

Exam Questions NSE7_EFW-6.4

Fortinet NSE 7 - Enterprise Firewall 6.4

https://www.2passeasy.com/dumps/NSE7_EFW-6.4/



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. Firewall monitor.
- B. Policy monitor.
- C. Logs.
- D. Crashlogs.

Answer: CD

NEW QUESTION 2

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

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

SHM FS alloc: 7110656

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

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

Answer: AC

NEW QUESTION 3

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 didn't match the sniffer filter.
- B. Number of total packets dropped by the FortiGate.
- C. Number of packets that matched the sniffer filter and were dropped by the FortiGate.

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

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=11655>

NEW QUESTION 4

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

- A. When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.
- 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 All FortiGate in ADOM, changes are automatically installed without creating a new revision history.
- D. When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

Answer: BD

Explanation:

CLI scripts can be run in three different ways: Device Database: By default, a script is executed on the device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard.

Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard.

Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don't need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.

NEW QUESTION 5

Examine the following partial outputs from two routing debug commands; then answer the question below:

```
#get router info routing-table database
S      0.0.0.0/. [20/0] via 10.200.2.254, port2, [10/0]
S      *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
# get router info routing-table all
S*     0.0.0.0/0 [10/0] via 10.200.1.254, port1
```

Why the default route using port2 is not displayed in the output of the second command?

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

Answer: C

Explanation:

<http://kb.fortinet.com/kb/viewContent.do?externalId=FD32103>

NEW QUESTION 6

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

Which statement about this setting is true?

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

Answer: D

NEW QUESTION 7

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

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

Answer: B

NEW QUESTION 8

Examine the output from the 'diagnose vpn tunnel list' command shown in the exhibit; then answer the question below.


```
#diagnose vpn tunnel list
name=Dial Up_0 ver=1 serial=5 10.200.1.1:4500->10.200.3.2: 64916 lgwy=static
nun=intf mode=dial_inst.bound if=2
parent=DialUp index=0
proxyid_um=1 child_num=0 refcnt=8 ilast=4 olast=4
stat: rxp=104 txp=8 rxb=27392 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 segno=70
natt: mode=silent draft=32 interval= 10 remote_port=64916
proxyid= DialUp proto=0 sa=1 ref=2 serial=1 add-route
src: 0:0.0.0.0.-255.255.255.255:0
dst: 0:10.0.10.10.-10.0.10.10:0
SA: ref=3 options= 00000086 type=00 soft=0 mtu=1422 expire =42521
replaywin=2048 seqno=9
life: type=01 bytes=0/0 timeout= 43185/43200
dec: spi=cb3a632a esp=aes key=16 7365e17a8fd555ec38bffa47d650c1a2
ah=sha1 key=20 946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
enc: spi=da6d28ac esp=aes key=16 3dcf44ac7c816782ea3d0c9a977ef543
ah=sha1 key=20 7cfde587592fc4635ab8db8ddf0d851d868b243f
dec:pkts/bytes=104/19926, enc:pkts/bytes=8/1024
```

Which command can be used to sniffer the ESP traffic for the VPN DialUP_0?

- A. diagnose sniffer packet any 'port 500'
- B. diagnose sniffer packet any 'esp'
- C. diagnose sniffer packet any 'host 10.0.10.10'
- D. diagnose sniffer packet any 'port 4500'

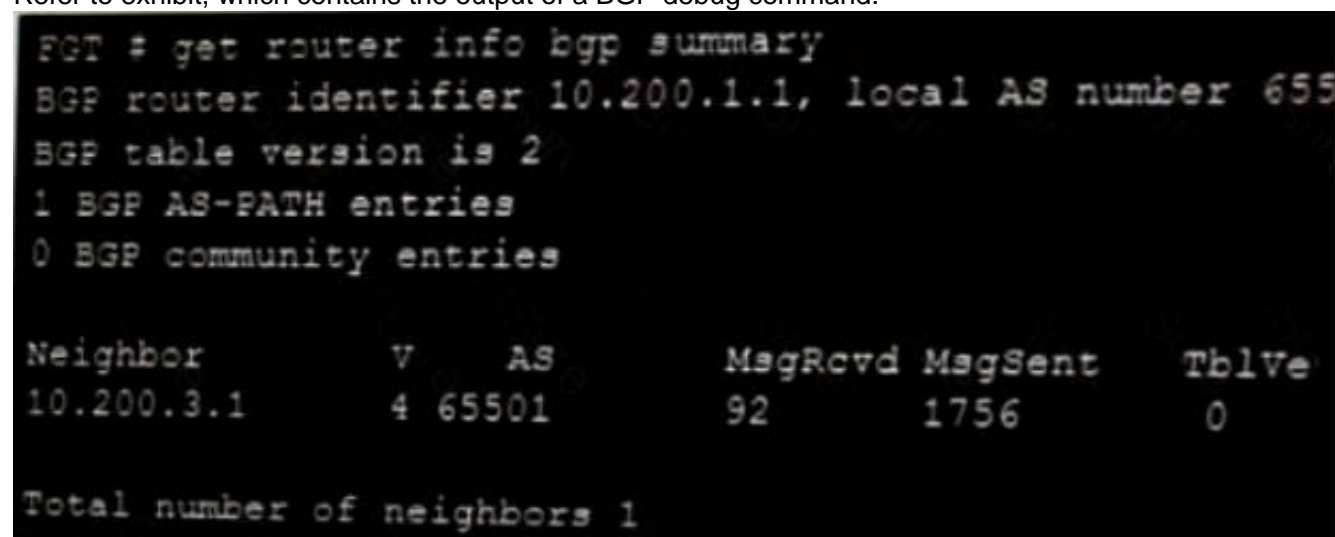
Answer: D

Explanation:

NAT-T is enabled. natt: mode=silentProtocol ESP is used. ESP is encapsulated in UDP port 4500 when NAT-T is enabled.

NEW QUESTION 9

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



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

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

Total number of neighbors 1
```

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

- A. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.
- B. The TCP session to 10.200.3.1 has not completed the 3-way handshake.
- C. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.
- D. The local router has received the BGP prefixes from the remote peer.

Answer: B

Explanation:

BGP neighbor states and how they change:

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

NEW QUESTION 10

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

- A. To enable IPS bypass mode
- B. To provide information regarding IPS sessions
- C. To disable the IPS engine
- D. To restart all IPS engines and monitors

Answer: D

NEW QUESTION 10

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: C

NEW QUESTION 11

What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

- A. av-failopen
- B. mem-failopen
- C. utm-failopen
- D. ips-failopen

Answer: A

Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Other_Profile_Consideratio

NEW QUESTION 13

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

Name	Remote
Comments	Comments
Network	
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Remote Gateway	Static IP Address <input checked="" type="checkbox"/>
IP Address	10.0.10.1
Interface	port1 <input checked="" type="checkbox"/>
Mode Config	<input type="checkbox"/>
NAT Traversal	<input checked="" type="checkbox"/>
Keepalive Frequency	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 17

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 19

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

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

Answer: B

NEW QUESTION 23

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

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

What statement is correct about this FortiGate?

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

Answer: D

NEW QUESTION 26

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 28

Examine the partial output from two web filter debug commands; then answer the question below:

```
# diagnose test application urlfilter 3
Domain | IP      DB Ver  T URL
34000000| 34000000  16.40224 P Bhttp://www.fgt99.com/
# get webfilter categories
g07 General Interest - Business:
  34 Finance and Banking
  37 Search Engines and Portals
  43 General Organizations
  49 Business
  50 Information and Computer Security
  51 Government and Legal Organizations
  52 Information Technology
```

Based on the above outputs, which is the FortiGuard web filter category for the web site www.fgt99.com?

- A. Finance and banking
- B. General organization.
- C. Business.
- D. Information technology.

Answer: C

NEW QUESTION 32

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

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

Answer: B

NEW QUESTION 35

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

```
# diagnose ips anomaly list

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

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

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

Answer: A

NEW QUESTION 36

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 38

In which two states is a given session categorized as ephemeral? (Choose two.)

- A. A TCP session waiting to complete the three-way handshake.
- B. A TCP session waiting for FIN ACK.
- C. A UDP session with packets sent and received.
- D. A UDP session with only one packet received.

Answer: BC

NEW QUESTION 43

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

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

Which statement is correct regarding this session?

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

Answer: B

NEW QUESTION 48

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 53

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

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000 ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
src: 0:10.1.2.0/255.255.0:0
dst: 0:10.1.1.0/255.255.255.0:0
SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
life: type=01 bytes=0/0 timeout=43177/43200
dec: spi=ccclf66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
ah=shal key=20 c68091d68753578785de6a7a6b276b506c527efe
enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
ah=shal key=20 889f7529887c215c25950be2ba83e6fela5367be
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

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

Answer: A

NEW QUESTION 55

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

```
FGT # get router info ospf interface port4
port4 is up, line protocol is up
  Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
  Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 4, Adjacent neighbor count is 2
  Crypt Sequence Number is 411
  Hello received 106 send 27, DD received 6 sent 3
  LS-Req received 2 sent 2, LS-Upd received 7 sent 17
  LS-Ack received 4 sent 3, Discarded 1
```

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

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

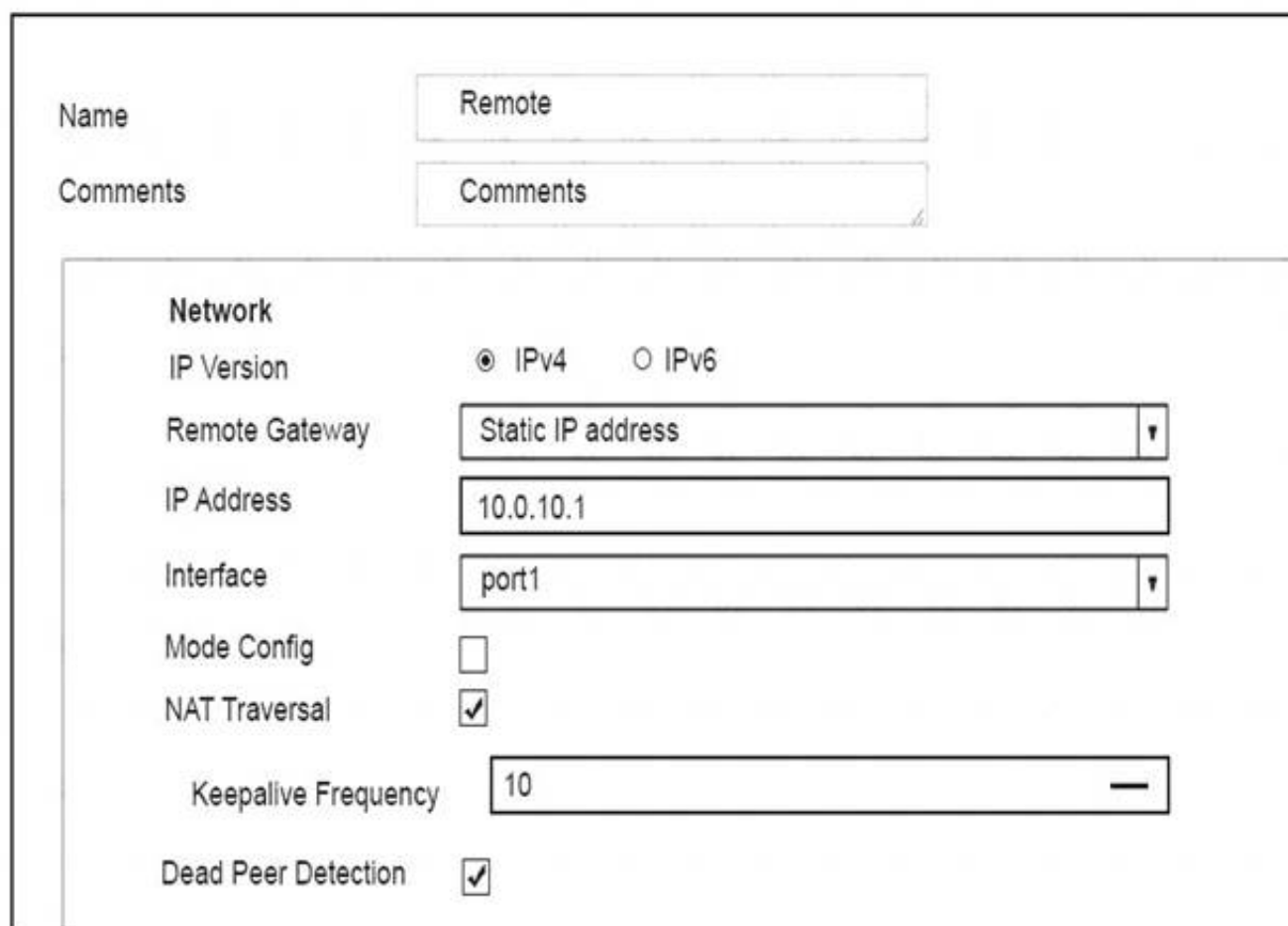
Answer: AB

Explanation:

Area 0.0.0.0 is the backbone area.

NEW QUESTION 56

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



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

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

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

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

Answer: B

NEW QUESTION 58

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 fssolist' 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 62

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 65

Refer to the exhibit, which shows a FortiGate configuration.

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

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

What must the administrator change to fix the issue?

- A. The administrator must increase webfilter-timeout.
- B. The administrator must disable webfilter-force-off.
- C. The administrator must change protocol to TCP.
- D. The administrator must enable fortiguard-anycast.

Answer: D

NEW QUESTION 66

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_EFW-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_EFW-6.4 Product From:

https://www.2passeasy.com/dumps/NSE7_EFW-6.4/

Money Back Guarantee

NSE7_EFW-6.4 Practice Exam Features:

- * NSE7_EFW-6.4 Questions and Answers Updated Frequently
- * NSE7_EFW-6.4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE7_EFW-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE7_EFW-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year