NSE7_EFW-6.0 Q&As

Fortinet NSE 7 - Enterprise Firewall 6.0

Pass Fortinet NSE7_EFW-6.0 Exam with 100% Guarantee

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

https://www.geekcert.com/nse7_efw-6-0.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

When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filler web requests when the client browser does not provide the server name indication (SNI) extension ?

A. FortiGate switches to the full SSL inspection method to decrypt the data.

B. FortiGate blocks the request without any further inspection.

C. FortiGate uses the Issued T: field in the server\\'s certificate.

D. FortiGate uses the requested URL from the user\\'s web browser.

Correct Answer: C

QUESTION 2

View the exhibit, which contains the output of a web filtering diagnose command, and then answer the question below.

```
# diagnose webfilter fortiguard statistics list
Rating Statistics:
==================
DNS failures                  :        273
DNS lookups                   :        280
Data send failures            :          0
Data read failures            :          0
Wrong package type            :          0
Hash table miss               :          0
Unknown server                :          0
Incorrect CRC                 :          0
Proxy request failures        :          0
Request timeout               :          1
Total requests                :       2409
Requests to FortiGuard servers :       1182
Server errored responses      :          0
Relayed rating                :          0
Invalid profile               :          0

Allowed                       :       1021
Blocked                       :       3909
Logged                        :       3927
Blocked Errors                :        565
Allowed Errors                :          0
Monitors                      :          0
Authenticates                 :          0
Warnings:                     :         18
Ovrd request timeout          :          0
Ovrd send failures            :          0
Ovrd read failures            :          0
Ovrd errored responses        :          0
...
```

```
# diagnose webfilter fortiguard statistics list
...
Cache Statistics:
=================
Maximum memory                :          0
Memory usage                  :          0

Nodes                         :          0
  Leaves                      :          0
  Prefix nodes                :          0
  Exact nodes                 :          0

Requests                      :          0
Misses                        :          0
Hits                          :          0
  Prefix hits                 :          0
  Exact hits                  :          0

No cache directives           :          0
Add after prefix              :          0
Invalid DB put                :          0
DB updates                    :          0

Percent full                  :         0%
  Branches                    :         0%
  Leaves                      :         0%
     Prefix nodes             :         0%
     Exact nodes              :         0%

Miss rate                     :         0%
Hit rate                      :         0%
  Prefix hits                 :         0%
  Exact hits                  :         0%
```

Which one of the following statements explains why the cache statistics are all zeros?

A. There are no users making web requests.

B. The administrator has reallocated the cache memory to a separate process.

C. The FortiGuard web filter cache is disabled in the FortiGate\\'s configuration.

D. FortiGate is using flow-based inspection which doesn\\'t use the cache.

Correct Answer: C

QUESTION 3

View the exhibit, which contains the partial output of a diagnose command, and then answer the question below.

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
  src: 0:10.1.2.0/255.255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
       ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
       ah=sha1 key=20 889f7529887c215c25950be2ba83e6fe1a5367be
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Based on the output, which one of the following statements is correct?

A. Quick mode selectors are disabled.

B. DPD is disabled.

C. Anti-replay is enabled.

D. Remote gateway IP is 10.200.5.1

Correct Answer: C

QUESTION 4

View the exhibit, which contains the output of a diagnose command, and then answer the question below.

```
FGT # diagnose debug rating
Locale        : english
Service       : Web-filter
Status        : Enable
License       : Contract
Service       : Antispam
Status        : Disable
Service       : Virus Outbreak Prevention
Status        : Disable
 -=- Server List (Mon Apr 19  10:41:32 20xx) -=-
IP                   Weight   RTT      Flags    TZ   Packets  Curr Lost     Total Lost
64.26.151.37         10       45                -5   262432   0             846
64.26.151.35         10       46                -5   329072   0             6806
66.117.56.37         10       75                -5   71638    0             275
65.210.95.240        20       71                -8   36875    0             92
209.222.147.36       20       103      DI       -8   34784    0             1070
208.91.112.194       20       107      D        -8   35170    0             1533
96.45.33.65          60       144               0    33728    0             120
80.85.69.41          71       226               1    33797    0             192
62.209.40.74         150      97                9    33754    0             145
121.111.236.179      45       44       F        -5   26410    26226         26227
```

Which statements are true regarding the output in the exhibit? (Choose two.)

A. FortiGate used 209.222.147.36 as the initial server to validate its contract.

B. Servers with the D flag are considered to be down.

C. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.

D. Servers with a negative TZ value are experiencing a service outage.

Correct Answer: AC

QUESTION 5

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer. If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any \\'esp\\'

B. diagnose sniffer packet any \\'tcp port 500 or tcp port 4500\\'

C. diagnose sniffer packet any \\'udp port 4500\\'

D. diagnose sniffer packet any \\'udp port 500\\'

Correct Answer: A