

# Fortinet

## Exam Questions NSE4\_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2



NEW QUESTION 1

Refer to the exhibits.  
Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object configuration.  
The WAN (port1) interface has the IP address 10.200.1.1/24.  
The LAN (port3) interface has the IP address 10.0.1.254/24.

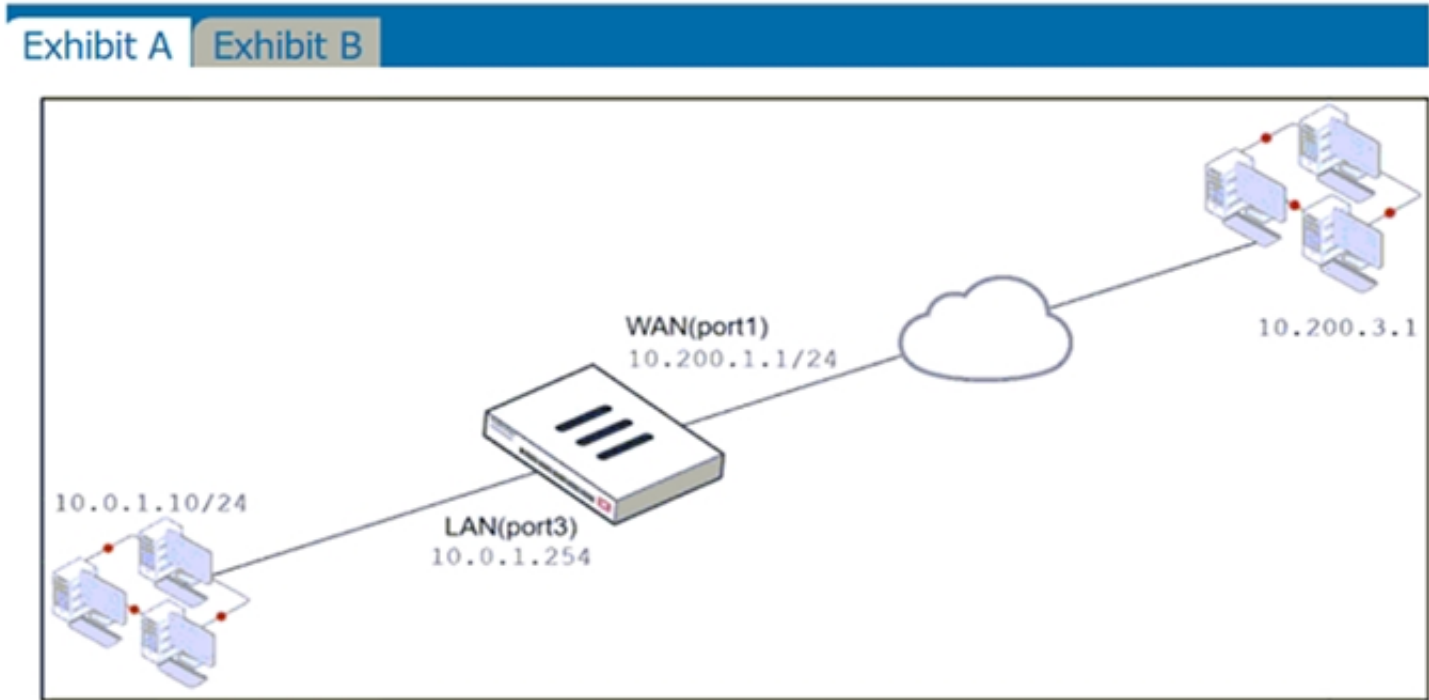


Exhibit A   Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type: IPv4

Name: VIP

Comments: Write a comment... 0/255

Color: Change

Network

Interface: WAN (port1)

Type: Static NAT

External IP address/range: 10.200.1.10

Map to

IPv4 address/range: 10.0.1.10

Optional Filters: ☐

Port Forwarding: ☒

Protocol: TCP UDP SCTP ICMP

Port Mapping Type: One to one Many to many

External service port: 10443

Map to IPv4 port: 443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

A. 10.0.1.254, 10.0.1.10, and 443, respectively  
B. 10.0.1.254, 10.0.1.10, and 10443, respectively  
C. 10.200.3.1, 10.0.1.10, and 443, respectively

Answer: C

NEW QUESTION 2

What are two functions of ZTNA? (Choose two.)

- A. ZTNA manages access through the client only.  
B. ZTNA manages access for remote users only.  
C. ZTNA provides a security posture check.  
D. ZTNA provides role-based access.

**Answer:** CD

### NEW QUESTION 3

What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)

- A. FortiGate uses fewer resources.
- B. FortiGate performs a more exhaustive inspection on traffic.
- C. FortiGate adds less latency to traffic.
- D. FortiGate allocates two sessions per connection.

**Answer:** AC

### NEW QUESTION 4

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

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

**Answer:** BC

### NEW QUESTION 5

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

What two conclusions can you make from the debug flow output? (Choose two.)

- A. The debug flow is for ICMP traffic.
- B. The default route is required to receive a reply.
- C. A new traffic session was created.
- D. A firewall policy allowed the connection.

**Answer:** AC

### NEW QUESTION 6

Refer to the exhibits.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook. Users are given access to the Facebook web application. They can play video content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts.

Exhibit A

Exhibit B

Edit Policy

Name ⓘ

Facebook SSL Inspection

Incoming Interface

port2

Outgoing Interface

port1

Source

all

Destination

all

Service

ALL

Firewall / Network Options

ⓘ Central NAT is enabled so NAT settings from matching [Central SNAT policies](#) will be applied.

Security Profiles

SSL Inspection

SSL

certificate-inspection

Exhibit A Exhibit B

Edit Policy

Name ⓘ

Facebook Access

Policy Mode ⓘ

Standard

Learn Mode

Incoming Interface

port2

+

×

Outgoing Interface

port1

+

×

Source

all

+

×

Destination

all

+

×

Schedule

always

▼

Service

App Default

Specify

Application

Facebook

Facebook\_Like.Button

Facebook\_Video.Play

+

×

×

×

URL Category

+

Action

✓ ACCEPT

⊘ DENY

Firewall/Network Options

Protocol Options

PROT

default

▼

Which part of the policy configuration must you change to resolve the issue?

- A. Force access to Facebook using the HTTP service.
- B. Make the SSL inspection a deep content inspection.
- C. Add Facebook in the URL category in the security policy.
- D. Get the additional application signatures required to add to the security policy.

Answer: B

NEW QUESTION 7

An administrator has configured the following settings:  
config system settings  
set ses-denied-traffic enable  
end  
config system global  
set block-session-timer 30  
end

What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. The number of logs generated by denied traffic is reduced.
- D. A session for denied traffic is created.

Answer: AC

NEW QUESTION 8

Refer to the exhibit.



```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(8ps/kbps): 26/0 rx speed(8ps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

- A. The session is in SYN\_SENT state.
- B. The session is in FIN\_ACK state.
- C. The session is in FTN\_WAIT state.
- D. The session is in ESTABLISHED state.

Answer: A

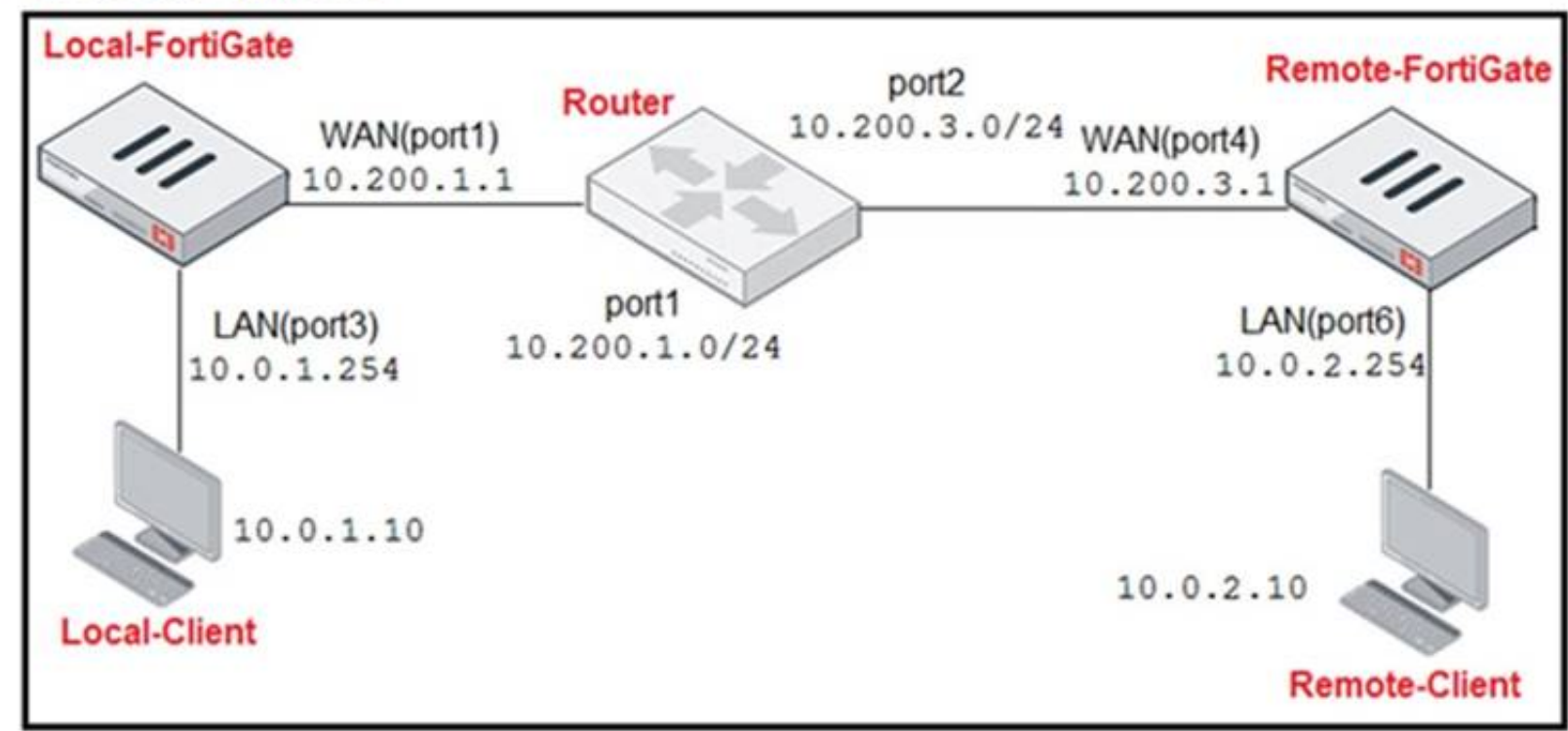
Explanation:

Indicates TCP (proto=6) session in SYN\_SENT state (proto=state=2) <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 9

Refer to the exhibit.

Network Diagram



Central SNAT Policies Local-FortiGate

ID	From	To	Source Address	Protocol Number	Destination Address	Translated Address
2	LAN(port3)	WAN(port1)	all	6	REMOTE_FORTIGATE	SNAT-Pool
1	LAN(port3)	WAN(port1)	all	1	all	SNAT-Remote1
3	LAN(port3)	WAN(port1)	all	2	all	SNAT-Remote

IP Pool Local-FortiGate

+ Create New ▾		Edit	Clone	Delete	Search	
Name ▾	External IP Range ▾	Type ▾	ARP Reply ▾			
SNAT-Pool	10.200.1.49-10.200.1.49	Overload		Enabled		
SNAT-Remote	10.200.1.149-10.200.1.149	Overload		Enabled		
SNAT-Remote1	10.200.1.99-10.200.1.99	Overload		Enabled		

Protocol Number Table

Protocol Number Table	
Protocol	Protocol Number
TCP	6
ICMP	1
IGMP	2

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200. 1. 1/24. The LAN (port3) interface has the IP address 10.0. 1.254/24. A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied. Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0. 1. 10) pings the IP address of Remote-FortiGate (10.200.3. 1)?

A. 10.200. 1. 149  
B. 10.200. 1. 1  
C. 10.200. 1.49  
D. 10.200. 1.99

Answer: D

NEW QUESTION 10

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.  
B. By default, the SSL VPN portal requires the installation of a client's certificate.  
C. By default, split tunneling is enabled.  
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 10

Examine this PAC file configuration. 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: AD

NEW QUESTION 12

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection  
B. Antivirus in flow-based inspection  
C. DNS filter  
D. Web application firewall  
E. Application control

Answer: ABE

Explanation:  
<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow>

NEW QUESTION 16

Refer to the exhibit.

Add Signatures

Type

Filter

Signature

Action

Block

Packet logging

Enable

Disable

Status

Enable

Disable

Default

Rate-based settings

Default

Specify

Exempt IPs

0

Edit IP Exemptions

Search

Q

Selected 1

All

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1					
FTP.Login.Failed		Server	All	Pass	

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

Answer: D

Explanation:

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 20

Which two statements are correct about a software switch on FortiGate? (Choose two.)

- A. It can be configured only when FortiGate is operating in NAT mode
- B. Can act as a Layer 2 switch as well as a Layer 3 router
- C. All interfaces in the software switch share the same IP address
- D. It can group only physical interfaces

Answer: AC

NEW QUESTION 24

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Edit Policy

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

Protocol Options

PRX default

Security Profiles

AntiVirus

AV default

Web Filter

DNS Filter

Application Control

IPS

SSL Inspection

SSL deep-inspection

Decrypted Traffic Mirror



Edit AntiVirus Profile

Name

Comments
 29/255

Detect Viruses

Block

Monitor

Feature set

Flow-based

Proxy-based

Inspected Protocols

HTTP ☒

SMTP ☒

POP3 ☒

IMAP ☒

FTP ☒

CIFS ☐

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ☒

Include Mobile Malware Protection ☒

Virus Outbreak Prevention ⓘ

Use FortiGuard Outbreak Prevention Database ☐

Use External Malware Block List ⓘ ⚠ ☐

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.
- C. The volume of traffic being inspected is too high for this model of FortiGate.
- D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

**Answer:** B

**Explanation:**

· "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately

· When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.

In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

**NEW QUESTION 28**

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

**Answer:** CD

**NEW QUESTION 30**

Which statement about the IP authentication header (AH) used by IPsec is true?

- A. AH does not provide any data integrity or encryption.
- B. AH does not support perfect forward secrecy.
- C. AH provides data integrity bur no encryption.
- D. AH provides strong data integrity but weak encryption.

**Answer:** C



NEW QUESTION 35

Refer to exhibit.  
An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.

NameAllow\_Twitter

CommentsWrite a comment...0/255

Feature setFlow-basedProxy-based

FortiGuard Category Based Filter

AllowMonitorBlockWarningAuthenticate

Name	Action
Medicine	Allow
News and Media	Allow
Social Networking	Block
Political Organizations	Allow
Reference	Allow
Global Religion	Allow
Shopping	Allow
Society and Lifestyles	Allow
Sports	Allow

Static URL Filter

Block invalid URLs

URL Filter

Create NewEditDeleteSearch

URL	Type	Action	Status
twitter.com	Wildcard	Allow	Enable

1

Block malicious URLs discovered by FortiSandbox

Content Filter

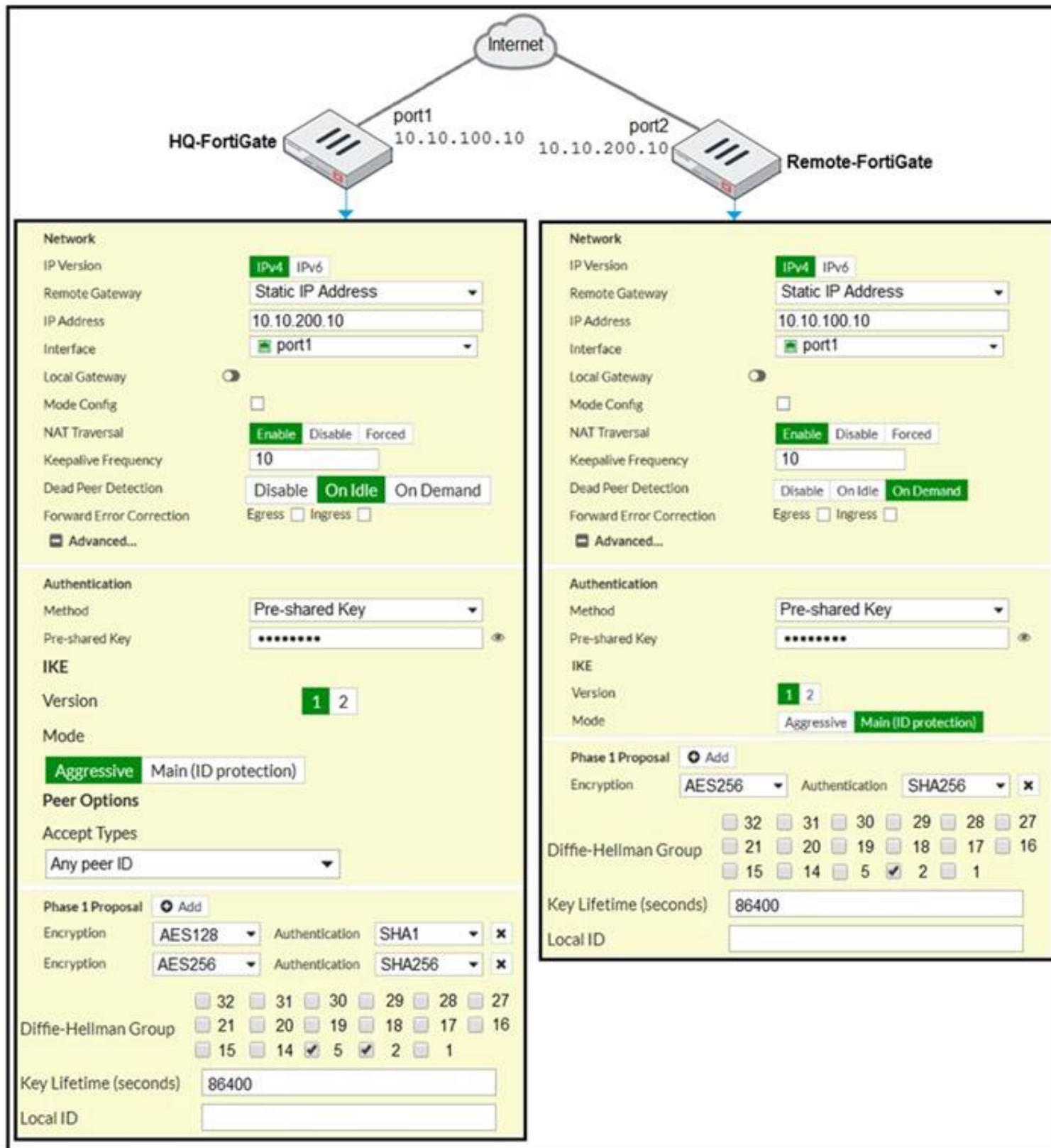
Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

- A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking
- B. On the Static URL Filter configuration, set Type to Simple
- C. On the Static URL Filter configuration, set Action to Exempt.
- D. On the Static URL Filter configuration, set Action to Monitor.

Answer: C

NEW QUESTION 36

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.



Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

- A. On HQ-FortiGate, set IKE mode to Main (ID protection).
- B. On both FortiGate devices, set Dead Peer Detection to On Demand.
- C. On HQ-FortiGate, disable Diffie-Helman group 2.
- D. On Remote-FortiGate, set port2 as Interface.

**Answer:** AD

#### NEW QUESTION 39

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE4\_FGT-7.2 Practice Exam Features:

- \* NSE4\_FGT-7.2 Questions and Answers Updated Frequently
- \* NSE4\_FGT-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4\_FGT-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE4\_FGT-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE4\\_FGT-7.2 Practice Test Here](#)**