



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 1

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

- A. Installing configuration changes to managed devices
- B. Importing interface mappings from managed devices
- C. Adding devices to FortiManager
- D. Previewing pending configuration changes for managed devices

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 2

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
    name: 'Hub2Spoke1'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
  SA
    lifetime/rekey: 43200/32137
    mtu: 1438
    tx-esp-seq: 2ce
    replay: enabled
  inbound
    spi: 01e54b14
    enc: aes-cb 914dc5d092667ed436ea7f6efb867976
    auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
  outbound
    spi: 3dd3545f
    enc: aes-cb 017b8ff6c4ba21eac99b22380b7de74d
```

praw709528

Based on the output, which two statements are correct? (Choose two.)

- A. Phase 2 authentication is set to sha1 on both sides.
- B. Anti-replay is disabled.
- C. Hub2Spoke1 is a policy-based VPN.
- D. Hub2Spoke1 is configured on interface wan2.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 3

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows the output of a debug command.

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 send 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

praw709528

Which two statements about the output are true? (Choose two.)

- A. The local FortiGate OSPF router ID is 0.0.0.4.
- B. Port4 is connected to the OSPF backbone area.
- C. In the network connected to port4, two OSPF routers are down.
- D. The local FortiGate is the backup designated router.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 4

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which contains the partial output of a diagnose command.

```
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=42403/0B 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 280e5cd6f9bacc65ac771556c464ffbd
    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
```

praw709528

Based on the output, which two statements are correct? (Choose two.)

- A. Anti-replay is enabled
- B. The remote gateway IP is 10.200.4.1.
- C. DPD is disabled.
- D. Quick mode selectors are disabled.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 5

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7. . . .
ike 0: IKEv2 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response. . .
ike 0: Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated
ike 0: Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: received peer identifier FQDN 'remote'
ike 0: Remotesite:3: negotiation result
ike 0: Remotesite:3: proposal id = 1:
ike 0: Remotesite:3:     protocol id = ISAKMP:
ike 0: Remotesite:3:     trans_id = KEY_IKE.
ike 0: Remotesite:3:     encapsulation = IKE/none.
ike 0: Remotesite:3:     type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: Remotesite:3:     type=OAKLEY_HASH_ALG, val=SHA.
ike 0: Remotesite:3:     type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: Remotesite:3:     type=OAKLEY_GROUP, val=MODP1024.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key
16:39915120ED73ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc
A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0: Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140,
id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

praw709528

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

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

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 6

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows the output of a BGP debug command.

```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor      V      AS      MsgRcvd  MsgSent  TblVer  InQ    OutQ    Up/Down  State/PfxRcd
10.125.0.60   4    65060    1698     1756    103     0       0    03:02:49      1
10.127.0.75   4    65075    2206     2250    102     0       0    02:45:55      1
100.64.3.1    4    65501    101      115     0       0       0    never          Active

Total number of neighbors 3
```

praw709528

Which statement about the exhibit is true?

- A. The local router has not established a TCP session with 100.64.3.1
- B. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.
- C. Since the counters were last reset, the 100.64.3.1 peer has never been down.
- D. The local router has received a total of three BGP prefixes from all peers.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 7

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which contains a TCL script configuration on FortiManager.

Type	TCL Script ▼
Run script on	Remote FortiGate... ▼
Script details	<pre>#!/ proc do_cmd {cmd} { puts [exec "\$cmd\n" "#" 10] } run_cmd "config system interface" run_cmd "edit port1" run_cmd "set ip 10.0.1.10 255.255.255.0" run_cmd "next" run_cmd "end"</pre>

An administrator has configured the TCL script on FortiManager, but the TCL script failed to apply any changes to the managed device after being run.

Why did the TCL script fail to make any changes to the managed device?

- A. The TCL script must start with #include <>.
- B. The TCL command run_cmd has not been created.
- C. Changes to an interface configuration can be made only by a CLI script.
- D. Incomplete commands are ignored in TCL scripts.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 8

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which contains the debug output of diagnose dvm device list.

```
FMG-VM64# diagnose dvm device list
There are currently 1 devices/vdoms managed:
TYPE      OID      SN      HA      IP      NAME      ADOM      IPS  FIRMWARE
fmg/      217     FGVM01... -    10.200.1.1 Local-FortiGate My_ADOM 15.0.0831 6.0 MR4 (1579)
faz enabled
          |- STATUS: db: modified; conf: in sync; cond: pending; dm: retrieved; conn: up

          |- vdom: [3] root flags:0 adom:My_ADOM pkg: [imported] Local-FortiGate_root
praw709528
```

Which two statements about the output shown in the exhibit are correct? (Choose two.)

- A. ADOMs are disabled on the FortiManager
- B. The FortiGate configuration is in sync with latest running revision history.
- C. There are pending device-level changes yet to be installed on Local-FortiGate.
- D. The policy package has been modified for Local-FortiGate.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 9

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows a FortiGate configuration.

```
config system fortiguard
  set protocol udp
  set port 8888
  set load-balance-servers 1
  set auto-join-forticloud enable
  set update-server-location any
  set sandbox-region ""
  set fortiguard-anycast disable
  set antispam-force-off disable
  set antispam-cache enable
  set antispam-cache-ttl 1800
  set antispam-cache-mpercent 2
  set antispam-timeout 7
  set webfilter-force-off enable
  set webfilter-cache enable
  set webfilter-cache-ttl 3600
  set webfilter-timeout 15
  set sdns-server-ip "208.91.112.220"
  set sdns-server-port 53
  unset sdns-options
  set source-ip 0.0.0.0
  set source-ip6 ::
  set proxy-server-ip 0.0.0.0
  set proxy-server-port 0
  set proxy-username ""
  set ddns-server-ip 0.0.0.0
  set ddns-server-port 443
end
```

praw709528

An administrator is troubleshooting a web filter issue on FortiGate. The administrator has configured a web filter profile and applied it to a policy; however, the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator change to fix the issue?

- A. The administrator must increase webfilter-timeout.
- B. The administrator must disable webfilter-force-off.
- C. The administrator must change protocol to TCP.
- D. The administrator must enable fortiguard-anycast.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 10

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

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 uses the CN information from the Subject field in the server certificate.
- B. FortiGate switches to the full SSL inspection method to decrypt the data.
- C. FortiGate uses the requested URL from the user's web browser.
- D. FortiGate blocks the request without any further inspection.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 11

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:H2S_0_1:1249: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0_1:  rcv shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000 100.64.3.1
10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0
ike 0:H2S_0: iif 13 10.1.1.254->10.1.2.254 route lookup oif 13
ike 0:H2S_0_0: forward shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 31 ver 1 mode 0, ext-ma
ike 0:H2S_0_0:1248: sent IKE msg (SHORTCUT-QUERY): 100.64.1.1:500->100.64.5.1:500, len=236,
id=e2beec89f13c7074/06a73dfb3a5d3b54:340a645c
ike 0: comes 100.64.5.1:500->100.64.1.1:500, ifindex=3. . .
ike 0: IKEv1 exchange=Informational id=e2beec89f13c7074/06a73dfb3a5d3b5d:26254ae9 len=236
ike 0:H2S_0_0:1248: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: rcv shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0 100.64.5.1
to 10.1.1.254 psk 64 ppk 0 ver 1 mode 0 ext-mapping 100.64.3.1:500
ike 0:H2S_0: iif 13.10.1.2.254->10.1.1.254 route lookup oif 13
ike 0:H2S_0_1: forward shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0
100.64.5.1 to 10.1.1.254 psk 64 ppk 0 ttl 31 ver 1 mode 0 ext-mapping 100.
```

praw709528

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 12

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Which two statements about OCVPN are true? (Choose two.)

- A. Only root vdom supports OCVPN.
- B. OCVPN supports static and dynamic IPs in WAN interface.
- C. OCVPN offers only Hub-Spoke VPNs.
- D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 13

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows a central management configuration.

```
config system central-management
  set type fortimanager
  set fmg "10.0.1.242"
  config server-list
    edit 1
      set server-type rating
      set addr-type ipv4
      set server-address 10.0.1.240
    next
    edit 2
      set server-type update
      set addr-type ipv4
      set server-address 10.0.1.243
    next
    edit 3
      set server-type rating
      set addr-type ipv4
      set server-address 10.0.1.244
    next
  end
  set include-default-servers enable
end
```

praw709528

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 14

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Which two statements about application layer test commands are true? (Choose two.)

- A. They display real-time application debugs.
- B. They are used to filter real-time debugs.
- C. Some of them can be used to restart an application.
- D. Some of them display statistics and configuration information about a feature or process.

Show Suggested Answer





Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 15

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

- A. mem failopen
- B. IPS failopen
- C. AV failopen
- D. UTM failopen

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 16

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device. The administrator decides to enable the setting link-failed-signal to fix the problem.

Which statement about this setting is true?

- A. It sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
- B. It sends a link failed signal to all connected devices.
- C. It disabled all the non-heartbeat interfaces in all HA members for two seconds after a failover.
- D. It forces the former primary device to shut down all its non-heartbeat interfaces for one second, while the failover occurs.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 17

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows the output of a diagnose command.

```
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 10:42:32 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 two statements about the output in the exhibit are true? (Choose two.)

- A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.
- B. Servers with a negative TZ value are experiencing a service outage.
- C. Servers with the D flag are considered to be down.
- D. FortiGate used 209.222.147.36 as the initial server to validate its contract.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 18

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows a session table entry.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=11 duration=35 expire=265 timeout=300 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=redir local may_dirty none app_ntf
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=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443(172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545(192.167.1.100:49545)
pos/ (before,after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
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
```

praw709528

Which statement about FortiGate inspection of this session is true?

- A. FortiGate forwarded this session without any inspection.
- B. FortiGate applied proxy-based inspection.
- C. FortiGate applied flow-based NGFW policy-based inspection.
- D. FortiGate applied flow-based inspection.

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 19

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

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

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

Show Suggested Answer



Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 20

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibits, which show the configuration on FortiGate and partial session information.

```
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
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

```
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:f7a1: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
rpd_b_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:
```

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. If the priority on route ID 1 were changes from 5 to 20, what would happen to traffic matching that user session?

- A. The session would remain in the session table, and its traffic would still egress from port1.
- B. The session would be deleted, and the client would need to start a new session.
- 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.

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 21

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows the output of diagnose sys session list.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 scokflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
origin-> sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=poat dir=org act=snat 10.0.1.10:65464->54.192.15.182:80 (100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464 (10.0.1.10:65464)
pos/ (before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

prw709528

If the HA ID for the primary device is 0, which statement about the output is true?

- A. This session cannot be synced with the secondary device.
- B. This session is for HA talk traffic.
- C. The inspection of this session has been offloaded to the secondary device.
- D. The master unit is processing this traffic

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 22

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows the output of diagnose sys session stat.

```
NGFW-1 # diagnose sys session stat
misc info:      session_count=591 setup_rate=0 exp_count=0 clash=
memory_tension_drop=0 ephemeral=0/65536 removable=0
delete=0, flush=0, dev_down=0/0
TCP session:
  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_rcv=00000000
url_rcv=00000000
av_rcv=00000000
fqdn_count=00000006
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

praw709528

Which two statements about the output shown in the exhibit are correct? (Choose two.)

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

Show Suggested Answer

Actual exam question from Fortinet's NSE7_EFW-6.4

Question #: 23

Topic #: 1

[\[All NSE7_EFW-6.4 Questions\]](#)

Refer to the exhibit, which shows a partial routing table.

```
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
. . .
praw709528
```

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

- A. Source IP address: 10.73.9.10, Destination IP address: 10.72.3.15
- B. Source IP address: 10.72.3.52, Destination IP address: 10.1.0.254
- C. Source IP address: 10.10.4.24, Destination IP address: 10.72.3.20
- D. Source IP address: 10.1.0.10, Destination IP address: 10.64.1.52

Show Suggested Answer