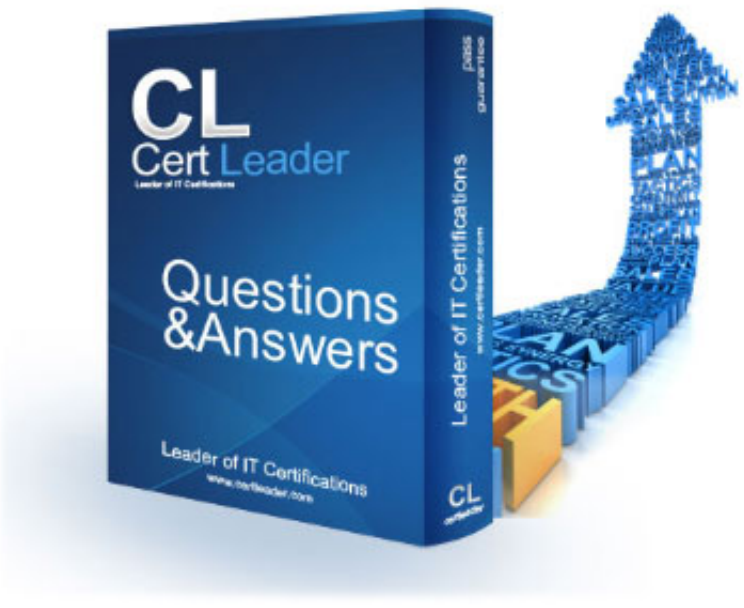
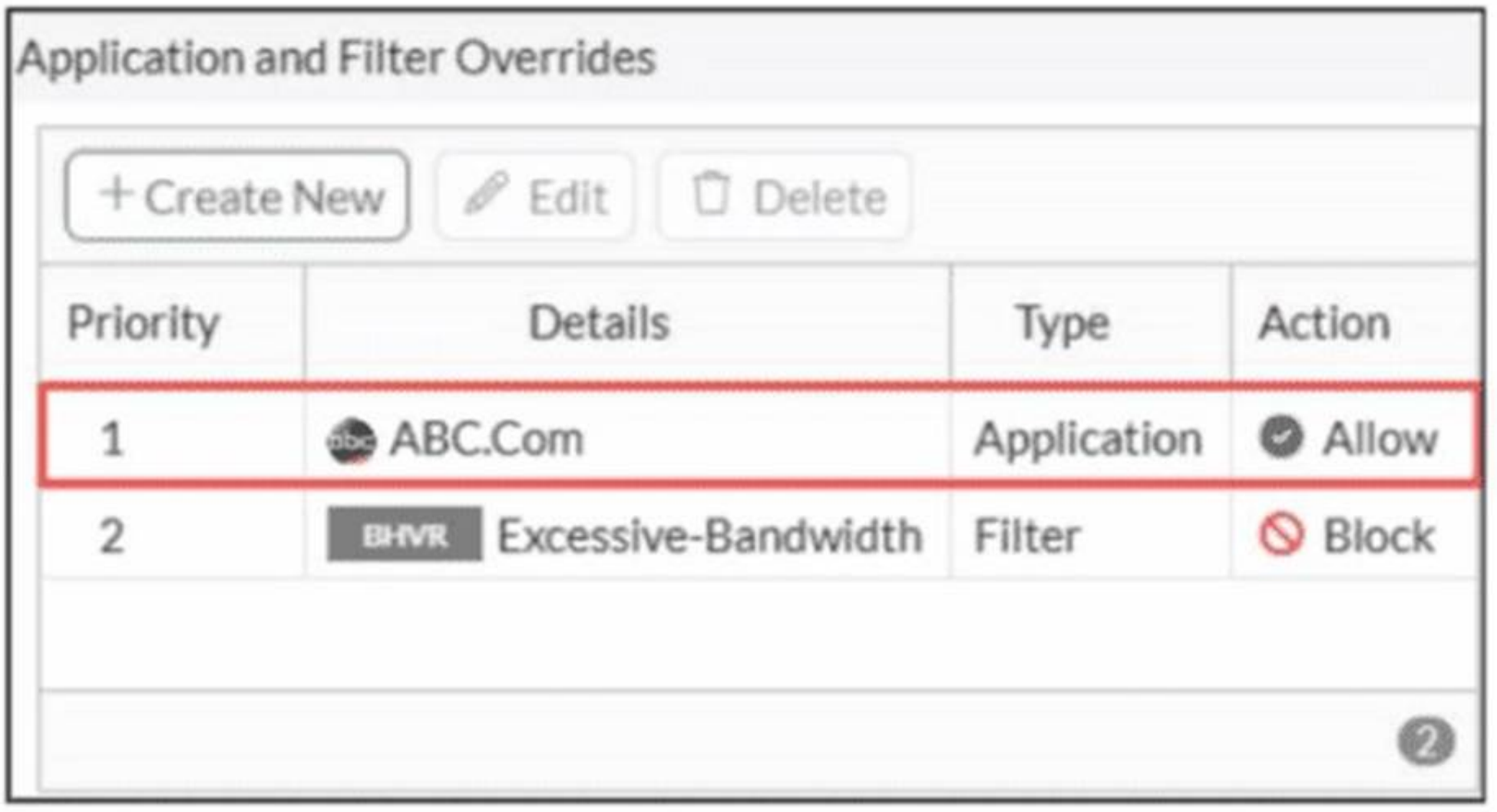
NSE4_FGT_AD-7.6 Dumps

Fortinet NSE 4 - FortiOS 7.6 Administrator

https://www.certleader.com/NSE4_FGT_AD-7.6-dumps.html



NEW QUESTION 1
Refer to the exhibit.



An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.
Why are there no logs generated under security logs for ABC.Com?

A. The ABC Com is hitting the category Excessive-Bandwidth.
B. The ABC.Com Type is set as Application instead of Filter.
C. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
D. The ABC Com Action is set to Allow

Answer: D

NEW QUESTION 2
Refer to the exhibit.

```
FortiGate # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract
\
Num. of servers : 1
Protocol        : https
Port            : 8888
Anycast         : Disable
Default servers : Not included

-=- Server List (Wed Sep 20 09:22:42 2023) -=-

IP                     Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost            Updated Time
10.0.1.241               -244      2 I        0                  122          0          0 Wed Sep 20 09:21:55 2023
```

Which two statements about the FortiGuard connection are true? (Choose two.)

A. The weight increases as the number of failed packets rises
B. You can configure unreliable protocols to communicate with FortiGuard Server.
C. FortiGate identified the FortiGuard Server using DNS lookup.
D. FortiGate is using the default port for FortiGuard communication.

Answer: AD

NEW QUESTION 3
Refer to the exhibit.

FortiGate SD-WAN zone configuration

An SD-WAN zone configuration on the FortiGate GUI is shown. Based on the exhibit, which statement is true?

A. The Underlay zone contains no member.
B. The virtual-wan-link and overlay zones can be deleted
C. The Underlay zone is the zone by default.
D. port2 and port3 are not assigned to a zone.

Answer: A

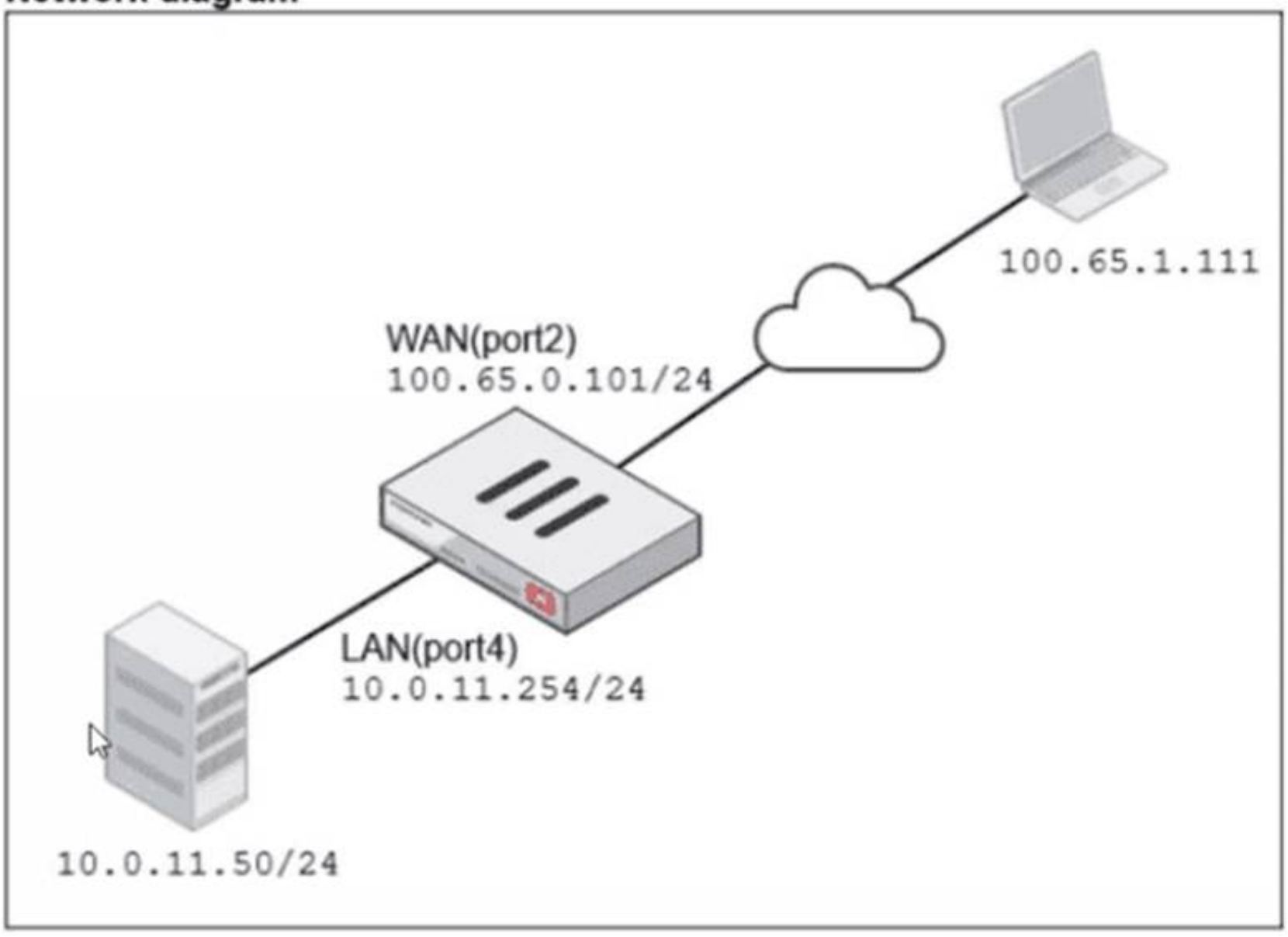
NEW QUESTION 4
There are multiple dialup IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels.
Which phase 1 setting you can configure to match the user to the tunnel?

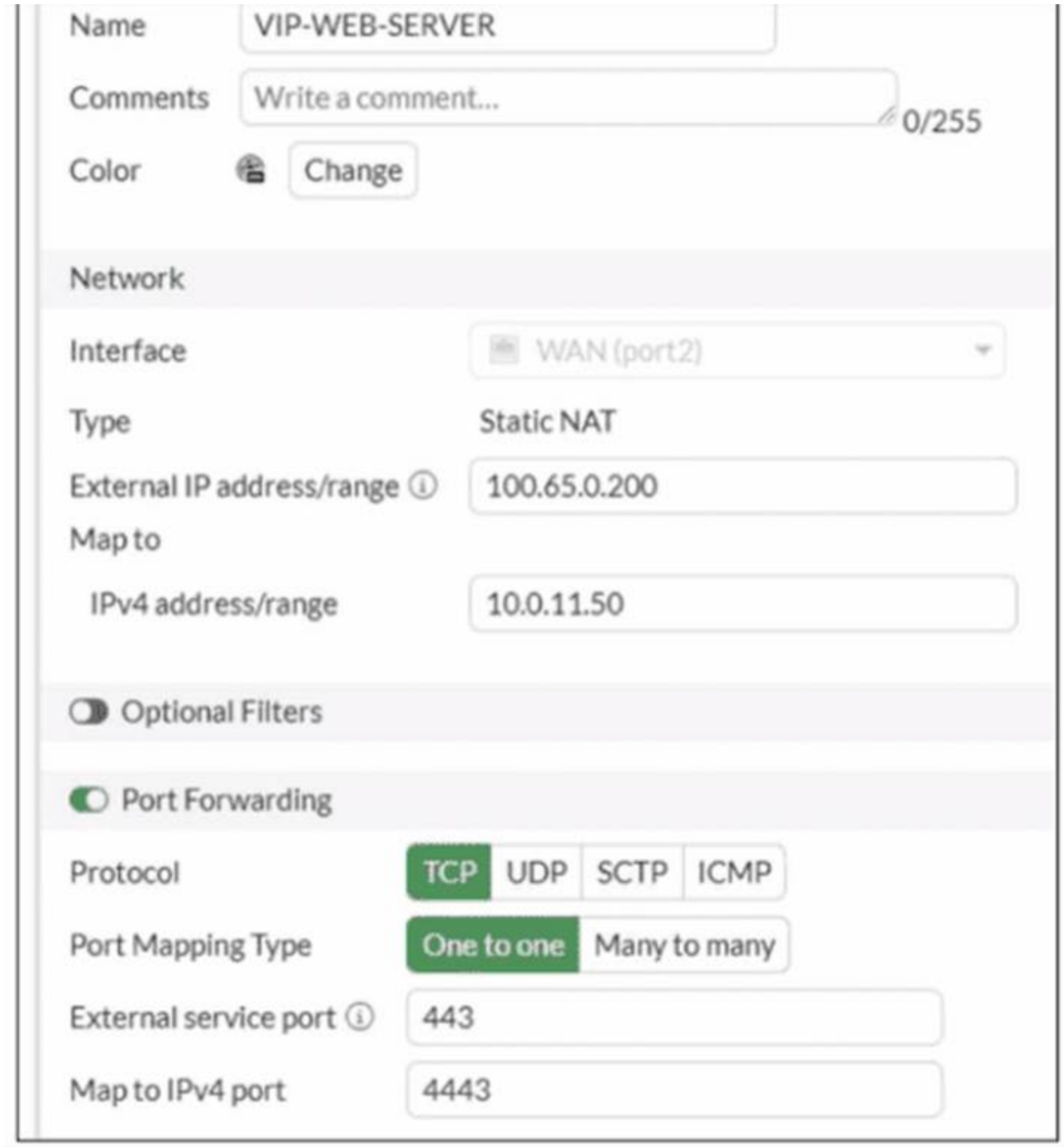
A. Local Gateway
B. Dead Peer Detection
C. Peer ID
D. IKE Mode Config

Answer: C

NEW QUESTION 5
Refer to the exhibits.

Network diagram





Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☐	Internet (1)	LAN (port4)	WAN (port2)	all	all	always	ALL	✓ ACCEPT		NAT
☐	Web_Server_Access (2)	WAN (port2)	LAN (port4)	all	VIP-WEB-SERVER	always	HTTPS	✓ ACCEPT		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. ill, 10.0.11.50, and 4443. respectively
D. 100.65.1.111, 10.0.11.50. and 443. respectively

Answer: C

NEW QUESTION 6
Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three answers)

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

Answer: ABD

NEW QUESTION 7
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 8
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

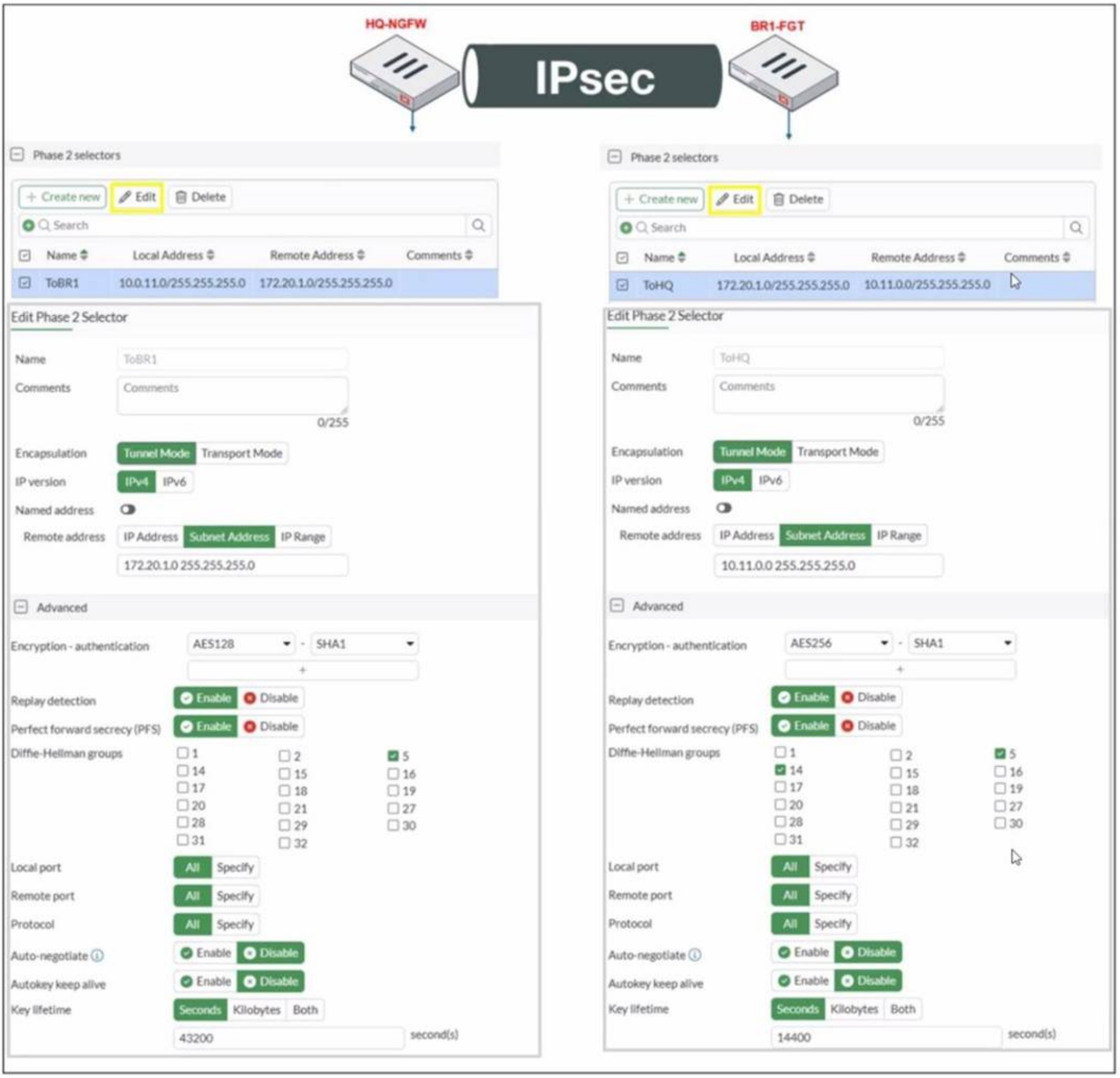
NEW QUESTION 9
An administrator manages a FortiGate model that supports NTurbo How does NTurbo acceleration enhance antivirus performance?

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 10
Refer to the exhibit.

IPsec tunnel configuration



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.
Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

A. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0.
B. On HQ-NGF
C. enable Diffie-Hellman Group 2.
D. On BR1-FG
E. set Seconds to 43200
F. On HQ-NGF
G. set Encryption to AES256.

Answer: AD

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 15
Which two statements are true about an HA cluster? (Choose two answers)

A. An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.
B. Link failover triggers a failover if the administrator sets the interface down on the primary device.
C. When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.
D. HA incremental synchronization includes FIB entries and IPsec SAs.

Answer: BD

NEW QUESTION 17
An administrator wanted to configure an IPS sensor to block traffic that triggers the signature set number of times during a specific time period. How can the administrator achieve the objective?

A. Use IPS group signatures, set rate-mode 60.
B. Use IPS packet logging option with periodical filter option.
C. Use IPS signatures, rate-mode periodical option.
D. Use IPS filter, rate-mode periodical option.

Answer: D

NEW QUESTION 22
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 25
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 26
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 29
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 34
What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device? (Choose two.)

A. Heartbeat IP addresses are used to distinguish between cluster members.
B. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.
C. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.
D. Heartbeat interfaces have virtual IP addresses that are manually assigned.

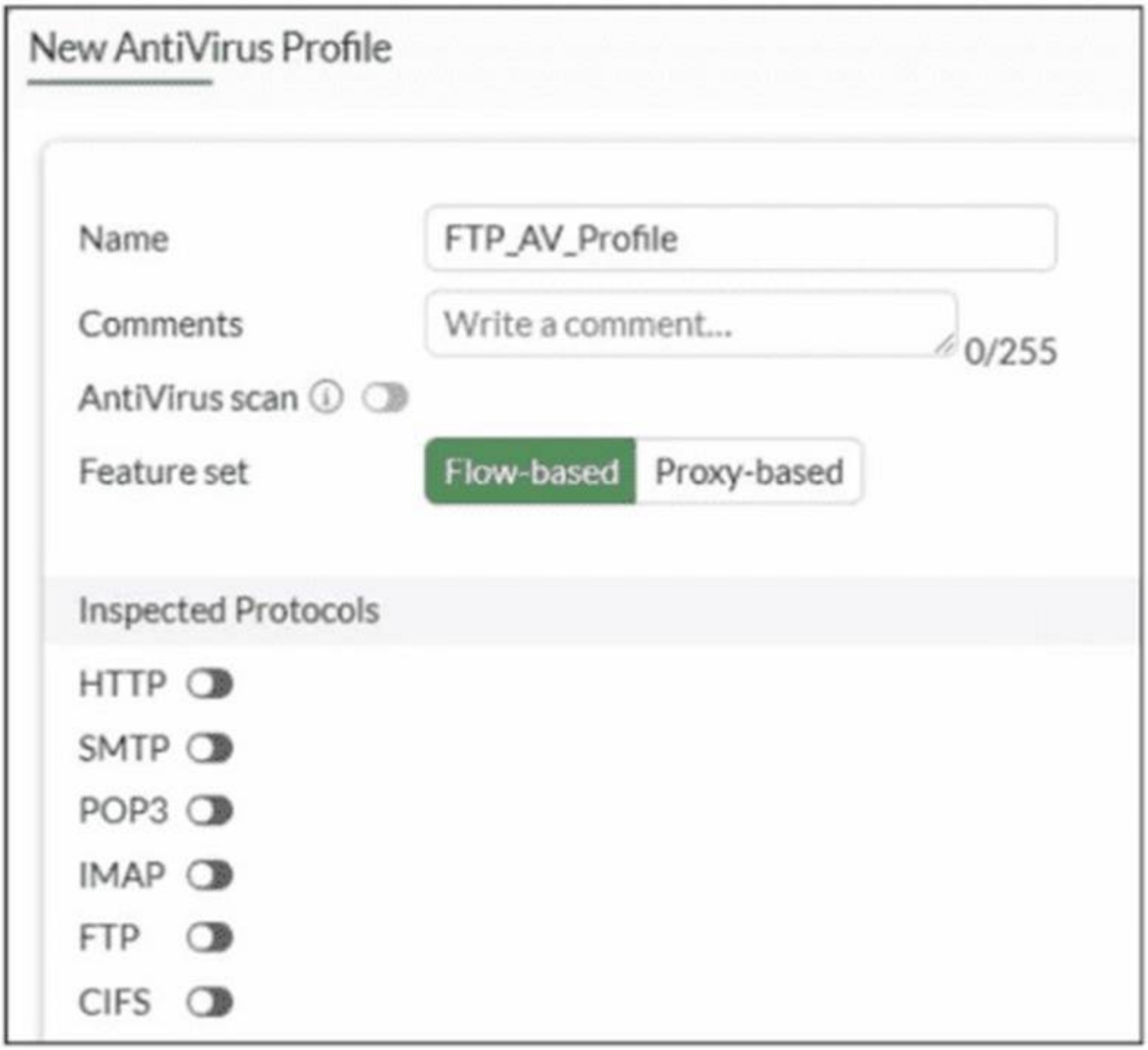
Answer: AC

NEW QUESTION 39
An administrator has configured a dialup IPsec VPN on FortiGate with add-route enabled. However, the static route is not showing in the routing table. Which two statements about this scenario are correct? (Choose two.)

A. The administrator must use a policy route instead of a static route for add-route to work properly.
B. The administrator must ensure phase 2 is successfully established
C. The administrator must define the remote network correctly in the phase 2 selectors.
D. The administrator must enable a dynamic routing protocol on the dialup interface.

Answer: BC

NEW QUESTION 44
Refer to the exhibit.



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 45
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" poluuid="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 50
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 52
Refer to the exhibit
A firewall policy to enable active authentication is shown.

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 55
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4_FGT_AD-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT_AD-7.6-dumps.html