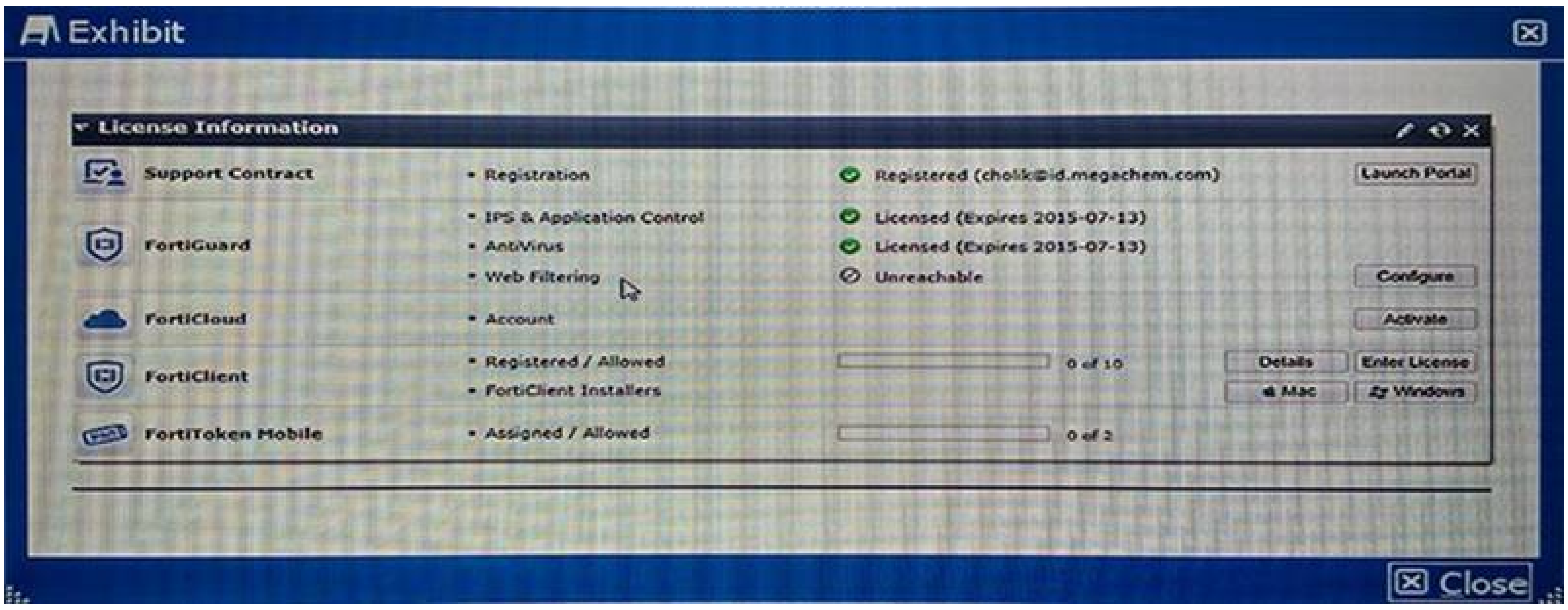
Fortinet

Exam Questions NSE8

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.



Support Contract	• Registration	Registered (cholk@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

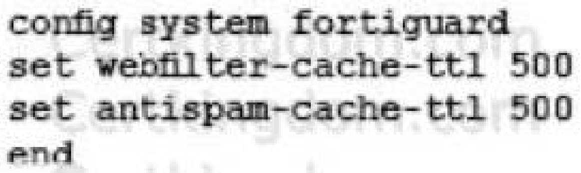
Explanation: If Web filtering shows unreachable then we have to verify, whether web filtering enabled in security policies or not.
Web filtering enabled in a policy but the port 8888 and 53 are not selected, means the policy blocking the ports.
References:

NEW QUESTION 2
A customer has the following requirements:
- local peer with two Internet links
- remote peer with one Internet link
- secure traffic between the two peers
- granular control with Accept policies
Which solution provides security and redundancy for traffic between the two peers?

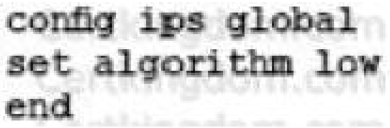
A. a fully redundant VPN with interface mode configuration
B. a partially redundant VPN with interface mode configuration
C. a partially redundant VPN with tunnel mode configuration
D. a fully redundant VPN with tunnel mode configuration

Answer: B

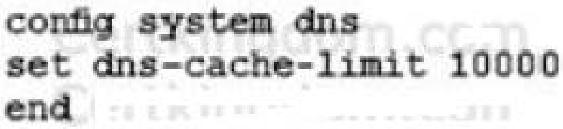
NEW QUESTION 3
You notice that your FortiGate's memory usage is very high and that the unit's performance is adversely affected. You want to reduce memory usage.
Which three commands would meet this requirement? (Choose three.)

A.


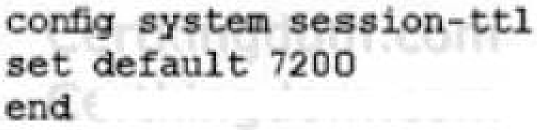
```
config system fortiguard
set webfilter-cache-ttl 500
set antispam-cache-ttl 500
end
```

B.


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

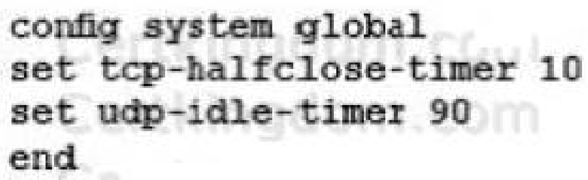
C.


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

D.


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

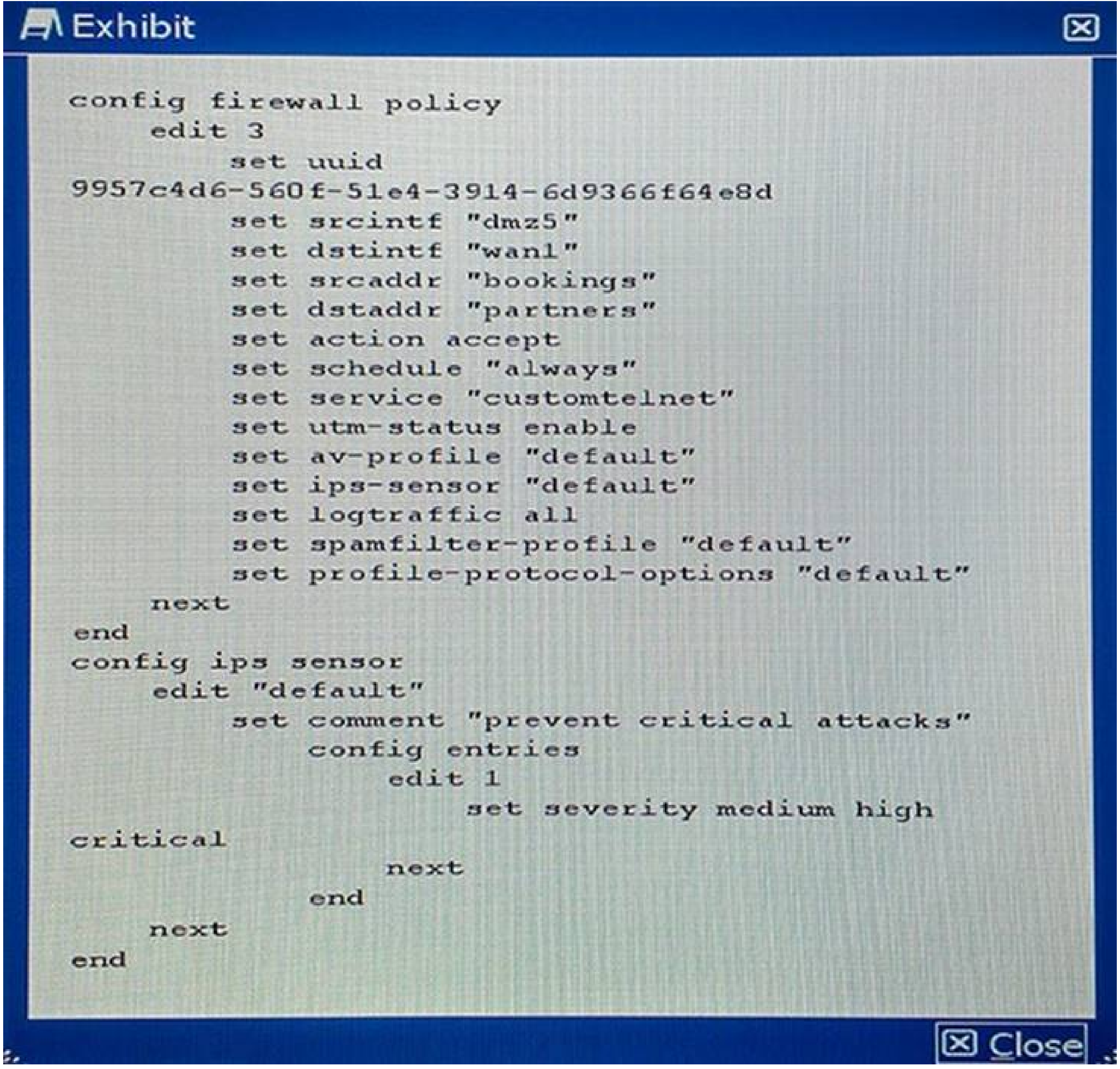
E.



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

Answer: ADE

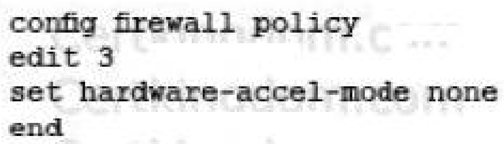
NEW QUESTION 4
Your NOC contracts the security team due to a problem with a new application flow. You are instructed to disable hardware acceleration for the policy shown in the exhibit for troubleshooting purposes.



```
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
```

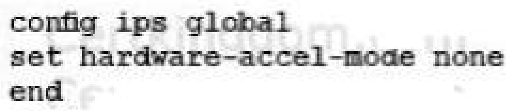
Which command will disable hardware acceleration for the new application policy?

A.



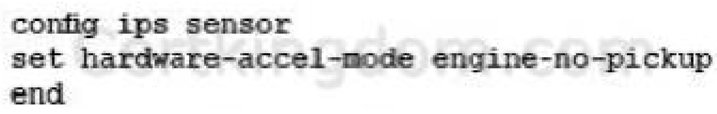
```
config firewall policy
edit 3
set hardware-accel-mode none
end
```

B.



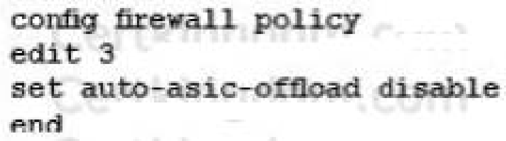
```
config ips global
set hardware-accel-mode none
end
```

C.



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

D.

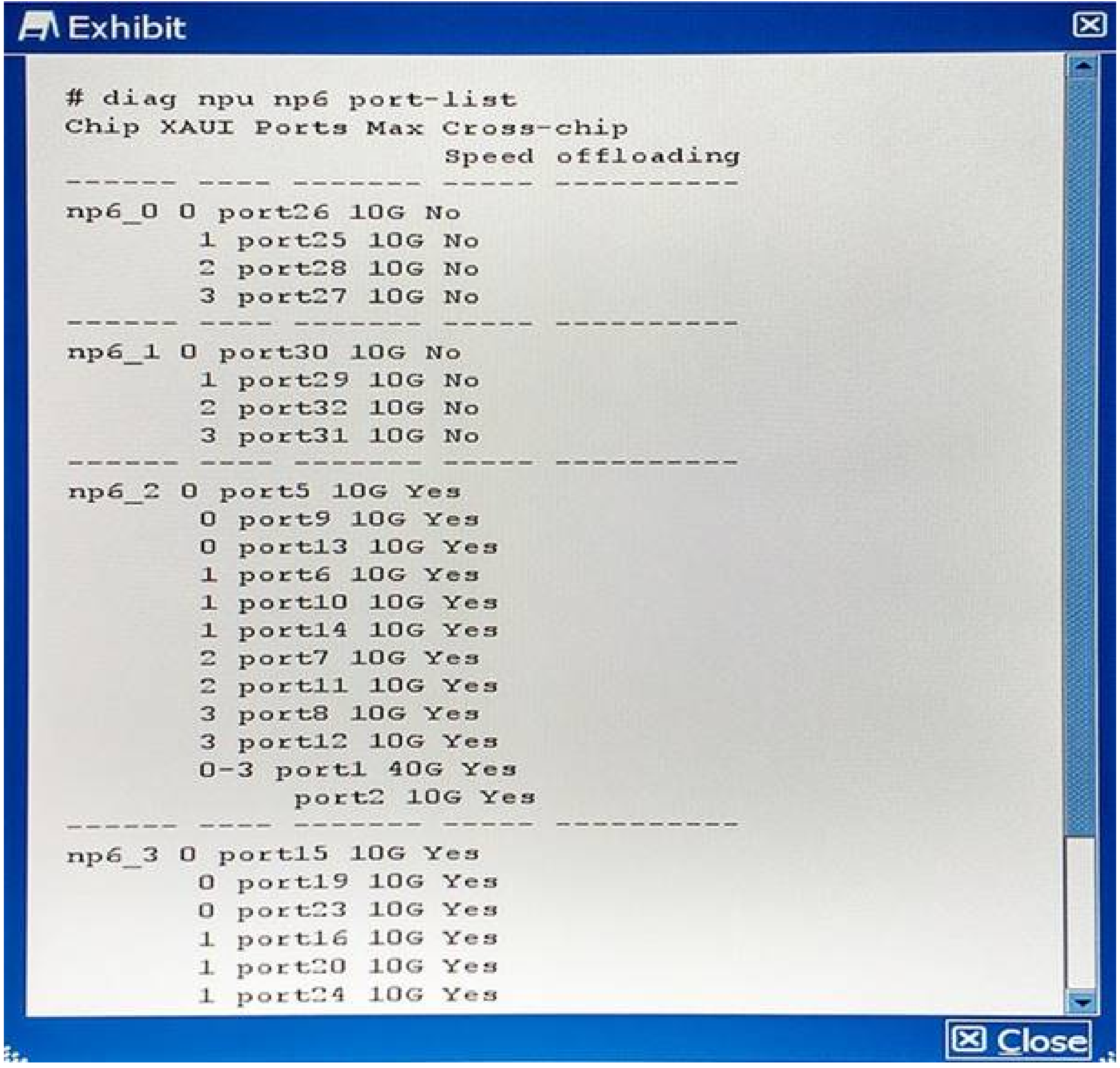


```
config firewall policy
edit 3
set auto-asic-offload disable
end
```

Answer: D

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

NEW QUESTION 5
Referring to the exhibit, you want to know if aggregating port7 and port22 will work. Which statement is correct?



```
# diag npu np6 port-list
Chip XAUI Ports Max Cross-chip
                Speed offloading
------ ---- ------- ----- ----------
np6_0  0    port26  10G   No
       1    port25  10G   No
       2    port28  10G   No
       3    port27  10G   No
------ ---- ------- ----- ----------
np6_1  0    port30  10G   No
       1    port29  10G   No
       2    port32  10G   No
       3    port31  10G   No
------ ---- ------- ----- ----------
np6_2  0    port5   10G   Yes
       0    port9   10G   Yes
       0    port13  10G   Yes
       1    port6   10G   Yes
       1    port10  10G   Yes
       1    port14  10G   Yes
       2    port7   10G   Yes
       2    port11  10G   Yes
       3    port8   10G   Yes
       3    port12  10G   Yes
       0-3  port1   40G   Yes
            port2   10G   Yes
------ ---- ------- ----- ----------
np6_3  0    port15  10G   Yes
       0    port19  10G   Yes
       0    port23  10G   Yes
       1    port16  10G   Yes
       1    port20  10G   Yes
       1    port24  10G   Yes
```

A. Yes, LACP is supported on all ports regardless if they are connected to the same NP6.
B. No, LACP is not supported on NP6 platforms.
C. No, LACP is only supported on ports connected to the same NP6.
D. Yes, LACP is supported on ports that are linked together with integrated Switch Fabric.

Answer: C

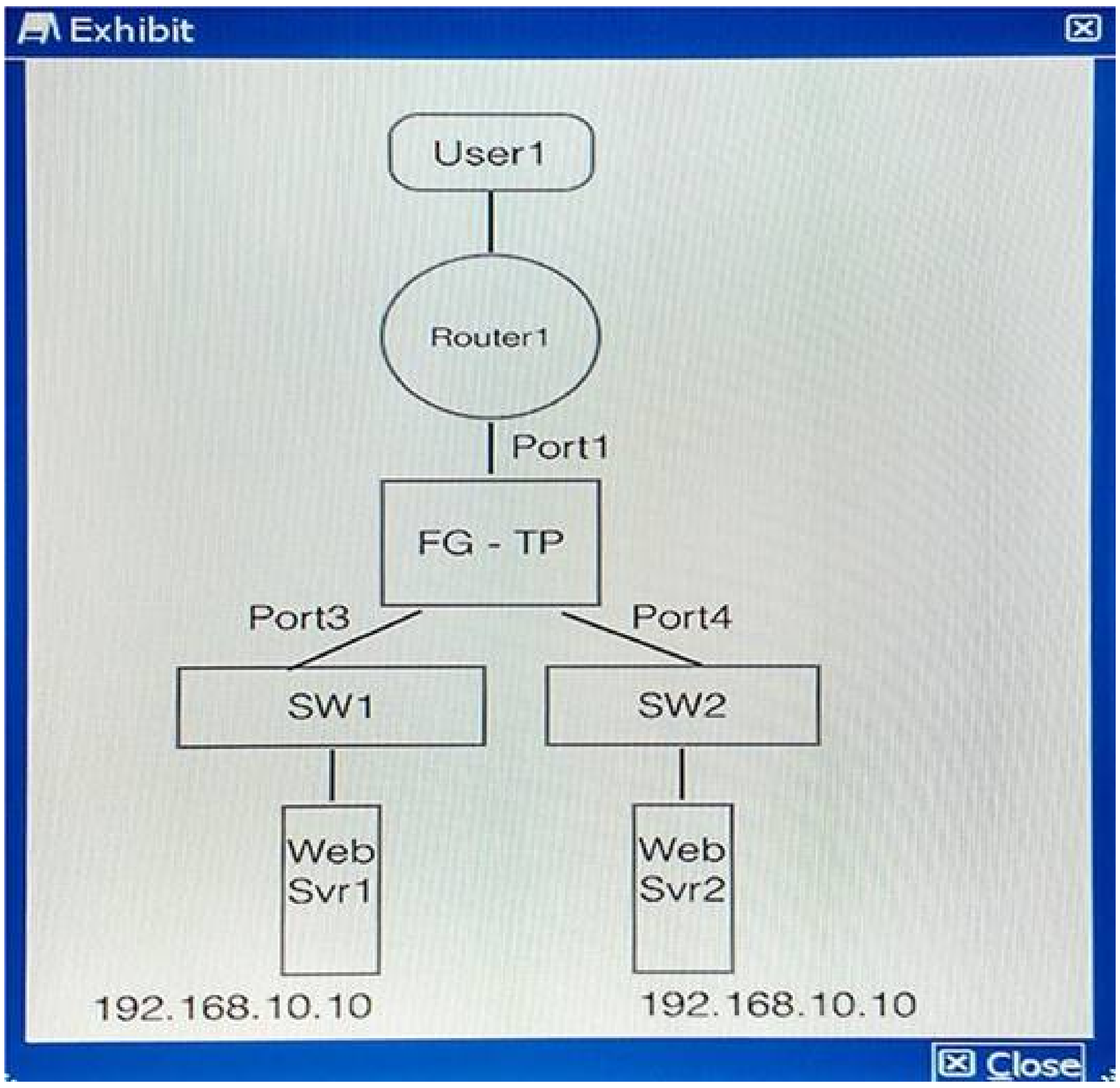
Explanation: References:
http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-hardware-acceleration- 52/NP6.htm

NEW QUESTION 6
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 7
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.



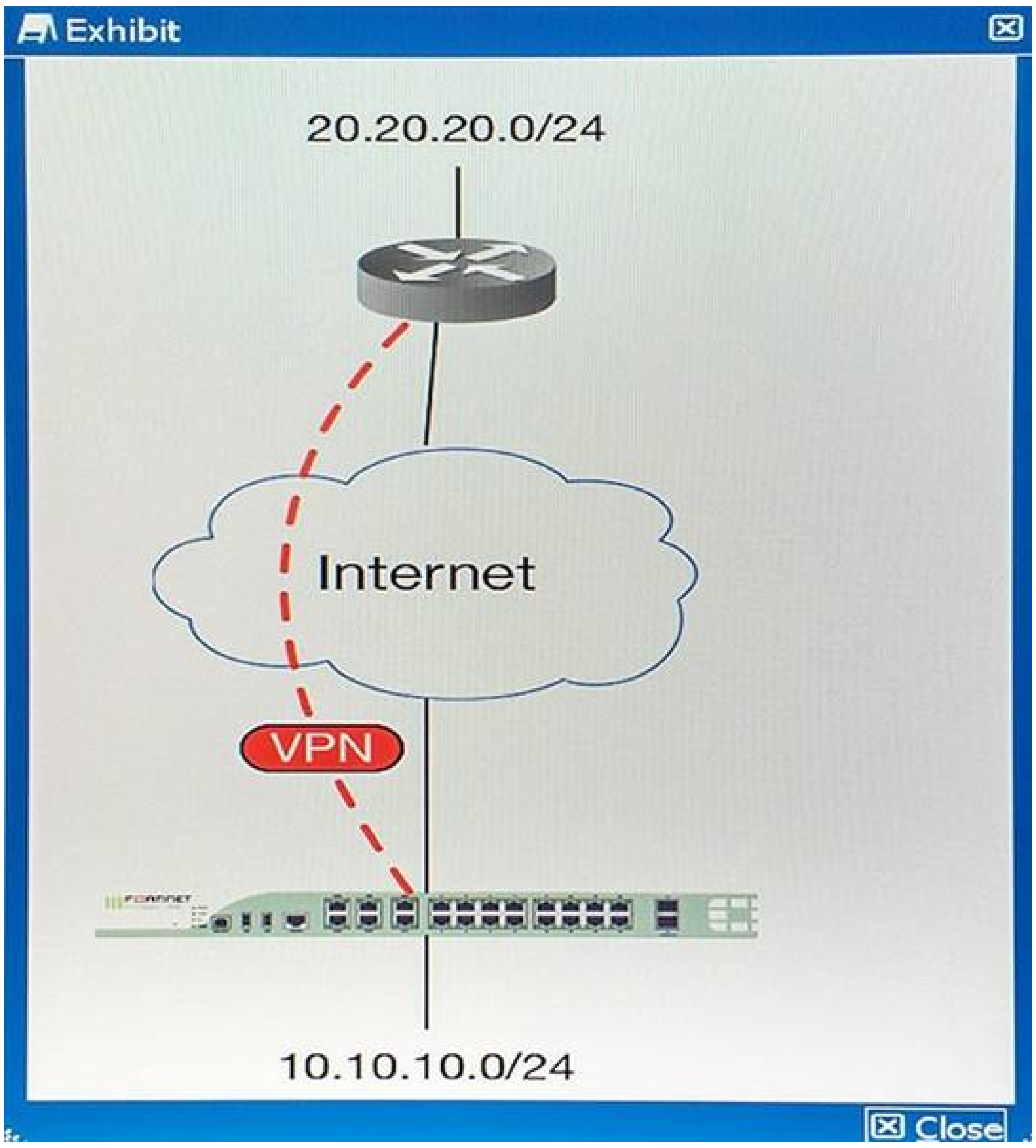
Which two statements about this scenario are true? (Choose two.)

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 8
You are asked to establish a VPN tunnel with a service provider using a third-party VPN device. The service provider has assigned subnet 30.30.30.0/24 for your outgoing traffic going towards the services hosted by the provider on network 20.20.20.0/24. You have multiple computers which will be accessing the remote services hosted by the service provider.

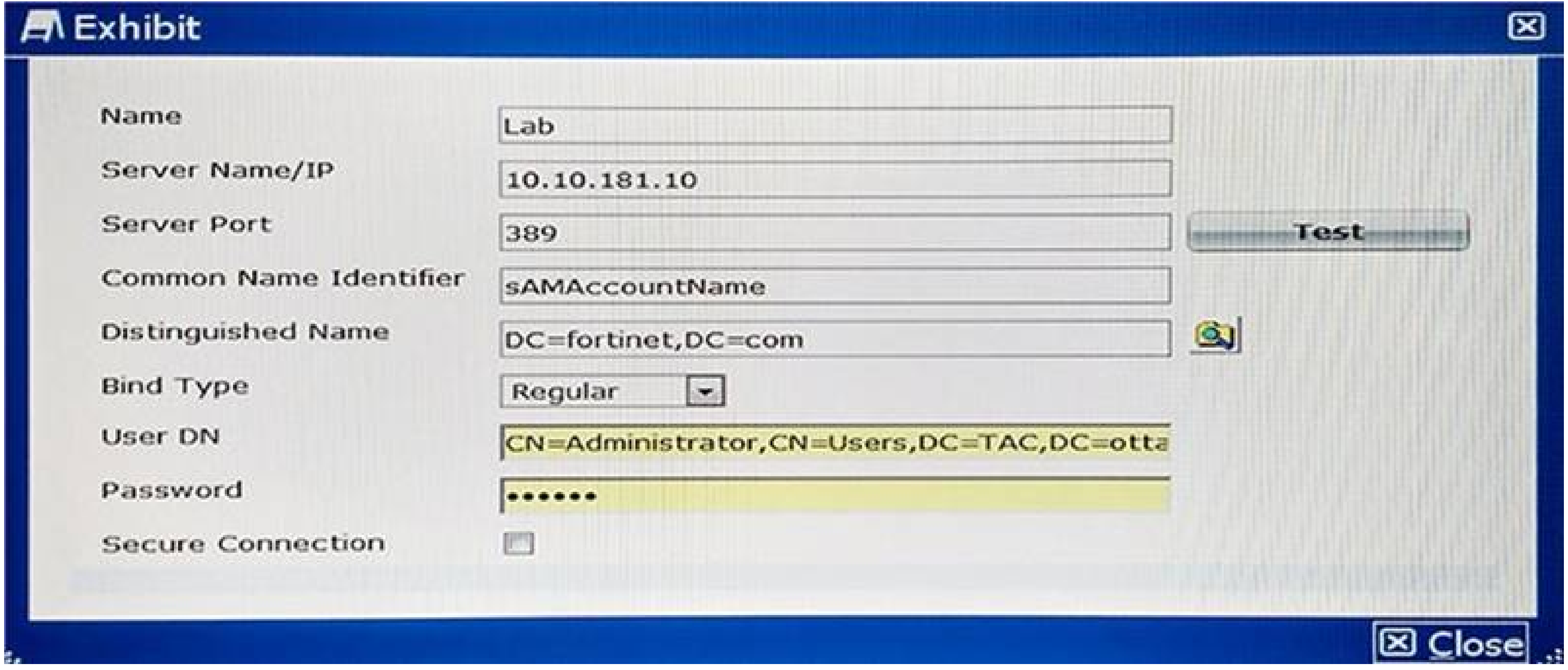


Which three configuration components meet these requirements? (Choose three.)

A. Configure an IP Pool of type Overload for range 30.30.30.10-30.30.30.10. Enable NAT on a policy from your LAN forwards the VPN tunnel and select that pool.
B. Configure IPsec phase 2 proxy IDs for a source of 10.10.10.0/24 and destination of 20.20.20.0/24.
C. Configure an IP Pool of Type One-to-One for range 30.30.30.10-30.30.30.10. Enable NAT on a policy from your LAN towards the VPN tunnel and select that pool.
D. Configure a static route towards the VPN tunnel for 20.20.20.0/24.
E. Configure IPsec phase 2 proxy IDs for a source of 30.30.30.0/24 and destination of 20.20.20.0/24.

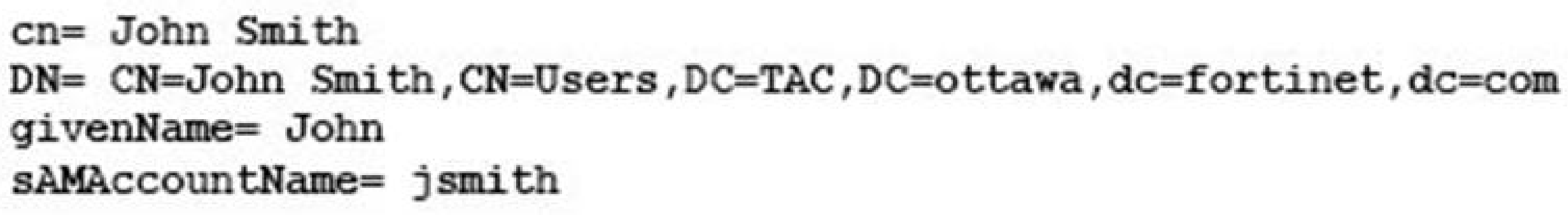
Answer: CDE

NEW QUESTION 9
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
A customer wants to install a FortiSandbox device to identify suspicious files received by an e-mail server. All the incoming e-mail traffic to the e-mail server uses the SMTPS protocol.
Which three solutions would be implemented? (Choose three.)

A. FortiGate device in transparent mode sending the suspicious files to the FortiSandbox
B. FortiSandbox in sniffer input mode
C. FortiMail device in gateway mode using the built-in MTA and sending the suspicious files to the FortiSandbox
D. FortiMail device in transparent mode acting as an SMTP proxy sending the suspicious files to the FortiSandbox
E. FortiGate device in NAT mode sending the suspicious files to the FortiSandbox

Answer: BCE

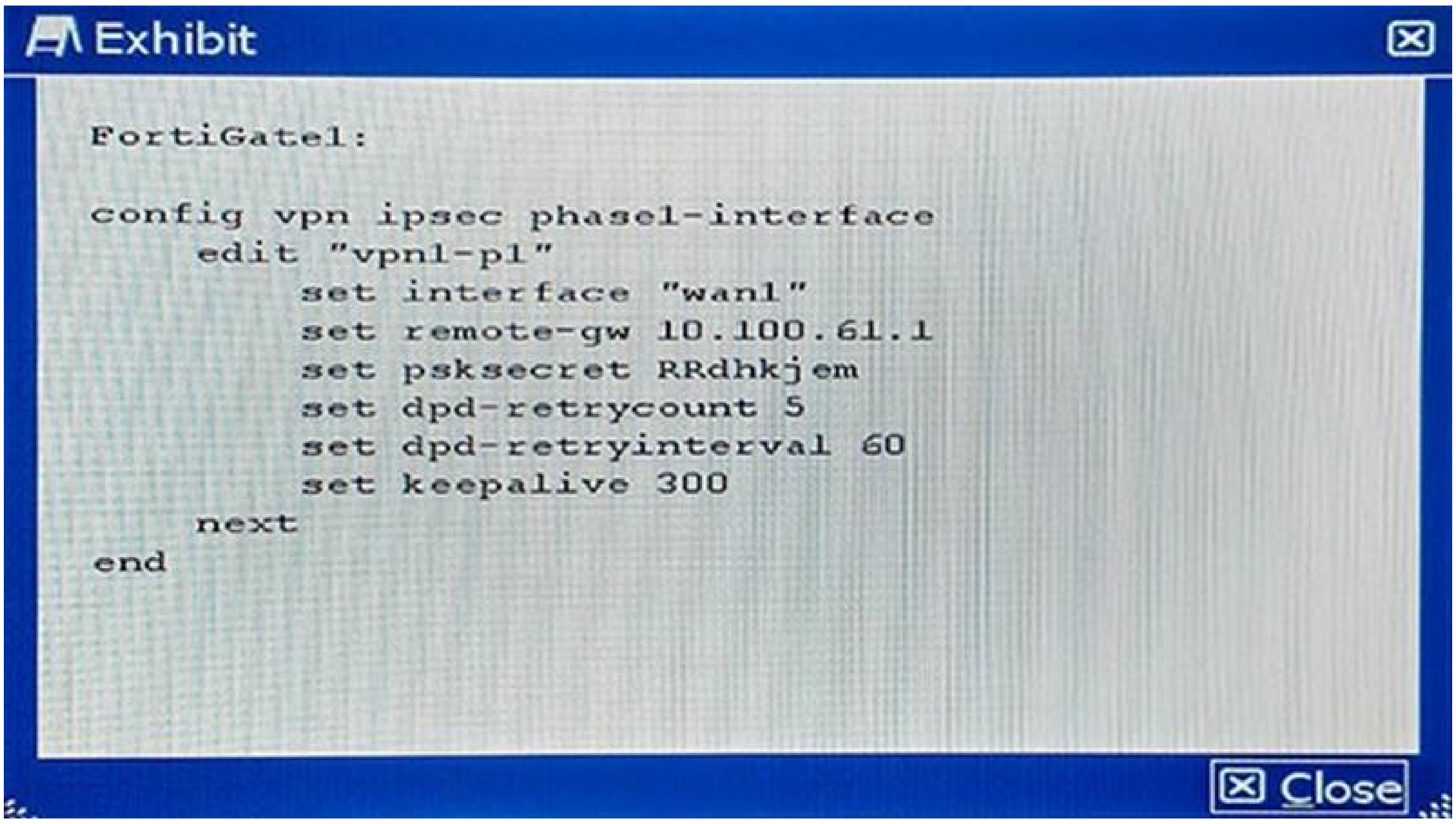
Explanation: References: http://kb.fortinet.com/kb/documentLink.do?externalID=FD34371

NEW QUESTION 10
Which Fortinet product is used for antispam protection?

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

Answer: B

NEW QUESTION 15
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

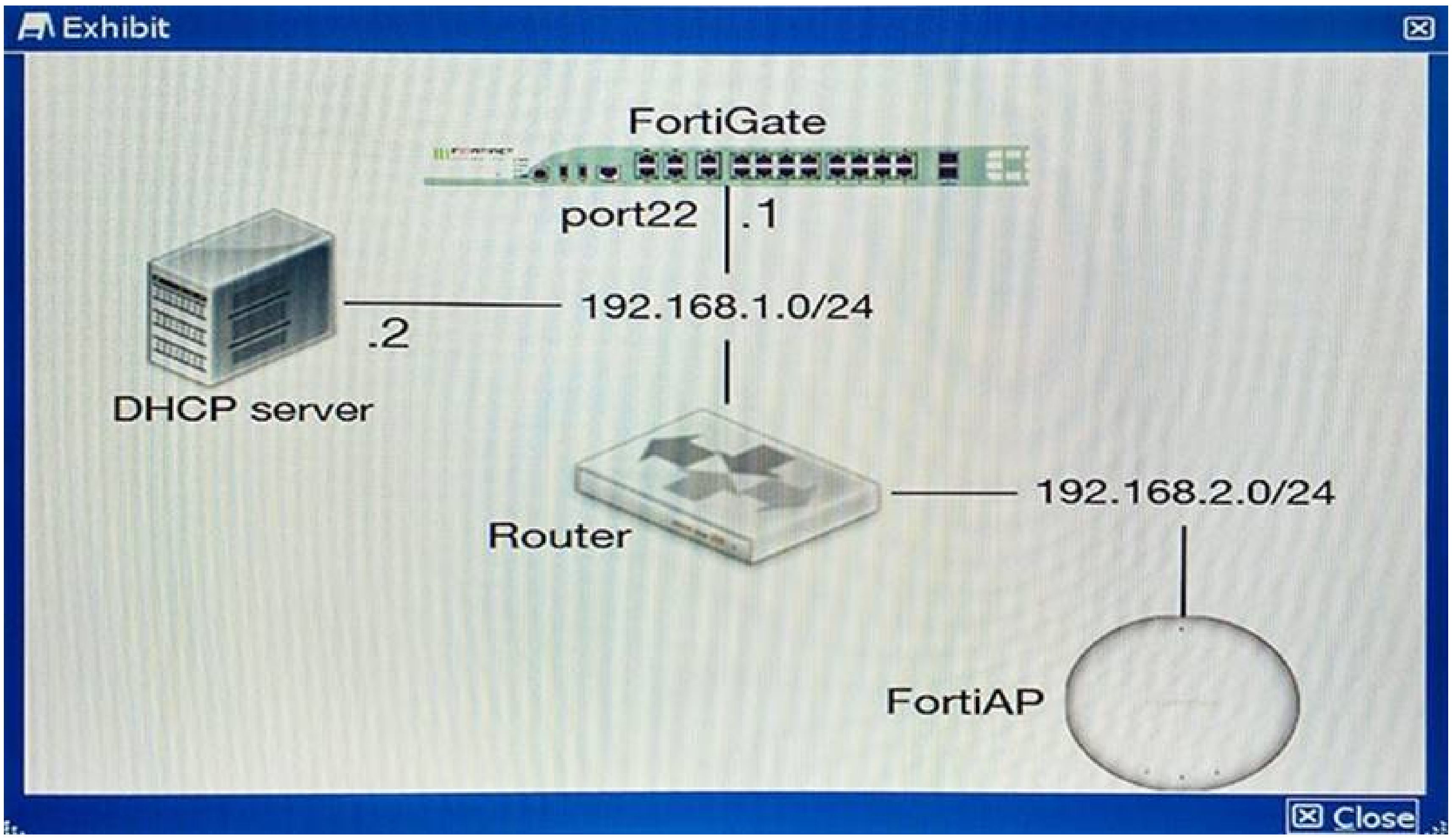
Explanation: References: http://kb.fortinet.com/kb/documentLink.do?externalID=FD35337

NEW QUESTION 17
You are asked to implement a wireless network for a conference center and need to provision a high number of access points to support a large number of wireless client
connections.
Which statement describes a valid solution for this requirement?

A. Use a captive portal for guest acces
B. Use both 2.4 GHz and 5 GHz band
C. Enable frequency and access point hand-of
D. Use more channels, thereby supporting more clients.
E. Use an open wireless network with no porta
F. Use both 2.4 GHz and 5 GHz band
G. Use 802.11ac capable access points and configure channel bonding to support greater throughput for wireless clients.
H. Use a pre-shared key only for wireless client securit
I. Use the 5 GHz band only for greater securit
J. Use 802.11ac capable access points and configure channel bonding to support greater throughput for wireless clients.
K. Use a captive portal for guest acces
L. Use both the 2.4 GHz and 5 GHz bands, and configure frequency steerin
M. Configure rogue access point detection in order to automatically control the transmit power of each AP.

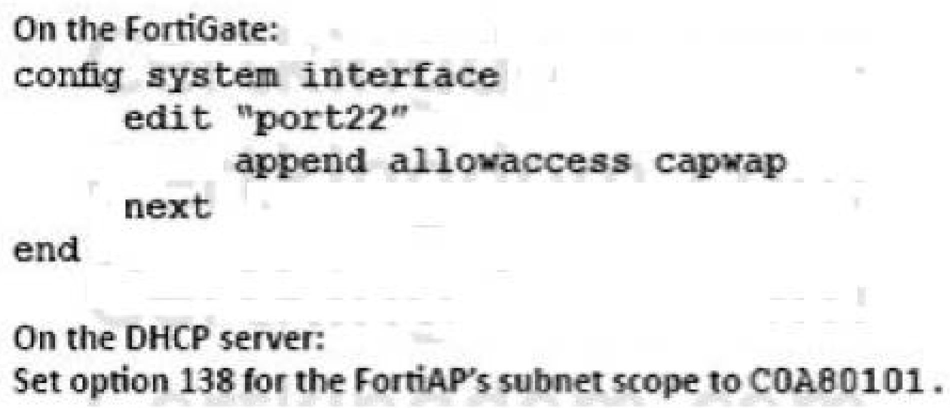
Answer: D

NEW QUESTION 21
You are installing a new FortiAP as shown in the exhibit, however, the FortiAP cannot discover the FortiGate. The FortiAP obtained an IP from the DHCP server and is reachable.



Which two configurations will resolve the problem? (Choose two.)

A.

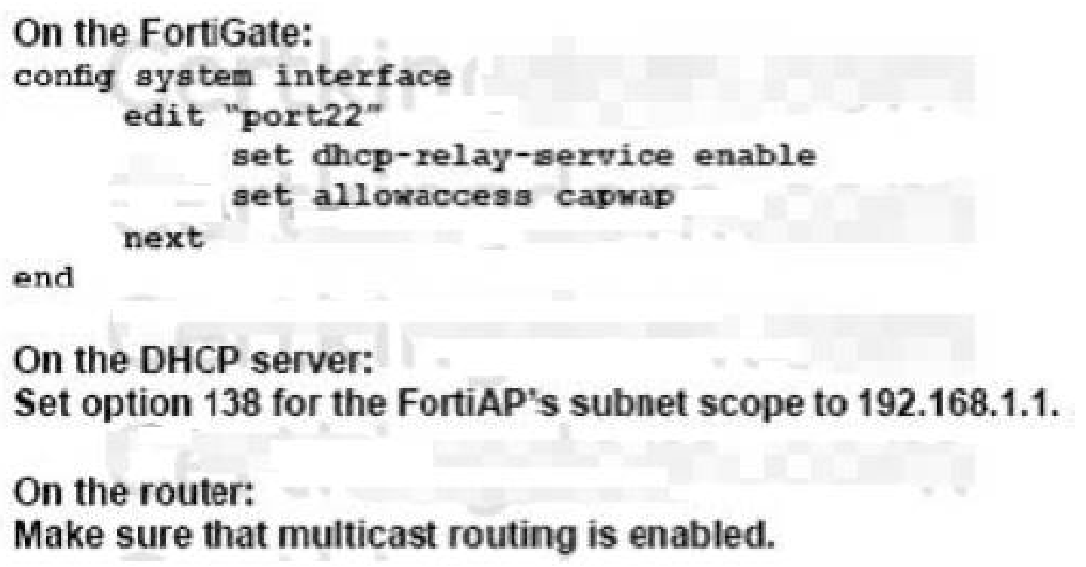


On the FortiGate:

```
config system interface
      edit "port22"
            append allowaccess capwap
      next
end
```

On the DHCP server:
Set option 138 for the FortiAP's subnet scope to C0A80101.

B.



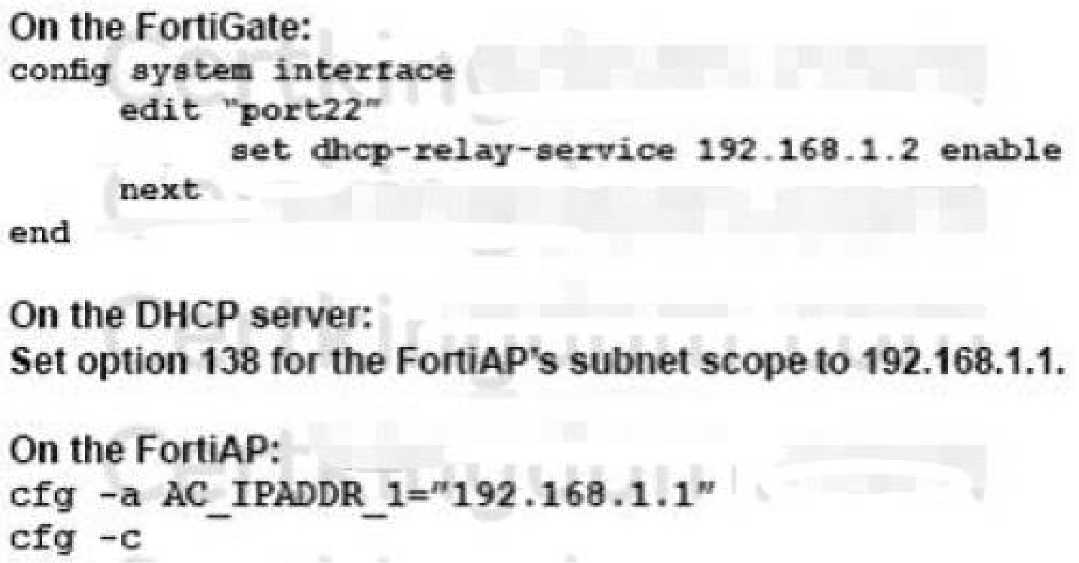
On the FortiGate:

```
config system interface
      edit "port22"
            set dhcp-relay-service enable
            set allowaccess capwap
      next
end
```

On the DHCP server:
Set option 138 for the FortiAP's subnet scope to 192.168.1.1.

On the router:
Make sure that multicast routing is enabled.

C.



On the FortiGate:

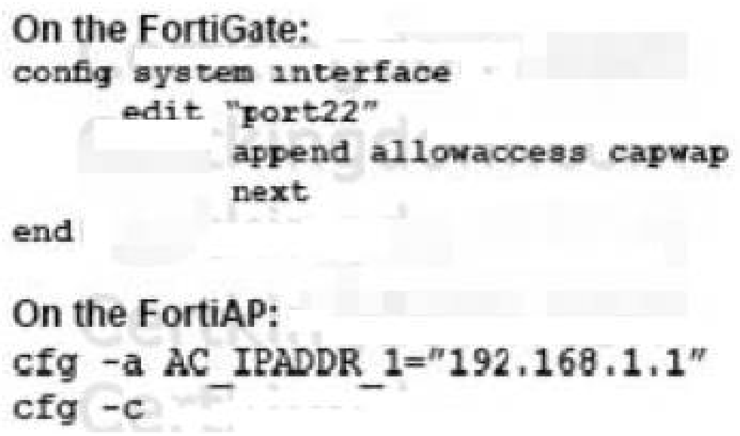
```
config system interface
      edit "port22"
            set dhcp-relay-service 192.168.1.2 enable
      next
end
```

On the DHCP server:
Set option 138 for the FortiAP's subnet scope to 192.168.1.1.

On the FortiAP:

```
cfg -a AC_IPADDR_1="192.168.1.1"
cfg -c
```

D.



On the FortiGate:

```
config system interface
      edit "port22"
            append allowaccess capwap
            next
end
```

On the FortiAP:

```
cfg -a AC_IPADDR_1="192.168.1.1"
cfg -c
```

Answer: BD

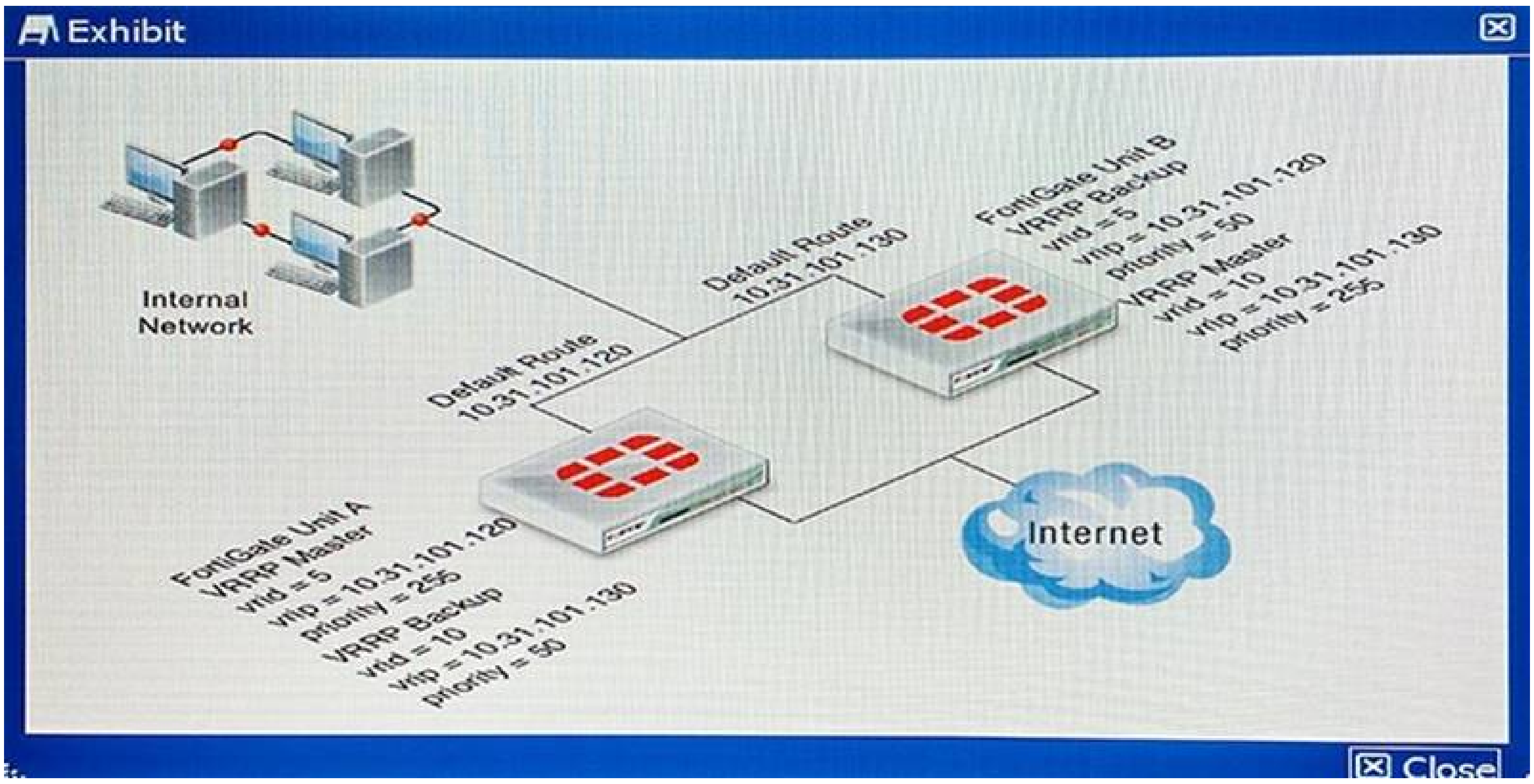
Explanation: https://forum.fortinet.com/tm.aspx?m=112739

NEW QUESTION 22
Which VPN protocol is supported by FortiGate units?

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

Answer: BC

NEW QUESTION 25
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.



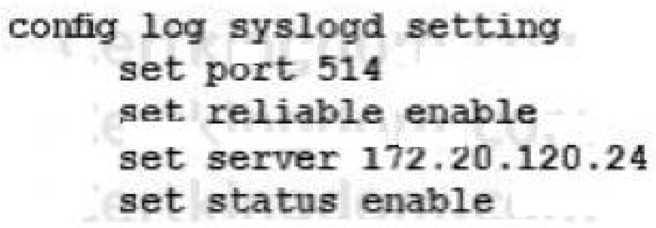
If FortiGate unit A fails, what would happen?

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.

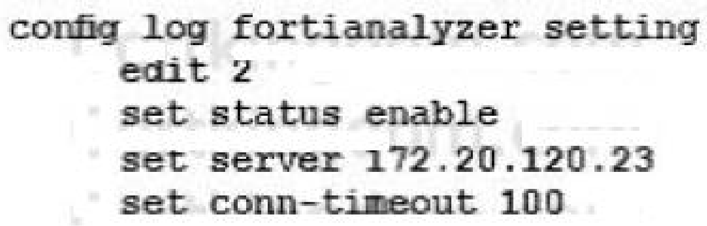
Answer: B

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

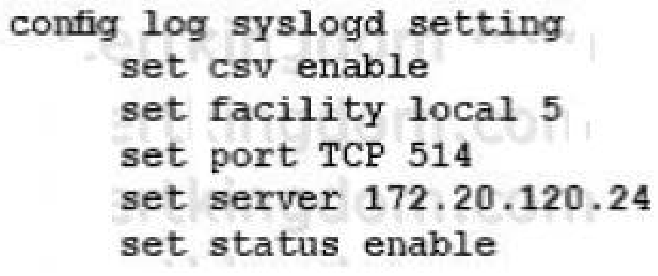
NEW QUESTION 27
The SECOPS team in your company has started a new project to store all logging data in a disaster recovery center. All FortiGates will log to a secondary FortiAnalyzer and establish a TCP session to send logs to the syslog server.
Which two configurations will achieve this goal? (Choose two.)

A.


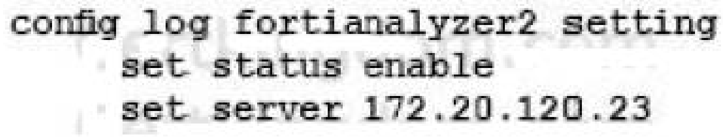
```
config log syslogd setting
       set port 514
       set reliable enable
       set server 172.20.120.24
       set status enable
```

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

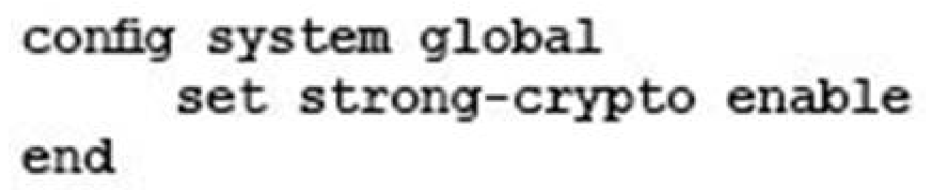
NEW QUESTION 31
There is an interface-mode IPsec tunnel configured between FortiGate1 and FortiGate2. You want to run OSPF over the IPsec tunnel. On both FortiGates. the IPsec tunnel is based on physical interface port1. Port1 has the default MTU setting on both FortiGate units.
Which statement is true 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
Given the following FortiOS 5.2 commands:



```
config system global
      set strong-crypto enable
end
```

Which vulnerability is being addresses when managing FortiGate through an encrypted management protocol?

A. Remote Exploit Vulnerability in Bash (ShellShock)
B. Information Disclosure Vulnerability in OpenSSL (Heartbleed)
C. SSL v3 POODLE Vulnerability
D. SSL/TLS MITM vulnerability (CVE-2014-0224)

Answer: C

Explanation: References: http://kb.fortinet.com/kb/documentLink.do?externalID=FD36913

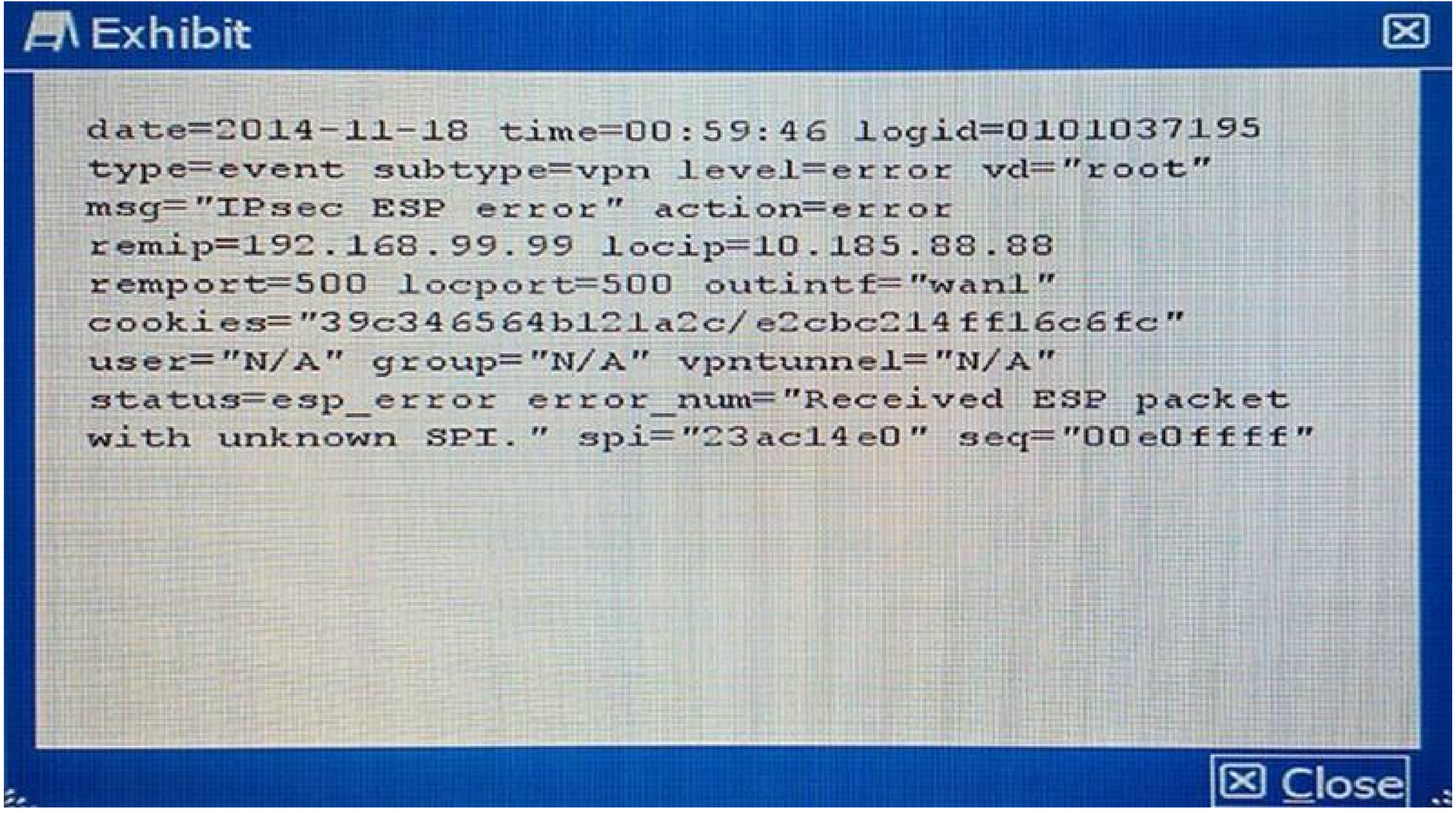
NEW QUESTION 35
You are an administrator of FortiGate devices that use FortiManager for central management. You need to add a policy on an ADOM, but upon selecting the ADOM drop- down list, you notice that the ADOM is in locked state. Workflow mode is enabled on your FortiManager to define approval or notification workflow when creating and installing policy changes.
What caused this problem?

A. Another administrator has locked the ADOM and is currently working on it.
B. There is pending approval waiting from a previous modification.
C. You need to use set workspace-mode workflow on the CLI.
D. You have read-only permission on Workflow Approve in the administrator profile.

Answer: D

Explanation: http://docs.fortinet.com/uploaded/files/2250/FortiManager-5.2.1-Administration-Guide.pdf

NEW QUESTION 39
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 44
Your FortiGate has multiple CPUs. You want to verify the load for each CPU. Which two commands will accomplish this task? (Choose two.)

A. get system performance status
B. diag system mpstat
C. diag system cpu stat
D. diag system top

Answer: AD

Explanation: References: http://kb.fortinet.com/kb/documentLink.do?externalID=13825

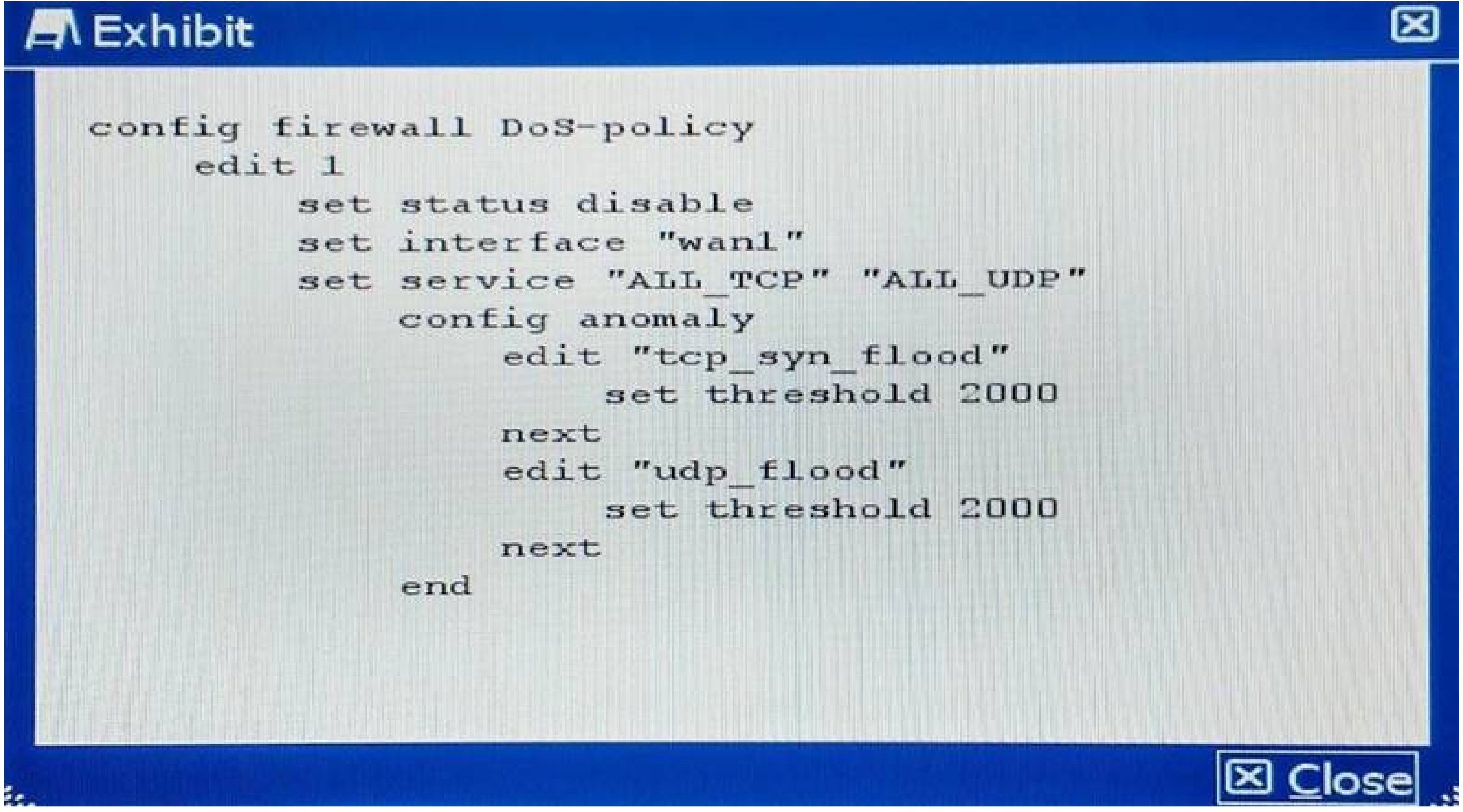
NEW QUESTION 47
You are asked to write a FortiAnalyzer report that lists the session that has consumed the most bandwidth. You are required to include the source IP, destination IP, application, application category, hostname, and total bandwidth consumed.
Which dataset meets these requirements?

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

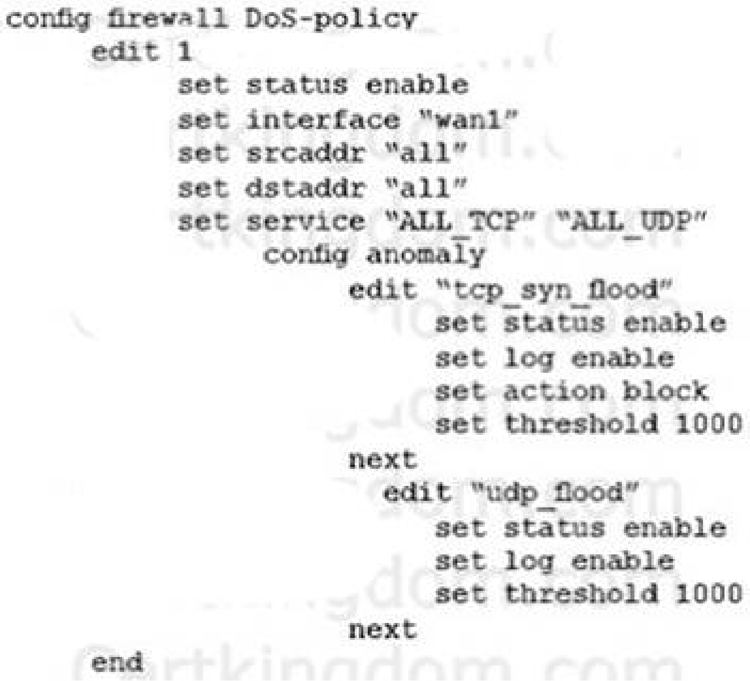
NEW QUESTION 51
A company wants to protect against Denial of Service attacks and has launched a new project. They want to block the attacks that go above a certain threshold and for some others they are just trying to get a baseline of activity for those types of attacks so they are
letting the traffic pass through without action. Given the following:
- The interface to the Internet is on WAN1.
- There is no requirement to specify which addresses are being protected or protected from.
- The protection is to extend to all services.
- The tcp_syn_flood attacks are to be recorded and blocked.
- The udp_flood attacks are to be recorded but not blocked.
- The tcp_syn_flood attack’s threshold is to be changed from the default to 1000. The exhibit shows the current DoS-policy.



```
config firewall DoS-policy
    edit 1
        set status disable
        set interface "wan1"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set threshold 2000
                next
                edit "udp_flood"
                    set threshold 2000
                next
            end
```

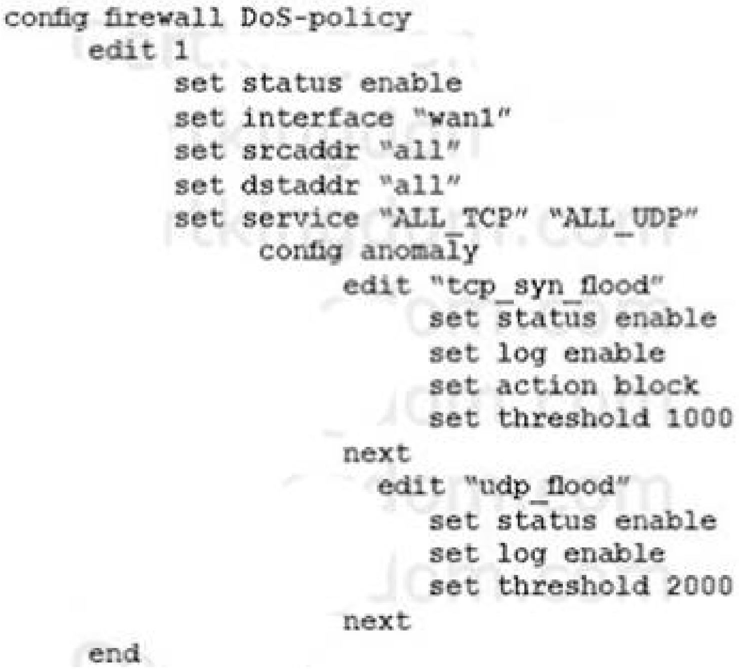
Which policy will implement the project requirements?

A.



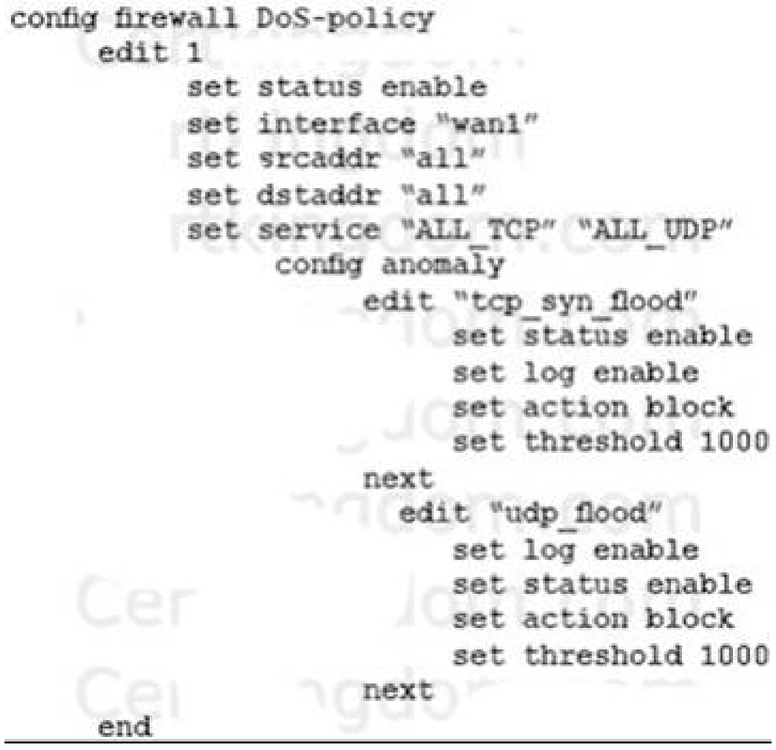
```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set log enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set status enable
                    set log enable
                    set threshold 1000
                next
    end
```

B.



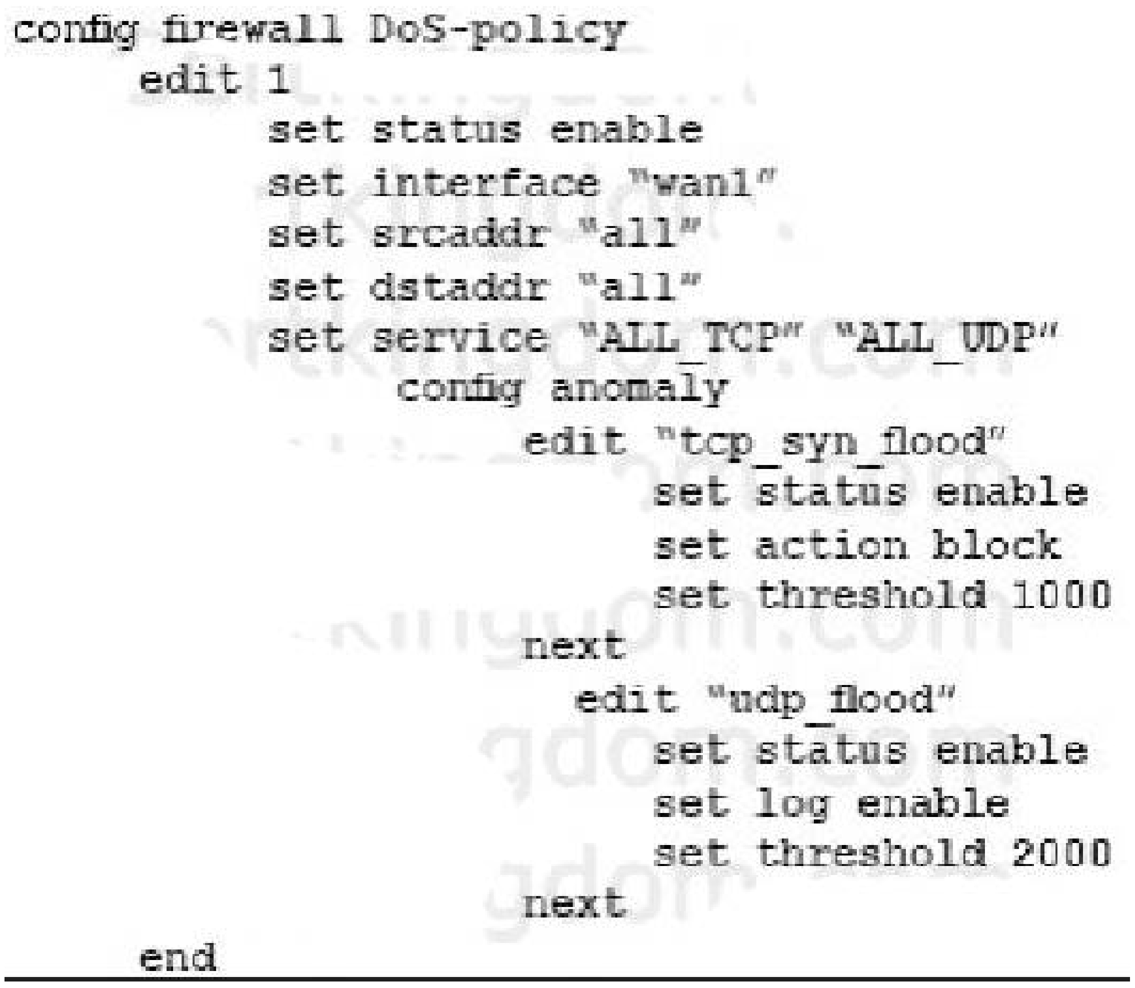
```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set log enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set status enable
                    set log enable
                    set threshold 2000
                next
    end
```

C.



```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set log enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set log enable
                    set status enable
                    set action block
                    set threshold 1000
                next
    end
```

D.



```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    set action block
                    set threshold 1000
                next
                  edit "udp_flood"
                    set status enable
                    set log enable
                    set threshold 2000
                next
    end
```

Answer: BD

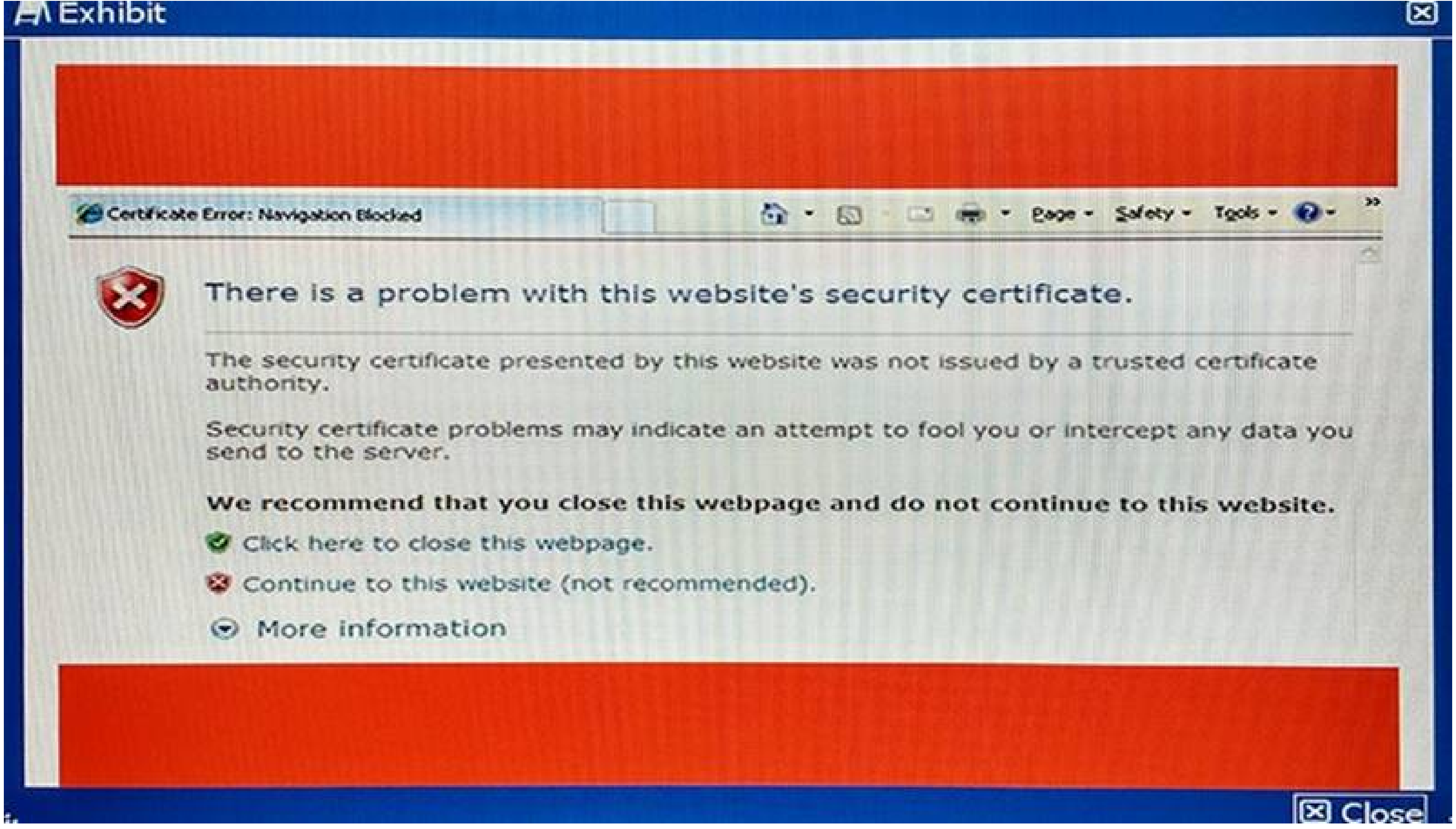
Explanation: B&D both have same policy which fulfills the above criteria. http://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-firewall-52/Examples/Example-%20DoS%20Policy.htm

NEW QUESTION 53
Virtual Domains (VDOMs) allow a FortiGate administrator to do what?

A. Group two or more FortiGate units to form a single virtual device.
B. Split a physical FortiGate unit into multiple virtual devices.
C. Create multiple VLANs in a single physical interface,
D. Group multiple physical interfaces to form a single virtual interface.

Answer: B

NEW QUESTION 55
You have replaced an explicit proxy Web filter with a FortiGate. The human resources department requires that all URLs be logged. Users are reporting that their browsers are now indicating certificate errors as shown in the exhibit.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Which step is a valid solution to the problem?

A. Make sure that the affected users' browsers are no longer set to use the explicit proxy.
B. Import the FortiGate's SSL CA certificate into the Web browsers.

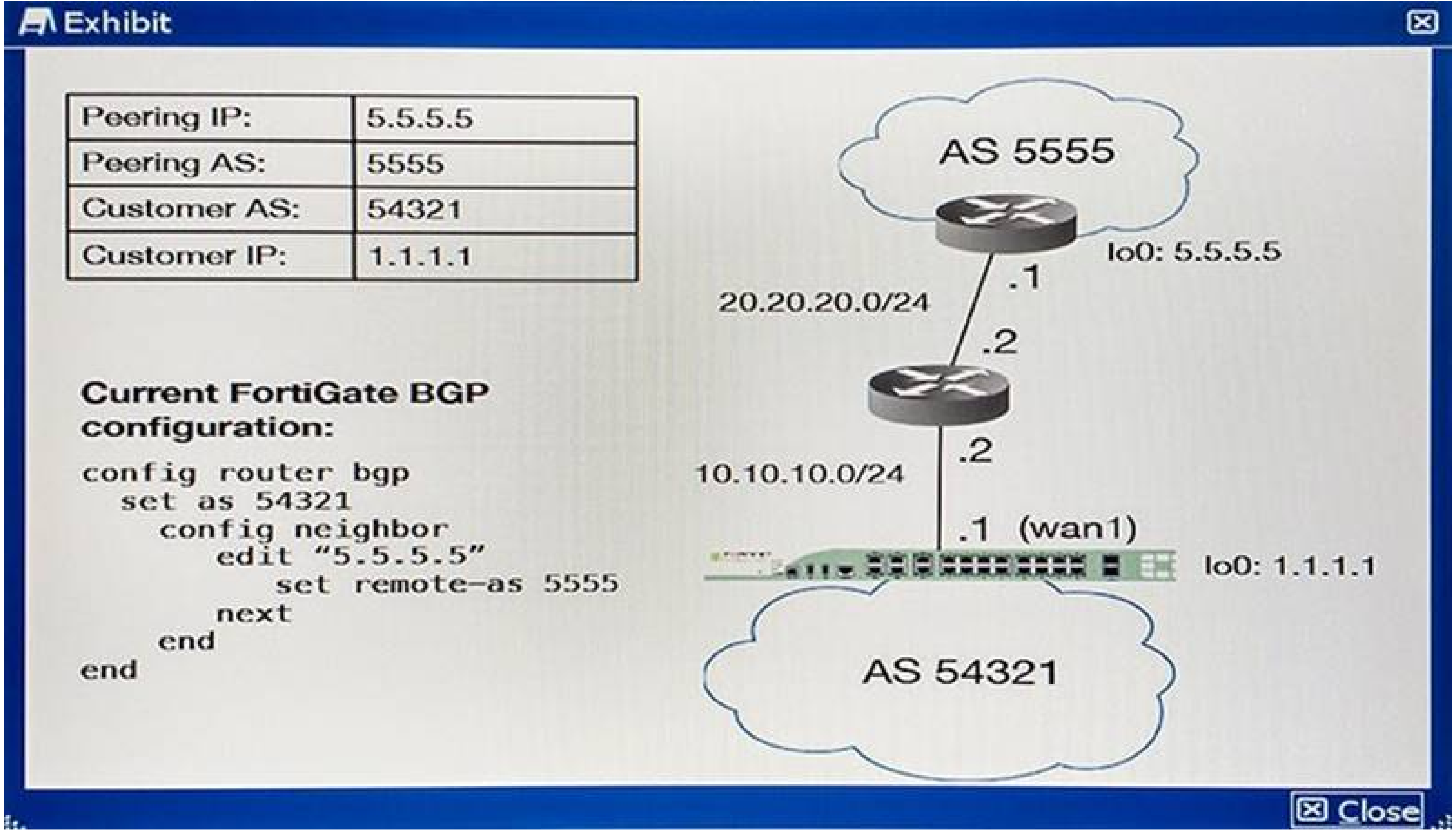
C. Change the Web filter policies on the FortiGate to only do certificate inspection.
D. Make a Group Policy to install the FortiGate's SSL certificate as a trusted host certificate on the Web browser.

Answer: D

Explanation: For https traffic inspection, client machine should install fortigate's ssl certificate

NEW QUESTION 60

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.

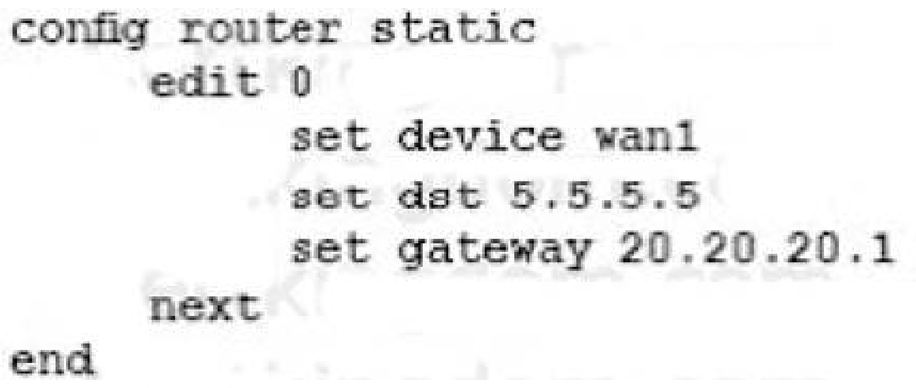


Peering IP:	5.5.5.5
Peering AS:	5555
Customer AS:	54321
Customer IP:	1.1.1.1

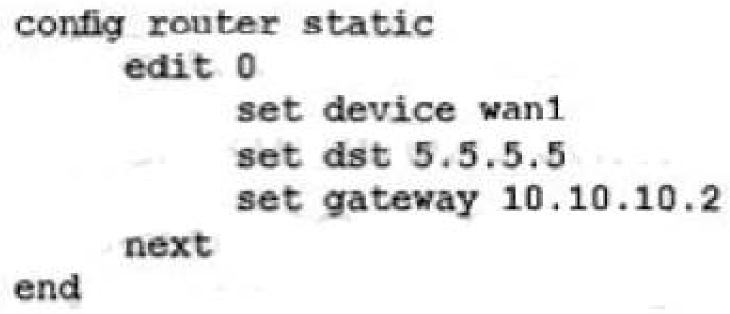
Current FortiGate BGP configuration:

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

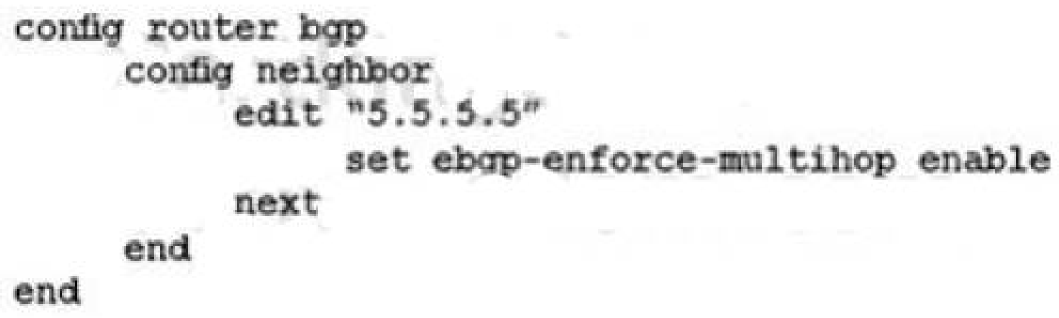
Which three missing configuration statements are needed to make this configuration functional? (Choose three.)

A.


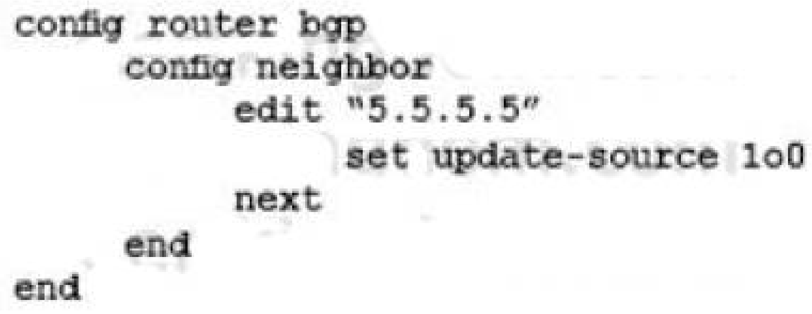
```
config router static
      edit 0
            set device wan1
            set dst 5.5.5.5
            set gateway 20.20.20.1
      next
end
```

B.


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

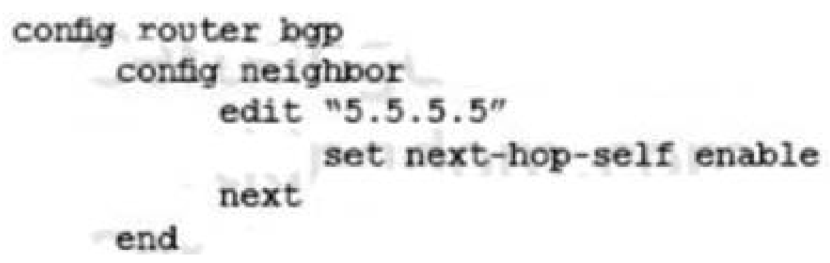
C.


```
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
```

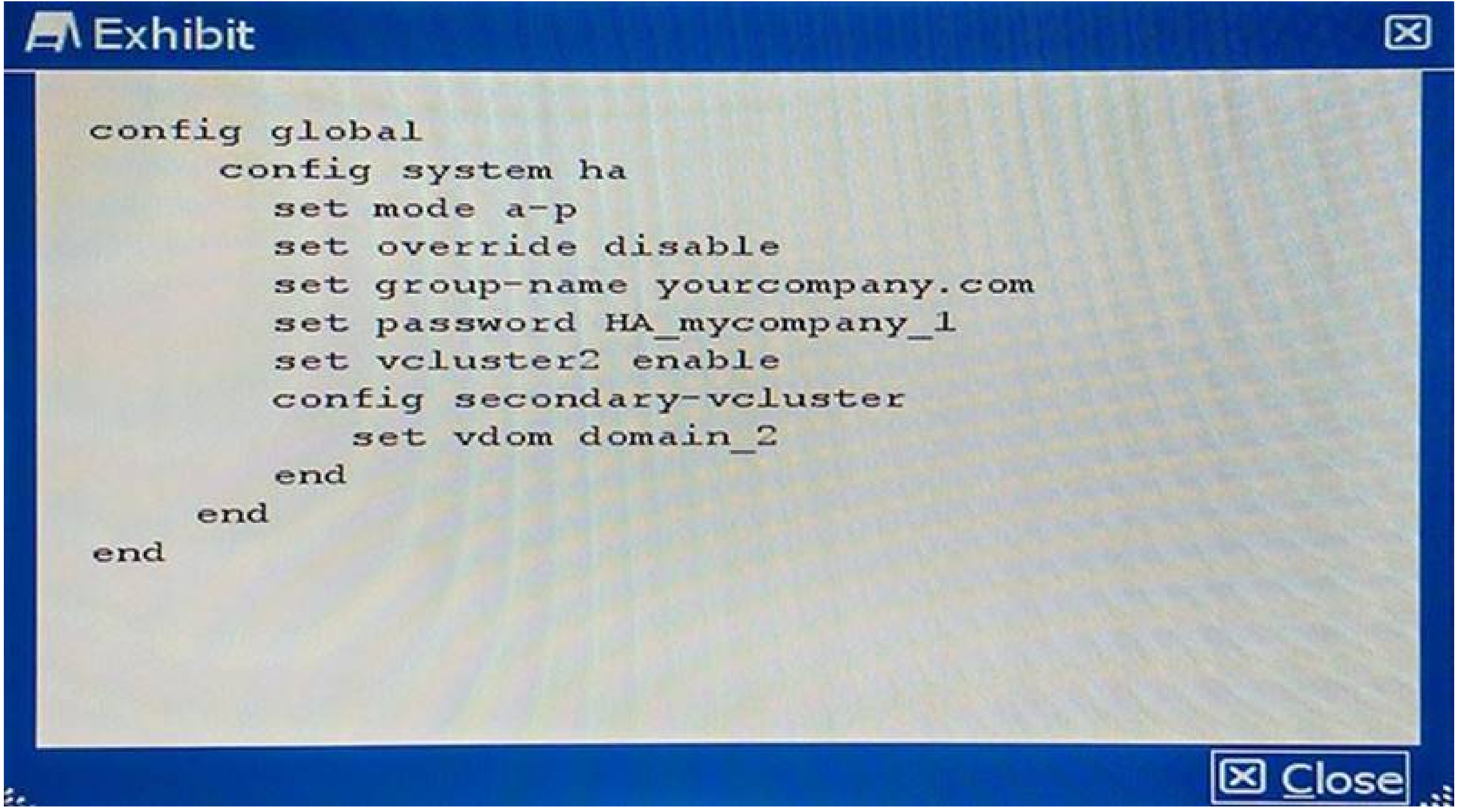
E.



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

Answer: CDE

NEW QUESTION 62
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 63
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 68
A data center for example.com hosts several separate Web applications. Users authenticate with all of them by providing their Active Directory (AD) login credentials. You do not have access to Example, Inc.'s AD server. Your solution must do the following:
- provide single sign-on (SSO) for all protected Web applications
- prevent login brute forcing
- scan FTPS connections to the Web servers for exploits
- scan Webmail for OWASP Top 10 vulnerabilities such as session cookie hijacking, XSS, and SQL injection attacks
Which solution meets these requirements?

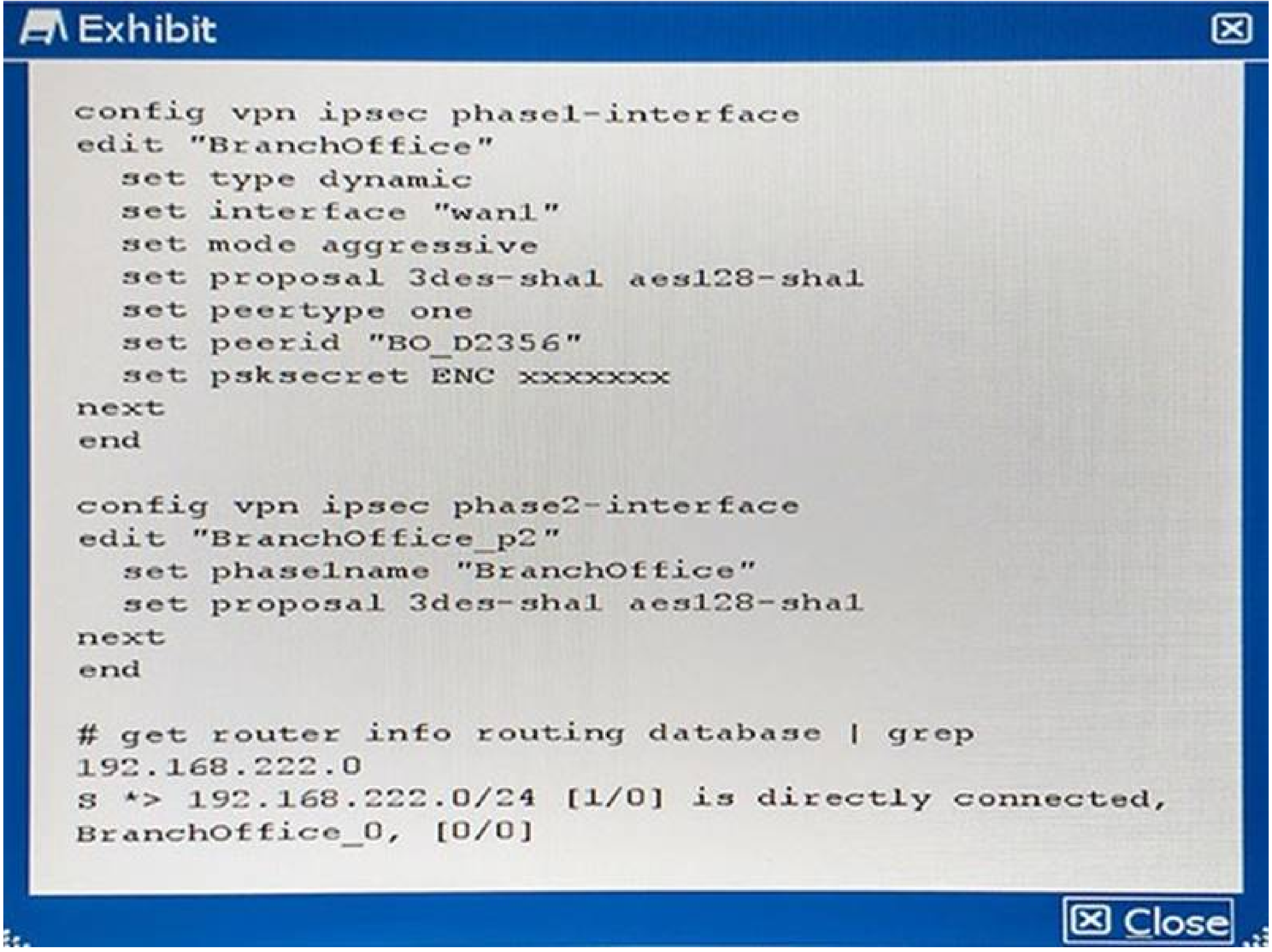
A. Apply FortiGate deep inspection to FTP
B. It must forward FTPS, HTTP, and HTTPS to FortiWe

C. Configure FortiWeb to query the AD server, and apply SSO for Web request
D. FortiWeb must forward FTPS directly to the Web servers without inspection, but proxy HTTP/HTTPS and block Web attacks.
E. Deploy FortiDDos to block brute force attack
F. Configure FortiGate to forward only FTPS, HTTP, and HTTPS to FortiWe
G. Configure FortiWeb to query the AD server, and apply SSO for Web request
H. Also configure it to scan FTPS and Web traffic, then forward allowed traffic to the Web servers.
I. Use FortiGate to authenticate and proxy HTTP/HTTPS; to verify credentials, FortiGate queries the AD serve
J. Also configure FortiGate to scan FTPS before forwarding, and to mitigate SYN flood
K. Configure FortiWeb to block Web attacks.
L. Install FSSO Agent on server
M. Configure FortiGate to inspect FTP
N. FortiGate will forward FTPS, HTTP, and HTTPS to FortiWe
O. FortiWeb must block Web attacks, then forward all traffic to the Web servers.

Answer: D

Explanation: FSSO agent integrate fortigate with AD then inspect bruteforce,FTPS,HTTP, and HTTPS using fortiweb and then forward all traffic to web server.
References:

NEW QUESTION 73
The FortiGate is an IPsec VPN hub. A VPN spoke protecting subnet 192.168.222.0/24 has successfully brought up a tunnel with the FortiGate. This remote network is present in the FortiGate routing table as shown in the exhibit.



```
config vpn ipsec phase1-interface
edit "BranchOffice"
   set type dynamic
   set interface "wan1"
   set mode aggressive
   set proposal 3des-sha1 aes128-sha1
   set peertype one
   set peerid "BO_D2356"
   set psksecret ENC xxxxxxx
next
end

config vpn ipsec phase2-interface
edit "BranchOffice_p2"
   set phase1name "BranchOffice"
   set proposal 3des-sha1 aes128-sha1
next
end

# get router info routing database | grep
192.168.222.0
S *> 192.168.222.0/24 [1/0] is directly connected,
BranchOffice_0, [0/0]
```

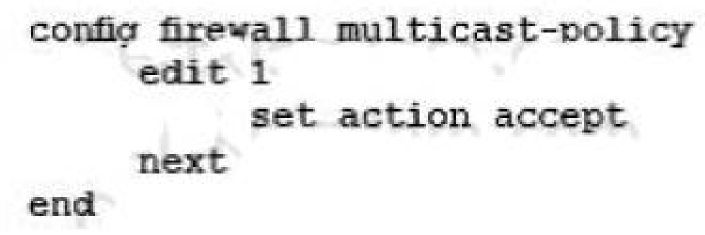
Which statement is true?

A. This subnet was learned during quick-mode negotiation and was dynamically injected into the routing table.
B. The FortiGate administrator configured this subnet as a locally connected subnet on the “BranchOffice” phase1 interface.
C. The route in the exhibit is bound to “BranchOffice_0” which is a tunnel other than “BranchOffice”.
D. The FortiGate administrator configured a static route for 192.168.222.0/24.

Answer: B

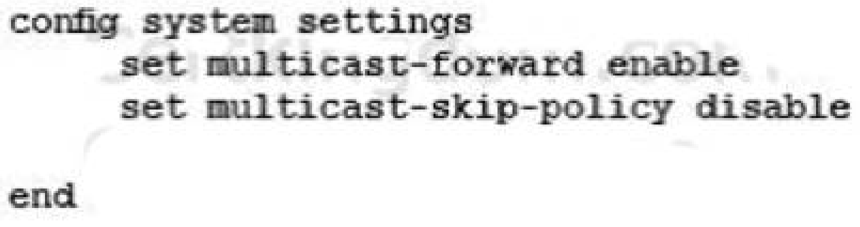
NEW QUESTION 75
A company has just installed a new FortiGate in their core to route and inspect traffic between their subnetted VLANs. The security department reports that after the installation, their IP video cameras no longer work. Research by the IT department shows that the video system uses a multicast stream to send the video to multiple video receivers.
Which two commands must be configured to resolve this problem? (Choose two.)

A.



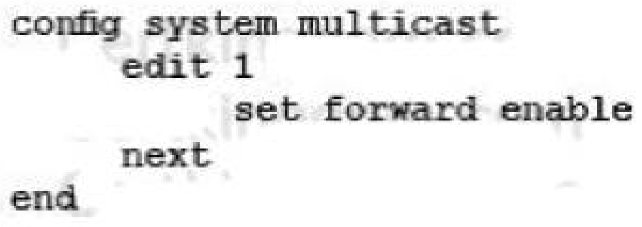
```
config firewall multicast-policy
    edit 1
        set action accept
    next
end
```

B.



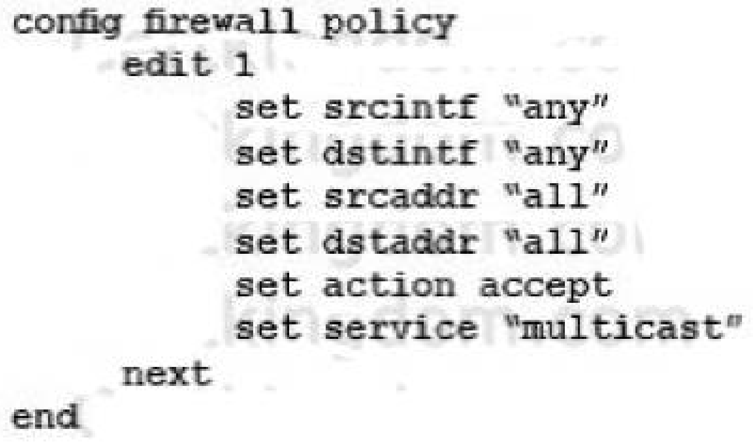
```
config system settings
    set multicast-forward enable
    set multicast-skip-policy disable

end
```

C.



```
config system multicast
    edit 1
        set forward enable
    next
end
```

D.

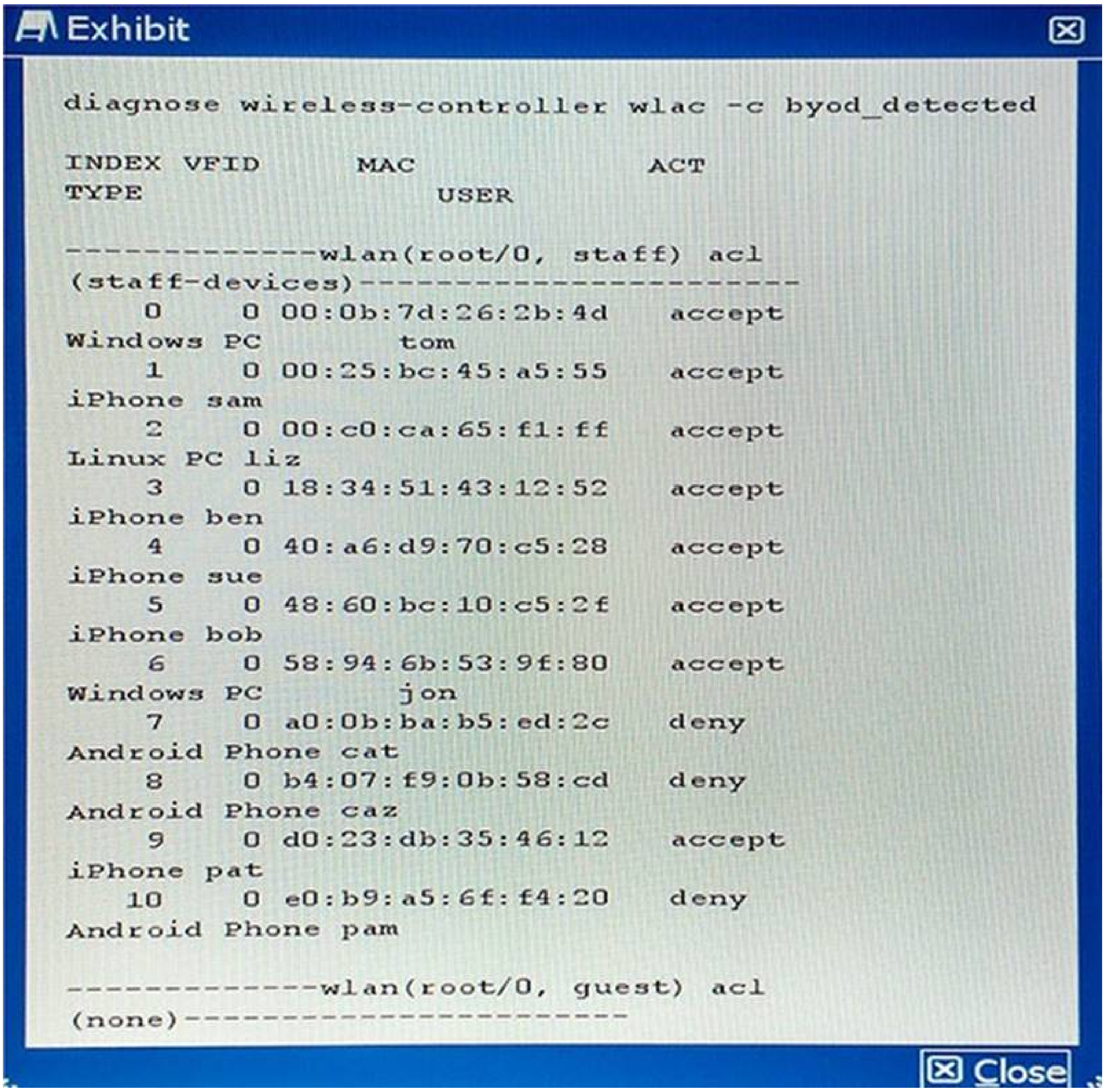


```
config firewall policy
    edit 1
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "multicast"
    next
end
```

Answer: BD

Explanation: http://kb.fortinet.com/kb/documentLink.do?externalID=FD36500

NEW QUESTION 76
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 77
......