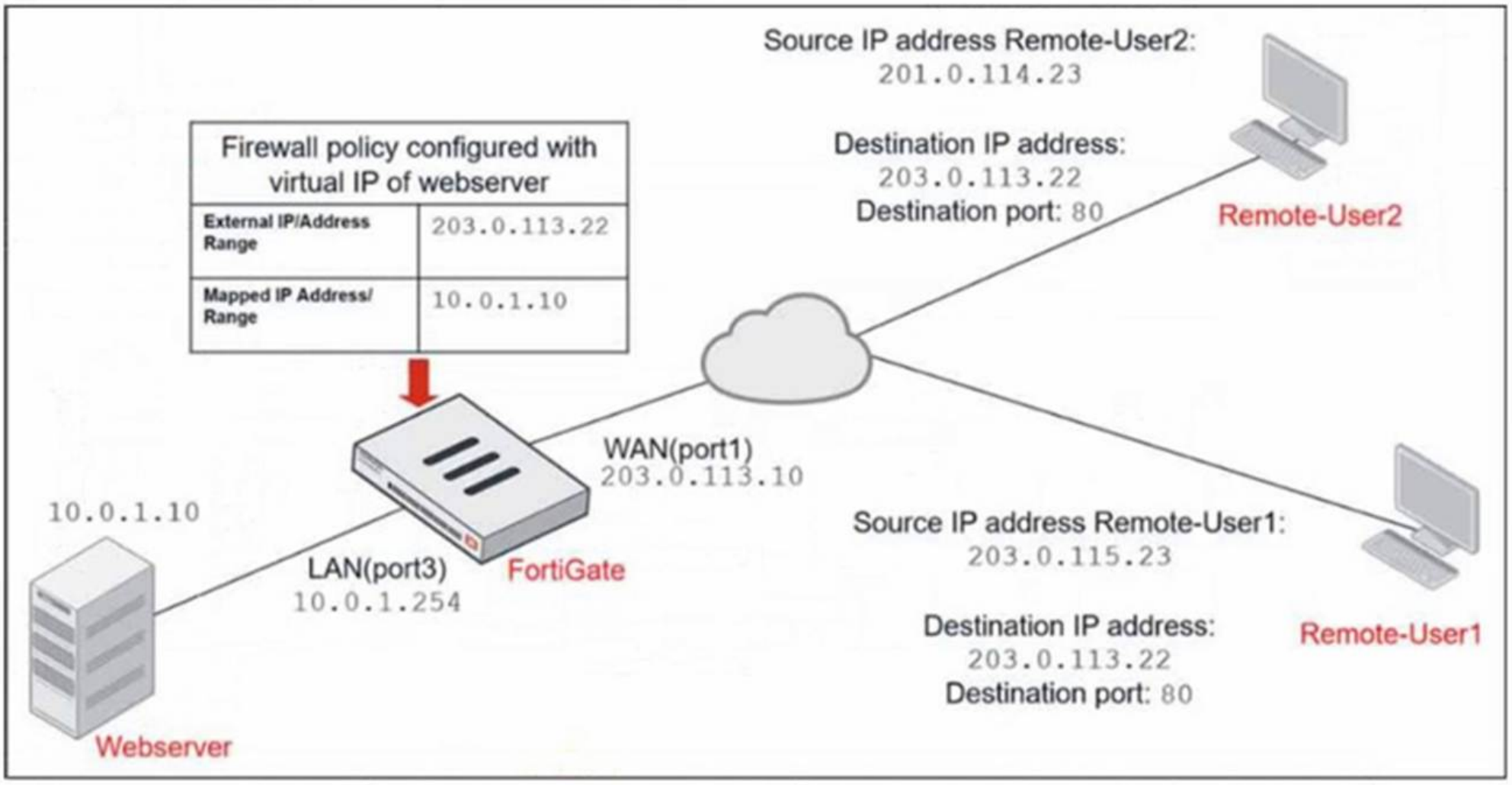
Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

NEW QUESTION 1
Refer to the exhibits.

Network diagram



Firewall address object

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.
The policy should work such thatRemote-User1must be able to access the Webserver while preventing Remote-User2from accessing theWebserver.
Which additional configuration can the administrator add to a deny firewall policy, beyond the default behavior, to blockRemote-User2from accessing theWebserver?

A. Disable match-vip in the Allow_access policy
B. Configure a One-to-One IP Pool object in a new policy.
C. Set the Destination address as Webserver in the Deny policy.
D. Set the Destination address as Deny_IP in the Allow_access policy.

Answer: C

Explanation:

To block Remote-User2's access to the Webserver, the deny policy must explicitly specify the Webserver as the destination address; otherwise, it denies traffic to all destinations, which is not the desired behavior.

NEW QUESTION 2
You are analyzing connectivity problems caused by intermediate devices blocking traffic in SSL VPN environment.
In which two ways can you effectively resolve the problem? (Choose two.)

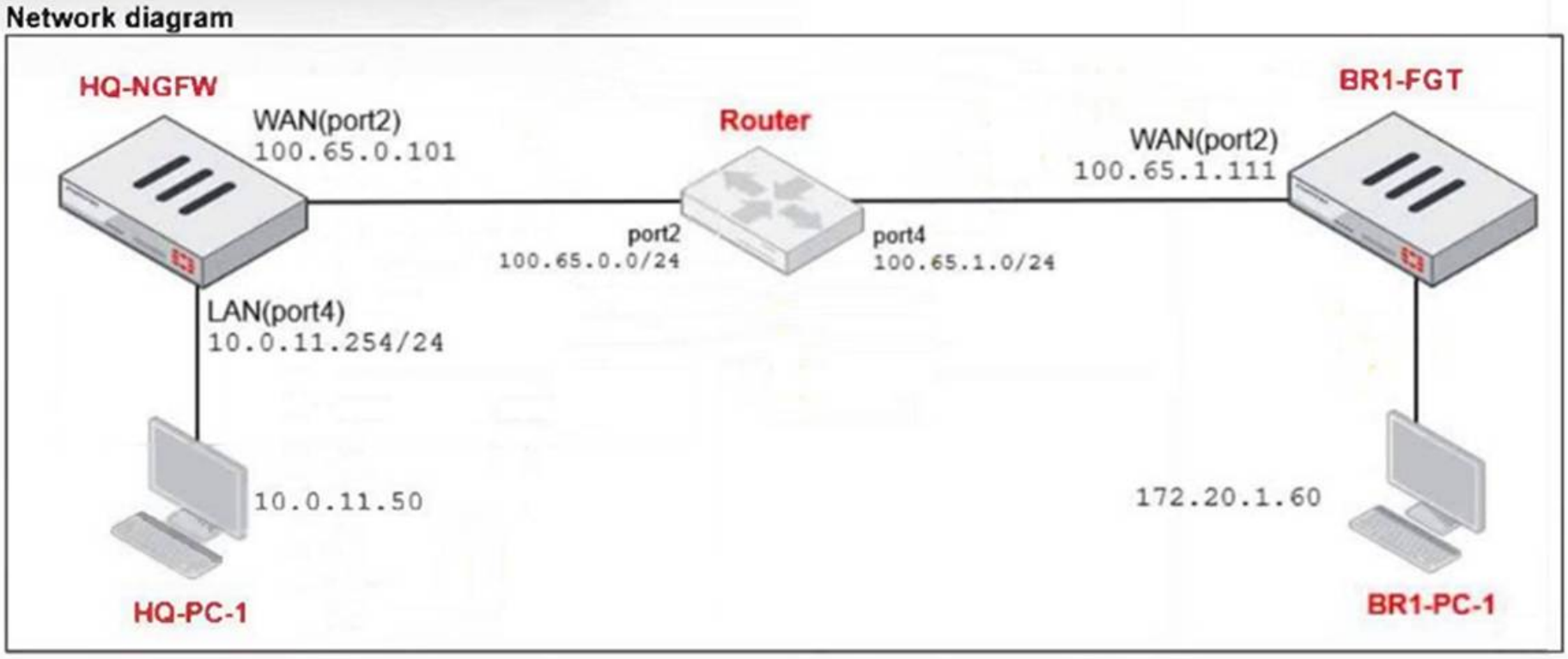
A. You can turn off IKE fragmentation to fix large certificate negotiation problems.
B. You should use IPsec to solve issues with fragment drops and large certificate exchanges.
C. You can use SSL VPN tunnel mode to prevent problems with blocked ESP and UDP ports (500 or 4500).
D. You can configure a hub-and-spoke topology with SSL VPN tunnels to bypass blocked UDP ports.

Answer: AC

Explanation:
Disabling IKE fragmentation helps resolve issues caused by intermediate devices blocking large fragmented packets during certificate negotiation.
Using SSL VPN tunnel mode encapsulates traffic over HTTPS, bypassing blocks on ESP and UDP ports commonly used by IPsec.

NEW QUESTION 3
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.
TheWAN (port2)interface has the IP address100.65.0.101/24.
TheLAN (port4)interface has the IP address10.0.11.254/24.
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. 100.65.0.99
D. 100.65.0.149

Answer: C

Explanation:
The ping traffic policy uses the IP pool named SNAT-Remote1, which has the external IP range 100.65.0.99. Therefore, traffic matching this policy (ping from HQ-PC-1 to BR1-FGT) will use 100.65.0.99 for source NAT.

NEW QUESTION 4
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 5
You have configured the FortiGate device for FSSO. A user is successful in log-in to windows, but their access to the internet is denied.
What should the administrator check first?

A. Whether the user is assigned to the correct AD group.
B. The FortiGate firewall policy settings for SSL decryption.
C. The FortiGate FSSO active users list for user??s IP address.
D. The windows event viewer for failed login attempts.

Answer: C

Explanation:
Checking the active users list verifies if FortiGate correctly associates the user with their IP address, ensuring proper policy enforcement for internet access.

NEW QUESTION 6
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 7
Refer to the exhibit.

The NOC team connects to the FortiGate GUI with theNOC_Accessadmin 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. 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

Explanation:
The admintimeout setting in the admin access profile controls the inactivity timeout for GUI sessions. Increasing this value will extend the session duration before automatic disconnection.

NEW QUESTION 8
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. Administrators cannot change the configuration.
B. FortiGate skips quarantine actions.
C. Administrators must restart FortiGate to allow new session.
D. FortiGate drops new sessions requiring inspection.

Answer: BD

Explanation:
In fail-open mode, FortiGate skips quarantine actions to maintain traffic flow despite IPS or antivirus failures. FortiGate drops new sessions that require inspection when in conserve mode and fail-open is enabled, to
protect the network from potentially harmful traffic.

NEW QUESTION 9
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 10
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 10
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.

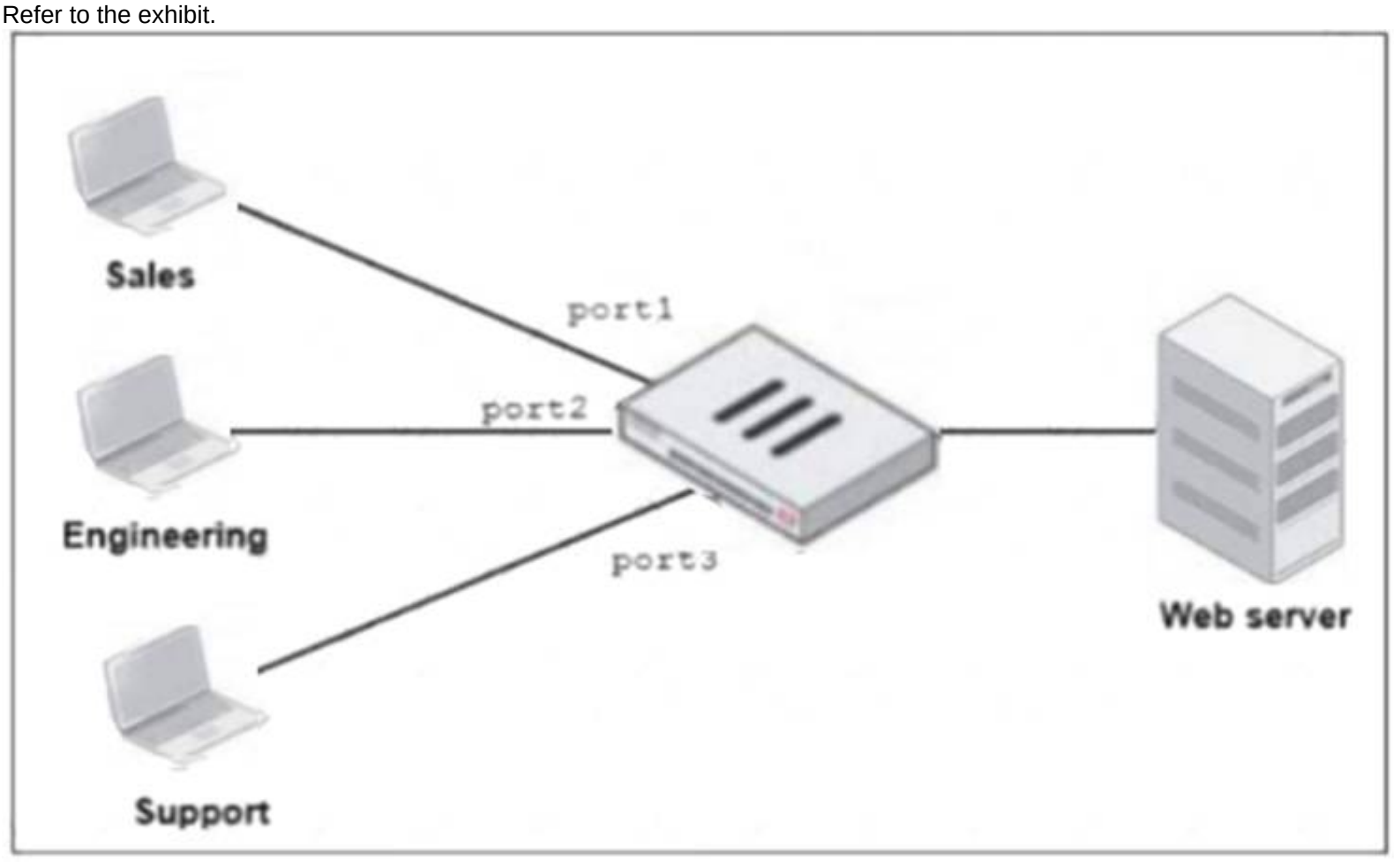
NEW QUESTION 13
Which two statements are correct when FortiGate enters conserve mode? (Choose two.)

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 17
Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.
Which action must the administrator perform to consolidate the two policies into one?

A. Create an Aggregate interface that includes port1 and port2 to create a single firewall policy.
B. Select port1 and port2 subnets in a single firewall policy.
C. Replace port1 and port2 with the any interface in a single firewall policy.

D. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy.

Answer: D

Explanation:
Enabling Multiple Interface Policies allows you to select multiple interfaces (like port1 and port2) in a single firewall policy, consolidating access rules for both Sales and Engineering to the web server.

NEW QUESTION 22
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 27
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. Enabled
B. On Idle
C. Disabled
D. On Demand

Answer: A

Explanation:
The "On Idle" DPD mode configures FortiGate to send DPD probes only when no inbound traffic is detected, meeting the requirement to send probes only when the tunnel is idle.

NEW QUESTION 32
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. FortiGate entered into IPS fail open state.
C. Administrator entered the command diagnose test application ipsmonitor 5.
D. Administrator entered the command diagnose test application ipsmonitor 99.

Answer: A

Explanation:
The output shows the IPS engine count as 0, indicating no active IPS engines are running. This typically means no firewall policy is referencing the IPS security profile, so the IPS profile is not being applied or triggered.

NEW QUESTION 36
.....

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