VCE & PDF
GeekCert.com

# NSE7_EFW-7.0<sup>Q&As</sup>

## Fortinet NSE 7 - Enterprise Firewall 7.0

## Pass Fortinet NSE7_EFW-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.geekcert.com/nse7_efw-7-0.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

**Instant Download** After Purchase

**100% Money Back** Guarantee

**365 Days** Free Update

**800,000+** Satisfied Customers

**QUESTION 1**

Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

A. FortiGate limits the number of simultaneous sessions per explicit web proxy user. This limit CANNOT be modified by the administrator.

B. FortiGate limits the total number of simultaneous explicit web proxy users.

C. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator

D. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials. This limit CANNOT be modified by the administrator.

Correct Answer: B

Explanation: https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-WAN-opt- 52/web_proxy.htm#Explicit2
The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

**QUESTION 2**

Examine the output of the `diagnose sys session list expectation\\' command shown in the exhibit; than answer the question below.

```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
flags=00000000
sockflag= 00000000 sockport=0 av_idx=0 use=3¶
origin-shaper=¶
reply-shaper=¶
per ip_shaper=¶
ha_id=0 policy_dir=1 tunnel=/¶
state=new complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)¶
hook= pre dir=org act=noop 0.0.0.0.:0-> 0.0.0.0:0 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial1=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd type=0 dd_mode=0¶
```

Which statement is true regarding the session in the exhibit?

A. It was created by the FortiGate kernel to allow push updates from FotiGuard.

B. It is for management traffic terminating at the FortiGate.

C. It is for traffic originated from the FortiGate.

D. It was created by a session helper or ALG.

Correct Answer: D

**QUESTION 3**

Which two configuration commands change the default behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. set av-failopen off

B. set av-failopen pass

C. set fail-open enable

D. set ips fail-open disable

Correct Answer: AC

Explanation: https://docs.fortinet.com/document/fortigate/7.2.4/administration- guide/194558/conserve-mode

**QUESTION 4**

View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.



The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

However, the IKE real time debug does not show any output. Why?

A. The debug output shows phases 1 and 2 negotiations only. Once the tunnel is up, it does not show any more output.

B. The log-filter setting was set incorrectly. The VPN\\'s traffic does not match this filter.

C. The debug shows only error messages. If there is no output, then the tunnel is operating normally.

D. The debug output shows phase 1 negotiation only. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Correct Answer: B

**QUESTION 5**

Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode?
(Choose two.)

A. IPS failopen

B. mem failopen

C. AV failopen D. UTM failopen

Correct Answer: AC