

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.leads4pass.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

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500,ifindex=7...
ike 0: IKEv1 exchange=Aggressive id=baf47d0988e9237f/2f405ef3952f6fda len=430
ike 0: in BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C0000000100000001000000300101000
ike 0:RemoteSite:4: initiator: aggressive mode get 1st response...
ike 0:RemoteSite:4: VID RFC 3947 4A131c81070358455C5728F20E95452F
ike 0:RemoteSite:4: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0:RemoteSite:4: peer is FortiGate/FortiOS (v5 b727)
ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C00000000
ike 0:RemoteSite:4: received peer identifier FQDN 'remote'
ike 0:RemoteSite:4: negotiation result
ike 0:RemoteSite:4: proposal id = 1:
ike 0:RemoteSite:4:   protocol id = ISAKMP:
ike 0:RemoteSite:4:     trans_id = KEY_IKE.
ike 0:RemoteSite:4:     encapsulation = IKE/none
ike 0:RemoteSite:4:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:RemoteSite:4:       type=OAKLEY_HASH_ALG, val=SHA.
ike 0:RemoteSite:4:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:RemoteSite:4:       type=OAKLEY_GROUP, val=MODP1024.
ike 0:RemoteSite:4: ISAKMP SA lifetime=86400
ike 0:RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key 16:B25B6C9384D8BDB24E3DA3DC90CF5E73
ike 0:RemoteSite:4: PSK authentication succeeded
ike 0:RemoteSite:4: authentication OK
ike 0:RemoteSite:4: add INITIAL-CONTACT
ike 0:RemoteSite:4: enc BAF47D0988E9237F405EF3952F6FDA081004010000000000000080140000181F2E48BFD8E9D603F
ike 0:RemoteSite:4: out BAF47D0988E9237F405EF3952F6FDA08100401000000000000008C2E3FC9BA061816A396F009A12
ike 0:RemoteSite:4: sent IKE msg (agg_i2send): 10.0.0.1:500-10.0.0.2:500, len=140, id=baf47d0988e9237f/2
ike 0:RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

Which of the following statements about this debug output are correct? (Choose two.)

- A. It shows a phase 1 negotiation.
- B. The initiator has provided remote as its IPsec peer ID.
- C. The negotiation is using AES128 encryption with CBC hash.
- D. The remote gateway IP address is 10.0.0.1.

Correct Answer: AB

QUESTION 2

View the central management configuration shown in the exhibit, and then answer the question below.

```
config system central-management
  set type fortimanager
  set fmg "10.0.1.242"
  config server-list
    edit 1
      set server-type rating
      set server-address 10.0.1.240
    next
    edit 2
      set server-type update
      set server-address 10.0.1.243
    next
    edit 3
      set server-type rating
      set server-address 10.0.1.244
    next
  end
  set include-default-servers enable
end
```

Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

- A. 10.0.1.244
- B. Public FortiGuard servers
- C. 10.0.1.240
- D. 10.0.1.242

Correct Answer: B

QUESTION 3

View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:H2S_0_0:2: received informational request
ike 0:H2S_0_0:2: processing notify type SHORTCUT_QUERY
ike 0:H2S_0_0: recv shortcut-query 409121717827462883 e501cb21acedd374/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 2 mode 0
ike 0:H2S_0_1: forward shortcut-query 409121717827462883
e501cb21acedd374/0000000000000000 100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl
ver 2 mode 0
...
...
ike 0:H2S_0_1:3: received informational request
ike 0:H2S_0_1:3: processing notify type SHORTCUT_REPLY
ike 0:H2S_0_1: recv shortcut-reply 409121717827462883 e501cb21acedd374/5478f99c94826e1c
100.64.5.1 to 10.1.1.254 psk 64 ppk 0
ike 0:H2S_0_0: forward shortcut-reply 409121717827462883
e501cb21acedd374/5478f99c94826e1c 100.64.5.1 to 10.1.1.254 psk 64 ppk 0 ttl 31
```

Based on the debug output, which phase-1 setting is enabled in the configuration of this VPN?

- A. auto-discovery-receiver
- B. auto-discovery-forwarder
- C. auto-discovery-sender
- D. auto-discovery-shortcut

Correct Answer: A

QUESTION 4

When using the SSL certificate inspection method to inspect HTTPS traffic, how does FortiGate filter 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 5

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     -5   262432   0          846
64.26.151.35  10     46    -5     -5   329072   0          6806
66.117.56.37  10     75    -5     -5   71638    0          275
65.210.95.240 20     71    -8     -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      0    33728    0          120
80.85.69.41   71     226   1      1    33797    0          192
62.209.40.74  150    97    9      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

[NSE7_EFW-6.0 PDF Dumps](#)

[NSE7_EFW-6.0 Practice Test](#)

[NSE7_EFW-6.0 Exam Questions](#)