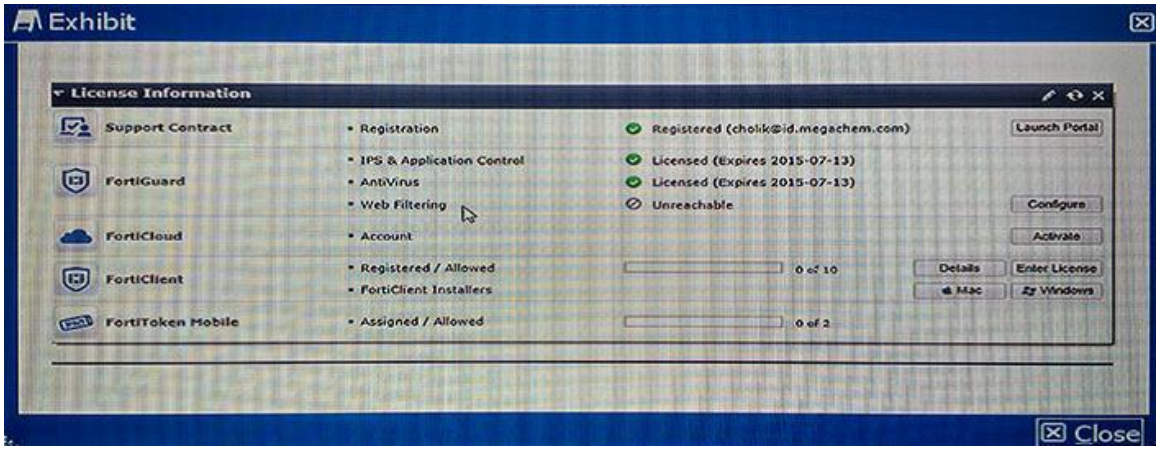
# Fortinet NSE8 Exam

**Volume: 65 Questions**

Question No: 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.




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.

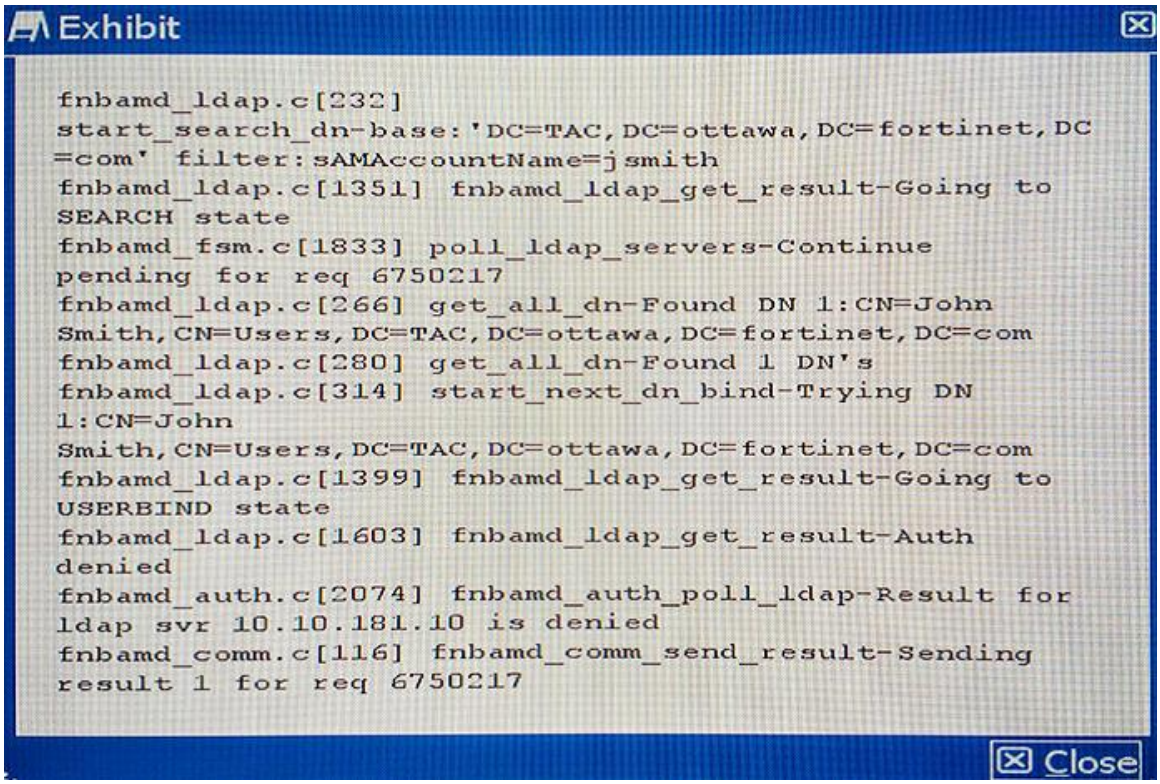
B. FortiGuard Web Filtering is not enabled in any firewall policy.

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: B,D

Question No: 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?




A. The LDAP administrator password in the FortiGate configuration is incorrect.

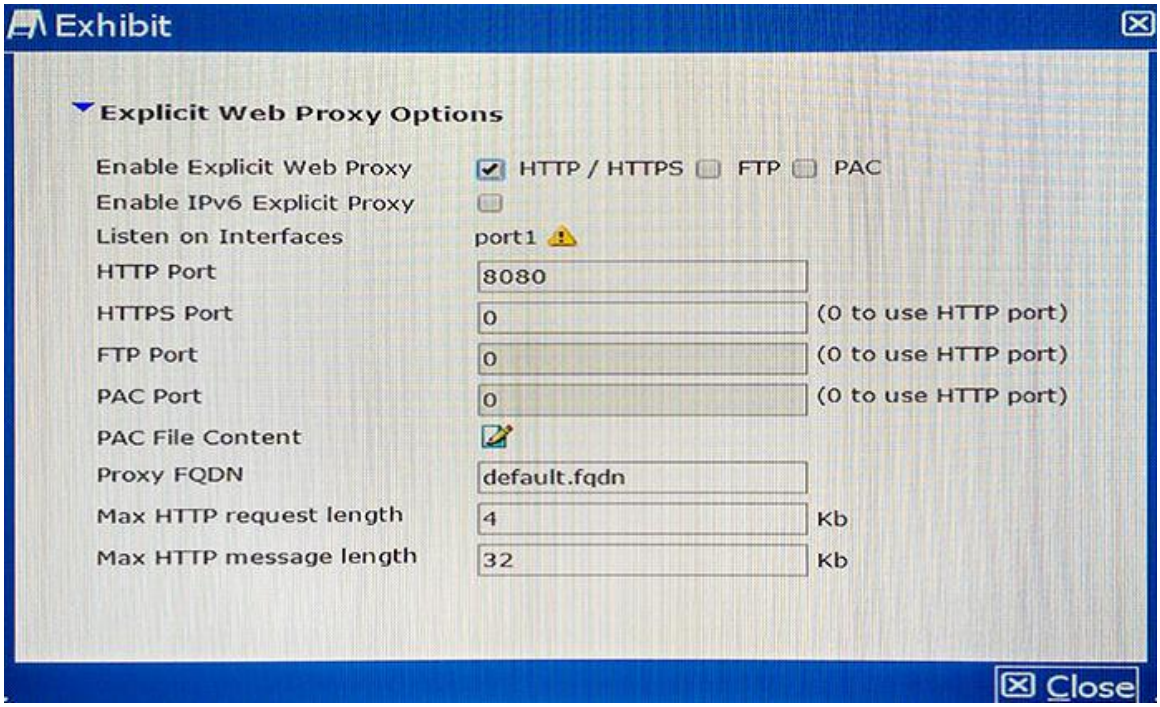
B. The user, John Smith, does have an account in the LDAP server.

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

Question No: 3
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. diagnose sniffer packet any 'host 172.16.10.4 and host 172.16.10.254' 3

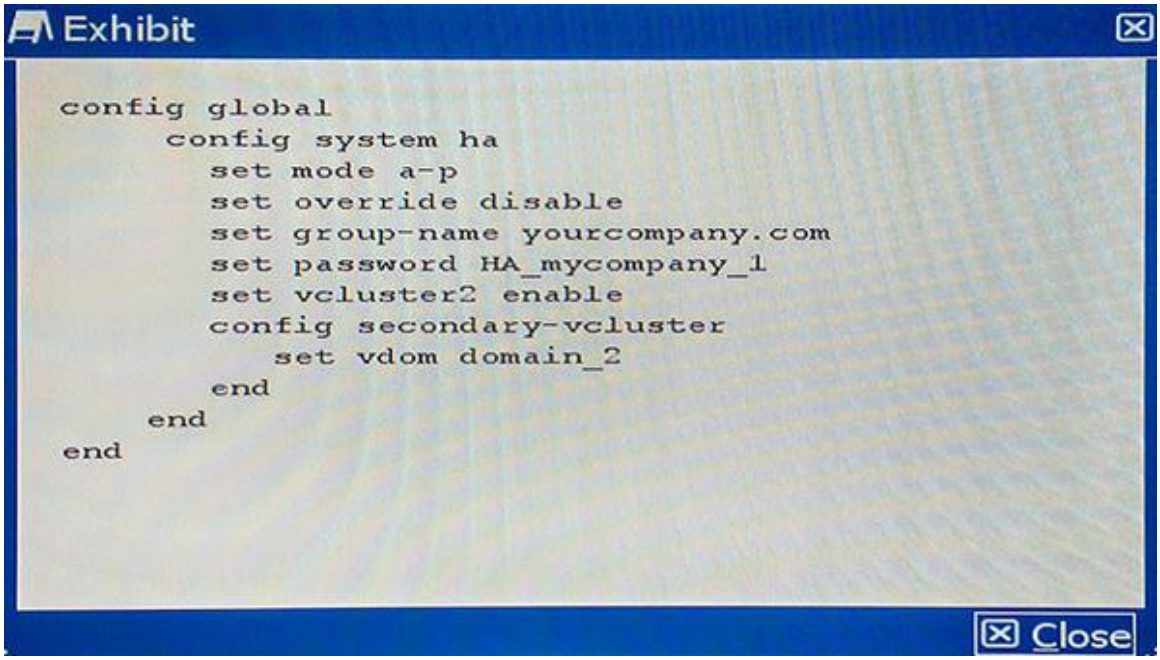
B. diagnose sniffer packet any 'host 172.16.10.254 and host 10.10.3.4' 3

C. diagnose sniffer packet any 'host 172.16.10.4 and port 8080' 3

D. diagnose sniffer packet any 'host 172.16.10.4 and host 10.10.3.4' 3

Answer: C,D

Question No: 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.
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

Question No: 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.

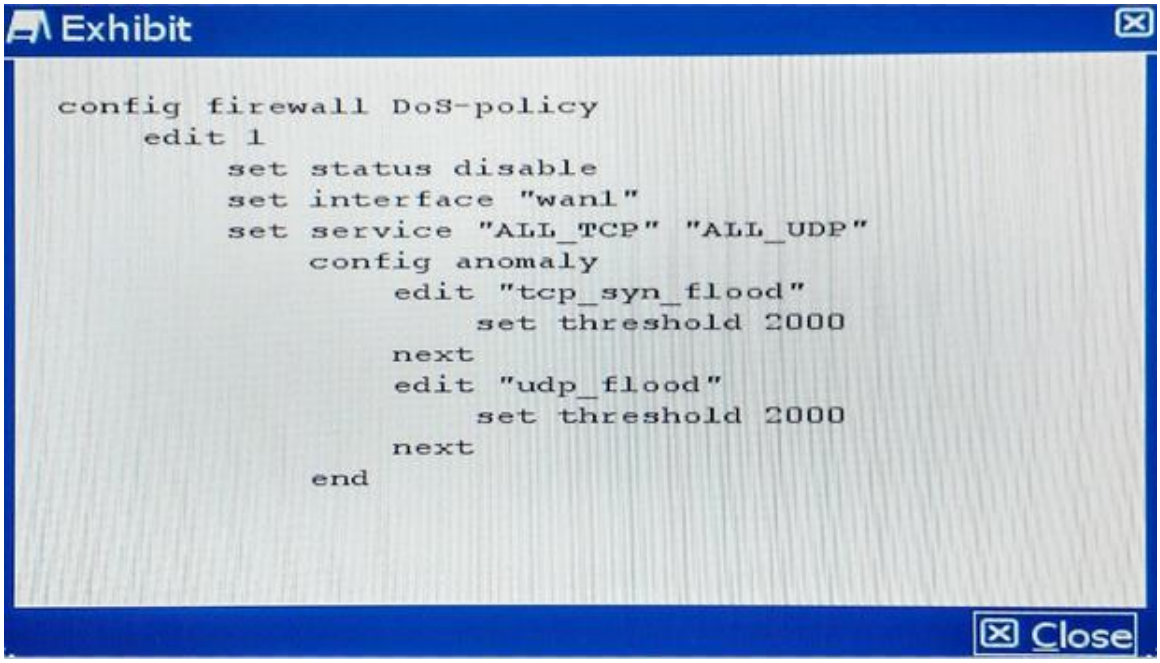
B. Deploy FortiDDos to block brute force attacks. Configure FortiGate to forward only FTPS, HTTP, and HTTPS to FortiWeb. Configure FortiWeb to query the AD server, and apply SSO for Web requests. Also configure it to scan FTPS and Web traffic, then forward allowed traffic to the Web servers.

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.

Answer: D

Question No: 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 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.
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.

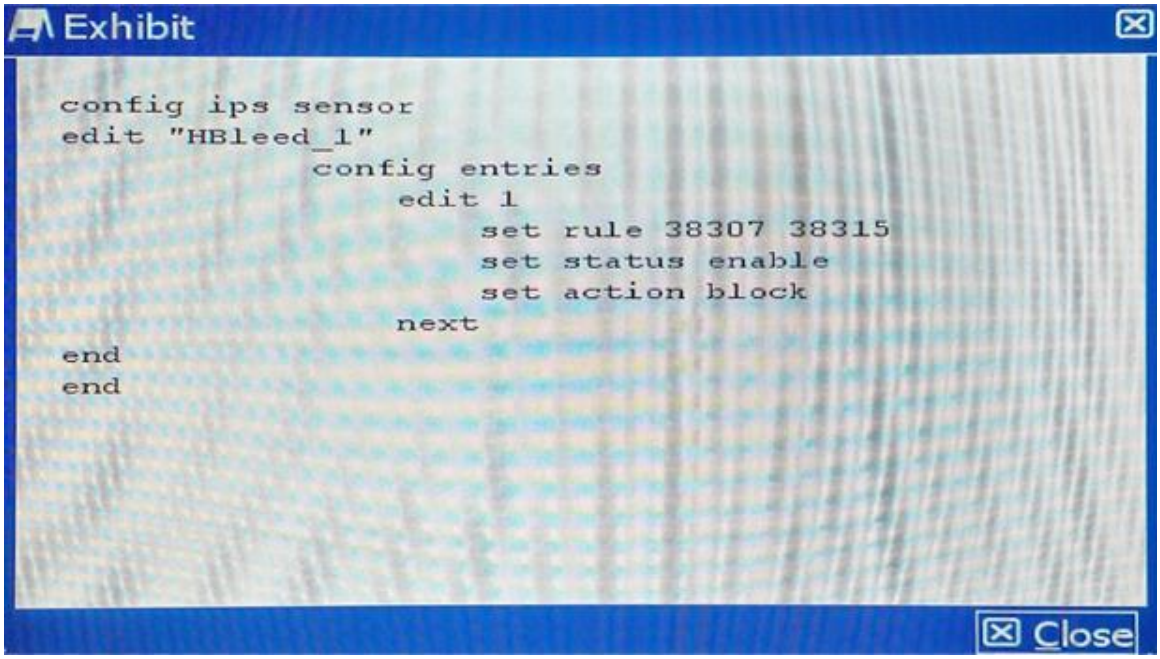
```
config firewall DoS-policy
     edit 1
          set status enable
          set interface "wan1"
          set srcaddr "all"
          set dstaddr "all"
          set service "ALL_TCP" "ALL_UDP"
               config anomaly
                    edit "tcp_syn_flood"
                         set status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

Question No: 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.)




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

Question No: 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.

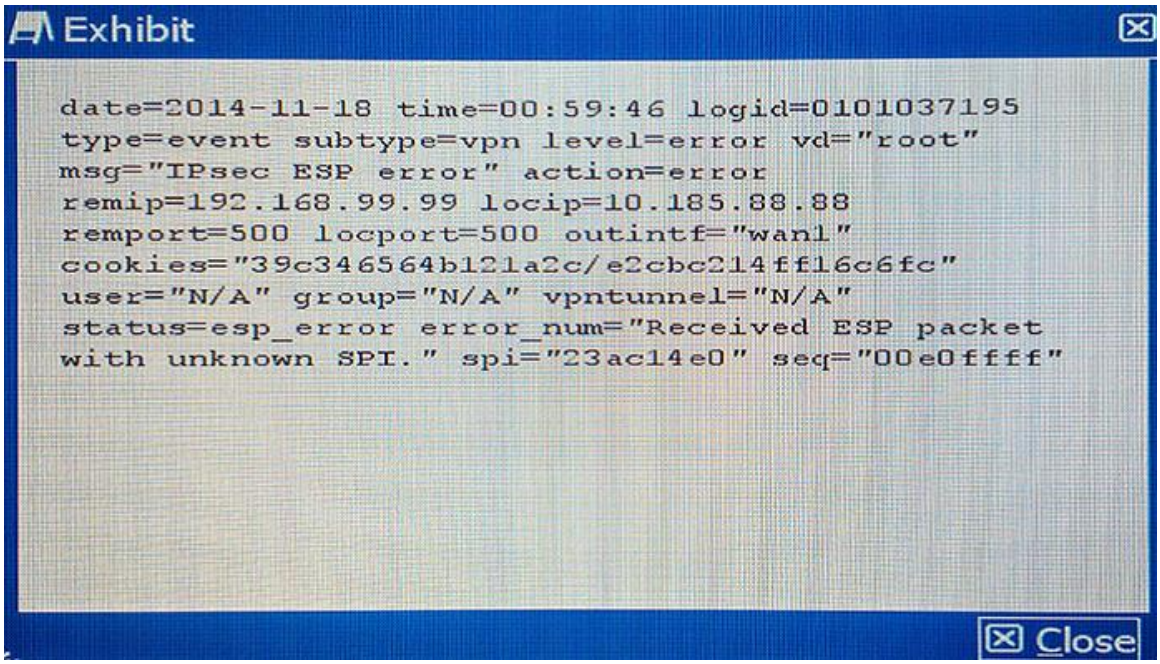
```
config system global
set hostname $SerialNum
end
```

D.

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

Answer: C

Question No: 9
Referring to the exhibit, which statement is true?




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