NSE7_EFW-6.4^{Q&As}

Fortinet NSE 7 - Enterprise Firewall 6.4

Pass Fortinet NSE7_EFW-6.4 Exam with 100% Guarantee

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

https://www.passapply.com/nse7_efw-6-4.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.

B. TCP half close.

C. TCP time wait.

D. TCP session time to live.

Correct Answer: A

http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=f gtandfile=CLI_get_Commands.58.25.html The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACKremains in the table. The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACKremains in the table. The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in thetable. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

QUESTION 2

What does the dirty flag mean in a FortiGate session?

A. Traffic has been blocked by the antivirus inspection.

B. The next packet must be re-evaluated against the firewall policies.

C. The session must be removed from the former primary unit after an HA failover.

D. Traffic has been identified as from an application that is not allowed.

Correct Answer: B

https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119andsliceId=1

QUESTION 3

Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.

B. SIP ALG supports SIP HA failover; SIP helper does not.

C. SIP ALG supports SIP over IPv6; SIP helper does not.

D. SIP ALG can create expected sessions for media traffic; SIP helper does not.

E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Correct Answer: BCD

QUESTION 4

```
NGFW-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 2
Debug: 0
Cluster Uptime: 0 days 4:23:19
Cluster state change time: 2019-01-25 10:19:46
Master selected using:
  <2019/01/25 10:19:46> FGVM010000077649 is selected as the master because it has the largest value
of override priority.
  <2019/01/25 10:19:40> FGVM010000077649 is selected as the master because it's the only member in
the cluster.
ses_pickup: disable
override: enable
Configuration Status:
    FGVM010000077649 (updated 1 seconds ago): in-sync
    FGVM010000077650 (updated 0 seconds ago): out-of-sync
System Usage stats:
    FGVM010000077649 (updated 1 seconds ago):
        sessions=27, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=56%
    FGVM010000077650 (updated 0 seconds ago):
        sessions=2, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=57%
HBDEV stats:
    FGVM010000077649 (updated 1 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=63817615/202024/0/0, tx=
71110281/121109/0/0
    FGVM010000077650 (updated 0 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=79469596/122024/0/0, tx=
30877890/107878/0/0
Master: NGFW-1      , FGVM010000077649, cluster index = 1
Slave : NGFW-2      , FGVM010000077650, cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master: FGVM010000077649, operating cluster index = 0
Slave : FGVM010000077650, operating cluster index = 1
```

Refer to the exhibit, which contains the output of get system ha status. Which two statements about the output are true? (Choose two.)

A. The slave configuration is synchronized with the master.

B. port7 is used as the HA heartbeat on all devices in the cluster.

C. Primary is selected based on the priority configured under config system ha.

D. The HA management IP is 169.254.0.2.

Correct Answer: BC

QUESTION 5

When does a RADIUS server send an Access-Challenge packet?

A. The server does not have the user credentials yet.

B. The server requires more information from the user, such as the token code for two- factor authentication.

C. The user credentials are wrong.

D. The user account is not found in the server.

Correct Answer: B