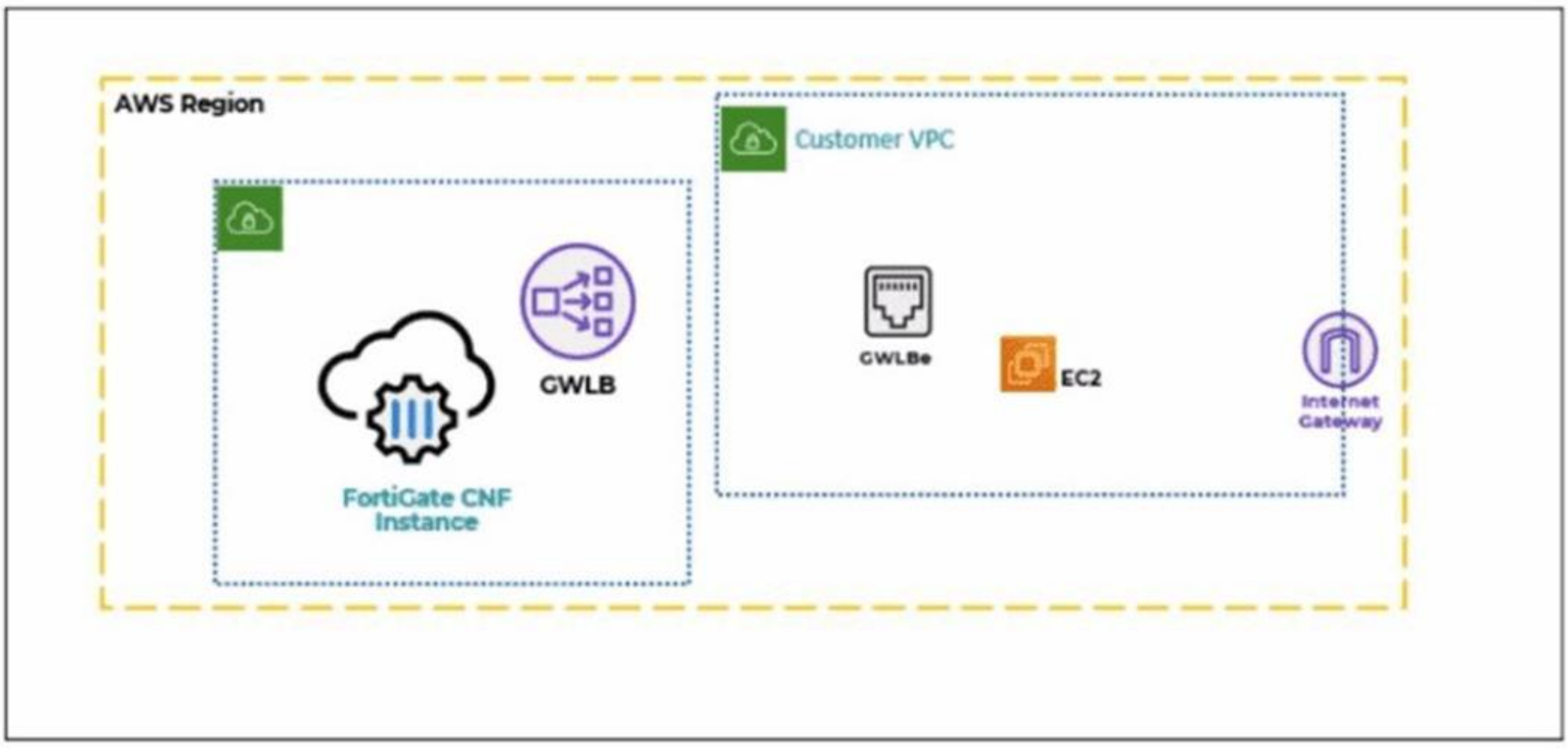
Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

https://www.2passeasy.com/dumps/NSE4_FGT_AD-7.6/

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

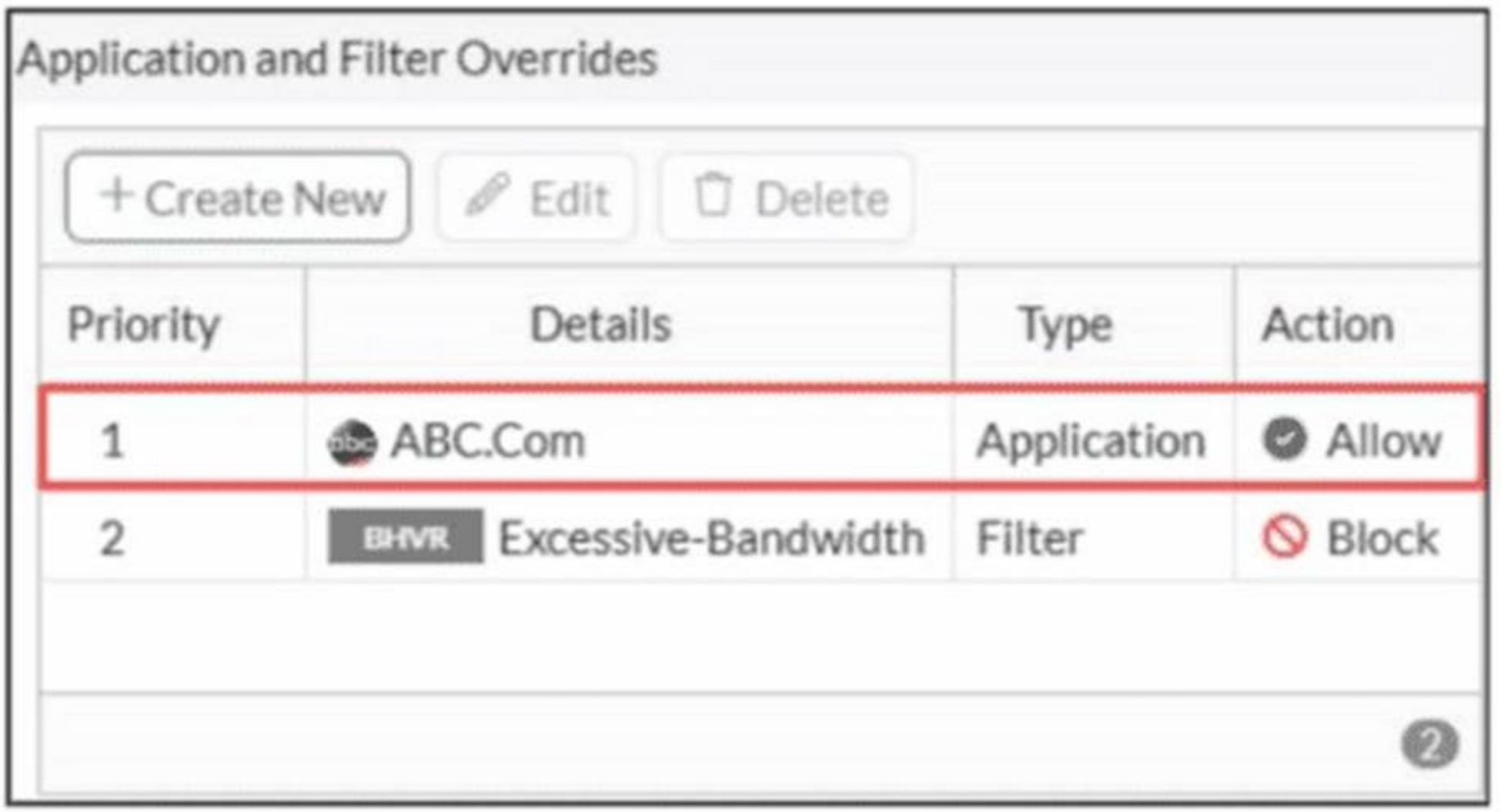


You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.
During the deployment, which components must the FortiGate CNF create to handle traffic from the EC2 instance?

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.



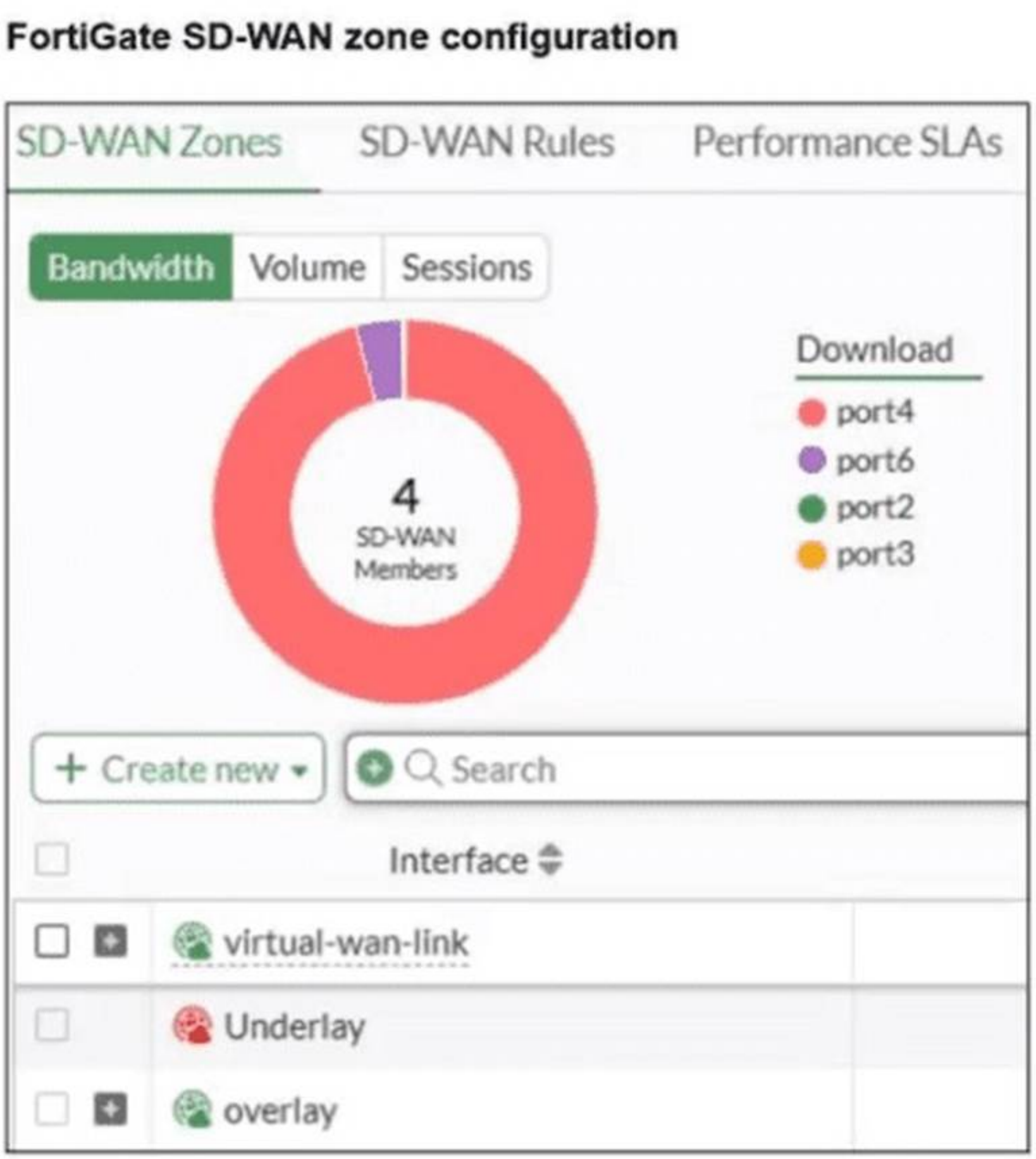
An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, 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
Refer to the exhibit.



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
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.

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 7
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.)

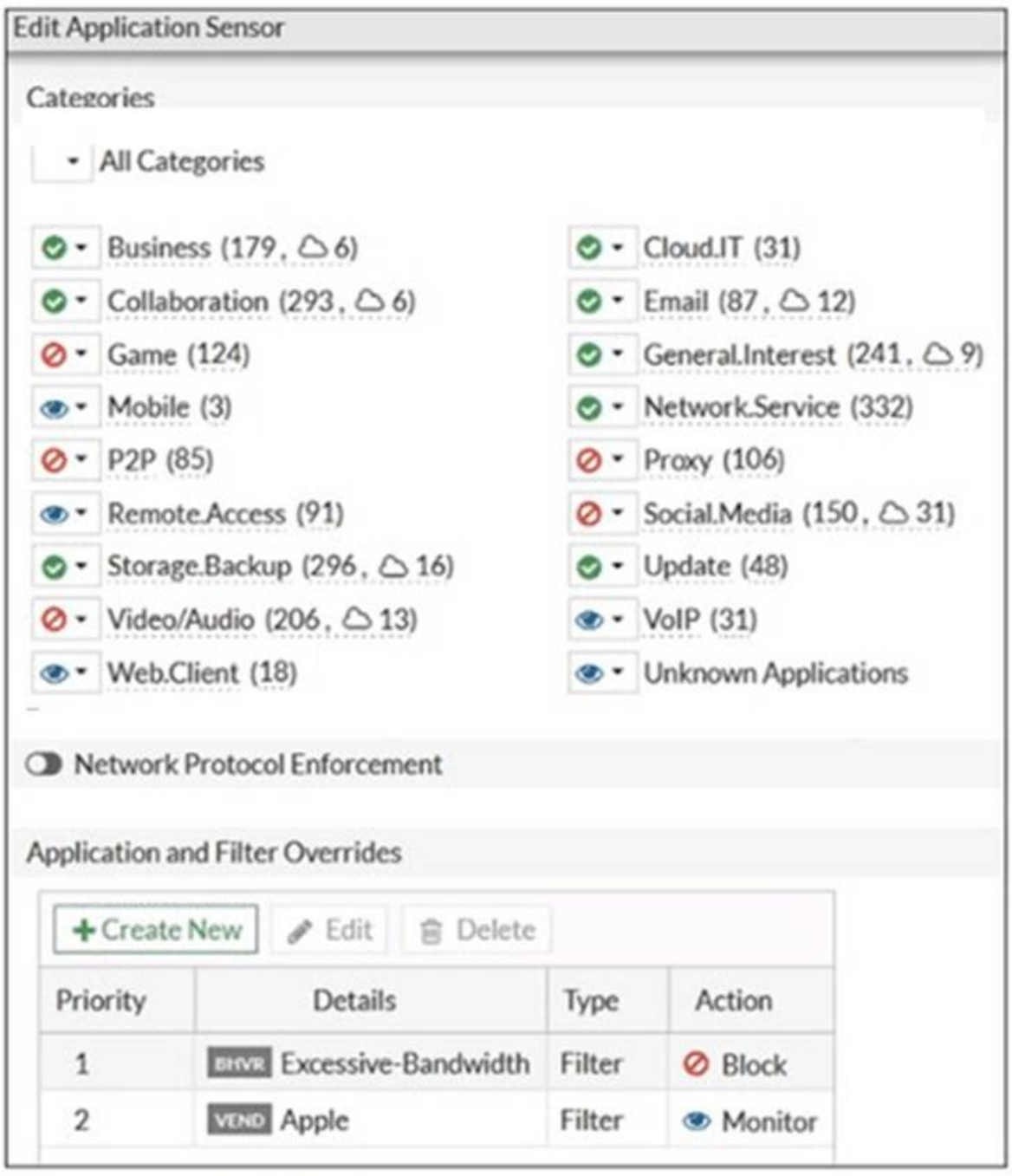
A. A packet with the source IP address 10.0.13.10 arriving on port2 is allowed if strict RPF is disabled.
B. A packet with the source IP address 10.100.110.10 arriving on port2 is allowed if strict RPF is enabled.

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.

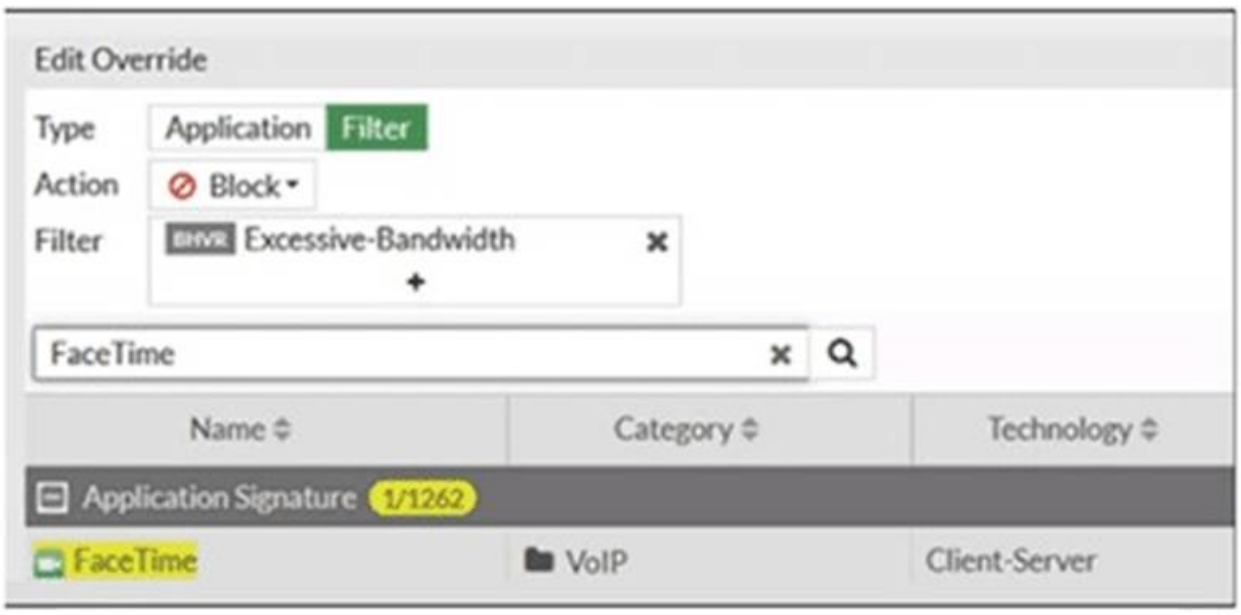
Answer: AC

NEW QUESTION 8
Refer to the exhibits.

Application sensor configuration



Application override configuration



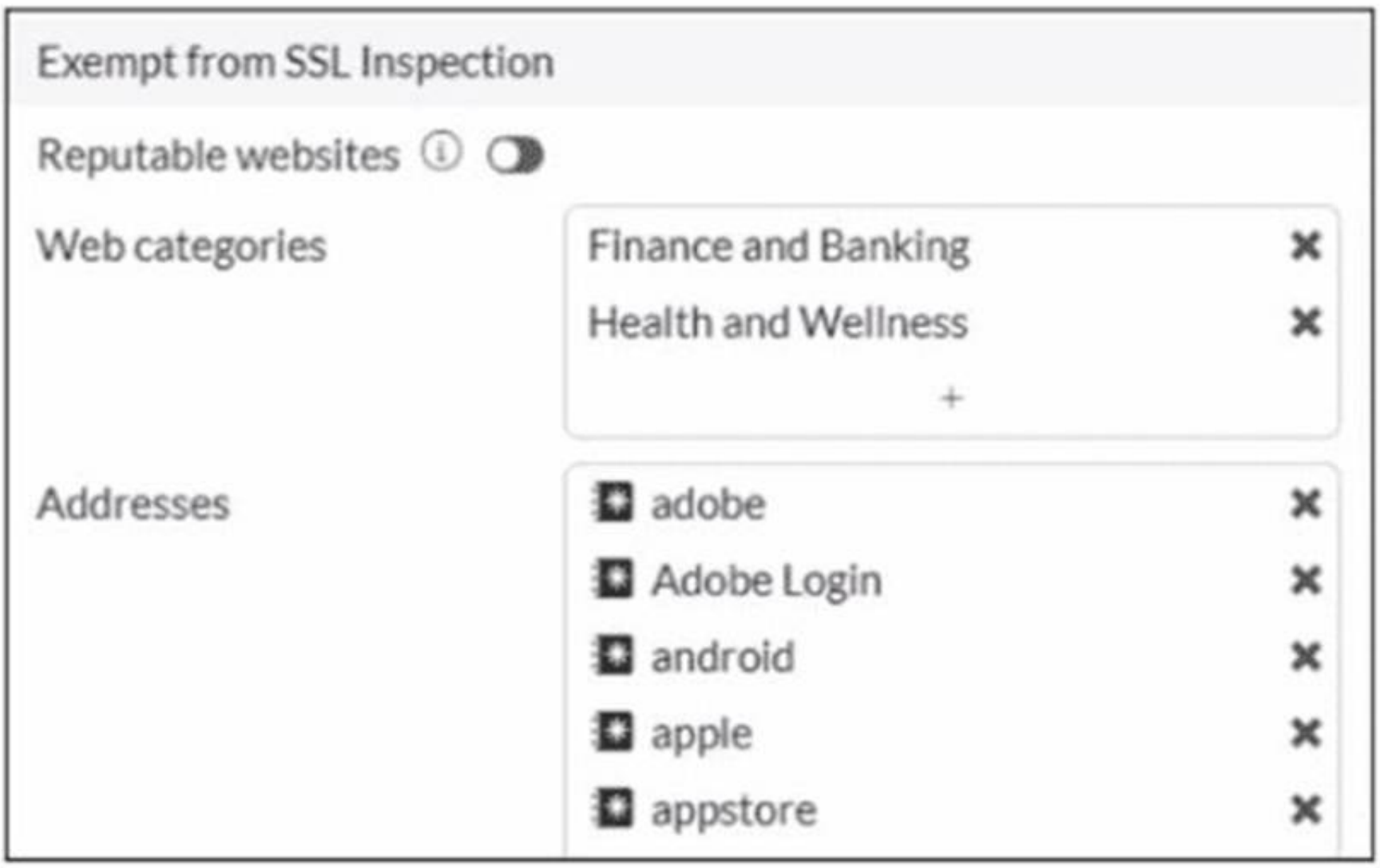
Filter override configuration

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 9
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 10
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

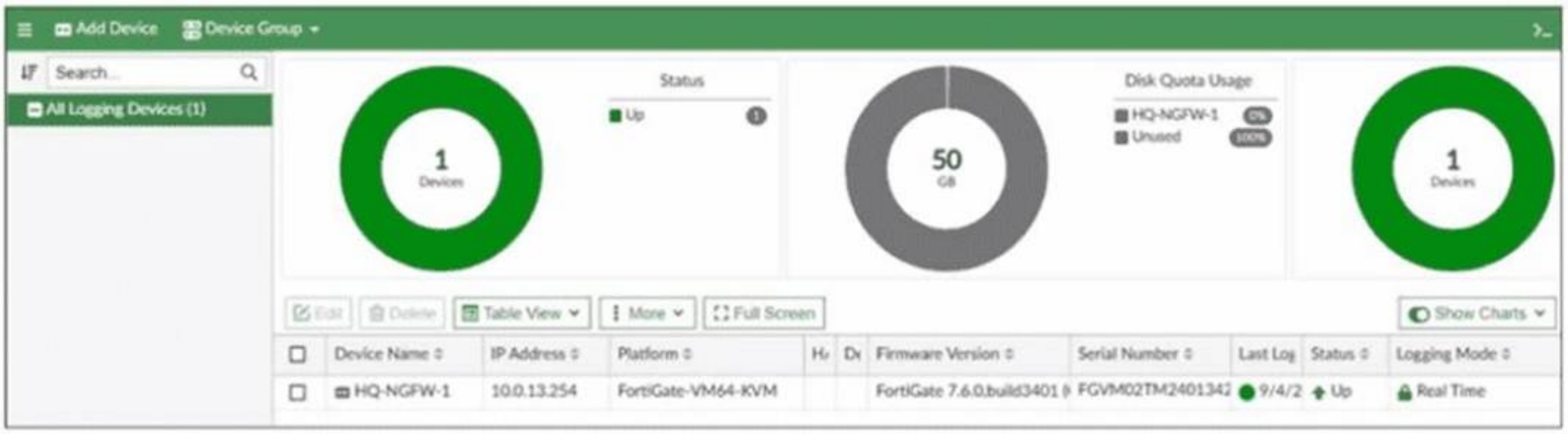
NEW QUESTION 10
An administrator wants to form an HA cluster using the FGCP protocol.
Which two requirements must the administrator ensure both members fulfill? (Choose two.)

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 14
The FortiGate device HQ-NGFW-1 with the IP address 10.0.13.254 sends logs to the FortiAnalyzer device with the IP address 10.0.13.125. The administrator

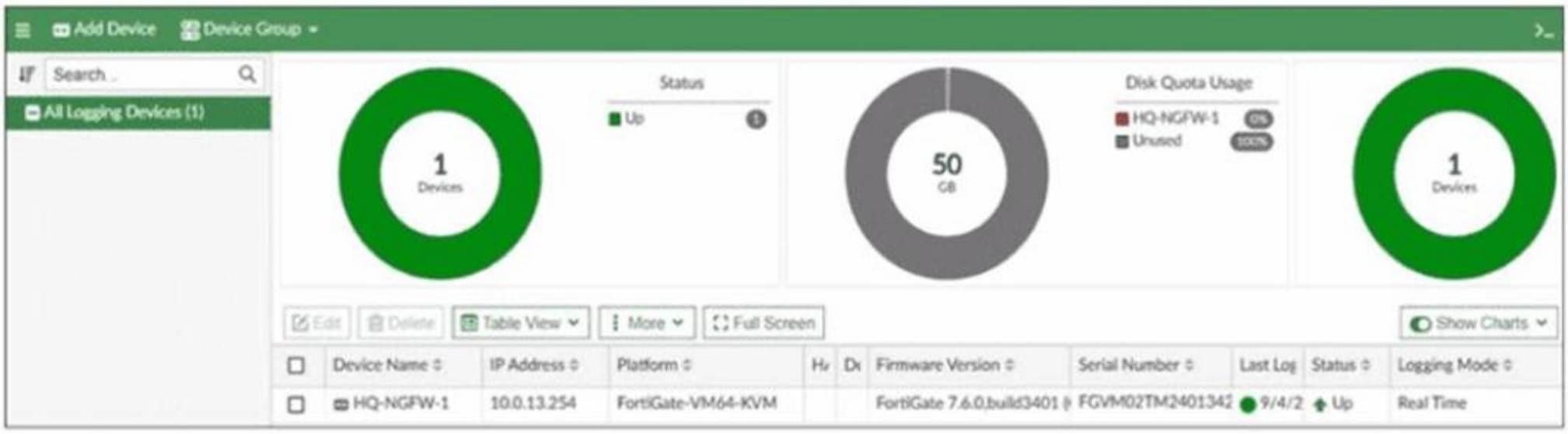
wants to verify that reliable logging is enabled on HQ-NGFW-1.
Which exhibit helps with the verification?
A)



B)

```
config log fortianalyzer setting
     set status enable
     set server "10.0.13.125"
     set serial "FAZ-VMTM24012176"
     set enc-algorithm high-medium
     set upload-option realtime
end
```

C)



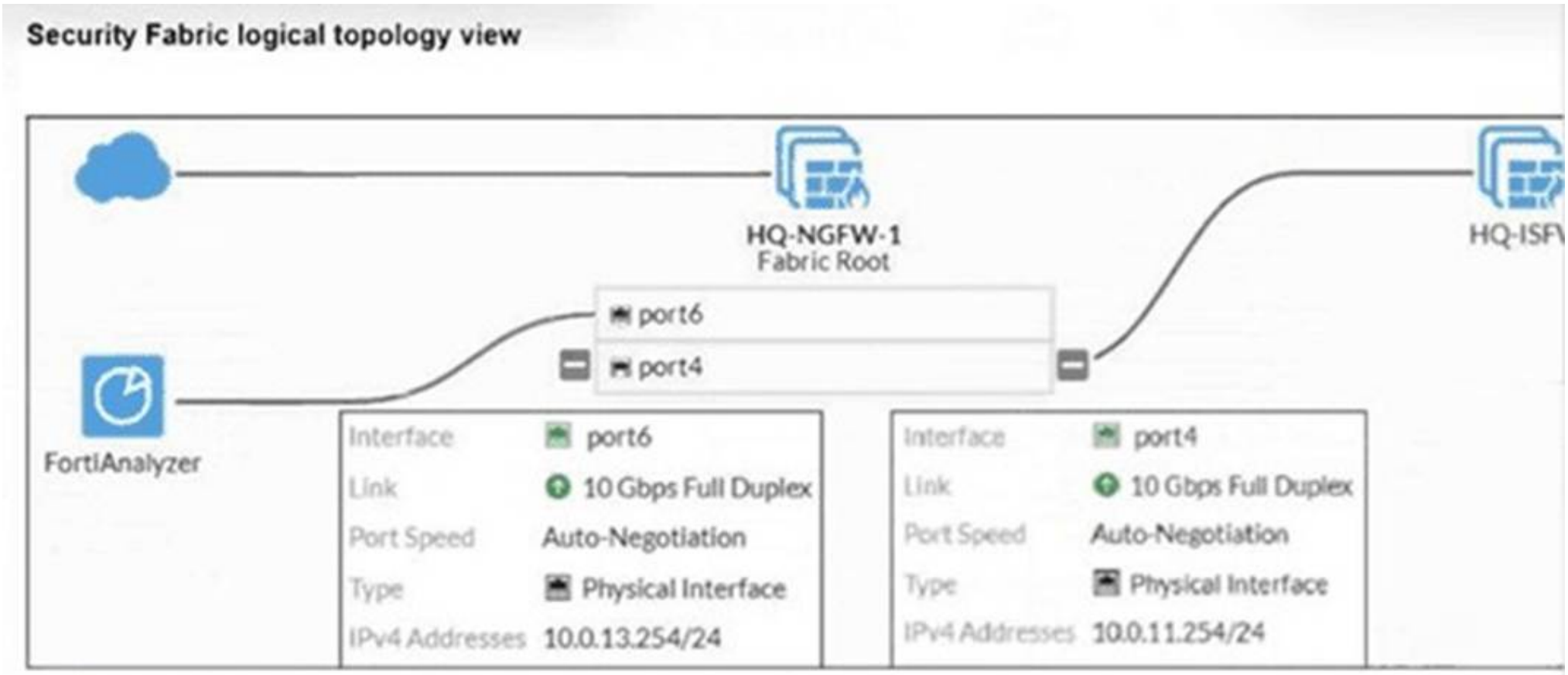
D)

```
HQ-NGFW-1 # diagnose sniffer packet any "host 10.0.13.125" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.0.13.125]
2.173071 port6 out 10.0.13.254.14974 -> 10.0.13.125.514: udp 347
3.334638 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: psh 4017477514 ack 2638032500
3.335098 port6 in 10.0.13.125.514 -> 10.0.13.254.23054: psh 2638032500 ack 4017477548
3.335129 port6 out 10.0.13.254.23054 -> 10.0.13.125.514: ack 2638032543
```

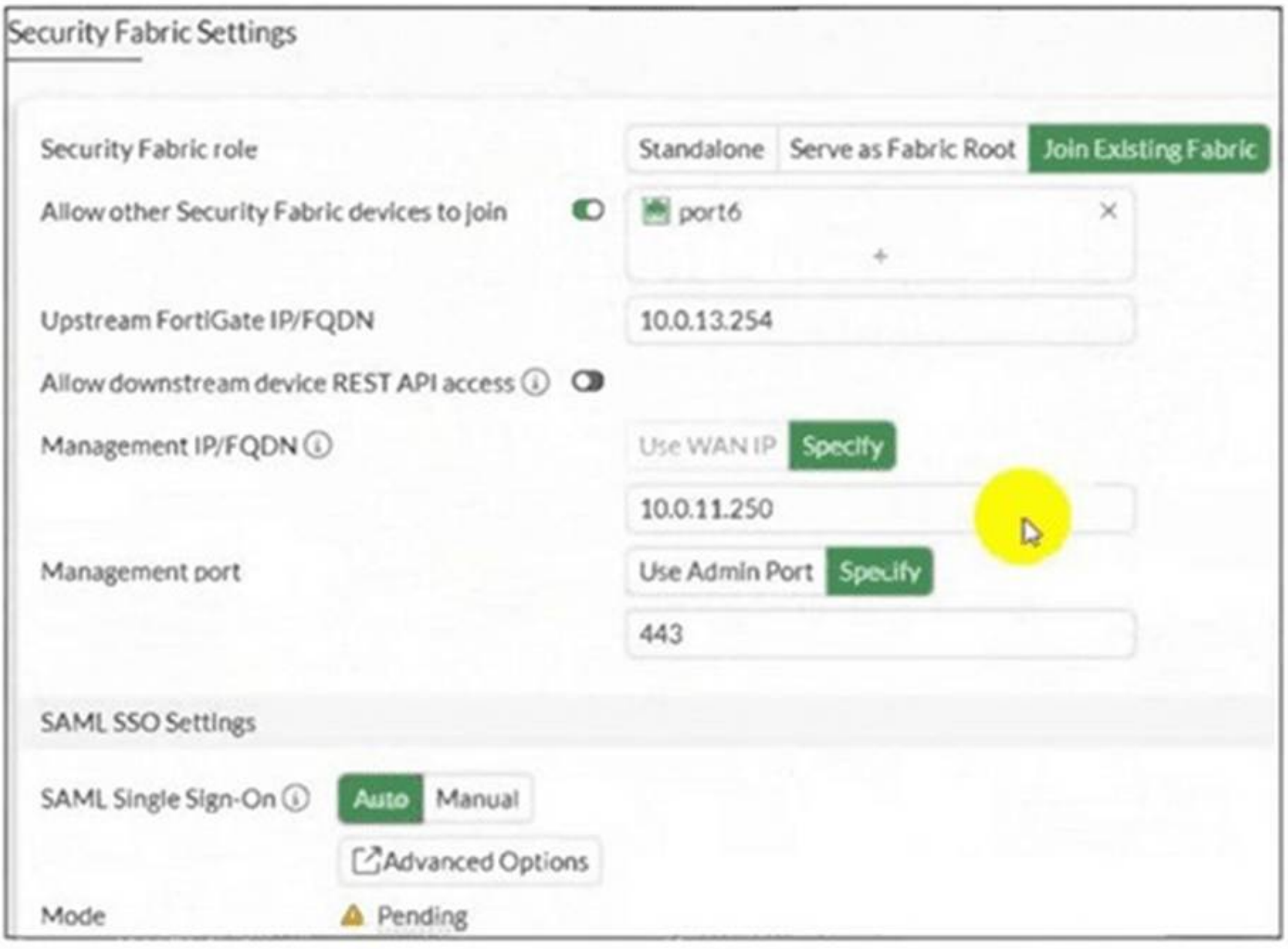
A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 16
Refer to the exhibits.



Security Fabric settings on HQ-ISFW-2



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 20
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 23
What are two features of collector agent advanced mode? (Choose two.)

A. In advanced mode, security profiles can be applied only to user groups, not individual users.
B. In advanced mod
C. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
D. Advanced mode uses the Windows convention—NetBios: Domain\Username.
E. Advanced mode supports nested or inherited groups.

Answer: BD

NEW QUESTION 27
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 29
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 30
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
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT_AD-7.6 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4_FGT_AD-7.6 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT_AD-7.6/

Money Back Guarantee

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