Fortinet.NSE7_EFW-7.0.v2023-03-17.q39

Exam Code:	NSE7_EFW-7.0
Exam Name:	Fortinet NSE 7 - Enterprise Firewall 7.0
Certification Provider:	Fortinet
Free Question Number:	39
Version:	v2023-03-17
# of views:	1296
# of Questions views:	390
https://www.exam-tests.com/NSE7_EFW-7.0-exam/Fortinet.NSE7_EFW-7.0.v2023-03-17.q39.html	

NEW QUESTION: 1
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. Policy monitor.
B. Logs.
C. Firewall monitor.
D. Crashlogs.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 2
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. IP headers.
B. IP payload.
C. Port names.
D. Ethernet headers.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 3
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 indentifier 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 has received the BGP prefixed from the remote peer.

B. The TCP session for the BGP connection to 10.200.3.1 is down.

C. The local peer is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.

D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

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 AESCBC and authentication to SHA2.

C. Change phase 1 encryption to AES256 and authentication to SHA256.

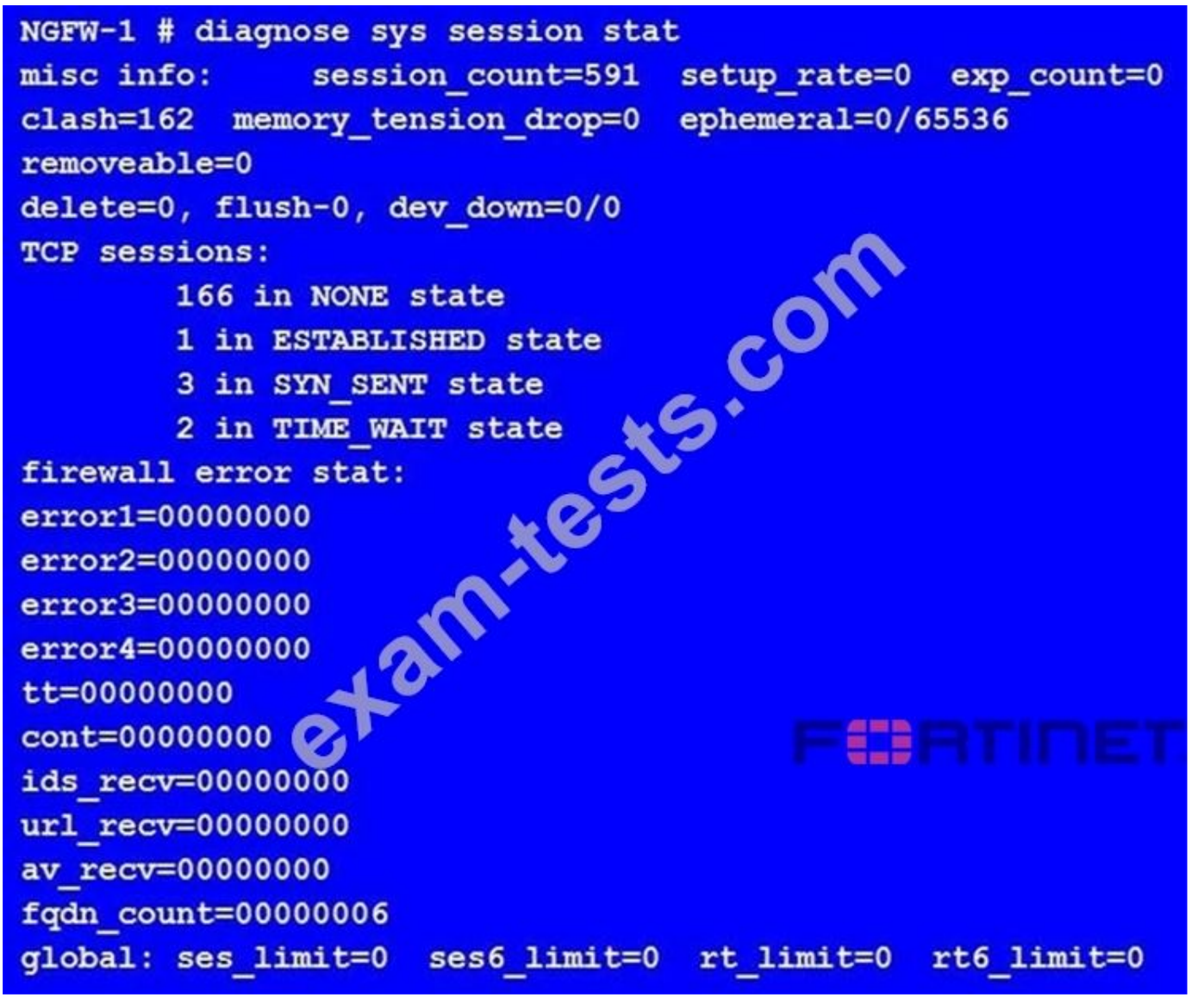
D. Change phase 1 encryption to AES128 and authentication to SHA512.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
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 entries in the NAT port table has been reached.
C. FortiGate does not have any available NAT port for a new connection.
D. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
Which of the following statements are correct regarding application layer test commands? (Choose two.)
A. Some of them can be used to restart an application.
B. Some of them display statistics and configuration information about a feature or process.
C. They display real-time application debugs.
D. They are used to filter real-time debugs.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
View the exhibit, which contains the output of diagnose sys session stat, and then answer the question below.



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: A,C (LEAVE A REPLY)

NEW QUESTION: 8

Refer to the exhibit, which shows a session entry .

Which statement about this session is true?

A. It is an ICMP session from 10.1.10.10 to 10.200.5. 1.

B. It is a TCP session in close_wait state, from 10. l. 10.10 to 10.200.1.1.

C. It is a TCP session in the established state, from 10.1.10.10 to 10.200.5.1.

D. It is an ICMP session from 10.1.10.10 to 10.200.1.1.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 9

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

Which statement about the exhibit is true?

A. Since the counters were last reset, the 10.200.3.1 peer has never been down.

B. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

C. The local router has not established a TCP session with 100.64.3.1.

D. The local router has received a total of three BGP prefixes from all peers.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 10

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

A. To disable the IPS engine

B. To provide information regarding IPS sessions

C. To enable IPS bypass mode

D. To restart all IPS engines and monitors

Answer: D (LEAVE A REPLY)

NEW QUESTION: 11

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

A. When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.

B. When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.

C. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

D. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

Answer: (SHOW ANSWER)

NEW QUESTION: 12

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

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

Neighbor        V    AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.125.0.60     4 65060     1698     1756     103    0     0 03:02:49            1
10.127.0.75     4 65075     2206     2250     102    0     0 02:45:55            1
10.200.3.1      4 65501      101      115       0    0     0 never              Active

Total number of neighbors 3
```

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

A. Local BGP peer has not received an OpenConfirm from 10.200.3.1.

B. The local BGP peer has received a total of 3 BGP prefixes.

C. BGP peer 10.200.3.1 has never been down since the BGP counters were cleared.

D. BGP state of the peer 10.125.0.60 is Established.

Answer: (SHOW ANSWER)

NEW QUESTION: 13

An administrator wants to capture ESP traffic between two FortiGates using the built-in sniffer.

If the administrator knows that there is no NAT device located between both FortiGates, what command should the administrator execute?

A. diagnose sniffer packet any 'udp port 500 or udp port 4500'

B. diagnose sniffer packet any 'esp'

C. diagnose sniffer packet any 'udp port 500'

D. diagnose sniffer packet any 'udp port 4500'

Answer: B (LEAVE A REPLY)

NEW QUESTION: 14

Which two statements about OCVPN are true? (Choose two.)

A. Only root vdom supports OCVPN.

B. OCVPN offers only Hub-Spoke VPNs.

C. OCVPN supports static and dynamic IPs in WAN interface.

D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Answer: (SHOW ANSWER)

NEW QUESTION: 15

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

A. There is no other route, to the same destination, with a higher distance.

B. The next-hop IP address is up.

C. The outgoing interface is up.

D. The link health monitor (if configured) is up.

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 16

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

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

A. Servers with the D flag are considered to be down.

B. Servers with a negative TZ value are experiencing a service outage.

C. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.

D. FortiGate used 209.222.147.3 as the initial server to validate its contract.

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 17

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

Which of the following statements about the exhibit are true? (Choose two.)

A. Port4 is connected to the OSPF backbone area.

B. The local FortiGate's OSPF router ID is 0.0.0.4

C. The local FortiGate has been elected as the OSPF backup designated router.

D. In the network on port4, two OSPF routers are down.

Answer: (SHOW ANSWER)

NEW QUESTION: 18

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

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

A. The Cached value is always the Active value plus the Inactive value

B. The unit is running a 32-bit FortiOS

C. The unit is in kernel conserve mode

D. Kernel indirectly accesses the low memory (LowTotal) through memory paging

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 19

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

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

A. FortiGate applied proxy-based inspection.

B. FortiGate applied explicit proxy-based inspection.

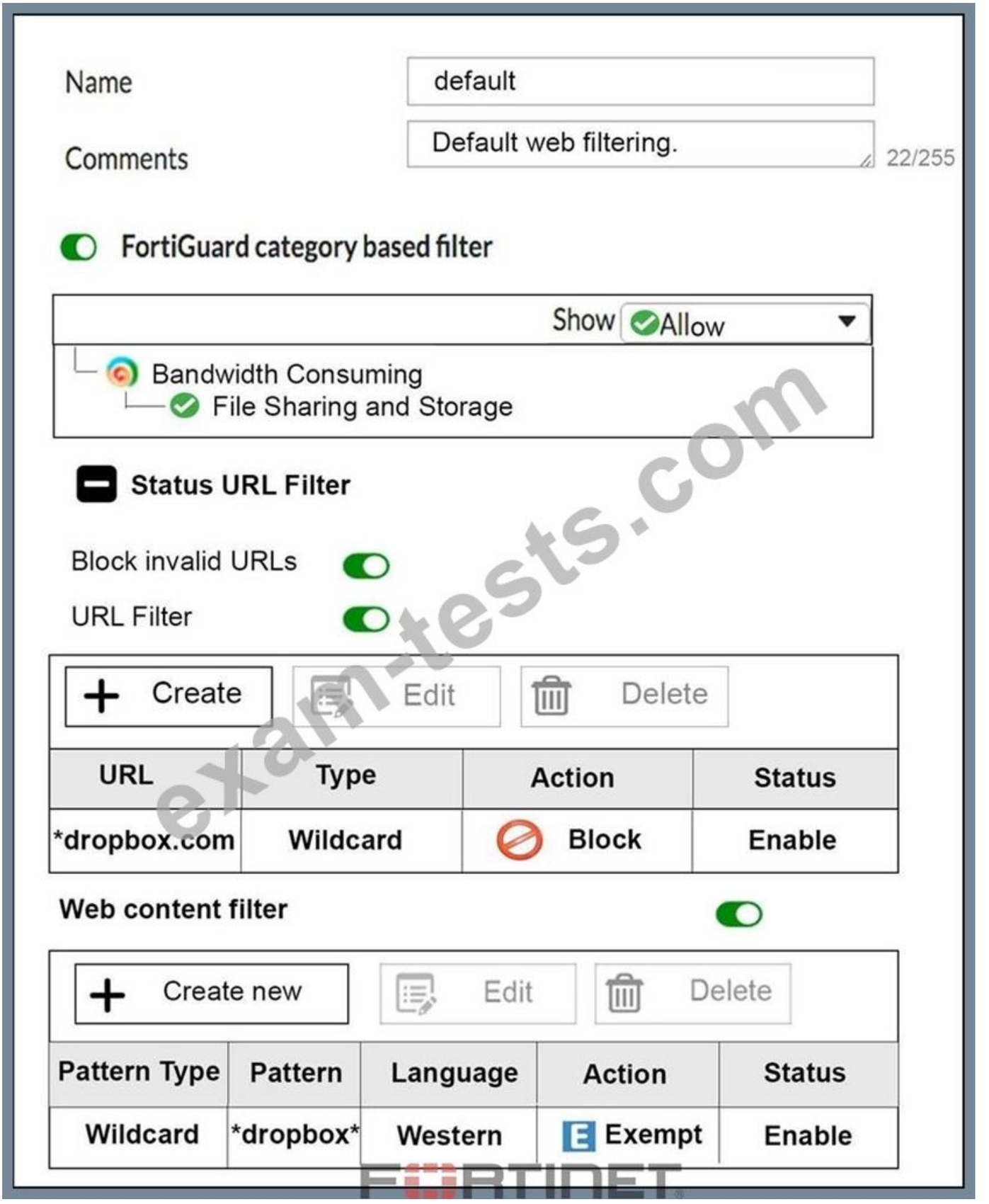
C. FortiGate forwarded this session without any inspection.

D. FortiGate applied flow-based inspection.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 20

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



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 (LEAVE A REPLY)

NEW QUESTION: 21
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 time wait.
B. TCP session time to live.
C. TCP half open.
D. TCP half close.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------------------------------------------
name=VPN ver=1 serial=1 10.200.5.1:0 -> 10.200.4.1:0
bound_if=3 lgwy=statistic/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refernt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
     src: 0:10.1.2.0/255.255.255.0:0
     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=204B seqno=1
esn=replaywin_lastseq=00000000
     life: type=01 bytes=0/0 timeout=43177/43200
     dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
          ah=sha1 key=20 c68091d68753578785de6a7a6b276b506e527
```

Based on the output, which two statements are correct? (Choose two.)
A. Anti-replay is enabled
B. DPD is disabled.
C. Quick mode selectors are disabled.
D. The remote gateway IP is 10.200.4.1.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)
A. A secondary unit is removed from the HA cluster.

B. The FortiGuard license for the primary unit is updated.
C. One of the monitored interfaces in the primary unit is disconnected.
D. Primary unit stops sending HA heartbeat keepalives.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 24
A FortiGate's portl is connected to a private network. Its port2 is connected to the Internet. Explicit web proxy is enabled in port1 and only explicit web proxy users can access the Internet. Web cache is NOT enabled. An internal web proxy user is downloading a file from the Internet via HTTP .
Which statements are true regarding the two entries in the FortiGate session table related with this traffic? (Choose two.)
A. One of the sessions has the IP address of port2 as the source IP address.
B. One session has the proxy flag on, the other one does not.
C. Both session have the local flag on.
D. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 25
View the exhibit, which contains the output of a real-time debug, Which statement about this output is true?

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

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training.fortinet.com:443, id=68, cat=255, vfname='root', vfid=0,
profile='default', type=0, client=10.1.10.1, url_source=1, url="/"
action=9(ftgd-allow) wf-act=5(ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

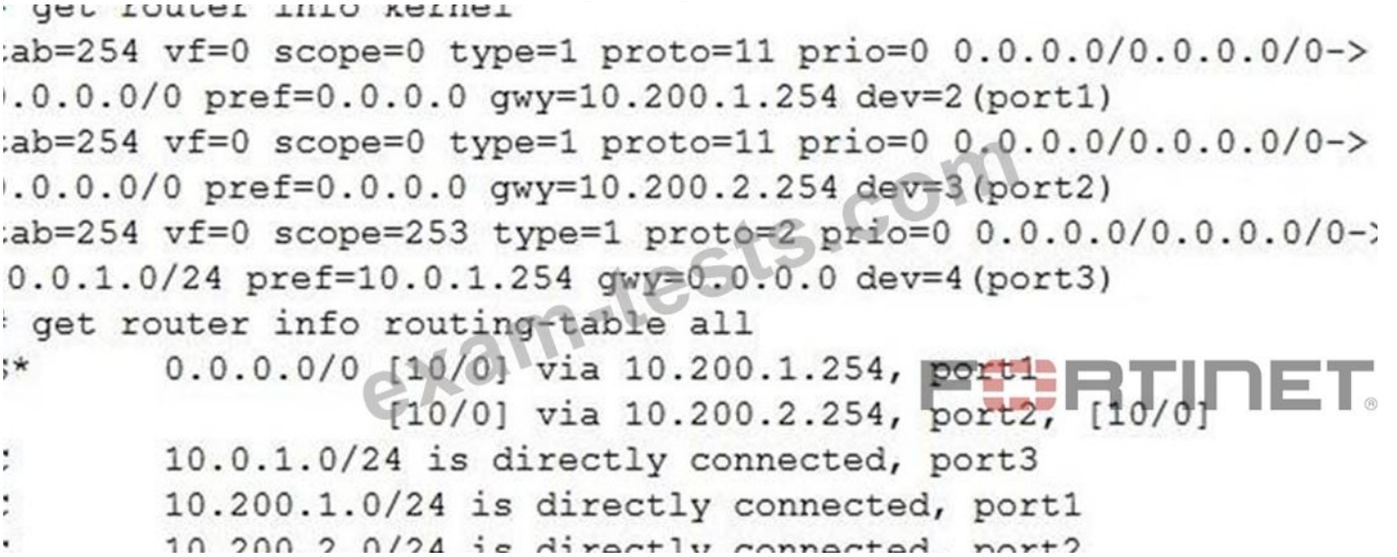
Which of the following statements is true regarding this output?
A. The server hostname Is training, fortinet.com.
B. FortiGate found the requested URL in its local cache.
C. This web request was inspected using the ftgd-allow web filler profile.
D. The requested URL belongs to category ID 255.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
What configuration changes can reduce the memory utilization in a FortiGate? (Choose two.)
A. Increase the FortiGuard cache time to live.
B. Reduce the maximum file size to inspect.
C. Reduce the session time to live.
D. Increase the TCP session timers.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 27

View these partial outputs from two routing debug commands:



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

A. Both port1 and port2

B. port2

C. port3

D. port1

Answer: (SHOW ANSWER)

NEW QUESTION: 28

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

A. Diagnose debug application fnbamd -1.

B. Diagnose radius console -log enable.

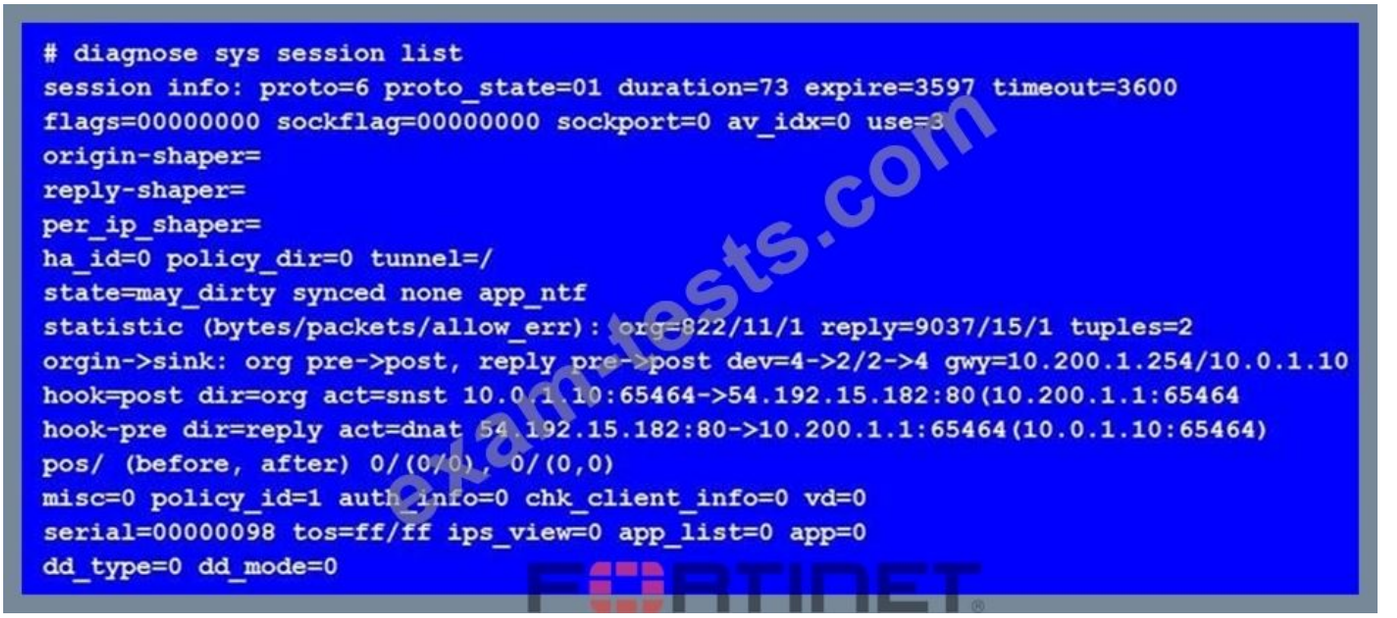
C. Diagnose debug application radius -1.

D. Diagnose authd console -log enable.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 29

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



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

A. This session is for HA heartbeat traffic.

B. This session cannot be synced with the slave unit.

C. This session is synced with the slave unit.

D. The inspection of this session has been offloaded to the slave unit.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 30

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

A. Add devices to FortiManager.

B. Preview pending configuration changes for managed devices.

C. Import interface mappings from managed devices.

D. Install configuration changes to managed devices.

E. Import policy packages from managed devices.

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 31

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

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

A. Source IP address 10.72.3.52, Destination IP address 10.1.0.254.

B. Source IP address 10.72.3.27, Destination IP address 10.1.0.52.

C. Source IP address 10.73.9.10, Destination IP address 10.72.3.15.

D. Source IP address 10.1.0.24, Destination IP address 10.72.3.20.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 32

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

A. BDR is responsible for forwarding link state information from one router to another.

B. Only the DR receives link state information from non-DR routers.

C. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.

D. FortiGate first checks the OSPF ID to elect a DR.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

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


Based on the output, which two statements are correct? (Choose two.)
A. Anti-replay is disabled.
B. Hub2Spoke1 is configured on interface wan2.
C. Phase 2 authentication is set to sha1 on both sides.
D. Hub2Spoke1 is a policy-based VPN.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 34
What is the purpose of an internal segmentation firewall (ISFW)?
A. It splits the network into multiple security segments to minimize the impact of breaches.
B. It is the first line of defense at the network perimeter.
C. It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.
D. It inspects incoming traffic to protect services in the corporate DMZ.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 35
Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

Which statement are true regarding the output in the exhibit? (Choose two.)
A. The TZ value represents the delta between each FortiGuard server's time zone and the FortiGate's time zone.
B. FortiGate will send the FortiGuard queries to the server with highest weight.
C. There are three FortiGuard servers that are not responding to the queries sent by the FortiGate.
D. A server's round trip delay (RTT) is not used to calculate its weight.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 36
Which statement about NGFW policy-based application filtering is true?
A. The IPS security profile is the only security option you can apply to the security policy with the action set to ACCEPT.
B. After IPS identifies the application, it adds an entry to a dynamic ISDB table.
C. After the application has been identified, the kernel uses only the Layer 4 header to match the traffic.
D. FortiGate will drop all packets until the application can be identified.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
Examine the following partial output from a sniffer command; then answer the question below.

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

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

A. Number of packets that matched the sniffer filter but could not be captured by the sniffer.

B. Number of packets that didn't match the sniffer filter.

C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.

D. Number of total packets dropped by the FortiGate.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 38

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 65
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS   MsgRcvd MsgSent   TblVe
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 TCP session to 10.200.3.1 has not completed the three-way handshake.

B. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.

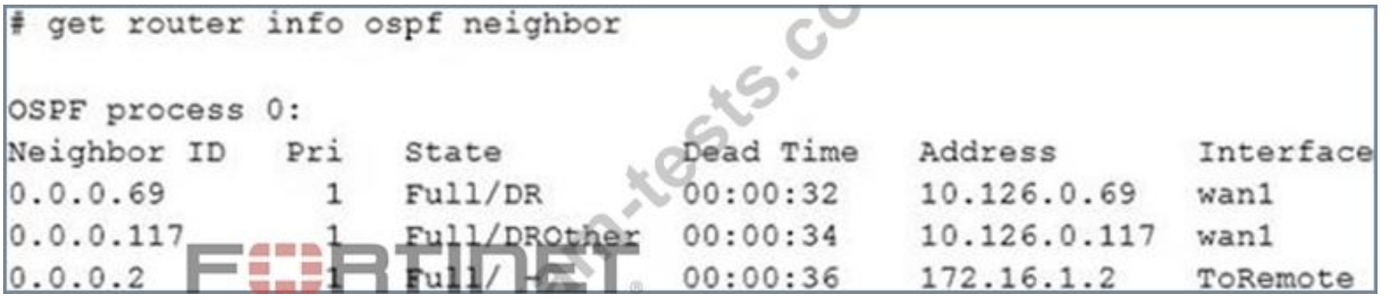
C. The local router has received the BGP prefixes from the remote peer.

D. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 39

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



```
# get router info ospf neighbor

OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.0.69          1   Full/DR         00:00:32    10.126.0.69     wan1
0.0.0.117         1   Full/DROther    00:00:34    10.126.0.117    wan1
0.0.0.2           1   Full/-          00:00:36    172.16.1.2      ToRemote
```

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

Which statement about the output is true?

A. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.

B. The local FortiGate is the designated router for the wan1 network.

C. The interface ToRemote is a point-to-point OSPF network.

D. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the war. l network.

Answer: C (LEAVE A REPLY)