

# DUMPS ARENA

## Fortinet NSE 7 - Enterprise Firewall 6.0

Fortinet NSE7 EFW-6.0

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

<https://dumpsarena.co>

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)

sales@dumpsarena.co  
dumpsarena.co

**QUESTION NO: 1**

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'

**ANSWER: A****QUESTION NO: 2**

How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

- A. FortiManager will respond to update requests only from a managed device.
- B. FortiManager can download and maintain local copies of FortiGuard databases.
- C. FortiManager supports only FortiGuard push update to managed devices.
- D. FortiManager does not support web filter rating requests.

**ANSWER: B****QUESTION NO: 3**

Which of the following statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose two.)

- A. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.
- B. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.
- C. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.
- D. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

**ANSWER: B C****QUESTION NO: 4**

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

```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

msg="received a request /tmp/.ipsengine_176_0_0.url.socket, addr len=37;
d=training.fortinet.com:80, id=289, cat=255, vname='root', vfid=0, profile='default',
type=0, client=10.0.1.10, url_source=1, url="/"
msg="Cache miss" user="N/A" src=10.0.1.10 sport=54218 dst=13.33.165.116 dport=80
service="http" hostname="training.fortinet.com" url="/" action=9(ftgd-block) vfi
act=3(BLOCK) user="N/A" src=10.0.1.10 sport=54218 dst=13.33.165.116 dport=80
service="http" cat=52 hostname="training.fortinet.com" url="/"
```

Which of the following statements are true regarding this output (Choose two.)

- A. This web request was inspected using the root web filter profile.
- B. The requested URL belongs to category ID 52.
- C. The web request was blocked by FortiGate.
- D. FortiGate found the requested URL in its local cache.

**ANSWER: A C****QUESTION NO: 5**

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

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st
message...
...
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278: protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278: trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278: encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278: type=OAKLEY_ENCRYPT_ALG,
val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278: type=OAKLEY_HASH_ALG,
val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278: type=AUTH_METHOD,
val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278: type=OAKLEY_GROUP,
val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/0000000000000000:278: protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278: trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278: encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278: type=OAKLEY_ENCRYPT_ALG,
val=AES_CBC, key-len=256.
ike 0:c49e59846861b0f6/0000000000000000:278: type=OAKLEY_HASH_ALG,
val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278: type=AUTH_METHOD,
val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278: type=OAKLEY_GROUP,
val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278: no SA
proposal chosen
```

Why didn't the tunnel come up?

- A. The remote gateway is using aggressive mode and the local gateway is configured to use main mode.
- B. The remote gateway's phase 1 configuration does not match the local gateway's phase 1 configuration.
- C. The remote gateway's phase 2 configuration does not match the local gateway's phase 2 configuration
- D. The pre-shared keys do not match.

**ANSWER: B**