

Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0



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

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 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

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 5

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 6

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

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

Answer: A

Explanation:

http://docs-legacy.fortinet.com/fos40hlp/43prev/wwhelp/wwhimpl/common/html/wwhelp.htm?context=fgt&file=CLI_get_Commands.58.25.html

The tcp-halfopen-timer controls for how long, after a SYN packet, a session without SYN/ACK remains in the table.

The tcp-halfclose-timer controls for how long, after a FIN packet, a session without FIN/ACK remains in the table.

The tcp-timewait-timer controls for how long, after a FIN/ACK packet, a session remains in the table. A closed session remains in the session table for a few seconds more to allow any out-of-sequence packet.

NEW QUESTION 7

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

An administrator has configured the TCL script on FortiManager, but the TCL script failed to apply any changes to the managed device after being run.

Type	TCL Script
Run script on	Remote FortiGate ...
Script details	<pre>#!/ proc do_cmd [cmd] { puts [exec "\$cmd\n" "# " 10] } run_cmd "config system interface " run_cmd "edit port1" run_cmd "set ip 10.0.1.10 255.255.255.0" run_cmd "next" run_cmd "end"</pre>

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

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

Answer: A

Explanation:

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

NEW QUESTION 8

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

```
FortiGate # get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.1.254 dev=3(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=10 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=100.64.2.254 dev=6(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.1.0.0/24 pref=10.1.0.254 gwy=0.0.0.0 dev=9(port3)

FortiGate # get router info routing-table all

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

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

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

Answer: A

Explanation:

ECMP pre-requisite is "routes must have the same destination and costs. In the case of static routes, costs include distance and priority". In this case traffic is routed through port 1 because of the lower priority. If we raise priority on port 1 to the value of 10 the traffic should be routed through both ports 1 and 2.

<https://docs.fortinet.com/document/fortigate/7.0.1/administration-guide/25967/equal-cost-multi-path>

NEW QUESTION 9

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 RFC 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 10

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

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7. . .
ike 0: IKEv2 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response. . .
ike 0: Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated
ike 0: Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: received peer identifier FQDN 'remote'
ike 0: Remotesite:3: negotiation result
ike 0: Remotesite:3: proposal id = 1:
ike 0: Remotesite:3:   protocol id = ISAKMP:
ike 0: Remotesite:3:   trans_id = KEY_IKE.
ike 0: Remotesite:3:   encapsulation = IKE/none.
ike 0: Remotesite:3:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: Remotesite:3:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0: Remotesite:3:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: Remotesite:3:   type=OAKLEY_GROUP, val=MODP1024.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key
16:39915120ED73ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc
A2FBD6BB6394401A06B89C022D4DF682081004010000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0: Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140,
id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```


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

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

Answer: BC

NEW QUESTION 10

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 11

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=ccclf66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
      ah=sha1 key=20 c68091d68753578785de6a7a6b276b506c527efe
  enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
      ah=sha1 key=20 889f7529887c215c25950be2ba83e6fe1a5367be
  dec: pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

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

Answer: AB

NEW QUESTION 16

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

```
ike 0:H2S_0_1:1249: notify msg received: SHORTCUT-QUERY
ike 0:H2S_0_1:  recv shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000 100.64.3.1
10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0
ike 0:H2S_0: iif 13 10.1.1.254->10.1.2.254 route lookup oif 13
ike 0:H2S_0_0: forward shortcut-query 12594932268010586978 4384dd592d62cd52/0000000000000000
100.64.3.1 10.1.1.254->10.1.2.254 psk 64 ppk 0 ttl 31 ver 1 mode 0, ext-ma
ike 0:H2S_0_0:1248: sent IKE msg (SHORTCUT-QUERY): 100.64.1.1:500->100.64.5.1:500, len=236,
id=e2beec89f13c7074/06a73dfb3a5d3b54:340a645c
ike 0: comes 100.64.5.1:500->100.64.1.1:500, ifindex=3. . .
ike 0: IKEv1 exchange=Informational id=e2beec89f13c7074/06a73dfb3a5d3b5d:26254ae9 len=236
ike 0:H2S_0_0:1248: notify msg received: SHORTCUT-REPLY
ike 0:H2S_0_0:  recv shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0 100.64.5.1
to 10.1.1.254 psk 64 ppk 0 ver 1 mode 0 ext-mapping 100.64.3.1:500
ike 0:H2S_0: iif 13.10.1.2.254->10.1.1.254 route lookup oif 13
ike 0:H2S_0_1: forward shortcut-reply 12594932268010586978 4384dd592d62cd52/89bf040f5f7408c0
100.64.5.1 to 10.1.1.254 psk 64 ppk 0 ttl 31 ver 1 mode 0 ext-mapping 100.
```

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

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

Answer: D

NEW QUESTION 20

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 21

Which statement about protocol options is true?

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

Answer: D

NEW QUESTION 26

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 min
 D-state is I , contact to validate contract info

NEW QUESTION 27

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 32

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 35

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 38

An administrator added the following Ipsec VPN to a FortiGate configuration:

```
configvpn ipsec phasel -interface edit "RemoteSite"
set type dynamic
set interface "port1"
set mode main
set psksecret ENC LCVkCiK2E2PhVUzZe next
end
config vpn ipsec phase2-interface edit "RemoteSite"
set phasel name "RemoteSite" set proposal 3des-sha256
next end
```

However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the Ipsec connection. The output is shown in the exhibit.

```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=716
ike 0:xxx/xxx:16: responder: main mode get 1st message...
ike 0:xxx/xxx:16: VID RFC 3947 4A131C81070358455C5728F20E95452F
...
ike 0:xxx/xxx:16: negotiation result
ike 0:xxx/xxx:16: proposal id = 1:
ike 0:xxx/xxx:16:   protocol id = ISAKMP:
ike 0:xxx/xxx:16:   trans_id = KEY IKE.
ike 0:xxx/xxx:16:   encapsulation = IKE/none
ike 0:xxx/xxx:16:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:xxx/xxx:16:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:xxx/xxx:16:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:xxx/xxx:16:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:xxx/xxx:16: ISAKMP SA lifetime=86400
ike 0:xxx/xxx:16: SA proposal chosen, matched gateway DialUpUsers
...
ike 0:DialUpUsers:16: sent IKE msg (ident_r1send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=380
ike 0:DialUpUsers:16: responder:main mode get 2nd message...
ike 0:DialUpUsers:16: NAT not detected
ike 0:DialUpUsers:16: sent IKE msg (ident_r2send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
ike 0:DialUpUsers:16: ISAKMP SA xxx/xxx key 16:3D33E2EF00BE927701B5C25B05A62415
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=108
ike 0:DialUpUsers:16: responder: main mode get 3rd message...
ike 0:DialUpUsers:16: probable pre-shared secret mismatch
ike 0:DialUpUsers:16: unable to parse msg
```

What is causing the IPsec problem in the phase 1 ?

- A. The incoming IPsec connection is matching the wrong VPN configuration
- B. The phrase-1 mode must be changed to aggressive
- C. The pre-shared key is wrong
- D. NAT-T settings do not match

Answer: C

NEW QUESTION 43

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 48

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 routers 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 52

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 54

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 56

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 57

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device.

What can the administrator do to fix this problem?

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

Answer: D

Explanation:

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

NEW QUESTION 62

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 66

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 71

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 72

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 73

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 78

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 80

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

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

Answer: B

NEW QUESTION 84

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

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 89

Which action will FortiGate take when using the default settings for SSL certificate inspection, where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate?

- A. FortiGate uses the CN information from the Subject field in the server certificate.

- B. FortiGate uses the first entry listed in the SAN field in the server certificate.
- C. FortiGate uses the SNI from the user's web browser.
- D. FortiGate closes the connection because this represents an invalid SSL/TLS configuration.

Answer: A

Explanation:

#Config firewall ssl-ssh-profile

edit <profile_name> config https

set sni-server-cert-check [enable* | strict | disable]

Enable: If the SNI does NOT match the CN or SAN fields in the returned server's certificate, FG uses the CN field instead of the SNI to obtain the FQDN.

Strict: If the SNI does NOT match the CN or SAN fields in the returned server's certificate, FG closes the connection.

Disable: FG does not check the SNI.

NEW QUESTION 93

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 95

A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fssso list' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

- A. The user student must not be listed in the CA's ignore user list.
- B. The user student must belong to one or more of the monitored user groups.
- C. The student workstation's IP subnet must be listed in the CA's trusted list.
- D. At least one of the student's user groups must be allowed by a FortiGate firewall policy.

Answer: AD

Explanation:

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

NEW QUESTION 100

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 105

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

- A. A process crash.
- B. Configuration changes.
- C. Changes in the status of any of the FortiGuard licenses.

D. System entering to and leaving from the proxy conserve mode.

Answer: AD

Explanation:

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

NEW QUESTION 110

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

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

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

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

Answer: D

NEW QUESTION 113

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 117

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

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

Raring Statistics:

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

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

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

Cache Statistics:

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

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

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

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

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

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

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

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

Answer: C

NEW QUESTION 121

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 126

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 130

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

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443 (172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545 (192.167.1.100:49545)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

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

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

Answer: A

Explanation:

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

NEW QUESTION 134

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 137

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

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

Answer: BC

Explanation:

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

NEW QUESTION 142

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

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

Answer: BC

NEW QUESTION 144

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

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

Answer: CDE

Explanation:

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

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

NEW QUESTION 149

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 153

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 157

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 161

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 165

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 169

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

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

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

Total number of neighbors 3
```

What can be concluded about the router in this scenario?

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

Answer: D

NEW QUESTION 171

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

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

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

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

Answer: AC

Explanation:

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

NEW QUESTION 173

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 176

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

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

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



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

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

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

Answer: D

Explanation:

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

NEW QUESTION 179

Which of the following statements are correct regarding application layer test commands? (Choose two.)

- A. They are used to filter real-time debugs.
- B. They display real-time application debugs.
- C. Some of them display statistics and configuration information about a feature or process.
- D. Some of them can be used to restart an application.

Answer: CD

Explanation:

Application layer test commands don't display info in real time, but they do show statistics and configuration info about a feature or process. You can also use some of these commands to restart a process or execute a change in its operation.

NEW QUESTION 182

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 183

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

```
# diagnose debug rating
Locale      : English
License     : Contract
Expiration  : Thu Sep 28 17:00:00 20XX
--- Server List (Thu APR 19 10:41:32 20XX) ---
IP          Weight  RTT   Flags  TZ   Packets  Curr Lost  Total Lost
64.26.151.37  10      45    -5     -5   262432   0          846
64.26.151.35  10      46    -5     -5   329072   0          6806
66.117.56.37  10      75    -5     -5   71638    0          275
66.210.95.240 20      71    -8     -8   36875    0          92
209.222.147.36 20      103   DI     -8   34784    0          1070
208.91.112.194 20      107   D      -8   35170    0          1533
96.45.33.65   60      144    0      0    33728    0          120
80.85.69.41   71      226    1      1    33797    0          192
62.209.40.74  150     97     9      9    33754    0          145
121.111.236.179 45      44     F     -5   26410   26226     26227
```

Which statements are true regarding the Weight value?

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

Answer: C

NEW QUESTION 187

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

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

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

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

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

Answer: AC

NEW QUESTION 188

.....

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](#)