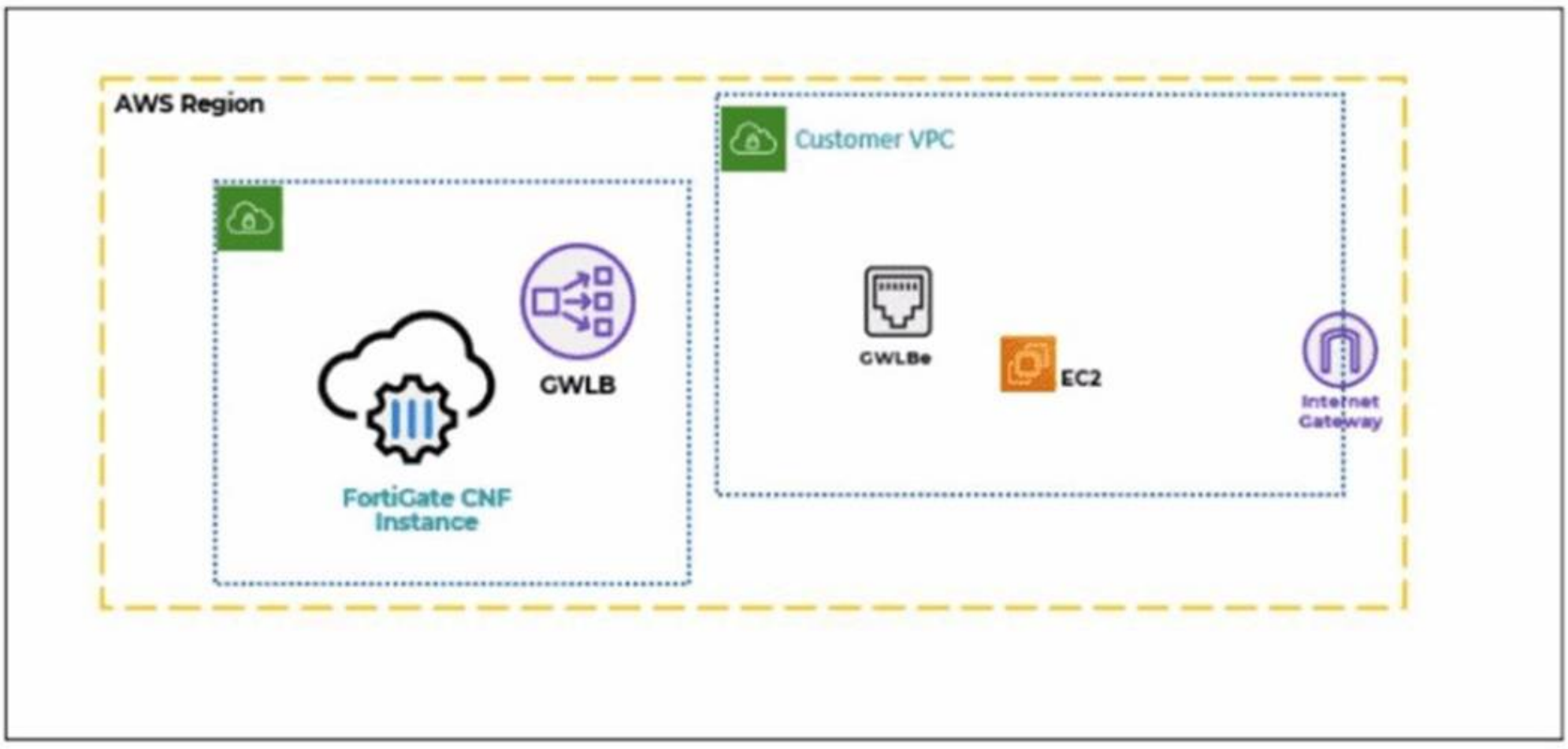

# Fortinet

## Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

**NEW QUESTION 1**
Refer to the exhibit.
A partial cloud topology is shown.

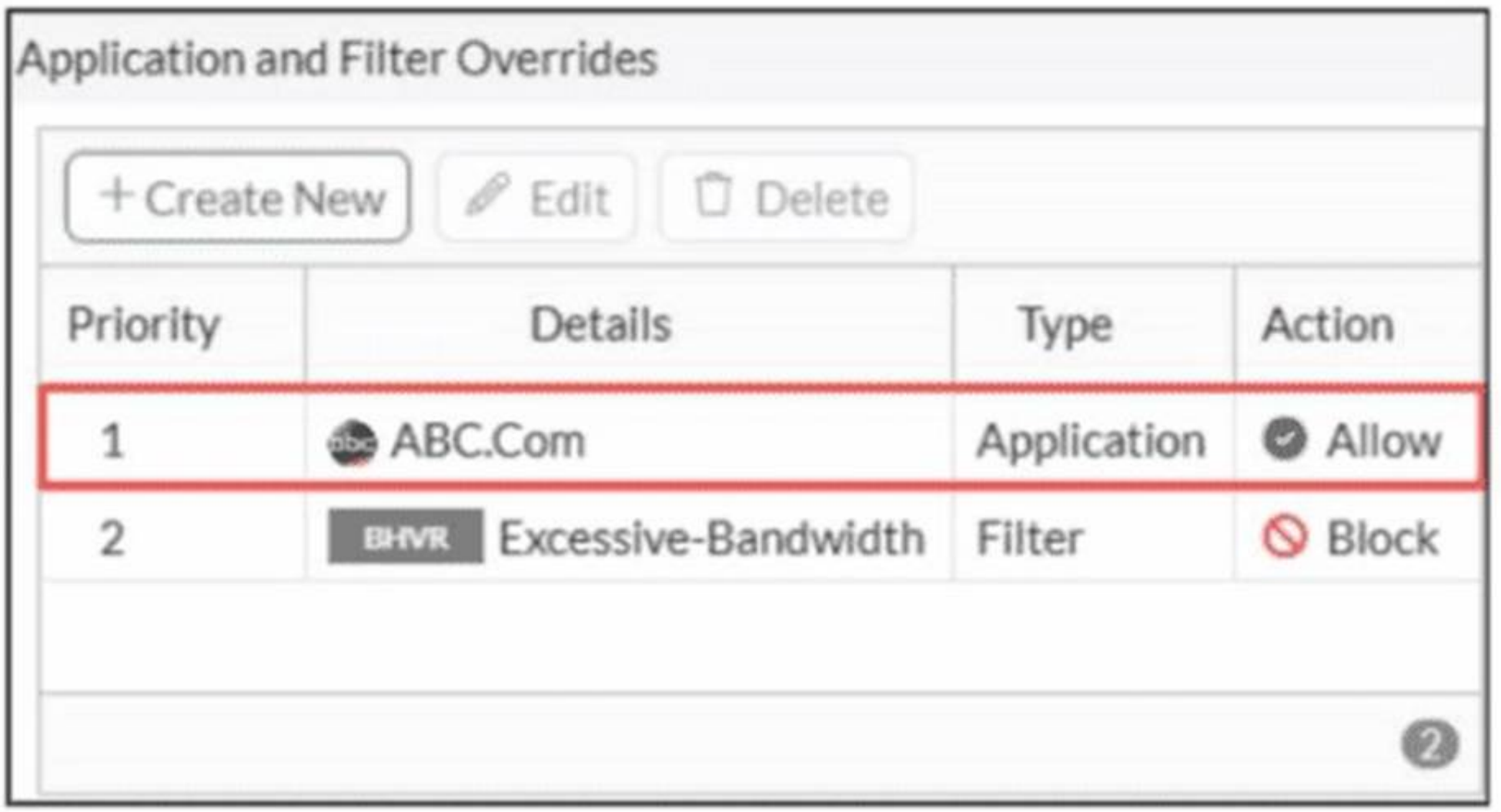



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.
During the deployment, which components must the FortiGate CNF create to handle traffic from the EC2 instance?

A. The customer VPC and GWLBe
B. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)
C. The CNF VP
D. customer VP
E. and GWLB
F. The GWL
G. GWLBe, and the internet gateway (IGW) in the customer VPC

**Answer:** B

**NEW QUESTION 2**
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

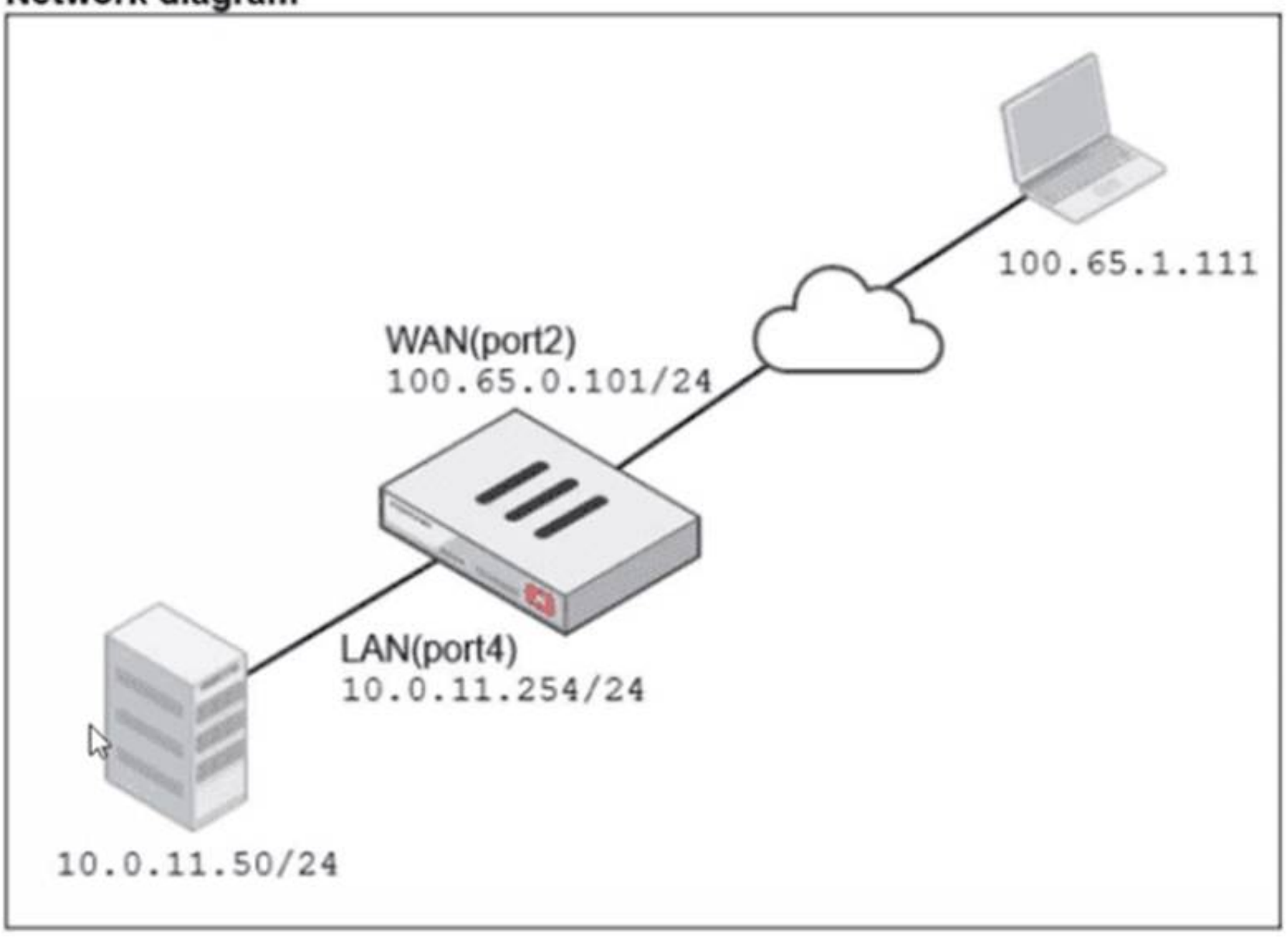
**NEW QUESTION 3**
There are multiple dialup IPsec VPNs configured in aggressive mode on the HQ FortiGate. The requirement is to connect dial-up users to their respective department VPN tunnels.
Which phase 1 setting you can configure to match the user to the tunnel?

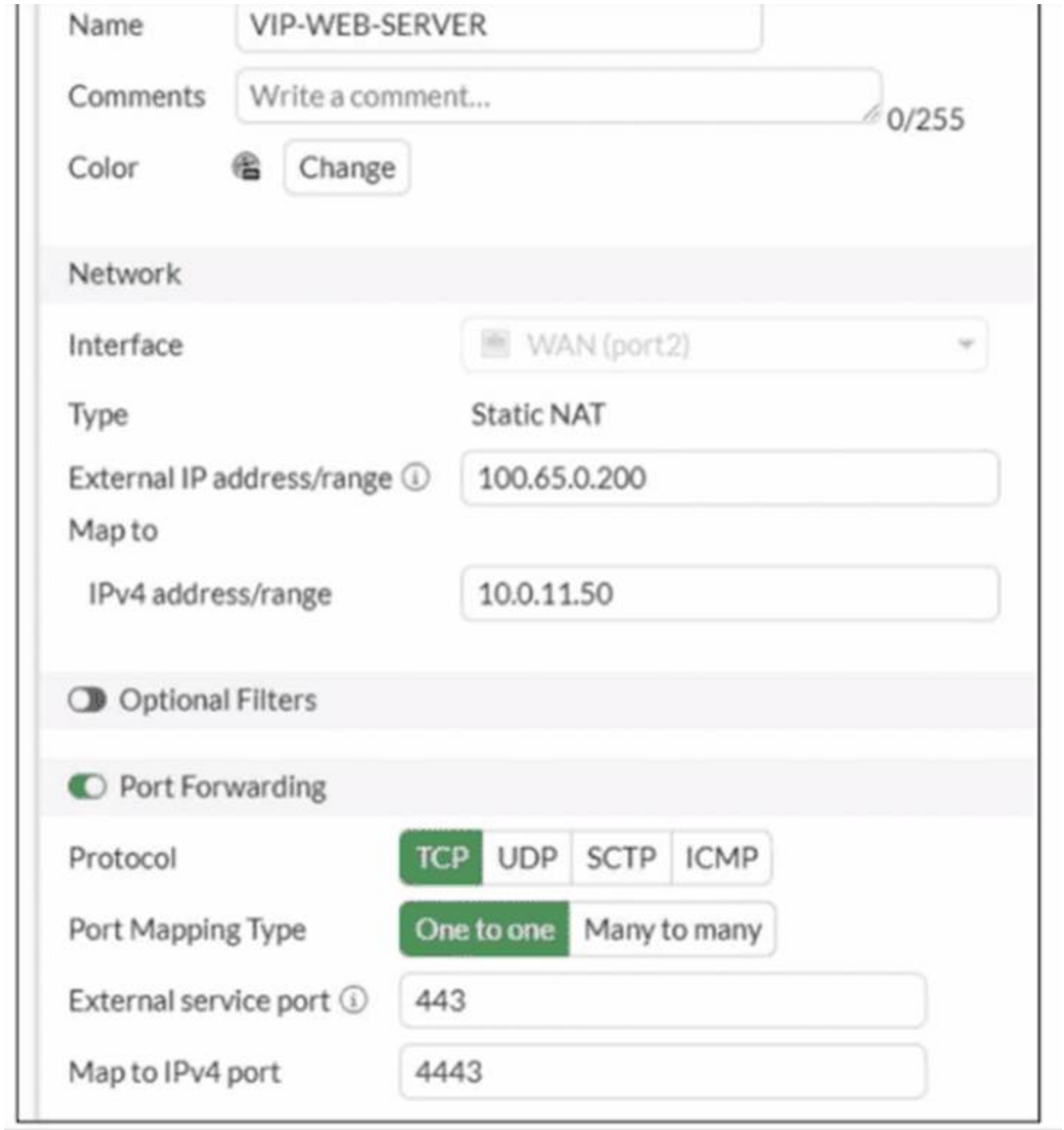
A. Local Gateway
B. Dead Peer Detection
C. Peer ID
D. IKE Mode Config

**Answer:** C

**NEW QUESTION 4**
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

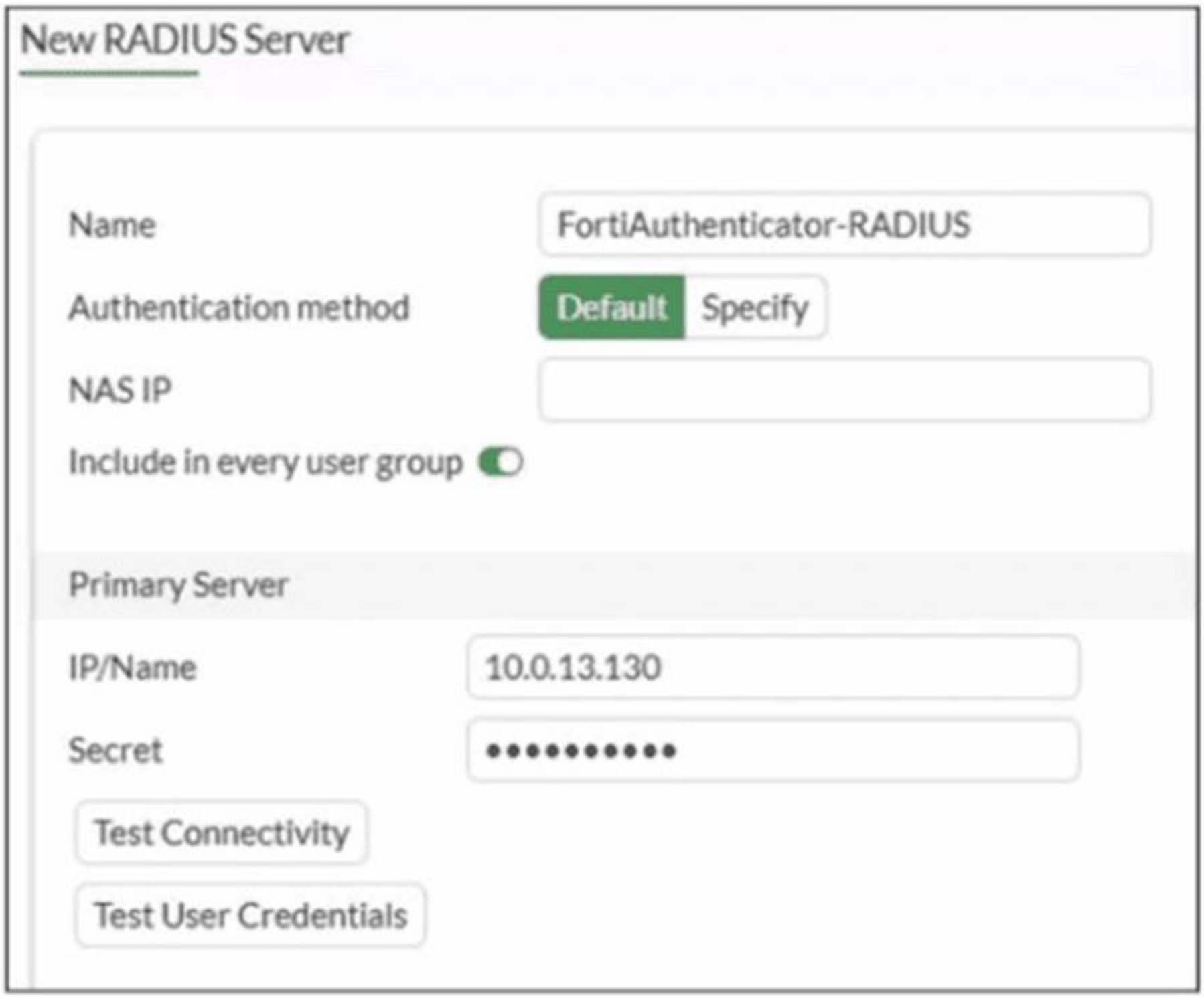
**NEW QUESTION 5**
An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.
Which DPD mode on FortiGate meets this requirement?

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

**Answer:** A

**NEW QUESTION 6**

Refer to the exhibit.
A RADIUS server configuration is shown.




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 7**
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

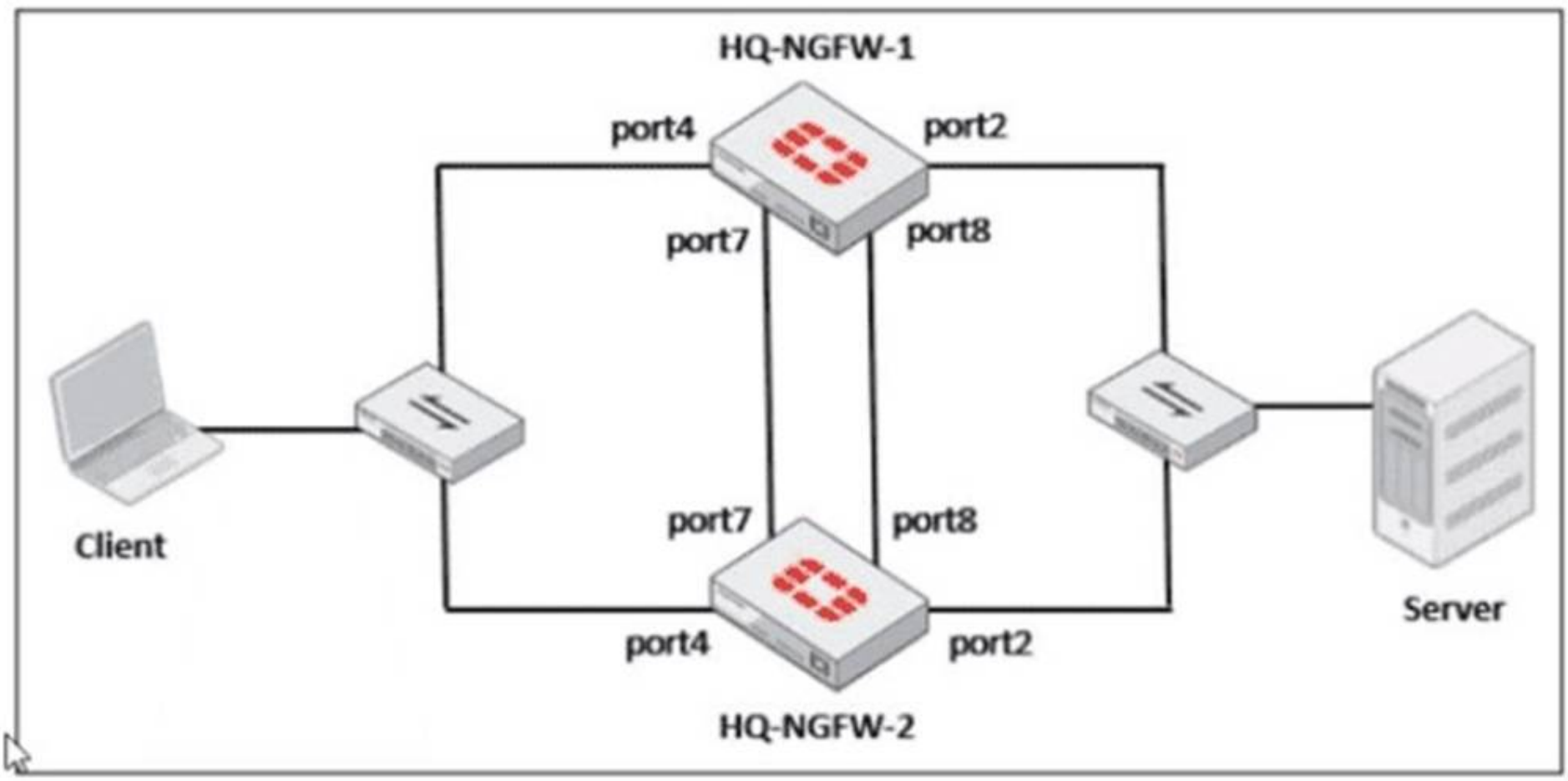
**NEW QUESTION 8**
A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is not part of the expected process?

A. The DC agent sends login event data directly to FortiGate.
B. FortiGate determines user identity based on the IP address in the FSSO list.
C. The collector agent forwards login event data to FortiGate.
D. The user logs into the windows domain.

**Answer:** A

**NEW QUESTION 9**
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"
```

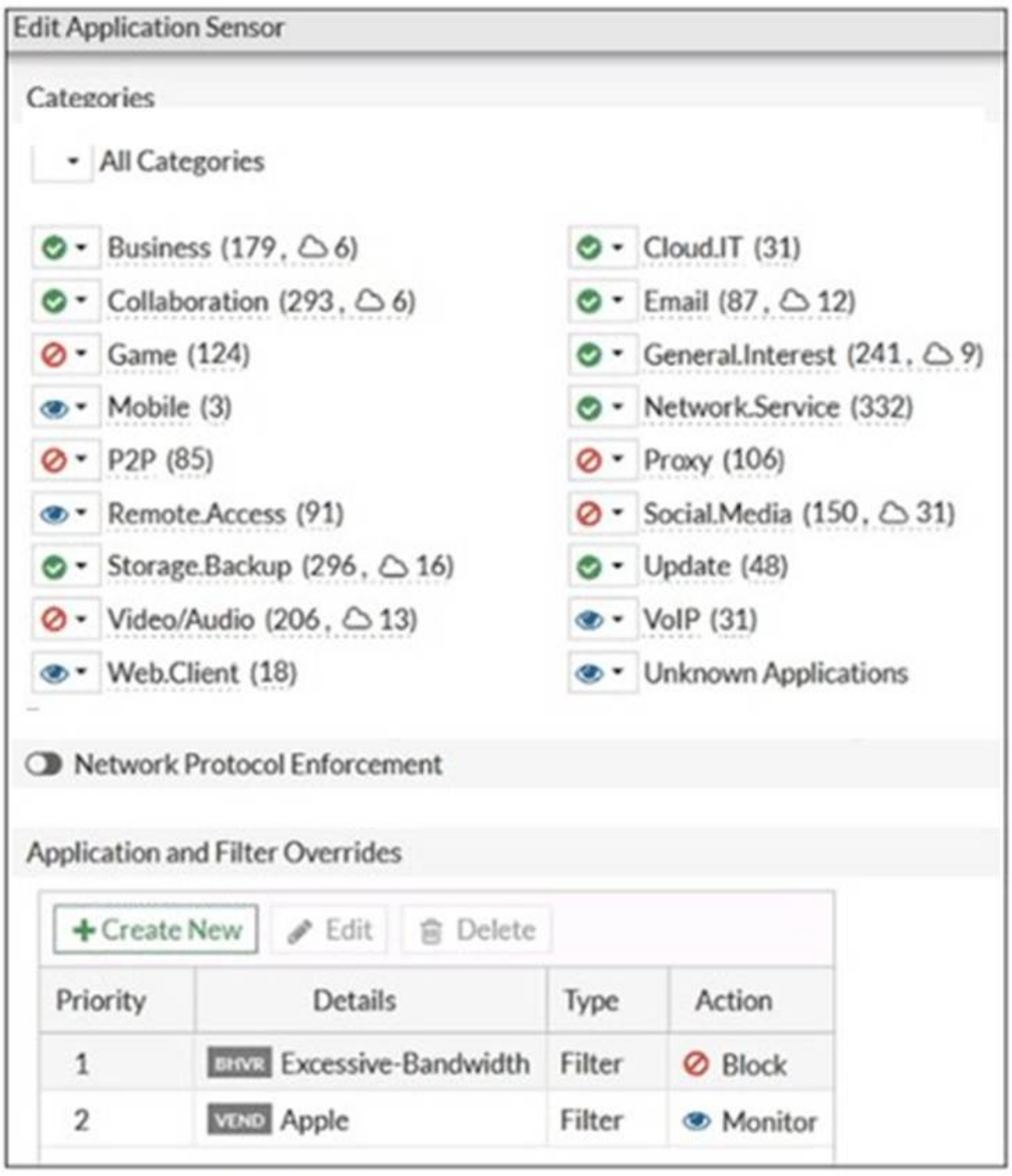
Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibits.
What would be the expected outcome in the HA cluster?

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.

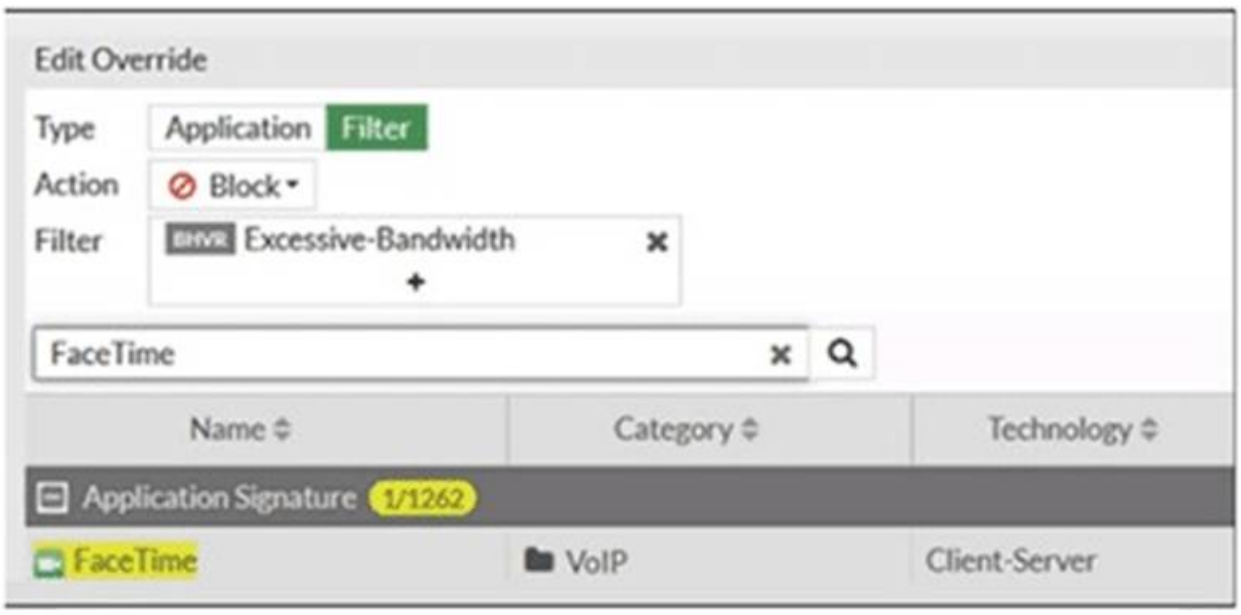
**Answer:** A

**NEW QUESTION 10**
Refer to the exhibits.

**Application sensor configuration**




**Application override configuration**




**Filter override configuration**

The exhibits show the application sensor configuration and the Excessive-Bandwidth and Apple filter details. Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming? (Choose one answer)

A. Apple FaceTime will be allowed, based on the Video/Audio category configuration.
B. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration.
C. Apple FaceTime will be allowed, based on the Apple filter configuration.
D. Apple FaceTime will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

**Answer:** B

**NEW QUESTION 10**
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 14**
An administrator wants to form an HA cluster using the FGCP protocol.
Which two requirements must the administrator ensure both members fulfill? (Choose two.)

A. They must have the same hard drive configuration.
B. They must have the same number of configured VDOMs.
C. They must have the heartbeat interfaces in the same subnet
D. They must have the same HA group ID.

**Answer:** BD

**NEW QUESTION 15**
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 20**
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 immediatel
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 23**
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

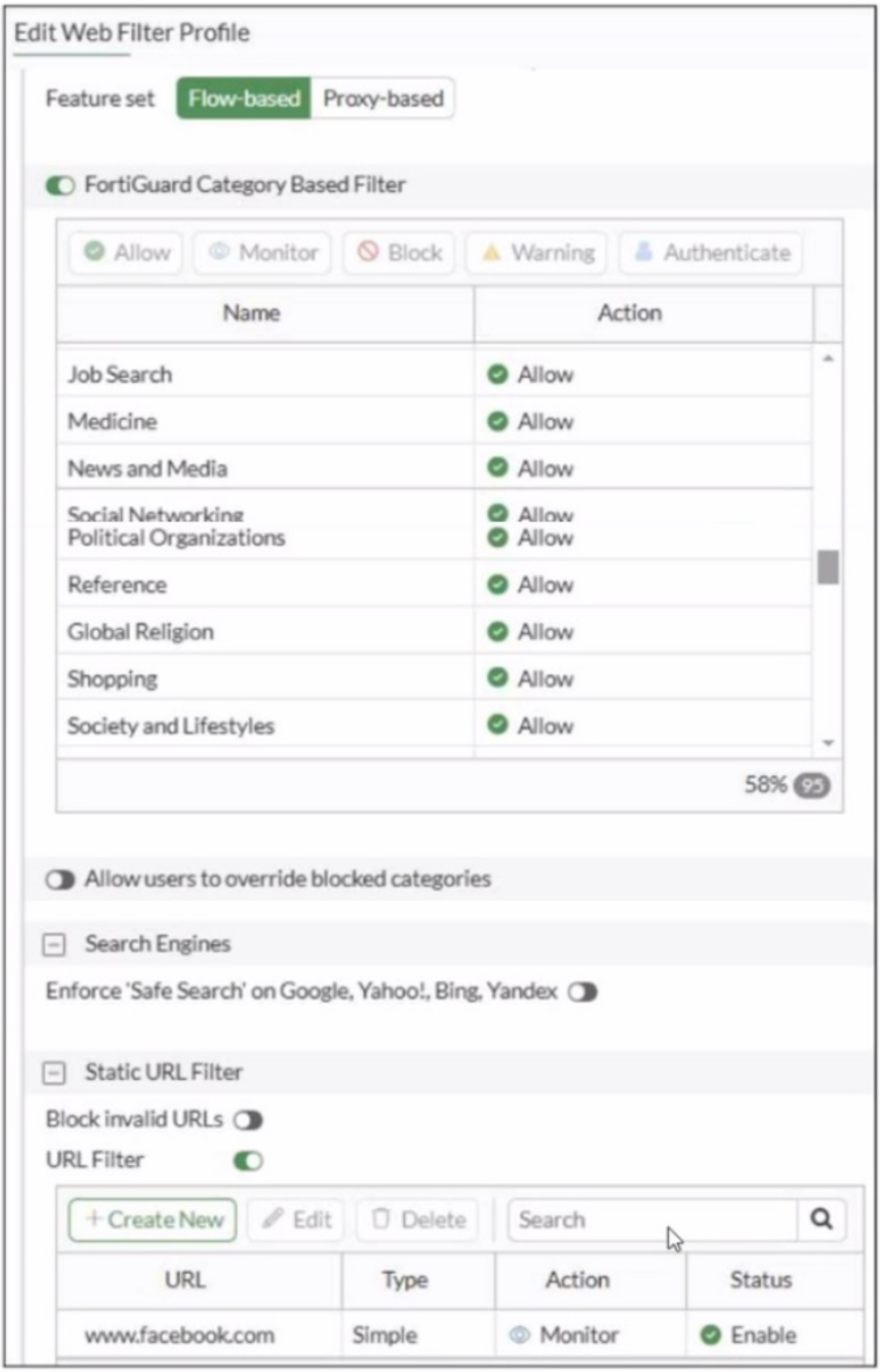
**NEW QUESTION 26**
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

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.

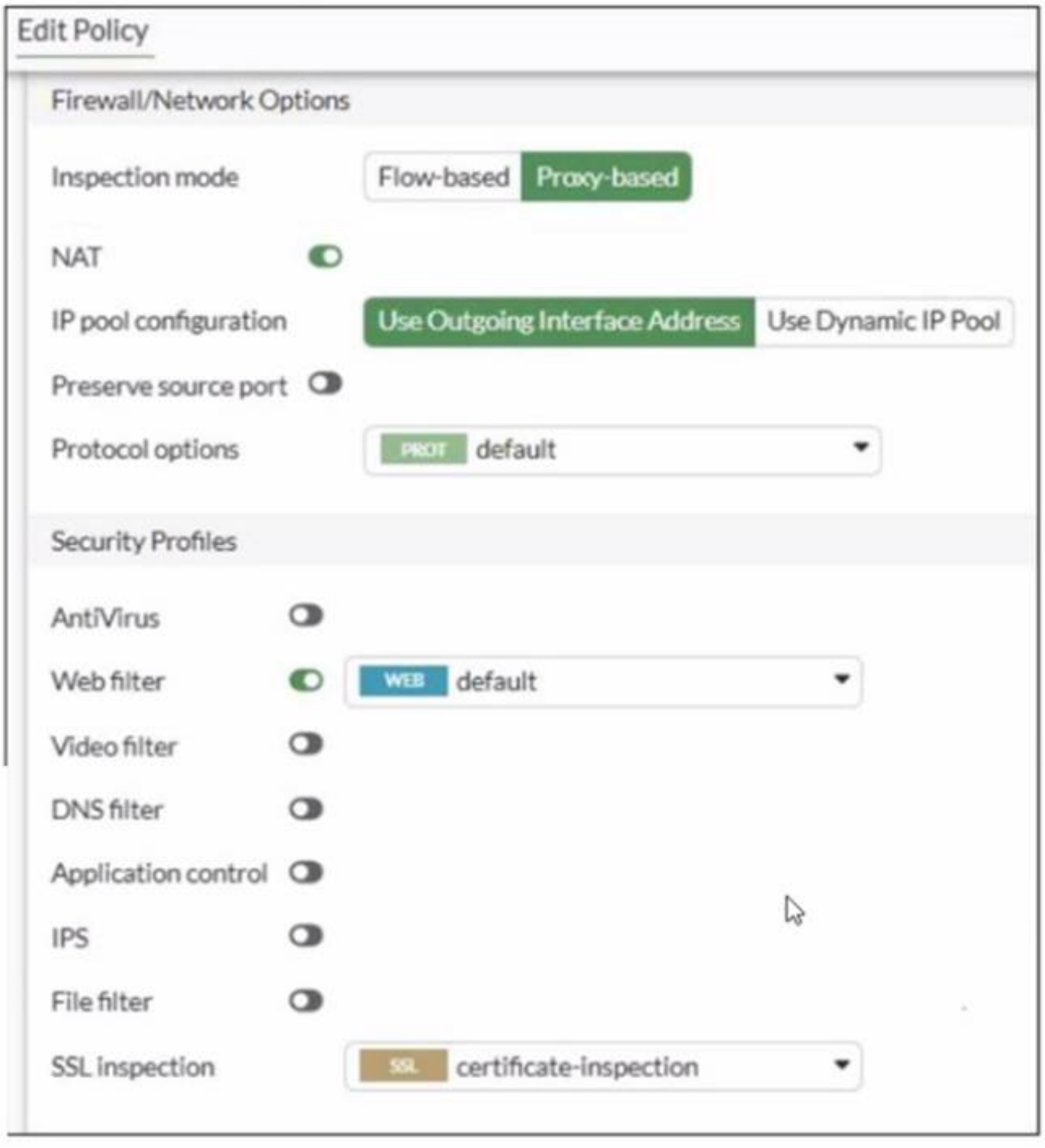
**Answer:** B

**NEW QUESTION 29**
Refer to the exhibits.

**Web filter profile configuration**



**Firewall policy configuration**




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 31**
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 |

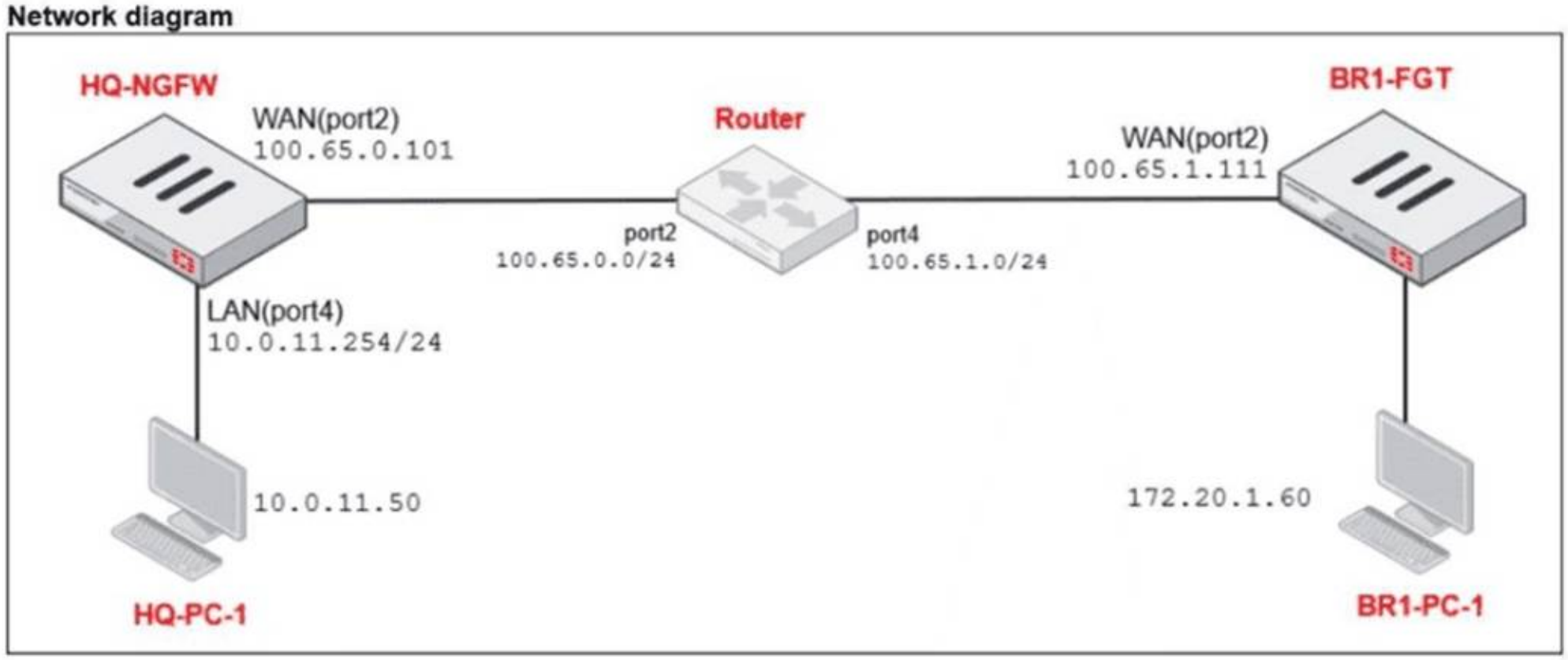
An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only. What are the two criteria that the administrator can use to achieve this objective? (Choose two.)

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 32**
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 37**
.....

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons 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 FirstTry

* NSE4_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year