

## Exam Questions NSE7\_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

[https://www.2passeasy.com/dumps/NSE7\\_EFW-7.0/](https://www.2passeasy.com/dumps/NSE7_EFW-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

Which two conditions must be met for a statistic route to be active in the routing table? (Choose two.)

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

**Answer: AC**

### NEW QUESTION 4

Examine the following partial outputs from two routing debug commands; then answer the question below.

```
# get router info kernel
tab=254 vf=0 scope=0type=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=0type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254 dev=3(port2)
tab=254 vf=0 scope=253type=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] dO.0.1.0/24 is directly connected, port3
```

dO.200.1.0/24 is directly connected, port1 d0.200.2.0/24 is directly connected, port2

Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

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

Answer: B

#### NEW QUESTION 5

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
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)
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 6

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

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

Answer: AC

#### NEW QUESTION 7

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 8**

How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

- A. FortiManager can download and maintain local copies of FortiGuard databases.
- B. FortiManager supports only FortiGuard push to managed devices.
- C. FortiManager will respond to update requests only if they originate from a managed device.
- D. FortiManager does not support rating requests.

**Answer:** A

**NEW QUESTION 9**

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 10

Refer to the exhibit, which contains a screenshot of some phase 1 settings.

The screenshot shows the configuration for a Remote VPN in FortiGate. The settings are as follows:

- Name:** Remote
- Comments:** (empty)
- IP Version:** IPv4
- Remote Gateway:** Static IP Address
- IP Address:** 10.0.10.1
- Interface:** port1
- Local Gateway:** disabled
- Mode Config:** disabled
- NAT Traversal:** Enable
- Keepalive Frequency:** 10
- Dead Peer Detection:** On Demand

The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands to an SSH session on FortiGate: diagnose vpn ike log-filter dst-addr4 10.0.10.1 diagnose debug application ike -1  
 However, the IKE real-time debug does not show any output. Why?

- A. The administrator must also run the command diagnose debug enable.
- B. The administrator must enable the following real-time debug: diagnose debug application ipsec -1.
- C. The log-filter setting is incorrect.
- D. The VPN traffic does not match this filter.
- E. The debug shows only error message.
- F. If there is no output, then the phase 1 and phase 2 configurations match.

**Answer:** A

#### Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-IPSec-VPN-Diagnostics-Possible-reasons/ta-p/1920>

#### NEW QUESTION 10

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
```

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 15

An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.  
 If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

- A. diagnose sniffer packet any 'ah'
- B. diagnose sniffer packet any 'ip proto 50'
- C. diagnose sniffer packet any 'udp port 4500'
- D. diagnose sniffer packet any 'udp port 500'

**Answer:** B

#### Explanation:

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p. 443 Phase 2 : ESP => IP protocol 50

This command will capture any packets that use the IP protocol number 50, which is ESP (Encapsulating Security Payload). ESP is used to encrypt and authenticate the phase 2 traffic between two FortiGate device1s.

#### NEW QUESTION 20

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:  recv 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:  recv 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.
```

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

Answer: D

#### NEW QUESTION 24

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	Block	Enable

Web content filter ☒

+ Create new

Edit

Delete

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	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 28

Which statement about protocol options is true?

- A. Protocol options allows administrators a streamlined method to instruct FortiGate to block all sessions corresponding to disabled protocols.
- B. Protocol options allows administrators the ability to configure the Any setting for all enabled protocols which provides the most efficient use of system resources.
- C. Protocol options allow administrators to configure a maximum number of sessions for each configured protocol.
- D. Protocol options allows administrators to configure which Layer 4 port numbers map to upper-layer protocols, such as HTTP, SMTP, FTP, and so on.

**Answer:** D

#### NEW QUESTION 31

What is the diagnose test application ipsmonitor 5 command used for?

- A. To enable IPS bypass mode
- B. To disable the IPS engine
- C. To restart all IPS engines and monitors
- D. To provide information regarding IPS sessions

**Answer:** A

#### Explanation:

# diagnose test application ipsmonitor 5: Toggle bypass status

\* 13: IPS session list

\* 98: Stop all IPS engines

\* 99: Restart all IPS engines and monitor

#### NEW QUESTION 35

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

```
# diagnose debug rating
Locale      : english
License     : Contract
Expiration   : Thu Sep 28 17:00:00 20xx
-- Server List (Thu Apr 19 10:41:32 20xx) --
```

IP	Weight	RTT	Flags	TZ	Packets	Curr Lost	Total Lost
64.26.151.37	10	45		-5	262432	0	846
64.26.151.35	10	46		-5	329072	0	6806
66.117.56.37	10	75		-5	71638	0	275
65.210.95.240	20	71		-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	33728	0	120
80.85.69.41	71	226		1	33797	0	192
62.209.40.74	150	97		9	33754	0	145
121.111.236.179	45	44	F	-5	26410	26226	26227

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

- A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.
- B. Servers with the D flag are considered to be down.
- C. Servers with a negative TZ value are experiencing a service outage.
- D. FortiGate used 209.222.147.3 as the initial server to validate its contract.

**Answer:** AD

#### Explanation:

\* A – because flag is Failed so fortigate will check if server is available every 15 minD-state is I , contact to validate contract info

#### NEW QUESTION 37

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



```
f 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
gwy=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 39

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

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

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

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

Answer: AC

### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD40578>

### NEW QUESTION 43

Which configuration can be used to reduce the number of BGP sessions in an IBGP network?

- A. Neighbor range
- B. Route reflector
- C. Next-hop-self
- D. Neighbor group

Answer: B

#### Explanation:

Route reflectors help to reduce the number of IBGP sessions inside an AS. A route reflector forwards the routes learned from one peer to the other peers. If you configure route reflectors, you don't need to create a full mesh IBGP network. All clients in a cluster only talk to route reflector to get sync routing updates. Route reflectors pass the routing updates to other route reflectors and border routers within the AS.

#### NEW QUESTION 45

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 46

A FortiGate has two default routes:

```
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 Internet traffic is currently using port1. The exhibit shows partial information for one sample session of Internet traffic from an internal user:

```
# 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=575/7/1 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
```

What would happen with the traffic matching the above session if the priority on the first default route (IDd1) were changed from 5 to 20?

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



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

**Answer:** D

#### NEW QUESTION 47

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 50

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



# diagnose webfilter fortiguard statistics list		# diagnose webfilter fortiguard statistics list	
Rating Statistics:		Cache Statistics:	
=====		=====	
DNS failures	: 273	Maximum memory	: 0
DNS lookups	: 280	Memory usage	: 0
Data send failures	: 0		
Data read failures	: 0	Nodes	: 0
Wrong package type	: 0	Leaves	: 0
Hash table miss	: 0	Prefix nodes	: 0
Unknown server	: 0	Exact nodes	: 0
Incorrect CRC	: 0		
Proxy request failures	: 0	Requests	: 0
Request timeout	: 1	Misses	: 0
Total requests	: 2409	Hits	: 0
Requests to FortiGuard servers	: 1182	Prefix hits	: 0
Server errored responses	: 0	Exact hits	: 0
Relayed rating	: 0		
Invalid profile	: 0	No cache directives	: 0
		Add after prefix	: 0
Allowed	: 1021	Invalid DB put	: 0
Blocked	: 3909	DB updates	: 0
Logged	: 3927		
Blocked Errors	: 565	Percent full	: 0%
Allowed Errors	: 0	Branches	: 0%
Monitors	: 0	Leaves	: 0%
Authenticates	: 0	Prefix nodes	: 0%
Warnings:	: 18	Exact nodes	: 0%
Ovrd request timeout	: 0		
Ovrd send failures	: 0	Miss rate	: 0%
Ovrd read failures	: 0	Hit rate	: 0%
Ovrd errored responses	: 0	Prefix hits	: 0%
...		Exact hits	: 0%

Which configuration change would result in non-zero results in the cache statistics section?

- A. set server-type rating under config system central-management
- B. set webfilter-cache enable under config system fortiguard
- C. set webfilter-force-off disable under config system fortiguard
- D. set ngfw-mode policy-based under config system settings

**Answer: B**

**Explanation:**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 362

### NEW QUESTION 53

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

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

**Answer: AC**

### NEW QUESTION 58

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

- A. Preview pending configuration changes for managed devices.
- B. Add devices to FortiManager.
- C. Import policy packages from managed devices.
- D. Install configuration changes to managed devices.
- E. Import interface mappings from managed devices.

**Answer: AD**

**Explanation:**

[https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager\\_Admin\\_Guide/1000\\_Device%20Manager/1200\\_ins](https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_ins)

There are 4 main wizards: Add Device: is used to add devices to central management and import their configurations.

Install: is used to install configuration changes from Device Manager or Policies & Objects to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.

Import policy: is used to import interface mapping, policy database, and objects associated with the managed devices into a policy package under the Policy & Object tab. It runs with the Add Device wizard by default and may be run at any time from the managed device list.

Re-install policy: is used to perform a quick install of the policy package. It doesn't give the ability to preview the changes that will be installed to the managed device.

### NEW QUESTION 60

Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network. What HA setting must be changed in one of the HA clusters to fix the problem?

- A. Group ID.
- B. Group name.
- C. Session pickup.
- D. Gratuitous ARPs.

**Answer:** A

**Explanation:**

[https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA\\_failoverVMAC.htm](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm)

**NEW QUESTION 61**

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=statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=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
    dat: 0:10.1.1.0/255.255.255.0:0
    SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/OB replaywin=204B seqno=1
esn=replaywin_lastseq=00000000
    life: type=01 bytes=0/0 timeout=43177/43200
    dec: spi=ccclf66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
        ah=sha1 key=20 c68091d68753578785de6a7a6b276b506e527
```

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

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

**Answer:** AC

**NEW QUESTION 64**

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 68**

When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI) extension?

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

**Answer:** A

**NEW QUESTION 70**

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 failed to apply any changes to the managed device after being executed. Why did the TCL script fail to make any changes to the managed device?

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

**Answer:** D

### NEW QUESTION 73

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 76

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

```
Spoke-2 # diagnose 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 tun_id=10.200.4.1 dst_mtu=1500 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0 options[0210]=create_dev
frag-rfc accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=10 olast=551 ad=/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=2
  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=10202 type=00 soft=0 mtu=1438 expire=42897/0B replaywin=2048
      seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=5ed4aaf8 esp=aes key=16 20d624b494b1c9bfe61ba9b7522448db
      ah=sha1 key=20 891cd9ba81f0e382de0d44127152cb5dba6c62d1
  enc: spi=3b574759 esp=aes key=16 3abf4e04edc09e4e88709750df9c117d
      ah=sha1 key=20 2d2618e867839866a279af5af70a64fa63a7bb52
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

- A. The remote gateway has quick mode selectors containing a destination subnet of 10.1.2.0/24.
- B. The remote gateway IP is 10.200.5.1.
- C. DPD is disabled.
- D. Anti-replay is enabled.

**Answer:** AD

### Explanation:

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 427, 444

Since the local subnet is 10.1.2.0/24, the remote gateway has the destination subnet as 10.1.2.0. The remote gateway IP is 10.200.4.1. DPD is enabled (dpd-



link=on)

#### NEW QUESTION 79

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

- A. set av-failopen off
- B. set av-failopen pass
- C. set fail-open enable
- D. set ips fail-open disable

**Answer:** AC

#### Explanation:

<https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/194558/conserve-mode>

#### NEW QUESTION 83

Which three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

- A. OSPF interface network types match.
- B. OSPF router IDs are unique.
- C. OSPF interface priority settings are unique.
- D. Authentication settings match.
- E. OSPF link costs match.

**Answer:** ABD

#### Explanation:

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 280

#### NEW QUESTION 85

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

```
# 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
10.200.3.1	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. For the peer 10.125.0.60, the BGP state of is Established.
- B. The local BGP peer has received a total of three BGP prefixes.
- C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.
- D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

**Answer:** AD

#### NEW QUESTION 90

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

```
# diagnose sys session list expectation

session info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook-pre dir=org act=dnat 10.171.121.38:0->10.200.1.1:60426(10.0.1.10:50365)
hook-pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What can you conclude from the output shown in the exhibit? (Choose two.)

- A. This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.
- B. This is an expected session created by the IPS engine.
- C. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.
- D. Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.0.1.10.

**Answer:** AD

**Explanation:**

Enterprise\_Firewall\_7.0\_Study\_Guide-Online.pdf p 110, 111, 115

### NEW QUESTION 93

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

```
# diagnose webfilter fortiguard statistics list
```

Rating Statistics:

```
=====
DNS failures          : 273
DNS lookups           : 280
Data send failures    : 0
Data read failures    : 0
Wrong package type    : 0
Hash table miss       : 0
Unknown server        : 0
Incorrect CRC         : 0
Proxy requests failures : 0
Request timeout       : 1
Total requests        : 2409
Requests to FortiGuard servers : 1182
Server errored responses : 0
Relayed rating        : 0
Invalid profile       : 0

Allowed              : 1021
Blocked              : 3909
Logged               : 3927
Blocked Errors       : 565
Allowed Errors       : 0
Monitors             : 0
Authenticates        : 0
Warnings             : 18
Ovrd request timeout : 0
Ovrd send failures   : 0
Ovrd read failures    : 0
Ovrd errored responses : 0
...
```

```
# diagnose webfilter fortiguard statistics list
```

Cache Statistics:

```
=====
Maximum memory      : 0
Memory usage        : 0

Nodes               : 0
Leaves              : 0
Prefix nodes        : 0
Exact nodes         : 0

Requests            : 0
Misses              : 0
Hits                : 0
Prefix hits         : 0
Exact hits          : 0

No cache directives : 0
Add after prefix    : 0
Invalid DB put      : 0
DB updates          : 0

Percent full        : 0%
Branches            : 0%
Leaves              : 0%
Prefix nodes        : 0%
Exact nodes         : 0%

Miss rate           : 0%
Hit rate            : 0%
Prefix hits         : 0%
Exact hits          : 0%
```

Which one of the following statements explains why the cache statistics are all zeros?

- A. The administrator has reallocated the cache memory to a separate process.
- B. There are no users making web requests.
- C. The FortiGuard web filter cache is disabled in the FortiGate's configuration.
- D. FortiGate is using a flow-based web filter and the cache applies only to proxy-based inspection.

Answer: C

#### NEW QUESTION 96

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.

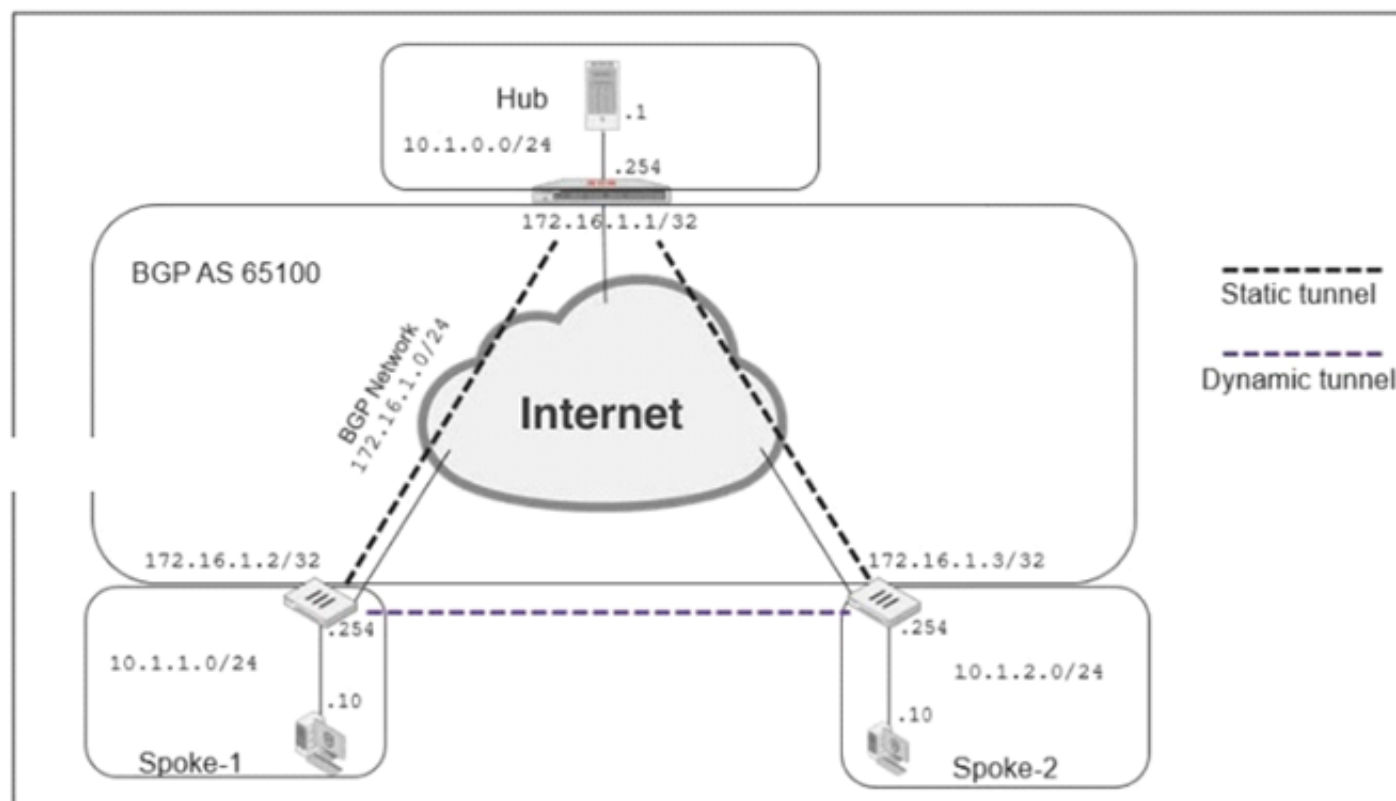
Answer: CD

#### 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 100

Exhibits:





```

show router bgp
router bgp
  as 65100
  router-id 172.16.1.1
fig neighbor-group
  edit "advpn"
    set remote-as 65100

    set route-reflector-client disable
  next

fig neighbor-range
  edit 1
    set prefix 172.16.1.0 255.255.255.0
    set neighbor-group "advpn"
  next

```

Refer to the exhibits, which contain the network topology and BGP configuration for a hub.

An administrator is trying to configure ADVPN with a hub-spoke VPN setup using iBGP. All the VPNs are up and connected to the hub. The hub is receiving route information from both spokes over iBGP; however, the spokes are not receiving route information from each other.

What change must the administrator make to the hub BGP configuration so that the routes learned by one spoke are forwarded to the other spokes?

- A. Configure an individual neighbor and remove neighbor-range configuration.
- B. Configure the hub as a route reflector client.
- C. Change the router id to 10.1.0.254.
- D. Make the configuration of remote-as different from the configuration of local-as.

**Answer: B**

**Explanation:**

Source:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-BGP-route-reflector/ta-p/191503> Source 2: RFC 4456

#### NEW QUESTION 105

An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

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

**Answer: A**

#### NEW QUESTION 110

Examine the following partial output from a sniffer command; then answer the question below.

```

# diagnose sniff packet any 'icmp' 4
interfaces= [any]
filters = [icmp]
2.101199 wan2 in 192.168.1.110-> 4.2.2.2: icmp: echo request
2.101400 wan1 out 172.17.87.16-> 4.2.2.2: icmp: echo request
.....
2.123500 wan2 out 4.2.2.2-> 192.168.1.110: icmp: echo reply
244 packets received by filter
5 packets dropped by kernel

```

What is the meaning of the packets dropped counter at the end of the sniffer?

- A. Number of packets that didn't match the sniffer filter.
- B. Number of total packets dropped by the FortiGate.
- C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.
- D. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

**Answer: D**

**Explanation:**

<https://kb.fortinet.com/kb/documentLink.do?externalID=11655>

#### NEW QUESTION 115

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 119**

How are bulk configuration changes made using FortiManager CLI scripts? (Choose two.)

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

**Answer:** CD

**Explanation:**

CLI scripts can be run in three different ways: Device Database: By default, a script is executed on the device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard. Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard. Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don't need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

**NEW QUESTION 122**

What is the diagnose test application ipsmonitor 99 command used for?

- A. To enable IPS bypass mode
- B. To provide information regarding IPS sessions
- C. To disable the IPS engine
- D. To restart all IPS engines and monitors

**Answer:** D

**NEW QUESTION 123**

A FortiGate device has the following LDAP configuration:

```
config user ldap
  edit "WindowsLDAP"
    set server "10.0.1.10"
    set cnid "cn"
    set dn "cn=user, dc=trainingAD, dc=training, dc=lab"
    set type regular
    set username "cn=administrator, cn=users, dc=trainingAD,
dc=training, dc=lab"
    set password xxxxx
  next
end
```

The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:

```
#diagnose debug application fnbamd -l
#diagnose debug enable
#diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Recv auth req 4 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[1700] fnbamd_ldap_get_result-Error in ldap result: 49
(Invalid credentials)
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 4
fnbamd_fsm.c[568] destroy_auth_session-delete session 4
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the above output, what FortiGate LDAP settings must the administrator check? (Choose two.)

- A. cnid.
- B. username.
- C. password.
- D. dn.

**Answer:** BC

**Explanation:**

<https://kb.fortinet.com/kb/viewContent.do?externalId=13141>

#### NEW QUESTION 126

An administrator has enabled HA session synchronization in a HA cluster with two members. Which flag is added to a primary unit's session to indicate that it has been synchronized to the secondary unit?

- A. redir.
- B. dirty.
- C. synced
- D. nds.

**Answer:** C

**Explanation:**

The synced sessions have the 'syncd' flag. The command 'diag sys session list' can be used to see the sessions on the member, with the associated flags.

#### NEW QUESTION 131

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 132

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

```
FortiGate # get router info routing-table database

Routing table for VRF=0
S      0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S      *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1

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
```

Why is the port2 default route not in the second command output?

- A. The port2 interface is disabled in the FortiGate configuration.
- B. The port1 default route has a lower distance than the default route using port2.
- C. The port1 default route has a higher priority value than the default route using port2.
- D. The port1 default route has a lower priority value than the default route using port2.

Answer: B

#### NEW QUESTION 137

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 140

View the exhibit, which contains the output of a real-time debug, Which statement about this output is true?

```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=687, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

Which of the following statements is true regarding this output?

- A. The requested URL belongs to category ID 255.
- B. The server hostname is training.fortinet.com.
- C. FortiGate found the requested URL in its local cache.
- D. This web request was inspected using the ftgd-allow web filter profile.

**Answer: C**

#### Explanation:

Example log for no local cache case: #id=93000 msg="pid=57 urlfilter\_main-723 in main.c received pkt:count=91 "IPS and WAD will only send request to urlfilter daemon when cache is missed. " So the WAD process by itself found the URL rating in the local cache and didn't ask for help from the URL process as in the example.

#### NEW QUESTION 143

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 148

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.

Answer: D

#### NEW QUESTION 151

Examine the output of the 'diagnose sys session list expectation' command shown in the exhibit; than answer the question below.

```
#diagnose sys session list expectation

session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
flags=00000000
sockflag=.00000000.sockport=0.av_idx=0.use=39
origin-shaper=9
reply-shaper=9
per-ip_shaper=9
ha_id=0.policy_dir=1.tunnel=/9
state=new complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)9
hook= pre dir=org act=noop 0.0.0.0.:0-> 0.0.0.0:0 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0.policy_id=1.auth_info=0.chk_client_info=0.vd=0
seriall=000000e9.tos=ff/ff.ips_view=0 app_list=0.app=0
dd type=0.dd_mode=09
```

Which statement is true regarding the session in the exhibit?

- A. It was created by the FortiGate kernel to allow push updates from FortiGuard.
- B. It is for management traffic terminating at the FortiGate.
- C. It is for traffic originated from the FortiGate.
- D. It was created by a session helper or ALG.

Answer: D

#### NEW QUESTION 153

View the exhibit, which contains the output of a diagnose command, and the answer the question below.

```
# diagnose debug rating
Locale       : English
License      : Contract
Expiration   : Thu Sep 28 17:00:00 20XX
--- Server List (Thu APR 19 10:41:32 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
66.210.95.240 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 statements are true regarding the Weight value?

- A. Its initial value is calculated based on the round trip delay (RTT).
- B. Its initial value is statically set to 10.
- C. Its value is incremented with each packet lost.
- D. It determines which FortiGuard server is used for license validation.

Answer: C

#### NEW QUESTION 157



.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7\_EFW-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7\_EFW-7.0 Product From:

[https://www.2passeasy.com/dumps/NSE7\\_EFW-7.0/](https://www.2passeasy.com/dumps/NSE7_EFW-7.0/)

## Money Back Guarantee

### **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