Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

NEW QUESTION 1
What is the primary FortiGate election process when the HA override setting is enabled?

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

Explanation:
When HA override is enabled, FortiGate uses the following election order: number of connected monitored ports, then device priority, followed by HA uptime, and finally FortiGate serial number as a tiebreaker.

NEW QUESTION 2
You have configured the below commands on a FortiGate.

```
config system settings
set strict-src-check enable
end
```

```
Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

A. FortiGate will enable strict RPF on ail its interfaces and port1 will be enable for asymmetric routing.
B. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
C. Port1 will be enabled with flexible RPF, and all other interfaces will be enabled for strict RPF
D. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.

Answer: B

Explanation:
The global setting enables strict source checking (RPF) on all interfaces by default. The per-interface setting disables the source check on port1, exempting it from strict RPF enforcement.

NEW QUESTION 3
A remote user reports slow SSL VPN performance and frequent disconnections. The user is located in an area with poor internet connectivity.
What setting should the administrator adjust to improve the user's experience?

A. Enable split tunneling to reduce VPN traffic.
B. Change the SSL VPN port to a non-standard port.
C. Increase the session timeout for inactive sessions.
D. Configure the DTLS timeout to accommodate high-latency connections.

Answer: D

Explanation:
Adjusting the DTLS timeout helps maintain SSL VPN stability and performance in environments with poor or high-latency internet connectivity by allowing more time for packet retransmissions before dropping the connection.

NEW QUESTION 4
A FortiGate firewall policy is configured with active authentication, however, the user cannot authenticate when accessing a website.
Which protocol must FortiGate allow even though the user cannot authenticate?

A. LDAP
B. TACASC+
C. Kerberos
D. DNS

Answer: D

Explanation:

DNS traffic must be allowed so the user can resolve domain names and reach the authentication server or web resources, even if authentication initially fails.

NEW QUESTION 5
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-2 with the parameter memory-failover-threshold setting
B. HQ-NGFW-2 with the parameter priority setting
C. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
D. HQ-NGFW-1 with the parameter override setting

Answer: D

Explanation:
The HA configuration shows that override is disabled (set override disable), but despite this, HQ-NGFW-1 has the higher priority (200) and is acting as the primary, as indicated by its higher resource usage and uptime.
Override allows the device with higher priority to take over as primary, so HQ-NGFW-1 is the primary device.

NEW QUESTION 6
What are three key routing principles in SD-WAN? (Choose three.)

A. By defaul
B. SD-WAN rules are skipped if the included SD-WAN members do not have a valid route to the destination.
C. SD-WAN rules have precedence over any other type of routes.
D. Regular policy routes have precedence over SD-WAN rules.
E. By defaul
F. SD-WAN rules are skipped if only one route to the destination is available.
G. By defaul
H. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

Answer: ABE

Explanation:
SD-WAN rules are skipped if none of the SD-WAN members have a valid route to the destination. SD-WAN rules take precedence over other route types.
SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member by default.

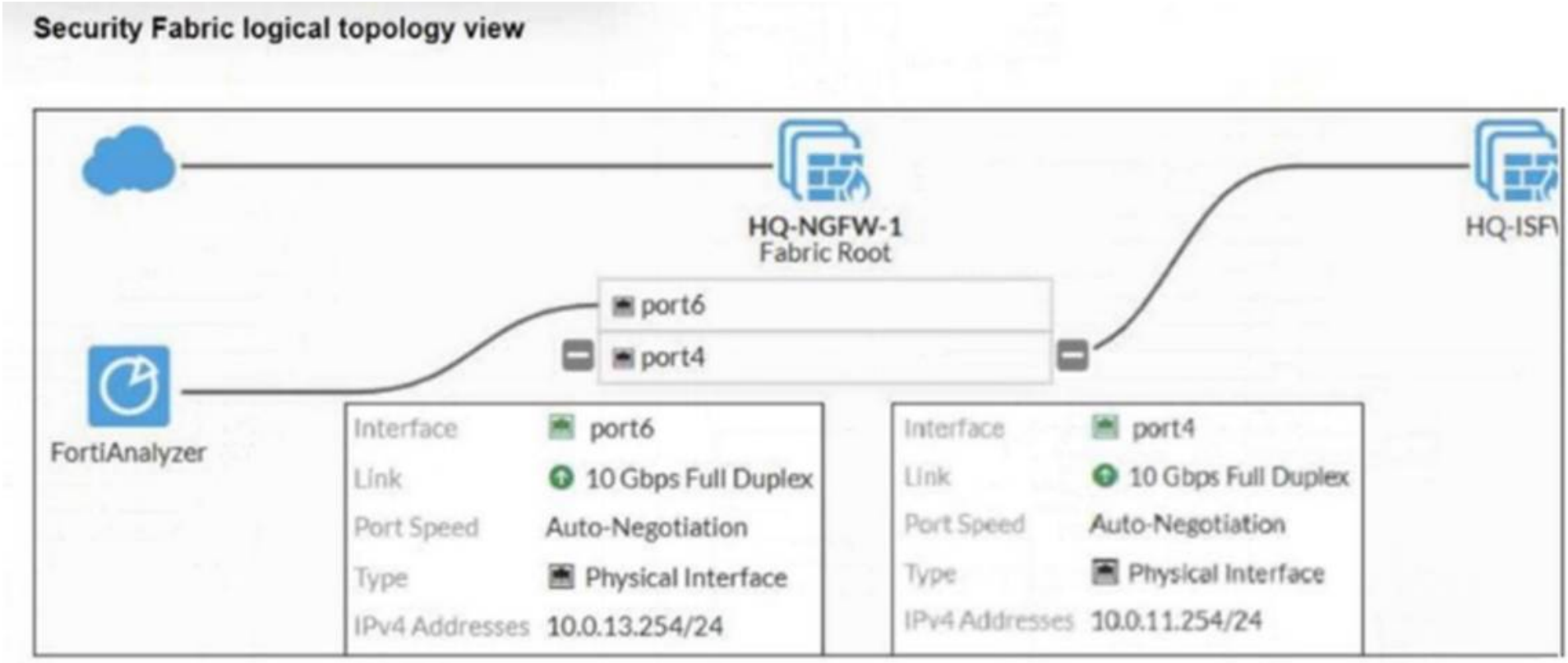
NEW QUESTION 7
An administrator notices that some users are unable to establish SSL VPN connections, while others can connect without any issues.
What should the administrator check first?

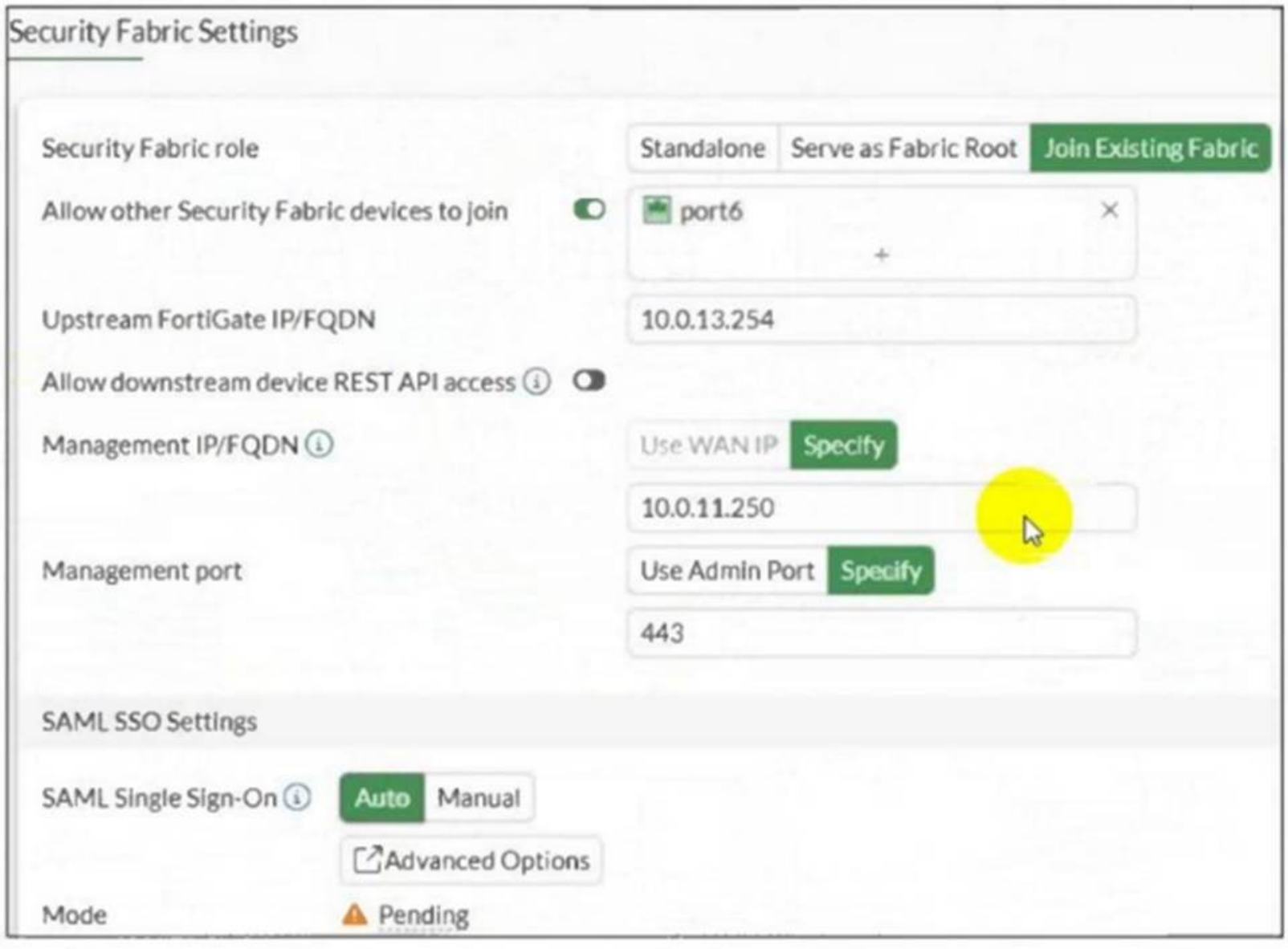
A. Ensure that the affected users are using the correct port number.
B. Ensure that user traffic is hitting the firewall policy.
C. Ensure that forced tunneling is enabled to reroute all traffic through the SSL VPN
D. Ensure that the HTTPS service is enabled on SSL VPN tunnel interface

Answer: B

Explanation:
If user traffic is not matching the appropriate firewall policy that permits SSL VPN, users will be unable to establish connections, making this the first aspect to verify.

NEW QUESTION 8
Refer to the exhibits.





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 staysPending.
What can be the two possible reasons? (Choose two.)

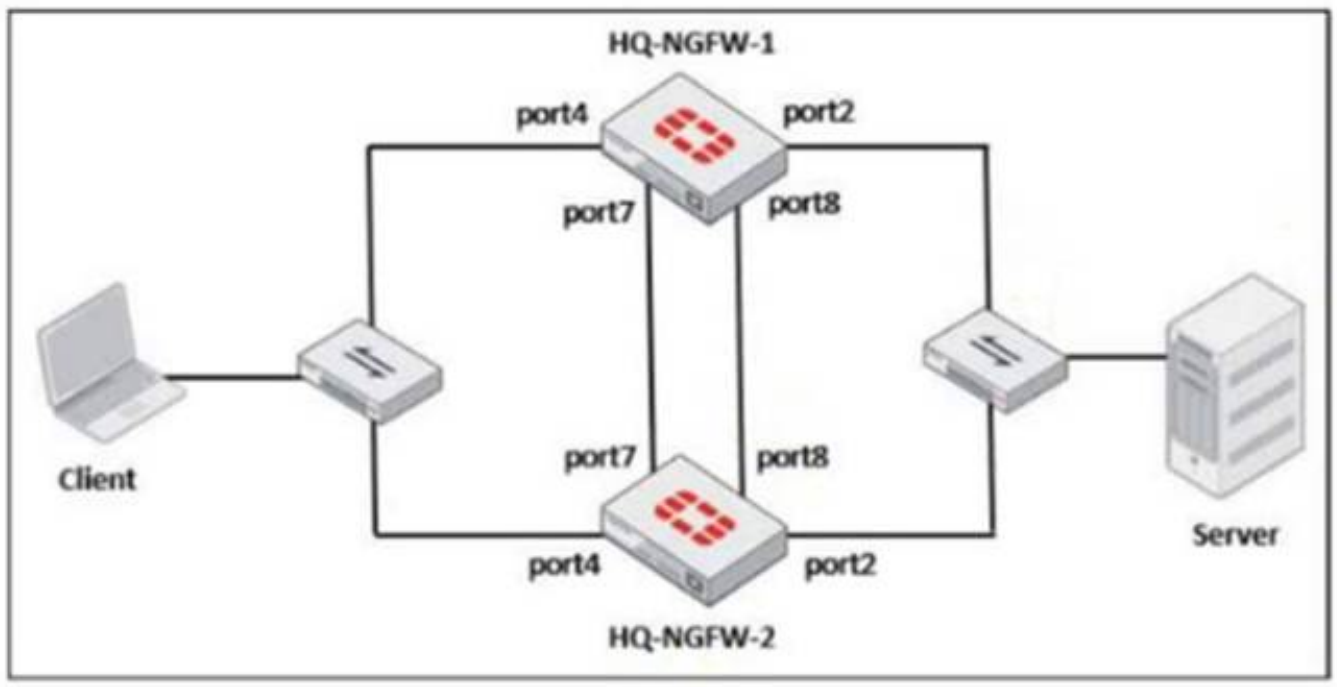
A. Upstream FortiGate IP must be set to 10.0.11.254.
B. SAML Single Sign-On must be set to Manual.
C. HQ-ISFW-2 must be authorized on HQ-ISFW.
D. Management IP must be set to 10.0.13.254.

Answer: AC

Explanation:
The Upstream FortiGate IP should match the IP address of the Fabric Root interface, which is 10.0.11.254, not 10.0.13.254.
The new device (HQ-ISFW-2) must be authorized on the Fabric Root (HQ-ISFW) before it can join the Security Fabric, otherwise the status remains pending.

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 theoverrideandpriorityparameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibit.
What would be the expected outcome in the HA cluster?

A. HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.
B. HQ-NGFW-2 will take over as the primary because it has the override enable setting and higher priority than HQ-NGFW-1.
C. HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority.
D. The HA cluster will become out of sync because the override setting must match on all HA members.

Answer: B

Explanation:
With override enabled on HQ-NGFW-2 and its higher priority (110 vs. 90), HQ-NGFW-2 will become the primary device, preempting HQ-NGFW-1 despite the current primary status.

NEW QUESTION 10
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 exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.
Based on the system performance output, what are the two possible outcomes? (Choose two.)

A. FortiGate has entered conserve mode.
B. Administrators can access FortiGate only through the console port.
C. Administrators can change the configuration.
D. FortiGate drops new sessions.

Answer: CD

Explanation:
Since memory usage is at 90%, exceeding the red threshold (88%), FortiGate enters a state where configuration changes are still allowed.
In this state, FortiGate drops new sessions to preserve resources and maintain stability.

NEW QUESTION 10
Which two statements are correct when FortiGate enters conserve mode? (Choose two.)

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

Explanation:
In conserve mode, FortiGate restricts configuration changes to preserve system stability.
When IPS fail-open is enabled, FortiGate continues forwarding traffic without IPS inspection during resource constraints (conserve mode).

NEW QUESTION 15
Which three statements explain a flow-based antivirus profile? (Choose three.)

A. FortiGate buffers the whole file but transmits to the client at the same time.
B. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.

C. If a virus is detected, the last packet is delivered to the client.
D. Flow-based inspection optimizes performance compared to proxy-based inspection.
E. The IPS engine handles the process as a standalone.

Answer: ABD

Explanation:
Flow-based antivirus buffers the entire file while simultaneously transmitting data to the client to minimize latency.
Flow-based inspection combines multiple scanning techniques from proxy-based modes for efficient detection. Flow-based inspection provides better performance by processing traffic on the fly without full proxy overhead.

NEW QUESTION 19
.....

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

FCP_FGT_AD-7.6 Practice Exam Features:

* FCP_FGT_AD-7.6 Questions and Answers Updated Frequently

* FCP_FGT_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FGT_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

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