Fortinet

Exam Questions NSE7_EFW-7.0

Fortinet NSE 7 - Enterprise Firewall 7.0

NEW QUESTION 1
An administrator has configured the following CLI script on FortiManager, which failed to apply any changes to the managed device after being executed.

```
# conf rout stat
#    edit 0
#        set gateway 10.20.121.2
#        set priority 20
#        set device "wan1"
#    next
# end
```

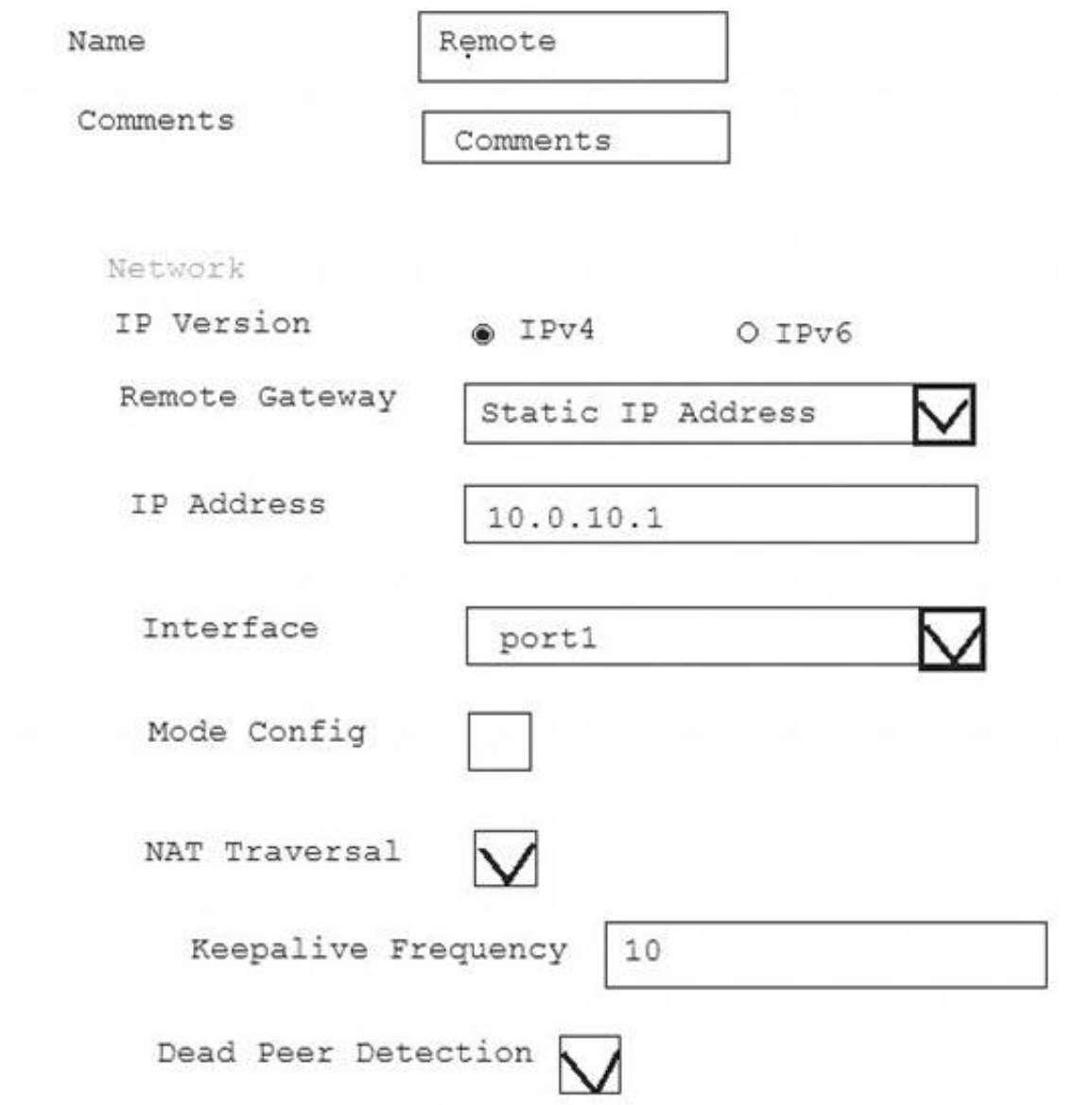
Why didn't the script make any changes to the managed device?

A. Commands that start with the # sign are not executed.
B. CLI scripts will add objects only if they are referenced by policies.
C. Incomplete commands are ignored in CLI scripts.
D. Static routes can only be added using TCL scripts.

Answer: A

Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc
A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

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



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

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

Answer: B

NEW QUESTION 3
Which two configuration settings change the behavior for content-inspected traffic while FortiGate is in conserve mode? (Choose two.)

A. IPS failopen
B. mem failopen
C. AV failopen
D. UTM failopen

Answer: AC

NEW QUESTION 4
Refer to the exhibit, which shows a central management configuration.

```
config system central-management
    set type fortimanager
    set fmg "10.0.1.242"
    config server-list
        edit 1
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.240
        next
        edit 2
            set server-type update
            set addr-type ipv4
            set server-address 10.0.1.243
        next
        edit 3
            set server-type rating
            set addr-type ipv4
            set server-address 10.0.1.244
        next
    end
    set include-default-servers enable
end
```

Which server will FortiGate choose for web filter rating requests, if 10.0.1.240 is experiencing an outage?

A. Public FortiGuard servers
B. 10.0.1.243
C. 10.0.1.242
D. 10.0.1.244

Answer: D

Explanation:
by default,(include-default-servers) enabled .this allows fortigate to communicate with the public fortiguard servers , if the fortimanger devices (configured in server-list) are unavailable .

NEW QUESTION 5
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 6
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 7
View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

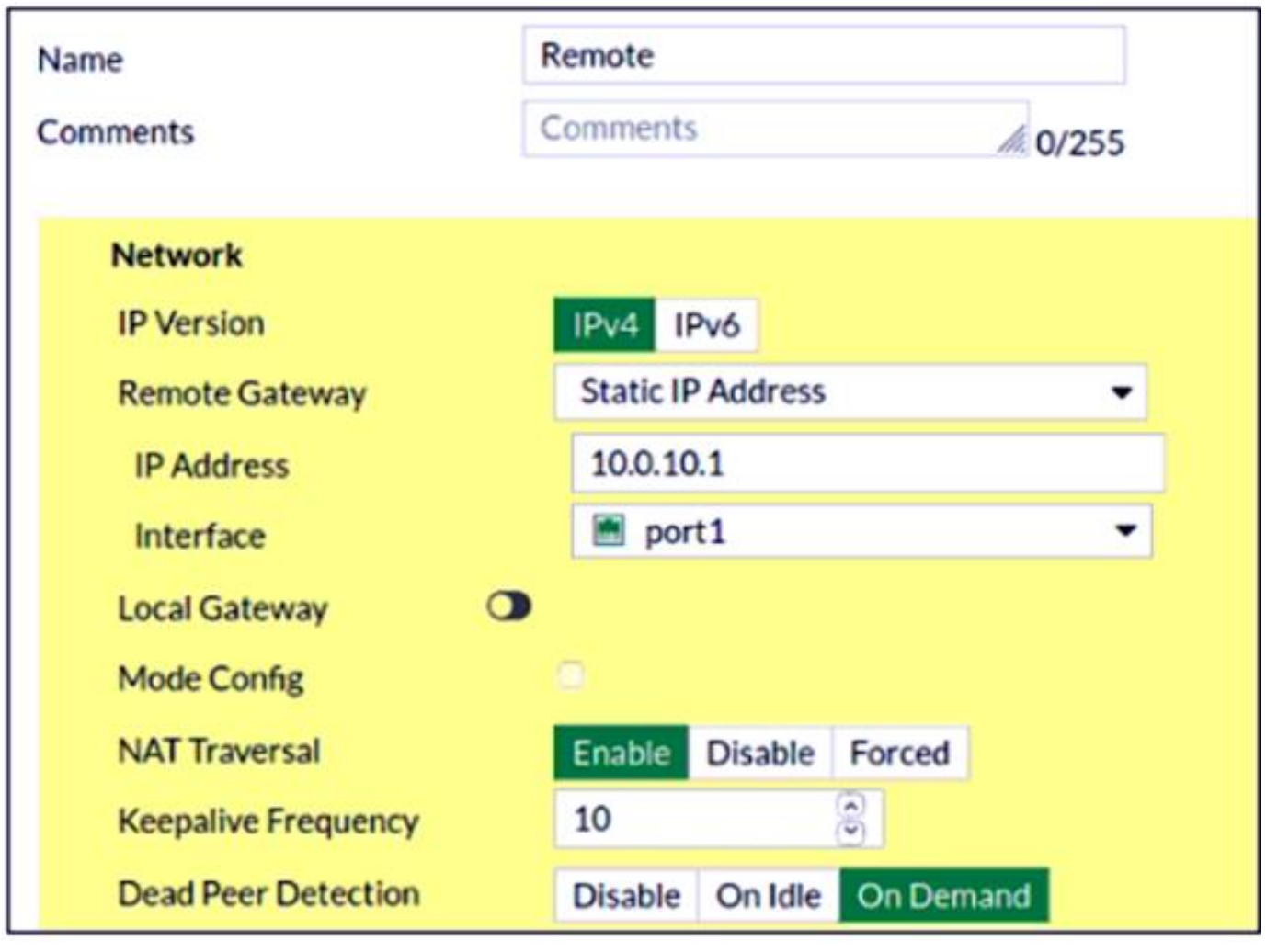
```
ike 0: comes 10.0.0.2:500-> 10.0.0.1:500, ifindex-7...
ike 0: IKEV1 exchange-Aggressive id-baf47d0988e9237f/2f405ef3952f6fda len 430
ike 0: in
BAF47D0988E9237F2F405EF3952F6FDA01100400000000000000001AE0400003C000000010000000100000030010100
ike 0: RemoteSite:4: initiator: aggressive mode get 1st response
ike 0: RemoteSite:4: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0: RemoteSite:4: VID DPD AFCAD71368A1F1c96B8696FC77570100
ike 0: RemoteSite:4: VID FORTIGATE 8299031757A36082C6A621DE000502D7
ike 0: RemoteSite:4: peer is FortiGate/FortiOS (v6 b932)
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: RemoteSite:4: received peer identifier FQDN 'remote'
ike 0: RemoteSite:4: negotiation result
ike 0: RemoteSite:4: proposal id = 1:
ike 0: RemoteSite:4:    protocol id - ISAKMP:
ike 0: RemoteSite:4:         trans_id - KEY_IKE.
ike 0: RemoteSite:4:         encapsulation - IKE/none
ike 0: RemoteSite:4:              type=OAKLEY_ENCRYPT_ALG,  val=AES_CBC, key-len=128
ike 0: RemoteSite:4:              type=OAKLEY_HASH_ALG, val-SHA
ike 0: RemoteSite:4:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: RemoteSite:4:              type=OAKLEY_GROUP, val=MODP1024.
ike 0: RemoteSite:4: ISAKMP SA lifetime=86400
ike 0: RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key
16:B25B6C9384D8BDB24E3DA3DC90CF5E73
ike 0: RemoteSite:4: PSK authentication succeeded
ike 0: RemoteSite:4: authentication OK
ike 0: RemoteSite:4: add INITIAL-CONTACT
ike 0: RemoteSite:4: enc
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000000801400001B1F2E48BFD8E9D603F
ike 0: RemoteSite:4: out
BAF47D0988E9237F2F405EF3952F6FDA08100401000000000000008c2E3FC9BA061816A396F009A12
ike 0: RemoteSite:4: sent IKE msg (agg_12send) : 10.0.0.1:500 ->10.0.0.2:500, len-140, id-
baf47d0988e9237f/2
ike 0: RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda
```

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

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

Answer: BD

NEW QUESTION 8
Refer to the exhibit, which contains a screenshot of some phase 1 settings.



The VPN is not up. To diagnose the issue, the administrator enters the following CLI commands to an SSH session on FortiGate: diagnose vpn ike log-filter dst-addr4 10.0.10.1 diagnose debug application ike -1
However, the IKE real-time debug does not show any output. Why?

A. The administrator must also run the command diagnose debug enable.
B. The administrator must enable the following real-time debug: diagnose debug application ipsec -1.
C. The log-filter setting is incorrec
D. The VPN traffic does not match this filter.
E. The debug shows only error message
F. If there is no output, then the phase 1 and phase 2 configurations match.

Answer: A

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-IPSec-VPN-Diagnostics-Possible-reasons/ta-p/1920

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

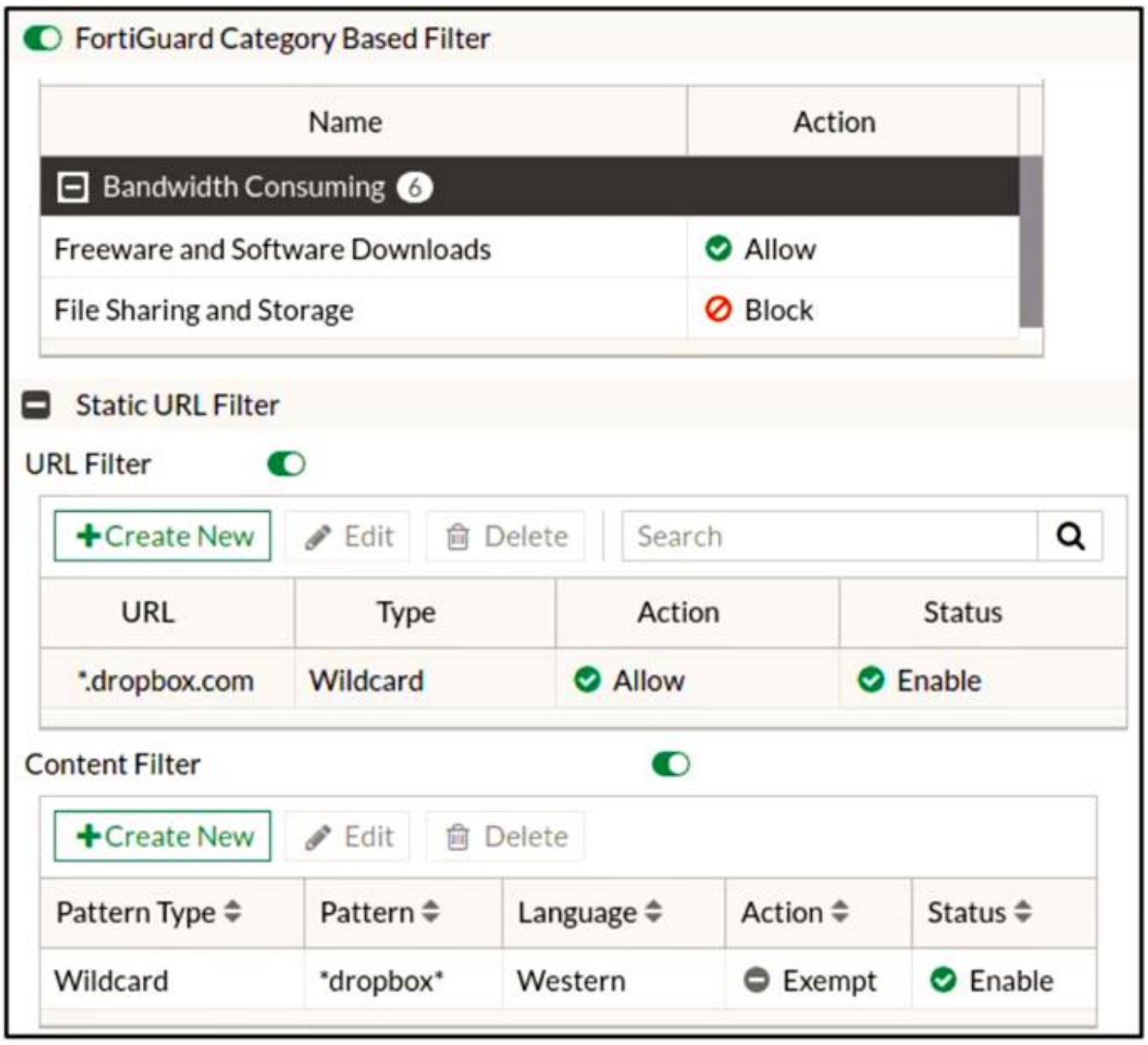
```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7. . . .
ike 0: IKEv2 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response. . .
ike 0: Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated
ike 0: Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: received peer identifier FQDN 'remote'
ike 0: Remotesite:3: negotiation result
ike 0: Remotesite:3: proposal id = 1:
ike 0: Remotesite:3:    protocol id = ISAKMP:
ike 0: Remotesite:3:         trans_id = KEY_IKE.
ike 0: Remotesite:3:         encapsulation = IKE/none.
ike 0: Remotesite:3:              type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: Remotesite:3:              type=OAKLEY_HASH_ALG, val=SHA.
ike 0: Remotesite:3:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: Remotesite:3:              type=OAKLEY_GROUP, val=MODP1024.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key
16:39915120ED73ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000000500B000018882A07BE09026CA8B2
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 remote gateway IP address is 10.0.0.1.
B. The initiator provided remote as its IPsec peer ID.
C. It shows a phase 1 negotiation.
D. The negotiation is using AES128 encryption with CBC hash.

Answer: BC

NEW QUESTION 10
Refer to the exhibit, which shows a partial web filter profile configuration.



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 block the connection, based on the FortiGuard category based filter configuration.
B. FortiGate will block the connection as an invalid URL.
C. FortiGate will exempt the connection, based on the Web Content Filter configuration.
D. FortiGate will allow the connection, based on the URL Filter configuration.

Answer: A

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 351 url filter -> FortiGuard Web Filter -> Web Content Filter -> Advanced Filter Options Allow -> Block

NEW QUESTION 10
Which two statements about the Security Fabric are true? (Choose two.)

A. Only the root FortiGate collects network information and forwards it to FortiAnalyzer.
B. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.
C. All FortiGate devices in the Security Fabric must have bidirectional FortiTelemetry connectivity.
D. Branch FortiGate devices must be configured first.

Answer: BC

NEW QUESTION 11
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 14
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 16
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 17
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 20
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 21
An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.

```
#   debug application fnbamd -1
#   diagnose debug enable
#   diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 5 for student in WindowsLDAP opt=27 prot=0
fnbamd_fsm.c[336] __compose_group_list_from_req-Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server
'WindowsLDAP'
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_auth_session-Total 1 server(s) to try
fnbamd_ldap.c[437] start_search_dn-base:'cn=user,dc=trainingAD,dc=training,dc=lab'
filter:cn=student
fnbamd_ldap.c[1730] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[2407] auth_ldap_result-Continue pending for req 5
fnbamd_ldap.c[480] get_all_dn-Found no DN
fnbamd_ldap.c[503] start_next_dn_bind-No more DN left
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 5
fnbamd_fsm.c[568] destroy_auth_session-delete session 5
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the output in the exhibit, what can cause this authentication problem?

A. User student is not found in the LDAP server.
B. User student is using a wrong password.
C. The FortiGate has been configured with the wrong password for the LDAP administrator.
D. The FortiGate has been configured with the wrong authentication schema.

Answer: A

NEW QUESTION 26
Which statement about protocol options is true?

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

Answer: D

NEW QUESTION 29
What is the diagnose test application ipsmenitor 5 command used for?

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

Answer: A

Explanation:
diagnose test application ipsmonitor 5: Toggle bypass status
* 13: IPS session list
* 98: Stop all IPS engines
* 99: Restart all IPS engines and monitor

NEW QUESTION 30
Refer to the exhibit, which contains the output of diagnose sys session list.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic(bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80(100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464(10.0.1.10:65464)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

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

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

Answer: C

NEW QUESTION 35
Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spoke1'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx  packets: 1025  bytes: 524402  errors: 0
  tx  packets: 641  bytes: 93  errors: 0
  dpd: on-demand/negotiated  idle: 20000ms  retry: 3  count: 0
  selectors
    name: 'Hub2Spoke1'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
    SA
      lifetime/rekey: 43200/32137
      mtu: 1438
      tx-esp-seq: 2ce
      replay: enabled
      inbound
        spi: 01e54b14
        enc:  aes-cb  914dc5d092667ed436ea7f6efb867976
        auth:   sha1  a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
      outbound
        spi: 3dd3545f
        enc:  aes-cb  017b8ff6c4ba21eac99b22380b7de74d
        auth:   sha1  edd8141f4956140eef703d9042621d3dbf5cd961
      NPU acceleration: encryption(outbound) decryption(inbound)
```

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

A. The npu_flag for this tunnel is 03.
B. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.
C. Anti-replay is enabled.
D. The npu_flag for this tunnel is 02.

Answer: AC

NEW QUESTION 36
An administrator added the following Ipsec VPN to a FortiGate configuration:
configvpn ipsec phasel -interface edit "RemoteSite"
set type dynamic
set interface "portl"
set mode main
set psksecret ENC LCVkCiK2E2PhVUzZe next
end
config vpn ipsec phase2-interface edit "RemoteSite"
set phasel name "RemoteSite" set proposal 3des-sha256
next end
However, the phase 1 negotiation is failing. The administrator executed the IKF real time debug while attempting the Ipsec connection. The output is shown in the exhibit.

```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=716
ike 0:xxx/xxx:16: responder: main mode get 1st message...
...
ike 0:xxx/xxx:16: negotiation result
ike 0:xxx/xxx:16: proposal id = 1:
ike 0:xxx/xxx:16:   protocol id = ISAKMP:
ike 0:xxx/xxx:16:       trans_id = KEY_IKE.
ike 0:xxx/xxx:16:       encapsulation = IKE/none
ike 0:xxx/xxx:16:           type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:xxx/xxx:16:           type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:xxx/xxx:16:           type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:xxx/xxx:16:           type=OAKLEY_GROUP, val=MODP2048.
ike 0:xxx/xxx:16: ISAKMP SA lifetime=86400
ike 0:xxx/xxx:16: SA proposal chosen, matched gateway DialUpUsers
...
ike 0:DialUpUsers:16: sent IKE msg (ident_r1send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
```

```
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=380
ike 0:DialUpUsers:16: responder:main mode get 2nd message...
ike 0:DialUpUsers:16: NAT not detected
ike 0:DialUpUsers:16: sent IKE msg (ident_r2send): 10.200.1.1:500->10.200.3.1:500, len
id=xxx/xxx
ike 0:DialUpUsers:16: ISAKMP SA xxx/xxx key 16:3D33E2EF00BE927701B5C25B05A62415
ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=xxx/xxx len=108
ike 0:DialUpUsers:16: responder: main mode get 3rd message...
ike 0:DialUpUsers:16: probable pre-shared secret mismatch
ike 0:DialUpUsers:16: unable to parse msg
```

What is causing the IPsec problem in the phase 1 ?

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

Answer: C

NEW QUESTION 38
View the global IPS configuration, and then answer the question below.

```
config ips global
    set fail-open disable
    set intelligent-mode disable
    set engine-count 0
    set algorithm engine-pick
end
```

Which of the following statements is true regarding this configuration?

A. IPS will scan every byte in every session.
B. FortiGate will spawn IPS engine instances based on the system load.
C. New packets will be passed through without inspection if the IPS socket buffer runs out of memory.

D. IPS will use the faster matching algorithm which is only available for units with more than 4 GB memory.

Answer: A

NEW QUESTION 42
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. Both session have the local flag on.
B. The destination IP addresses of both sessions are IP addresses assigned to FortiGate's interfaces.
C. One session has the proxy flag on, the other one does not.
D. One of the sessions has the IP address of port2 as the source IP address.

Answer: AD

NEW QUESTION 45
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 47
Examine the output of the 'diagnose debug rating' command shown in the exhibit; then answer the question below.

```
# diagnose debug rating
Locale       : english
License      : Contract
Expiration   : Wed Mar 27 17:00:00 20xx
-=- Server List (Mon Apr 16 15:32:55 20xx) -=-
IP                Weight   RTT   Flags   TZ   Packets   Curr Lost   Total Los
69.195.205.101    10       45             -5   262432    0           846
69.195.205.102    10       46             -5   329072    0           6806
209.222.147.43    10       75             -5   71638     0           275
96.45.33.65       20       71             -8   36875     0           92
208.91.112.196    20       103    DI      -8   34784     0           1070
208.91.112.198    20       107    D       -8   35170     0           1533
80.85.69.41       60       144            0    33728     0           120
62.209.40.73      71       226            1    33797     0           192
121.111.236.180   150      197            9    33754     0           145
69.195.205.103    45       44     F       -5   26410     26226       26227
```

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

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

Answer: BC

NEW QUESTION 51
Examine the following traffic log; then answer the question below.

date-20xx-02-01 time=19:52:01 devname=master device_id="xxxxxxx" log_id=0100020007 type=event subtype=system pri critical vd=root service=kemel status=failure msg="NAT port is exhausted."
What does the log mean?

A. There is not enough available memory in the system to create a new entry in the NAT port table.
B. The limit for the maximum number of simultaneous sessions sharing the same NAT port has been reached.
C. FortiGate does not have any available NAT port for a new connection.
D. The limit for the maximum number of entries in the NAT port table has been reached.

Answer: B

NEW QUESTION 56
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# diagnose hardware sysinfo conserve
memory conserve mode:                on
total RAM:                        3040 MB
memory used:                      2706 MB 89% of total RAM
Memory freeable:                   334 MB 11% of total RAM
memory used + freeable threshold extreme:  2887 MB 95% of total RAM
memory used threshold red:        2675 MB 88% of total RAM
memory used threshold green:      2492 MB 82% of total RAM
```

Which one of the following statements about this FortiGate is correct?

A. It is currently in system conserve mode because of high CPU usage.
B. It is currently in extreme conserve mode because of high memory usage.
C. It is currently in proxy conserve mode because of high memory usage.
D. It is currently in memory conserve mode because of high memory usage.

Answer: D

NEW QUESTION 59
Refer to the exhibit, which shows a FortiGate configuration.

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

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

A. Increase webfilter-timeout.
B. Change protocol to TCP.
C. Enable fortiguard-anycast.
D. Disable webfilter-force-off.

Answer: D

NEW QUESTION 62
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 63
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 68
Which statement about IKE and IKE NAT-T is true?

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

Answer: C

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

NEW QUESTION 71
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 74
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 is receiving the BGP keepalives from the remote peer but it has not received any BGP prefix yet.
B. The TCP session for the BGP connection to 10.200.3.1 is down.
C. The local peer has received the BGP prefixed from the remote peer.
D. The local peer is receiving the BGP keepalives from the remote peer but it has not received the OpenConfirm yet.

Answer: B

Explanation:
http://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4

NEW QUESTION 76
Which two statements about conserve mode are true? (Choose two.)

A. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
B. FortiGate starts dropping all new sessions when the system memory reaches the configured redthreshold.
C. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
D. FortiGate exits conserve mode when the system memory goes below the configured green threshold.

Answer: AD

NEW QUESTION 78
Examine the output from the 'diagnose debug authd fsso list' command; then answer the question below.
diagnose debug authd fsso list —FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is
NOT the one used by the workstation INTERNAL2. TRAINING. LAB.
What should the administrator check?

A. The IP address recorded in the logon event for the user STUDENT.
B. The DNS name resolution for the workstation name INTERNAL2. TRAININ
C. LAB.
D. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2.TRAININ
E. LAB.
F. The reserve DNS lookup forthe IP address 192.168.3.1.

Answer: C

NEW QUESTION 83
Refer to the exhibit, which shows the output of a diagnose command

```
FGT # diagnose debug rating
Locale       : english
Service      : Web-filter
Status       : Enable
License      : Contract
Service      : Antispam
Status       : Disable
Service      : Virus Outbreak Prevention
Status       : Disable
 -=- Server List (Mon Apr 19 10:41:32 20xx) -=-
IP                   Weight  RTT    Flags   TZ  Packets   Curr Lost     Total Lost
64.26.151.37         10      45             -5   262432    0             846
64.26.151.35         10      46             -5   329072    0             6806
66.117.56.37         10      75             -5   71638     0             275
65.210.95.240        20      71             -8   36875     0             92
209.222.147.36       20      103     DI     -8   34784     0             1070
208.91.112.194       20      107     D      -8   35170     0             1533
96.45.33.65          60      144             0   33728     0             120
80.85.69.41          71      226             1   33797     0             192
62.209.40.74         150     97              9   33754     0             145
121.111.236.179      45      44      F      -5   26410     26226         26227
```

What can you conclude from the RTT value?

A. Its value represents the time it takes to receive a response after a rating request is sent to a particular server.
B. Its value is incremented with each packet lost.
C. It determines which FortiGuard server is used for license validation.
D. Its initial value is statically set to 10.

Answer: A

NEW QUESTION 87
When using the SSL certificate inspection method for HTTPS traffic, how does FortiGate filter web requests when the browser client does not provide the server name indication (SNI) extension?

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

Answer: A

NEW QUESTION 88
Which action will FortiGate take when using the default settings for SSL certificate inspection, where the server name indication (SNI) does not match either the common name (CN) or any of the subject altemative names (SAN) in the server certificate?

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

Answer: A

Explanation:
#Config firewall ssl-ssh-profile
edit <profile_name> config https
set sni-server-cert-check [enable* | strict | disable]
Enable: If the SNI does NOT match the CN or SAN fields in the returned server's certificate, FG uses the CN field instead of the SNI to obtain the FQDN.
Strict: If the SNI does NOT match the CN or SAN fields in the returned server's certificate, FG closes the connection.
Disable: FG does not check the SNI.

NEW QUESTION 91
View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106, sent 27, DD received 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

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

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

Answer: BC

NEW QUESTION 94
The logs in a FSSO collector agent (CA) are showing the following error: failed to connect to registry: PIKA1026 (192.168.12.232)
What can be the reason for this error?

A. The CA cannot resolve the name of the workstation.
B. The FortiGate cannot resolve the name of the workstation.
C. The remote registry service is not running in the workstation 192.168.12.232.
D. The CA cannot reach the FortiGate with the IP address 192.168.12.232.

Answer: C

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD30548

NEW QUESTION 95
A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fsso list' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

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

Answer: AD

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

NEW QUESTION 99
Refer to the exhibit, which contains the partial output of a diagnose command.

```
Spoke-2 # diagnose 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 tun_id=10.200.4.1 dst_mtu=1500 dpd-
link=on remote_location=0.0.0.0 weight=1
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0 options[0210]=create_dev
frag-rfc  accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=10 olast=551 ad=/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=2
  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=10202 type=00 soft=0 mtu=1438 expire=42897/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=5ed4aaf8 esp=aes key=16 20d624b494b1c9bfe61ba9b7522448db
       ah=sha1 key=20 891cd9ba81f0e382de0d44127152cb5dba6c62d1
  enc: spi=3b574759 esp=aes key=16 3abf4e04edc09e4e88709750df9c117d
       ah=sha1 key=20 2d2618e867839866a279af5af70a64fa63a7bb52
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

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

A. The remote gateway has quick mode selectors containing a destination subnet of 10.1.2.0/24.
B. The remote gateway IP is 10.200.5.1.
C. DPD is disabled.
D. Anti-replay is enabled.

Answer: AD

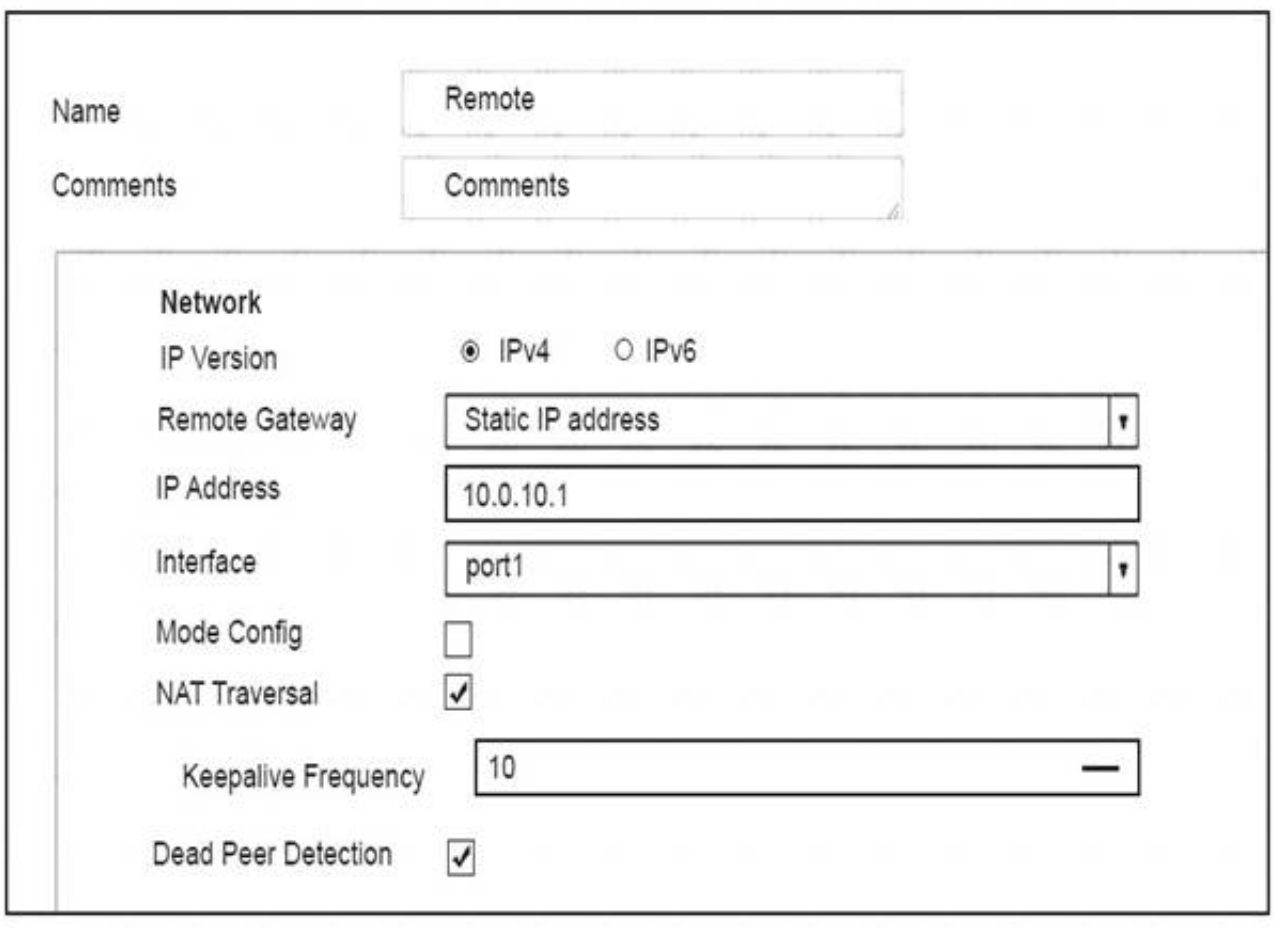
Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 427, 444
Since the local subnet is 10.1.2.0/24, the remote gateway has the destination subnet as 10.1.2.0. The remote gateway IP is 10.200.4.1. DPD is enabled (dpd-link=on)

NEW QUESTION 104
Which statement about memory conserve mode is true?

A. A FortiGate exits conserve mode when the configured memory use threshold reaches yellow.
B. A FortiGate starts dropping all the new and old sessions when the configured memory use threshold reaches extreme.
C. A FortiGate starts dropping new sessions when the configured memory use threshold reaches red
D. A FortiGate enters conserve mode when the configured memory use threshold reaches red

Answer: D

NEW QUESTION 109
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 onl
B. Once the tunnel is up, it does not show any more output.
C. The log-filter setting was set incorrectl
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 onl
H. After that, the administrator must enable the following real time debug: diagnose debug application ipsec -1.

Answer: B

NEW QUESTION 112
Refer to the exhibit, which shows the output of a diagnose command.

```
# diagnose sys session list expectation

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

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

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

Answer: AD

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 110, 111, 115

NEW QUESTION 114
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 117
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 119
Which two statements about the Security Fabric are true? (Choose two.)

A. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer.
B. Only the root FortiGate sends logs to FortiAnalyzer.
C. Only FortiGate devices with fabric-object-unification set to default will receive and synchronize global CMDB objects sent by the root FortiGate.
D. FortiGate uses FortiTelemetry protocol to communicate with FortiAnalyzer.

Answer: AC

Explanation:
FortiGate's to Root uses FortiTelemetry (TCP-8013) FortiTelemetry is also used for FortiClient communication Root Fortigate to FortiAnalyzer uses API (TCP-443)

NEW QUESTION 123
View the exhibit, which contains an entry in the session table, and then answer the question below.

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

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

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

Answer: A

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

NEW QUESTION 127
View these partial outputs from two routing debug commands:

```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.1.254
dev=2(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0 gwy=10.200.2.254
dev=3(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.1.0/24 pref=10.0.1.254 gwy=0.0.0.0
dev=4(port3)
# get router info routing-table all
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1
                 [10/0] via 10.200.2.254, port2, [10/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
```

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

A. Both port1 and port2
B. port3
C. port1
D. port2

Answer: C

NEW QUESTION 130
Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.

Configuration | Session

```
config system global
    set snat-route-change disable
end
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

Configuration | Session

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c5b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

An administrator would like to test session failover between the two service provider connections.
What changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Configure set snat-route-change enable.
B. Change the priority of the port2 static route to 5.
C. Change the priority of the port1 static route to 11.
D. unset snat-route-change to return it to the default setting.

Answer: AC

Explanation:
Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 148-149

NEW QUESTION 132
In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two.)

A. It provides VM license validation services.
B. It supports rating requests from non-FortiGate devices.
C. It caches available firmware updates for unmanaged devices.
D. It can be configured as an update server, a rating server, or both.

Answer: AD

NEW QUESTION 136
Refer to the exhibit, which contains the output of the diagnose vpn tunnel list. Which command will capture ESP traffic for the VPN named DialUp_0?

A. diagnose sniffer packet any ‘esp and host 10.200.3.2’
B. diagnose sniffer packet any ‘ip proto 50’
C. diagnose sniffer packet any ‘host 10.0.10.10’
D. diagnose sniffer packet any ‘port 4500’

Answer: D

NEW QUESTION 138
You have configured FortiManager as a local FDS to provide FortiGate AV and IPS updates, but FortiGate devices are not receiving updates to their AV signature databases, IPS engines, or IPS signature databases.
Which two settings need to be verified for these features to function? (Choose two.)

A. FortiGate needs to have the server list entry for FortiManager set to server-type update under config system central-management.
B. FortiManager needs to be the license validation server for FortiGate devices trying to retrieve updated AV and IPS packages.
C. Service access needs to be enabled on FortiManager under System Settings > Network.
D. FortiGate needs to have include-default-servers disabled under config system central-management.

Answer: AC

Explanation:
NSE 7.0 Guide page 184-185

NEW QUESTION 139
An administrator is running the following sniffer in a FortiGate: diagnose sniffer packet any “host 10.0.2.10” 2
What information is included in the output of the sniffer? (Choose two.)

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

Answer: BC

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

NEW QUESTION 142
View the exhibit, which contains a partial output of an IKE real-time debug, and then answer the question below.

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

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

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

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

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

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

Answer: B

NEW QUESTION 147
Which statement about NGFW policy-based application filtering is true?

A. After the application has been identified, the kernel uses only the Layer 4 header to match the traffic.
B. The IPS security profile is the only security option you can apply to the security policy with the action set to ACCEPT.
C. After IPS identifies the application, it adds an entry to a dynamic ISDB table.
D. FortiGate will drop all packets until the application can be identified.

Answer: D

NEW QUESTION 151
Which two conditions would prevent a static route from being added to the routing table? (Choose two.)

A. There is another other route to the same destination, with a lower distance.
B. The route has a lower priority value than another route to the same destination.
C. The next-hop IP address is unreachable.
D. The interface specified in the route configuration is down

Answer: AD

Explanation:
The routing table contains only the static route with the lowest distance https://community.fortinet.com/t5/FortiGate/Technical-Note-Routing-behavior-depending-on-distance-and/ta-p/

NEW QUESTION 155
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 158
Refer to the exhibit, which shows partial outputs from two routing debug commands.

```
FortiGate # get router info routing-table database

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S    *> 0.0.0.0/0 [10/0] via 100.64.1.254, port1

FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

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

A. The port2 interface is disabled in the FortiGate configuration.
B. The port1 default route has a lower distance than the default route using port2.
C. The port1 default route has a higher priority value than the default route using port2.
D. The port1 default route has a lower priority value than the default route using port2.

Answer: B

NEW QUESTION 160
View the exhibit, which contains the output of get sys ha status, and then answer the question below.

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

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

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

Answer: AD

NEW QUESTION 164
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 166
Refer to the exhibit, which shows the output of a diagnose command.

```
FGT # diagnose debug rating
Locale        : english
Service       : Web-filter
Status        : Enable
License       : Contract
Service       : Antispam
Status        : Disable
Service       : Virus Outbreak Prevention
Status        : Disable
 -=- Server List (Mon Apr 19 10:41:32 20xx) -=-
IP                   Weight  RTT    Flags   TZ  Packets   Curr Lost     Total Lost
64.26.151.37         10      45             -5   262432    0             846
64.26.151.35         10      46             -5   329072    0             6806
66.117.56.37         10      75             -5   71638     0             275
65.210.95.240        20      71             -8   36875     0             92
209.222.147.36       20      103     DI     -8   34784     0             1070
208.91.112.194       20      107     D      -8   35170     0             1533
96.45.33.65          60      144             0   33728     0             120
80.85.69.41          71      226             1   33797     0             192
62.209.40.74         150     97              9   33754     0             145
121.111.236.179      45      44      F      -5   26410     26226         26227
```

What can be concluded about the debug output in this scenario?

A. Servers with a negative TZ value are less preferred for rating requests.
B. There is a natural correlation between the value in the Packets field and the value in the Weight field.
C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
D. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.

Answer: B

NEW QUESTION 167
View the central management configuration shown in the exhibit, and then answer the question below.

```
config system central-management
   set type fortimanager
   set fmg "10.0.1.242"
   config server-list
      edit 1
         set server-type rating
         set server-address 10.0.1.240
      next
      edit 2
         set server-type update
         set server-address 10.0.1.243
      next
      edit 3
         set server-type rating
         set server-address 10.0.1.244
      next
   end
   set include-default-servers enable
end
```

Which server will FortiGate choose for antivirus and IPS updates if 10.0.1.243 is experiencing an outage?

A. 10.0.1.240
B. One of the public FortiGuard distribution servers
C. 10.0.1.244
D. 10.0.1.242

Answer: B

NEW QUESTION 168
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 172
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 173
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 176
.....

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