



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

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

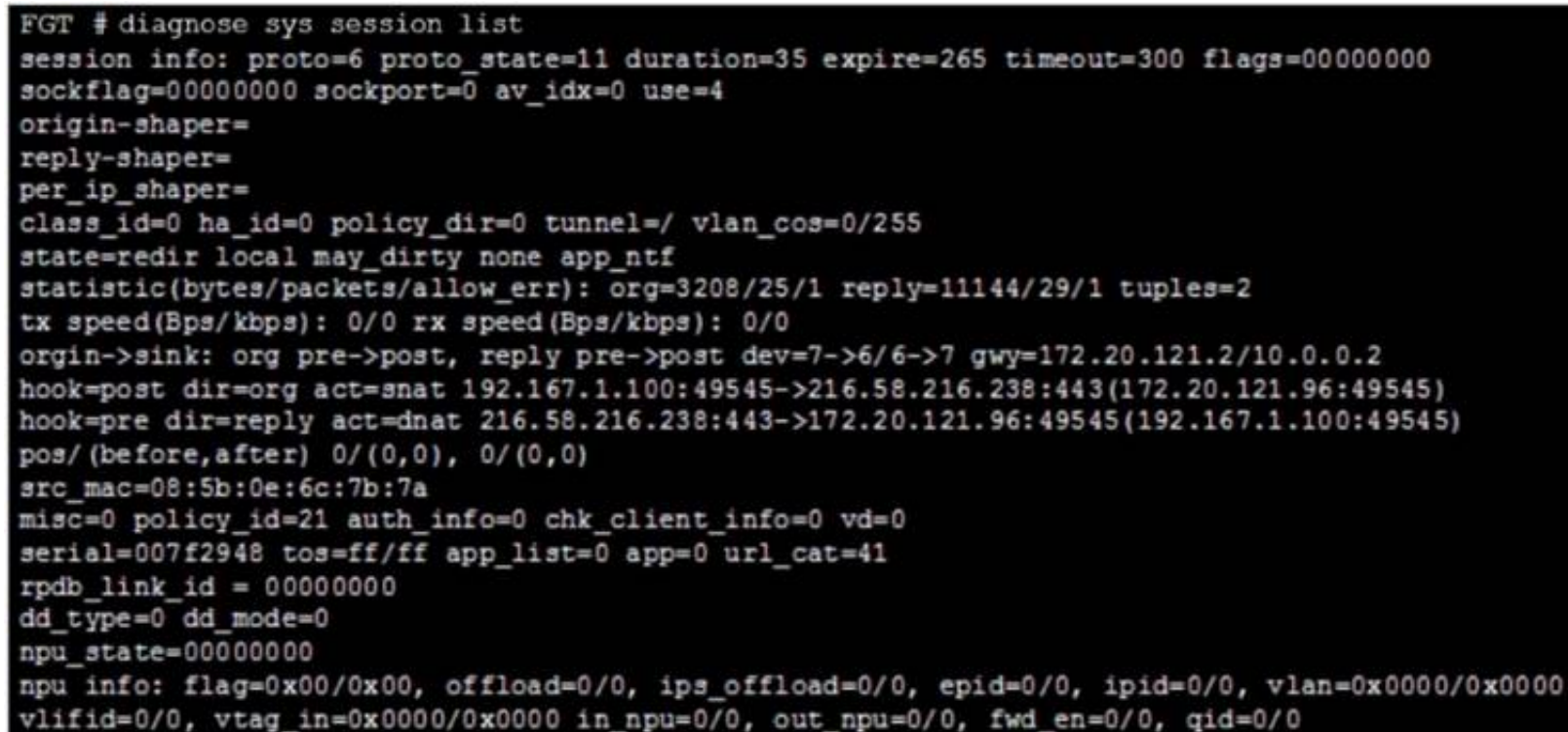
Explanation:

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 2

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 3

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 4

Which ADVPN configuration must be configured using a script on FortiManager, when using VPN Manager to manage FortiGate VPN tunnels?

- A. Set protected network to all
- B. Enable AD-VPN in IPsec phase 1
- C. Configure IP addresses on IPsec virtual interfaces
- D. Disable add-route on hub

Answer: B

NEW QUESTION 5

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 6

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

```
ike 0: comes 10.0.0.2:500-> 10.0.0.1:500, ifindex-7...
ike 0: IKEV1 exchange-Aggressive id-baf47d0988e9237f/2f405ef3952f6fda len 430
ike 0: in
BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C0000000100000001000000300101000
ike 0: RemoteSite:4: initiator: aggressive mode get 1st response
ike 0: RemoteSite:4: VID RPC 3947 4A131C81070358455C5728F20E95452F
ike 0: RemoteSite:4: VID DPD APCAD71368A1F1c96B8696FC77570100
ike 0: RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0: RemoteSite:4: peer is FortiGate/FortiOS (v6 b932)
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: RemoteSite:4: received peer identifier FQDN 'remote'
ike 0: RemoteSite:4: negotiation result
ike 0: RemoteSite:4: proposal id = 1:
ike 0: RemoteSite:4:   protocol id - ISAKMP:
ike 0: RemoteSite:4:   trans_id - KEY_IKE.
ike 0: RemoteSite:4:   encapsulation - IKE/none
ike 0: RemoteSite:4:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: RemoteSite:4:   type=OAKLEY_HASH_ALG, val=SHA
ike 0: RemoteSite:4:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: RemoteSite:4:   type=OAKLEY_GROUP, val=MODP1024.
ike 0: RemoteSite:4: ISAKMP SA lifetime=86400
ike 0: RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key
16:B25B6C9384D8BDB24E3DA3DC90CF5E73
ike 0: RemoteSite:4: PSK authentication succeeded
ike 0: RemoteSite:4: authentication OK
ike 0: RemoteSite:4: add INITIAL-CONTACT
ike 0: RemoteSite:4: enc
BAF47D0988E9237F2F405EF3952F6FDA081004010000000000000080140000181F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000008c2E3FC9BA061816A396F009A12
ike 0: RemoteSite:4: sent IKE msg (agg_12send) : 10.0.0.1:500 ->10.0.0.2:500, len-140, id-
baf47d0988e9237f/2
ike 0: RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

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

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

Answer: BD

NEW QUESTION 7

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

FortiGuard Category Based Filter

Name	Action
<div><div></div>Bandwidth Consuming 6</div>	
Freeware and Software Downloads	<div>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 8

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.

Your Partner of IT Exam

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

- C. DPD is disabled.
- D. Quick mode selectors are disabled.

Answer: AB

NEW QUESTION 9

View the exhibit, which contains a partial web filter profile configuration, and then answer the question below.

Name

default

Comments

Default web filtering.22/255

FortiGuard category based filter

Show

Allow

Bandwidth Consuming

File Sharing and Storage

Status URL Filter

Block invalid URLs

URL Filter

Create

Edit

Delete

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

Web content filter

Create new

Edit

Delete

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 10

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

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

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

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

Answer: AD

NEW QUESTION 10

Examine the output of the 'diagnose ips anomaly list' command shown in the exhibit; then answer the question below.

```
# diagnose ips anomaly list
```

```
list nids meter:
```

id=ip_dst_session	ip=192.168.1.10	dos_id=2	exp=3646	pps=0	freq=0
id=udp_dst_session	ip=192.168.1.10	dos_id=2	exp=3646	pps=0	freq=0
id=udp_scan	ip=192.168.1.110	dos_id=1	exp=649	pps=0	freq=0
id=udp_flood	ip=192.168.1.110	dos_id=2	exp=653	pps=0	freq=0
id=tcp_src_session	ip=192.168.1.110	dos_id=1	exp=5175	pps=0	freq=8
id=tcp_port_scan	ip=192.168.1.110	dos_id=1	exp=175	pps=0	freq=0
id=ip_src_session	ip=192.168.1.110	dos_id=1	exp=5649	pps=0	freq=30
id=udp_src_session	ip=192.168.1.110	dos_id=1	exp=5649	pps=0	freq=22

Which IP addresses are included in the output of this command?

- A. Those whose traffic matches a DoS policy.
- B. Those whose traffic matches an IPS sensor.
- C. Those whose traffic exceeded a threshold of a matching DoS policy.
- D. Those whose traffic was detected as an anomaly by an IPS sensor.

Answer: A

NEW QUESTION 15

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


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

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

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

Answer: A

NEW QUESTION 16

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 21

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     -5   262432   0          846
64.26.151.35 10      46    -5     -5   329072   0          6806
66.117.56.37 10      75    -5     -5   71638    0          275
65.210.95.240 20      71    -8     -8   36875    0          92
209.222.147.36 20      103   DI     -8   34784    0          1070
208.91.112.194 20      107   D      -8   35170    0          1533
96.45.33.65 60      144    0      0    33728    0          120
80.85.69.41 71      226    1      1    33797    0          192
62.209.40.74 150     97     9      9    33754    0          145
121.111.236.179 45      44    F      -5   26410    26226     26227
```

Which 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 25

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

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

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

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

Answer: C

NEW QUESTION 26

Examine the output of the 'get router info ospf interface' command shown in the exhibit; then answer the question below.

```
# 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 7 sent 9
    LS-Req received 2 sent 2, LS-Upd received 7 sent 5
    LS-Ack received 4 sent 3, Discarded 1
```

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

- A. The port4 interface is connected to the OSPF backbone area.
- B. The local FortiGate has been elected as the OSPF backup designated router.
- C. There are at least 5 OSPF routers connected to the port4 network.
- D. Two OSPF routers are down in the port4 network.

Answer: AC

Explanation:

on BROADCAST network there are 4 neighbors, among which 1*DR +1*BDR. So our FG has 4 neighbors, but create adjacency only with 2 (with DR and BDR). 2 neighbors DROther (not down).

NEW QUESTION 30

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

```
#dia hardware sysinfo shm
SHM counter:          150
SHM allocated:         0
SHM total:           625057792
conserve mode: on - mem
system last entered: Mon Apr 24 16:36:37 2017
sys fd last entered: n/a
SHM FS total:   641236992
SHM FS free:    641208320
SHM FS avail:   641208320
SHM FS alloc:   28672
```

What statement is correct about this FortiGate?

- A. It is currently in system conserve mode because of high CPU usage.
- B. It is currently in FD conserve mode.
- C. It is currently in kernel conserve mode because of high memory usage.
- D. It is currently in system conserve mode because of high memory usage.

Answer: D

NEW QUESTION 34

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-[enable|disable])

NEW QUESTION 36

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

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
    name: 'Hub2Spoke1'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
  SA
    lifetime/rekey: 43200/32137
    mtu: 1438
    tx-esp-seq: 2ce
    replay: enabled
  inbound
    spi: 01e54b14
    enc: aes-cb 914dc5d092667ed436ea7f6efb867976
    auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
  outbound
    spi: 3dd3545f
    enc: aes-cb 017b8ff6c4ba21eac99b22380b7de74d
    auth: sha1 edd8141f4956140eef703d9042621d3dbf5cd961
  NPU acceleration: encryption(outbound) decryption(inbound)
```


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

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

Answer: AC

NEW QUESTION 40

View the global IPS configuration, and then answer the question below.

```
config ips global
    set fail-open disable
    set intelligent-mode disable
    set engine-count 0
    set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

- A. IPS will scan every byte in every session.
- B. FortiGate will spawn IPS engine instances based on the system load.
- C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.
- D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Answer: A

NEW QUESTION 45

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 50

When does a RADIUS server send an Access-Challenge packet?

- A. The server does not have the user credentials yet.
- B. The server requires more information from the user, such as the token code for two-factor authentication.
- C. The user credentials are wrong.
- D. The user account is not found in the server.

Answer: B

NEW QUESTION 54

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 55

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

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

What does the log mean?

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

Answer: B

NEW QUESTION 59

Which statement is true regarding File description (FD) conserve mode?

- A. IPS inspection is affected when FortiGate enters FD conserve mode.
- B. A FortiGate enters FD conserve mode when the amount of available description is less than 5%.
- C. FD conserve mode affects all daemons running on the device.
- D. Restarting the WAD process is required to leave FD conserve mode.

Answer: B

NEW QUESTION 60

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 64

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

```
# diagnose hardware sysinfo conserve
memory conserve mode:          on
total RAM:                     3040 MB
memory used:                   2706 MB 89% of total RAM
Memory freeable:              334 MB 11% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red:     2675 MB 88% of total RAM
memory used threshold green:   2492 MB 82% of total RAM
```

Which one of the following statements about this FortiGate is correct?

- A. It is currently in system conserve mode because of high CPU usage.
- B. It is currently in extreme conserve mode because of high memory usage.
- C. It is currently in proxy conserve mode because of high memory usage.
- D. It is currently in memory conserve mode because of high memory usage.

Answer: D

NEW QUESTION 67

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

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

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

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

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

Answer: BC

NEW QUESTION 70

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 72

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	
Incorrect CRC : 0	Requests : 0
Proxy request failures : 0	Misses : 0
Request timeout : 1	Hits : 0
Total requests : 2409	Prefix hits : 0
Requests to FortiGuard servers : 1182	Exact hits : 0
Server errored responses : 0	
Relayed rating : 0	No cache directives : 0
Invalid profile : 0	Add after prefix : 0
	Invalid DB put : 0
Allowed : 1021	DB updates : 0
Blocked : 3909	
Logged : 3927	Percent full : 0%
Blocked Errors : 565	Branches : 0%
Allowed Errors : 0	Leaves : 0%
Monitors : 0	Prefix nodes : 0%
Authenticates : 0	Exact nodes : 0%
Warnings: 18	
Ovrd request timeout : 0	Miss rate : 0%
Ovrd send failures : 0	Hit rate : 0%
Ovrd read failures : 0	Prefix hits : 0%
Ovrd errored responses : 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 75

Examine the output of the 'get router info ospf neighbor' command shown in the exhibit; then answer the question below.

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 wan1
0.0.0.2 1 Full/- 00:00:36 172.16.1.2 ToRemote

Which statements are true regarding the output in the exhibit? (Choose two.) Refer to the exhibit, which shows the output of a debug command.
Which statement about the output is true?

- A. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wan1 network.
- B. I network.
- C. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.
- D. The local FortiGate is the designated router for the wan1 network.
- E. The interface ToRemote is a point-to-point OSPF network.

Answer: D

Explanation:

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html>

NEW QUESTION 77

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 78

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

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 79

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

NEW QUESTION 81

Examine the output of the 'get router info bgp summary' command shown in the exhibit; then answer the question below.

Student# get router info bgp summary

BGP router identifier 10.200.1.1, local AS number 65500

BGP table version is 2

1 BGP AS-PATH entries

0 BGP community entries

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.200.3.1	4	65501	92	112	0	0	0	never	Connect

Total number of neighbors 1

Which statement can explain why the state of the remote BGP peer 10.200.3.1 is Connect?

- A. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
- B. The TCP session for the BGP connection to 10.200.3.1 is down.
- C. The local peer has received the BGP prefixed from the remote peer.
- D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Answer: B

Explanation:

<http://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4>

NEW QUESTION 83

Which real time debug should an administrator enable to troubleshoot RADIUS authentication problems?

- A. Diagnose debug application radius -1.
- B. Diagnose debug application fnbamd -1.
- C. Diagnose authd console -log enable.
- D. Diagnose radius console -log enable.

Answer: B

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD32838>

NEW QUESTION 85

Examine the output from the 'diagnose debug authd fsso list' command; then answer the question below.

diagnose debug authd fsso list —FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is

NOT the one used by the workstation INTERNAL2. TRAINING. LAB.

What should the administrator check?

- A. The IP address recorded in the logon event for the user STUDENT.
- B. The DNS name resolution for the workstation name INTERNAL2. TRAININ
- C. LAB.
- D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2.TRAININ
- E. LAB.
- F. The reserve DNS lookup forthe IP address 192.168.3.1.

Answer: C

NEW QUESTION 88

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 91

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

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

Answer: AD

NEW QUESTION 92

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 96

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 101

Examine the output of the 'get router info bgp summary' command shown in the exhibit; 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 statements are true regarding the output in the exhibit? (Choose two.)

- A. BGP state of the peer 10.125.0.60 is Established.
- B. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.
- C. Local BGP peer has not received an OpenConfirm from 10.200.3.1.
- D. The local BGP peer has received a total of 3 BGP prefixes.

Answer: AC

NEW QUESTION 103

Which statement about memory conserve mode is true?

- A. A FortiGate exits conserve mode when the configured memory use threshold reaches yellow.
- B. A FortiGate starts dropping all the new and old sessions when the configured memory use threshold reaches extreme.
- C. A FortiGate starts dropping new sessions when the configured memory use threshold reaches red
- D. A FortiGate enters conserve mode when the configured memory use threshold reaches red

Answer: D

NEW QUESTION 108

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

Name	Remote
Comments	Comments

Network

IP Version ☒ IPv4 ☐ IPv6

Remote Gateway Static IP address ▼

IP Address 10.0.10.1

Interface port1 ▼

Mode Config ☐

NAT Traversal ☒

Keepalive Frequency 10 —

Dead Peer Detection ☒

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

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

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

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

Answer: B

NEW QUESTION 113

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

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

The administrator does not have access to the remote gateway.

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

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

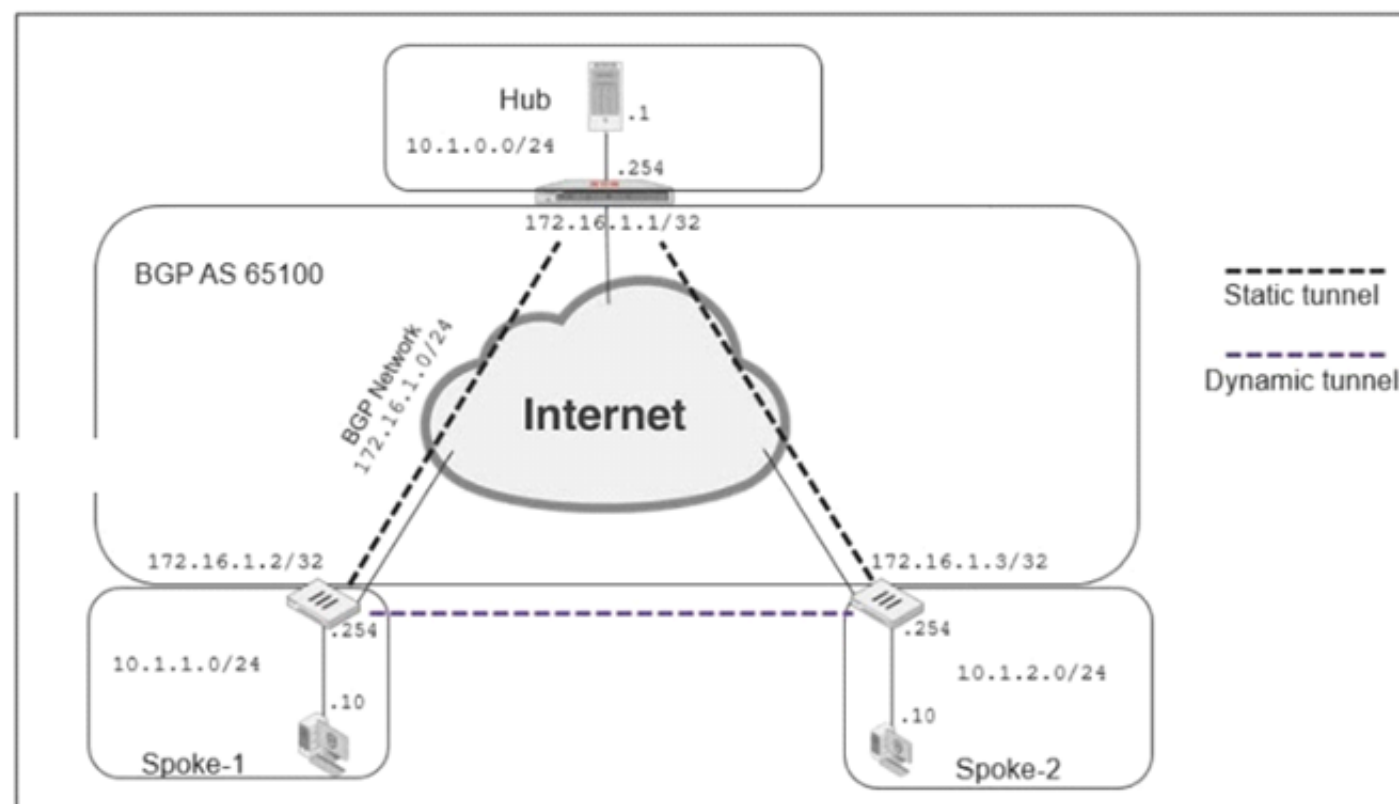
Answer: D

Explanation:

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

NEW QUESTION 116

Exhibits:



```

now 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 120

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 123

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 124

View these partial outputs from two routing debug commands:

```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254
dev=2(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev=4(port3)
# get router info routing-table all
S*    0.0.0.0/0 [10/0] via 10.200.1.254, port1
      [10/0] via 10.200.2.254, port2, [10/0]
C     10.0.1.0/24 is directly connected, port3
C     10.200.1.0/24 is directly connected, port1
C     10.200.2.0/24 is directly connected, port2
```

Which outbound interface will FortiGate use to route web traffic from internal users to the Internet?

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

Answer: C

NEW QUESTION 125

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

```

Configuration Session
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

```

```

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

```

An administrator would like to test session failover between the two service provider connections.
 What changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

- A. Configure set snat-route-change enable.
- B. Change the priority of the port2 static route to 5.
- C. Change the priority of the port1 static route to 11.
- D. unset snat-route-change to return it to the default setting.

Answer: AC

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 148-149

NEW QUESTION 129

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two.)

- A. It provides VM license validation services.
- B. It supports rating requests from non-FortiGate devices.
- C. It caches available firmware updates for unmanaged devices.
- D. It can be configured as an update server, a rating server, or both.

Answer: AD

NEW QUESTION 133

You have configured FortiManager as a local FDS to provide FortiGate AV and IPS updates, but FortiGate devices are not receiving updates to their AV signature databases, IPS engines, or IPS signature databases.

Which two settings need to be verified for these features to function? (Choose two.)

- A. FortiGate needs to have the server list entry for FortiManager set to server-type update under config system central-management.
- B. FortiManager needs to be the license validation server for FortiGate devices trying to retrieve updated AV and IPS packages.
- C. Service access needs to be enabled on FortiManager under System Settings > Network.
- D. FortiGate needs to have include-default-servers disabled under config system central-management.

Answer: AC

Explanation:

NSE 7.0 Guide page 184-185

NEW QUESTION 134

Which statement about NGFW policy-based application filtering is true?

- A. After the application has been identified, the kernel uses only the Layer 4 header to match the traffic.
- B. The IPS security profile is the only security option you can apply to the security policy with the action set to ACCEPT.
- C. After IPS identifies the application, it adds an entry to a dynamic ISDB table.
- D. FortiGate will drop all packets until the application can be identified.

Answer: D

NEW QUESTION 137

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 -1
#diagnose debug enable
#diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd 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_ist_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 139

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

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

Answer: AD

Explanation:

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

NEW QUESTION 144

An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth) and IKE mode configuration. The administrator has also enabled the IKE real time debug:

diagnose debug application ike-1 diagnose debug enable

In which order is each step and phase displayed in the debug output each time a new dial-up user is connecting to the VPN?

- A. Phase1; IKE mode configuration; XAuth; phase 2.
- B. Phase1; XAuth; IKE mode configuration; phase2.
- C. Phase1; XAuth; phase 2; IKE mode configuration.
- D. Phase1; IKE mode configuration; phase 2; XAuth.

Answer: B

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/IKE_Packet

NEW QUESTION 149

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

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

Answer: BDE

NEW QUESTION 154

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 159

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 160

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 162

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

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

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

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

Answer: B

NEW QUESTION 167

.....

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/>