

# Fortinet

## Exam Questions NSE7\_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0



### NEW QUESTION 1

View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

```
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
```

Which of the following statements about the exhibit are true? (Choose two.)

- A. The local router's BGP state is Established with the 10.125.0.60 peer.
- B. Since the counters were last reset, the 10.200.3.1 peer has never been down.
- C. The local router has received a total of three BGP prefixes from all peers.
- D. The local router has not established a TCP session with 100.64.3.1.

**Answer: AD**

### NEW QUESTION 2

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:

```
# diagnose ip router bgp all enable
# diagnose ip router bgp level info
# diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byte
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

Which statements are true regarding the output in the exhibit? (Choose two.)

- A. BGP peers have successfully interchanged Open and Keepalive messages.
- B. Local BGP peer received a prefix for a default route.
- C. The state of the remote BGP peer is OpenConfirm.
- D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

**Answer: AB**

### NEW QUESTION 3

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
rpd_b_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
```

Which statement about FortiGate behavior relating to this session is true?

- A. FortiGate redirected the client to the captive portal to authenticate, so that a correct policy match could be made.
- B. FortiGate forwarded this session without any inspection.
- C. FortiGate is performing security profile inspection using the CP
- D. FortiGate applied only IPS inspection to this session.

**Answer: C**

**Explanation:**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 91, 92 First digit of "proto\_state" value at 1 and considering all counters are at 0 for HW acceleration means CPU usage

**NEW QUESTION 4**

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
```

Which server will FortiGate choose for web filter rating requests, if 10.0.1.240 is experiencing an outage?

- A. Public FortiGuard servers
- B. 10.0.1.243
- C. 10.0.1.242
- D. 10.0.1.244

**Answer: D**

**Explanation:**

by default, ( include-default-servers ) enabled .this allows fortigate to communicate with the public fortiguard servers , if the fortimanager devices (configured in server-list) are unavailable .



**NEW QUESTION 5**

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

A. Firewall monitor.  
B. Policy monitor.  
C. Logs.  
D. Crashlogs.

**Answer:** CD

**NEW QUESTION 6**

An administrator has decreased all the TCP session timers to optimize the FortiGate memory usage. However, after the changes, one network application started to have problems. During the troubleshooting, the administrator noticed that the FortiGate deletes the sessions after the clients send the SYN packets, and before the arrival of the SYN/ACKs. When the SYN/ACK packets arrive to the FortiGate, the unit has already deleted the respective sessions. Which TCP session timer must be increased to fix this problem?

A. TCP half open.  
B. TCP half close.  
C. TCP time wait.  
D. TCP session time to live.

**Answer:** A

**Explanation:**

[http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI\\_get\\_Commands.58.25.html](http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI_get_Commands.58.25.html)  
The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACK remains in the table.  
The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACK remains in the table.  
The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in the table. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

**NEW QUESTION 7**

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

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>

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

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

**Answer:** A

**Explanation:**

<https://docs.fortinet.com/document/fortimanager/7.2.2/administration-guide/914165/tcl-scripts>

**NEW QUESTION 8**

Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # 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=100.64.1.254 dev=3(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=100.64.2.254 dev=6(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9(port3)

FortiGate # get router info routing-table all

Routing table for VRF=0
S*   0.0.0.0/0 [10/0] via 100.64.1.254, port1
      [10/0] via 100.64.2.254, port2, [10/0]
C    10.1.0.0/24 is directly connected, port3
S    10.1.10.0/24 [10/0] via 10.1.0.1, port3
C    100.64.1.0/24 is directly connected, port1
C    100.64.2.0/24 is directly connected, port2
```

Which change must an administrator make on FortiGate to route web traffic from internal users to the internet, using ECMP?

- A. Set the priority of the static default route using port1 to 10. Most Voted
- B. Set the priority of the static default route using port2 to 1.
- C. Set preserve-session-route to enable.
- D. Set snat-route-change to enable.

**Answer: A**

**Explanation:**

ECMP pre-requisite is "routes must have the same destination and costs. In the case of static routes, costs include distance and priority". In this case traffic is routed through port 1 because of the lower priority. If we raise priority on port 1 to the value of 10 the traffic should be routed through both ports 1 and 2.  
<https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/25967/equal-cost-multi-path>

**NEW QUESTION 9**

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
A2FBD6BB6394401A06B89C022D4DF682081004010000000000000500B000018882A07BE09026CA8B2
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
```

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.

**Answer: BC**

**NEW QUESTION 10**

Refer to the exhibit, which shows a partial web filter profile configuration.

FortiGuard Category Based Filter

Name	Action
<div><div></div>Bandwidth Consuming 6</div>	
Freeware and Software Downloads	<div></div> Allow
File Sharing and Storage	<div></div> Block

Static URL Filter

URL Filter

+ Create New

Edit

Delete

Search

URL	Type	Action	Status
*.dropbox.com	Wildcard	<div></div> Allow	<div></div> Enable

Content Filter

+ Create New

Edit

Delete

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	<div></div> Exempt	<div></div> Enable

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

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

Answer: A

Explanation:

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 351 url filter -> FortiGuard Web Filter -> Web Content Filter -> Advanced Filter Options Allow -> Block

NEW QUESTION 10

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

- A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
- B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.
- C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
- D. Branch FortiGate devices must be configured first.

Answer: BC

NEW QUESTION 12

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

Create

Edit

Delete

URL	Type	Action	Status
*dropbox.com	Wildcard	<div></div> Block	Enable

Web content filter

Create new

Edit

Delete

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	<div>E</div> Exempt	Enable

Which action will FortiGate take if a user attempts to access 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.

Answer: B

Explanation:

fortigate does it in order Static URL -> FortiGuard -> Content -> Advanced (java, cookie removal..)so block it in first step

NEW QUESTION 14

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.

Answer: AB

NEW QUESTION 16

An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

```
# debug application fnbamd -1
# diagnose debug enable
# diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 5 for student in WindowsLDAP opt=27 prot=0
fnbamd_fsm.c[336] __compose_group_list_from_req-Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server
'WindowsLDAP'
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_auth_session-Total 1 server(s) to try
fnbamd_ldap.c[437] start_search_dn-base:'cn=user,dc=trainingAD,dc=training,dc=lab'
filter:cn=student
fnbamd_ldap.c[1730] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[2407] auth_ldap_result-Continue pending for req 5
fnbamd_ldap.c[480] get_all_dn-Found no DN
fnbamd_ldap.c[503] start_next_dn_bind-No more DN left
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 5
fnbamd_fsm.c[568] destroy_auth_session-delete session 5
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the output in the exhibit, what can cause this authentication problem?

- A. User student is not found in the LDAP server.
- B. User student is using a wrong password.
- C. The FortiGate has been configured with the wrong password for the LDAP administrator.
- D. The FortiGate has been configured with the wrong authentication schema.

**Answer: A**

#### NEW QUESTION 17

Refer to the exhibit, which contains 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 sockflag=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
gw=100.64.1.254/10.0.1.10
hook-post 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
```

If the HA ID for the primary unit is zero (0), which statement about the output is true?

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

**Answer: C**

#### NEW QUESTION 20

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
    auth: sha1 edd8141f4956140eef703d9042621d3dbf5cd961
  NPU acceleration: encryption(outbound) decryption(inbound)
```

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

- A. The npu\_flag for this tunnel is 03.
- B. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.
- C. Anti-replay is enabled.
- D. The npu\_flag for this tunnel is 02.

**Answer:** AC

#### NEW QUESTION 25

A FortiGate's port1 is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP. Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)

- A. Both session have the local flag on.
- B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.
- C. One session has the proxy flag on, the other one does not.
- D. One of the sessions has the IP address of port2 as the source IP address.

**Answer:** AD

#### NEW QUESTION 29

Refer to the exhibit, which shows a session entry. Which statement about this session is true?

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tup
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
origin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.1
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

- A. It is an ICMP session from 10.1.10.10 to 10.200.5. 1.
- B. It is a TCP session in close\_wait state, from 10.
- C. 10.10 to 10.200.1.1.
- D. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
- E. It is a TCP session in the established state, from 10.1.10.10 to 10.200.5.1.

**Answer:** A

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/1969>

**NEW QUESTION 31**

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 sent 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
```

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

- A. In the network connected to port 4, two OSPF routers are down.
- B. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.5.
- C. Based on the network type of port 4, OSPF hello packets will be sent to 224.0.0.6.
- D. There are a total of 5 OSPF routers attached to the Port4 network segment.

**Answer:** BD

**NEW QUESTION 34**

What are two functions of automation stitches? (Choose two.)

- A. Automation stitches can be configured on any FortiGate device in a Security Fabric environment.
- B. An automation stitch configured to execute actions sequentially can take parameters from previous actions as input for the current action.
- C. Automation stitches can be created to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.
- D. An automation stitch configured to execute actions in parallel can be set to insert a specific delay between actions.

**Answer:** BC

**Explanation:**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 23, 26

**NEW QUESTION 37**

Examine the following traffic log; then answer the question below.

date=20xx-02-01 time=19:52:01 devname=master device\_id="xxxxxxx" log\_id=0100020007 type=event subtype=system pri critical vd=root service=kemel status=failure msg="NAT port is exhausted."

What does the log mean?

- A. There is not enough available memory in the system to create a new entry in the NAT port table.
- B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
- C. FortiGate does not have any available NAT port for a new connection.
- D. The limit for the maximum number of entries in the NAT port table has been reached.

**Answer:** B

**NEW QUESTION 39**

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.

What can the administrator do to fix this problem?

- A. Configure remote link monitoring to detect an issue in the forwarding path.
- B. Configure set send-garp-on-failover enable under config system ha on both cluster members.
- C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.
- D. Configure set link-failed-signal enable under config system ha on both cluster members.

**Answer:** D

**Explanation:**

Virtual MAC Address and Failover - The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port. - Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces): #Config system ha set link-failed-signal enable end - This simulates a link failure that clears the related entries from MAC table of the switches.



**NEW QUESTION 44**

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
    edit 2
        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:

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=17 expire=7 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic(bytes/packets/allow_err): org=57555/7/1 reply=23367/19/1 tuples=2
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)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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 remain in the session table, and its traffic would still egress from port1.
- B. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
- C. The session would remain in the session table, and its traffic would start to egress from port2.
- D. The session would be deleted, so the client would need to start a new session.

**Answer:** A

**Explanation:**

<http://kb.fortinet.com/kb/documentLink.do?externalID=FD40943>

**NEW QUESTION 48**

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
...
```

Assuming all the appropriate firewall policies are configured, what two changes would an administrator need to make if they wanted to send traffic from a client directly connected to port3, to a server directly connected to port4? (Choose two.)

- A. Configure route leaking between VRF 12 and VRF 21.
- B. Disable auto-asic-offload as this is not supported between VRF instances.
- C. Configure RIPv2 to exchange route information between the VRF instances.
- D. Configure route leaking between port3 and port4.
- E. Enable SNAT on the relevant firewall policies to prevent RPF check drops.

**Answer:** AE

**Explanation:**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 148, 159

**NEW QUESTION 51**

Which statement about IKE and IKE NAT-T is true?

- A. IKE is used to encapsulate ESP traffic in some situations, and IKE NAT-T is used only when the local FortiGate is using NAT on the IPsec interface.
- B. IKE is the standard implementation for IKEv1 and IKE NAT-T is an extension added in IKEv2.
- C. They both use UDP as their transport protocol and the port number is configurable.
- D. They each use their own IP protocol number.

**Answer:** C

**Explanation:**

IKE without NAT-T runs over UDP port 500. IKE with NAT-T runs over UDP port 4500. It can be configurable - <https://docs.fortinet.com/document/fortigate/7.0.0/new-features/33578/configurable-ike-port>

**NEW QUESTION 53**

Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

- A. FortiGate first checks the OSPF ID to elect a DR.
- B. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.
- C. BDR is responsible for forwarding link state information from one router to another.
- D. Only the DR receives link state information from non-DR routers.

**Answer:** B

**NEW QUESTION 58**

What does the dirty flag mean in a FortiGate session configured for NGFW policy mode?

- A. The existing session table entry has been updated with the app\_id and the firewall policy table needs to be checked for a match.
- B. The application or URL category is unknown and needs to be rescanned by the IPS engine to try to identify the Layer 7 details.
- C. The URL category for this session has been updated by FortiGuard and the session needs to be checked against the policy again to ensure proper web filtering is applied.
- D. Traffic has been identified as coming from an application that is not allowed and the relevant replacement message needs to be displayed to the user, if configured.

**Answer:** A

**Explanation:**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 99

**NEW QUESTION 62**

What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)

- A. Reduce the session time to live.

- B. Increase the TCP session timers.
- C. Increase the FortiGuard cache time to live.
- D. Reduce the maximum file size to inspect.

**Answer:** AD

#### NEW QUESTION 67

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.

**Answer:** AD

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828>

#### NEW QUESTION 72

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

```
ike 0:9268ab9dea63aa3/0000000000000000:591: responder: main mode get 1st message...
ike 0:9268ab9dea63aa3/0000000000000000:591: incoming proposal:
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 0:
ike 0:9268ab9dea63aa3/0000000000000000:591: protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591: trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591: encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id=0:
ike 0:9268ab9dea63aa3/0000000000000000:591: protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591: trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591: encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: my proposal, gw VPN:
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591: protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591: trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591: encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591: protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591: trans_id = KEY_IKE.
ike 0:9268ab9dea63aa3/0000000000000000:591: encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_GROUP, val=MODP2048.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
ike 0:9268ab9dea63aa3/0000000000000000:591: proposal id = 1:
ike 0:9268ab9dea63aa3/0000000000000000:591: protocol id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591: trans_id = ISAKMP:
ike 0:9268ab9dea63aa3/0000000000000000:591: encapsulation = IKE/none
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_ENCRYPT_ALG, val=AES-CBC,
key-len=128
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9268ab9dea63aa3/0000000000000000:591: type=OAKLEY_GROUP, val=MODP1536.
ike 0:9268ab9dea63aa3/0000000000000000:591: ISAKMP SA lifetime=86400
```

The administrator does not have access to the remote gateway. Based on the debug output, what configuration changes can the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. Change phase 1 encryption to 3DES and authentication to SHA128.
- B. Change phase 1 encryption to AES128 and authentication to SHA512.
- C. Change phase 1 encryption to AESCBC and authentication to SHA2.
- D. Change phase 1 encryption to AES256 and authentication to SHA256.



Answer: D

#### NEW QUESTION 76

View the exhibit, which contains a screenshot of some phase-1 settings, and then answer the question below.

The screenshot shows the configuration for a phase-1 VPN named "Remote". The settings are as follows:

- Name:** Remote
- Comments:** Comments
- Network:**
  - IP Version:** ☒ IPv4 ☐ IPv6
  - Remote Gateway:** Static IP address
  - IP Address:** 10.0.10.1
  - Interface:** port1
  - Mode Config:** ☐
  - NAT Traversal:** ☒
  - Keepalive Frequency:** 10
  - Dead Peer Detection:** ☒

The VPN is up, and DPD packets are being exchanged between both IPsec gateways; however, traffic cannot pass through the tunnel. To diagnose, the administrator enters these CLI commands:

```
diagnose vpn ike log-filter src-add4 10.0.10.1
diagnose debug application ike-1
diagnose debug enable
```

However, the IKE real time debug does not show any output. Why?

- A. The debug output shows phases 1 and 2 negotiations onl
- B. Once the tunnel is up, it does not show any more output.
- C. The log-filter setting was set incorrectl
- D. The VPN's traffic does not match this filter.
- E. The debug shows only error message
- F. If there is no output, then the tunnel is operating normally.
- G. The debug output shows phase 1 negotiation onl
- H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Answer: B

#### NEW QUESTION 77

Refer to the exhibits.

```
config vpn ipsec phase1-interface
edit "user-1"
set type dynamic
set interface "port1"
set mode main
set xauthtype auto
set authusrgrp "Users-1"
set peertype any
set dhgrp 14 15 19
set proposal aes128-sha256 aes256-sha384
set psksecret <encrypted_password>
next
```

Which contain the partial configurations of two VPNs on FortiGate.

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.

Which two changes must administrator make to fix the issue? (Choose two.)

- A. Use different pre-shared keys on both VPNs
- B. Enable Mode Config on both VPNs.
- C. Set up specific peer IDs on both VPNs.
- D. Change to aggressive mode on both VPNs.

Answer: CD



**Explanation:**

To set peer-id, the VPN must be set in aggressive mode - <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-Peer-IDs-to-select-an-IPSec-dialup/ta-p>

**NEW QUESTION 81**

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

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot::624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change can the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. In the phase 1 network configuration, set the IKE version to 2.
- B. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.
- C. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
- D. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.

**Answer: D**

**Explanation:**

<https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/238852>



**NEW QUESTION 85**

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

- A. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer.
- B. Only the root FortiGate sends logs to FortiAnalyzer.
- C. Only FortiGate devices with fabric-object-unification set to default will receive and synchronize global CMDB objects sent by the root FortiGate.
- D. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.

**Answer:** AC

**Explanation:**

FortiGate's to Root uses FortiTelemetry (TCP-8013) FortiTelemetry is also used for FortiClient communication Root Fortigate to FortiAnalyzer uses API (TCP-443)

**NEW QUESTION 90**

View the exhibit, which contains an entry in the session table, and then answer the question below.

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
orgin->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)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
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
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
```

Which one of the following statements is true regarding FortiGate's inspection of this session?

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

**Answer:** A

**Explanation:**

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

**NEW QUESTION 91**

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=0 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. port1
- D. port2

**Answer:** C

#### NEW QUESTION 96

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

- A. Some of them display real-time application debugs.
- B. Some of them can be used to restart an application.
- C. Some of them display statistics and configuration information about a feature or process.
- D. Some of them only display output, after you run the diagnose debug console enable command.

**Answer:** BC

#### NEW QUESTION 97

Which of the following conditions must be met for a static route to be active in the routing table? (Choose three.)

- A. The next-hop IP address is up.
- B. There is no other route, to the same destination, with a higher distance.
- C. The link health monitor (if configured) is up.
- D. The next-hop IP address belongs to one of the outgoing interface subnets.
- E. The outgoing interface is up.

**Answer:** CDE

#### Explanation:

A configured static route only goes to routing table from routing database when all the following are met :

- The outgoing interface is up
- There is no other matching route with a lower distance
- The link health monitor (if configured) is successful
- The next-hop IP address belongs to one of the outgoing interface subnets

#### NEW QUESTION 99

An administrator has been assigned the task of creating a set of firewall policies which must be evaluated before any custom policies defined within the policy packages of managed FortiGate devices, across all 25 ADOMs in FortiManager.

How should the administrator accomplish this task?

- A. Create a footer policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this footer policy to all other ADOMs.
- B. Create a header policy in the Global ADOM containing the firewall policies that must be evaluated first, and then assign this header policy to all other ADOMs.
- C. Move the FortiGate devices into a single globally scoped ADOM, and merge policy packages, inserting the new firewall policies at the top.
- D. Use a CLI script from the root ADOM on FortiManager to push these new policies to all FortiGate devices, through the FGFM tunnel.

**Answer:** B

#### Explanation:

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 244

#### NEW QUESTION 104

Which two conditions would prevent a static route from being added to the routing table? (Choose two.)

- A. There is another other route to the same destination, with a lower distance.
- B. The route has a lower priority value than another route to the same destination.
- C. The next-hop IP address is unreachable.
- D. The interface specified in the route configuration is down

**Answer:** AD

#### Explanation:

The routing table contains only the static route with the lowest distance <https://community.fortinet.com/t5/FortiGate/Technical-Note-Routing-behavior-depending-on-distance-and/ta-p/>

#### NEW QUESTION 105

An administrator has configured a FortiGate device with two VDOMs: root and internal. The administrator has also created an inter-VDOM link that connects both VDOMs. The objective is to have each VDOM advertise some routes to the other VDOM via OSPF through the inter-VDOM link. What OSPF configuration settings must match in both VDOMs to have the OSPF adjacency successfully forming? (Choose three.)

- A. Router ID.
- B. OSPF interface area.
- C. OSPF interface cost.
- D. OSPF interface MTU.
- E. Interface subnet mask.

**Answer:** BDE

#### NEW QUESTION 108

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=162
               memory_tension_drop=0 ephemeral=0/65536 removeable=0
delete=0, flush=0, dev_down=0/0 ses_walkers=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
fqdn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

Which statement about the output shown in the exhibit is correct?

- A. There are two sessions that have not been removed in case of any out-of-order packets that arrive.
- B. There are 166 TCP sessions waiting to complete the three-way handshake.
- C. 162 sessions have been deleted because of memory page exhaustion.
- D. All the sessions in the session table are TCP sessions.

**Answer: A**

#### NEW QUESTION 110

View the exhibit, which contains the output of get sys ha status, and then answer the question below.

```
NGFW # get sys ha status
HA Health Status: ok
Model: FortiGate0VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 01:07:35
Master selected using:
<2017/04/24 09:43:44> FGVM010000077649 is selected as the master because it has the largest value of override pr
<2017/04/24 08:50:53> FGVM010000077 is selected as the master because it's the only member in the cluster.
ses_pickup: disable
override: enable
Configuration Status:
FGVM010000077649(updated 1 seconds ago): in-sync
FGVM010000077650(updated 0 seconds ago): out-of-sync
System Usage stats:
FGVM010000077649(updated 1 seconds ago):
sessions=30, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-60%
FGVM010000077650(updated 0 seconds ago):
sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-61%
HBDEV stats:
FGVM010000077649(updated 1 seconds ago):
port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7358367/17029/25/0, tx=7721830/17182/0/0
FGVM010000077650(updated 0 seconds ago):
port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7793722/17190/0/0, tx=8940374/20806/0/0
Master: NGFW      , FGVM010000077649
Slave : NGFW-2    , FGVM010000077650
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:0 FGVM010000077649
Slave :1 FGVM010000077650
```

Which statements are correct regarding the output? (Choose two.)

- A. The slave configuration is not synchronized with the master.
- B. The HA management IP is 169.254.0.2.
- C. Master is selected because it is the only device in the cluster.
- D. port 7 is used the HA heartbeat on all devices in the cluster.

**Answer: AD**

**NEW QUESTION 112**

Refer to the exhibit, which shows the output of get system ha status. NGFW-1 and NGFW-2 have been up for a week.

```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2021-10-18 12:07:47
Primary selected using:
<2021/10/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is larger than peer member
FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
FGVM010000077649(updated 4 seconds ago): in-sync
FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage Stats:
FGVM010000077649(updated 4 seconds ago):
sessions=166, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=45%
FGVM010000077650(updated 1 seconds ago):
sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=44%
HBDEV stats:
FGVM010000077649(updated 4 seconds ago):
port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
FGVM010000077650(updated 1 seconds ago):
port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
Primary : NGFW-1 , FGVM010000077649, HA cluster index = 1
Secondary : NGFW-2 , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

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

- A. If FGVM...649 is rebooted, FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.
- B. If no action is taken, the primary FortiGate will leave the cluster due to the current sync status.
- C. If port7 becomes disconnected on the secondary, both FortiGate devices will elect itself the primary.
- D. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.

**Answer:** AC

**Explanation:**

\* A. If FGVM...649 is rebooted, FGVM...650 will become the primary that is normal since it will be the only active firewall and retain that role since override is disabled. Even after FGVM...649 rejoins the cluster, 650 will not fail over as slave. C. If port7 (heartbeat port) becomes disconnected on the secondary, both FortiGate devices will elect itself the primary because when heartbeat communication fails, all cluster members think they are the primary unit (condition referred to as Split Brain) <https://docs.fortinet.com/document/fortigate/6.4.0/best-practices/493254/heartbeat-interfaces>

**NEW QUESTION 115**

Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*0.0.0.0/0 [10/0] via 10.200.1.254, port1
C10.200.1.0/24 is directly connected, port1
S192.168.0.0/16 [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
set as 65500
set router-id 10.200.1.1
set network-import-check enable
set ebgp-multipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

The BGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

- A. Enable the redistribution of connected routers into BGP.
- B. Enable the redistribution of static routers into BGP.
- C. Disable the setting network-import-check.
- D. Enable the setting ebgp-multipath.

**Answer:** C

**NEW QUESTION 116**

View the central management configuration shown in the exhibit, and then answer the question below.

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

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

- A. 10.0.1.240
- B. One of the public FortiGuard distribution servers
- C. 10.0.1.244
- D. 10.0.1.242

**Answer: B**

#### NEW QUESTION 117

Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.

```
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=0x0000/0x000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

If the priority on route ID 2 were changed from 10 to 0, what would happen to traffic matching that user session?

- A. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
- B. The session would remain in the session table, and its traffic would egress from port2.
- C. The session would be deleted, and the client would need to start a new session.
- D. The session would remain in the session table, and its traffic would egress from port1.

**Answer: D**

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Using-SNAT-route-change-to-update-existing-NAT/>

#### NEW QUESTION 119

What does the dirty flag mean in a FortiGate session?

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

**Answer: B**

**Explanation:**

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119&sliceId=1>

#### NEW QUESTION 122

An administrator cannot connect to the GUI of a FortiGate unit with the IP address 10.0.1.254. The administrator runs the debug flow while attempting the connection using HTTP. The output of the debug flow is shown in the exhibit:

```
# diagnose debug flow filter port 80
# diagnose debug flow trace start 5
# diagnose debug enable

id=20085 trace_id=5 msg="vd-root received a packet(proto=6,
10.0.1.10:57459->10.0.1.254:80) from port3. flag [S], seq 3190430861, ack
0, win 8192"
id=20085 trace_id=5 msg="allocate a new session-0000008c"
id=20085 trace_id=5 msg="iprope_in_check() check failed on policy 0, drop"
```

Based on the error displayed by the debug flow, which are valid reasons for this problem? (Choose two.)

- A. HTTP administrative access is disabled in the FortiGate interface with the IP address 10.0.1.254.
- B. Redirection of HTTP to HTTPS administrative access is disabled.
- C. HTTP administrative access is configured with a port number different than 80.
- D. The packet is denied because of reverse path forwarding check.

**Answer: AC**

#### NEW QUESTION 126

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE7\_EFW-7.0 Practice Exam Features:

- \* NSE7\_EFW-7.0 Questions and Answers Updated Frequently
- \* NSE7\_EFW-7.0 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE7\_EFW-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE7\_EFW-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE7\\_EFW-7.0 Practice Test Here](#)**