Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator

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)
```

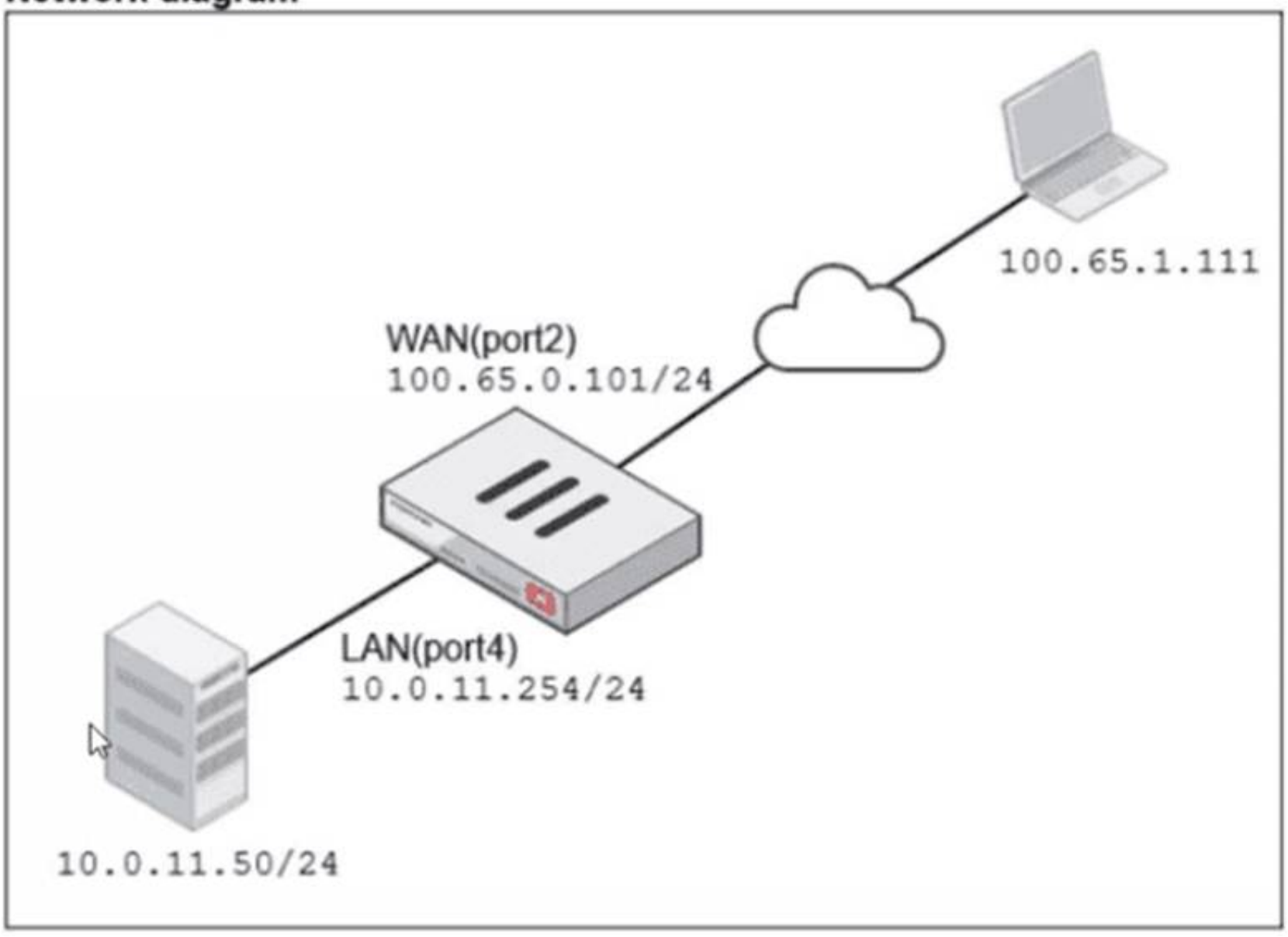
Which two conclusions can you make from the debug flow output? (Choose two answers)

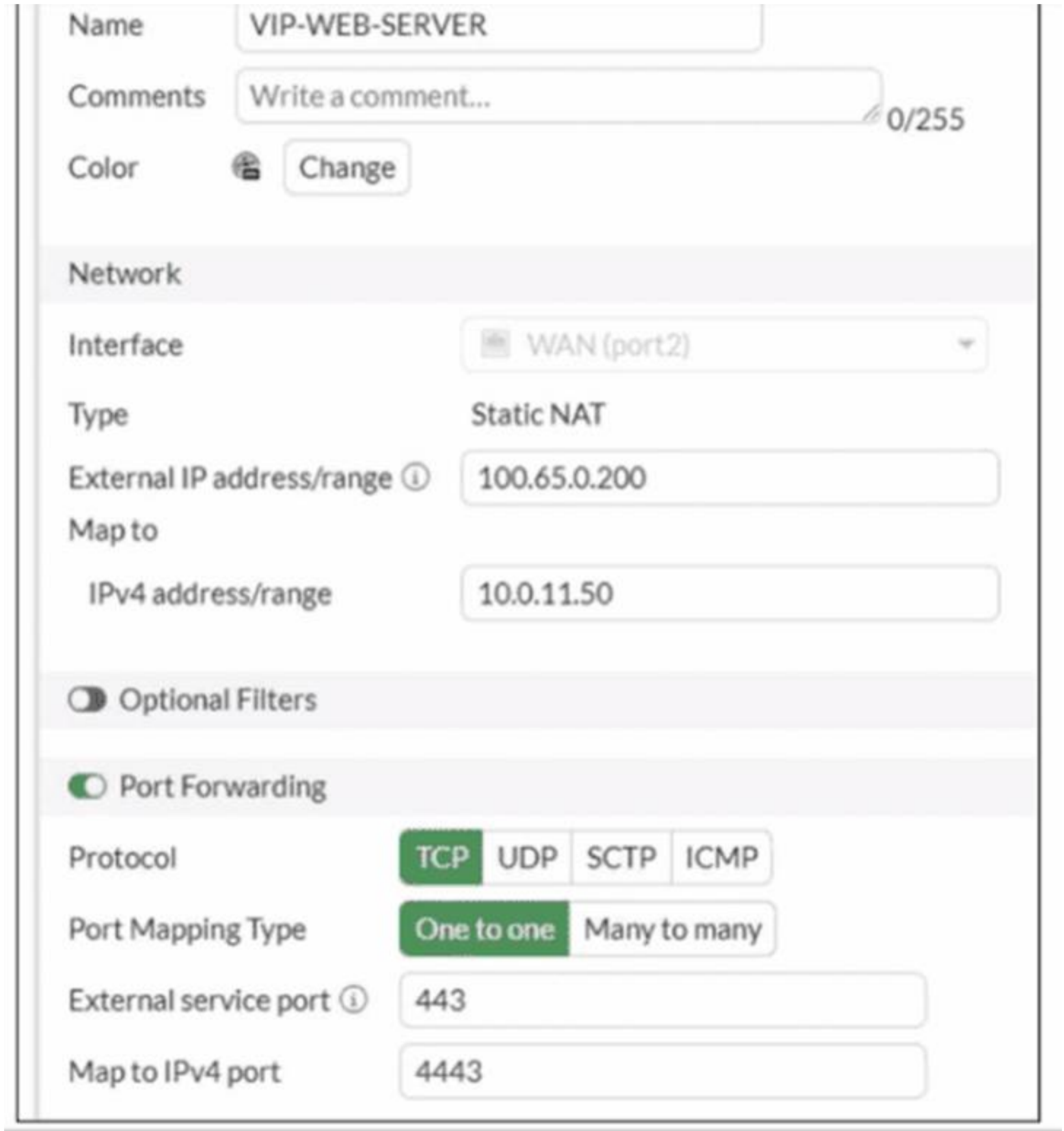
A. The default gateway is configured on port2.
B. The RPF check fails.
C. The debug flow is for UDP traffic.
D. The matching firewall policy denies the traffic.

Answer: AD

NEW QUESTION 2
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 3
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 4
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 5
Refer to the exhibit.

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
            pid = 2044, engine count = 0 (+1)
            0 - pid:2074:2074 cfg:1 master:0 run:1
```

As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit What could be the possible reason of the diagnose output shown in the exhibit?

A. There is a no firewall policy configured with an IPS security profile.
B. Administrator entered the command diagnose test application ipsmonitor 5.
C. FortiGate entered into IPS fail open state.
D. Administrator entered the command diagnose test application ipsmonitor 99.

Answer: A

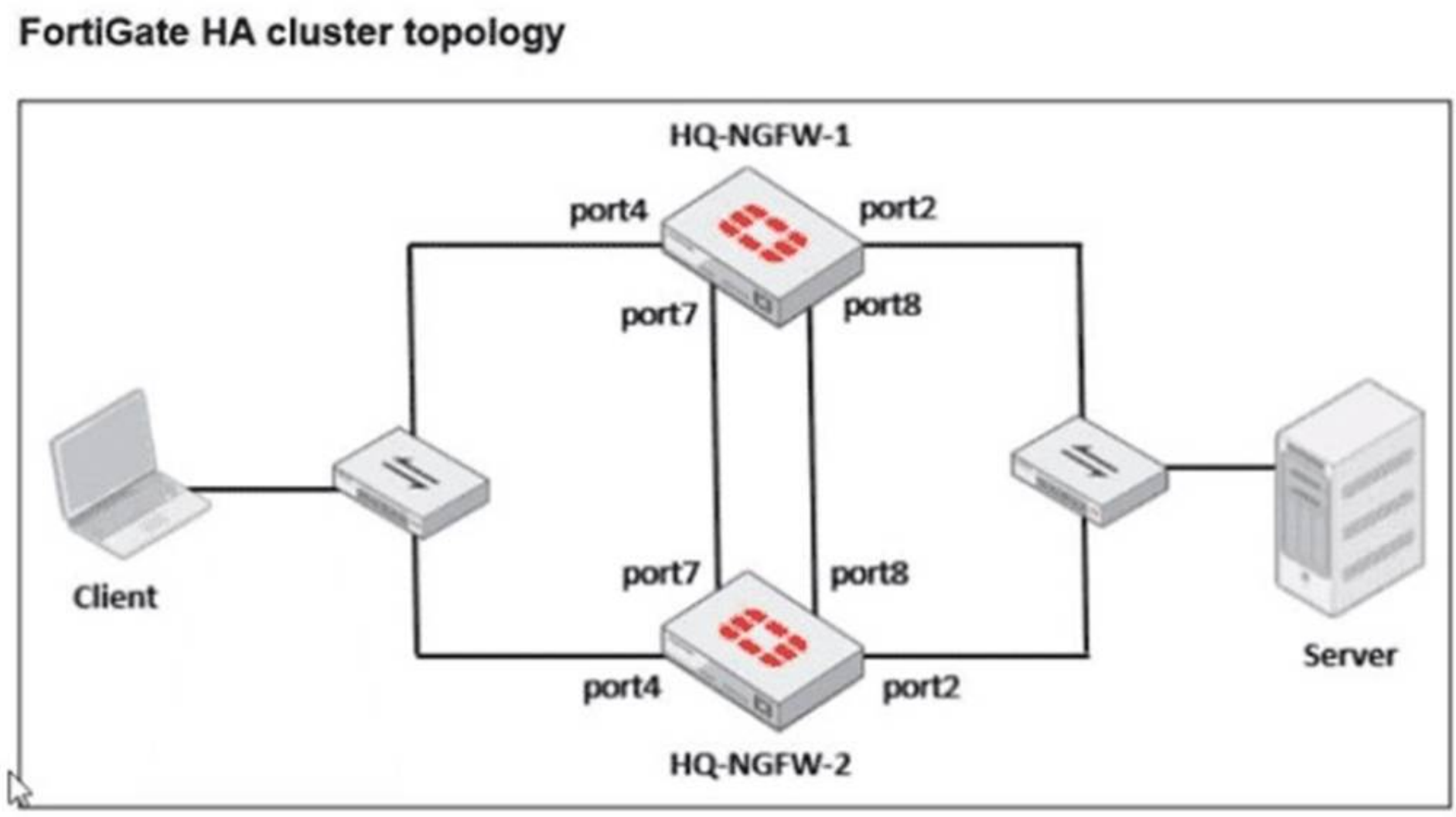
NEW QUESTION 6
Refer to the exhibit.

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
Refer to the exhibits.



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

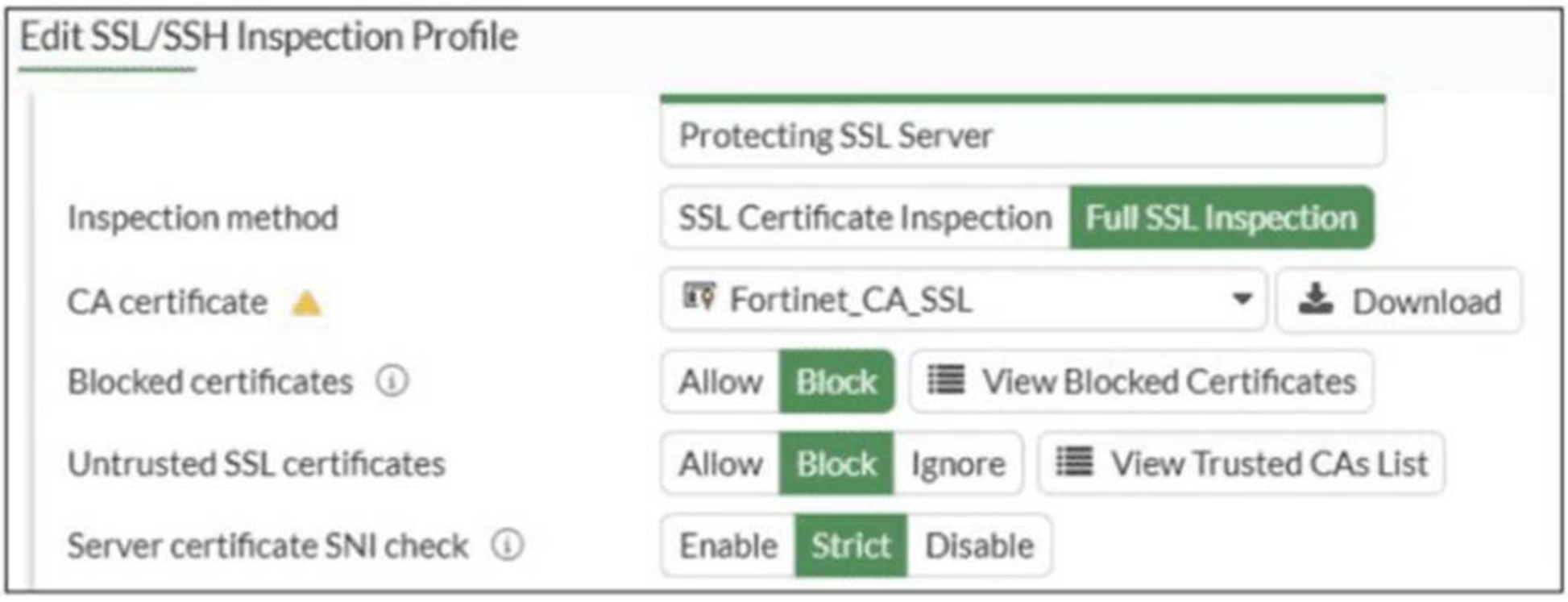
NEW QUESTION 8
Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Choose two.)

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

Answer: AC

NEW QUESTION 9

Refer to the exhibit.



What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

A. FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.
B. FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
C. FortiGate will close the connection if the SNI does not match the CN or SAN fields.
D. FortiGate will close the connection if the SNI does not match the CN and SAN fields

Answer: C

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 10
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?

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 15
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 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 21
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 23
Refer to the exhibit
A firewall policy to enable active authentication is shown.

Policy	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port4 → port2 1								
Internet (1)	HQ_SUBNET Remote-users	all	always	ALL_ICMP HTTPS HTTP	ACCEPT	NAT	Standard	Category_Monitor certificate-inspection

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 24
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 28
.....

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