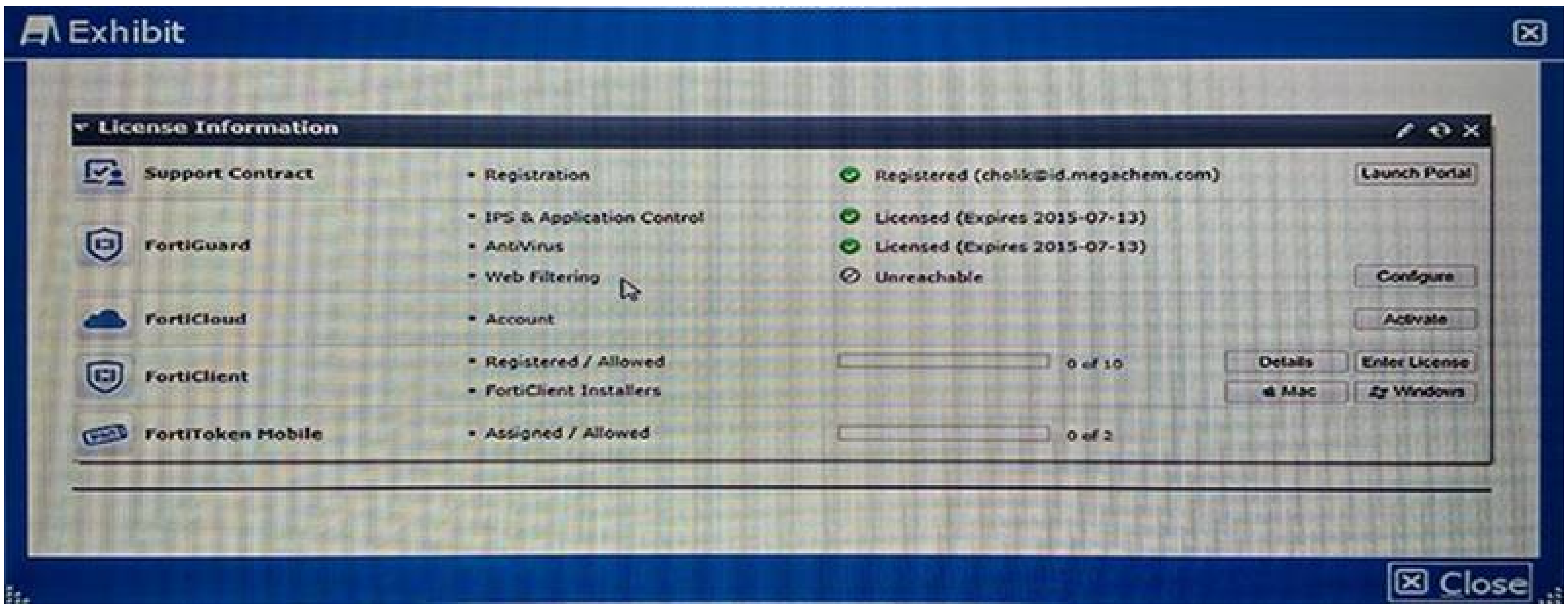
Exam Questions NSE8

NSE8

https://www.2passeasy.com/dumps/NSE8/

NEW QUESTION 1

The dashboard widget indicates that FortiGuard Web Filtering is not reachable. However, AntiVirus, IPS, and Application Control have no problems as shown in the exhibit.



License Information

Support Contract	• Registration	Registered (cholik@id.megachem.com)
FortiGuard	• IPS & Application Control	Licensed (Expires 2015-07-13)
	• AntiVirus	Licensed (Expires 2015-07-13)
	• Web Filtering	Unreachable
FortiCloud	• Account	
FortiClient	• Registered / Allowed	0 of 10
	• FortiClient Installers	
FortiToken Mobile	• Assigned / Allowed	0 of 2

You contacted Fortinet’s customer service and discovered that your FortiGuard Web Filtering contract is still valid for several months.
What are two reasons for this problem? (Choose two.)

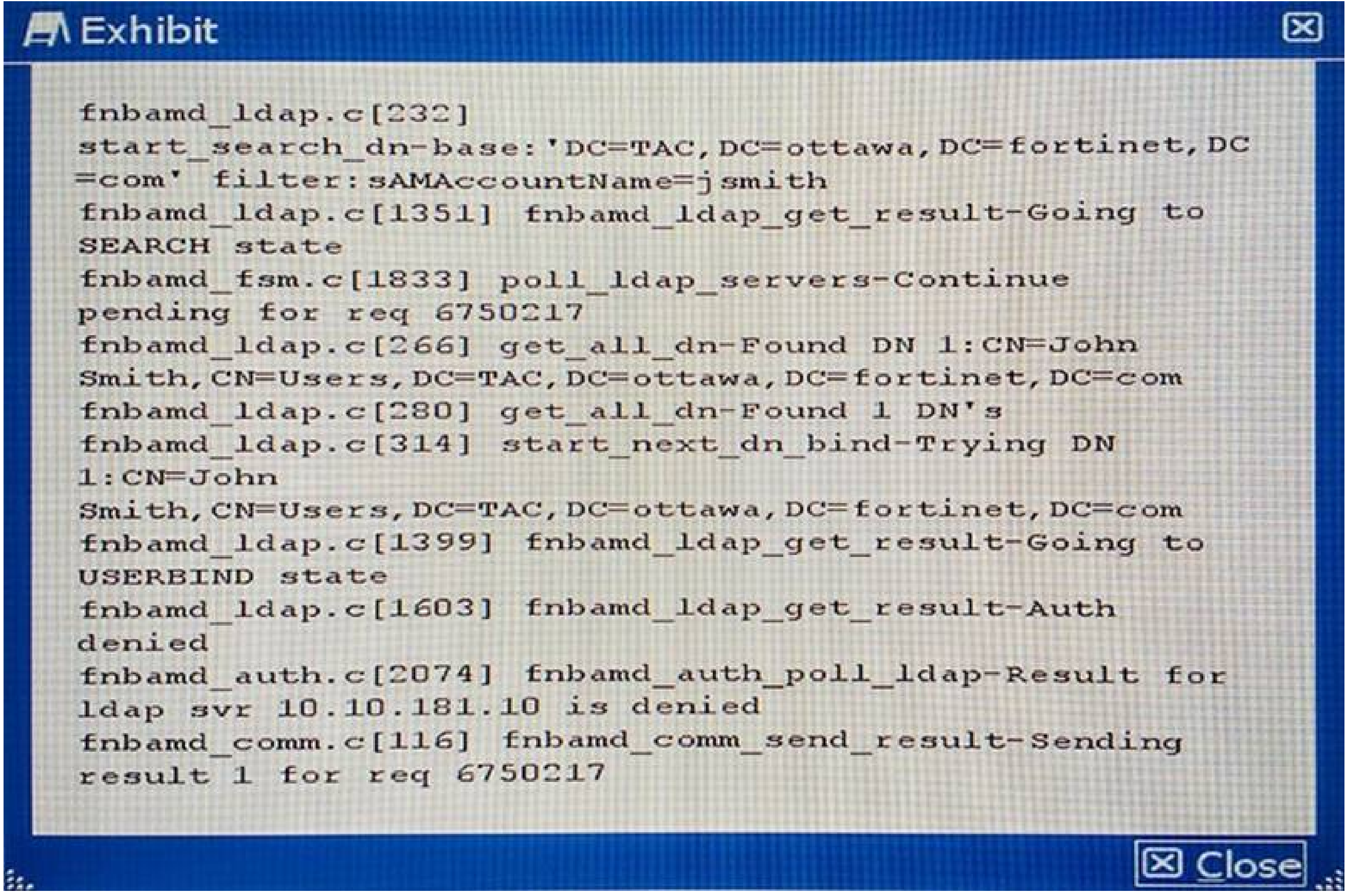
A. You have another security device in front of FortiGate blocking ports 8888 and 53.
B. FortiGuard Web Filtering is not enabled in any firewall policy.
C. You did not enable Web Filtering cache under Web Filtering and E-mail Filtering Options.
D. You have a firewall policy blocking ports 8888 and 53.

Answer: BD

Explanation: If Web filtering shows unreachable then we have to verify, whether web filtering enabled in security policies or not.
Web filtering enabled in a policy but the port 8888 and 53 are not selected, means the policy blocking the ports.
References:

NEW QUESTION 2

A customer is authenticating users using a FortiGate and an external LDAP server. The LDAP user, John Smith, cannot authenticate. The administrator runs the debug command diagnose debug application fnbamd 255 while John Smith attempts the authentication:
Based on the output shown in the exhibit, what is causing the problem?



```
fnbamd_ldap.c[232]
start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC
=com' filter:sAMAccountName=jsmith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to
SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue
pending for req 6750217
fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John
Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
fnbamd_ldap.c[280] get_all_dn-Found 1 DN's
fnbamd_ldap.c[314] start_next_dn_bind-Trying DN
1:CN=John
Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
fnbamd_ldap.c[1399] fnbamd_ldap_get_result-Going to
USERBIND state
fnbamd_ldap.c[1603] fnbamd_ldap_get_result-Auth
denied
fnbamd_auth.c[2074] fnbamd_auth_poll_ldap-Result for
ldap svr 10.10.181.10 is denied
fnbamd_comm.c[116] fnbamd_comm_send_result-Sending
result 1 for req 6750217
```

A. The LDAP administrator password in the FortiGate configuration is incorrect.
B. The user, John Smith, does have an account in the LDAP server.
C. The user, John Smith, does not belong to any allowed user group.
D. The user, John Smith, is using an incorrect password.

Answer: A

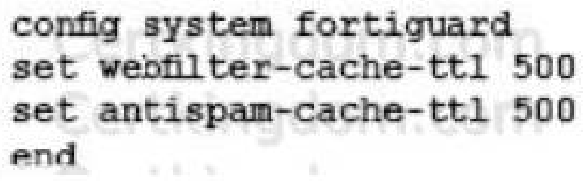
Explanation: Fortigate not binded with LDAP server because of failed authentication. References:

NEW QUESTION 3
You verified that application control is working from previous configured categories. You just added Skype on blocked signatures. However, after applying the profile to your firewall policy, clients running Skype can still connect and use the application.
What are two causes of this problem? (Choose two.)

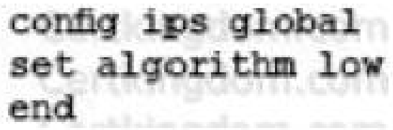
A. The application control database is not updated.
B. SSL inspection is not enabled.
C. A client on the network was already connected to the Skype network and serves as relay prior to configuration changes to block Skype
D. The FakeSkype.botnet signature is included on your application control sensor.

Answer: AB

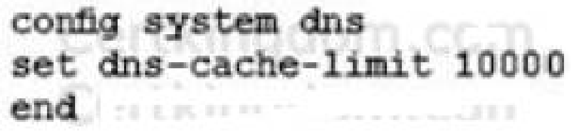
NEW QUESTION 4
You notice that your FortiGate’s memory usage is very high and that the unit’s performance is adversely affected. You want to reduce memory usage.
Which three commands would meet this requirement? (Choose three.)

A.


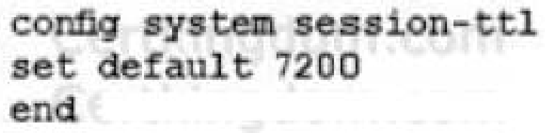
```
config system fortiguard
set webfilter-cache-ttl 500
set antispam-cache-ttl 500
end
```

B.


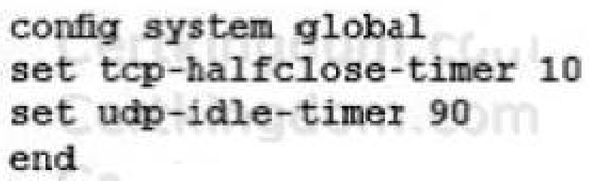
```
config ips global
set algorithm low
end
```

C.


```
config system dns
set dns-cache-limit 10000
end
```

D.


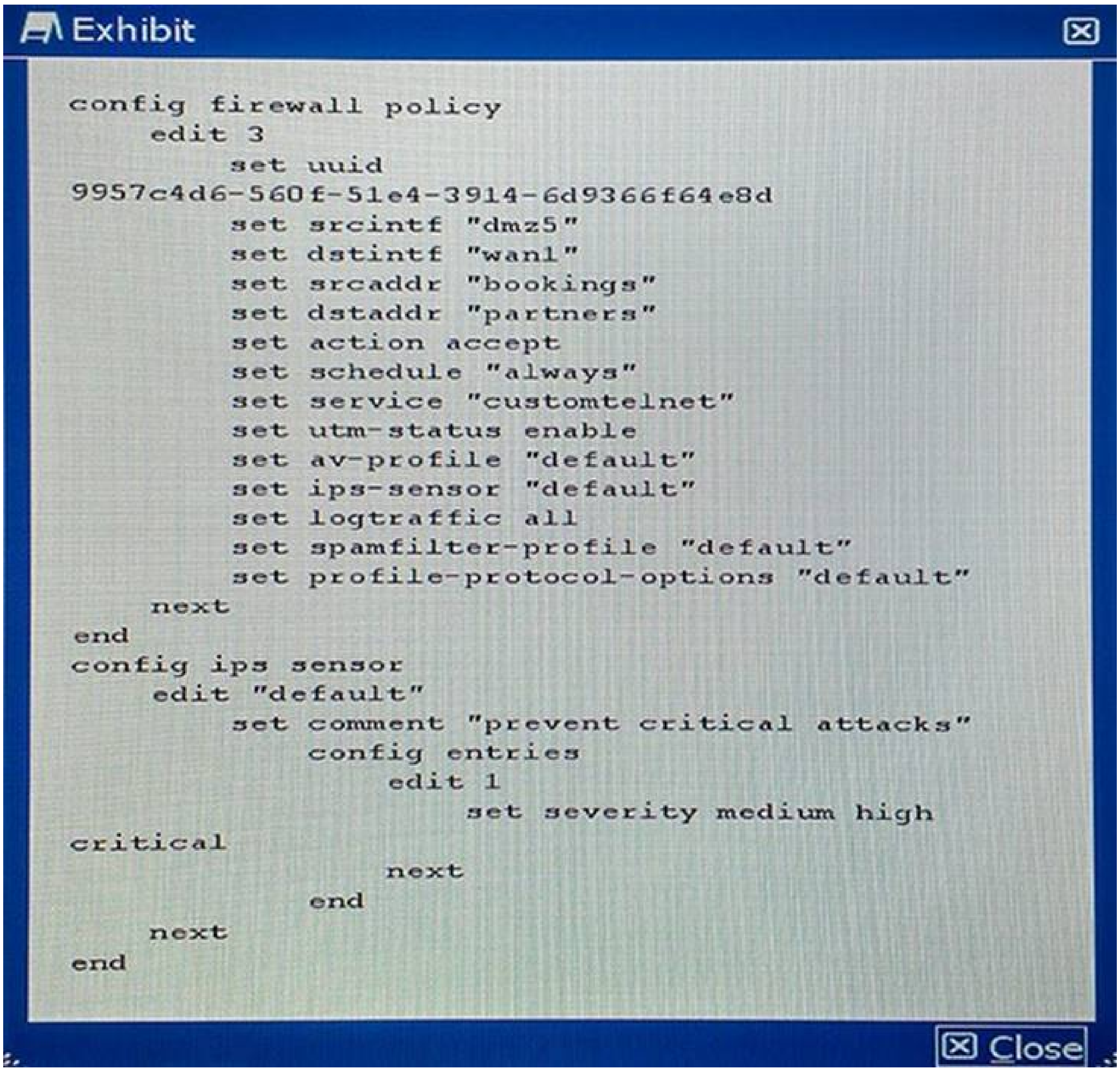
```
config system session-ttl
set default 7200
end
```

E.


```
config system global
set tcp-halfclose-timer 10
set udp-idle-timer 90
end
```

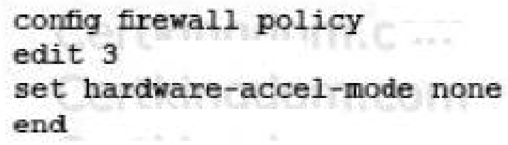
Answer: ADE

NEW QUESTION 5
Your NOC contracts the security team due to a problem with a new application flow. You are instructed to disable hardware acceleration for the policy shown in the exhibit for troubleshooting purposes.

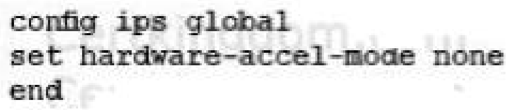


```
config firewall policy
    edit 3
        set uuid
9957c4d6-560f-51e4-3914-6d9366f64e8d
        set srcintf "dmz5"
        set dstintf "wan1"
        set srcaddr "bookings"
        set dstaddr "partners"
        set action accept
        set schedule "always"
        set service "customtelnet"
        set utm-status enable
        set av-profile "default"
        set ips-sensor "default"
        set logtraffic all
        set spamfilter-profile "default"
        set profile-protocol-options "default"
    next
end
config ips sensor
    edit "default"
        set comment "prevent critical attacks"
            config entries
                edit 1
                    set severity medium high
critical
                next
            end
    next
end
```

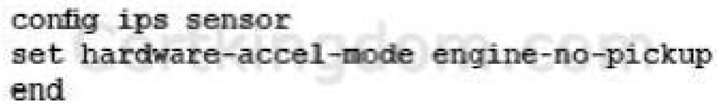
Which command will disable hardware acceleration for the new application policy?

A.


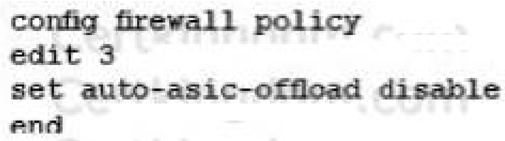
```
config firewall policy
edit 3
set hardware-accel-mode none
end
```

B.


```
config ips global
set hardware-accel-mode none
end
```

C.


```
config ips sensor
set hardware-accel-mode engine-no-pickup
end
```

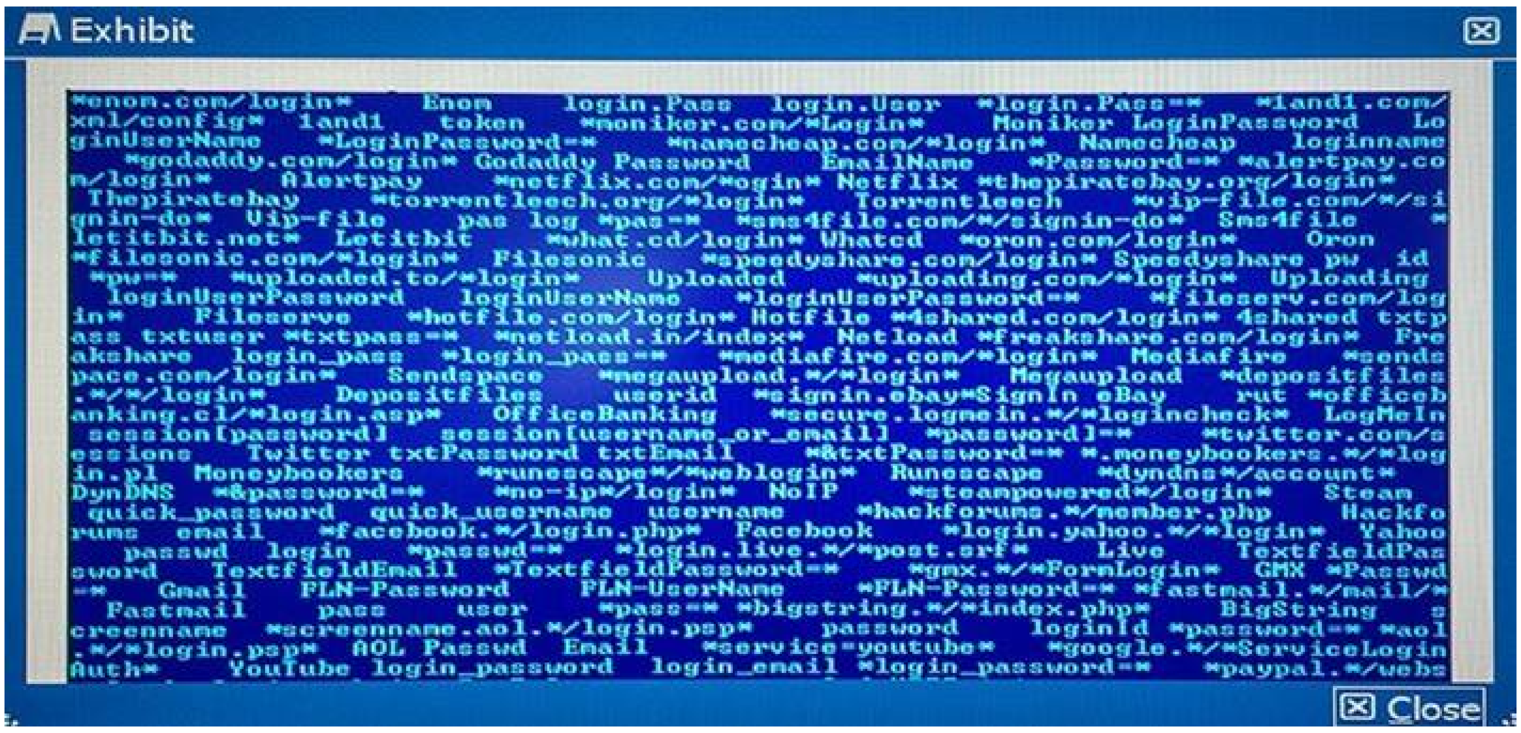
D.


```
config firewall policy
edit 3
set auto-asic-offload disable
end
```

Answer: D

Explanation: References:
http://docs.fortinet.com/uploaded/files/1607/fortigate-hardware-accel-50.pdf

NEW QUESTION 6
Your marketing department uncompressed and executed a file that the whole department received using Skype.



```
*enon.com/login*    Enom    login.Pass  login.User  *login.Pass=*   *1and1.com/
xml/config*  1and1   token   *moniker.com/*Login*    Moniker LoginPassword   Lo
ginUserName   *LoginPassword=*   *namecheap.com/*login*  Namecheap   loginname
   *godaddy.com/login* Godaddy Password    EmailName    *Password=* *alertpay.co
m/login*    Alertpay    *netflix.com/*ogin* Netflix *thepiratebay.org/login*
 Thepiratebay    *torrentleech.org/*login*   Torrentleech    *vip-file.com/*/si
gnin-do*  Vip-file     pas log *pas=*   *sms4file.com/*/signin-do*  Sms4file    *
letitbit.net*  Letitbit    *what.cd/login* Whatcd  *oron.com/login*    Oron
*filesonic.com/*login*  Filesonic   *speedyshare.com/login* Speedyshare pw  id
 *pw=*   *uploaded.to/*login*    Uploaded    *uploading.com/*login*  Uploading
  loginUserPassword   loginUserName   *loginUserPassword=*    *fileserv.com/log
in*    Fileserve   *hotfile.com/login* Hotfile *4shared.com/login* 4shared txtp
ass txtuser *txtpass=*   *netload.in/index*  Netload *freakshare.com/login*  Fre
akshare  login_pass  *login_pass=*    *mediafire.com/*login*  Mediafire    *sends
pace.com/login*   Sendspace   *megaupload.*/*login*   Megaupload  *depositfiles
.*/*/login*    Depositfiles    userid  *signin.ebay*SignIn eBay    rut *officeb
anking.cl/*login.asp*   OfficeBanking   *secure.logmein.*/*logincheck*  LogMeIn
 session[password]   session[username_or_email]  *password]=*    *twitter.com/s
essions   Twitter txtPassword txtEmail     *&txtPassword=* *.moneybookers.*/*log
in.pl  Moneybookers     *runescape*/*weblogin*  Runescape    *dyndns*/account*
DynDNS  *&password=*    *no-ip*/login*  NoIP     *steampowered*/login*    Steam
 quick_password  quick_username  username     *hackforums.*/member.php    Hackfo
rums  email   *facebook.*/login.php*  Facebook    *login.yahoo.*/*login*  Yahoo
   passwd  login   *passwd=*    *login.live.*/*post.srf*     Live     TextfieldPas
sword    TextfieldEmail  *TextfieldPassword=*     *gmx.*/*FormLogin*  GMX *Passwd
=*    Gmail    FLN-Password     FLN-UserName     *FLN-Password=* *fastmail.*/mail/*
  Fastmail    pass     user    *pass=* *bigstring.*/*index.php*     BigString    s
creenname   *screenname.aol.*/login.psp*     password      loginId *password=* *aol
.*/*login.psp*  AOL Passwd  Email     *service=youtube*     *google.*/*ServiceLogin
Auth*     YouTube login_password  login_email *login_password=*    *paypal.*/webs
```

Reviewing the exhibit, which two details do you determine from your initial analysis of the payload?

A. The payload contains strings that the malware is monitoring to harvest credentials.
B. This is a type of Trojan that will download and pirate movies using your Netflix credentials.
C. This type of threat of a DDoS attack using instant messaging to send e-mails to further spread the infection.
D. This threat payload is uploading private user videos which are then used to extort Bitcoin payments.

Answer: B

NEW QUESTION 7
An administrator wants to assign static IP addresses to users connecting tunnel-mode SSL VPN. Each SSL VPN user must always get the same unique IP address which is never assigned to any other user.
Which solution accomplishes this task?

A. TACACS+ authentication with an attribute-value (AV) pair containing each user’s IP address.
B. RADIUS authentication with each user’s IP address stored in a Vendor Specific Attribute (VSA).
C. LDAP authentication with an LDAP attribute containing each user’s IP address.
D. FSSO authentication with an LDAP attribute containing each user’s IP address.

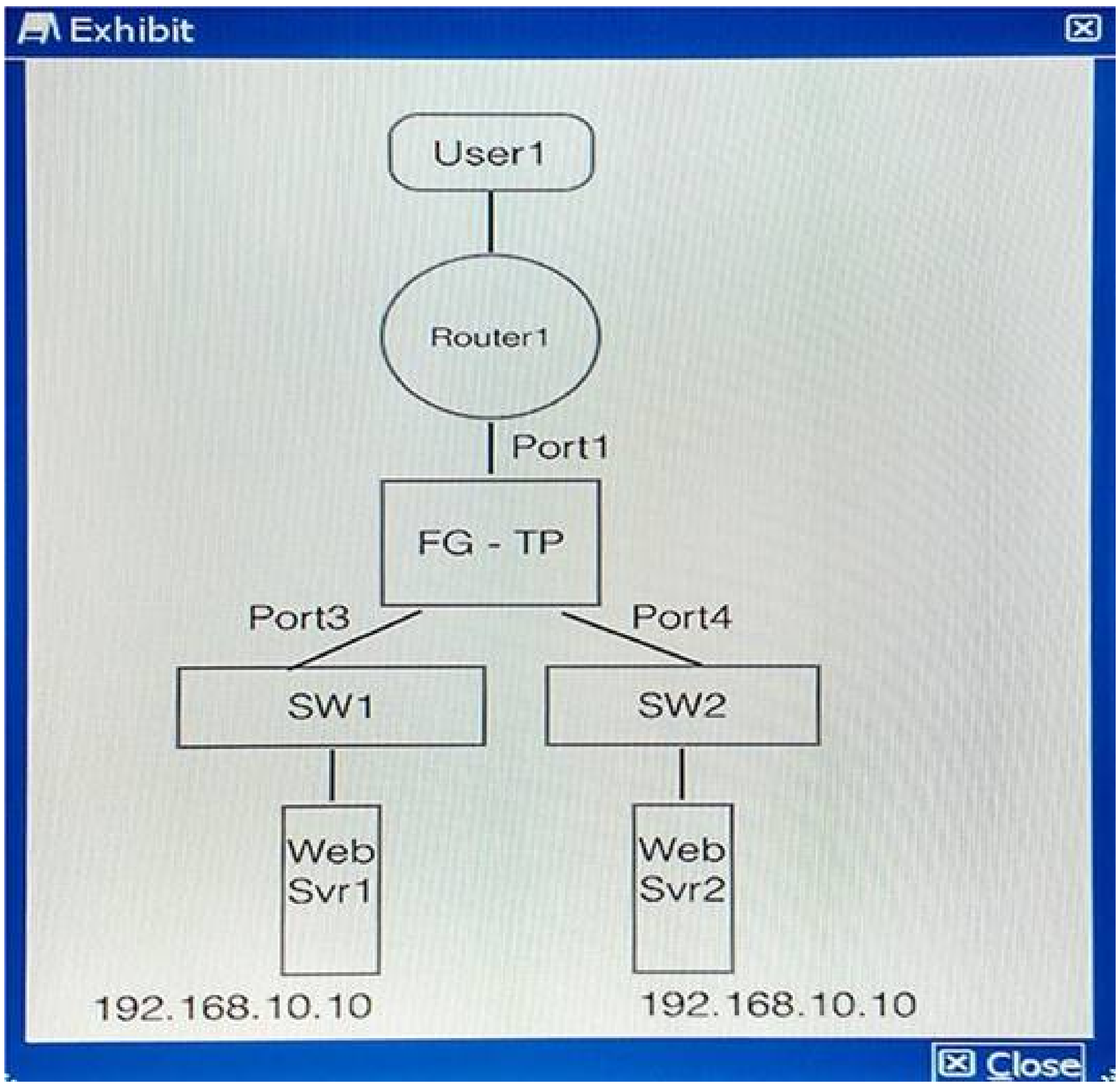
Answer: D

NEW QUESTION 8
Which command detects where a routing path is broken?

A. exec traceroute <destination>
B. exec route ping <destination>
C. diag route null
D. diag debug route <destination>

Answer: A

NEW QUESTION 9
You have implemented FortiGate in transparent mode as shown in the exhibit. User1 from the Internet is trying to access the 192.168.10.10 Web servers.



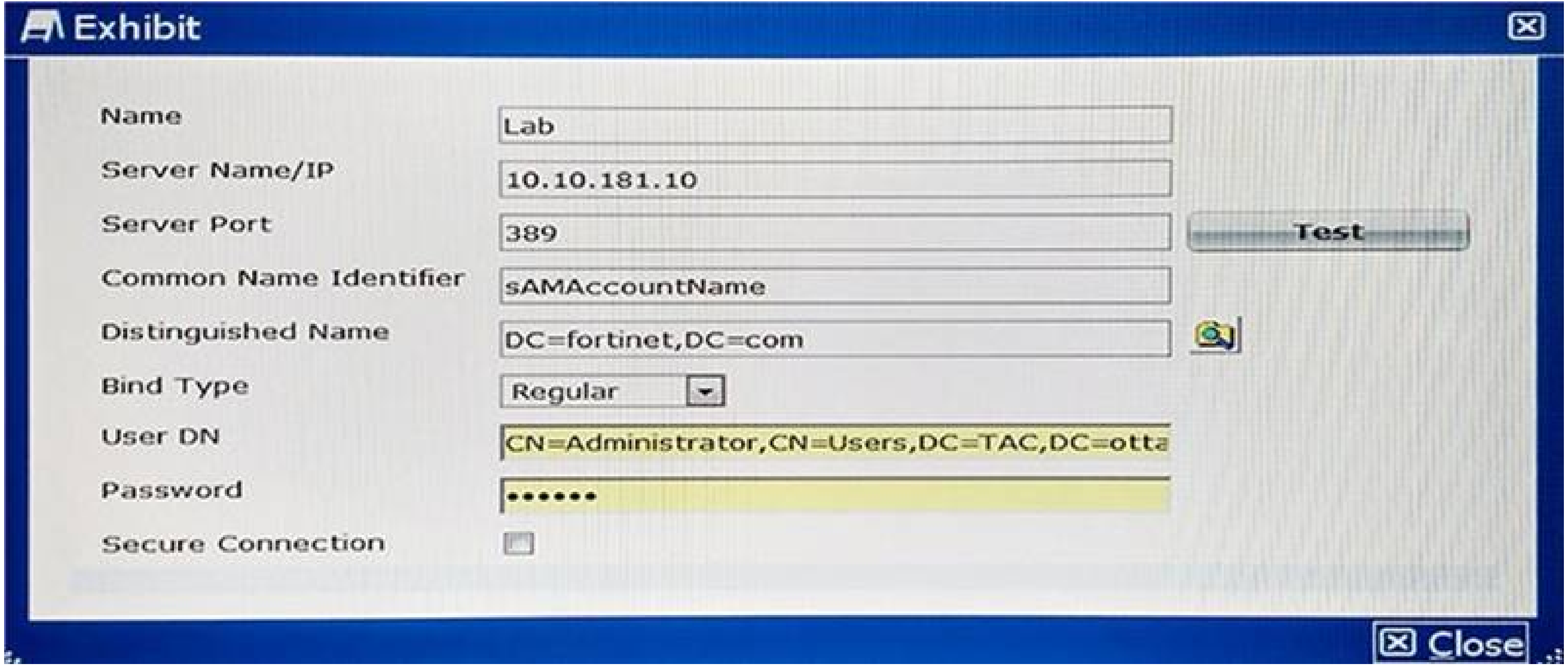
Which two statements about this scenario are true? (Choose two.)

A. User1 would be able to access the Web server intermittently.
B. User1 would not be able to access any of the Web servers at all.
C. FortiGate learns Web servers MAC address when the Web servers transmit packets.
D. FortiGate always flood packets to both Web servers at the same time.

Answer: AC

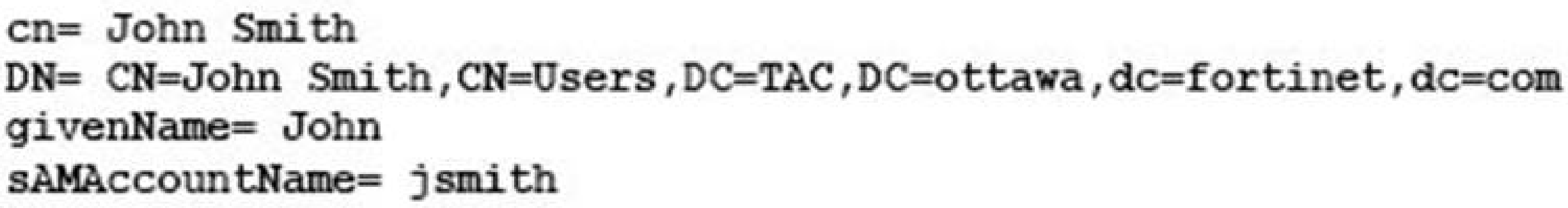
Explanation: Both servers have same ip address, so there will be intermittent we server connectivity from outside and whichever web server forwards packets fortigate learns its mac address.

NEW QUESTION 10
The exhibit shows an LDAP server configuration in a FortiGate device.



Name	Lab
Server Name/IP	10.10.181.10
Server Port	389
Common Name Identifier	sAMAccountName
Distinguished Name	DC=fortinet,DC=com
Bind Type	Regular
User DN	CN=Administrator,CN=Users,DC=TAC,DC=otta
Password	••••••
Secure Connection	□

The LDAP user, John Smith, has the following LDAP attributes:



```
cn= John Smith
DN= CN=John Smith,CN=Users,DC=TAC,DC=ottawa,dc=fortinet,dc=com
givenName= John
sAMAccountName= jsmith
```

John Smith’s LDAP password is ABC123.
Which CLI command should you use to test the LDAP authentication using John Smith’s credentials?

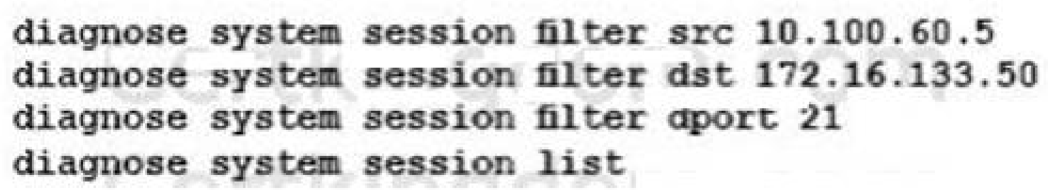
A. diagnose test authserver ldap Lab jsmith ABC123
B. diagnose test authserver ldap-direct Lab jsmith ABC123

C. diagnose test authserver ldap Lab ‘John Smith’ ABC123
D. diagnose test authserver ldap-direct Lab john ABC123

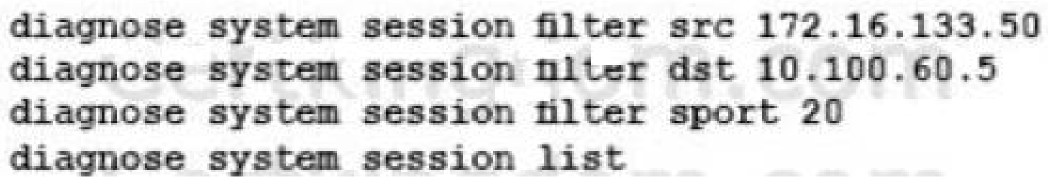
Answer: A

Explanation: References: https://forum.fortinet.com/tm.aspx?m=119178

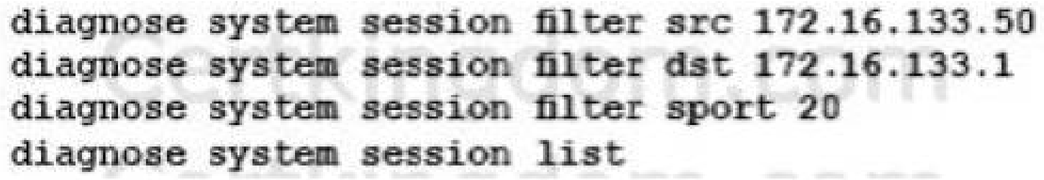
NEW QUESTION 10
You are investigating a problem related to FTP active mode. You use a test PC with IP address 10.100.60.5 to connect to the FTP server at 172.16.133.50 and transfer a large file. The FortiGate translates source address (SNAT) in network 10.100.60.0/24 to the IP address 172.16.133.1.
Which two groups of CLI commands allow you to see information related to this FTP connection (Choose two.)

A.


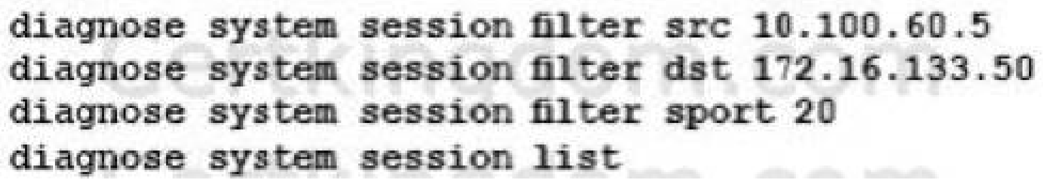
```
diagnose system session filter src 10.100.60.5
diagnose system session filter dst 172.16.133.50
diagnose system session filter dport 21
diagnose system session list
```

B.


```
diagnose system session filter src 172.16.133.50
diagnose system session filter dst 10.100.60.5
diagnose system session filter sport 20
diagnose system session list
```

C.


```
diagnose system session filter src 172.16.133.50
diagnose system session filter dst 172.16.133.1
diagnose system session filter sport 20
diagnose system session list
```

D.


```
diagnose system session filter src 10.100.60.5
diagnose system session filter dst 172.16.133.50
diagnose system session filter sport 20
diagnose system session list
```

Answer: AD

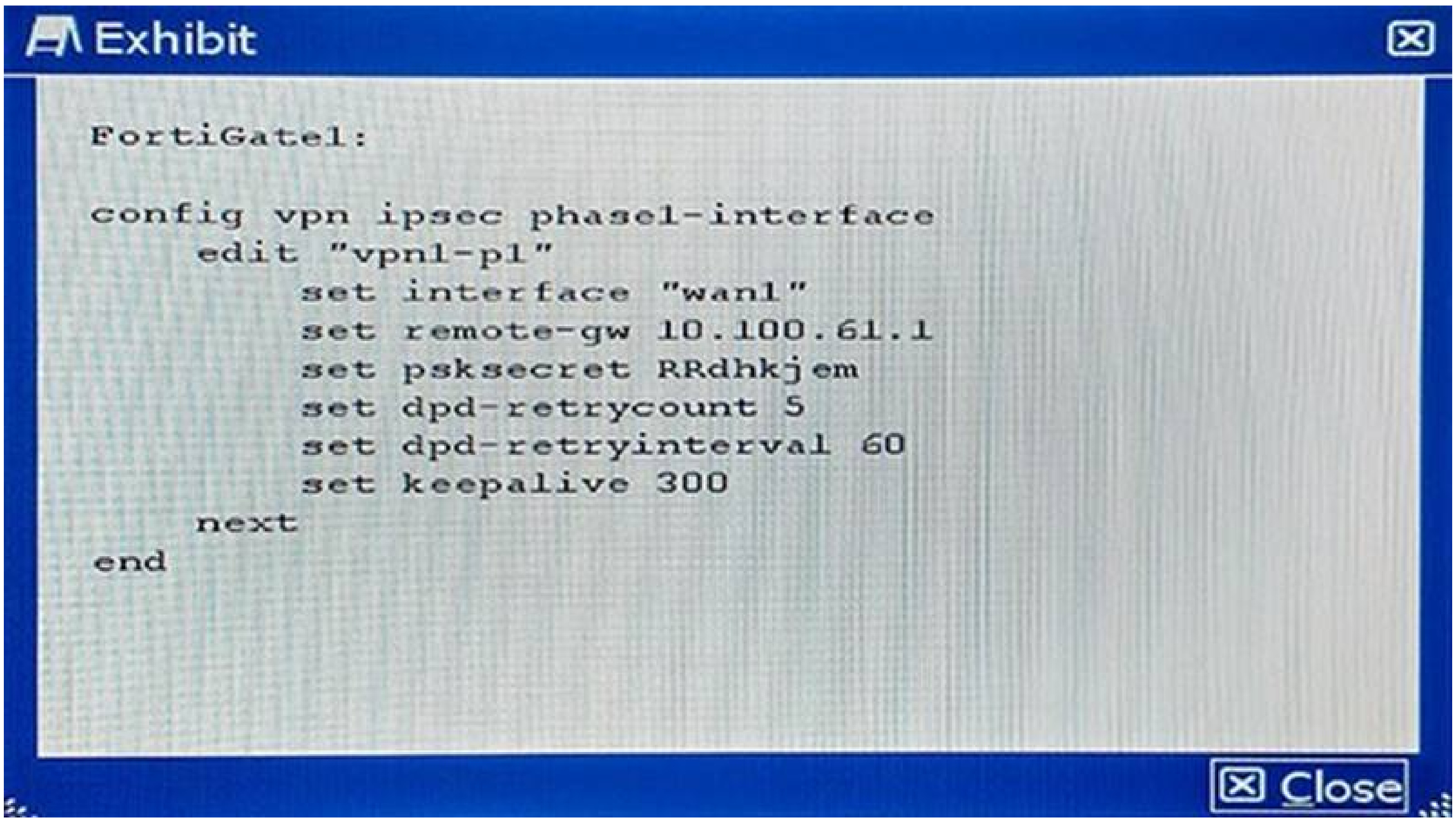
Explanation: FTP active on port 21 and passive uses port 20

NEW QUESTION 11
Which Fortinet product is used for antispam protection?

A. FortiSwitch
B. FortiGate
C. FortiWeb
D. FortiDB

Answer: B

NEW QUESTION 14
FortiGate1 has a gateway-to-gateway IPsec VPN to FortiGate2. The entire IKE negotiation between FortiGate1 and FortiGate2 is on UDP port 500. A PC on FortuGate2’s local area network is sending continuous ping requests over the VPN tunnel to a PC of FortiGate1’s local area network. No other traffic is sent over the tunnel.



```
FortiGate1:

config vpn ipsec phase1-interface
    edit "vpn1-p1"
        set interface "wan1"
        set remote-gw 10.100.61.1
        set psksecret RRdhkjem
        set dpd-retrycount 5
        set dpd-retryinterval 60
        set keepalive 300
    next
end
```

Which statement is true on this scenario?

A. FortiGate1 sends an R-U-THERE packet every 300 seconds while ping traffic is flowing.
B. FortiGate1 sends an R-U-THERE packet if pings stop for 300 seconds and no IKE packet is received during this period.
C. FortiGate1 sends an R-U-THERE packet if pings stop for 60 seconds and no IKE packet is received during this period.
D. FortiGate1 sends an R-U-THERE packet every 60 seconds while ping traffic is flowing.

Answer: C

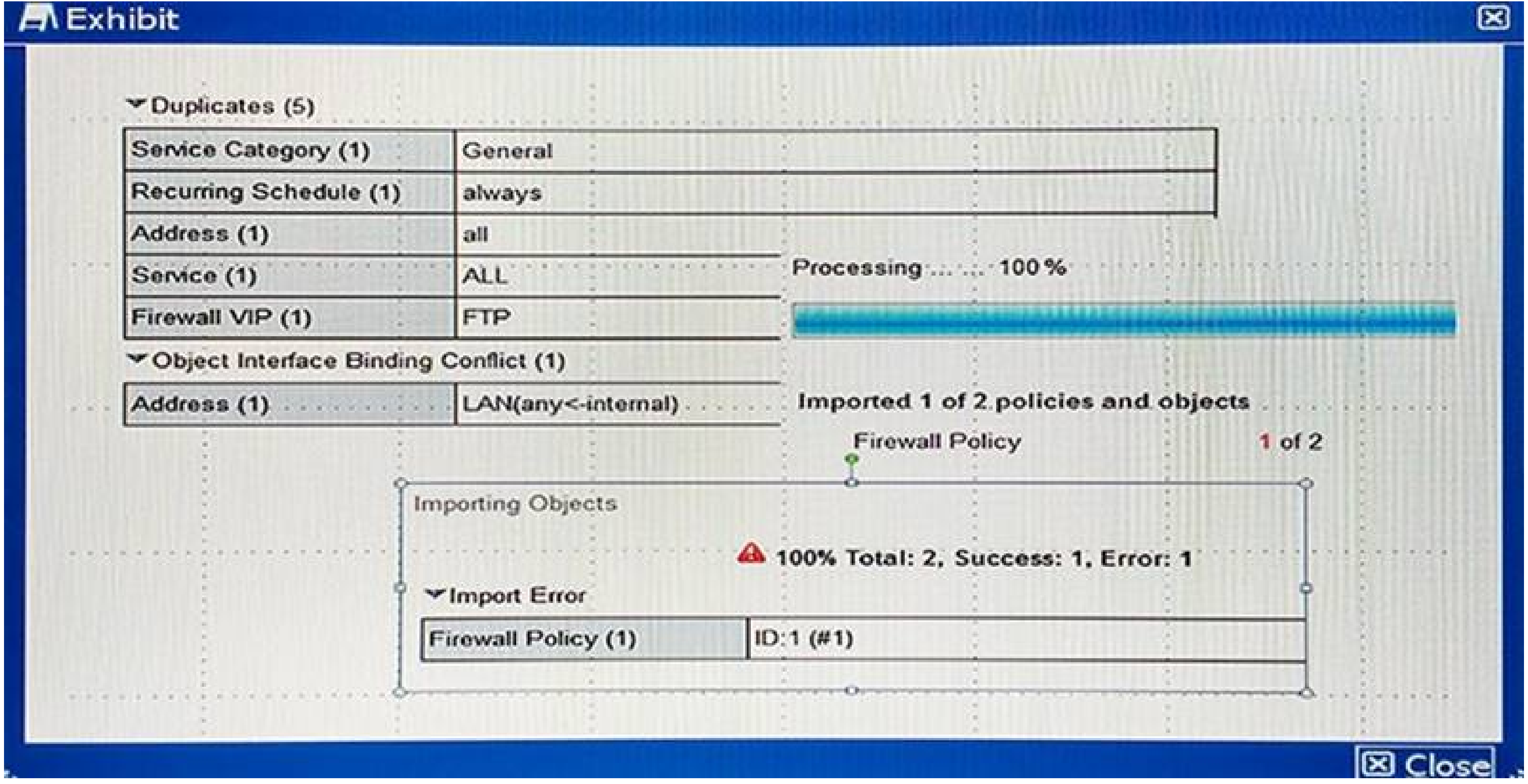
Explanation: References: http://kb.fortinet.com/kb/documentLink.do?externalID=FD35337

NEW QUESTION 15
Which VPN protocol is supported by FortiGate units?

A. E-LAN
B. PPTP
C. DMVPN
D. OpenVPN

Answer: BC

NEW QUESTION 20



Duplicates (5)

Service Category (1)	General
Recurring Schedule (1)	always
Address (1)	all
Service (1)	ALL
Firewall VIP (1)	FTP

Processing ...... 100 %

Object Interface Binding Conflict (1)

Address (1)	LAN(any<-internal)

Imported 1 of 2 policies and objects

Firewall Policy 1 of 2

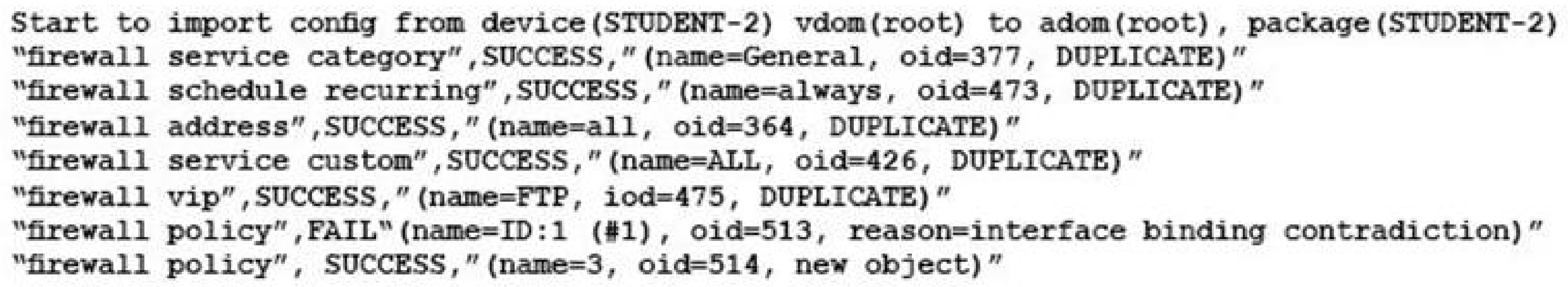
Importing Objects

100% Total: 2, Success: 1, Error: 1

Import Error

Firewall Policy (1)	ID:1 (#1)

Given the following error message:



```
Start to import config from device(STUDENT-2) vdom(root) to adom(root), package(STUDENT-2)
"firewall service category",SUCCESS,"(name=General, oid=377, DUPLICATE)"
"firewall schedule recurring",SUCCESS,"(name=always, oid=473, DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=364, DUPLICATE)"
"firewall service custom",SUCCESS,"(name=ALL, oid=426, DUPLICATE)"
"firewall vip",SUCCESS,"(name=FTP, iod=475, DUPLICATE)"
"firewall policy",FAIL"(name=ID:1 (#1), oid=513, reason=interface binding contradiction)"
"firewall policy", SUCCESS,"(name=3, oid=514, new object)"
```

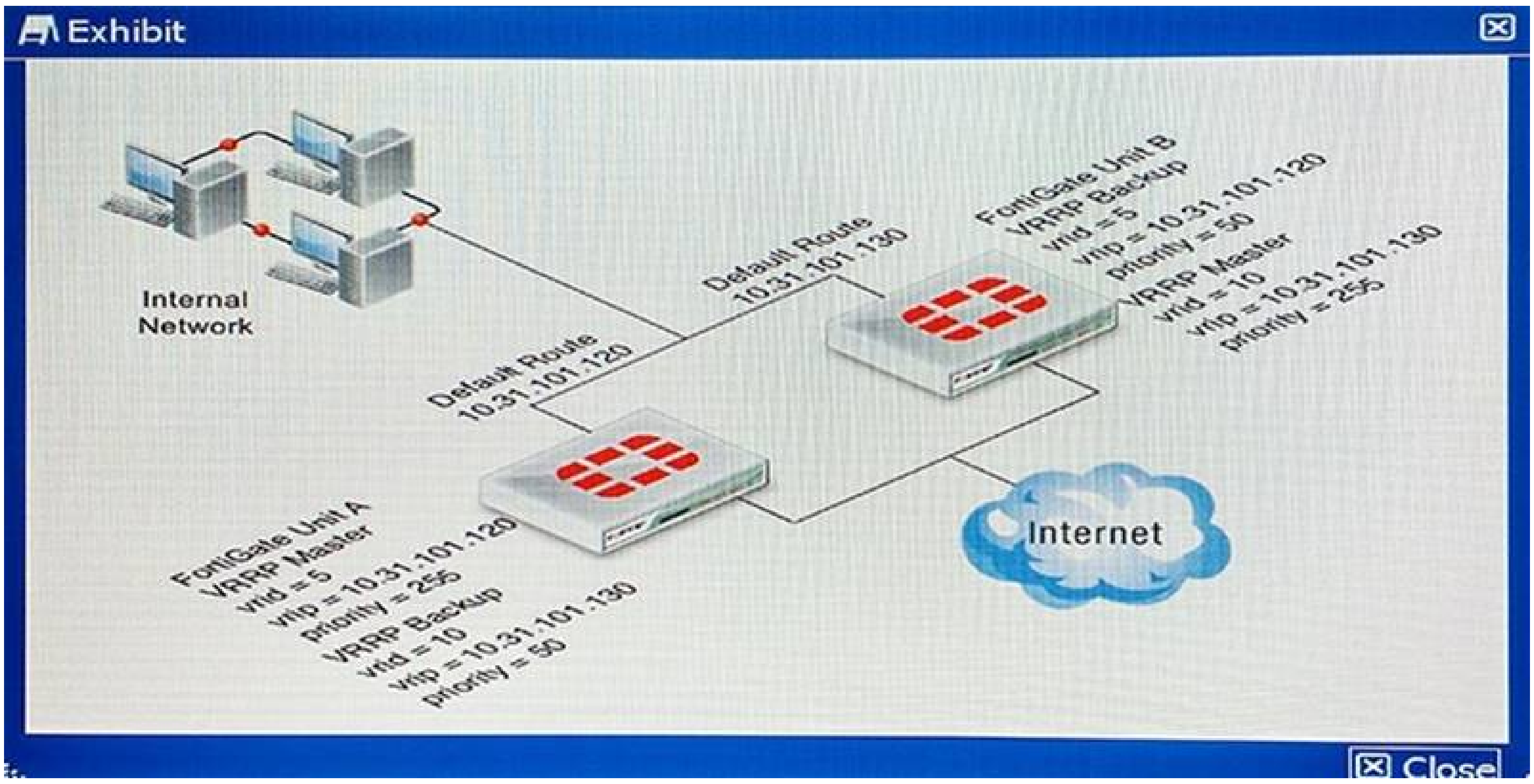
FortiManager fails to import policy ID 1. What is the problem?

A. FortiManager already has Address LAN which has interface mapping set to “internal” in its database, it is contradicting with the STUDENT-2 FortiGate device which has address LAN mapped to “any”.
B. FortiManager already has address LAN which has interface mapping set to “any” in its database; this conflicts with the STUDENT-2 FortiGate device which has address “LAN”mapped to “internal”.
C. Policy ID 1 for this managed FortiGate device already exists on the FortiManager policy package named STUDENT-2.
D. Policy ID 1 does not have interface mapping on FortiManager.

Answer: D

Explanation: References: http://kb.fortinet.com/kb/documentLink.do?externalID=FD38544

NEW QUESTION 21
Referring to the diagram shown in the exhibit, you deployed VRRP load balancing using two FortiGate units and two VRRP groups with a VRRP virtual MAC address enabled on both FortiGate’s port2 interface. During normal operation, both FortiGate units are processing traffic and the VRRP groups are used to load balance the traffic between the two FortiGate units.



If FortiGate unit A fails, what would happen?

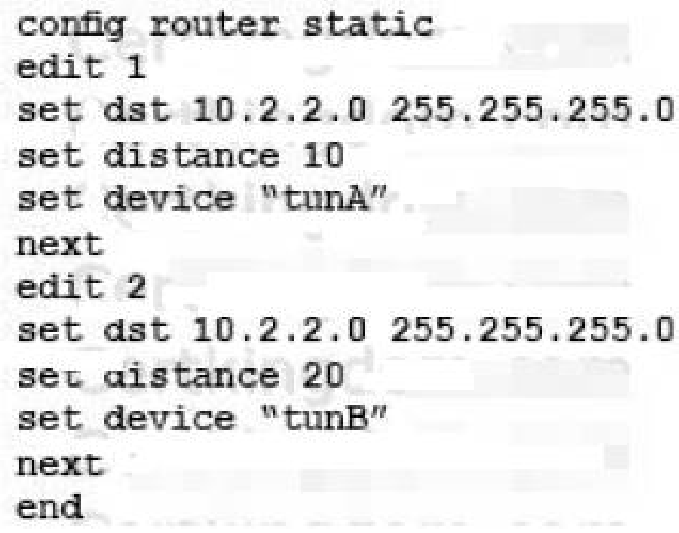
A. The FortiGate Unit B port2 interface sends gratuitous ARPs to associate the VRRPvirtual router IP address with its own MAC address, and all traffic fails over to it.
B. The FortiGate Unit B port2 interface will use virtual MAC addresses of 00-00-5e-00-01- 05 and 00-00-5e-00-01-0a, and all traffic fails over to it.
C. The FortiGate Unit B port2 interface will use virtual MAC addresses of 00-a0-5e-00-01- 05 and 00-a0-5e-00-01-0a, and all traffic fails over to it.
D. The FortiGate Unit B port2 interface will use the physical MAC addresses of the FortiGate Unit A port2 interface, and all traffic fails over to it.

Answer: B

Explanation: If primary fails secondary device uses virtual mac address to forward traffic

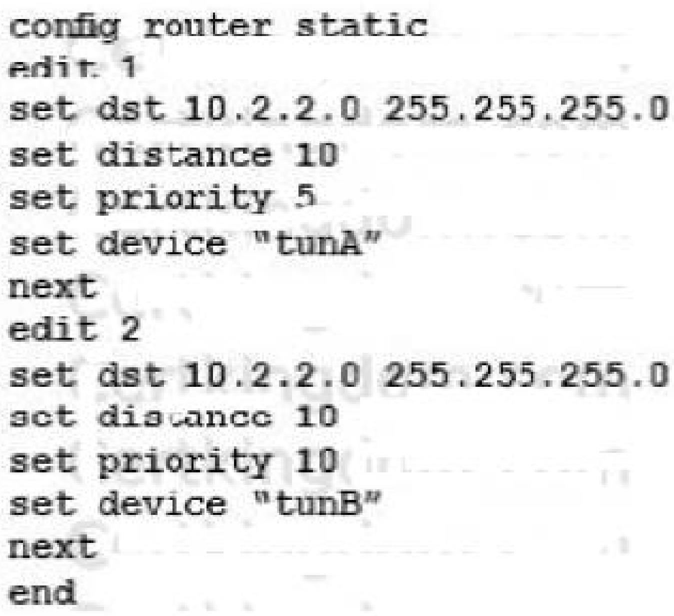
NEW QUESTION 24
The FortiGate is used as an IPsec gateway at a branch office. Two tunnels, tunA and tunB, are established between this FortiGate and the headquarters’ IPsec gateway. The branch office’s subnet is 10.1.1.0/24. The headquarters’ subnet is 10.2.2.0/24. The desired usage for tunA and tunB has been defined as follows:
- sessions initiated from 10.1.1.0/24 to 10.2.2.0/24 must be routed out over tunA when tunA is up
- sessions initiated from 10.1.1.0/24 to 10.2.2.0/24 have to be routed out over tunB when tunA is down
- sessions initiated from 10.2.2.0/24 can ingress either on tunA or on tunB Which static routing configuration meets the requirements?

A.



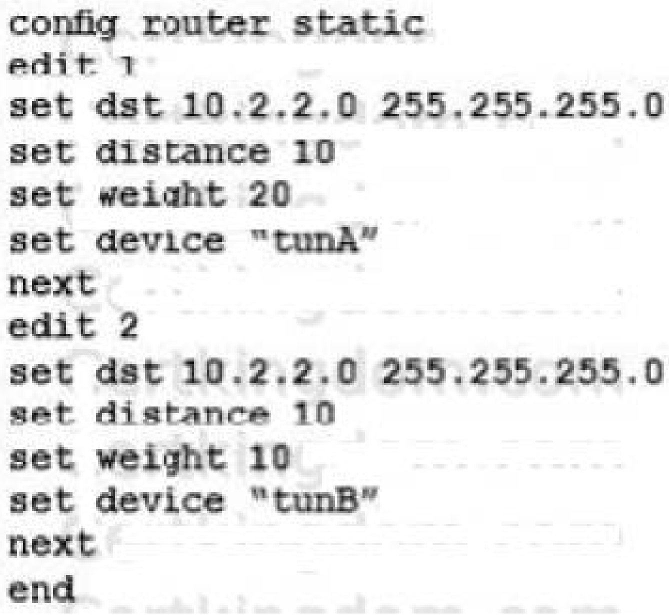
```
config router static
edit 1
set dst 10.2.2.0 255.255.255.0
set distance 10
set device "tunA"
next
edit 2
set dst 10.2.2.0 255.255.255.0
set distance 20
set device "tunB"
next
end
```

B.



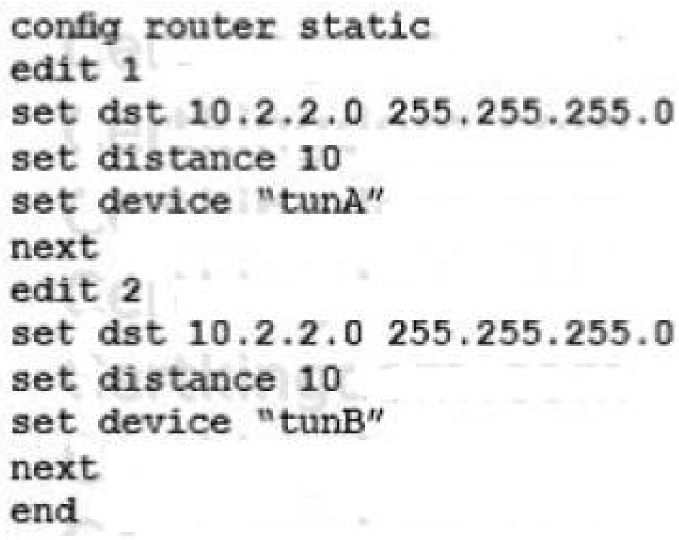
```
config router static
edit 1
set dst 10.2.2.0 255.255.255.0
set distance 10
set priority 5
set device "tunA"
next
edit 2
set dst 10.2.2.0 255.255.255.0
set distance 10
set priority 10
set device "tunB"
next
end
```

C.



```
config router static
edit 1
set dst 10.2.2.0 255.255.255.0
set distance 10
set weight 20
set device "tunA"
next
edit 2
set dst 10.2.2.0 255.255.255.0
set distance 10
set weight 10
set device "tunB"
next
end
```

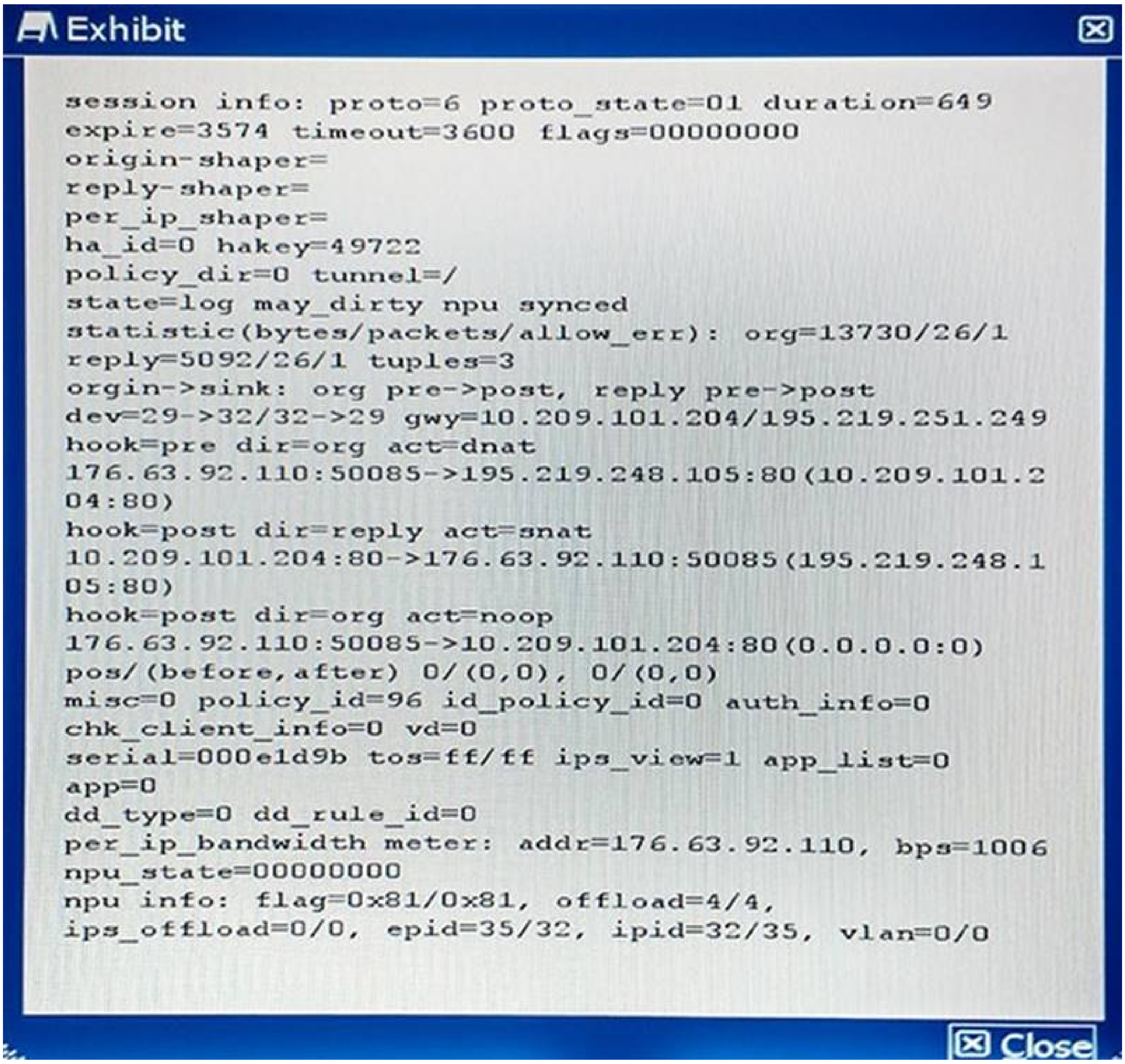
D.



```
config router static
edit 1
set dst 10.2.2.0 255.255.255.0
set distance 10
set device "tunA"
next
edit 2
set dst 10.2.2.0 255.255.255.0
set distance 10
set device "tunB"
next
end
```

Answer: C

NEW QUESTION 27
Referring to the configuration shown in the exhibit, which three statements are true? (Choose three.)



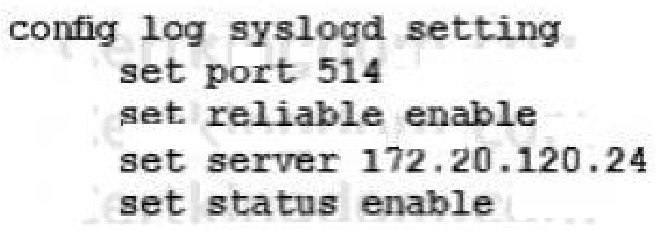
```
session info: proto=6 proto_state=01 duration=649
expire=3574 timeout=3600 flags=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 hakey=49722
policy_dir=0 tunnel=/
state=log may_dirty npu synced
statistic(bytes/packets/allow_err): org=13730/26/1
reply=5092/26/1 tuples=3
orgin->sink: org pre->post, reply pre->post
dev=29->32/32->29 gwy=10.209.101.204/195.219.251.249
hook=pre dir=org act=dnat
176.63.92.110:50085->195.219.248.105:80(10.209.101.2
04:80)
hook=post dir=reply act=snat
10.209.101.204:80->176.63.92.110:50085(195.219.248.1
05:80)
hook=post dir=org act=noop
176.63.92.110:50085->10.209.101.204:80(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=96 id_policy_id=0 auth_info=0
chk_client_info=0 vd=0
serial=000e1d9b tos=ff/ff ips_view=1 app_list=0
app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=176.63.92.110, bps=1006
npu_state=00000000
npu info: flag=0x81/0x81, offload=4/4,
ips_offload=0/0, epid=35/32, ipid=32/35, vlan=0/0
```

A. Traffic logging is disabled in policy 96.
B. TCP handshake is completed and no FIN/RST has been forwarded.
C. No packet has hit this session in the last five minutes.
D. No QoS is applied to this traffic.
E. The traffic goes through a VIP applied to policy 96.

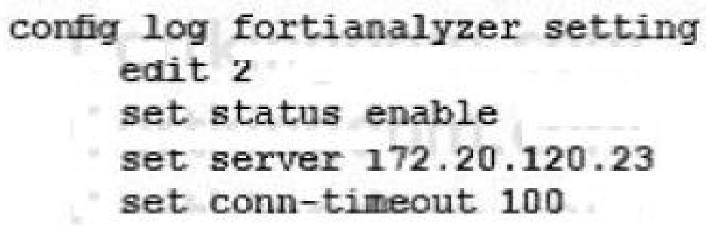
Answer: BCE

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

NEW QUESTION 28
The SECOPS team in your company has started a new project to store all logging data in a disaster recovery center. All FortiGates will log to a secondary FortiAnalyzer and establish a TCP session to send logs to the syslog server.
Which two configurations will achieve this goal? (Choose two.)

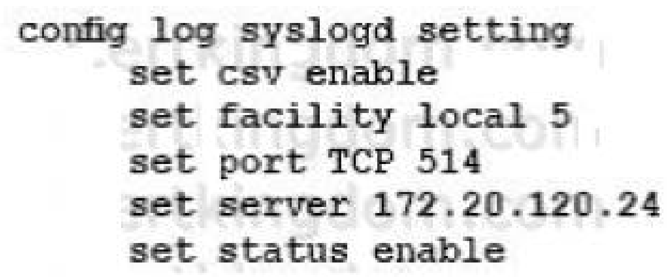
A.


```
config log syslogd setting
    set port 514
    set reliable enable
    set server 172.20.120.24
    set status enable
```

B.


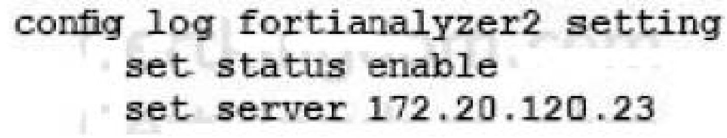
```
config log fortianalyzer setting
    edit 2
    set status enable
    set server 172.20.120.23
    set conn-timeout 100
```

C.



```
config log syslogd setting
      set csv enable
      set facility local 5
      set port TCP 514
      set server 172.20.120.24
      set status enable
```

D.



```
config log fortianalyzer2 setting
      set status enable
      set server 172.20.120.23
```

Answer: AC

Explanation: https://forum.fortinet.com/tm.aspx?m=122848

NEW QUESTION 29

There is an interface-mode IPsec tunnel configured between FortiGate1 and FortiGate2. You want to run OSPF over the IPsec tunnel. On both FortiGates. the IPsec tunnel is based on physical interface port1. Port1 has the default MTU setting on both FortiGate units.
Which statement is true about this scenario?

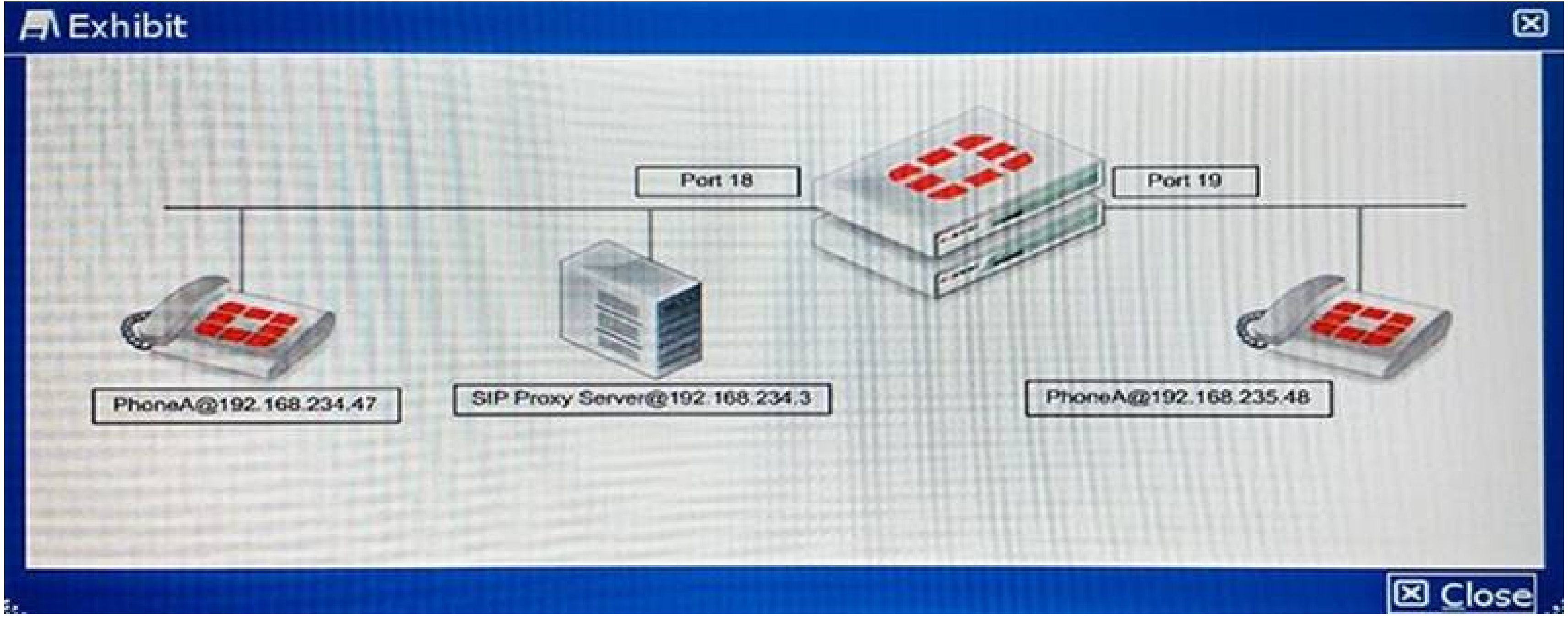
A. A multicast firewall policy must be added on FortiGate1 and FortiGate2 to allow protocol 89.
B. The MTU must be set manually in the OSPF interface configuration.
C. The MTU must be set manually on the IPsec interface.
D. An IP address must be assigned to the IPsec interface on FortiGate1 and FortiGate2.

Answer: B

Explanation: If MTU doesn’t match then the neighbour ship gets stuck in exchange state.

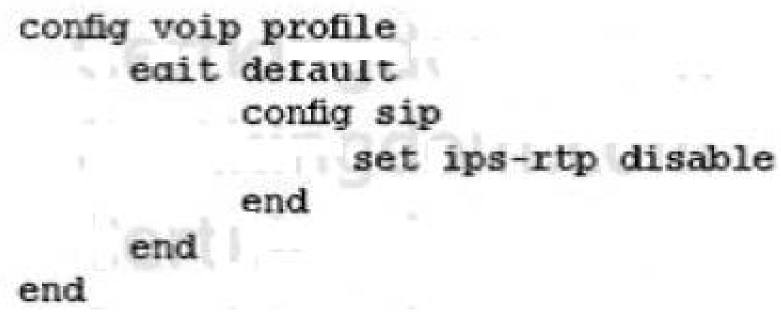
NEW QUESTION 34

Referring to the exhibit, users are reporting that their FortiFones ring but when they pick up, the cannot hear each other. The FortiFones use SIP to communicate with the SIP Proxy Server and RTP between the phones.



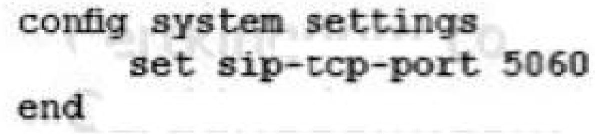
Which configuration change will resolve the problem?

A.



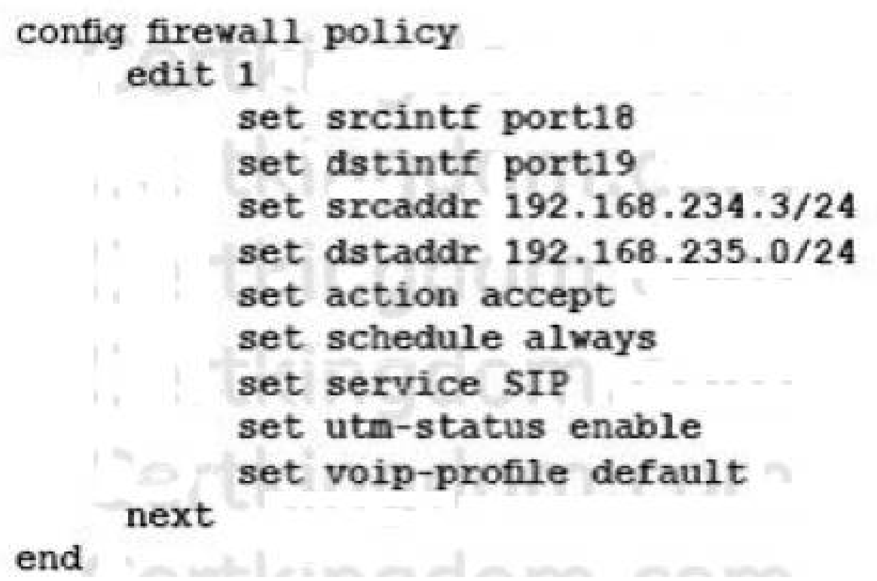
```
config voip profile
      edit default
            config sip
                  set ips-rtp disable
            end
      end
end
```

B.



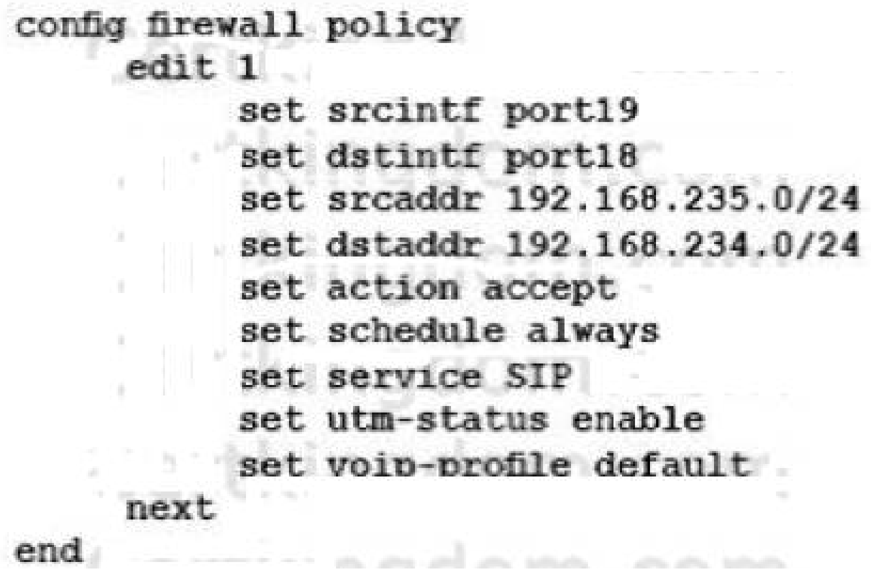
```
config system settings
      set sip-tcp-port 5060
end
```

C.



```
config firewall policy
    edit 1
        set srcintf port18
        set dstintf port19
        set srcaddr 192.168.234.3/24
        set dstaddr 192.168.235.0/24
        set action accept
        set schedule always
        set service SIP
        set utm-status enable
        set voip-profile default
    next
end
```

D.



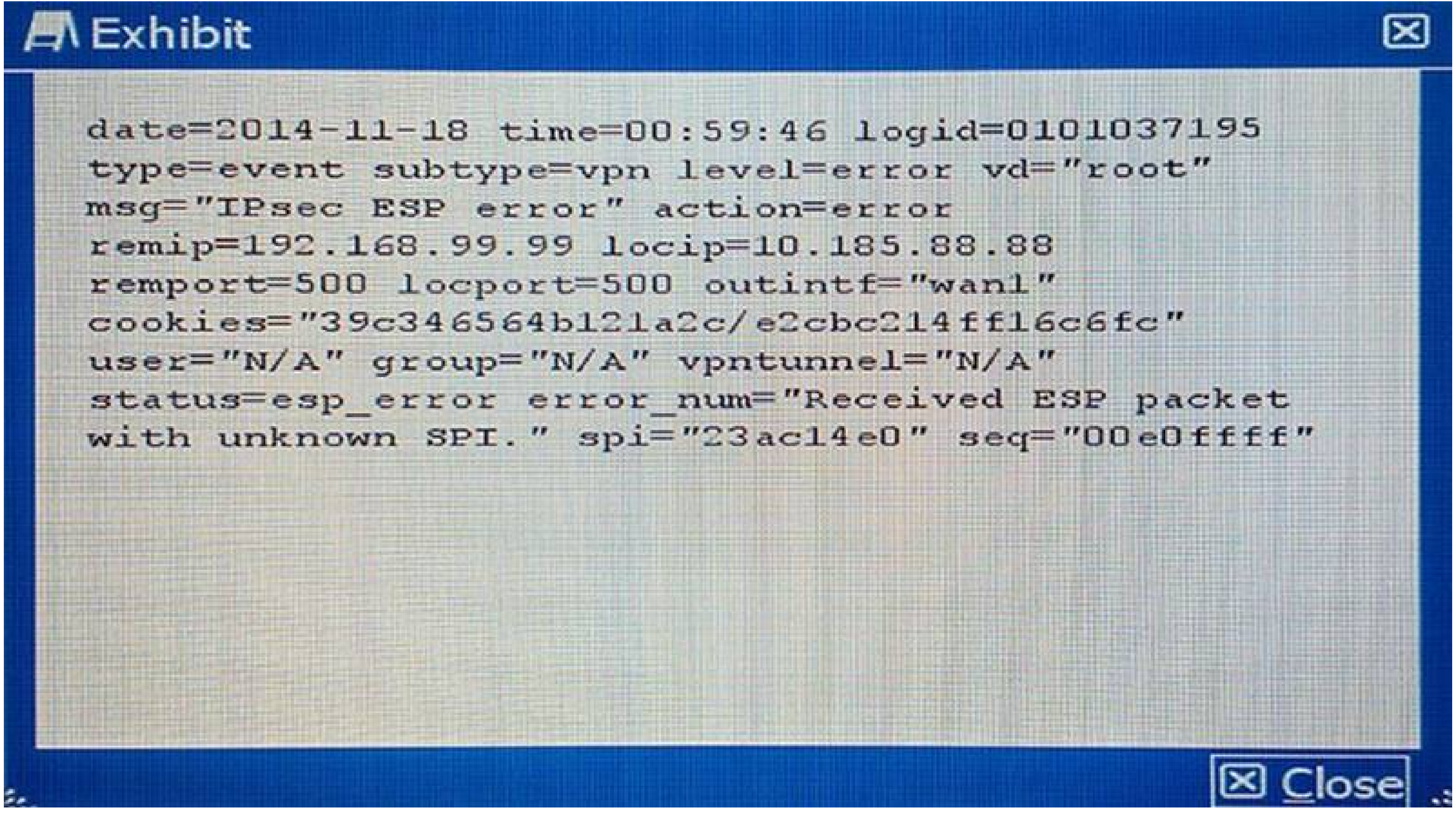
```
config firewall policy
    edit 1
        set srcintf port19
        set dstintf port18
        set srcaddr 192.168.235.0/24
        set dstaddr 192.168.234.0/24
        set action accept
        set schedule always
        set service SIP
        set utm-status enable
        set voip-profile default
    next
end
```

Answer: C

Explanation: References: http://docs.fortinet.com/uploaded/files/2813/fortigate-sip-54.pdf

NEW QUESTION 37

Referring to the exhibit, which statement is true?



```
date=2014-11-18 time=00:59:46 logid=0101037195
type=event subtype=vpn level=error vd="root"
msg="IPsec ESP error" action=error
remip=192.168.99.99 locip=10.185.88.88
remport=500 locport=500 outintf="wan1"
cookies="39c346564b121a2c/e2cbc214ff16c6fc"
user="N/A" group="N/A" vpntunnel="N/A"
status=esp_error error_num="Received ESP packet
with unknown SPI." spi="23ac14e0" seq="00e0ffff"
```

A. The packet failed the HMAC validation.
B. The packet did not match any of the local IPsec SAs.
C. The packet was protected with an unsupported encryption algorithm.
D. The IPsec negotiation failed because the SPI was unknown.

Answer: A

Explanation: http://kb.fortinet.com/kb/viewContent.do?externalId=FD33101

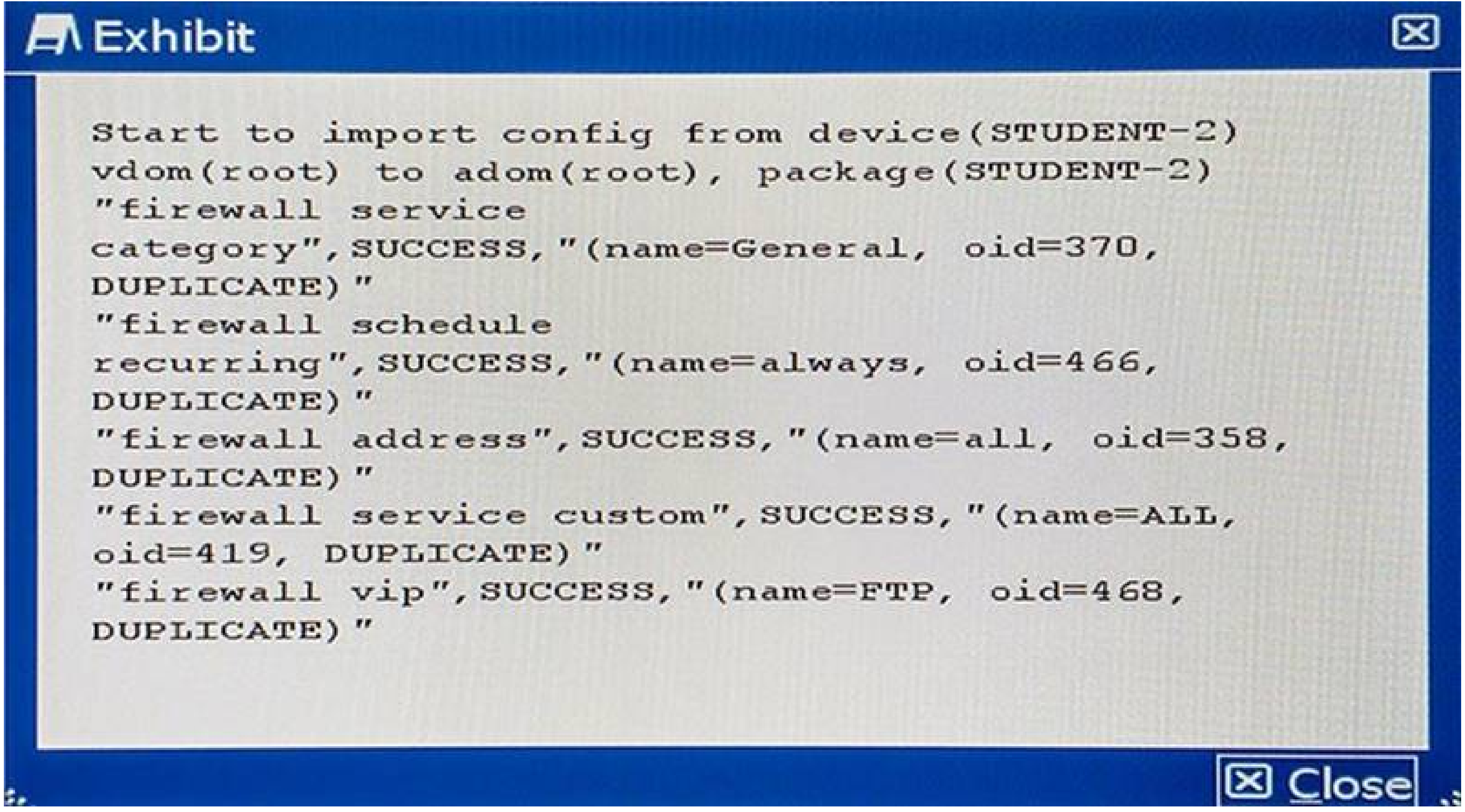
NEW QUESTION 40
You are asked to write a FortiAnalyzer report that lists the session that has consumed the most bandwidth. You are required to include the source IP, destination IP, application, application category, hostname, and total bandwidth consumed.
Which dataset meets these requirements?

A. select from_itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce(‘sentbyte”, 0) +coalesce(‘recbyte “, 0)) as bandwidth from $log where $filter LIMIT 1
B. select from_itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce(‘sentbyte”, 0) +coalesce(‘recbyte“, 0)) as bandwidth from $log where $filter LIMIT 1
C. select from_itime(itime) as timestamp, srcip, dstip, app, appcat, hostname, sum(coalesce(‘sentbyte”, 0) +coalesce(‘rcvdbyte“, 0)) as bandwidth from $log where $filter LIMIT 1
D. select from_itime(itime) as timestamp, sourceip, destip, app, appcat, hostname, sum(coalesce(‘sentbyte’, 0)+coalesce(‘rcvdbyte“, 0)) as bandwidth from $log where $filter LIMIT 1

Answer: C

Explanation: References:
http://docs.fortinet.com/uploaded/files/2617/fortianalyzer-5.2.4-dataset-reference.pdf

NEW QUESTION 41
The output shown in the exhibit from FortiManager is displayed during an import of the device configuration.
Which statement describes the correct action taken for these duplicate objects?



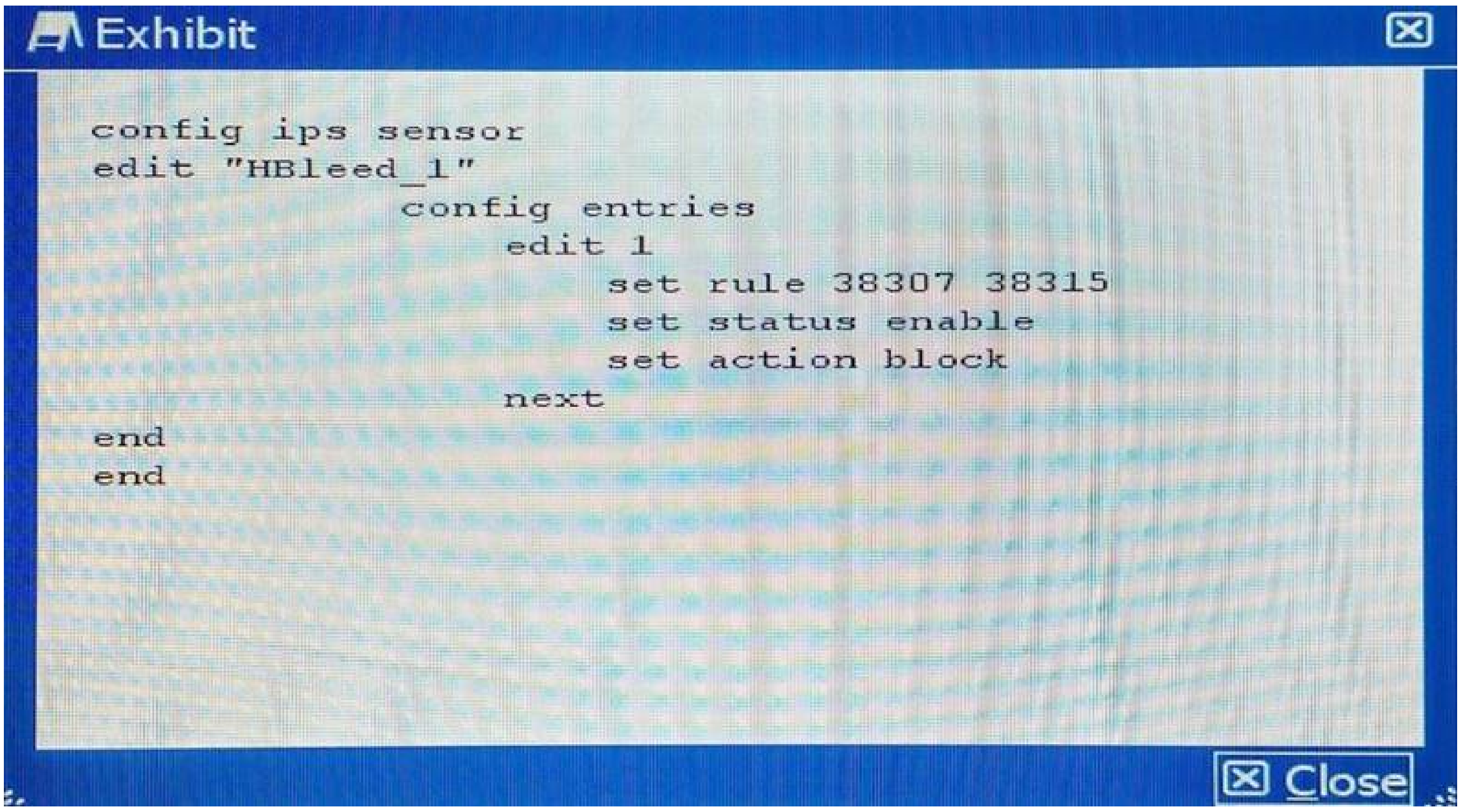
```
Start to import config from device(STUDENT-2)
vdom(root) to adom(root), package(STUDENT-2)
"firewall service
category",SUCCESS,"(name=General, oid=370,
DUPLICATE)"
"firewall schedule
recurring",SUCCESS,"(name=always, oid=466,
DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=358,
DUPLICATE)"
"firewall service custom",SUCCESS,"(name=ALL,
oid=419, DUPLICATE)"
"firewall vip",SUCCESS,"(name=FTP, oid=468,
DUPLICATE)"
```

A. The import fails because of the duplicate entries detected which exist in the ADOM database.
B. FortiManager installs these duplicate objects to the managed device from the ADOM database.
C. FortiManager does not import these duplicate entries into the ADOM database because they already exist in the ADOM database.
D. FortiManager creates indexed duplicate entries for these objects in the ADOM database.

Answer: B

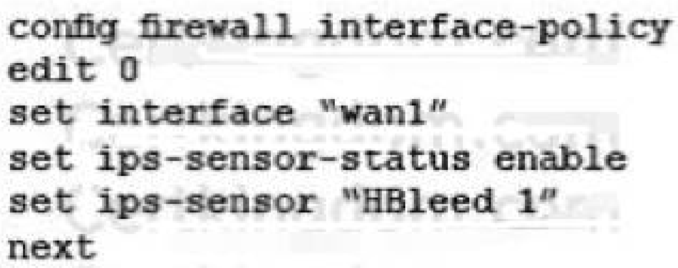
Explanation: References:
http://docs.fortinet.com/uploaded/files/2905/FortiManager-5.4.0-Administration-Guide.pdf

NEW QUESTION 42
Your security department has requested that you implement the OpenSSL.TLS.Heartbeat.Information.Disclosure signature using an IPS sensor to scan traffic destined to the FortiGate. You must log all packets that attempt to exploit this vulnerability.
Referring to the exhibit, which two configurations are required to accomplish this task? (Choose two.)



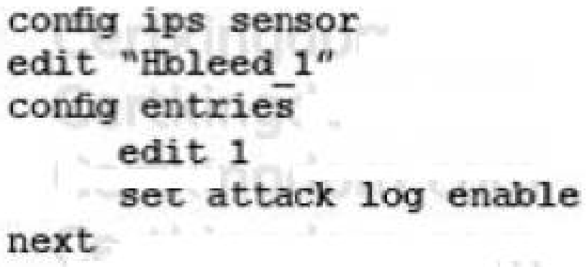
```
config ips sensor
edit "HBleed_1"
            config entries
                edit 1
                    set rule 38307 38315
                    set status enable
                    set action block
                next
end
end
```

A.



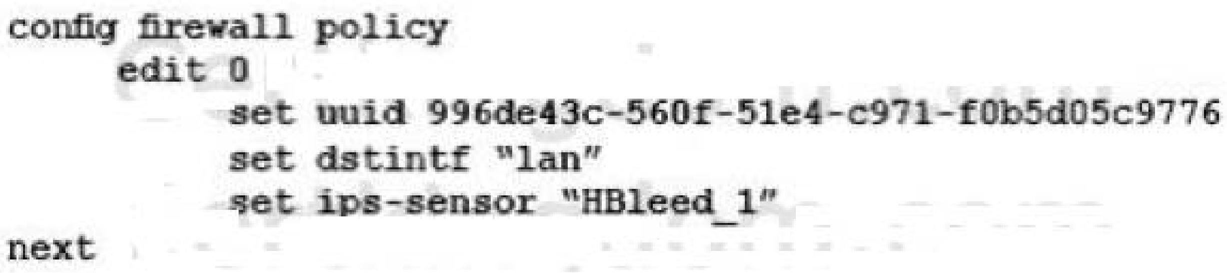
```
config firewall interface-policy
edit 0
set interface "wan1"
set ips-sensor-status enable
set ips-sensor "HBleed 1"
next
```

B.



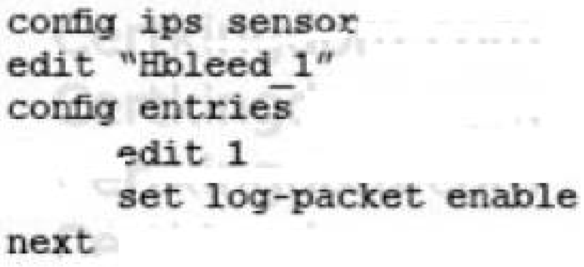
```
config ips sensor
edit "Hbleed_1"
config entries
     edit 1
     set attack log enable
next
```

C.



```
config firewall policy
     edit 0
          set uuid 996de43c-560f-51e4-c971-f0b5d05c9776
          set dstintf "lan"
          set ips-sensor "HBleed_1"
next
```

D.



```
config ips sensor
edit "Hbleed_1"
config entries
     edit 1
     set log-packet enable
next
```

Answer: B

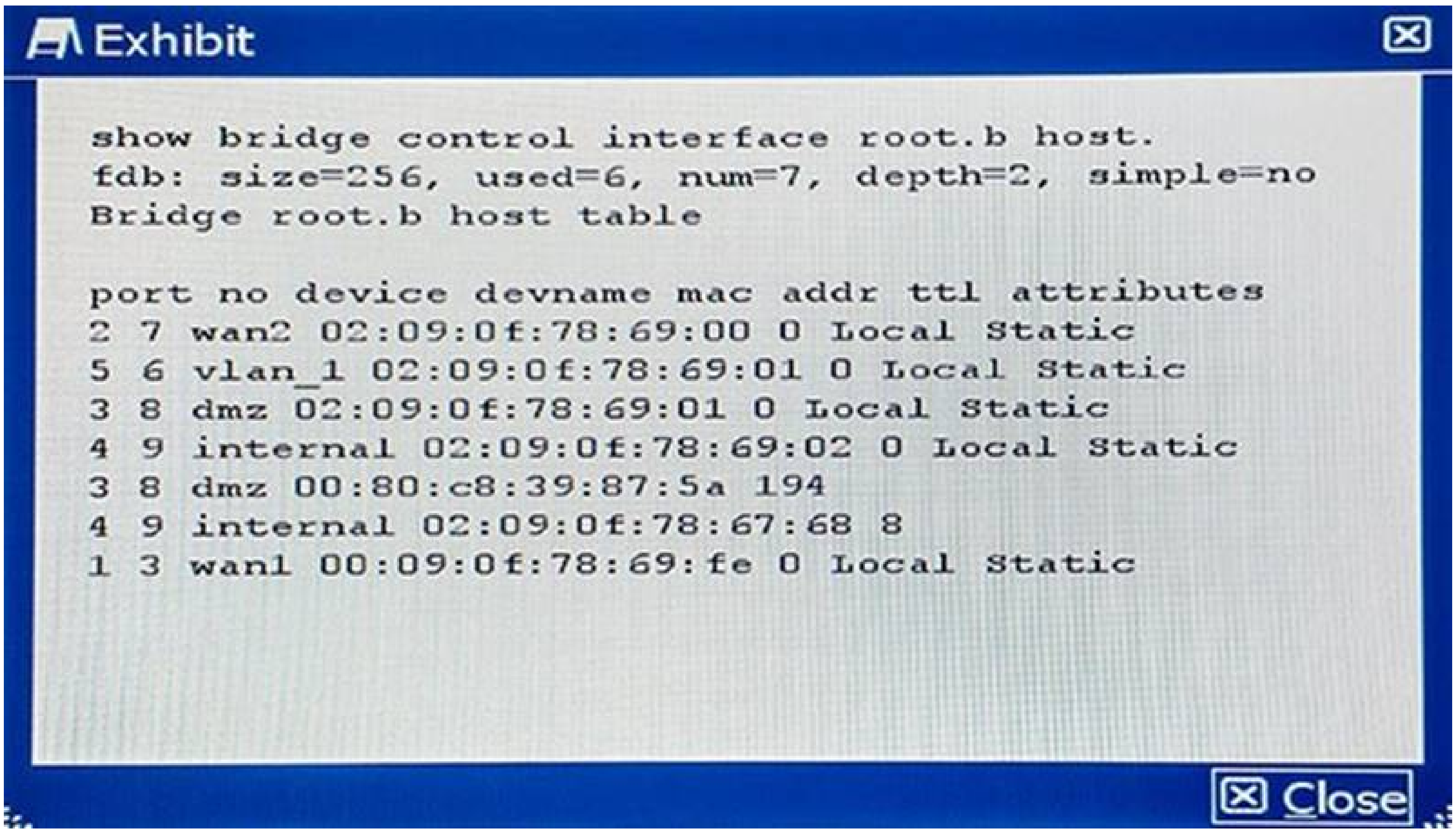
Explanation: http://defadhil.blogspot.in/2014/04/how-to-protect-fortigate-from.html

NEW QUESTION 46
Which two features are supported only by FortiMail but not by FortiGate? (Choose two.)

A. DNSBL
B. built-in MTA
C. end-to-end IBE encryption
D. FortiGuard Antispam

Answer: AB

NEW QUESTION 49
Referring to the command output shown in the exhibit, how many hosts are connected to the FortiGate?



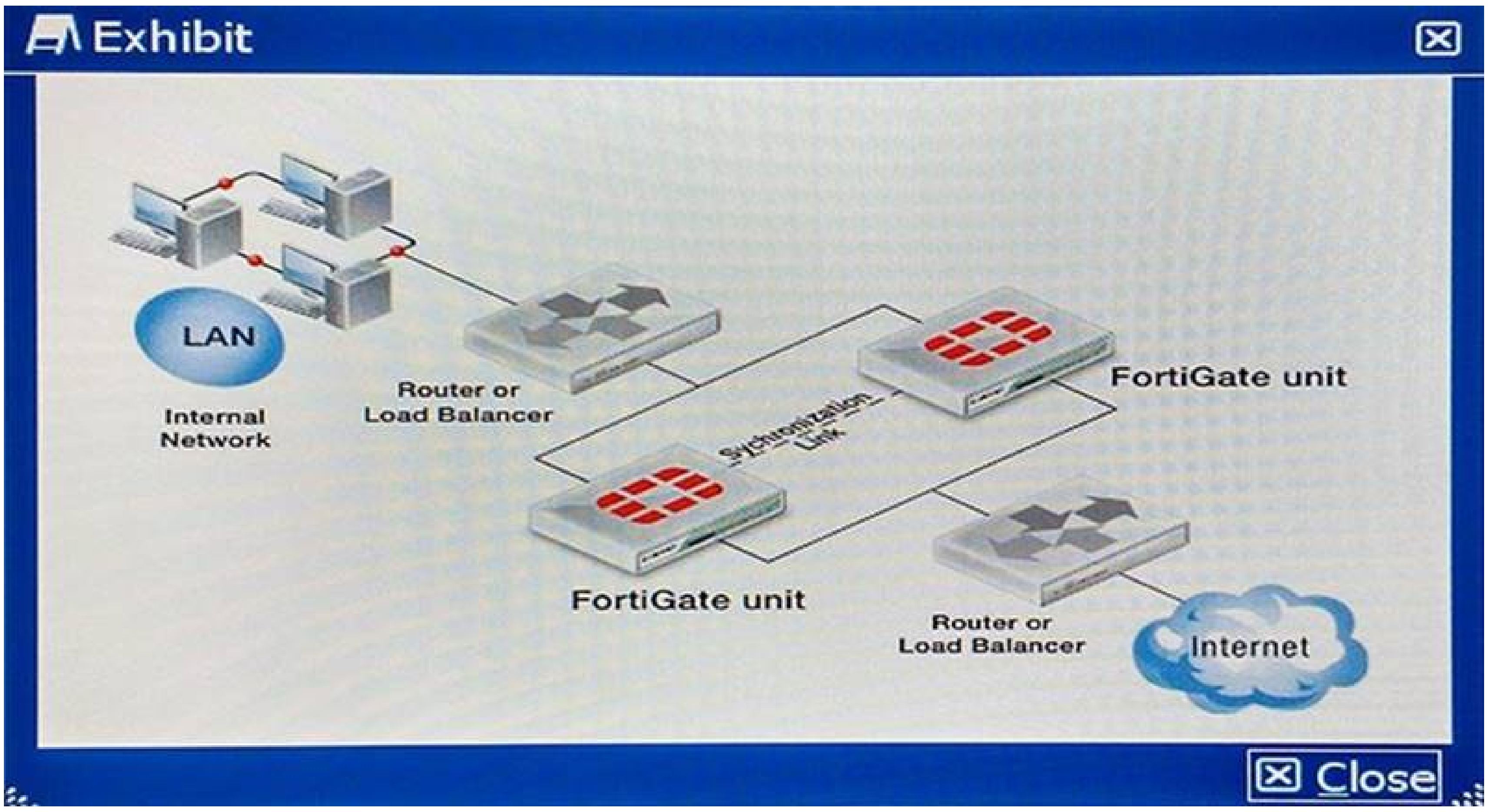
```
show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table

port no device devname mac addr ttl attributes
2 7 wan2 02:09:0f:78:69:00 0 Local Static
5 6 vlan_1 02:09:0f:78:69:01 0 Local Static
3 8 dmz 02:09:0f:78:69:01 0 Local Static
4 9 internal 02:09:0f:78:69:02 0 Local Static
3 8 dmz 00:80:c8:39:87:5a 194
4 9 internal 02:09:0f:78:67:68 8
1 3 wan1 00:09:0f:78:69:fe 0 Local Static
```

A. 7
B. 6
C. 2
D. 256

Answer: B

Explanation: References:
http://cookbook.fortinet.com/troubleshooting-fortigate-installation/

NEW QUESTION 53
A customer just bought an additional FortiGate device and plans to use their existing load balancer to distribute traffic across two FortiGate units participating on a BGP network serving different neighbors. The customer has mixed traffic of IPv4 and IPv6 TCP, UDP, and ICMP. The two FortiGate devices shown in the exhibit should be redundant to each other so that the NAT session and active session tables will synchronize and fail over to the unit that is still operating without any loss of data if one of the units fail.



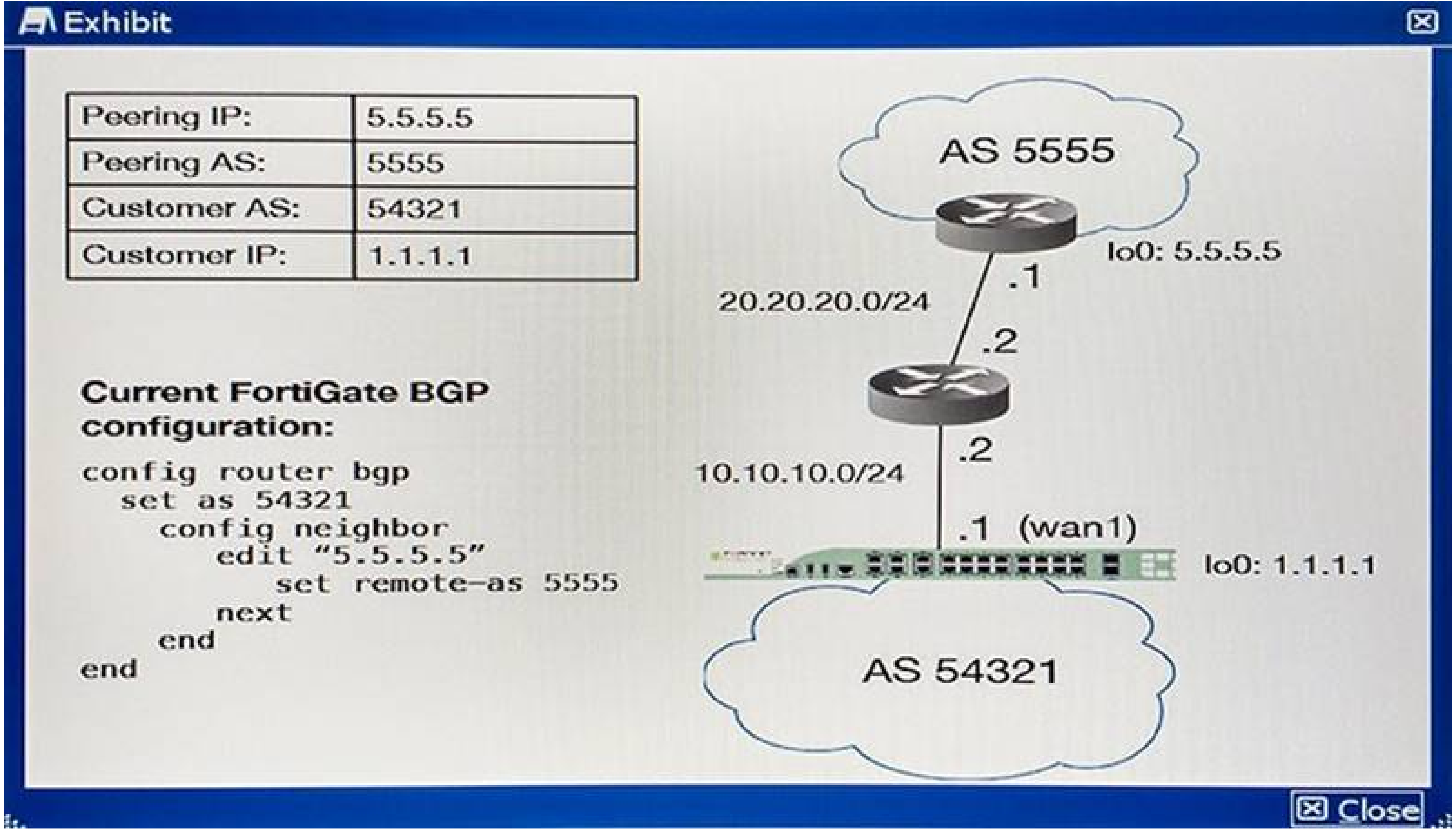
Which high availability solution would you implement?

A. FortiGate Cluster Protocol (FGCP)
B. Fortinet redundant UTM protocol (FRUP)
C. FortiGate Session Life Support Protocol (FGSP)
D. Virtual Router Redundancy Protocol (VRRP)

Answer: A

Explanation: References:
http://docs.fortinet.com/uploaded/files/1074/fortigate-ha-40-mr2.pdf

NEW QUESTION 54
You must establish a BGP peering with a service provider. The provider has supplied you with BGP peering parameters and you performed the basic configuration shown in the exhibit on your FortiGate unit. You notice that your peering session is not coming up.

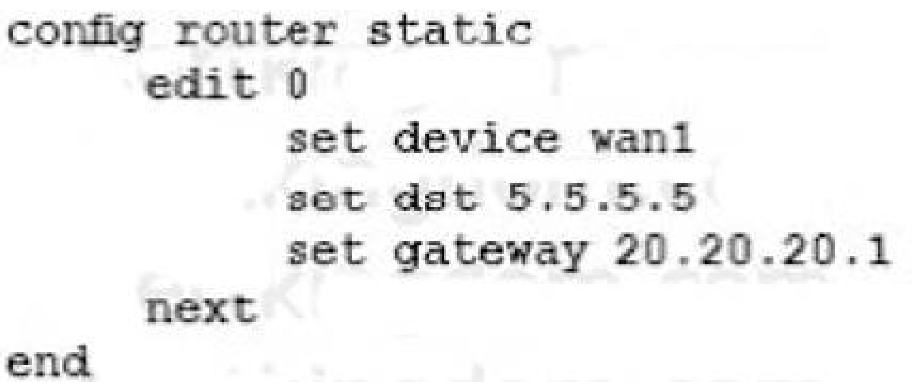


Peering IP:	5.5.5.5
Peering AS:	5555
Customer AS:	54321
Customer IP:	1.1.1.1

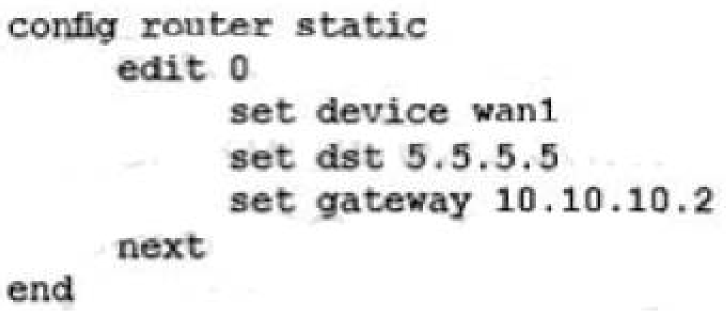
Current FortiGate BGP configuration:

```
config router bgp
   set as 54321
      config neighbor
         edit "5.5.5.5"
            set remote-as 5555
         next
      end
end
```

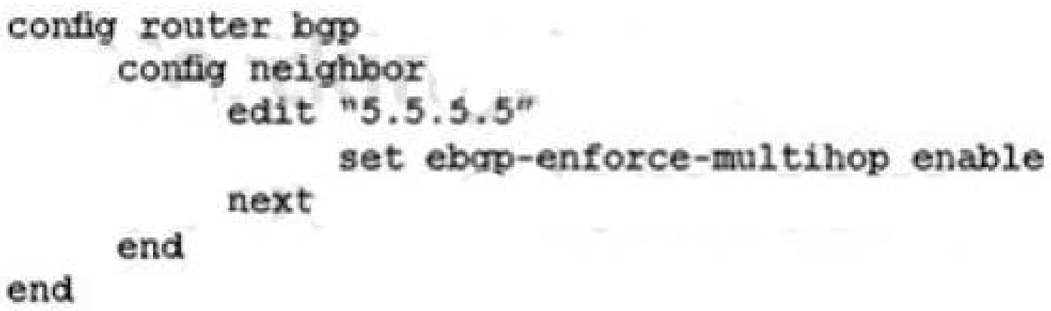
Which three missing configuration statements are needed to make this configuration functional? (Choose three.)

A.


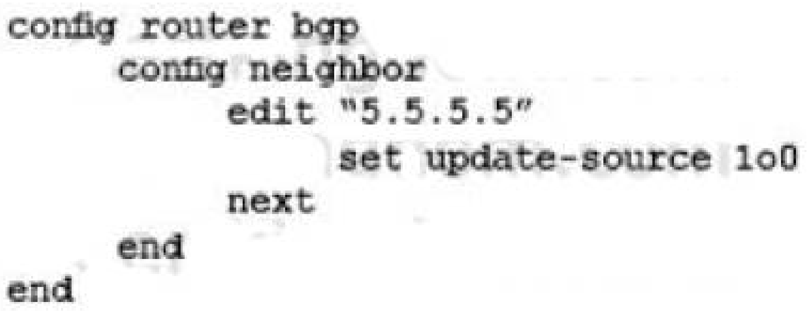
```
config router static
     edit 0
          set device wan1
          set dst 5.5.5.5
          set gateway 20.20.20.1
     next
end
```

B.


```
config router static
     edit 0
          set device wan1
          set dst 5.5.5.5
          set gateway 10.10.10.2
     next
end
```

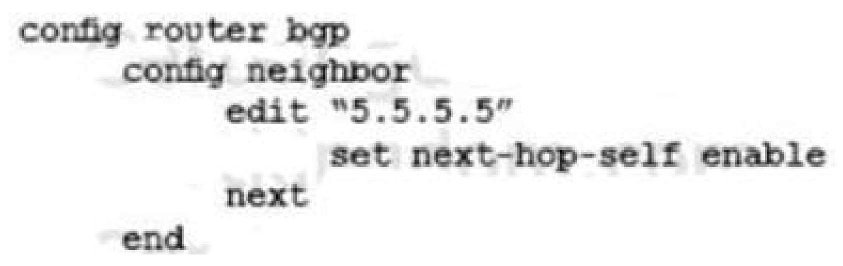
C.


```
config router bgp
     config neighbor
          edit "5.5.5.5"
               set ebgp-enforce-multihop enable
          next
     end
end
```

D.


```
config router bgp
     config neighbor
          edit "5.5.5.5"
               set update-source lo0
          next
     end
end
```

E.



```
config router bgp
    config neighbor
        edit "5.5.5.5"
            set next-hop-self enable
        next
    end
```

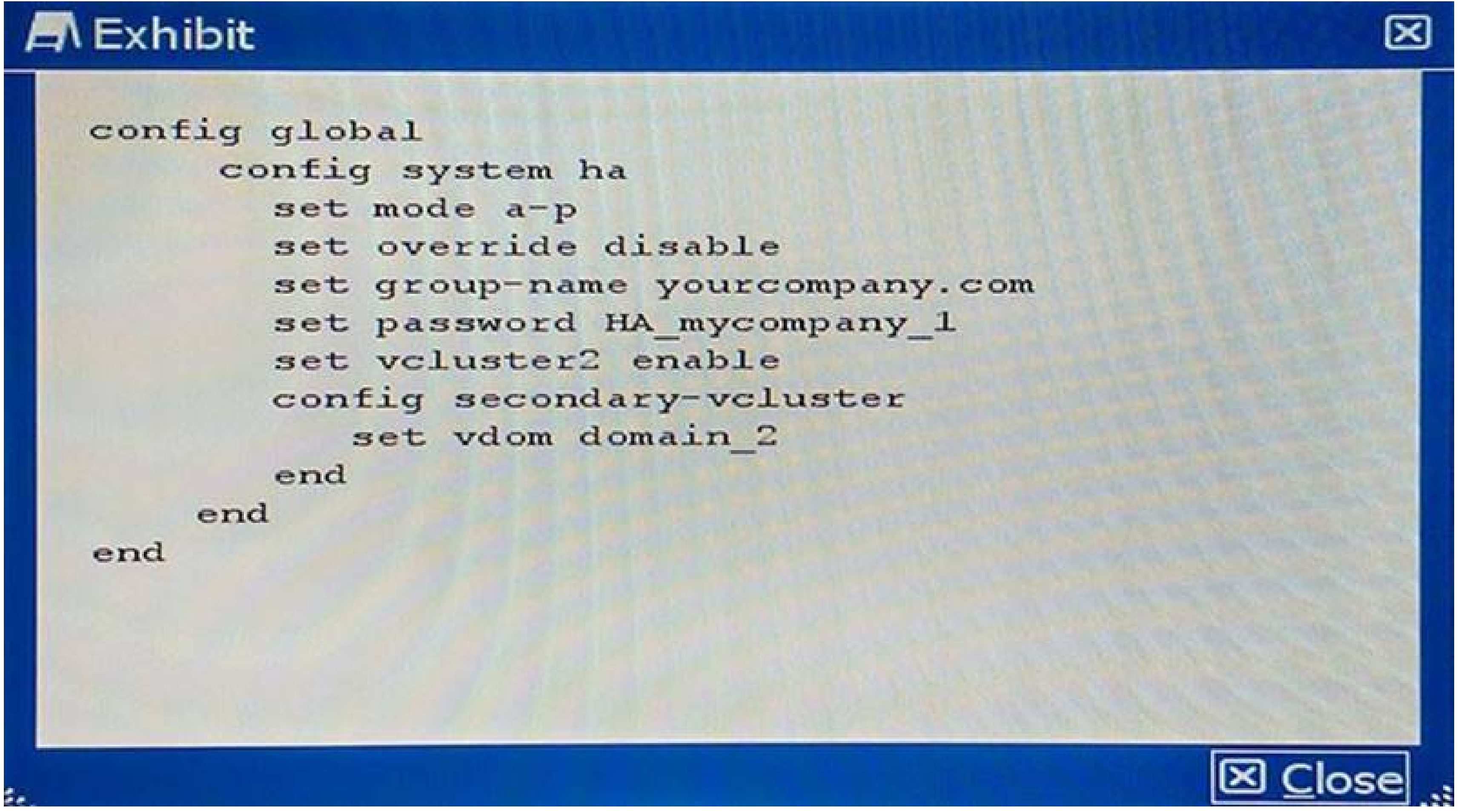
Answer: CDE

NEW QUESTION 55
You are asked to design a secure solution using Fortinet products for a company. The company recently has Web servers that were exploited and defaced. The customer has also experienced Denial or Service due to SYN Flood attacks. Taking this into consideration, the customer's solution should have the following requirements:
- management requires network-based content filtering with man-in-the-middle inspection
- the customer has no existing public key infrastructure but requires centralized certificate management
- users are tracked by their active directory username without installing any software on their hosts
- Web servers that have been exploited need to be protected from the OWASP Top 10
- notification of high volume SYN Flood attacks when a threshold has been triggered Which three solutions satisfy these requirements? (Choose three.)

A. FortiGate
B. FortiClient
C. FortiWeb
D. FortiAuthenticator
E. FortiDDOS

Answer: ACE

NEW QUESTION 60
Your colleague has enabled virtual clustering to load balance traffic between the cluster units. You notice that all traffic is currently directed to a single FortiGate unit. Your colleague has applied the configuration shown in the exhibit.



```
config global
    config system ha
        set mode a-p
        set override disable
        set group-name yourcompany.com
        set password HA_mycompany_1
        set vcluster2 enable
        config secondary-vcluster
            set vdom domain_2
        end
    end
end
```

Which step would you perform to load balance traffic within the virtual cluster?

A. Issue the diagnose sys ha reset-uptime command on the unit that is currently processing traffic to enable load balancing.
B. Add an additional virtual cluster high-availability link to enable cluster load balancing.
C. Input Virtual Cluster domain 1 and Virtual Cluster domain 2 device priorities for each cluster unit.
D. Use the set override enable command on both units to allow the secondary unit to load balance traffic.

Answer: C

Explanation: References:

NEW QUESTION 62
Which three configuration scenarios will result in an IPsec negotiation failure between two FortiGate devices? (Choose three.)

A. mismatched phase 2 selectors
B. mismatched Anti-Replay configuration
C. mismatched Perfect Forward Secrecy
D. failed Dead Peer Detection negotiation
E. mismatched IKE version

Answer: ACE

Explanation: In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key. Either enable or disable PFS on both the tunnel peers; otherwise, the LAN-to-LAN (L2L) IPsec tunnel is not established

NEW QUESTION 63
You have received an issue report about users not being able to use a video conferencing application. This application uses two UDP ports and two TCP ports to communicate with servers on the Internet. The network engineering team has confirmed there is no routing problem. You are given a copy of the FortiGate configuration.
Which three configuration objects will you inspect to ensure that no policy is blocking this traffic? (Choose three.)

A. config firewall interface-policy
B. config firewall DoS-policy
C. config firewall policy
D. config firewall multicast-policy
E. config firewall sniffer-policy

Answer: BCE

NEW QUESTION 68
You have deployed two FortiGate devices as an HA pair. One FortiGate will process traffic while the other FortiGate is a standby. The standby monitors the primary for failure and only takes the role of processing traffic if it detects that the primary FortiGate has failed.
Which style of FortiGate HA does this scenario describe?

A. active-passive HA
B. active-active HA
C. partial mesh HA
D. full mesh HA

Answer: A

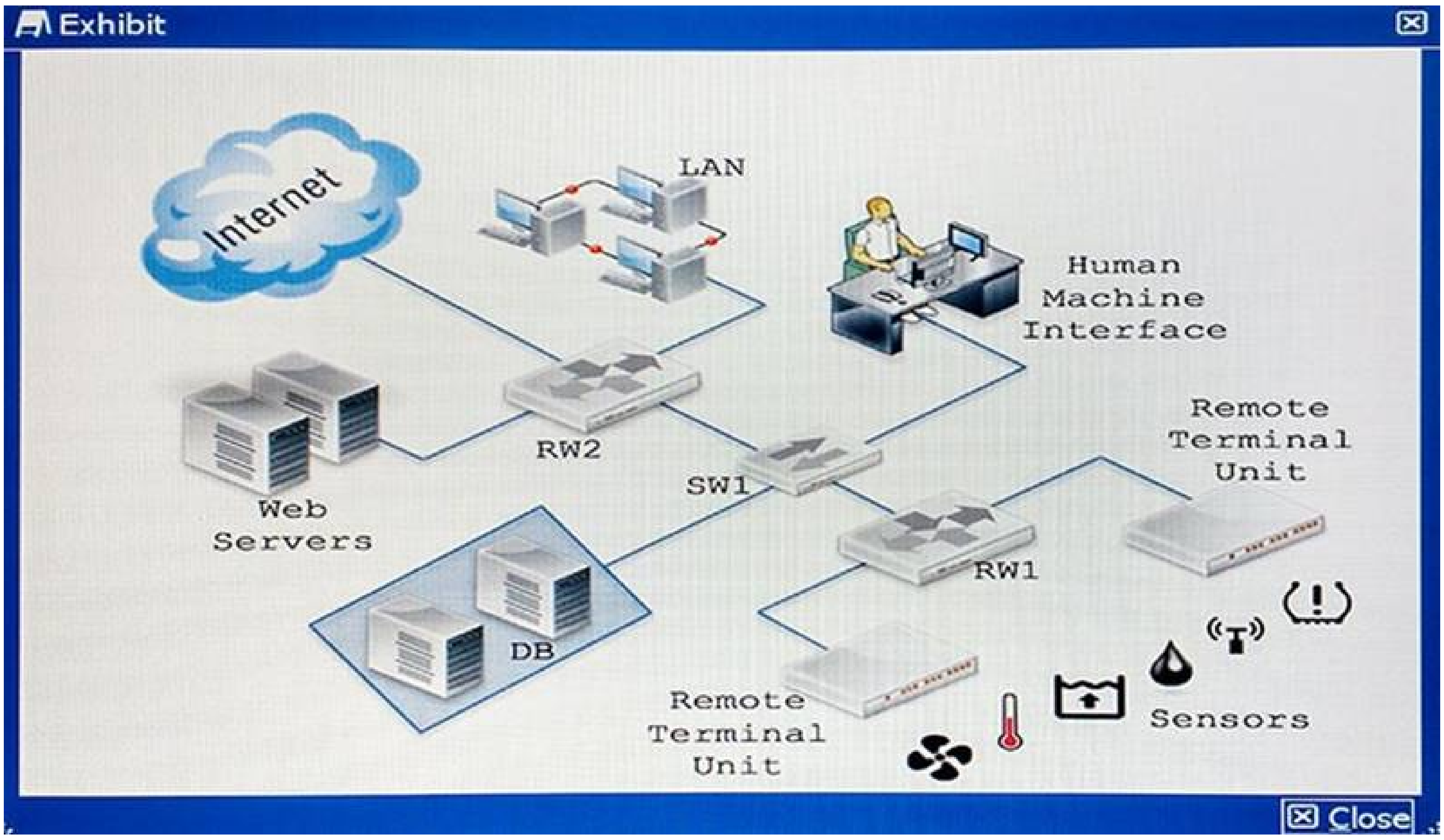
NEW QUESTION 69
You are hosting Web applications that must be PCI DSS compliant. The Web applications are protected by a FortiWeb. Compliance will be tested during the quarterly security review.
In this scenario, which three FortiWeb features should you use? (Choose three.)

A. Vulnerability Scan
B. Auto-learning
C. Syn Cookie
D. Credit Card Detection
E. the command.

Answer: ACD

Explanation: References:
http://help.fortinet.com/fweb/551/Content/FortiWeb/fortiweb-admin/web_protection.htm

NEW QUESTION 70
How would you apply security to the network shown in the exhibit?



A. Replace RW1 with a ruggedized FortiGate and RW2 with a normal FortiGat
B. Enable industrial category on the application contro
C. Place a FortiGate to secure Web server
D. Configure IPsec to secure sensors dat
E. Place a ruggedized FortiAP to provide Wi-Fi to the sensors.
F. Replace RW1 with a normal FortiGate and RW2 with a ruggedized FortiGat
G. Enable industrial category on the application contro
H. Place a FortiGate to secure Web server
I. Configure IPsec to secure sensors dat
J. Place a FortiAP to provide Wi-Fi to the sensors.
K. Replace RW1 with a normal FortiGate and RW2 with a ruggedized FortiGat
L. Enable industrial category on the Web filte
M. Place a FortiWeb to secure Web server
N. Configure IPsec to secure sensors dat
O. Place a ruggedized FortiAP to provide Wi-Fi to the sensors.
P. Replace RW1 with a normal FortiGate and RW2 with a ruggedized FortiGat
Q. Enable industrial category on the application contro
R. Place a FortiWeb to secure Web server
S. Configure IPsec to secure sensors dat
T. Place a ruggedized FortiAP to provide Wi-Fi to the sensors.

Answer: D

NEW QUESTION 75
A university is looking for a solution with the following requirements:
- wired and wireless connectivity
- authentication (LDAP)
- Web filtering, DLP and application control
- data base integration using LDAP to provide access to those students who are up-to-date with their monthly payments
- support for an external captive portal Which solution meets these requirements?

A. FortiGate for wireless controller and captive portalFortiAP for wireless connectivityFortiAuthenticator for user authentication and REST API for DB integrationFortiSwitch for PoE connectivityFortiAnalyzer for log and report
B. FortiGate for wireless controllerFortiAP for wireless connectivityFortiAuthenticator for user authentication, captive portal and REST API for DB integrationFortiSwitch for PoE connectivityFortiAnalyzer for log and report
C. FortiGate for wireless control and user authenticationFortiAuthenticator for captive portal and REST API for DB integrationFortiAP for wireless connectivityFortiSwitch for PoE connectivityFortiAnalyzer for log and report
D. FortiGate for wireless controllerFortiAP for wireless connectivity and captive portalFortiSwitch for PoE connectivityFortiAuthenticator for user authentication and REST API for DB integrationFortiAnalyzer for log and reports

Answer: A

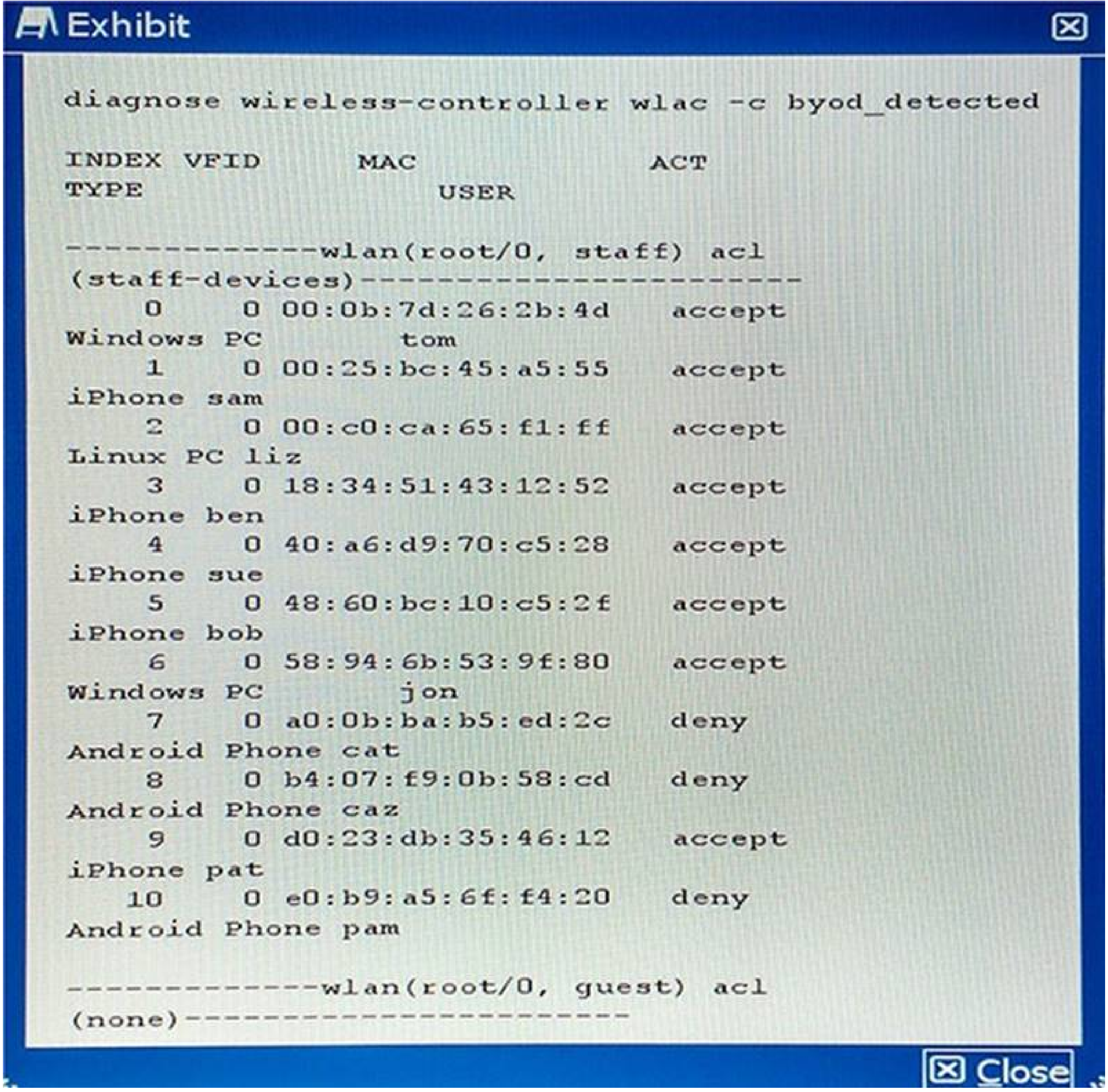
NEW QUESTION 79
You notice that memory usage is high and FortiGate has entered conserve mode. You want FortiGate's IPS engine to focus only on exploits and attacks that are applicable to your specific network.
Which two steps would you take to reduce RAM usage without weakening security? (Choose two.)

A. Configure IPS to pass files that are larger than a specific threshold, instead of buffering and scanning them.
B. Reduce the size of the signature three (filters) that FortiGate must search by disabling scans for applications and OS stacks that do not exist on your network.
C. Disable application control for protocols that are not used on your network.

D. Disable IPS for traffic destined for the FortiGate itself.

Answer: BD

NEW QUESTION 84
The wireless controller diagnostic output is shown in the exhibit. Which three statements are true? (Choose three.)



```
diagnose wireless-controller wlac -c byod_detected

INDEX VFID        MAC                ACT
TYPE                    USER

-------------wlan(root/0, staff) acl
(staff-devices)-----------------------
    0     0 00:0b:7d:26:2b:4d    accept
Windows PC        tom
    1     0 00:25:bc:45:a5:55    accept
iPhone sam
    2     0 00:c0:ca:65:f1:ff    accept
Linux PC liz
    3     0 18:34:51:43:12:52    accept
iPhone ben
    4     0 40:a6:d9:70:c5:28    accept
iPhone sue
    5     0 48:60:bc:10:c5:2f    accept
iPhone bob
    6     0 58:94:6b:53:9f:80    accept
Windows PC        jon
    7     0 a0:0b:ba:b5:ed:2c    deny
Android Phone cat
    8     0 b4:07:f9:0b:58:cd    deny
Android Phone caz
    9     0 d0:23:db:35:46:12    accept
iPhone pat
   10     0 e0:b9:a5:6f:f4:20    deny
Android Phone pam

-------------wlan(root/0, guest) acl
(none)-----------------------
```

A. Firewall policies using device types are blocking Android devices.
B. An access control list applied to the VAP interface blocks Android devices.
C. This is a CAPWAP control channel diagnostic command.
D. There are no wireless clients connected to the guest wireless network.
E. The “src-vis” process is active on the staff wireless network VAP interface.

Answer: ACD

Explanation: References:
http://docs.fortinet.com/uploaded/files/1083/fortigate-managing-devices-50.pdf

NEW QUESTION 87
A FortiGate is deployed in the NAT/Route operation mode. This operation mode operates at which OSI layer?

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

Answer: C

NEW QUESTION 91
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE8 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE8 Product From:

https://www.2passeasy.com/dumps/NSE8/

Money Back Guarantee

NSE8 Practice Exam Features:

* NSE8 Questions and Answers Updated Frequently

* NSE8 Practice Questions Verified by Expert Senior Certified Staff

* NSE8 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE8 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year