

# Fortinet

## Exam Questions NSE7\_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0



**NEW QUESTION 1**

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

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

**Answer:** AC

**NEW QUESTION 2**

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

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

**Answer:** AB

**NEW QUESTION 3**

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](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 4**

Examine the IPsec configuration shown in the exhibit; then answer the question below.

Name	<input type="text" value="Remote"/>	
Comments	<input type="text" value="Comments"/>	
Network		
IP Version	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6
Remote Gateway	<input type="text" value="Static IP Address"/>	<input checked="" type="checkbox"/>
IP Address	<input type="text" value="10.0.10.1"/>	
Interface	<input type="text" value="port1"/>	<input checked="" type="checkbox"/>
Mode Config	<input type="checkbox"/>	
NAT Traversal	<input checked="" type="checkbox"/>	
Keepalive Frequency	<input type="text" value="10"/>	
Dead Peer Detection	<input checked="" type="checkbox"/>	

An administrator wants to monitor the VPN by enabling the IKE real time debug using these commands: `diagnose vpn ike log-filter src-addr4 10.0.10.1`  
`diagnose debug application ike -1`  
`diagnose debug enable`  
The VPN is currently up, there is no traffic crossing the tunnel and DPD packets are being interchanged between both IPsec gateways. However, the IKE real time debug does NOT show any output. Why isn't there any output?

- A. The IKE real time shows the phases 1 and 2 negotiations onl
- B. It does not show any more output once the tunnel is up.
- C. The log-filter setting is set incorrectl
- D. The VPN's traffic does not match this filter.
- E. The IKE real time debug shows the phase 1 negotiation onl
- F. For information after that, the administrator must use the IPsec real time debug instead: `diagnose debug application ipsec -1`.
- G. The IKE real time debug shows error messages onl
- H. If it does not provide any output, it indicates that the tunnel is operating normally.

**Answer: B**

#### NEW QUESTION 5

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
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary 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 6

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 7

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: IKEv1 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 16:39915120ED73E520787C801DE3678916
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 A2FBD6BB6394401A06B89C022D4DF682081004010000000000000500B000018882A078E09026CA8B2
ike 0:Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF6820810040100000000000005C64D5CBA90B873F150CB8B5CC2A
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 initiator provided remote as its IPsec peer ID.
- B. It shows a phase 2 negotiation.
- C. Perfect Forward Secrecy (PFS) is enabled in the configuration.
- D. The local gateway IP address is 10.0.0.1.

**Answer:** AD

**Explanation:**

A because : received peer identifier FQDN 'remote' D because : ike 0: comes 10.0.0.2:500 -> 10.0.0.1:500

**NEW QUESTION 8**

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 9**

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 10

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 14

Four FortiGate devices configured for OSPF connected to the same broadcast domain. The first unit is elected as the designated router The second unit is elected as the backup designated router Under normal operation, how many OSPF full adjacencies are formed to each of the other two units?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

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 20

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 22

An administrator wants to capture encrypted phase 2 traffic between two FortiGate devices using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGate devices, which command should the administrator run?

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

**Answer:** B

#### Explanation:

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

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

#### NEW QUESTION 25

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 26

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

Passing Certification Exams Made Easy

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



```
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 28

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

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

- A. This is an expected session created by a session helper.
- B. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.0.1.10.
- C. Traffic in the original direction (coming from the IP address 10.171.122.38) will be routed to the next-hop IP address 10.200.1.1.
- D. This is an expected session created by an application control profile.

**Answer:** AC

#### NEW QUESTION 32

View the IPS exit log, and then answer the question below.

# diagnose test application ipsmonitor 3 ipsengine exit log"

pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017 code = 11, reason: manual

What is the status of IPS on this FortiGate?

- A. IPS engine memory consumption has exceeded the model-specific predefined value.
- B. IPS daemon experienced a crash.
- C. There are communication problems between the IPS engine and the management database.
- D. All IPS-related features have been disabled in FortiGate's configuration.

**Answer:** D

**Explanation:**

The command diagnose test application ipsmonitor includes many options that are useful for troubleshooting purposes. Option 3 displays the log entries generated every time an IPS engine process stopped. There are various reasons why these logs are generated: Manual: Because of the configuration, IPS no longer needs to run (that is, all IPS-related features have been disabled)

**NEW QUESTION 37**

View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
origin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement is correct regarding this session?

- A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
- B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
- C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
- D. It is a TCP session in CLOSE\_WAIT state from 10.1.10.10 to 10.200.1.1.

**Answer:** B

**NEW QUESTION 38**

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 39**

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



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

IP	Weight	RTT	Flags	TZ	Packets	Curr Lost	Total Lost
64.26.151.37	10	45		-5	262432	0	846
64.26.151.35	10	46		-5	329072	0	6806
66.117.56.37	10	75		-5	71638	0	275
65.210.95.240	20	71		-8	36875	0	92
209.222.147.36	20	103	DI	-8	34784	0	1070
208.91.112.194	20	107	D	-8	35170	0	1533
96.45.33.65	60	144		0	33728	0	120
80.85.69.41	71	226		1	33797	0	192
62.209.40.74	150	97		9	33754	0	145
121.111.236.179	45	44	F	-5	26410	26226	26227

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

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

**Answer:** AD

**Explanation:**

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

#### NEW QUESTION 40

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
gwy=100.64.1.254/10.0.1.10
hook-post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook-pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

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

**Answer:** C

#### NEW QUESTION 45

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

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

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

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

**Answer:** AC

**Explanation:**

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

#### NEW QUESTION 50

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 55

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 59

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 61

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 66

Refer to the exhibit, which shows 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 has a different AS number than the remote peer.
- B. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the openConfirm yet.
- C. The local router initiated the BGP session to 10.200.3.1 but did not receive a response.
- D. The router 10.200.3.1 has authentication configured for BGP and the local router does not.

**Answer: C**

#### NEW QUESTION 68

Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

IP	Weight	RTT	Flags	TZ	Packets	Curr Lost	Total Lost
69.195.205.101	10	45		-5	262432	0	846
69.195.205.102	10	46		-5	329072	0	6806
209.222.147.43	10	75		-5	71638	0	275
96.45.33.65	20	71		-8	36875	0	92
208.91.112.196	20	103	DI	-8	34784	0	1070
208.91.112.198	20	107	D	-8	35170	0	1533
80.85.69.41	60	144		0	33728	0	120
62.209.40.73	71	226		1	33797	0	192
121.111.236.180	150	197		9	33754	0	145
69.195.205.103	45	44	F	-5	26410	26226	26227

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

- A. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.
- B. The TZ value represents the delta between each FortiGuard server's time zone and the FortiGate's time zone.
- C. FortiGate will send the FortiGuard queries to the server with highest weight.
- D. A server's round trip delay (RTT) is not used to calculate its weight.

**Answer: BC**

#### NEW QUESTION 71

An administrator has created a VPN community within VPN Manager on FortiManager. They also added gateways to the VPN community and are now trying to create firewall policies to permit traffic over the tunnel; however, the VPN interfaces are not listed as available options. What step must the administrator take to resolve this issue?

- A. Install the VPN community and gateway configuration to the FortiGate devices, in order for the interfaces to be displayed within Policy & Objects on FortiManager
- B. Set up all of the phase 1 settings in the VPN community that they neglected to set up initiall
- C. The interfaces will be automatically generated after the administrator configures all of the required settings.
- D. Refresh the device status from the Device Manager so that FortiGate will populate the IPsec interfaces.
- E. Create interface mappings for the IPsec VPN interfaces, before they can be used in a policy.

**Answer: A**

#### Explanation:

\* - Create a VPN Community 2- Install VPN Configuration 3- Add IPsec Firewall Policies 4- Install the Policies

#### NEW QUESTION 72

Examine the partial output from the IKE real time debug shown in the exhibit; then answer the question below.



```
#diagnose debug application ike -1
#diagnose debug enable
ike 0: ....: 75: responder: aggressive mode get 1st message...
...
ike 0: ....:76: incoming proposal:
ike 0: ....:76: proposal id = 0:
ike 0: ....:76: protocol id= ISAKMP:
ike 0: ....:76: trans_id = KEY_IKE.
ike 0: ....:76: encapsulation = IKE/none
ike 0: ....:76: type= OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0: ....:76: type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ....:76: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ....:76: type=OAKLEY_GROUP, val=MODP2048.
ike 0: ....:76: ISAKMP SA lifetime=86400
ike 0: ....:76: my proposal, gw Remote:
ike 0: ....:76: proposal id=1:
ike 0: ....:76: protocol id= ISAKMP:
ike 0: ....:76: trans_id= KEY_IKE.
ike 0: ....:76: encapsulation = IKE/none
ike 0: ....:76: type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0: ....:76: type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ....:76: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ....:76: type=OAKLEY_GROUP, val=MODP2048.
ike 0: ....:76: ISAKMP SA lifetime=86400
ike 0: ....:76: proposal id=1:
ike 0: ....:76: protocol id= ISAKMP:
ike 0: ....:76: trans_id= KEY_IKE.
ike 0: ....:76: encapsulation = IKE/none
ike 0: ....:76: type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0: ....:76: type= OAKLEY_HASH_ALG, val=SHA2_256.
ike 0: ....:76: type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: ....:76: type=OAKLEY_GROUP, val=MODP1536.
ike 0: ....:76: ISAKMP SA lifetime=86400
ike 0: ....:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0: ....:76: no SA proposal chosen
```

Why didn't the tunnel come up?

- A. IKE mode configuration is not enabled in the remote IPsec gateway.
- 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. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

**Answer: C**

#### NEW QUESTION 74

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 78

A FortiGate has two default routes:

```
config router static
  edit 1
    set gateway 10.200.1.254
    set priority 5
    set device "port1"
  next
  edit 2
    set gateway 10.200.2.254
    set priority 10
    set device "port2"
  next
end
```

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

```
# diagnose sys session list
Session info: proto=6 proto_state=01 duration =17 expire=7 timeout=3600
flags= 00000000 sockflag=00000000 sockport=0 av idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic (bytes/packets/allow_err): org=575/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:64907(10.0.1.10:64907)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

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

**Answer:** D

#### NEW QUESTION 83

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

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

**Answer:** BC

#### Explanation:

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

#### NEW QUESTION 88

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 89**

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 93**

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 97**

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 101

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 103**

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 107**

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 112

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 114

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

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

**Answer:** AC

#### NEW QUESTION 117

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 119

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 120

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 124

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 128

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 IPAddress: 10.72.3.52. Destination IP address: 10.1.0.254
- C. Source IPAddress: 10.10.4.24, Destination IPAddress: 10.72.3.20
- D. Source IPAddress: 10.73.9.10, Destination IPAddress: 10.72.3.15

**Answer: AB**

#### NEW QUESTION 130

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

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

**Answer: A**

#### NEW QUESTION 134

View the exhibit, which contains the output of a debug command, and 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 of the following statements about the exhibit are true? (Choose two.)

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

**Answer:** BC

#### NEW QUESTION 136

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

```
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=20000 ms 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: 0:10.1.1.2.0/255.255.0:0
  dst: 0:10.1.1.0/255.255.255.0:0
  SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
  life: type=01 bytes=0/0 timeout=43177/43200
  dec: spi=cccl1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
    ah=shal key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
    ah=shal key20 889f7529887c215c25950be2ba83e6fela5367be
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Based on the output, which of the following statements is correct?

- A. Anti-reply is enabled.
- B. DPD is disabled.
- C. Quick mode selectors are disabled.
- D. Remote gateway IP is 10.200.5.1.

**Answer:** A

#### NEW QUESTION 137

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 138

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 143

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 147

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 149

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

```
# diagnose sys session list expectation

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

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

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



Answer: AD

**Explanation:**

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

**NEW QUESTION 154**

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 156

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 160

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

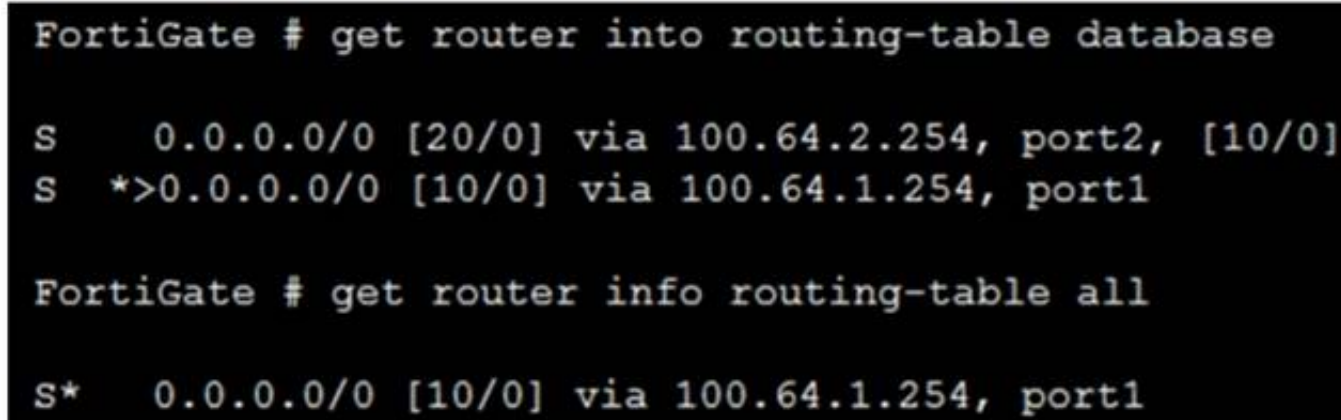
**Answer: CD**

#### 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 161

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 165

What is the purpose of an internal segmentation firewall (ISFW)?

- A. It inspects incoming traffic to protect services in the corporate DMZ.
- B. It is the first line of defense at the network perimeter.
- C. It splits the network into multiple security segments to minimize the impact of breaches.

D. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

**Answer:** C

**Explanation:**

ISFW splits your network into multiple security segments. They serve as a breach containers from attacks that come from inside.

**NEW QUESTION 166**

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

```
ike 0:H2S_0_1: shortcut 10.200.5.1:0 10.1.2.254->10.1.1.254
...
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-OFFER): 10.200.1.1:500->10.200.5.1:500,
len=164, id=4134df8580d5cdd/ce54851612c7432f:a21f14fe
ike 0: comes 10.200.5.1:500->10.200.1.1:500,ifindex=3....
ike 0: IKEv1 exchange=Informational id=4134df8580d5bcdd/ce54851612c7432f:6266ee8c
len=196

ike 0:H2S_0_1:15: notify msg received: SHORTCUR-QUERY
ike 0:H2S_0_1: recv shortcut-query 16462343159772385317

ike 0:H2S_0_0:16: senr IKE msg (SHORTCUT-QUERY): 10.200.1.1:500->10.200.3.1:500,
len=196, id=7c6b6cca6700a935/dba061eaf51b89f7:b326df2a
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=3....
ike 0: IKEv1 exchange=Informational id=7c6b6cca6700a935/dba061eaf51b89f7:1c1dbf39
len=188

ike 0:H2S_0_0:16: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0: recv shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64
ike 0:H2S_0_0: shortcut-reply route to 10.1.2.254 via H2S_0_1 29
ike 0:H2S: forward shortcut-reply 16462343159772385317
f97a7565a441e2aa/667d3e2e3442211e 10.200.3.1 to 10.1.2.254 psk 64 ttl 31
ike 0:H2S_0_1:15: enc
...
ike 0:H2S_0_1:15: sent IKE msg (SHORTCUT-REPLY): 10.200.1.1:500->10.200.5.1:500,
len=188, id=4134df8580d5bcdd/ce54851612c7432f:70ed6d2c
```

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

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

**Answer:** B

**NEW QUESTION 168**

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-Recv auth req 4 for student in WindowsLDAP
opt=27 prot=0
fnbamd_fsm.c[336] _compose_group_list_from_req_Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] fnbamd_cfg-get_ldap_list_by_server-Loading LDAP server
'WindowsLDAP'
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_auth_session-Total 1 server (s) to try
fnbamd_ldap.c[1700] fnbamd_ldap_get_result-Error in ldap result: 49
(Invalid credentials)
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 4
fnbamd_fsm.c[568] destroy_auth_session-delete session 4
authenticate 'student' against 'WindowsLDAP' failed!
```

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

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

**Answer:** BC

**Explanation:**

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

#### NEW QUESTION 170

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 173

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 175

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

```
# 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
```

If the default settings are in place, what can be concluded about the conserve mode shown in the exhibit?

- A. FortiGate is currently blocking all new sessions regardless of the content inspection requirements or configuration settings due to high memory use.
- B. FortiGate is currently allowing new sessions that require flow-based or proxy-based content inspection but is not performing inspection on those sessions.
- C. FortiGate is currently blocking new sessions that require flow-based or proxy-based content inspection.
- D. FortiGate is currently allowing new sessions that require flow-based content inspection and blocking sessions that require proxy-based content inspection.

Answer: C

#### NEW QUESTION 178

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

```
NGFW # get sys ha status
HA Health Status: ok
Model: FortiGate0VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 01:07:35
Master selected using:
<2017/04/24 09:43:44> FGVM010000077649 is selected as the master because it has the largest value of override pr
<2017/04/24 08:50:53> FGVM010000077 is selected as the master because it's the only member in the cluster.
ses_pickup: disable
override: enable
Configuration Status:
FGVM010000077649(updated 1 seconds ago): in-sync
FGVM010000077650(updated 0 seconds ago): out-of-sync
System Usage stats:
FGVM010000077649(updated 1 seconds ago):
sessions=30, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-60%
FGVM010000077650(updated 0 seconds ago):
sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory-61%
HBDEV stats:
FGVM010000077649(updated 1 seconds ago):
port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7358367/17029/25/0, tx=7721830/17182/0/0
FGVM010000077650(updated 0 seconds ago):
port7: physical/10000full, up, rx-bytes/packets/dropped/errors=7793722/17190/0/0, tx=8940374/20806/0/0
Master: NGFW      , FGVM010000077649
Slave : NGFW-2    , FGVM010000077650
number of vcluster: 1
vcluster 1: work 169.254.0.2
Master:0 FGVM0100000077649
Slave :1 FGVM0100000077650
```

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

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

**Answer:** AD

#### NEW QUESTION 180

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 181

Examine the following partial output from two system debug commands; then answer the question below.



```
# diagnose hardware sysinfo memory
MemTotal: 3092728 kB
MemFree: 1954204 kB
MemShared: 0 kB
Buffers: 284 kB
Cached: 143004 kB
SwapCached: 0 kB
Active: 34092 kB
Inactive: 109256 kB
HighTotal 1179648 kB
HighFree: 853516 kB
LowTotal: 1913080 kB
LowFree: 1100688 kB
SwapTotal: 0 kB
SwapFree: 0 kB
# diagnose hardware sysinfo shm
SHM counter: 285
SHM allocated: 6823936
SHM total: 623452160
concermode: 0
shm last entered: n/a
system last entered: n/a
SHM FS total: 639725568
SHM FS free: 632614912
```

SHM FS alloc: 7110656

Which of the following statements are true regarding the above outputs? (Choose two.)

- A. The unit is running a 32-bit FortiOS
- B. The unit is in kernel conserve mode
- C. The Cached value is always the Active value plus the Inactive value
- D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Answer: AC

#### NEW QUESTION 184

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

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 187**

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 190**

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 191**

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

```
config system global
    set snat-route-change disable
end

config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
origin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907 -> 54.239.158.170.80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlfid=0/0, vtag_in=0x0000/0x000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 193

What does the dirty flag mean in a FortiGate session?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 197

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

Which statement about this setting is true?

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



**Answer:** D

**NEW QUESTION 200**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

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

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

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