



Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view. Why is the policy order different in these two views?

- A. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
- B. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
- C. Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.
- D. Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.

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

Refer to the exhibit.

A RADIUS server configuration is shown.

New RADIUS Server

Name

FortiAuthenticator-RADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☒

Primary Server

IP/Name

10.0.13.130

Secret

••••••••••

Test Connectivity

Test User Credentials

An administrator added a configuration for a new RADIUS server. While configuring, the administrator enabled "Include in every user group." What is the impact of enabling "Include in every user group" in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.
- D. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.

Answer: A

NEW QUESTION 5

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 6

Which two statements describe characteristics of automation stitches? (Choose two answers)

- A. Actions involve only devices included in the Security Fabric.
- B. An automation stitch can have multiple triggers.
- C. Multiple actions can run in parallel.
- D. Triggers can involve external connectors.

Answer: CD

NEW QUESTION 7

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

☐

Video filter

☐

DNS filter

☐

Application control

☒

APP
default

IPS

☐

File filter

☐

SSL inspection

SSL
certificate-inspection

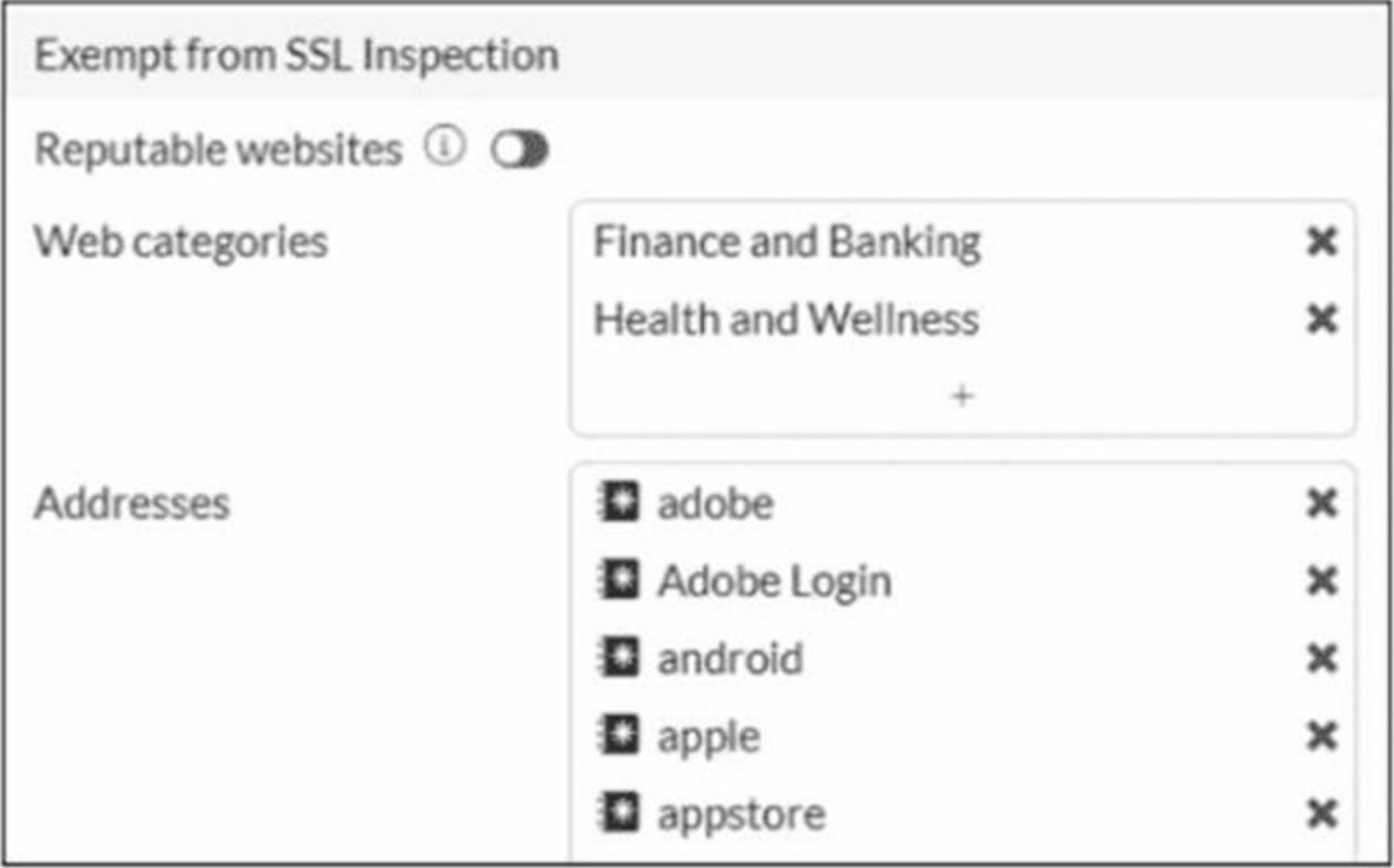
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. Which two actions would you take to resolve the issue? (Choose two.)

- A. Set SSL inspection to deep-content inspection.
- B. Move up Google in the Application and Filter Overrides section to set its priority lot
- C. Add "Google".com to the URL category in the security profile.
- D. Change the Inspection mode to Flow-based
- E. Set the action for Google in the Application and Filter Overrides section to Allow

Answer: BE

NEW QUESTION 8

Refer to the exhibit.



The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit For which two reasons are these web categories exempted? (Choose two.)

- A. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
- B. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.
- C. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
- D. The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.

Answer: BC

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 exhibit.

Profile Name
Monitoring_Access
NOC_Access
prof_admin
super_admin

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?

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

Answer: B

NEW QUESTION 10

What is the primary FortiGate election process when the HA override setting is enabled? (Choose one answer)

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

Answer: A

NEW QUESTION 15

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 17

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 24

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 27

Which two statements are correct when the FortiGate device enters conserve mode? (Choose two.)

- A. FortiGate refuses to accept configuration changes.
- B. FortiGate halts complete system operation and requires a reboot to regain available resources.
- C. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.
- D. FortiGate continues to run critical security actions, such as quarantine.

Answer: AC

NEW QUESTION 29

When configuring firewall policies, which of the following is true regarding the policy ID? (Choose two.)

- A. A firewall policy ID identifies the order of policy execution in firewall policies.
- B. A policy ID cannot be modified once a policy is created.
- C. You can create a policy in CLI with policy ID 0.
- D. It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.

Answer: BC

NEW QUESTION 32

Refer to the exhibit.

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

Which two ways can you view the log messages shown in the exhibit? (Choose two.)

- A. By right-clicking the implicit deny policy.

- B. Using the FortiGate CLI command diagnose log test
- C. By filtering by policy universally unique identifier (UUID) and application name in the log entry
- D. In the Forward Traffic section

Answer: CD

NEW QUESTION 33

Refer to the exhibit

A firewall policy to enable active authentication is shown.

Policy	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port4 → port2 1								
Internet (1)	HQ_SUBNET Remote-users	all	always	ALL_ICMP HTTPS HTTP	ACCEPT	NAT	Standard	Category_Monitor certificate-inspection

When attempting to access an external website using an active authentication method, the user is not presented with a login prompt. What is the most likely reason for this situation?

- A. No matching user account exists for this user.
- B. The Remote-users group must be set up correctly in the FSSO configuration.
- C. The Remote-users group is not added to the Destination
- D. The Service DNS is required in the firewall policy.

Answer: D

NEW QUESTION 37

Refer to the exhibits.

Web filter profile configuration

Edit Web Filter Profile

Feature set

Flow-based

Proxy-based

☒ FortiGuard Category Based Filter

Allow

Monitor

Block

Warning

Authenticate

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% 93

☐ Allow users to override blocked categories

☐ Search Engines

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

☐ Static URL Filter

Block invalid URLs ☐

URL Filter ☒

+ Create New

Edit

Delete

Search

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?

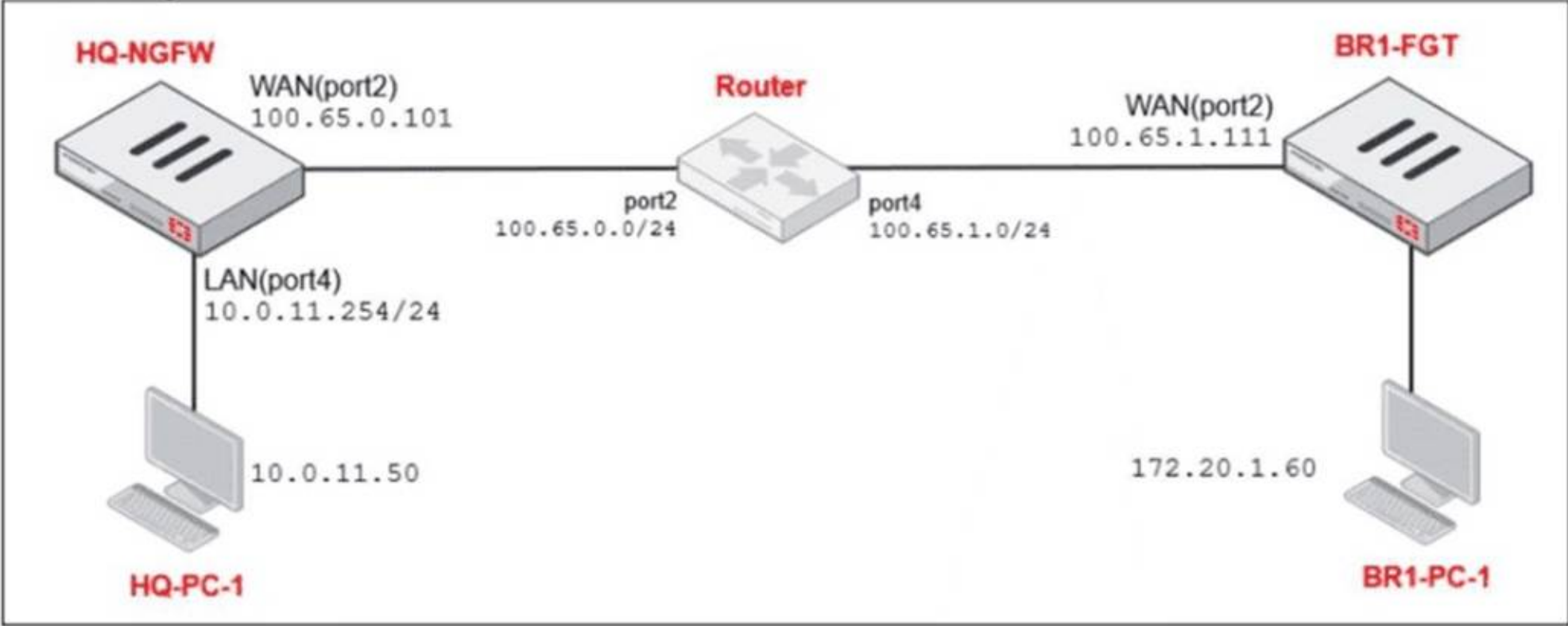
- A. The web rating override configuration is incorrect.
- B. The web filter profile feature set is configured incorrectly.
- C. The firewall policy inspection mode is incorrect.
- D. For ww
- E. faceboo
- F. co
- G. the URL filter action is incorrect.

Answer: C

NEW QUESTION 40

Refer to the exhibits.

Network diagram



NAT IP pool configuration

	Name	External IP Range	Type	ARP Reply
☐	SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
☐	SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
☐	SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
IGMP traffic (4)	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.
The WAN (port2) interface has the IP address 100.65.0.101/24.
The LAN (port4) interface has the IP address 10.0.11.254/24.
Which IP address will be used to source NAT (SNAT) the traffic, if the user on HQ-PC-1 (10.0.11.50) pings the IP address of BR-FGT (100.65.1.111)?

- A. 100.65.0.101
- B. 100.65.0.49
- C. 100.65.0.149
- D. 100.65.0.99

Answer: D

NEW QUESTION 44

.....

Relate Links

100% Pass Your NSE4_FGT_AD-7.6 Exam with ExamBible Prep Materials

https://www.exambible.com/NSE4_FGT_AD-7.6-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>