



Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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/ [10/0] via 10.200.1.254, port1 [10/0] via 10.200.2.254, port2, [10/0] d0.0.1.0/24 is directly connected, port3
d0.200.1.0/24 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 4

An administrator has configured the following CLI script on FortiManager, which failed to apply any changes to the managed device after being executed.

```
# conf rout stat
#     edit 0
#         set gateway 10.20.121.2
#         set priority 20
#         set device "wan1"
#     next
# end
```

Why didn't the script make any changes to the managed device?

- A. Commands that start with the # sign are not executed.
- B. CLI scripts will add objects only if they are referenced by policies.
- C. Incomplete commands are ignored in CLI scripts.
- D. Static routes can only be added using TCL scripts.

Answer: A

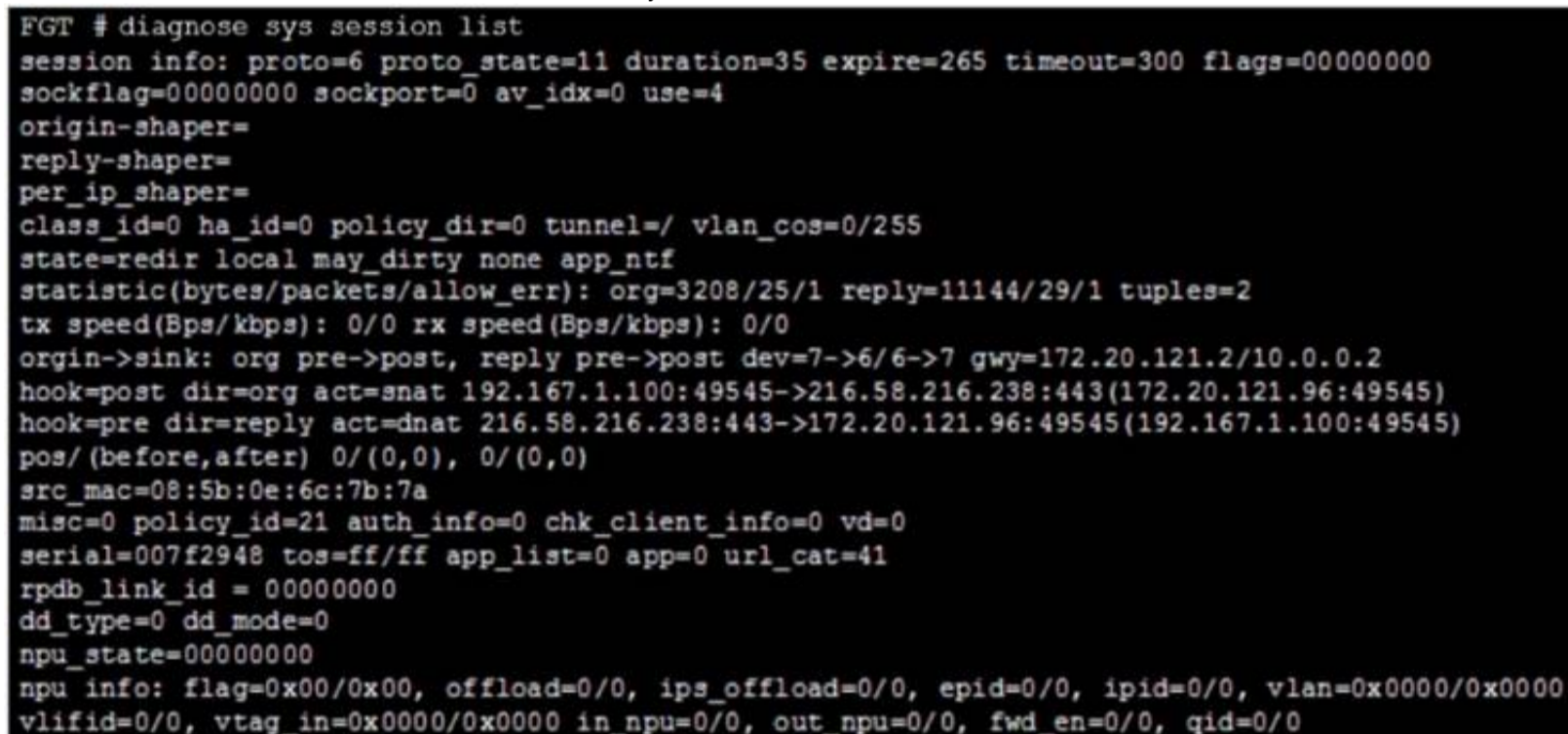
Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc

A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

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
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 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 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
orgin->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 device is 0, what will happen if the primary fails and the secondary becomes the primary?

- A. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.
- B. The secondary device has this session synchronized; however, because application control is applied, the session will be marked dirty and have to be re-evaluated after failover.
- C. The session state will be preserved but the kernel will need to re-evaluate the session due to NAT being applied.
- D. The session will be removed from the session table of the secondary device due to the presence of allowed error packets, which will force the client to restart the session with the server.

Answer: A

Explanation:

<https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-see-if-a-session-is-synced-in-HA/ta-p/1941>

NEW QUESTION 8

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

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

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

Total number of neighbors 3
```

Which statement about the exhibit is true?

- A. The local router has received a total of three BGP prefixes from all peers.
- B. The local router has not established a TCP session with 100.64.3.1.
- C. Since the counters were last reset, the 10.200.3.1 peer has never been down.
- D. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

Answer: B

NEW QUESTION 9

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 10

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 10

The CLI command set intelligent-mode <enable | disable> controls the IPS engine's adaptive scanning behavior. Which of the following statements describes IPS adaptive scanning?

- A. Determines the optimal number of IPS engines required based on system load.
- B. Downloads signatures on demand from FDS based on scanning requirements.
- C. Determines when it is secure enough to stop scanning session traffic.
- D. Choose a matching algorithm based on available memory and the type of inspection being performed.

Answer: C

Explanation:

Configuring IPS intelligenceStarting with FortiOS 5.2, intelligent-mode is a new adaptive detection method. This command is enabled the default and it means that the IPS engine will perform adaptive scanning so that, for some traffic, the FortiGate can quickly finish scanning and offload the traffic to NPU or kernel. It is a balanced method which could cover all known exploits. When disabled, the IPS engine scans every single byte.

```
config ips globalset intelligent-mode {enable|disable}end
```

NEW QUESTION 13

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 17

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 18

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

FortiGuard Category Based Filter

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

Static URL Filter

URL Filter

+ Create New

Edit

Delete

Search

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

Content Filter

+ Create New

Edit

Delete

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

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 23

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 24

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

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0

-----
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
  src: 0:10.1.2.0/255.255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
life: type=01 bytes=0/0 timeout=43177/43200
dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
    ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
    ah=sha1 key=20 889f7529887c215c25950be2ba83e6fe1a5367be
dec: pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

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

Answer: AB

NEW QUESTION 25

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 29

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 31

Which of the following statements are true regarding the SIP session helper and the SIP application layer gateway (ALG)? (Choose three.)

- A. SIP session helper runs in the kernel; SIP ALG runs as a user space process.
- B. SIP ALG supports SIP HA failover; SIP helper does not.
- C. SIP ALG supports SIP over IPv6; SIP helper does not.
- D. SIP ALG can create expected sessions for media traffic; SIP helper does not.
- E. SIP helper supports SIP over TCP and UDP; SIP ALG supports only SIP over UDP.

Answer: BCD

NEW QUESTION 33

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

- A. route-reflector enable
- B. route-reflector-server enable
- C. route-reflector-client enable
- D. route-reflector-peer enable

Answer: C

Explanation:

[https://docs.fortinet.com/document/fortigate/7.0.11/cli-reference/572620/config-router-bgp set route-reflector-client \[enable|disable\]](https://docs.fortinet.com/document/fortigate/7.0.11/cli-reference/572620/config-router-bgp-set-route-reflector-client)

NEW QUESTION 34

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=Users, dc=trainingAD, dc=training, dc=lab"
    set type regular
    set username "dc=trainingAD, dc=training, dc=lab"
    set password xxxxxxxx
  next
end
```

The administrator executed the 'dsquery' command in the Windows LDAP server 10.0.1.10, and got the following output:

>dsquery user -samid administrator

"CN=Administrator, CN=Users, DC=trainingAD, DC=training, DC=lab" Based on the output, what FortiGate LDAP setting is configured incorrectly?

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

Answer: B

Explanation:

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516>

NEW QUESTION 38

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

- A. Only the DR receives link state information from non-DR routers.
- B. Non-DR and non-BDR routers form full adjacencies to DR only.
- C. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.
- D. FortiGate first checks the OSPF ID to elect a DR.

Answer: C

Explanation:

Some special IP multicast addresses are reserved for OSPF: 224.0.0.5: All OSPF routers must be able to transmit and listen to this address. 224.0.0.6: All DR and BDR routers must be able to transmit and listen to this address. <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>

NEW QUESTION 43

Refer to the exhibit, which shows a FortiGate configuration.

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

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

- A. Increase webfilter-timeout.
- B. Change protocol to TCP.
- C. Enable fortiguard-anycast.
- D. Disable webfilter-force-off.

Answer: D

NEW QUESTION 46

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	Nodes : 0
Data read failures : 0	Leaves : 0
Wrong package type : 0	Prefix nodes : 0
Hash table miss : 0	Exact nodes : 0
Unknown server : 0	Requests : 0
Incorrect CRC : 0	Misses : 0
Proxy request failures : 0	Hits : 0
Request timeout : 1	Prefix hits : 0
Total requests : 2409	Exact hits : 0
Requests to FortiGuard servers : 1182	No cache directives : 0
Server errored responses : 0	Add after prefix : 0
Relayed rating : 0	Invalid DB put : 0
Invalid profile : 0	DB updates : 0
Allowed : 1021	Percent full : 0%
Blocked : 3909	Branches : 0%
Logged : 3927	Leaves : 0%
Blocked Errors : 565	Prefix nodes : 0%
Allowed Errors : 0	Exact nodes : 0%
Monitors : 0	Miss rate : 0%
Authenticates : 0	Hit rate : 0%
Warnings : 18	Prefix hits : 0%
Ovrd request timeout : 0	Exact hits : 0%
Ovrd send failures : 0	
Ovrd read failures : 0	
Ovrd errored responses : 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 48

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

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st message...
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:   trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:   encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:   trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:   encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn't the tunnel come up?

- A. The pre-shared keys do not match.
- B. The remote gateway's phase 2 configuration does not match the local gateway's phase 2 configuration.
- C. The remote gateway's phase 1 configuration does not match the local gateway's phase 1 configuration.
- D. The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

Answer: C

NEW QUESTION 53

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

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

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

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

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

- A. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.
- B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.
- C. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.
- D. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

Answer: BC

NEW QUESTION 54

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 57

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=shal 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 61

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

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

Answer: AD

NEW QUESTION 66

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
```

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

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

Answer: AB

NEW QUESTION 71

What events are recorded in the crashlogs of a FortiGate device? (Choose two.)

- A. A process crash.
- B. Configuration changes.
- C. Changes in the status of any of the FortiGuard licenses.
- D. System entering to and leaving from the proxy conserve mode.

Answer: AD

Explanation:

diagnose debug crashlog read 275: 2014-08-05 13:03:53 proxy=acceptor service=imap session fail mode=activated276: 2014-08-05 13:03:53 proxy=acceptor service=ftp session fail mode=activated277: 2014-08-05 13:03:53 proxy=acceptor service=nntp session fail mode=activated278: 2014-08-06 11:05:47 service=kernel conserve=on free="45034 pages" red="45874 pages" msg="Kernel279: 2014-08-06 11:05:47 enters conserve mode"280: 2014-08-06 13:07:16 service=kernel conserve=exit free="86704 pages" green="68811 pages"281: 2014-08-06 13:07:16 msg="Kernel leaves conserve mode"282: 2014-08-06 13:07:16 proxy=imd sysconserve=exited total=1008 free=349 marginenter=201283: 2014-08-06 13:07:16 marginexit=302

NEW QUESTION 76

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 78

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

```

FGT # get router info bgp summary
BGP router identifier 10.200.1.1, local AS number 655
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V    AS      MsgRcvd MsgSent  TblVer
10.200.3.1    4 65501      92      1756      0

Total number of neighbors 1

```

Which statement explains why the state of the 10.200.3.1 peer is Connect?

- A. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.
- B. The TCP session to 10.200.3.1 has not completed the three-way handshake.
- C. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.
- D. The local router has received the BGP prefixes from the remote peer.

Answer: B

Explanation:

BGP neighbor states and how they change:

- Idle: Initial state
- Connect: Waiting for a successful three-way TCP connection
- Active: Unable to establish the TCP session
- OpenSent: Waiting for an OPEN message from the peer
- OpenConfirm: Waiting for the keepalive message from the peer
- Established: Peers have successfully exchanged OPEN and keepalive messages

NEW QUESTION 83

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 thenext-hop IP address 10.0.1.10.

Answer: AD

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 110, 111, 115

NEW QUESTION 85

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 90

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 91

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

```
FGT # get router info ospf neighbor

OSPF process 0:
Neighbor ID      Pri   State           Dead Time   Address        Interface
0.0.0.69         1     Full/DR         00:00:32   10.126.0.69    wan1
0.0.0.117        1     Full/DROther    00:00:34   10.126.0.117   wan2
0.0.0.2          1     Full/-         00:00:38   172.16.1.2     ToRemote
```

What can be concluded from the debug command output?

- A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.
- B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.
- C. There are more than two OSPF routers on the wan2 network.
- D. The interface ToRemote is a broadcast OSPF network.

Answer: C

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 296

NEW QUESTION 94

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

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

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

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's output?

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

Answer: D

NEW QUESTION 98

An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any "host 10.0.2.10" 2
What information is included in the output of the sniffer? (Choose two.)

- A. Ethernet headers.
- B. IP payload.
- C. IP headers.
- D. Port names.

Answer: BC

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=11186>

NEW QUESTION 99

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 104

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

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

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

Total number of neighbors 3
```

What can be concluded about the router in this scenario?

- A. The router 100.64.3.1 needs to update the local AS number in its BGP configuration in order to bring up the BGP session with the local router.
- B. The State/PfxRcd for neighbor 100.64.3.1 will not change until an administrator on the local router adjusts the inbound route filtering so that prefixes received can be added to the RIB.
- C. All of the neighbors displayed are part of a single BGP configuration on the local router with the neighbor-range set to a value of 4.
- D. The BGP session with peer 10.127.0.75 is up.

Answer: D

NEW QUESTION 106

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

```
FGT # diagnose debug rating
Locale      : english
Service     : Web-filter
Status      : Enable
License     : Contract
Service     : Antispam
Status      : Disable
Service     : Virus Outbreak Prevention
Status      : Disable

-- Server List (Mon Apr 19 10:41:32 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
```

What can be concluded about the debug output in this scenario?

- A. Servers with a negative TZ value are less preferred for rating requests.
- B. There is a natural correlation between the value in the Packets field and the value in the Weight field.
- C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
- D. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

Answer: B

NEW QUESTION 108

A FortiGate is configured as an explicit web proxy. Clients using this web proxy are reposting DNS errors when accessing any website. The administrator executes the following debug commands and observes that the n-d ns-timeout counter is increasing:

```
#diagnose test application wad 2200
#diagnose test application wad 104
DNS Stats:
n_dns_reqs=878  n_dns_fails= 2  n_dns_timeout=875
n_dns_success=0

n_snd_retries=0  n_snd_fails=0 n_snd_success=0 n_dns_overflow=0
n_build_fails=0
```

What should the administrator check to fix the problem?

- A. The connectivity between the FortiGate unit and the DNS server.
- B. The connectivity between the client workstations and the DNS server.
- C. That DNS traffic from client workstations is allowed by the explicit web proxy policies.
- D. That DNS service is enabled in the explicit web proxy interface.

Answer: A

NEW QUESTION 110

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&slcid=1>

NEW QUESTION 115

Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

- A. FortiGate limits the number of simultaneous sessions per explicit web proxy use
- B. This limit CANNOT be modified by the administrator.
- C. FortiGate limits the total number of simultaneous explicit web proxy users.
- D. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator
- E. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials.This limit CANNOT be modified by the administrator.

Answer: B

Explanation:

https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-WAN-opt-52/web_proxy.htm#Explicit2

The explicit proxy does not limit the number of active sessions for each user. As a result the actual explicit proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.

NEW QUESTION 120

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	262432	0	846
64.26.151.35	10	46		-5	329072	0	6806
66.117.56.37	10	75		-5	71638	0	275
66.210.95.240	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 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 122

.....

Relate Links

100% Pass Your NSE7_EFW-7.0 Exam with ExamBible Prep Materials

https://www.exambible.com/NSE7_EFW-7.0-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>