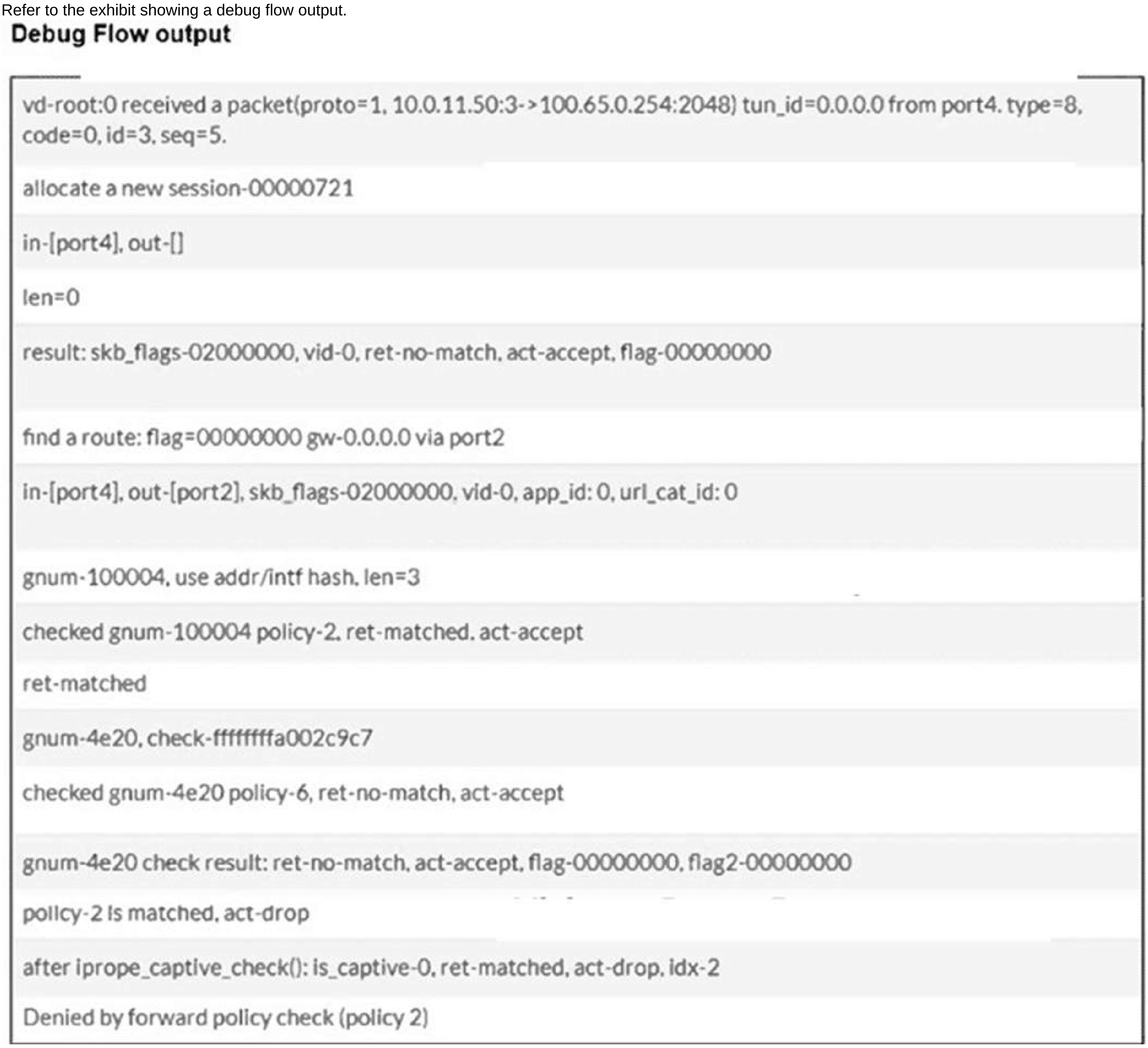
Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

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

NEW QUESTION 1
Refer to the exhibit showing a debug flow output.



Debug Flow output

```
vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4. type=8,
code=0, id=3, seq=5.
allocate a new session-00000721
in-[port4], out-[]
len=0
result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
find a route: flag=00000000 gw-0.0.0.0 via port2
in-[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
gnum-100004, use addr/intf hash, len=3
checked gnum-100004 policy-2, ret-matched, act-accept
ret-matched
gnum-4e20, check-ffffffffa002c9c7
checked gnum-4e20 policy-6, ret-no-match, act-accept
gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000
policy-2 is matched, act-drop
after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-2
Denied by forward policy check (policy 2)
```

Which two conclusions can you make from the debug flow output? (Choose two answers)

A. The default gateway is configured on port2.
B. The RPF check fails.
C. The debug flow is for UDP traffic.
D. The matching firewall policy denies the traffic.

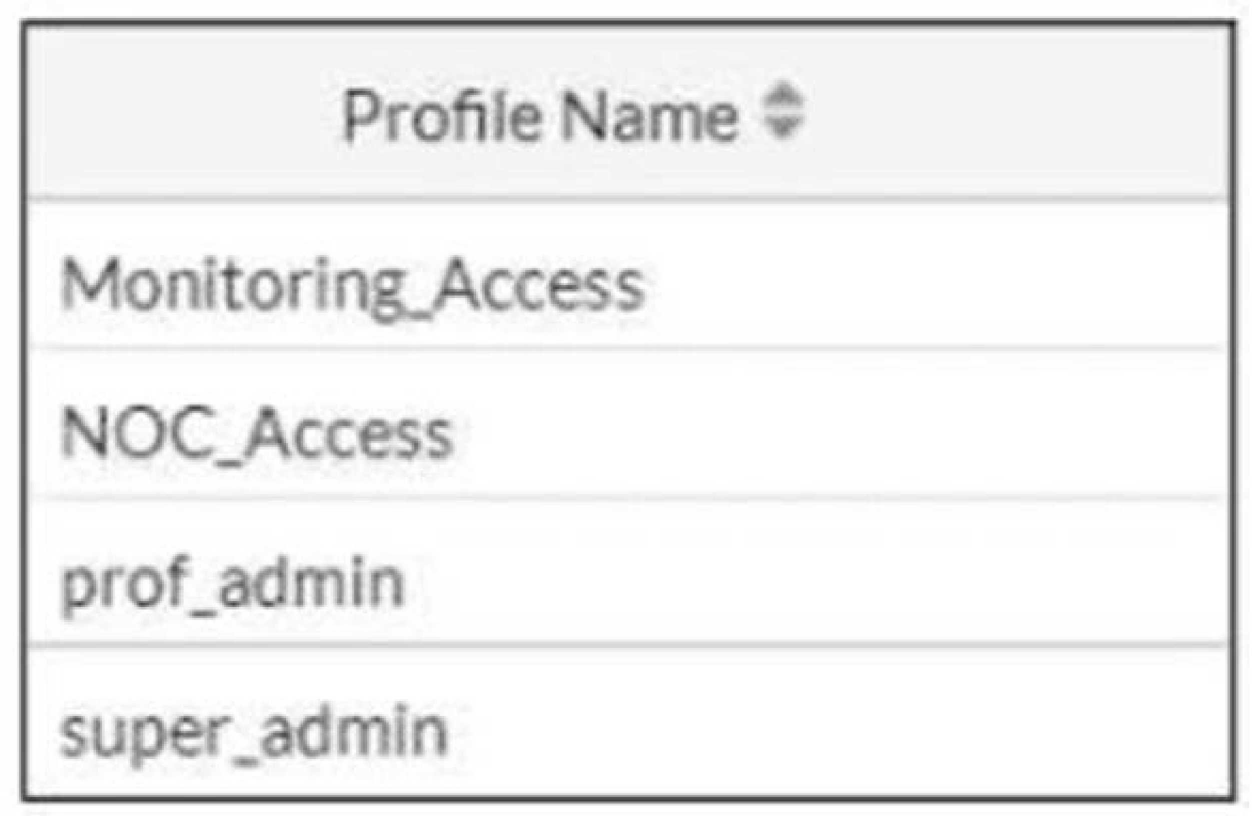
Answer: AD

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
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 4
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

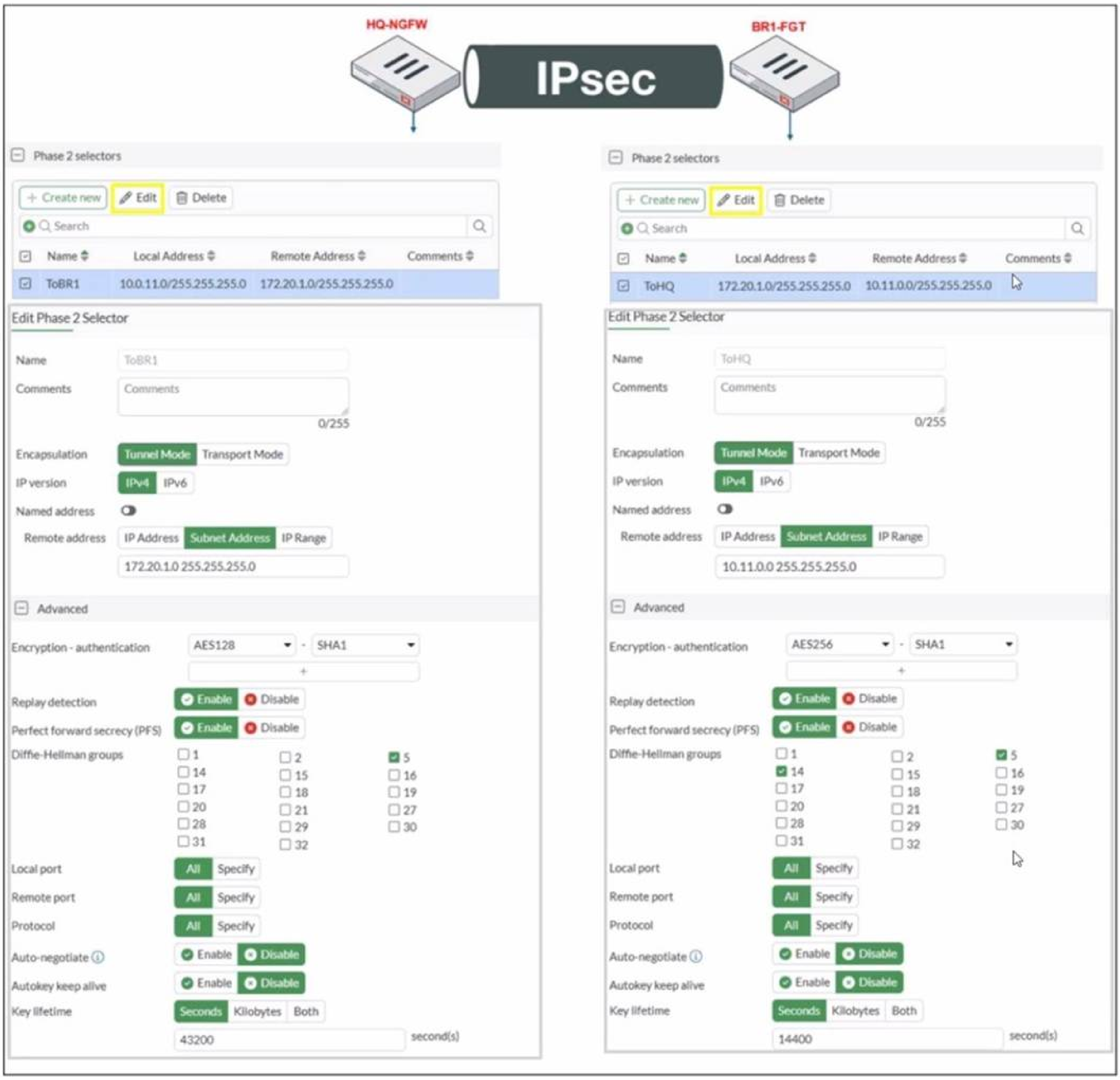
NEW QUESTION 5
Which two statements describe characteristics of automation stitches? (Choose two answers)

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 6
Refer to the exhibit.

IPsec tunnel configuration



HQ-NGFW

Phase 2 selectors

+ Create new | Edit | Delete

Search

☑	Name	Local Address	Remote Address	Comments
☑	ToBR1	10.0.11.0/255.255.255.0	172.20.1.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToBR1
Comments: Comments 0/255
Encapsulation: [✓ Tunnel Mode] Transport Mode
IP version: [✓ IPv4] IPv6
Named address: ○
Remote address: IP Address [✓ Subnet Address] IP Range
172.20.1.0 255.255.255.0

Advanced

Encryption - authentication: AES128 - SHA1
Replay detection: [✓ Enable] Disable
Perfect forward secrecy (PFS): [✓ Enable] Disable
Diffie-Hellman groups:
□ 1 □ 2 ☑ 5
□ 14 □ 15 □ 16
□ 17 □ 18 □ 19
□ 20 □ 21 □ 27
□ 28 □ 29 □ 30
□ 31 □ 32
Local port: [✓ All] Specify
Remote port: [✓ All] Specify
Protocol: [✓ All] Specify
Auto-negotiate: Enable [✓ Disable]
Autokey keep alive: Enable [✓ Disable]
Key lifetime: [✓ Seconds] Kilobytes Both
43200 second(s)

BR1-FGT

Phase 2 selectors

+ Create new | Edit | Delete

Search

☑	Name	Local Address	Remote Address	Comments
☑	ToHQ	172.20.1.0/255.255.255.0	10.11.0.0/255.255.255.0	

Edit Phase 2 Selector

Name: ToHQ
Comments: Comments 0/255
Encapsulation: [✓ Tunnel Mode] Transport Mode
IP version: [✓ IPv4] IPv6
Named address: ○
Remote address: IP Address [✓ Subnet Address] IP Range
10.11.0.0 255.255.255.0

Advanced

Encryption - authentication: AES256 - SHA1
Replay detection: [✓ Enable] Disable
Perfect forward secrecy (PFS): [✓ Enable] Disable
Diffie-Hellman groups:
□ 1 □ 2 ☑ 5
☑ 14 □ 15 □ 16
□ 17 □ 18 □ 19
□ 20 □ 21 □ 27
□ 28 □ 29 □ 30
□ 31 □ 32
Local port: [✓ All] Specify
Remote port: [✓ All] Specify
Protocol: [✓ All] Specify
Auto-negotiate: Enable [✓ Disable]
Autokey keep alive: Enable [✓ Disable]
Key lifetime: [✓ Seconds] Kilobytes Both
14400 second(s)

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

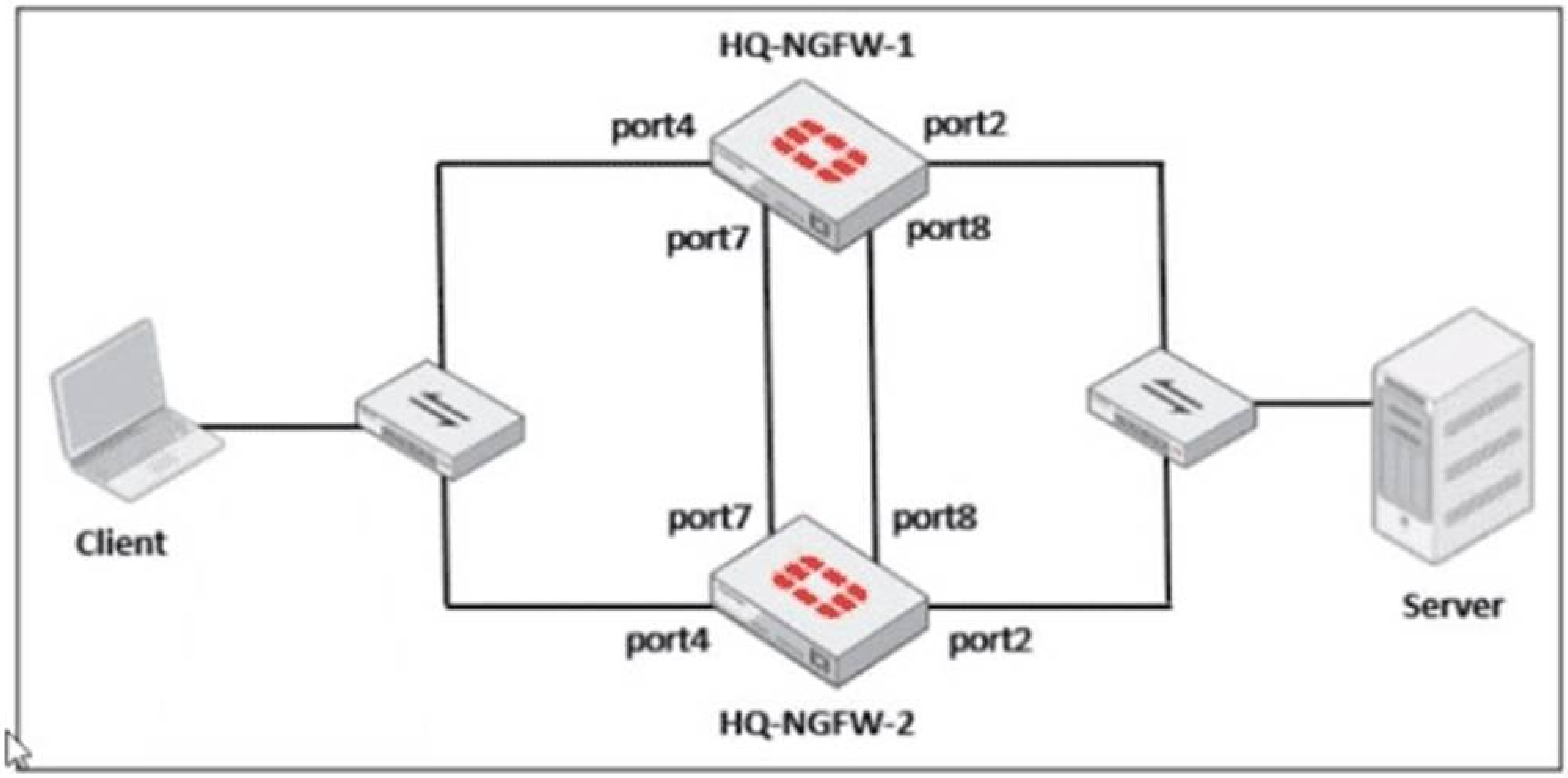
NEW QUESTION 7
A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode. Which step is not part of the expected process?

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.

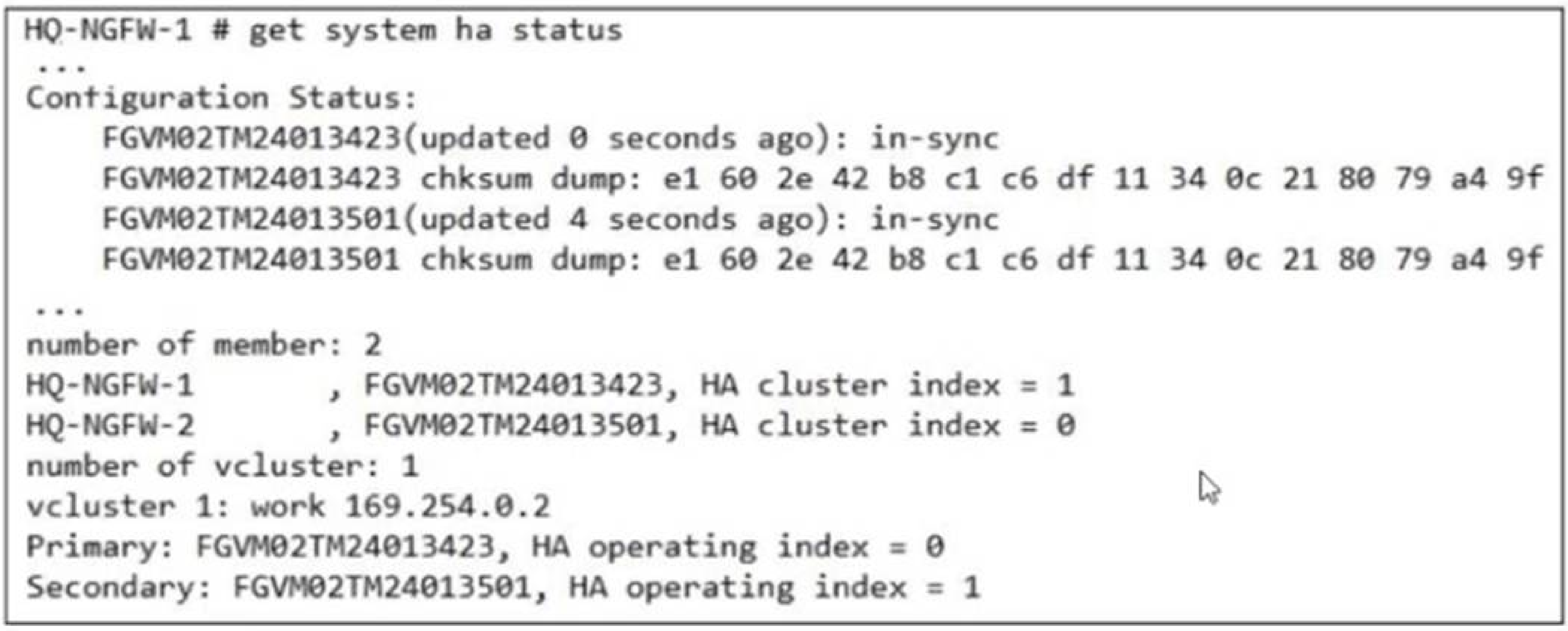
Answer: A

NEW QUESTION 8
Refer to the exhibits.

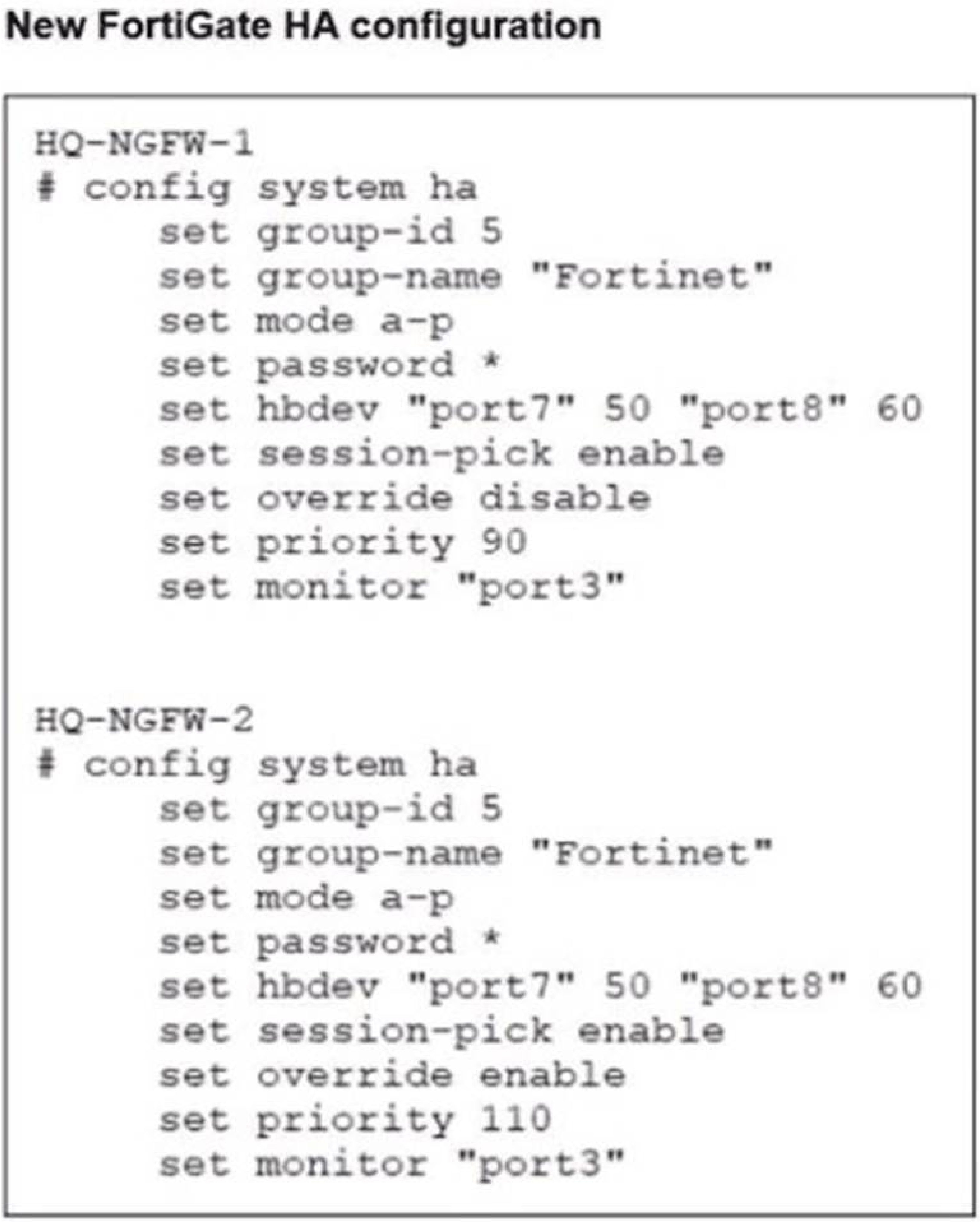
FortiGate HA cluster topology



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 9
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 10
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 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 13
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 16
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.

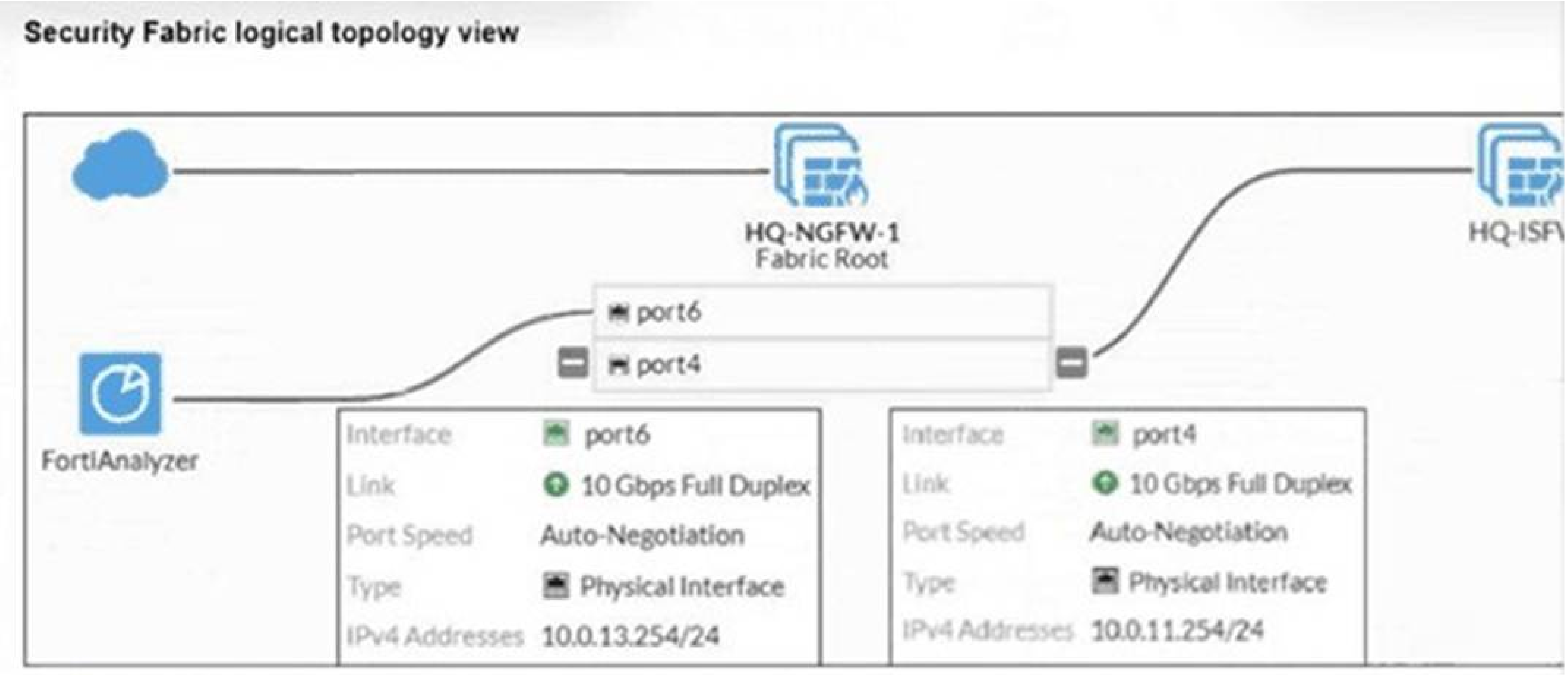
Answer: D

NEW QUESTION 21
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

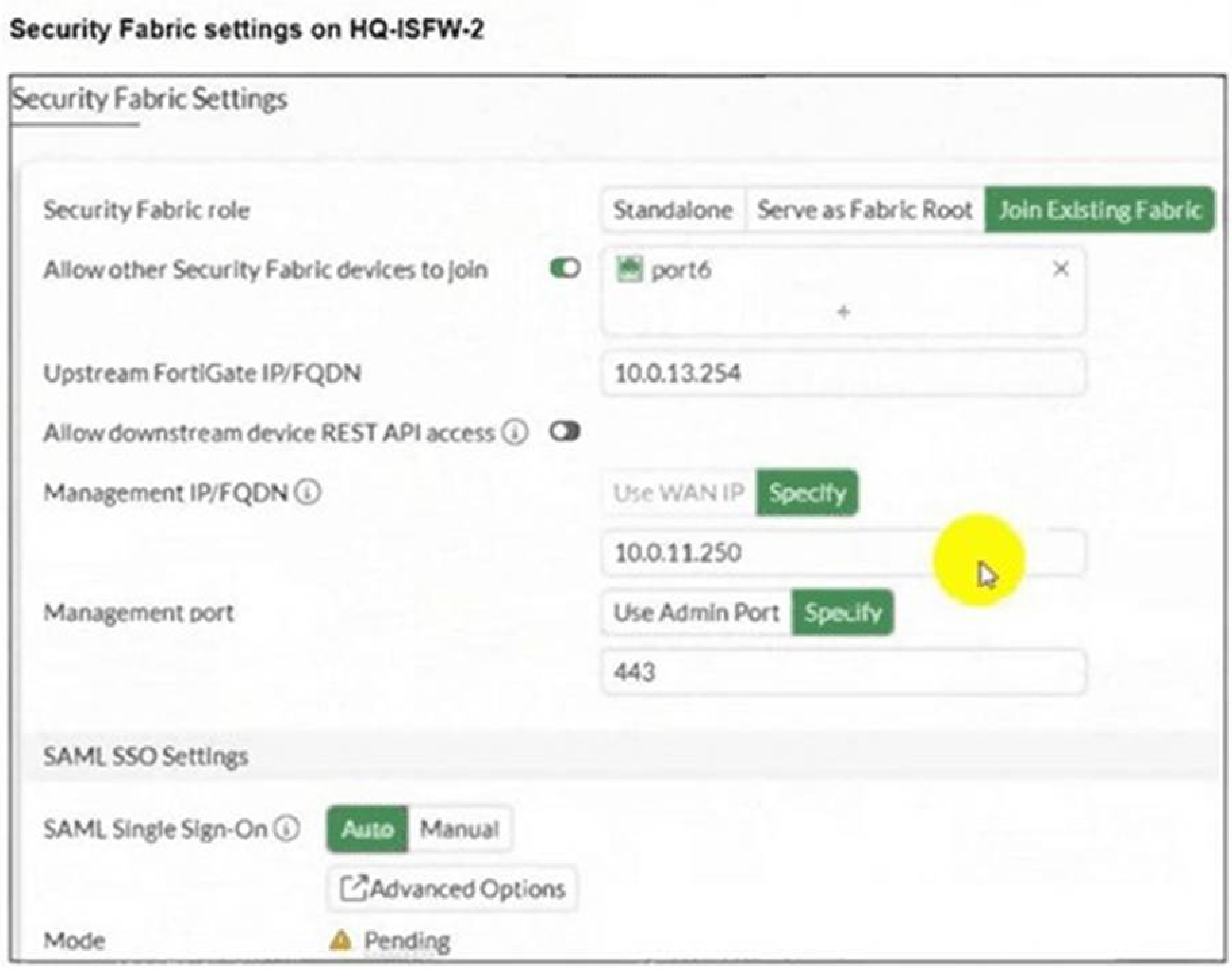
Answer: A

NEW QUESTION 22
Refer to the exhibits.


Security Fabric logical topology view

Interface	port6
Link	10 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	Physical Interface
IPv4 Addresses	10.0.13.254/24

Interface	port4
Link	10 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	Physical Interface
IPv4 Addresses	10.0.11.254/24


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: 10.0.13.254

Allow downstream device REST API access ⓘ: ○

Management IP/FQDN ⓘ: Use WAN IP | [✓ Specify]

10.0.11.250

Management port: Use Admin Port | [✓ Specify]

443

SAML SSO Settings

SAML Single Sign-On ⓘ: [✓ Auto] | Manual

Advanced Options

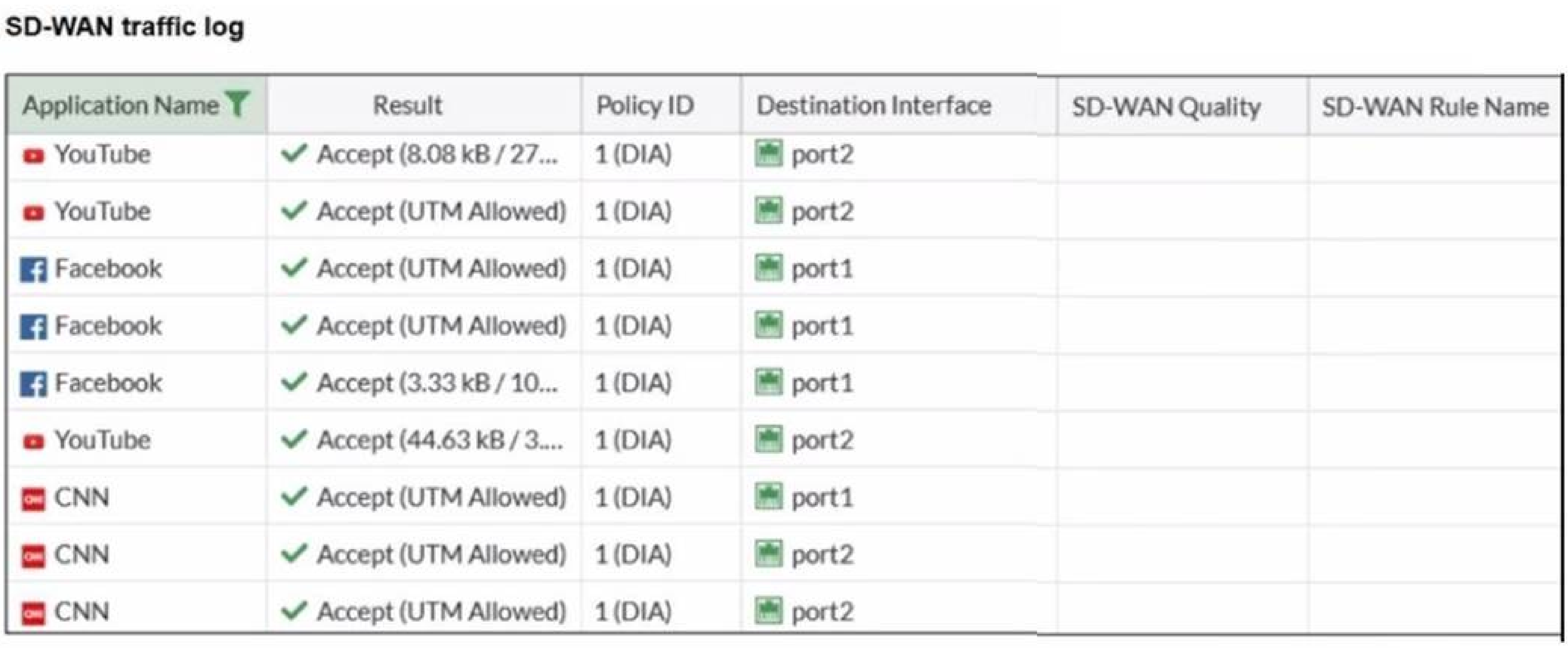
Mode: ⚠ Pending

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 25
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.

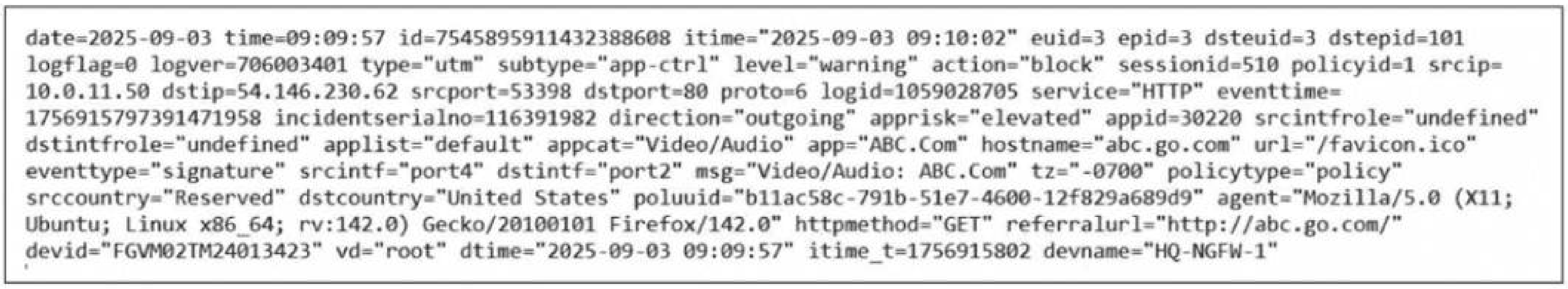
Answer: D

NEW QUESTION 28
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 31
Refer to the exhibit.



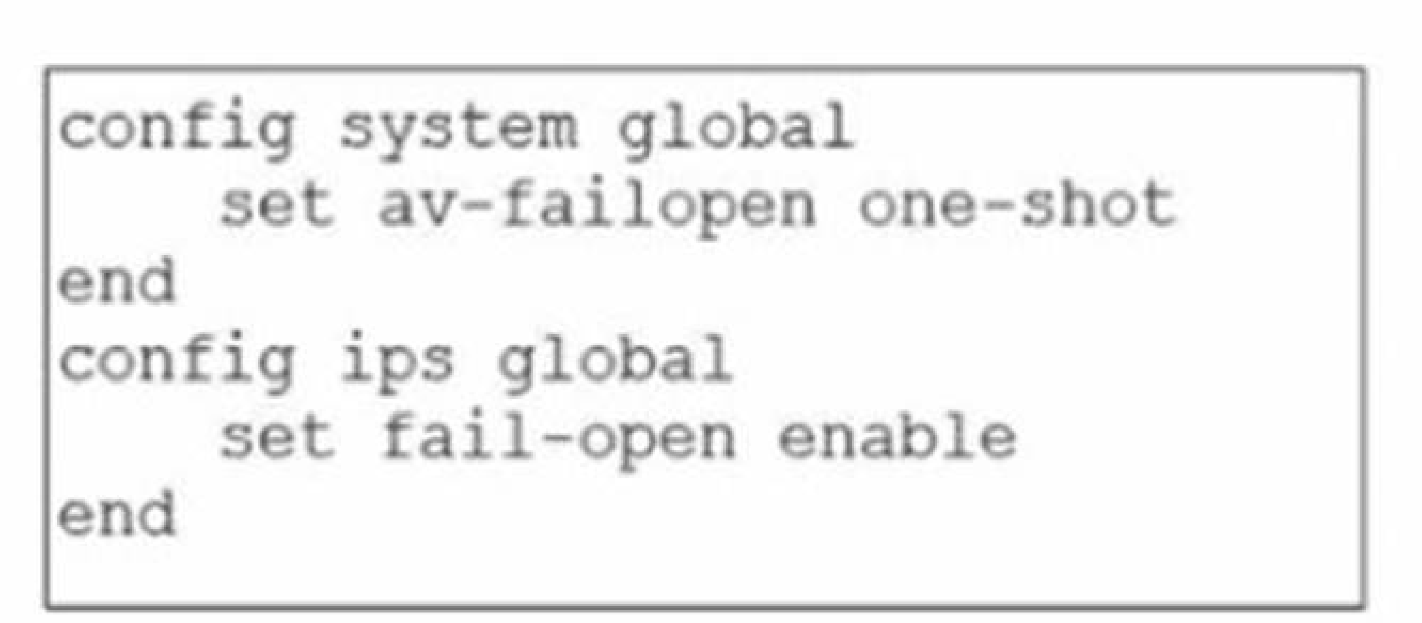
```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 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 34
Refer to the exhibit.



```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```

Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

A. FortiGate drops new sessions requiring inspection.
B. Administrators must restart FortiGate to allow new sessions.
C. Administrators cannot change the configuration.
D. FortiGate skips quarantine actions.

Answer: CD

NEW QUESTION 35
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 36
......