Fortinet

Exam Questions NSE7_EFW-7.0

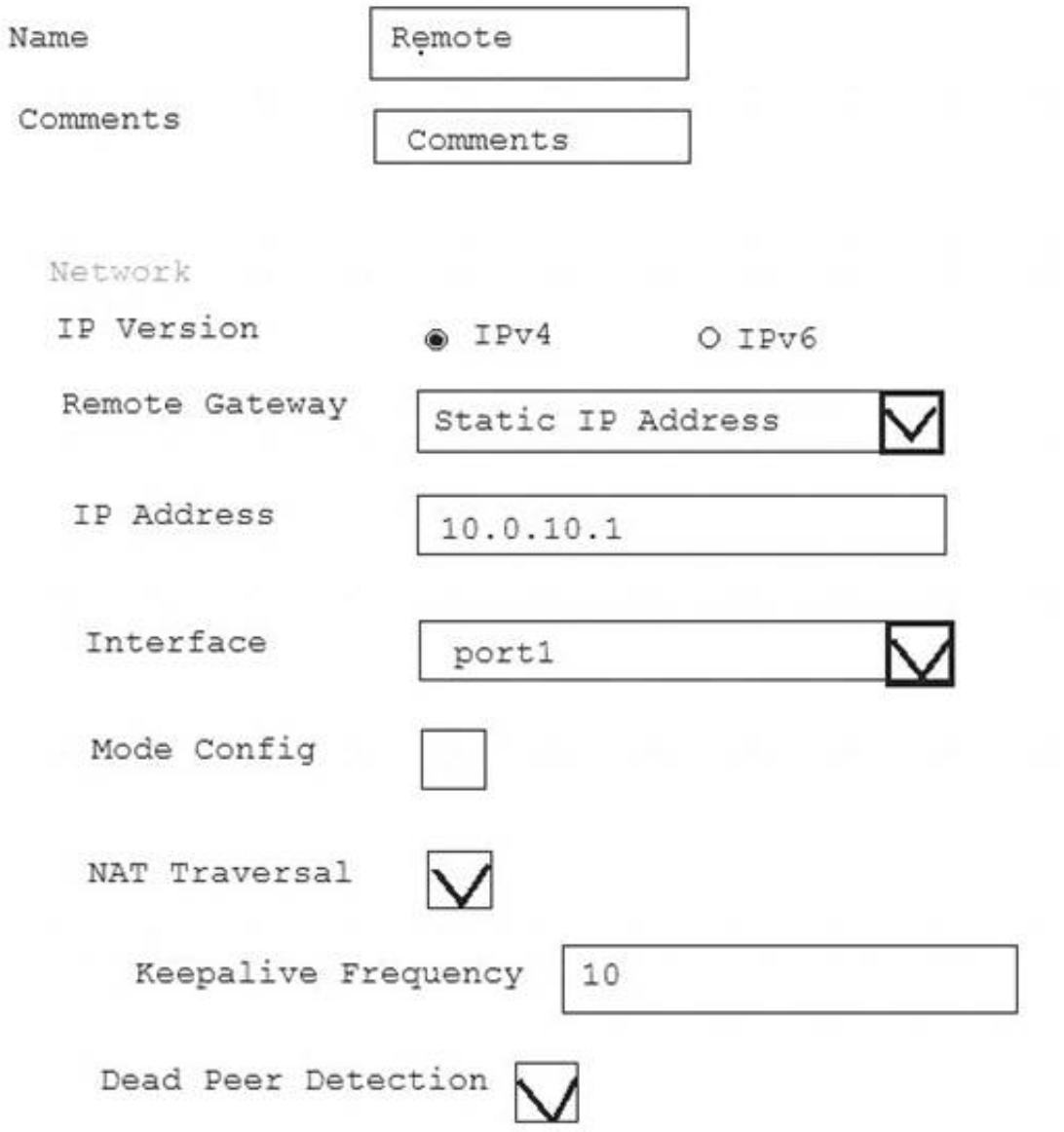
Fortinet NSE 7 - Enterprise Firewall 7.0

NEW QUESTION 1
Examine the following partial outputs from two routing debug commands; then answer the question below.
# get router info kernel
tab=254 vf=0 scope=0type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254 dev=2(port1)
tab=254 vf=0 scope=0type=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=10.200.2.254 dev=3(port2)
tab=254 vf=0 scope=253type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/.->10.0.1.0/24 pref=10.0.1.254
gwy=0.0.0.0 dev=4(port3)
# get router info routing-table all s*0.0.0.0/0 [10/0] via 10.200.1.254, portl [10/0] via 10.200.2.254, port2, [10/0] dO.0.1.0/24 is directly connected, port3
dO.200.1.0/24 is directly connected, portl d0.200.2.0/24 is directly connected, port2
Which outbound interface or interfaces will be used by this FortiGate to route web traffic from internal users to the Internet?

A. port!
B. port2.
C. Both portl and port2.
D. port3.

Answer: B

NEW QUESTION 2
Examine the IPsec configuration shown in the exhibit; then answer the question below.



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
Refer to the exhibit, which contains 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
```

Which statement about the exhibit is true?

A. The local router has received a total of three BGP prefixes from all peers.
B. The local router has not established a TCP session with 100.64.3.1.
C. Since the counters were last reset, the 10.200.3.1 peer has never been down.
D. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

Answer: B

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 A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A078E09026CA8B2
ike 0:Remotesite:3: out A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000005C64D5CBA90B873F150CB8B5CC2A
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
How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

A. FortiManager can download and maintain local copies of FortiGuard databases.
B. FortiManager supports only FortiGuard push to managed devices.
C. FortiManager will respond to update requests only if they originate from a managed device.
D. FortiManager does not support rating requests.

Answer: A

NEW QUESTION 6
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 7
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 8
View the IPS exit log, and then answer the question below.
# diagnose test application ipsmonitor 3 ipsengine exit log”
pid = 93 (cfg), duration = 5605322 (s) at Wed Apr 19 09:57:26 2017 code = 11, reason: manual
What is the status of IPS on this FortiGate?

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

Answer: D

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

NEW QUESTION 9
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:253000:27: responder: main mode get 1st message...
ike 0:253000:27: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:253000:27: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:253000:27: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:253000:27: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:253000:27: incoming proposal:
ike 0:253000:27: proposal id = 0:
ike 0:253000:27:   protocol id = ISAKMP:
ike 0:253000:27:      trans_id = KEY_IKE.
ike 0:253000:27:      encapsulation = IKE/none
ike 0:253000:27:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:253000:27:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:253000:27:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:253000:27:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: my proposal, gw Remotesite:
ike 0:253000:27: proposal id = 1:
ike 0:253000:27:   protocol id = ISAKMP:
ike 0:253000:27:      trans_id = KEY_IKE.
ike 0:253000:27:      encapsulation = IKE/none
ike 0:253000:27:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:253000:27:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:253000:27:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:253000:27:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:253000:27: ISAKMP SA lifetime=86400
ike 0:253000:27: negotiation failure
ike Negot:253a8cbe6335e6fd/0000000000000000:27: no SA proposal chosen
```

Why did the tunnel not come up?

A. The local gateway has configured less secure encryption and hashing algorithms compared to the remote gateway.
B. The Diffie-Hellman group does not match on the local and remote gateways.
C. The proposal ID does not match between local and remote gateways.
D. The encapsulation method for phase 2 is set to none on local and remote gateways.

Answer: A

Explanation:
local gateway: encryption AES-128, hash SHA remote gateway: encryption AES-256, hash SHA-256 So local gateway has less secure settings

NEW QUESTION 10
Which two statements about OCVPN are true? (Choose two.)

A. Only root vdom supports OCVPN.
B. OCVPN supports static and dynamic IPs in WAN interface.
C. OCVPN offers only Hub-Spoke VPNs.
D. FortiGate devices under different FortiCare accounts can be used to form OCVPN.

Answer: AB

NEW QUESTION 10
Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx  packets: 1025  bytes: 524402  errors: 0
  tx  packets: 641  bytes: 93  errors: 0
  dpd: on-demand/negotiated  idle: 20000ms  retry: 3  count: 0
  selectors
    name: 'Hub2Spoke1'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
    SA
      lifetime/rekey: 43200/32137
      mtu: 1438
      tx-esp-seq: 2ce
      replay: enabled
      inbound
        spi: 01e54b14
        enc:  aes-cb  914dc5d092667ed436ea7f6efb867976
        auth:   sha1  a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
      outbound
        spi: 3dd3545f
        enc:  aes-cb  017b8ff6c4ba21eac99b22380b7de74d
        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 12
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 dont' need to
create a full mesh IBGP network. All clients in a cluster only talck 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 17
Refer to the exhibit, which shows a session entry. Which statement about this session is true?

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout
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 tup
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.
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.1
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
```

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.
C. 10.10 to 10.200.1.1.
D. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
E. It is a TCP session in the established state, from 10.1.10.10 to 10.200.5.1.

Answer: A

Explanation:
https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/1969

NEW QUESTION 21
Which statement is true regarding File description (FD) conserve mode?

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

Answer: B

NEW QUESTION 24
Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

A. Only the DR receives link state information from non-DR routers.
B. Non-DR and non-BDR routers form full adjacencies to DR only.
C. Non-DR and non-BDR routers send link state updates and acknowledgements to 224.0.0.6.
D. FortiGate first checks the OSPF ID to elect a DR.

Answer: C

Explanation:
Some special IP multicast addresses are reserved for OSPF: 224.0.0.5: All OSPF routers must be able to transmit and listen to this address. 224.0.0.6: All DR and BDR routers must be able to transmit and listen to this address. https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

NEW QUESTION 29
Refer to the exhibit, which shows the output of a web filtering diagnose command.

```
# diagnose webfilter fortiguard statistics list
Rating Statistics:
==================
DNS failures                  :        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 request 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 configuration change would result in non-zero results in the cache statistics section?

A. set server-type rating under config system central-management
B. set webfilter-cache enable under config system fortiguard
C. set webfilter-force-off disable under config system fortiguard
D. set ngfw-mode policy-based under config system settings

Answer: B

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 362

NEW QUESTION 31
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 32
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. TheOSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wa
B. l network.
C. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.
D. The local FortiGate is the designated router for the wan1 network.
E. The interface ToRemote is a point-to-point OSPF network.

Answer: D

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

NEW QUESTION 33
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 37
Which two tasks are automated using the Install Wizard on FortiManager? (Choose two.)

A. Preview pending configuration changes for managed devices.
B. Add devices to FortiManager.
C. Import policy packages from managed devices.
D. Install configuration changes to managed devices.
E. Import interface mappings from managed devices.

Answer: AD

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/1200_ins
There are 4 main wizards:Add Device: is used to add devices to central management and import their configurations.
Install: is used to install configuration changes from Device Manager or Policies & Objects to the managed devices. It allows you to preview the changes and, if the administrator doesn't agree with the changes, cancel and modify them.

Import policy: is used to import interface mapping, policy database, and objects associated with the managed devices into a policy package under the Policy & Object tab. It runs with the Add Device wizard by default and may be run at any time from the managed device list.
Re-install policy: is used to perform a quick install of the policy package. It doesn't give the ability to preview the changes that will be installed to the managed device.

NEW QUESTION 39
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 41
What does the dirty flag mean in a FortiGate session configured for NGFW policy mode?

A. The existing session table entry has been updated with the app_id and the firewall policy table needs to be checked for a match.
B. The application or URL category is unknown and needs to be rescanned by the IPS engine to try to identify the Layer 7 details.
C. The URL category for this session has been updated by FortiGuard and the session needs to be checked against the policy again to ensure proper web filtering is applied.
D. Traffic has been identified as coming from an application that is not allowed and the relevant replacement message needs to be displayed to the user, if configured.

Answer: A

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 99

NEW QUESTION 43
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=nntp 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 45
View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

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

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

Total number of neighbors 3
```

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

A. For the peer 10.125.0.60, the BGP state of is Established.
B. The local BGP peer has received a total of three BGP prefixes.
C. Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.
D. The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

Answer: AD

NEW QUESTION 47
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 52
Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
iike 0:620000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:      trans_id = KEY_IKE.
ike 0:624000:98:      encapsulation = IKE/none
ike 0:624000:98:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

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

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

Answer: D

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

NEW QUESTION 55
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 56
Refer to the exhibit, which shows the output of a debug command.

```
FGT # 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    wan2
0.0.0.2           1   Full/ -         00:00:38      172.16.1.2      ToRemote
```

What can be concluded from the debug command output?

A. The OSPF router with the ID 0.0.0.69 has its OSPF priority set to 0.
B. The local FortiGate has a different MTU value from the OSPF router with ID 0.0.0.2, based on the state information.
C. There are more than two OSPF routers on the wan2 network.
D. The interface ToRemote is a broadcast OSPF network.

Answer: C

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 296

NEW QUESTION 59
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 60
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 65
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-miltipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

TheBGP 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 70
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 71
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 73
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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