

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

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. NetAPI polling can increase bandwidth usage in large networks.
- C. The NetSessionEnum function is used to track user logouts.
- D. The collector agent must search Windows application event logs.

Answer: B

Explanation:

NetAPI polling mode involves frequent queries to domain controllers, which can cause increased bandwidth usage, especially in large networks with many login events.

NEW QUESTION 3

Which two statements describe characteristics of automation stitches? (Choose two.)

- 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

Explanation:

Automation stitches can execute multiple actions concurrently (in parallel).
Triggers for automation stitches can come from external connectors beyond just Fortinet devices.

NEW QUESTION 4

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 5

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?

- 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 6

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. TACAS+
- 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 7

An administrator wanted to configure an IPS sensor to block traffic that triggers a 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 filter, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

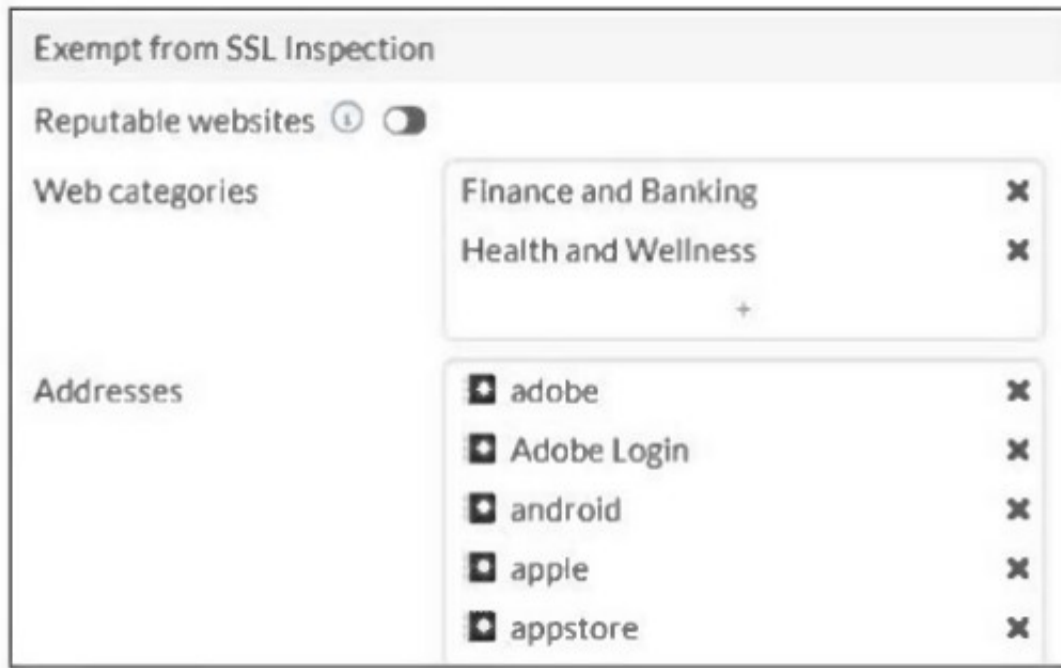
Answer: C

Explanation:

The IPS filter with the rate-mode set to "periodical" allows the administrator to block traffic that triggers a signature a specified number of times within a defined time period, meeting the requirement.

NEW QUESTION 8

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 FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.
- B. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
- C. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
- D. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.

Answer: AD

Explanation:

FortiGate's temporary SSL certificate may cause access denial to sites using HTTP Strict Transport Security (HSTS), so such sites are exempted from deep SSL inspection. Legal regulations require exemption of certain categories to protect user privacy and sensitive information, so these web categories are excluded from SSL inspection.

NEW QUESTION 9

When configuring a FortiGate in a multi-WAN setup, why would an administrator enable session preservation on an interface?

- A. To allow the FortiGate to dynamically change interfaces for all active sessions when a WAN link fails
- B. To make sure all sessions without source NAT enabled always use the primary WAN link
- C. To improve security by forcing users to authenticate again when the WAN link changes
- D. To ensure that existing SSL VPN connections remain on the same interface even if route changes occur

Answer: D

Explanation:

Session preservation keeps active sessions, such as SSL VPNs, tied to the original interface to prevent disruption when WAN routes change.

NEW QUESTION 10

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 default
- 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 default
- F. SD-WAN rules are skipped if only one route to the destination is available.
- G. By default
- 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 13

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 17

Refer to the exhibits.

Security Fabric logical topology view



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.)

- 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

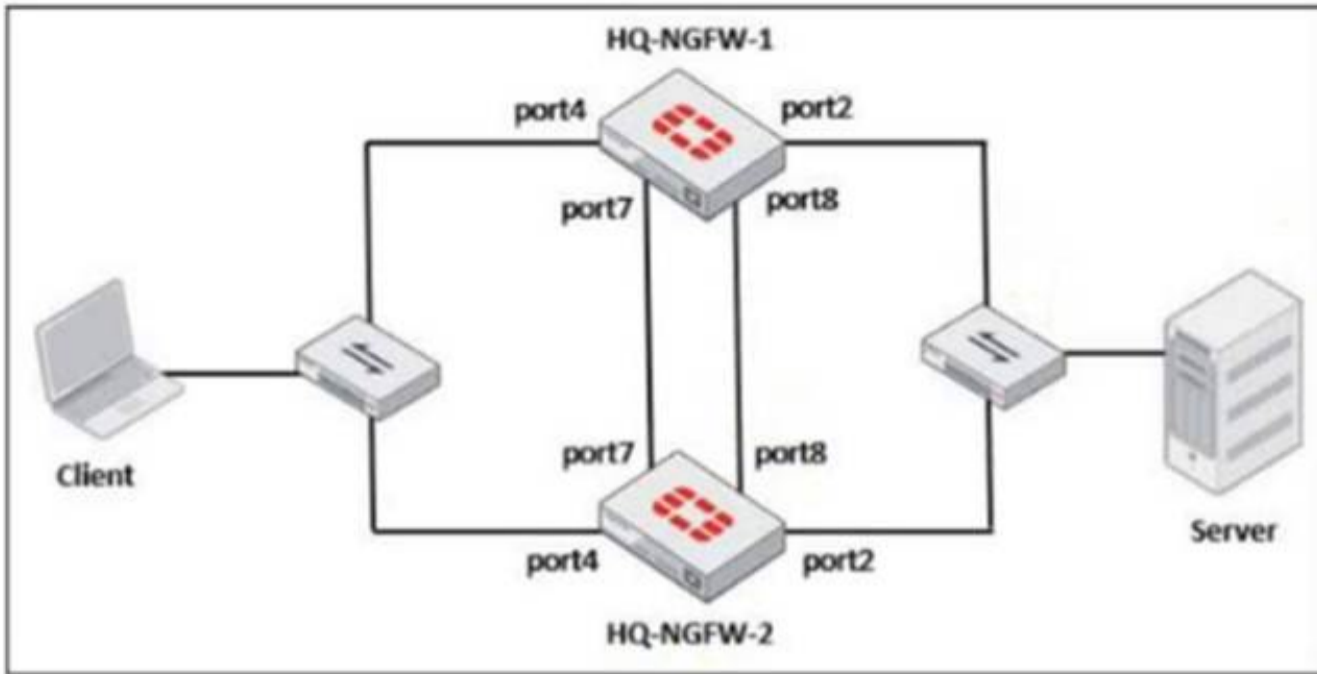
Explanation:

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 19

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 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 21

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A. They rely on session loss and jitter.
- B. They can be measured actively or passively.
- C. They are applied in a SD-WAN rule lowest cost strategy.
- D. They monitor the state of the FortiGate device.
- E. All the SLA targets can be configured.

Answer: ABE

Explanation:

SD-WAN SLAs monitor metrics like packet loss and jitter to evaluate link performance. SLA measurements can be performed using active probing or passive monitoring. Administrators can configure all SLA target parameters to define performance criteria.

NEW QUESTION 22

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 24

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.

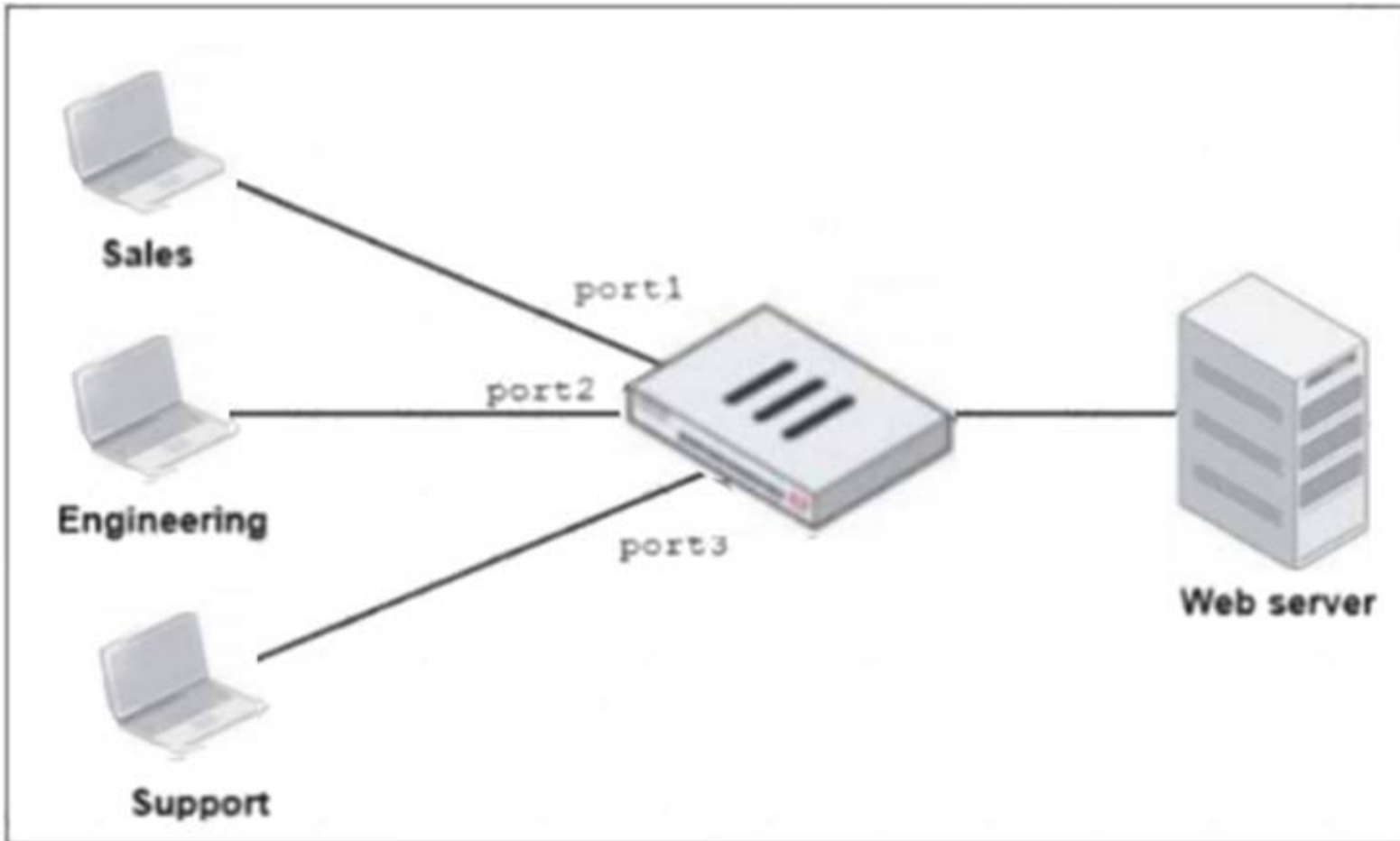
Answer: BD

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 26

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 28

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 31

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)

- A. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
- B. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP.
- C. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.
- D. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.

Answer: AD

NEW QUESTION 33

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 35

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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 First Try
- * FCP_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FGT_AD-7.6 Practice Test Here](#)