

Fortinet.FCP_FGT_AD-7.4.by.David.23q

Number: FCP_FGT_AD-7.4
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: FCP_FGT_AD-7.4

Exam Name: FCP - FortiGate 7.4 Administrator



Exam A

QUESTION 1

Which method allows management access to the FortiGate CLI without network connectivity?

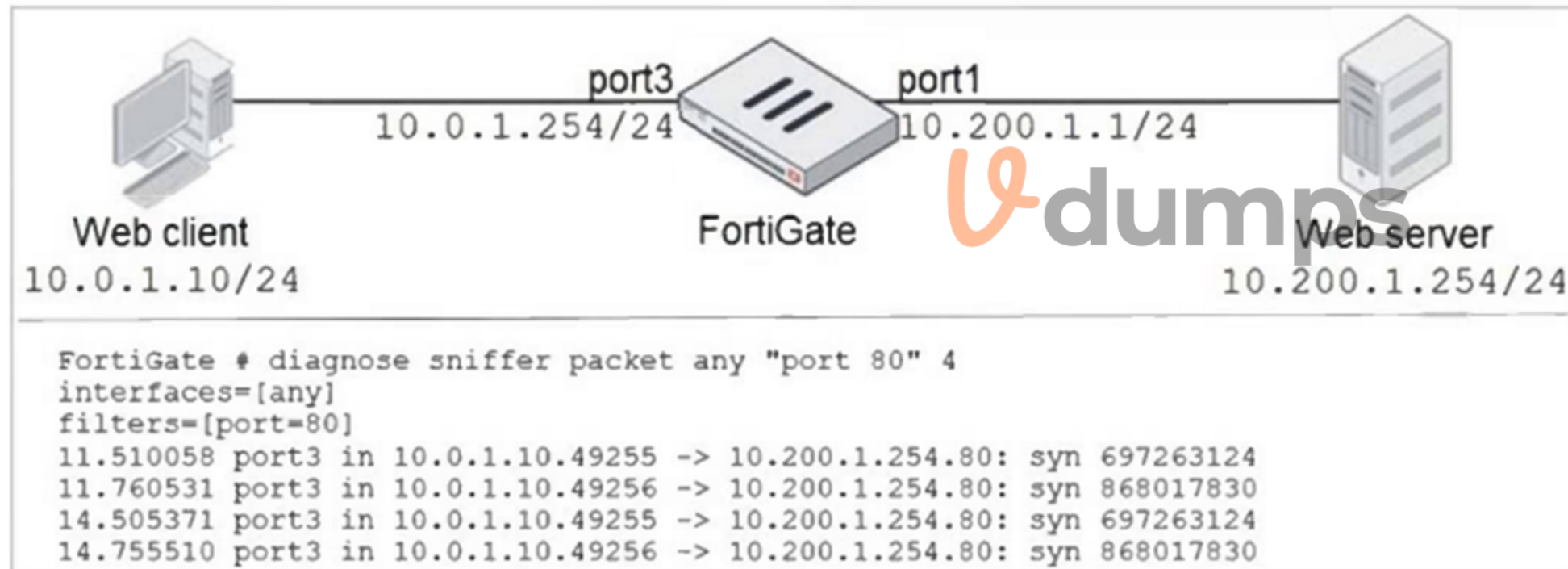
- A. SSH console
- B. CLI console widget
- C. Serial console
- D. Telnet console

Correct Answer: B

Section:

QUESTION 2

Refer to the exhibit.



In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output shown in the exhibit. What should the administrator do next, to troubleshoot the problem?

- A. Execute a debug flow.
- B. Capture the traffic using an external sniffer connected to port1.
- C. Execute another sniffer on FortiGate, this time with the filter 'hose 10.o.1.10'.
- D. Run a sniffer on the web server.

Correct Answer: A

Section:

QUESTION 3

Refer to the exhibit.

FortiGate web filter profile configuration

Edit Web Filter Profile

Name: Corporate

Comments: Write a comment... 0/255

Feature set: **Flow-based** Proxy-based

FortiGuard Category Based Filter

Allow Monitor Block Warning Authenticate

Name	Action
Bandwidth Consuming 6	
Freeware and Software Downloads	Allow
File Sharing and Storage	Allow
Streaming Media and Download	Allow
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	
Malicious Websites	Block

35% 91

The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category. What are two solutions for satisfying the requirement? (Choose two.)

- A. Configure a separate firewall policy with action Deny and an FQDN address object for *. download, com as destination address.
- B. Set the Freeware and Software Downloads category Action to Warning
- C. Configure a web override rating for download, com and select Malicious Websites as the subcategory.
- D. Configure a static URL filter entry for download, com with Type and Action set to Wildcard and Block, respectively.

Correct Answer: C, D

Section:

QUESTION 4

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover.

Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

- A. Enable Dead Peer Detection
- B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
- C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

Correct Answer: A, C

Section:

QUESTION 5

Refer to the exhibits.



Application sensor configuration

Edit Application Sensor

Categories

- All Categories
- Business (179, 6)
- Collaboration (293, 6)
- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, 16)
- Video/Audio (206, 13)
- Web.Client (18)
- Cloud.IT (31)
- Email (87, 12)
- General.Interest (241, 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)
- VoIP (31)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	<input type="checkbox"/> Block
2	Apple	Filter	<input type="checkbox"/> Monitor

Vdumps

Application and Filter override configuration

The image displays two screenshots of the 'Edit Override' configuration interface. The top screenshot shows a configuration for 'FaceTime' with Type 'Filter', Action 'Block', and Filter 'Excessive-Bandwidth'. The bottom screenshot shows a configuration for 'FaceTime' with Type 'Filter', Action 'Monitor', and Filter 'Apple'. Both screenshots show a table with columns for Name, Category, and Technology, and a summary bar for Application Signature.

Name	Category	Technology
FaceTime	VoIP	Client-Server

Application Signature 1/1262

Name	Category	Technology
FaceTime	VoIP	Client-Server

Application Signature 1/33

The exhibits show the application sensor configuration and the Excessive-Bandwidth and Apple filter details. Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

- A. Apple FaceTime will be allowed, based on the Video/Audio category configuration.
- B. Apple FaceTime will be allowed, based on the Apple filter configuration.
- C. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.
- D. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.

Correct Answer: D

Section:

QUESTION 6

An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

- A. SSL VPN idle-timeout
- B. SSL VPN login-timeout
- C. SSL VPN dtls-hello-timeout
- D. SSL VPN session-ttl

Correct Answer: B

Section:

QUESTION 7

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate.
Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

- A. Allow & Warning
- B. Trust & Allow
- C. Allow
- D. Block & Warning
- E. Block

Correct Answer: A, B, E

Section:

QUESTION 8

Refer to the exhibit, which shows the IPS sensor configuration.



Edit IPS Sensor

Name:

Comments: 0/255

Block malicious URLs

IPS Signatures and Filters

[+ Create New](#) [Edit](#) [Delete](#)

Details	Exempt IPs	Action	Packet Logging
Microsoft.Windows.iSCSI.Target.DoS	0	Monitor	Enabled
Windows		Block	Disabled

Vdumps

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

- A. The sensor will gather a packet log for all matched traffic.
- B. The sensor will reset all connections that match these signatures.
- C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.
- D. The sensor will block all attacks aimed at Windows servers.

Correct Answer: C, D

Section:

QUESTION 9

Which statement is a characteristic of automation stitches?

- A. They can be run only on devices in the Security Fabric.
- B. They can be created only on downstream devices in the fabric.
- C. They can have one or more triggers.
- D. They can run multiple actions at the same time.

Correct Answer: D

Section:

QUESTION 10

What is the primary FortiGate election process when the HA override setting is disabled?

- A. Connected monitored ports > Priority > System uptime > FortiGate serial number
- B. Connected monitored ports > System uptime > Priority > FortiGate serial number
- C. Connected monitored ports > Priority > HA uptime > FortiGate serial number
- D. Connected monitored ports > HA uptime > Priority > FortiGate serial number

Correct Answer: C

Section:

QUESTION 11

Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

- A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.
- B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.
- C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
- D. The client FortiGate requires a manually added route to remote subnets.

Correct Answer: A, B

Section:

QUESTION 12

Refer to the exhibit.



Firewall policies

ID	Name	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN to WAN 1										
1	Full_Access	LAN (port3)	WAN (port1) WAN (port2)	all	all	always	ALL	ACCEPT	IP Pool	NAT
WAN to LAN 3										
2	Deny	WAN (port1)	LAN (port3)	Deny_IP	all	always	ALL	DENY		
3	Allow_access	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
4	Webserver	WAN (port1)	LAN (port3)	all	Webserver	always	ALL	ACCEPT		Disabled
Implicit 1										
0	Implicit Deny	any	any	all	all	always	ALL	DENY		

Which statement about this firewall policy list is true?

- A. The Implicit group can include more than one deny firewall policy.
- B. The firewall policies are listed by ID sequence view.
- C. The firewall policies are listed by ingress and egress interfaces pairing view.
- D. LAN to WAN, WAN to LAN, and Implicit are sequence grouping view lists.

Correct Answer: C

Section:

QUESTION 13

An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

- A. SSL VPN idle-timeout
- B. SSL VPN login-timeout
- C. SSL VPN dtls-hello-timeout
- D. SSL VPN session-ttl

Correct Answer: B

Section:

QUESTION 14

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate.
Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

- A. Allow & Warning
- B. Trust & Allow
- C. Allow
- D. Block & Warning
- E. Block

Correct Answer: A, B, E

Section:

QUESTION 15

Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three.)

- A. Manual with load balancing
- B. Lowest Cost (SLA) with load balancing
- C. Best Quality with load balancing
- D. Lowest Quality (SLA) with load balancing
- E. Lowest Cost (SLA) without load balancing

Correct Answer: A, C, D

Section:

QUESTION 16

Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

- A. Pre-shared key and certificate signature as authentication methods
- B. Extended authentication (XAuth) to request the remote peer to provide a username and password
- C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
- D. No certificate is required on the remote peer when you set the certificate signature as the authentication method

Correct Answer: A, B

Section:

QUESTION 17

Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

- A. Checksums of devices are compared against each other to ensure configurations are the same.
- B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.
- C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster
- D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

Correct Answer: A, B

Section:

QUESTION 18

Refer to the exhibit.

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.
0"
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw=10.200.1.254
via port1"
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

Why did FortiGate drop the packet?

- A. 11 matched an explicitly configured firewall policy with the action DENY
- B. It failed the RPF check.
- C. The next-hop IP address is unreachable.
- D. It matched the default implicit firewall policy

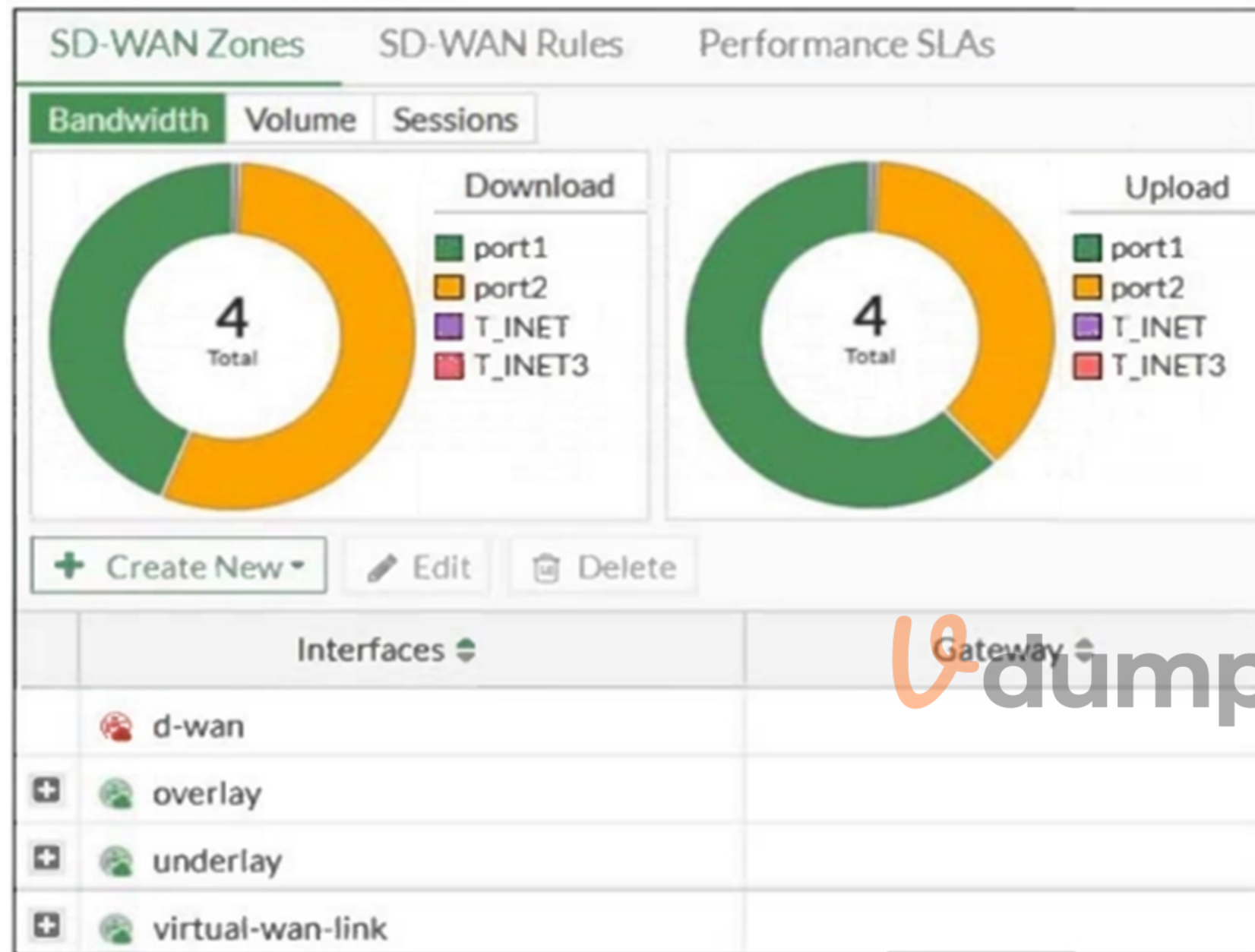
Correct Answer: D

Section:

QUESTION 19

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration



Based on the exhibit, which statement is true?

- A. The underlay zone contains port1 and
- B. The d-wan zone contains no member.
- C. The d-wan zone cannot be deleted.
- D. The virtual-wan-link zone contains no member.

Correct Answer: B

Section:

QUESTION 20

Which two statements describe how the RPF check is used? (Choose two.)

- A. The RPF check is run on the first sent packet of any new session.

- B. The RPF check is run on the first reply packet of any new session.
- C. The RPF check is run on the first sent and reply packet of any new session.
- D. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

Correct Answer: A, D

Section:

QUESTION 21

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad. Which IPsec Wizard template must the administrator apply?

- A. Remote Access
- B. Site to Site
- C. Dial up User
- D. iHub-and-Spoke

Correct Answer: A

Section:

QUESTION 22

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

System Performance output



```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```


Memory usage threshold settings

```
config system global
  set memory-use-threshold-red 88
  set memory-use-threshold-extreme 95
  set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

- A. FortiGate will start sending all files to FortiSandbox for inspection.
- B. FortiGate has entered conserve mode.
- C. Administrators cannot change the configuration.
- D. Administrators can access FortiGate only through the console port.

Correct Answer: B, D

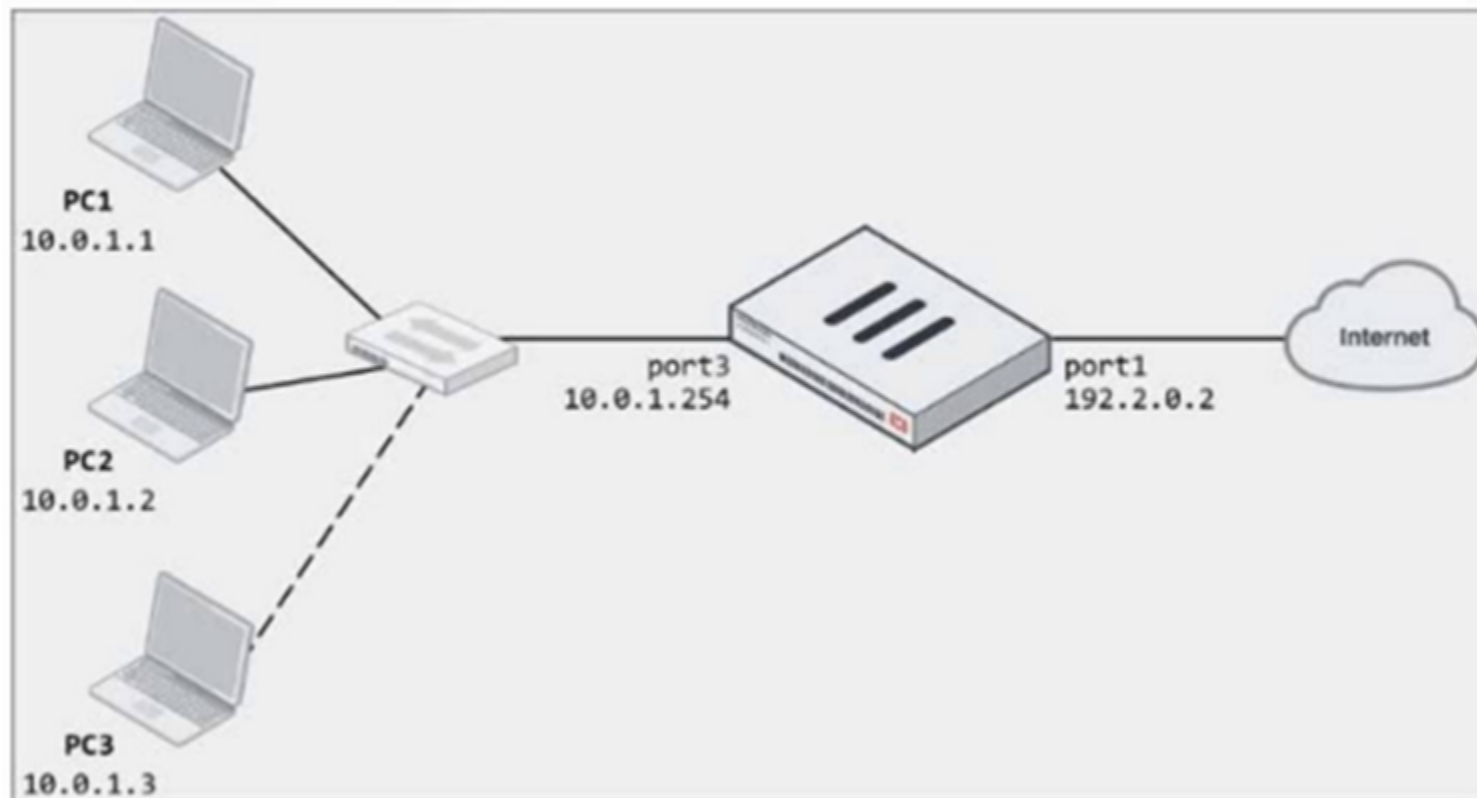
Section:

QUESTION 23

Refer to the exhibits.


Network diagram

The logo for Vdumps.com, featuring a stylized orange 'V' followed by the word 'dumps' in a grey sans-serif font.



Dynamic IP pool

Edit Dynamic IP Pool

Name	<input type="text" value="internet-pool"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Type	<input type="text" value="One-to-One"/>
External IP Range 	<input type="text" value="192.2.0.10-192.2.0.11"/>
ARP Reply	<input checked="" type="checkbox"/>

 **vdumps**

Firewall policy

Edit Policy

Name	LAN-to-Internet
Incoming Interface	LAN (port3) <input type="checkbox"/>
Outgoing Interface	WAN (port1) <input type="checkbox"/>
Source	all <input type="checkbox"/>
Destination	all <input type="checkbox"/>
Schedule	always
Service	ALL <input type="checkbox"/>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input type="checkbox"/> Proxy-based <input checked="" type="checkbox"/>

Firewall/Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address Use Dynamic IP Pool

internet-pool

Preserve Source Port

Protocol Options

PROT default

The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device. Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet. Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

- A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field.
- B. In the IP pool configuration, set endip to 192.2.0.12.
- C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.
- D. In the IP pool configuration, set cype to overload.

Correct Answer: B, D

Section:

