NSE4_FGT-7.2$^{\text{Q\&As}}$

Fortinet NSE 4 - FortiOS 7.2

Pass Fortinet NSE4_FGT-7.2 Exam with 100% Guarantee

QUESTION 1

An employee needs to connect to the office through a high-latency internet connection.

Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

A. idle-timeout

B. login-timeout

C. udp-idle-timer

D. session-ttl

Correct Answer: B

FortiGate Infrastructure 7.2 Study Guide (p.222):

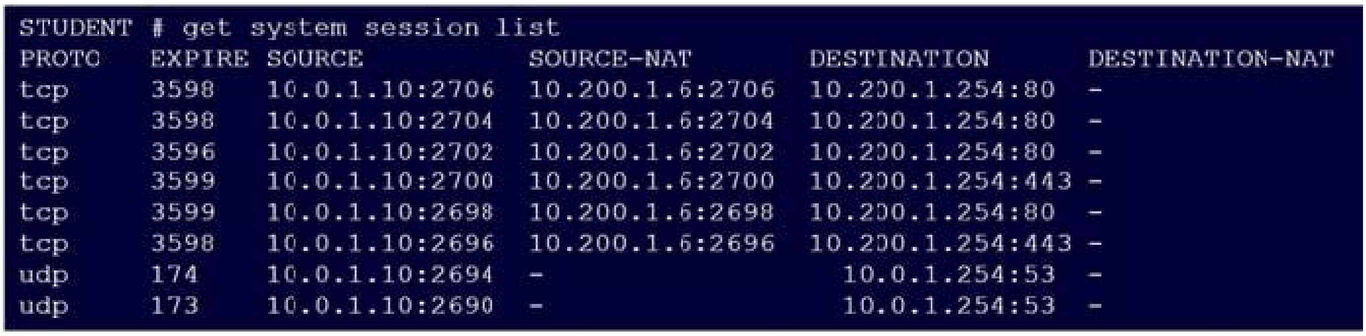
"When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under config vpn ssl

settings have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN

connections."

QUESTION 2

Refer to the exhibit.



```
STUDENT # get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT        DESTINATION        DESTINATION-NAT
tcp     3598   10.0.1.10:2706   10.200.1.6:2706   10.200.1.254:80    -
tcp     3598   10.0.1.10:2704   10.200.1.6:2704   10.200.1.254:80    -
tcp     3596   10.0.1.10:2702   10.200.1.6:2702   10.200.1.254:80    -
tcp     3599   10.0.1.10:2700   10.200.1.6:2700   10.200.1.254:443   -
tcp     3599   10.0.1.10:2698   10.200.1.6:2698   10.200.1.254:80    -
tcp     3598   10.0.1.10:2696   10.200.1.6:2696   10.200.1.254:443   -
udp     174    10.0.1.10:2694   -                   10.0.1.254:53    -
udp     173    10.0.1.10:2690   -                   10.0.1.254:53    -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

A. Destination NAT is disabled in the firewall policy.

B. One-to-one NAT IP pool is used in the firewall policy.

C. Overload NAT IP pool is used in the firewall policy.

D. Port block allocation IP pool is used in the firewall policy.

Correct Answer: B

FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

QUESTION 3

Which two statements are true about the FGCP protocol? (Choose two.)

A. FGCP elects the primary FortiGate device.

B. FGCP is not used when FortiGate is in transparent mode.

C. FGCP runs only over the heartbeat links.

D. FGCP is used to discover FortiGate devices in different HA groups.

Correct Answer: AC

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:

FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a

variety of factors, such as the device\\'s priority, to determine which device should be the primary.

FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices.

FGCP does not run over other types of links, such as data links.

Reference:

https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol

FortiGate Infrastructure 7.2 Study Guide (p.292): "FortiGate HA uses the Fortinet- proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health

of members. To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces."

QUESTION 4

An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value. Which timeout option should be configured on FortiGate?

A. auth-on-demand

B. soft-timeout

C. idle-timeout

D. new-session

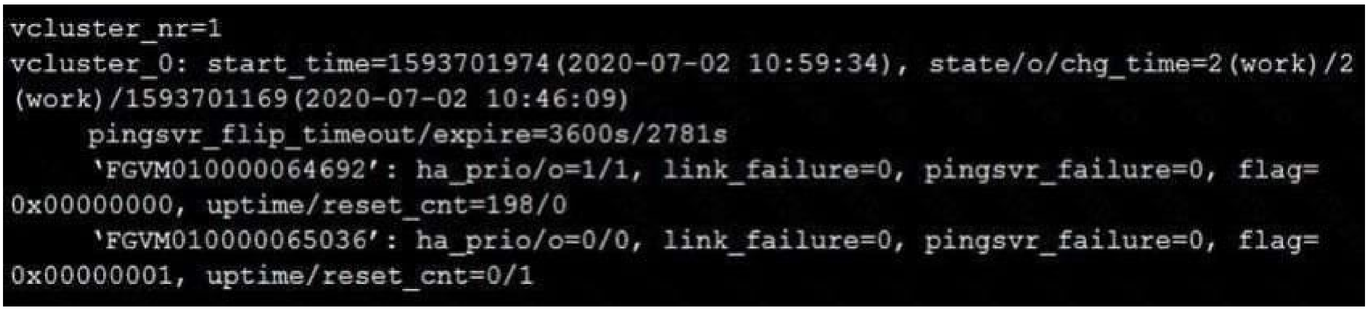
E. hard-timeout

Correct Answer: E

Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221#:~:text=Hard%20timeout%3A%20User%20
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Explanation-of-auth-timeout-types-for-Firewall/ta-p/189423

QUESTION 5

Refer to the exhibit.



```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
     pingsvr_flip_timeout/expire=3600s/2781s
     'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
     'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

The override setting is enable for the FortiGate with SN FGVM010000064692.

Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.

B. FortiGate devices are not in sync because one device is down.

C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.

D. FortiGate SN FGVM010000064692 has the higher HA priority.

Correct Answer: AD

Study Guide

NSE4_FGT-7.2 PDF Dumps NSE4_FGT-7.2 VCE Dumps NSE4_FGT-7.2 Exam Questions