Fortinet

Exam Questions FCP_FGT_AD-7.6

FCP - FortiGate 7.6 Administrator

NEW QUESTION 1
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 2
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 3
A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy.
When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.
The administrator confirms that the traffic matches the configured firewall policy. What are two reasons for the failed virus detection by FortiGate? (Choose two.)

A. The selected SSL inspection profile has certificate inspection enabled.
B. The website is exempted from SSL inspection.
C. The El CAR test file exceeds the protocol options oversize limit.
D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: BD

NEW QUESTION 4
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 5
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 6
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 SLAtargets 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 7
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
```

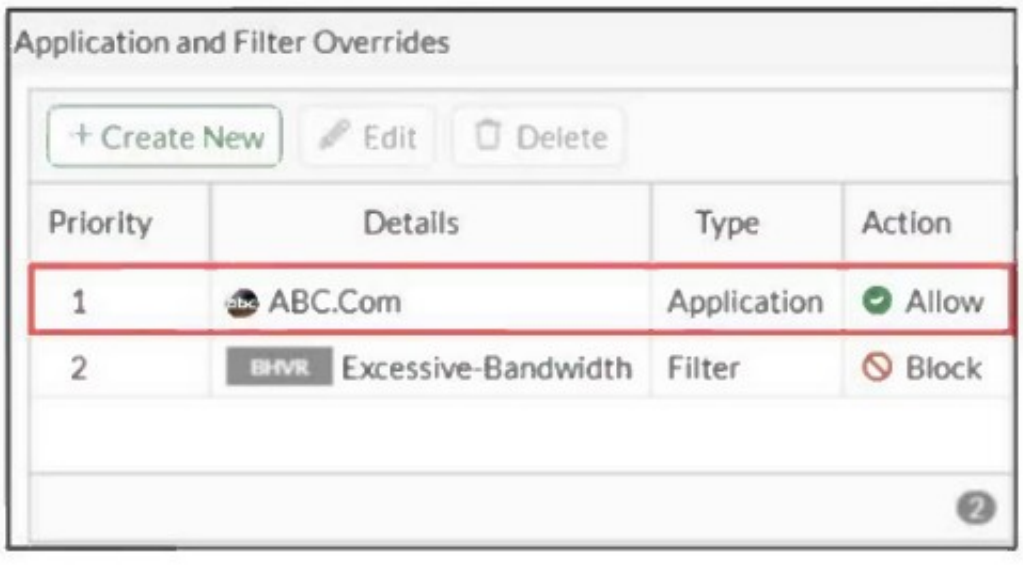
The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.
Based on the system performance output, what are the two possible outcomes? (Choose two.)

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 8
Refer to the exhibit.



An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow. This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.
Why are there no logs generated under security logs for ABC.Com?

A. The ABC.Com Type is set as Application instead of Filter.
B. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
C. The ABC.Com Action is set to Allow.
D. The ABC.Com is hitting the category Excessive-Bandwidth.

Answer: A

Explanation:
When the action is set to Allow in an application override, traffic matching this override is allowed without generating security logs because it bypasses deeper inspection and blocking.

NEW QUESTION 10
.....

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