

T estpassport Q&A



La meilleure qualité le meilleur service

<http://www.testpassport.fr>

Service de mise à jour gratuit pendant un an

Exam : **NSE7_EFW_6.2**

Title : Fortinet NSE 7 - Enterprise
Firewall 6.2

Version : DEMO

1.A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website.

The administrator executes the following debug commands and observes that the n-dns-timeout counter is increasing:

```
#diagnose test application wad 2200
```

```
#diagnose test application wad 104
```

DNS Stats:

```
n_dns_reqs=878  n_dns_fails= 2  n_dns_timeout=875
```

```
n_dns_success=0
```

```
n_snd_retries=0  n_snd_fails=0 n_snd_success=0 n_dns_overflow=0
```

```
n_build_fails=0
```

What should the administrator check to fix the problem?

- A. The connectivity between the FortiGate unit and the DNS server.
- B. The connectivity between the client workstations and the DNS server.
- C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.
- D. That DNS service is enabled in the explicit web proxy interface.

Answer: A

2.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.

Answer: A

Explanation:

http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=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 the table. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

3.Examine the output from the 'diagnose debug authd fssolist' command; then answer the question below.

```
# diagnose debug authd fssolist —FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAINING  
NGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is NOT the one
```

used by the workstation INTERNAL2. TRAINING. LAB.

What should the administrator check?

- A. The IP address recorded in the logon event for the user STUDENT.
- B. The DNS name resolution for the workstation name INTERNAL2. TRAINING. LAB.
- C. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2. TRAINING. LAB.
- D. The reserve DNS lookup for the IP address 192.168.3.1.

Answer: C

4. What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

- A. A process crash.
- B. Configuration changes.
- C. Changes in the status of any of the FortiGuard licenses.
- D. System entering to and leaving from the proxy conserve mode.

Answer: A D

Explanation:

diagnose debug crashlog read

```
275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated
276: 2014-08-05 13:03:53 proxy=acceptor service=ftp session fail mode=activated
277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated
278: 2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel
279: 2014-08-06 11:05:47 enters conserve mode"
280: 2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages"
281: 2014-08-06 13:07:16 msg="Kernel leaves conserve mode"
282: 2014-08-06 13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201283: 2014-08-06 13:07:16 marginexit=302
```

5. An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem.

Which statement is correct regarding this command?

- A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.
- B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
- C. Sends a link failed signal to all connected devices.
- D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

Answer: A