

Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1

There are multiple dialup IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels.

Which phase 1 setting you can configure to match the user to the tunnel?

- A. Local Gateway
- B. Dead Peer Detection
- C. Peer ID
- D. IKE Mode Config

Answer: C

NEW QUESTION 2

You have configured the below commands on a FortiGate.

```
config system settings
set strict-src-check enable
end
```

```
Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

- A. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
- B. FortiGate will enable strict RPF on all its interfaces and port1 will be enable for asymmetric routing.
- C. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.
- D. Port1 will be enabled with flexible RP
- E. and all other interfaces will be enabled for strict RPF

Answer: A

NEW QUESTION 3

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.

Which DPD mode on FortiGate meets this requirement?

- A. On Demand
- B. Enabled
- C. On Idle
- D. Usabled

Answer: A

NEW QUESTION 4

What are two features of FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check.
- D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: BC

NEW QUESTION 5
Refer to the exhibit.



The NOC team connects to the FortiGate GUI with the NOC_Access admin profile. They request that their GUI sessions do not disconnect too early during inactivity. What must the administrator configure to answer this specific request from the NOC team? (Choose one answer)

- A. Move NOC_Access to the top of the list to ensure all profile settings take effect.
- B. Increase the offline value of the Override Idle Timeout parameter in the NOC_Access admin profile.
- C. Ensure that all NOC_Access users are assigned the super_admin role to guarantee access.
- D. Increase the admintimeout value under config system accprofile NOC_Access.

Answer: D

NEW QUESTION 6

You have configured an application control profile, set peer-to-peer traffic to Block under the Categories tab. and applied it to the firewall policy. However, your peer-to-peer traffic on known ports is passing through the FortiGate without being blocked. What FortiGate settings should you check to resolve this issue?

- A. FortiGuard category ratings
- B. Network Protocol Enforcement
- C. Replacement Messages for UDP-based Applications
- D. Application and Filter Overrides

Answer: B

NEW QUESTION 7

Refer to the exhibits.

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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

The system performance output and default configuration of high memory usage thresholds on a FortiGate device are shown. Based on the system performance output, what are the two possible outcomes? (Choose two.)

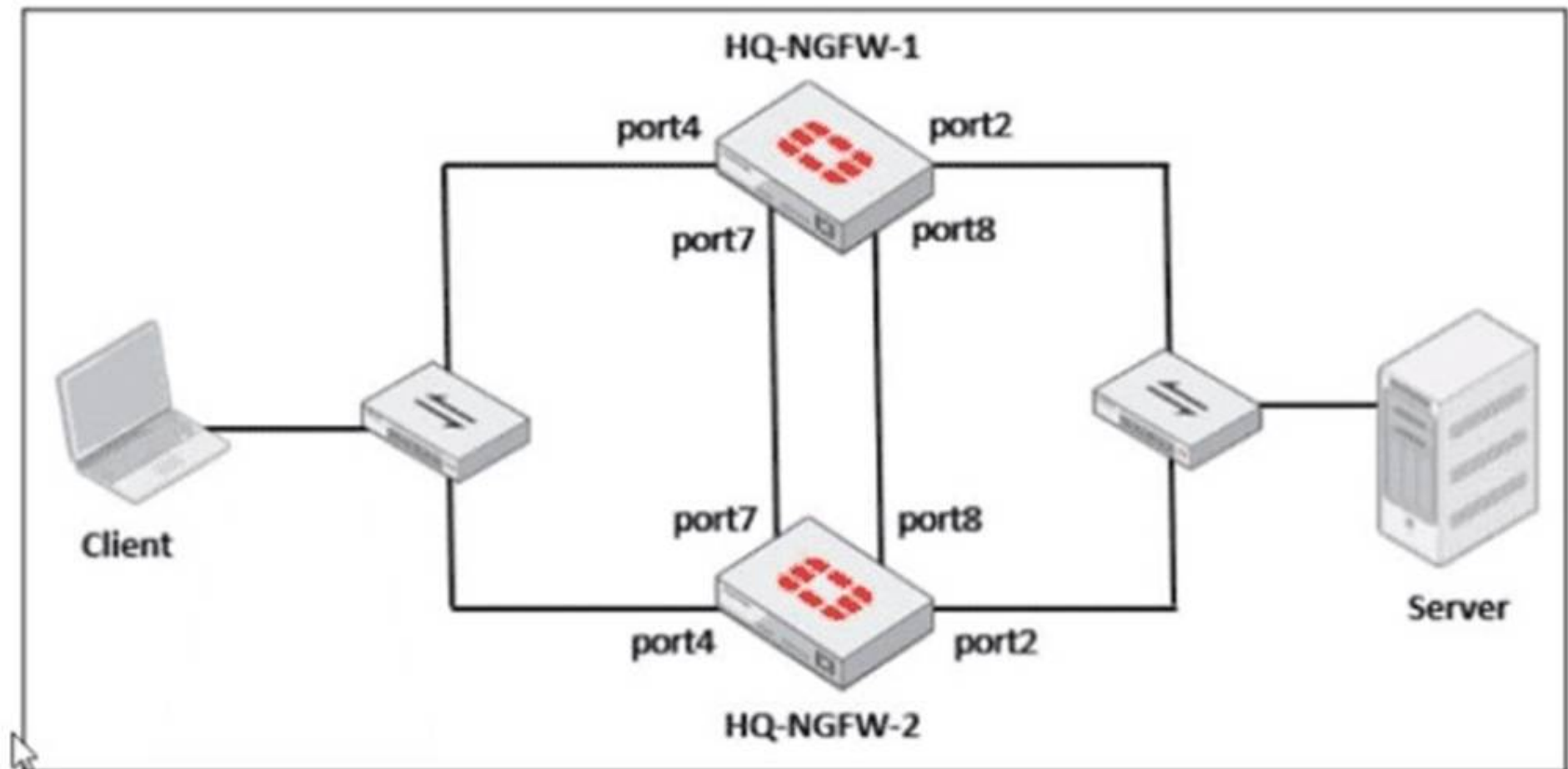
- A. Administrators can access FortiGate only through the console port.

- B. FortiGate has entered conserve mode.
- C. FortiGate drops new sessions.
- D. Administrators can change the configuration.

Answer: BD

NEW QUESTION 8
Refer to the exhibits.

FortiGate HA cluster topology



Current HA status

```
HQ-NGFW-1 # get system ha status
...
Configuration Status:
  FGVM02TM24013423(updated 0 seconds ago): in-sync
  FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
  FGVM02TM24013501(updated 4 seconds ago): in-sync
  FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1      , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2      , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, HA operating index = 1
```

New FortiGate HA configuration

```
HQ-NGFW-1
# config system ha
    set group-id 5
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port7" 50 "port8" 60
    set session-pick enable
    set override disable
    set priority 90
    set monitor "port3"

HQ-NGFW-2
# config system ha
    set group-id 5
    set group-name "Fortinet"
    set mode a-p
    set password *
    set hbdev "port7" 50 "port8" 60
    set session-pick enable
    set override enable
    set priority 110
    set monitor "port3"
```

Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibits. What would be the expected outcome in the HA cluster?

- A. HQ-NGFW-2 will take over as the primary because it has the override enable setting and higher priority than HQ-NGFW-1.
- B. HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority
- C. The HA cluster will become out of sync because the override setting must match on all HA members.
- D. HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.

Answer: A

NEW QUESTION 9

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A. They rely on session loss and jitter.
- B. They monitor the state of the FortiGate device.
- C. All the SLA targets can be configured.
- D. They are applied in a SD-WAN rule lowest cost strategy.
- E. They can be measured actively or passively.

Answer: CDE

NEW QUESTION 10
Refer to the exhibits.

Application sensor

Edit Application Sensor

Categories

Mixed ▾
All Categories

Business (157, ☁ 6)

Collaboration (266, ☁ 13)

Game (83)

Mobile (3)

Operational Technology

Proxy (189)

Social Media (113, ☁ 29)

Update (48)

VoIP (23)

Unknown Applications

Cloud/IT (72, ☁ 12)

Email (76, ☁ 11)

General Interest (254, ☁ 15)

Network Service (338)

P2P (55)

Remote Access (96)

Storage/Backup (150, ☁ 20)

Video/Audio (148, ☁ 17)

Web Client (24)

Network Protocol Enforcement

Application and Filter Overrides

+ Create New

Edit

Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	Block
2	VEND Google	Filter	Monitor
2			

Firewall policy

Edit Policy

Firewall/Network Options

Inspection mode

Flow-based
Proxy-based

NAT

☒

IP pool configuration

Use Outgoing Interface Address
Use Dynamic IP Pool

Preserve source port

☐

Protocol options

PROT
default

Security Profiles

AntiVirus

☐

Web filter

☐

DNS filter

☐

Application control

☒
APP
default

IPS

☐

File filter

☐

SSL inspection

SSL
deep-inspection

Decrypted traffic mirror

☐

Logging Options

Log allowed traffic

☒
Security events
All sessions

You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. Which two factors can you observe from these configurations? (Choose two.)

- A. YouTube access is blocked based on Excessive-Bandwidth Application and Filter override settings.
- B. Facebook access is blocked based on the category filter settings.
- C. Facebook access is allowed but you cannot play Facebook videos based on Video/Audio category filter settings.
- D. YouTube search is allowed based on the Google Application and Filter override settings.

Answer: AB

NEW QUESTION 10

You have created a web filter profile named restrictmedia-profile with a daily category usage quota. When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down. What could be the reason?

- A. The web filter profile is already referenced in another firewall policy.
- B. The firewall policy is in no-inspection mode instead of deep-inspection.
- C. The naming convention used in the web filter profile is restricting it in the firewall policy.
- D. The inspection mode in the firewall policy is not matching with web filter profile feature set.

Answer: D

NEW QUESTION 14

Refer to the exhibits.

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32 kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds.
Which FortiGate is the primary?

- A. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
- B. HQ-NGFW-2 with the parameter priority setting
- C. HQ-NGFW-1 with the parameter override setting
- D. HQ-NGFW-2 with the parameter memory-failover-threshold setting

Answer: D

NEW QUESTION 19

Refer to the exhibits.

Security Fabric logical topology view



Security Fabric settings on HQ-ISFW-2

Security Fabric Settings

Security Fabric role: ☐ Standalone ☐ Serve as Fabric Root ☒ Join Existing Fabric

Allow other Security Fabric devices to join: ☒ port6 +

Upstream FortiGate IP/FQDN:

Allow downstream device REST API access: ☒

Management IP/FQDN: ☐ Use WAN IP ☒ Specify

Management port: ☐ Use Admin Port ☒ Specify

SAML SSO Settings

SAML Single Sign-On: ☒ Auto ☐ Manual Advanced Options

Mode: Pending

An administrator wants to add HQ-ISFW-2 in the Security Fabric. HQ-ISFW-2 is in the same subnet as HQ-ISFW. After configuring the Security Fabric settings on HQ-ISFW-2, the status stays Pending. What can be the two possible reasons? (Choose two answers)

- A. Upstream FortiGate IP must be set to 10.0.11.254.
- B. SAML Single Sign-On must be set to Manual.
- C. HQ-ISFW-2 must be authorized on HQ-ISFW.
- D. Management IP must be set to 10.0.13.254.

Answer: AC

NEW QUESTION 22

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively. Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

- A. Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.
- B. Both interfaces must have the interface role assigned.
- C. Both interfaces must have directly connected routes on the routing table.

D. Both interfaces must have IP addresses assigned.

Answer: CD

NEW QUESTION 26

Refer to the exhibit.

SD-WAN traffic log

Application Name 	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
 YouTube	 Accept (8.08 kB / 27...	1 (DIA)	 port2		
 YouTube	 Accept (UTM Allowed)	1 (DIA)	 port2		
 Facebook	 Accept (UTM Allowed)	1 (DIA)	 port1		
 Facebook	 Accept (UTM Allowed)	1 (DIA)	 port1		
 Facebook	 Accept (3.33 kB / 10...	1 (DIA)	 port1		
 YouTube	 Accept (44.63 kB / 3....	1 (DIA)	 port2		
 CNN	 Accept (UTM Allowed)	1 (DIA)	 port1		
 CNN	 Accept (UTM Allowed)	1 (DIA)	 port2		
 CNN	 Accept (UTM Allowed)	1 (DIA)	 port2		

The administrator configured SD-WAN rules and set the FortiGate traffic log page to display SD-WAN-specific columns: SD-WAN Quality and SD-WAN Rule Name. FortiGate allows the traffic according to policy ID 1 placed at the top. This is the policy that allows SD-WAN traffic. Despite these settings, the traffic logs do not show the name of the SD-WAN rule used to steer those traffic flows. What could be the reason?

- A. SD-WAN rule names do not appear immediately.
- B. The administrator must refresh the page.
- C. There is no application control profile applied to the firewall policy.
- D. Destinations in the SD-WAN rules are configured for each application, but feature visibility is not enabled.
- E. FortiGate load balanced the traffic according to the implicit SD-WAN rule.

Answer: D

NEW QUESTION 29

Refer to the exhibit.

New AntiVirus Profile

Name

Comments

 0/255

AntiVirus scan ⓘ

☐

Feature set

Flow-based

Proxy-based

Inspected Protocols

HTTP

☐

SMTP

☐

POP3

☐

IMAP

☐

FTP

☐

CIFS

☐

Why is the Antivirus scan switch grayed out when you are creating a new antivirus profile for FTP?

- A. Antivirus scan is disabled under System -> Feature visibility
- B. None of the inspected protocols are active in this profile.
- C. The Feature Set for the profile is Flow-based but it must be Proxy-based
- D. FortiGat
- E. with less than 2 GB RAM
- F. does not support the Antivirus scan feature.

Answer: B

NEW QUESTION 33

Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

- A. The collector agent uses a Windows API to query DCs for user logins.
- B. The NetSessionEnum function is used to track user logouts.
- C. NetAPI polling can increase bandwidth usage in large networks.
- D. The collector agent must search Windows application event logs.

Answer: B

NEW QUESTION 35

Refer to the exhibits.

Web filter profile configuration

Edit Web Filter Profile

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

☒ FortiGuard Category Based Filter

Name	Action
Job Search	☒ Allow
Medicine	☒ Allow
News and Media	☒ Allow
Social Networking	☒ Allow
Political Organizations	☒ Allow
Reference	☒ Allow
Global Religion	☒ Allow
Shopping	☒ Allow
Society and Lifestyles	☒ Allow

58% **95**

☐ Allow users to override blocked categories

☐ Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☐

☐ Static URL Filter

Block invalid URLs ☐

URL Filter ☒

URL	Type	Action	Status
www.facebook.com	Simple	☐ Monitor	☒ Enable

Firewall policy configuration

Edit Policy

Firewall/Network Options

Inspection mode

Flow-based

Proxy-based

NAT

☒

IP pool configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve source port

☐

Protocol options

PROT

default

Security Profiles

AntiVirus

☐

Web filter

☒

WEB

default

Video filter

☐

DNS filter

☐

Application control

☐

IPS

☐

File filter

☐

SSL inspection

SSL

certificate-inspection

FortiGuard block page



A web filter profile configuration and firewall policy configuration are shown.
 You are trying to access www. facebook.com, but you are redirected to a FortiGuard web filtering block page.
 Based on the exhibits, what is the possible cause of the issue?

- A. The web rating override configuration is incorrect.
- B. The web filter profile feature set is configured incorrectly.
- C. The firewall policy inspection mode is incorrect.
- D. For ww
- E. facebook
- F. co
- G. the URL filter action is incorrect.

Answer: C

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_AD-7.6 Practice Exam Features:

- * NSE4_FGT_AD-7.6 Questions and Answers Updated Frequently
- * NSE4_FGT_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE4_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT_AD-7.6 Practice Test Here](#)