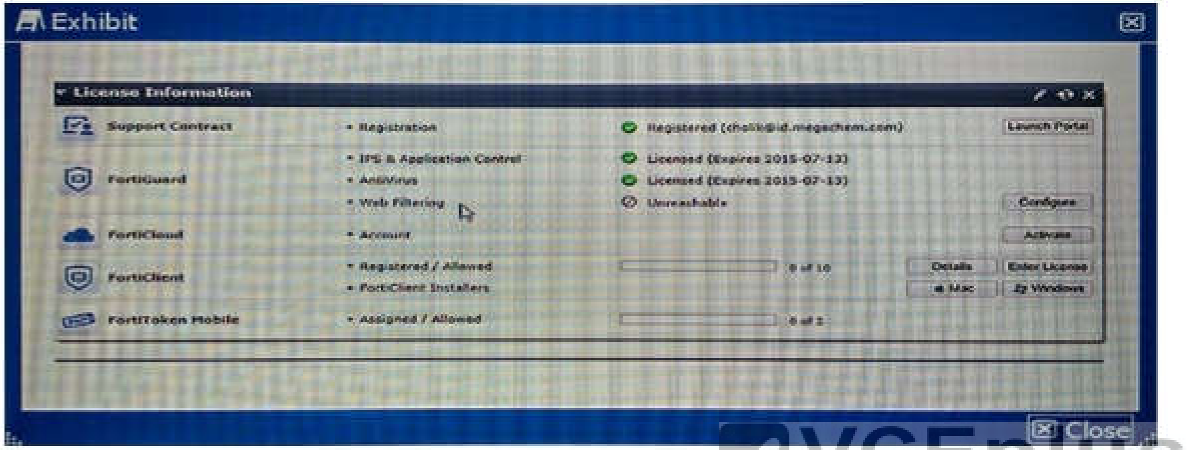
Fortinet.Premium.NSE8.by.VCEplus.65q

Number: NSE8 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.5

Exam Code: NSE8
Exam Name: Fortinet Network Security Expert 8 Written (800)
Certification Provider: Fortinet
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-nse8/

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 (chollk@id.megachem.com)	Launch Portal
FortiGuard	• IPS & Application Control	Licensed (Expires 2015-07-13)	
	• AntiVirus	Licensed (Expires 2015-07-13)	
	• Web Filtering	Unreachable	Configure
FortiCloud	• Account		Activate
FortiClient	• Registered / Allowed	0 of 10	Details Enter License
	• FortiClient Installers		Mac Windows
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.

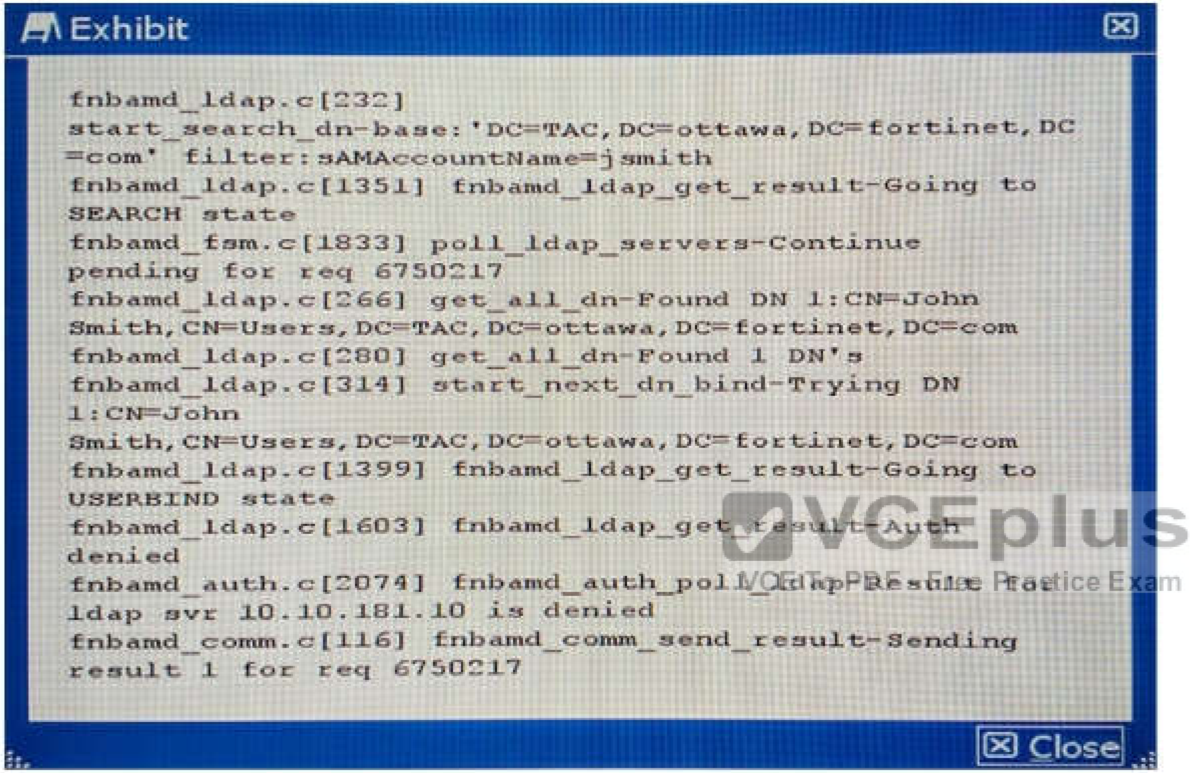
D. You have a firewall policy blocking ports 8888 and 53.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
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.
Reference:
http://cookbook.fortinet.com/troubleshooting-web-filtering/

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
```

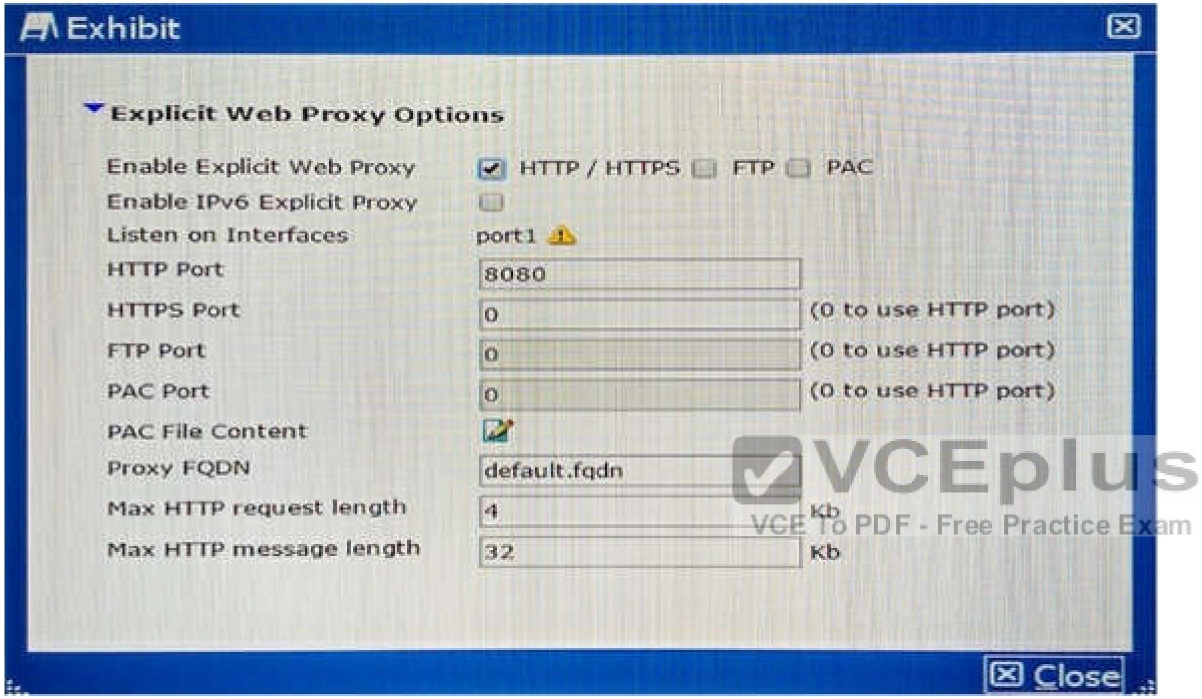
A. The LDAP administrator password in the FortiGate configuration is incorrect
B. The user, John Smith, does have an account in the LDAP server.
C. The user, John Smith, does not belong to any allowed user group.
D. The user, John Smith, is using an incorrect password.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Fortigate not binded with LDAP server because of failed authentication.
Reference:
http://kb,fortinet,com/kb/documentLink.do?extemalID=FD31886

QUESTION 3



Explicit Web Proxy Options

Enable Explicit Web Proxy ☑ HTTP / HTTPS □ FTP □ PAC
Enable IPv6 Explicit Proxy □
Listen on Interfaces port1 ⚠
HTTP Port 8080
HTTPS Port 0 (0 to use HTTP port)
FTP Port 0 (0 to use HTTP port)
PAC Port 0 (0 to use HTTP port)
PAC File Content
Proxy FQDN default.fqdn
Max HTTP request length 4 Kb
Max HTTP message length 32 Kb

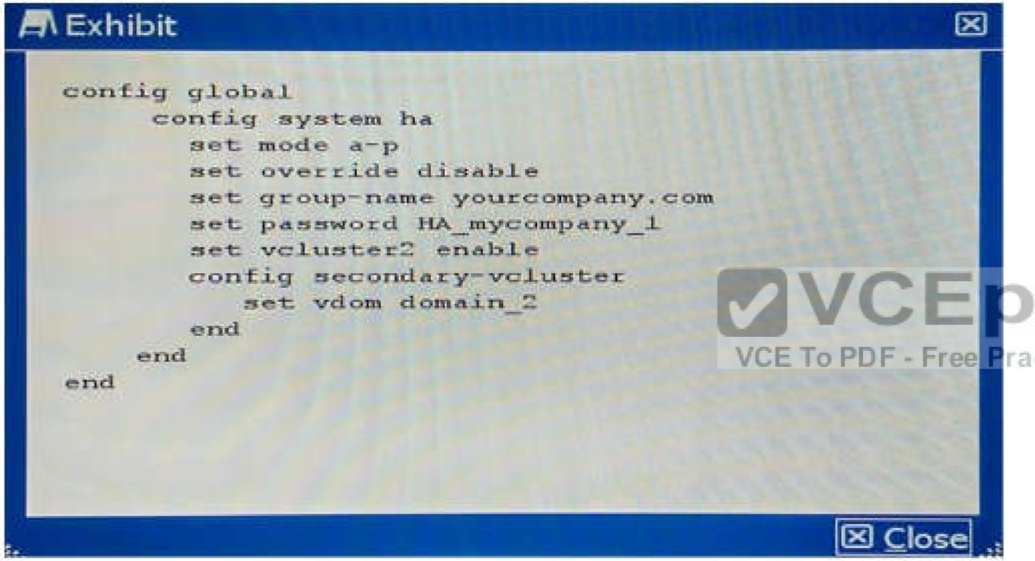
The exhibit shows an explicit Web proxy configuration in a FortiGate device. The FortiGate is installed between a client with the IP address 172.16.10.4 and a Web server using port 80 with the IP address 10.10.3.4. The client Web browser is properly sending HTTP traffic to the FortiGate Web proxy IP address 172.16.10.254.
Which two sniffer commands will capture this HTTP traffic? (Choose two.)

A. diagnosesnifferpacketany'host172.16.10.4andhost172.16.10.254' 3
B. diagnosesnifferpacketany'host172.16.10.254 and host 10.10.3.4' 3
C. diagnosesnifferpacketany'host172.16.10.4andport8080' 3
D. diagnosesnifferpacketany'host172.16.10.4andhost10.10.3.4' 3

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sniffer should run between webproxy to Webserver
And also Sniffer between client machine to web proxy connectivity as it is in explicit mode. Reference:
http://www.maxnetwork.org/fortigate-packet-capture

QUESTION 4
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
http://docs.fortinet.com/uploaded/files/1088/fortigate-ha-50.pdf

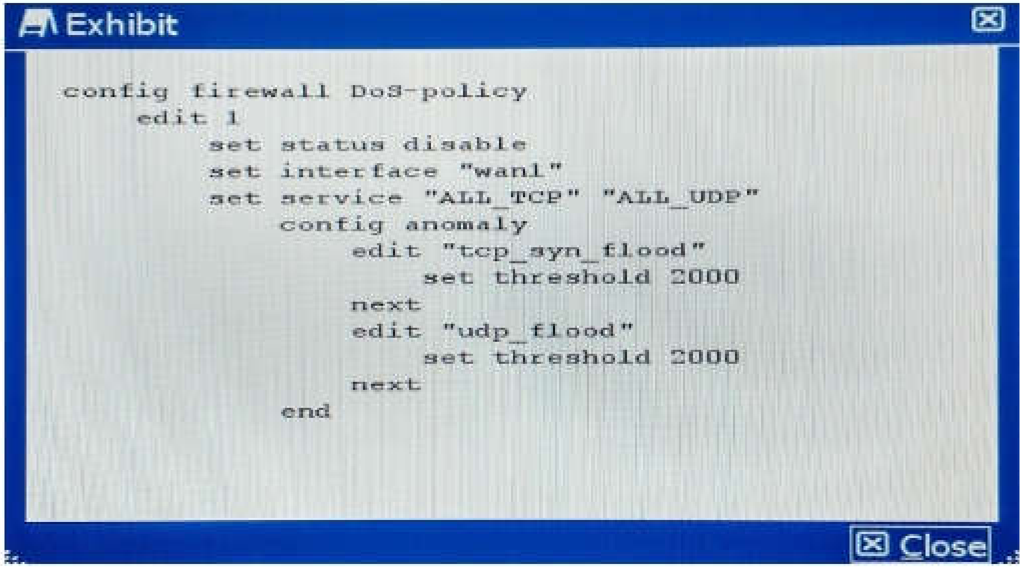
QUESTION 5
A data center for example.com hosts several separate Web applications. Users authenticate with all of them by providing their Active Directory (AD) login credentials. You do not have access to Example, Inc.'s AD server. Your solution must do the following:
-provide single sign-on (SSO) for 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 FTPS. It must forward FTPS, HTTP, and HTTPS to FortiWeb. Configure FortiWeb to query the AD server, and apply SSO for Web requests. FortiWeb must forward FTPS directly to the Web servers without inspection, but proxy HTTP/HTTPS and block Web attacks.
B. Deploy FortiDDos to block brute force attacks. Configure FortiGate to forward only FTPS, HTTP, and HTTPS to FortiWeb. Configure FortiWeb to query the AD server, and apply SSO for Web requests. Also configure it to scan FTPS and Web traffic, then forward allowed traffic to the Web servers.
C. Use FortiGate to authenticate and proxy HTTP/HTTPS; to verify credentials, FortiGate queries the AD server, Also configure FortiGate to scan FTPS before forwarding, and to mitigate SYN floods. Configure FortiWeb to block Web attacks.
D. Install FSSO Agent on servers. Configure FortiGate to inspect FTPS. FortiGate will forward FTPS, HTTP, and HTTPS to FortiWeb. FortiWeb must block Web attacks, then forward all traffic to the Web servers.

Correct Answer: D
Section: (none)
Explanation

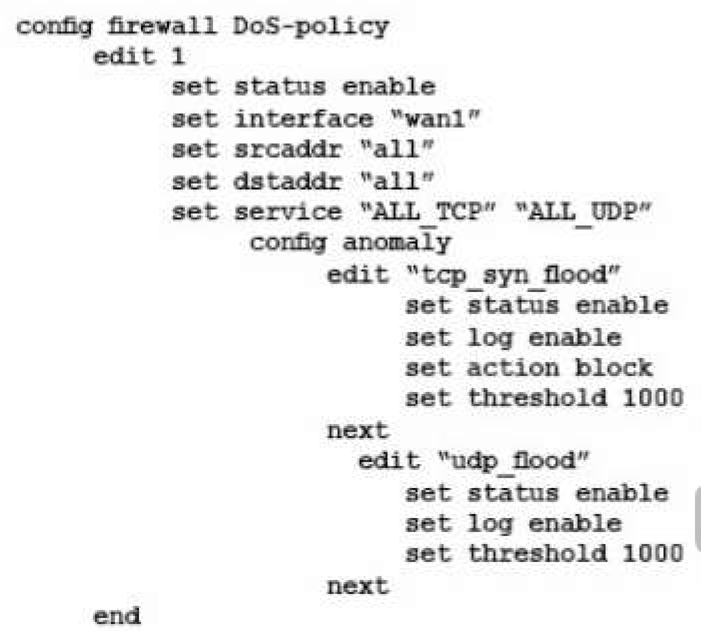
Explanation/Reference:

QUESTION 6
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 WAN 1.
-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.



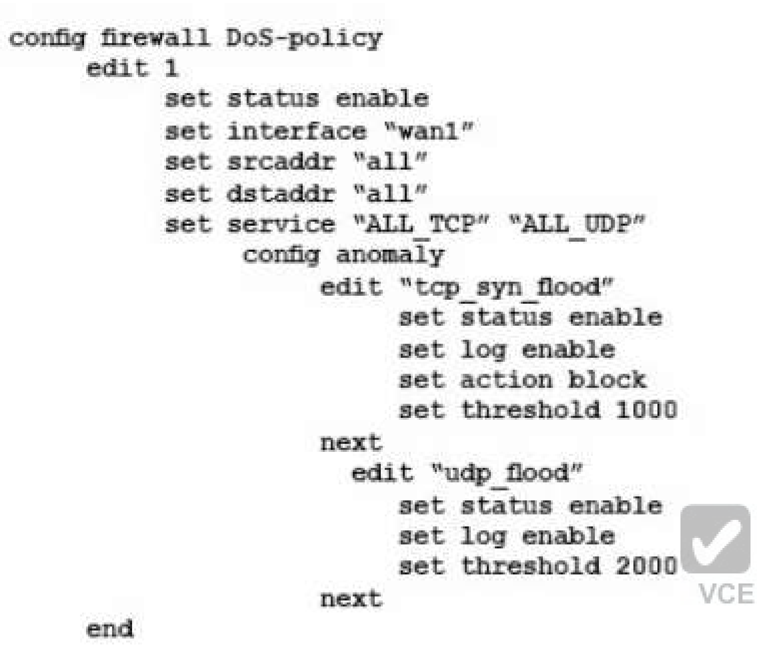
```
config firewall DoS-policy
    edit 1
        set status disable
        set interface "wan1"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set threshold 2000
                next
                edit "udp_flood"
     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

A)



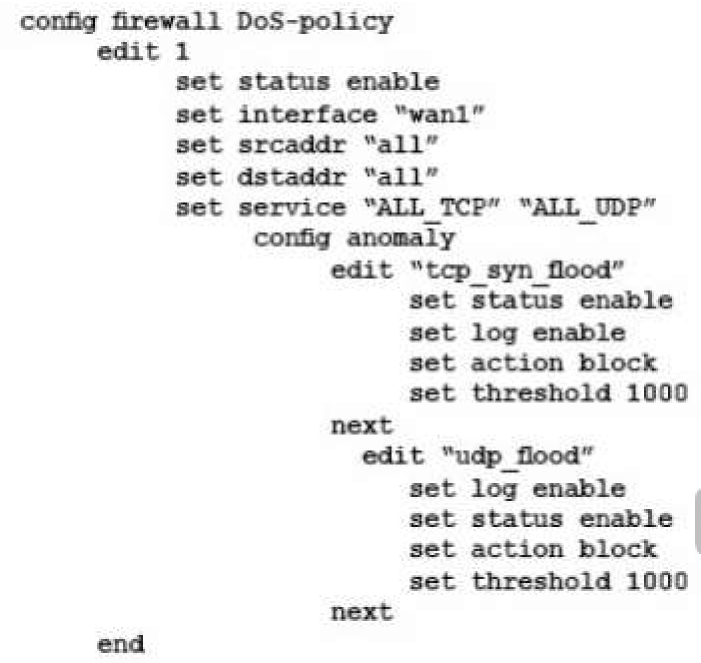
```
config firewall DoS-policy
    edit 1
        set status enable
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL_TCP" "ALL_UDP"
            config anomaly
                edit "tcp_syn_flood"
                    set status enable
                    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)



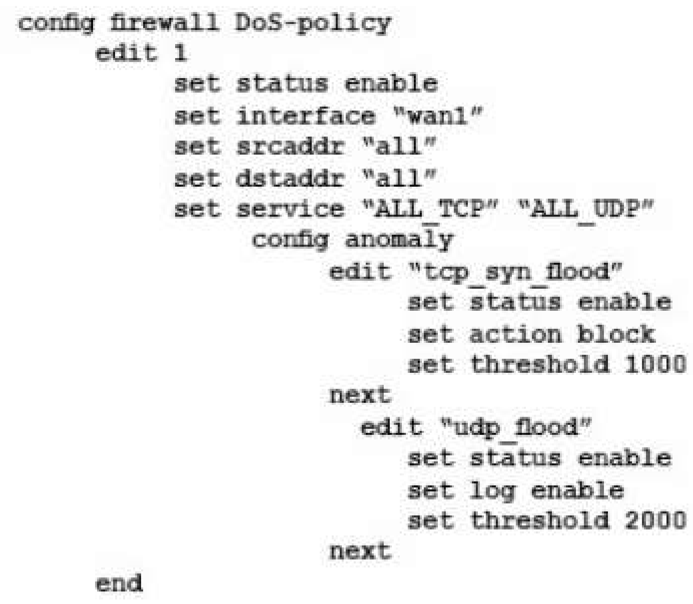
```
config firewall DoS-policy
    edit 1
        set status enable
        set interface “wan1”
        set srcaddr “all”
        set dstaddr “all”
        set service “ALL_TCP” “ALL_UDP”
            config anomaly
                edit “tcp_syn_flood”
                    set status enable
                    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
```

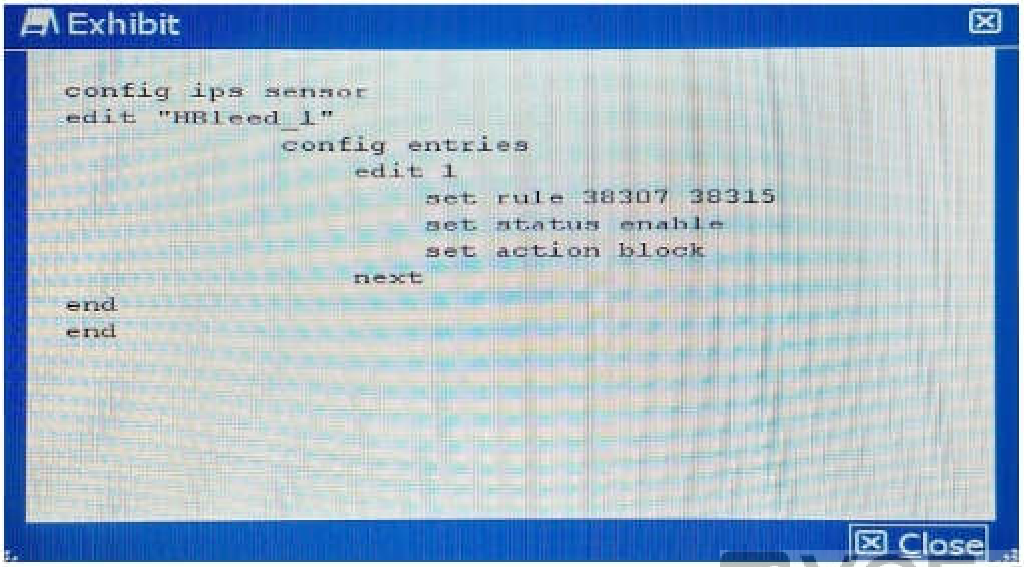
A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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

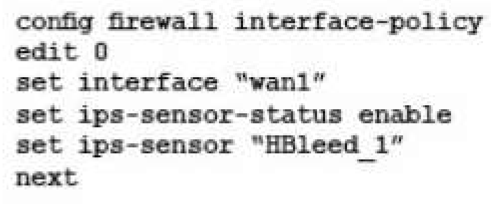
QUESTION 7
Your security department has requested that you implement the OpenSSL.TLS.Heartbeat.Information.Disclosure signature using an IPS sensor to scan traffic destined to the FortiGate. You must log all packets that attempt to exploit this vulnerability.

Referring to the exhibit, which two configurations are required to accomplish this task? (Choose two.)



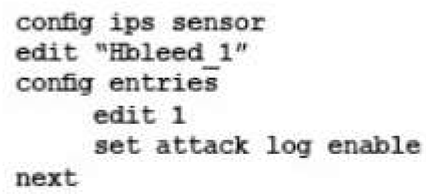
```
config ips sensor
edit "HBleed_1"
            config entries
                edit 1
                    set rule 38307 38315
                    set status enable
                    set action block
                next
end
end
```

A)



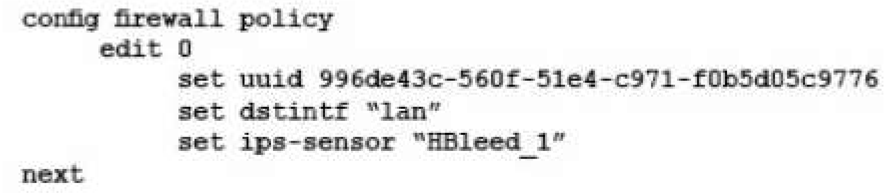
```
config firewall interface-policy
edit 0
set interface "wan1"
set ips-sensor-status enable
set ips-sensor "HBleed_1"
next
```

B)



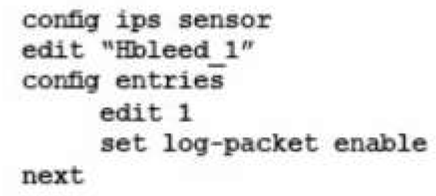
```
config ips sensor
edit "Hbleed_1"
config entries
     edit 1
     set attack log enable
next
```

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
```

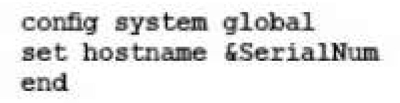
A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: AB
Section: (none)
Explanation

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

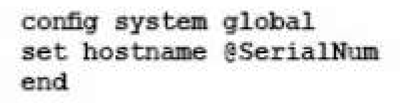
QUESTION 8
Which command syntax would you use to configure the serial number of a FortiGate as its host name?

A)



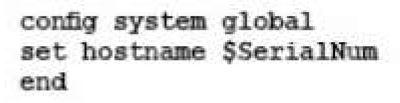
```
config system global
set hostname &SerialNum
end
```

B)



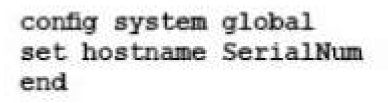
```
config system global
set hostname @SerialNum
end
```

C)



```
config system global
set hostname $SerialNum
end
```

D)



```
config system global
set hostname SerialNum
end
```

A. Option A
B. Option B
C. Option C
D. Option D

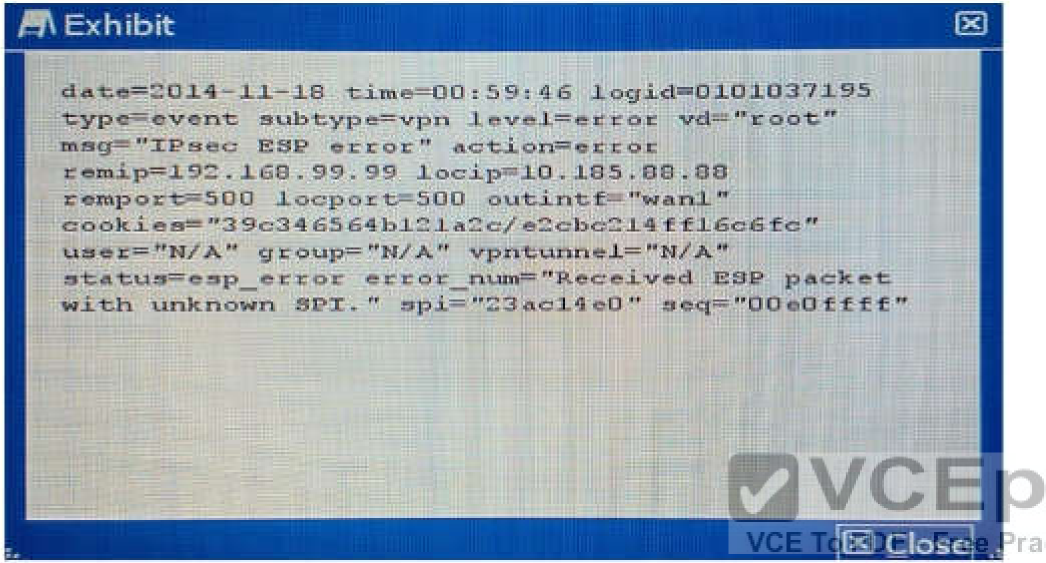
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

http://docs.fortinet.com/uploaded/files/2002/FortiOS%20Handbook%20-%20System%20Administration%205.2.pdf

QUESTION 9

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"
```

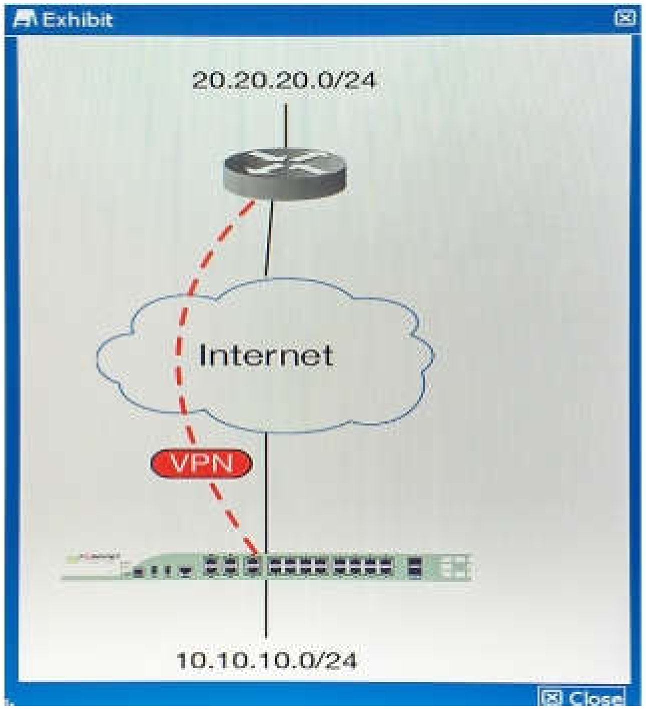
A. The packet failed the HMAC validation.
B. The packet did not match any of the local IPsec SAs.
C. The packet was protected with an unsupported encryption algorithm.
D. The IPsec negotiation failed because the SPI was unknown.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: http://kb.fortinet.com/kb/viewContent.do?externa11d=FD33101

QUESTION 10

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.)

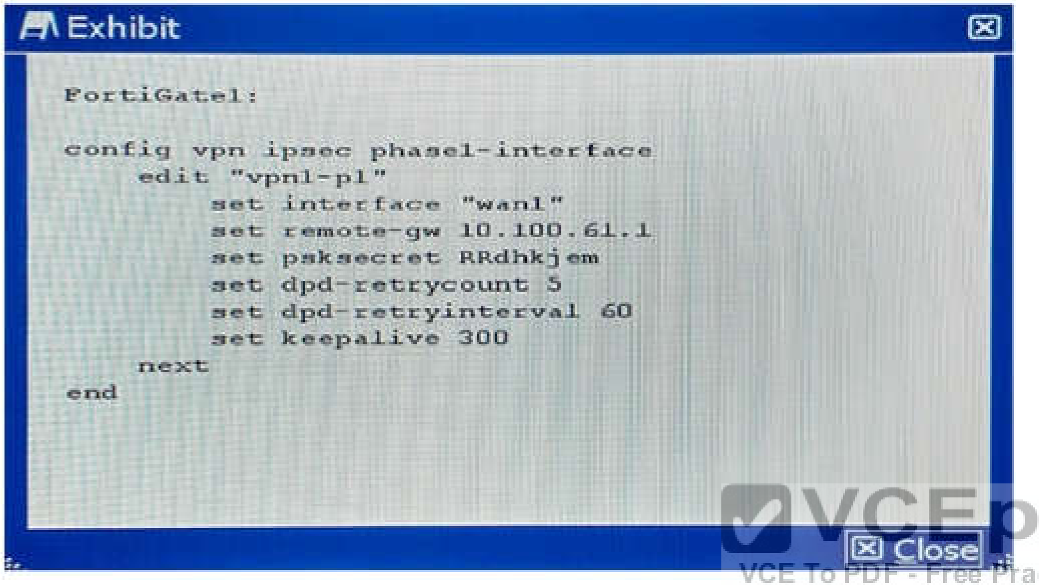
A. Configure an IP Pool of type Overload for range 30.30.30.10-30.30.30.10. Enable NAT on a policy from your LAN forwards the VPN tunnel and select that pool.
B. Configure IPsec phase 2 proxy IDs fora source of 10.10.10.0/24 and destination of 20.20.20.0/24.
C. Configure an IP Pool of Type One-to-One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

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

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
```

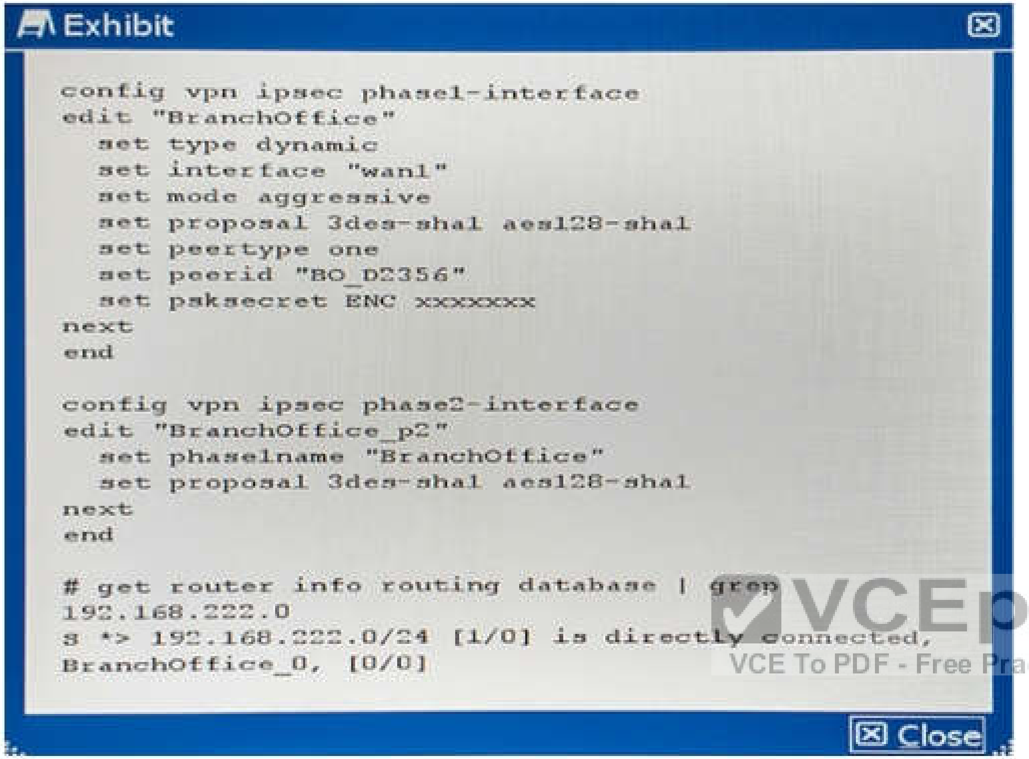
Which statement is true on this scenario?

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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 12
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13

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 portl. Port! 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.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 14
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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 15
Which three statements about throughput on a wireless network are true? (Choose three.)

A. A wireless device labelled as 300 Mbps should be expected to provide a throughput of 300Mbps.
B. Be careful to ensure the capabilities of the wireless clients match those of the access points, in order to achieve higher throughput.
C. Reducing the duty cycles of the wireless media by generating fewer beacons may improve throughput.

D. Because of the higher level of RF noise that is typical in the 2.4 GHz ISM band, throughput of 2.4 GHz devices will typically be less than 5 GHz devices.
E. Because of the full-duplex nature of the medium and the minimal overhead generated by CSMA/CA, the actual aggregate throughput is typically close to the data rate.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
http://www.tp-link.in/faq-499.html

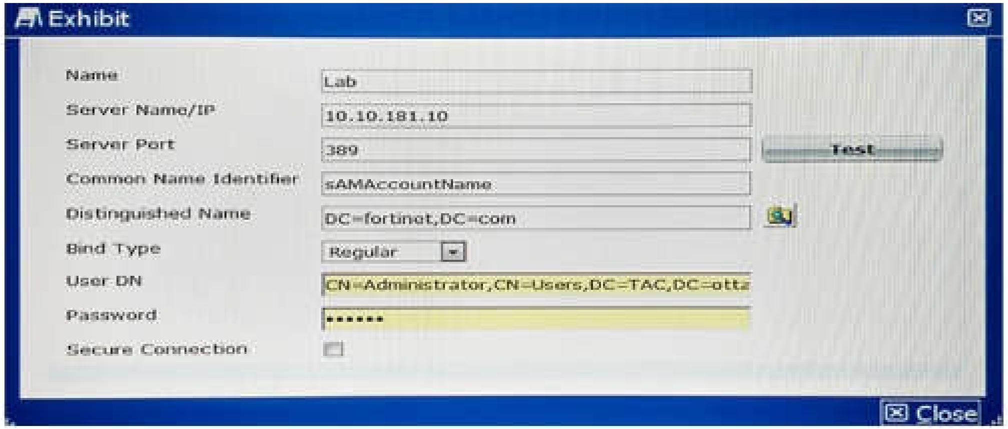
QUESTION 16
An administrator wants to assign static IP addresses to users connecting tunnel-mode SSL VPN. Each SSL VPN user must always get the same unique IP address which is never assigned to any other user.
Which solution accomplishes this task?

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.

Correct Answer: D
Section: (none)
Explanation

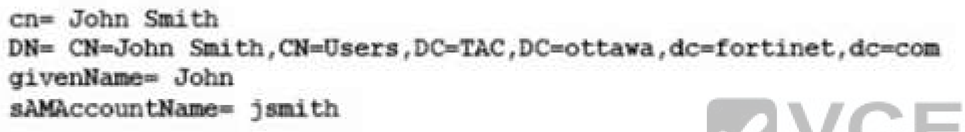
Explanation/Reference:

QUESTION 17



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 exhibit shows an LDAP server configuration in a FortiGate device. 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
```

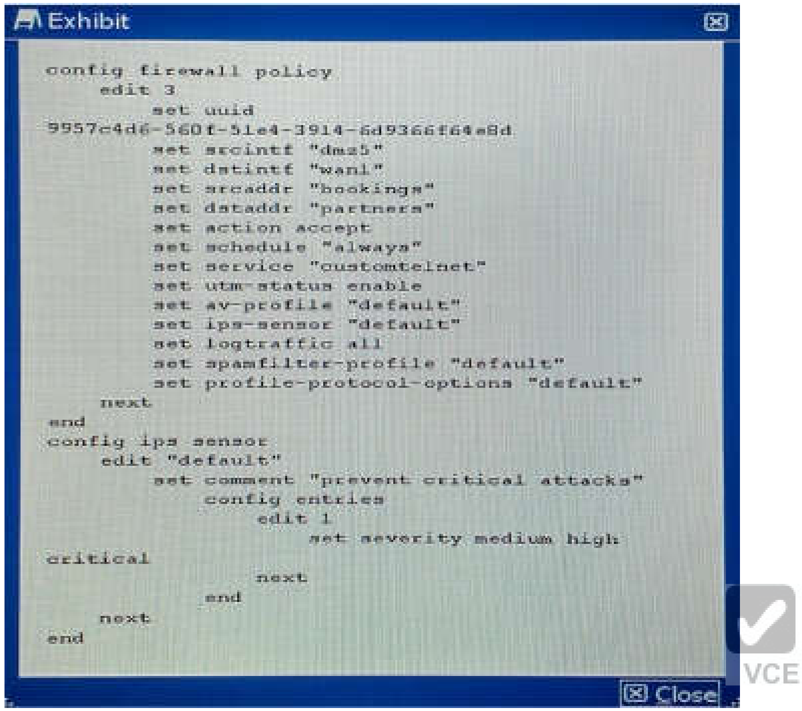
John Smith's LDAP password is ABC123.
Which CLI command should you use to test the LDAP authentication using John Smith's credentials?

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

Correct Answer: A
Section: (none)
Explanation

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

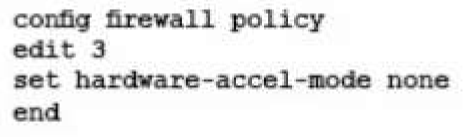
QUESTION 18
Your NOC contracts the security team due to a problem with a new application flow. You are instructed to disable hardware acceleration for the policy shown in the exhibit for troubleshooting purposes.



```
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
```

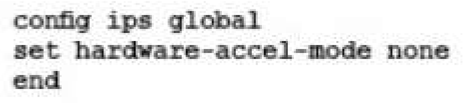
Which command will disable hardware acceleration for the new application policy?

A)



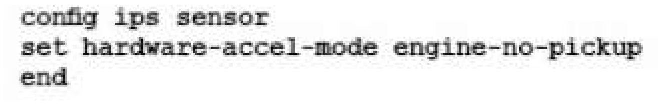
```
config firewall policy
edit 3
set hardware-accel-mode none
end
```

B)



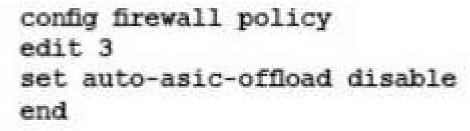
```
config ips global
set hardware-accel-mode none
end
```

C)



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

D)



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

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 19
Your company uses a cluster of two FortiGate 3600C units in active-passive mode to protect the corporate network. The FortiGate cluster sends its logs to a FortiAnalyzer and you have configured scheduled weekly reports for the Internet bandwidth usage of each corporate VLAN. During a scheduled maintenance window, you make a series of configuration changes. When the next FortiAnalyzer weekly report is generated, you notice that Internet bandwidth usage reported by the FortiAnalyzer is far less than expected.
What is the reason for this discrepancy?

A. You applied an antivirus profile on some of the policies, and no traffic can be accelerated.
B. You disabled all security profiles on some of the firewall policies, and the traffic matching those policies is now accelerated.
C. You enabled HA session-pickup, which is turn disabled session accounting
D. You changed from active-passive to active-active, causing the session traffic counters to become inaccurate.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Because of Active/Active failover traffic segregate to boxes where it reduces the bandwidth utilization

QUESTION 20
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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
A cafe offers free Wi-Fi. Customers1 portable electronic devices often do not have antivirus software installed and may be hosting worms without their knowledge.
You must protect all customers from any other customers' infected devices that join the same SSID.
Which step meets the requirement?

A. Enable deep SSH inspection with antivirus and IPS.
B. Use a captive portal to redirect unsecured connections such as HTTP and SMTP to their secured equivalents, preventing worms on infected clients from tampering with other customer traffic.
C. Use WPA2 encryption and configure a policy on FortiGate to block all traffic between clients.
D. Use WPA2 encryption, and enable “Block Intra-SSID Traffic".

Correct Answer: D
Section: (none)
Explanation