



# NSE7\_EFW<sup>Q&As</sup>

NSE7 Enterprise Firewall - FortiOS 5.4

**Pass Fortinet NSE7\_EFW Exam with 100% Guarantee**

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

[https://www.pass4itsure.com/nse7\\_efw.html](https://www.pass4itsure.com/nse7_efw.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**

Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

- A. FortiGate limits the number of simultaneous sessions per explicit web proxy user. This limit CANNOT be modified by the administrator.
- B. FortiGate limits the total number of simultaneous explicit web proxy users.
- C. FortiGate limits the number of simultaneous sessions per explicit web proxy user. The limit CAN be modified by the administrator.
- D. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials. This limit CANNOT be modified by the administrator.

Correct Answer: C

---

**QUESTION 2**

An administrator added the following Ipsec VPN to a FortiGate configuration:

```
configvpn ipsec phasel -interface
```

```
edit "RemoteSite"
```

```
set type dynamic
```

```
set interface "port1"
```

```
set mode main
```

```
set psksecret ENC LCVkCiK2E2PhVUzZe
```

```
next
```

```
end
```

```
config vpn ipsec phase2-interface
```

edit "RemoteSite" set phasel name "RemoteSite" set proposal 3des-sha256 next end However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while

attempting the Ipsec connection. The output is shown in the exhibit.



```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=716
ike 0:xxx/xxx:16: responder: main mode get 1st message...
ike 0:xxx/xxx:16: VID RFC 3947 4A131C8107035B455C5728F20E95452F
...
ike 0:xxx/xxx:16: negotiation result
ike 0:xxx/xxx:16: proposal id = 1:
ike 0:xxx/xxx:16:   protocol id = ISAKMP:
ike 0:xxx/xxx:16:     trans_id = KEY IKE.
ike 0:xxx/xxx:16:     encapsulation = IKE/none
ike 0:xxx/xxx:16:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:xxx/xxx:16:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:xxx/xxx:16:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:xxx/xxx:16:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:xxx/xxx:16: ISAKMP SA lifetime=86400
ike 0:xxx/xxx:16: SA proposal chosen, matched gateway DialUpUsers
...
ike 0:DialUpUsers:16: sent IKE msg (ident_r1send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=380
ike 0:DialUpUsers:16: responder:main mode get 2nd message...
ike 0:DialUpUsers:16: NAT not detected
ike 0:DialUpUsers:16: sent IKE msg (ident_r2send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
ike 0:DialUpUsers:16: ISAKMP SA xxx/xxx key 16:3D33E2EF00BE927701B5C25B05A62415
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=108
ike 0:DialUpUsers:16: responder: main mode get 3rd message...
ike 0:DialUpUsers:16: probable pre-shared secret mismatch
ike 0:DialUpUsers:16: unable to parse msg
```

What is causing the IPsec problem in the phase 1 ?

- A. The incoming IPsec connection is matching the wrong VPN configuration
- B. The phase-1 mode must be changed to aggressive
- C. The pre-shared key is wrong
- D. NAT-T settings do not match

Correct Answer: C

### QUESTION 3

View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.



Name: default

Comments: Default web filtering. 22/255

FortiGuard category based filter

Show  Allow

- Bandwidth Consuming
- File Sharing and Storage

Status URL Filter

Block invalid URLs

URL Filter

|   |                                     |                                       |
|---|-------------------------------------|---------------------------------------|
| <input type="button" value="+ Create"/> | <input type="button" value="Edit"/> | <input type="button" value="Delete"/> |
|---|-------------------------------------|---------------------------------------|

| URL          | Type     | Action                                    | Status |
|--------------|----------|---|--------|
| *dropbox.com | Wildcard | <input checked="" type="checkbox"/> Block | Enable |

Web content filter

|   |                                     |                                       |
|---|-------------------------------------|---------------------------------------|
| <input type="button" value="+ Create new"/> | <input type="button" value="Edit"/> | <input type="button" value="Delete"/> |
|---|-------------------------------------|---------------------------------------|

| Pattern Type | Pattern   | Language | Action                                     | Status |
|--------------|-----------|----------|--|--------|
| Wildcard     | *dropbox* | Western  | <input checked="" type="checkbox"/> Exempt | Enable |



Which action will FortiGate take if a user attempts to access [www.dropbox.com](http://www.dropbox.com), which is categorized as File Sharing and Storage?

- A. FortiGate will exempt the connection based on the Web Content Filter configuration.
- B. FortiGate will block the connection based on the URL Filter configuration.
- C. FortiGate will allow the connection based on the FortiGuard category based filter configuration.
- D. FortiGate will block the connection as an invalid URL.

Correct Answer: B

---

#### QUESTION 4

Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

- A. Primary unit stops sending HA heartbeat keepalives.
- B. The FortiGuard license for the primary unit is updated.
- C. One of the monitored interfaces in the primary unit is disconnected.
- D. A secondary unit is removed from the HA cluster.

Correct Answer: AB

---

#### QUESTION 5

A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the ``diagnose debug authd fssolist'` command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

- A. The user student must not be listed in the CA's ignore user list.
- B. The user student must belong to one or more of the monitored user groups.
- C. The student workstation's IP subnet must be listed in the CA's trusted list.
- D. At least one of the student's user groups must be allowed by a FortiGate firewall policy.

Correct Answer: BD