



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

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 3

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?

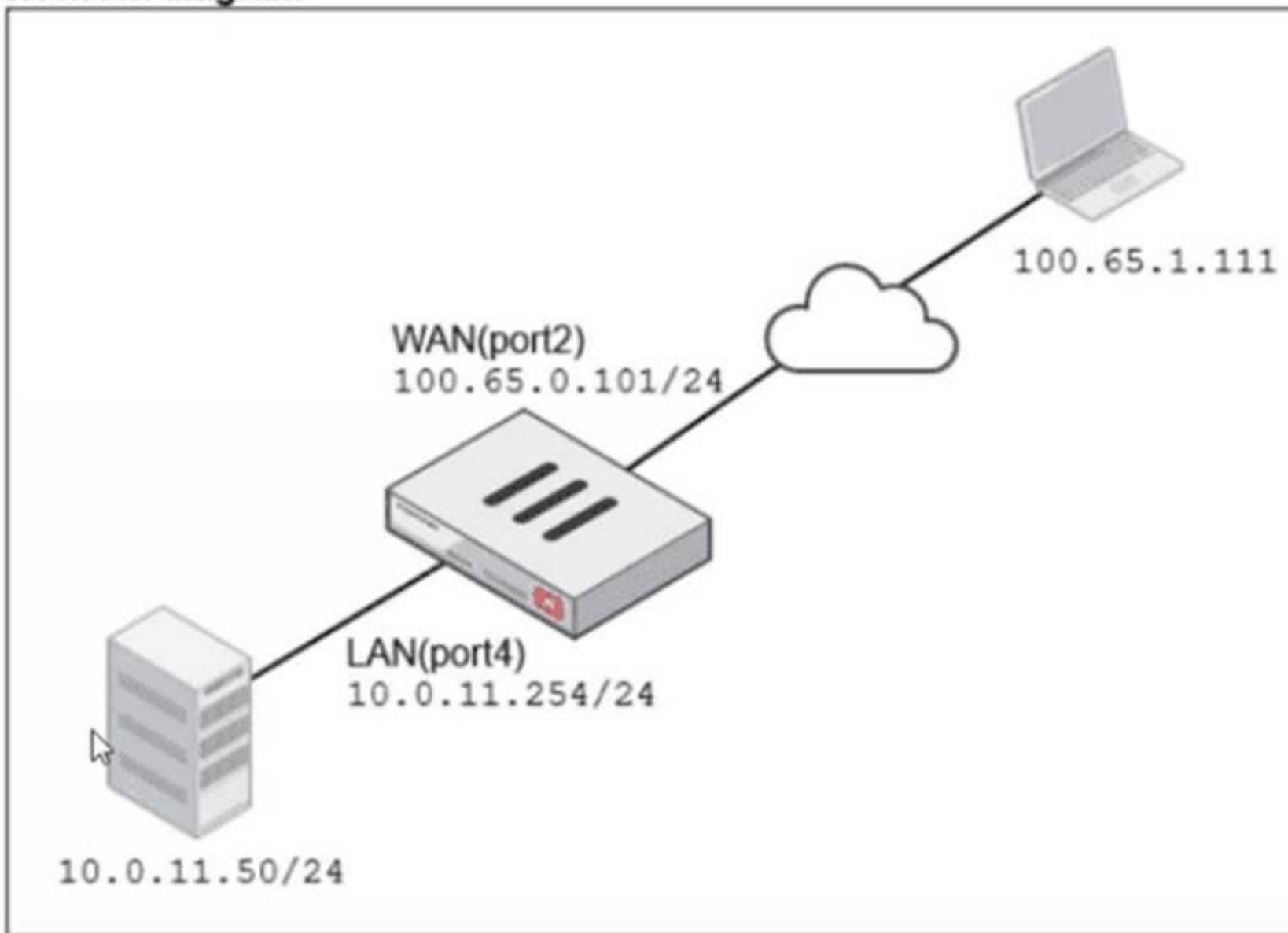
- A. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
- B. FortiGate will enable strict RPF on all its interfaces and port1 will be enable for asymmetric routing.
- C. The global configuration will take precedence and FortiGate will enable strict RPF 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 4

Refer to the exhibits.

Network diagram



Name: VIP-WEB-SERVER

Comments: Write a comment... 0/255

Color: Change

Network

Interface: WAN (port2)

Type: Static NAT

External IP address/range: 100.65.0.200

Map to:

IPv4 address/range: 10.0.11.50

Optional Filters

Port Forwarding

Protocol: TCP UDP SCTP ICMP

Port Mapping Type: One to one Many to many

External service port: 443

Map to IPv4 port: 4443

Firewall policies

Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
<input type="checkbox"/> Internet (1)	LAN (port4)	WAN (port2)	all	all	always	ALL	<input checked="" type="checkbox"/> ACCEPT		<input checked="" type="checkbox"/> NAT
<input type="checkbox"/> Web_Server_Access (2)	WAN (port2)	LAN (port4)	all	VIP-WEB-SERVER	always	HTTPS	<input checked="" type="checkbox"/> ACCEPT		<input checked="" type="checkbox"/> Disabled

A diagram of a FortiGate device connected to the network VIP object and firewall policy configurations are shown. 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. If the host 100.65.1.111 sends a TCP SYN packet on port 443 to 100.65.0.200. what will the source address, destination address, and destination port of the packet be at the time FortiGate forwards the packet to the destination?

- A. 10.0.11.254, 100.65.0.200. and 443, respectively
- B. 10.0.11.254, 10.0.15.50, and 4443. respectively
- C. 100.65.1.111, 10.0.11.50, and 4443. respectively
- D. 100.65.1.111, 10.0.11.50. and 443. respectively

Answer: C

NEW QUESTION 5

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 6

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 7

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? (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 8

An administrator manages a FortiGate model that supports NTurbo How does NTurbo acceleration enhance antivirus performance?

- A. For flow-based inspectio
- B. NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.
- C. For flow-based inspectio
- D. NTurbo creates two inspection sessions on the FortiGate device.
- E. For proxy-based inspectio
- F. NTurbo offloads traffic to the content processor.
- G. For proxy-based inspectio
- H. NTurbo buffers the whole file and then sends it to the antivirus engine.

Answer: A

NEW QUESTION 9

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 10

Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Choose two.)

- A. FortiSASE Firewall-as-a-Service (FWaaS)
- B. The proxy auto-configuration (PAC) file
- C. VPN policies
- D. FortiExtender

Answer: AC

NEW QUESTION 10

FortiGate is integrated with FortiAnalyzer and FortiManager.

When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

- A. Universally Unique Identifier
- B. Policy ID
- C. Sequence ID
- D. Log ID

Answer: A

NEW QUESTION 11

Refer to the exhibit.

Destination	Gateway IP	Interface	Status
0.0.0.0/0	100.65.0.254	port2	Enabled
10.10.10.0/24	100.66.0.254	port3	Enabled
10.0.13.0/24	10.0.13.125	port6	Enabled

Based on the routing table shown in the exhibit, which two statements are true? (Choose two.)

- A. A packet with the source IP address 10.0.13.10 arriving on port2 is allowed if strict RPF is disabled.
- B. A packet with the source IP address 10.100.110.10 arriving on port2 is allowed if strict RPF is enabled.
- C. A packet with the source IP address 10.100.110.10 arriving on port3 is allowed if strict RPF is disabled.
- D. A packet with the source IP address 10.10.10.10 arriving on port2 is allowed if strict RPF is enabled.

Answer: AC

NEW QUESTION 13

Which two statements are correct when FortiGate enters conserve mode? (Choose two answers)

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

Answer: BD

NEW QUESTION 16

Refer to the exhibits.

Application sensor

Edit Application Sensor

Categories

Mixed ▾ All Categories

Business (157, 📄 6)

Cloud/IT (72, 📄 12)

Collaboration (266, 📄 13)

Email (76, 📄 11)

Game (83)

General Interest (254, 📄 15)

Mobile (3)

Network Service (338)

Operational Technology

P2P (55)

Proxy (189)

Remote Access (96)

Social Media (113, 📄 29)

Storage/Backup (150, 📄 20)

Update (48)

Video/Audio (148, 📄 17)

VoIP (23)

Web Client (24)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

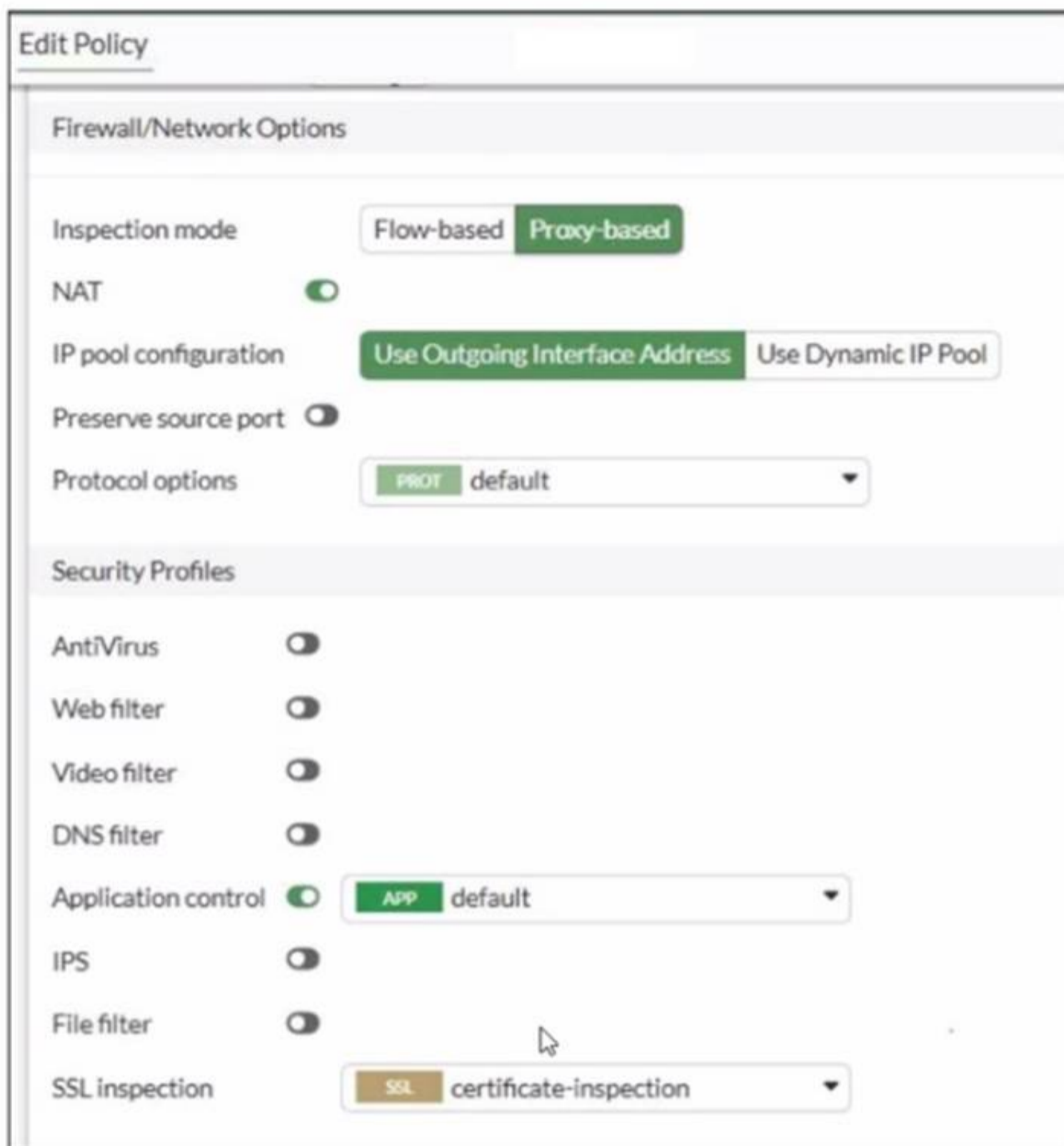
+ Create New
✎ Edit
🗑 Delete

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

Your Partner of IT Exam

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

Firewall policy



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 21

Which three statements explain a flow-based antivirus profile? (Choose three answers)

- A. FortiGate buffers the whole file but transmits to the client at the same time.
- B. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
- C. If a virus is detected, the last packet is delivered to the client.
- D. Flow-based inspection optimizes performance compared to proxy-based inspection.
- E. The IPS engine handles the process as a standalone.

Answer: ABD

NEW QUESTION 26

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	<input checked="" type="checkbox"/> Block
2	VEND Google	Filter	<input checked="" type="checkbox"/> 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 28

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 33

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 37

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors. What is the reason for the certificate warning errors?

- A. The option invalid SSL certificates is set to allow on the SSL/SSH inspection profile.
- B. The matching firewall policy is set to proxy inspection mode.
- C. The browser does not trust the certificate used by FortiGate for SSL inspection.
- D. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

Answer: C

NEW QUESTION 38

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 RA
- F. does not support the Antivirus scan feature.

Answer: B

NEW QUESTION 41

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	<input checked="" type="radio"/> Allow
Medicine	<input checked="" type="radio"/> Allow
News and Media	<input checked="" type="radio"/> Allow
Social Networking	<input checked="" type="radio"/> Allow
Political Organizations	<input checked="" type="radio"/> Allow
Reference	<input checked="" type="radio"/> Allow
Global Religion	<input checked="" type="radio"/> Allow
Shopping	<input checked="" type="radio"/> Allow
Society and Lifestyles	<input checked="" type="radio"/> 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

+ Create New
 Edit
 Delete

Search

URL	Type	Action	Status
www.facebook.com	Simple	<input type="radio"/> Monitor	<input checked="" type="checkbox"/> 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 45

Refer to the exhibit.
 A routing table is shown

Network	Gateway IP	Interfaces	Distance	Metric	Priority	Type
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
100.65.0.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Static
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only. What are the two criteria that the administrator can use to achieve this objective? (Choose two.)

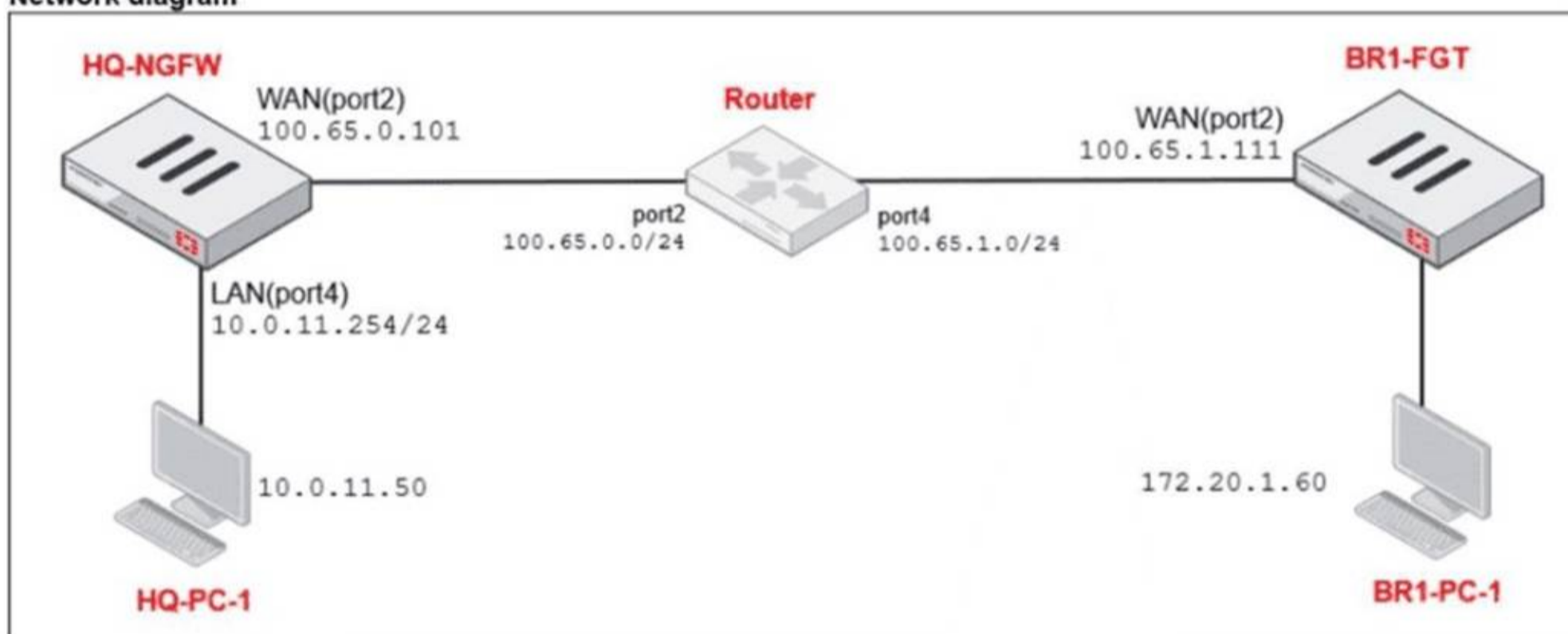
- A. The new static route must have the priority set to 3.
- B. The new static route must have the metric set to 1.
- C. The existing static route through port3 must have the distance set to 11.
- D. The new static route must have the distance set to 9

Answer: CD

NEW QUESTION 50

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 52

.....

Relate Links

100% Pass Your NSE4_FGT_AD-7.6 Exam with Exam Bible 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/>