



# NSE7\_EFW-6.0<sup>Q&As</sup>

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](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

View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.

```
NGFW-1 # diagnose sys session stat
misc info:      session_count=591 setup_rate=0 exp_count=0 clash=162
                memory_tension_drop=0 ephemeral=0/65536 removeable=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
    166 in NONE state
     1 in ESTABLISHED state
     3 in SYN_SENT state
     2 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000006
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

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

- A. There are 166 TCP sessions waiting to complete the three-way handshake.
- B. All the sessions in the session table are TCP sessions.
- C. There are 0 ephemeral sessions.
- D. No sessions have been deleted because of memory pages exhaustion.

Correct Answer: CD

## QUESTION 2

What does the dirty flag mean in a FortiGate session?

- A. The session must be removed from the former primary unit after an HA failover.
- B. Traffic has been identified as from an application that is not allowed.
- C. The next packet must be re-evaluated against the firewall policies.
- D. Traffic has been blocked by the antivirus inspection.



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/OB replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
life: type=01 bytes=0/0 timeout=43177/43200
dec: spi=cccl1f66d esp=aes key=16 280e5cd619bacc65ac771556c464ffbd
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 these partial outputs from two routing debug commands:



```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254
dev=2(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev=4(port3)
# get router info routing-table all
S*    0.0.0.0/0 [10/0] via 10.200.1.254, port1
      [10/0] via 10.200.2.254, port2, [10/0]
C     10.0.1.0/24 is directly connected, port3
C     10.200.1.0/24 is directly connected, port1
C     10.200.2.0/24 is directly connected, port2
```

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

- A. Both port1 and port2
- B. port3
- C. port2
- D. port1

Correct Answer: A

## QUESTION 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.

Correct Answer: B

[NSE7\\_EFW-6.0 PDF Dumps](#)

[NSE7\\_EFW-6.0 VCE Dumps](#)

[NSE7\\_EFW-6.0 Study Guide](#)