# 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.pass4itsure.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**

Which of the following statements are correct regarding application layer test commands? (Choose two.)

A. Some of them display statistics and configuration information about a feature or process.

B. They are used to filter real-time debugs.

C. They display real-time application debugs.

D. Some of them can be used to restart an application.

Correct Answer: AD

**QUESTION 2**

View the exhibit, which contains a partial routing table, and then answer the question below.

```
FGT # get router info routing-table all
...
Routing table for VRF=7
C       10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C       10.1.0.0/24 is directly connected, port3
S       10.10.4.0/24 [10/0] via 10.1.0.100, port3
C       10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S       10.1.0.0/24 [10/0] via 10.72.3.254, port4
C       10.72.3.0/24 is directly connected, port4
S       192.168.2.0/24 [10/0] via 10.72.3.254, port4
...
```

Assuming all the appropriate firewall policies are configured, which of the following pings will FortiGate route? (Choose two.)

A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.

B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.

C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.

D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Correct Answer: BC

**QUESTION 3**

View the following FortiGate configuration.

```
config system global
     set snat-route-change disable
end
config router static
     edit 1
          set gateway 10.200.1.254
          set priority 5
          set device "port1"
     next
     edit2
          set gateway 10.200.2.254
          set priority 10
          set device "port2"
     next
end
```

All traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

If the priority on route ID 1 were changed from 5 to 20, what would happen to traffic matching that user\\'s session?

A. The session would be deleted, so the client would need to start a new session.

B. The session would remain in the session table, and its traffic would still egress from port1.

C. The session would remain in the session table, and its traffic would start to egress from port2.

D. The session would remain in the session table, but its traffic would now egress from both port1 and port2.

Correct Answer: B

**QUESTION 4**

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 BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C000000010000000100000030010100
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 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:RemoteSite:4: received peer identifier FQDN 'remore'
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 BAF47D0988E9237F405EF3952F6FDA08100401000000000000000801400001812E48BFD8E9D603F
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 5**

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

NSE7_EFW-6.0 VCE Dumps | NSE7_EFW-6.0 Practice Test | NSE7_EFW-6.0 Exam Questions