDOM2 is operating in NAT Route mode. There is an inteface VDOM link between both VDOMs. A client workstation with the IP address 10.0.1.10/24 is connected to port2. A web server with the IP address 10.200.1.2/24 is connected to port1. What is required in the FortiGate configuration to route and allow connections from the client workstation to the web server? (Choose two.)

A. A static or dynamic route in VDOM2 with the subnet 10.0.1.0/24 as the destination.

B. A static or dynamic route in VDOM1 with the subnet 10.200.1.0/24 as the destination.

C. One firewall policy in VDOM1 with port2 as the source interface and InterVDOM0 as the destination interface.

D. One firewall policy in VDOM2 with InterVDOM1 as the source interface and port1 as the destination interface.

Correct Answer: C

QUESTION 4

Which action can be applied to each filter in the application control profile?

A. Block, monitor, warning, and quarantine

B. Allow, monitor, block and learn

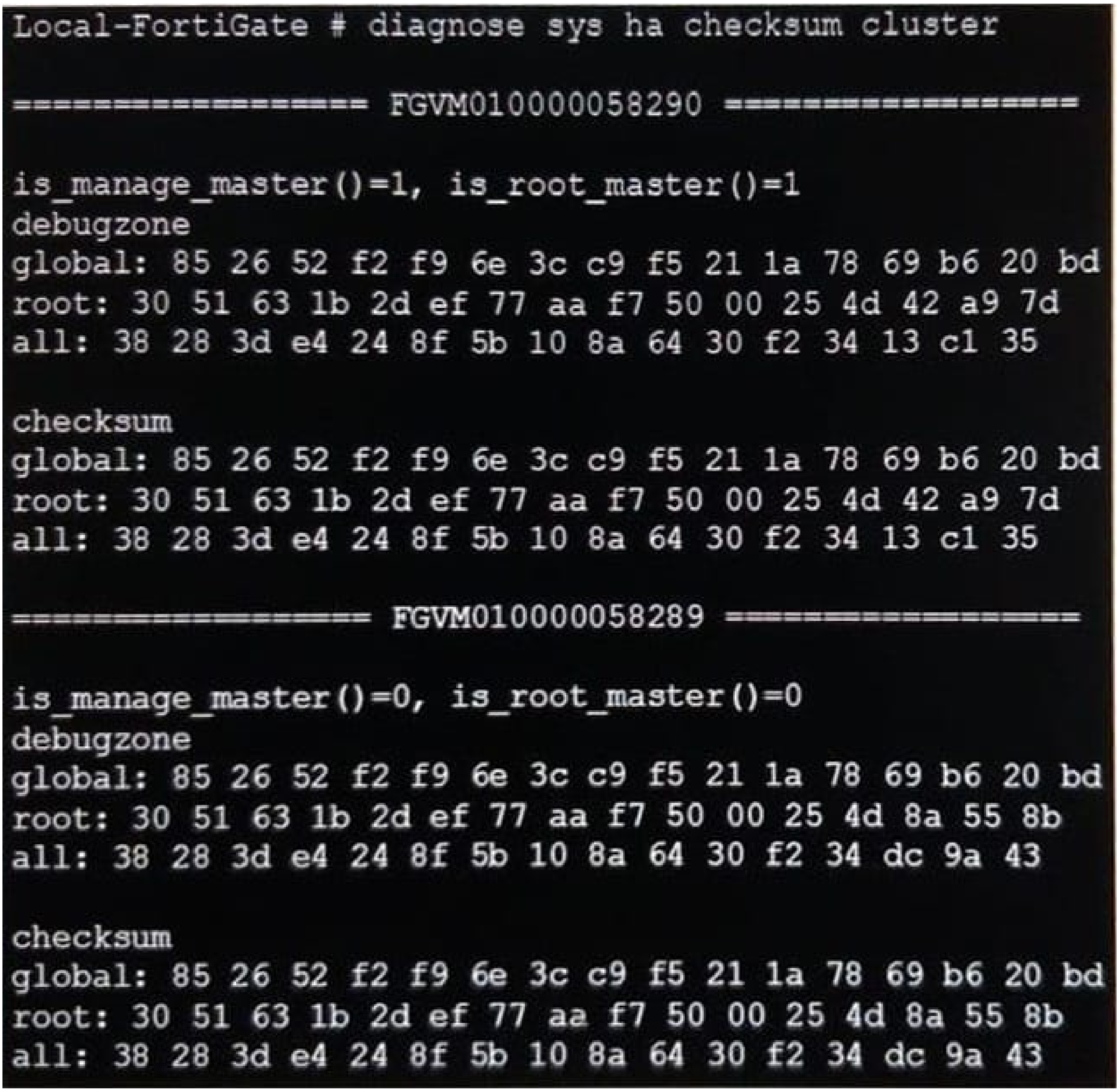
C. Allow, block, authenticate, and warning

D. Allow, monitor, block, and quarantine

Correct Answer: D

QUESTION 5

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.

Correct Answer: BC

Dumps