Vendor: Fortinet

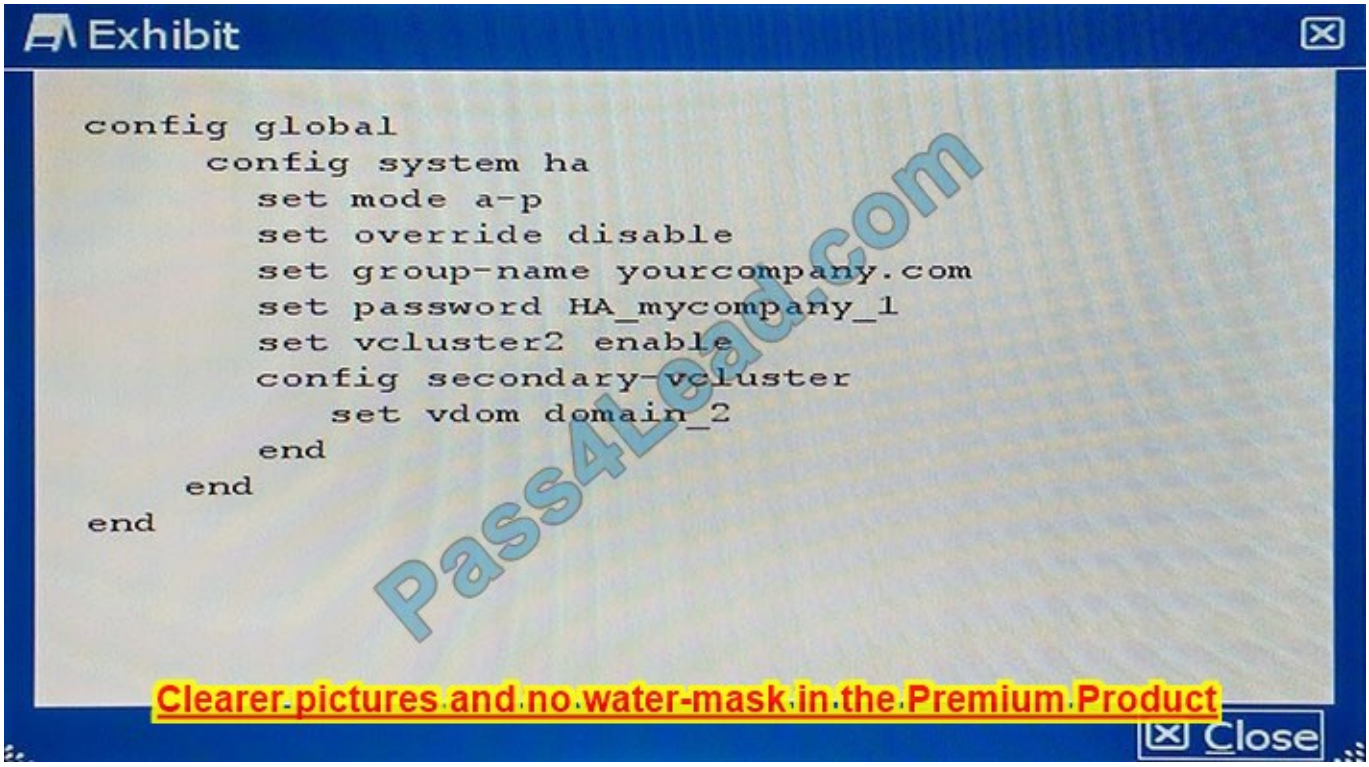
Exam Code:NSE8

Exam Name: Fortinet Network Security Expert 8 Written (800)

Version: Demo

QUESTION 1

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.

Correct Answer: C

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

---

QUESTION 2

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.

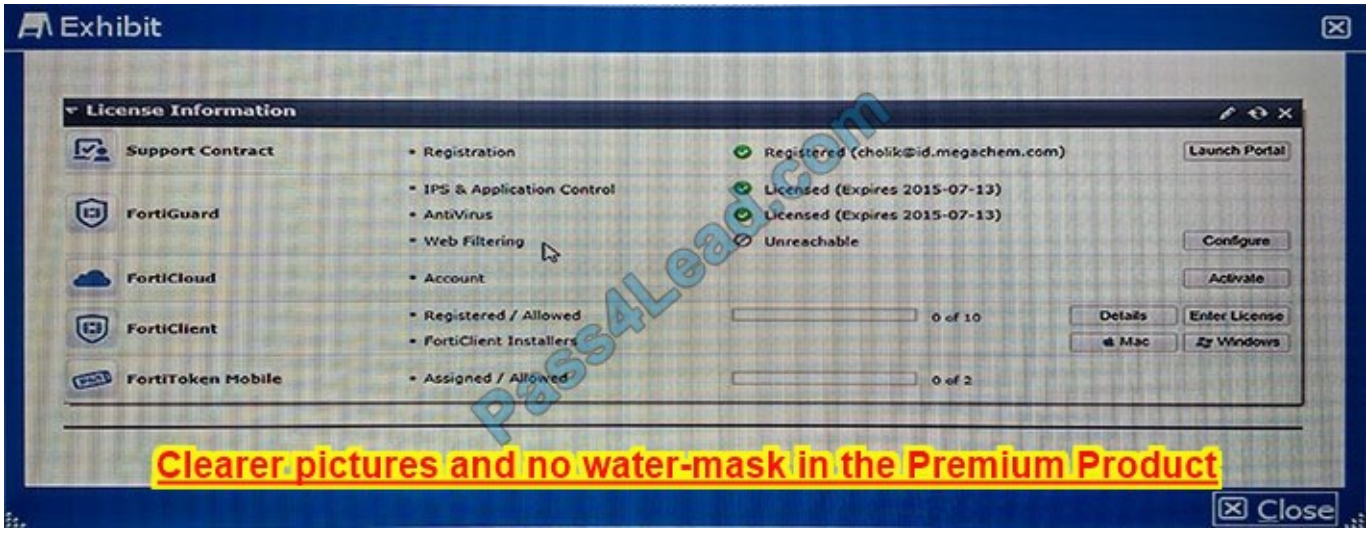
Correct Answer: D

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

Reference: http://cookbook.fortinet.com/providing-single-sign-using-ldap-fsso-agent-advanced-mode-expert/

QUESTION 3

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.

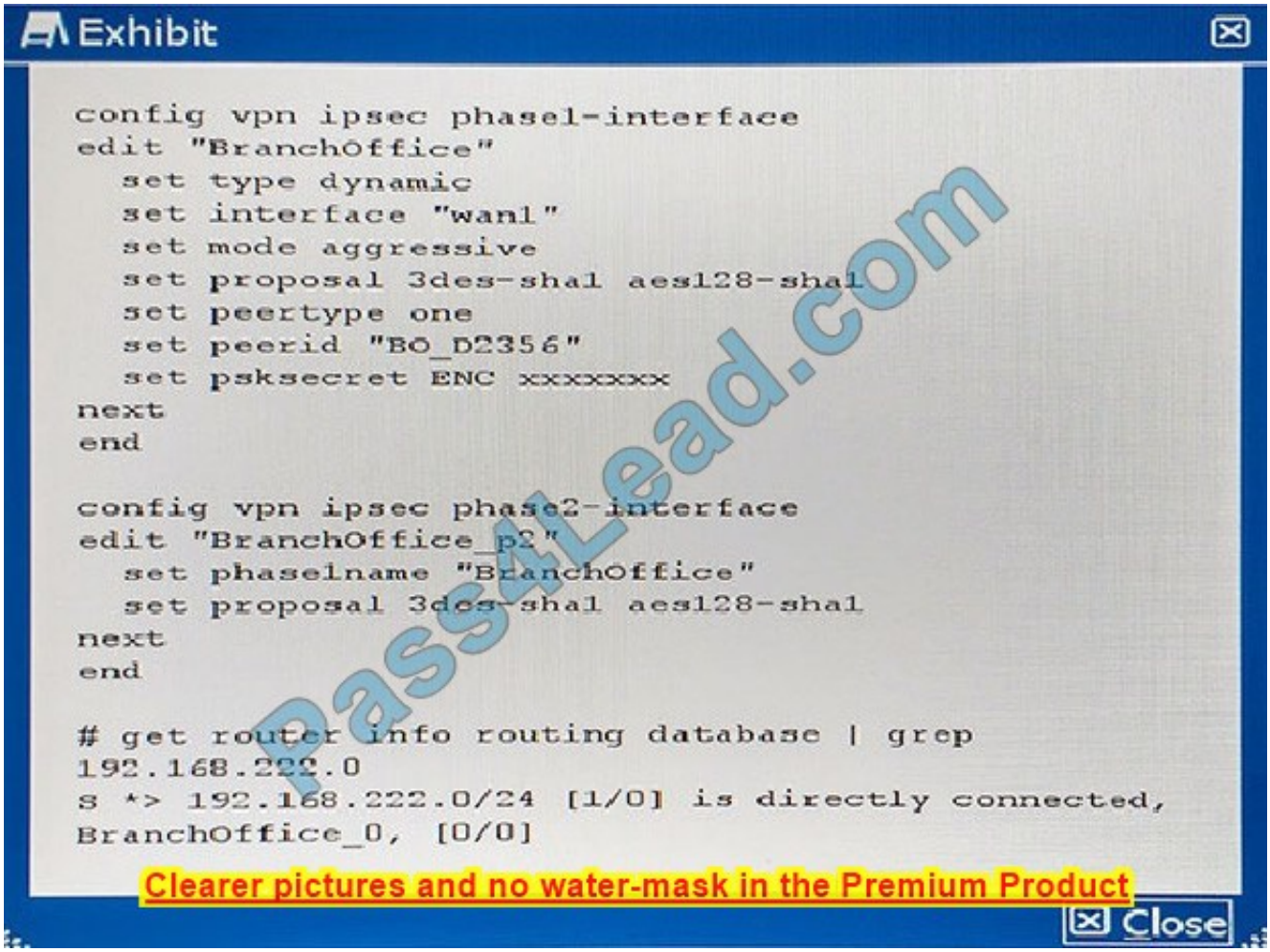
Correct Answer: BD

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 4

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.



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

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.

Exhibit

```
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
```


Close

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
```


A. B. C.

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

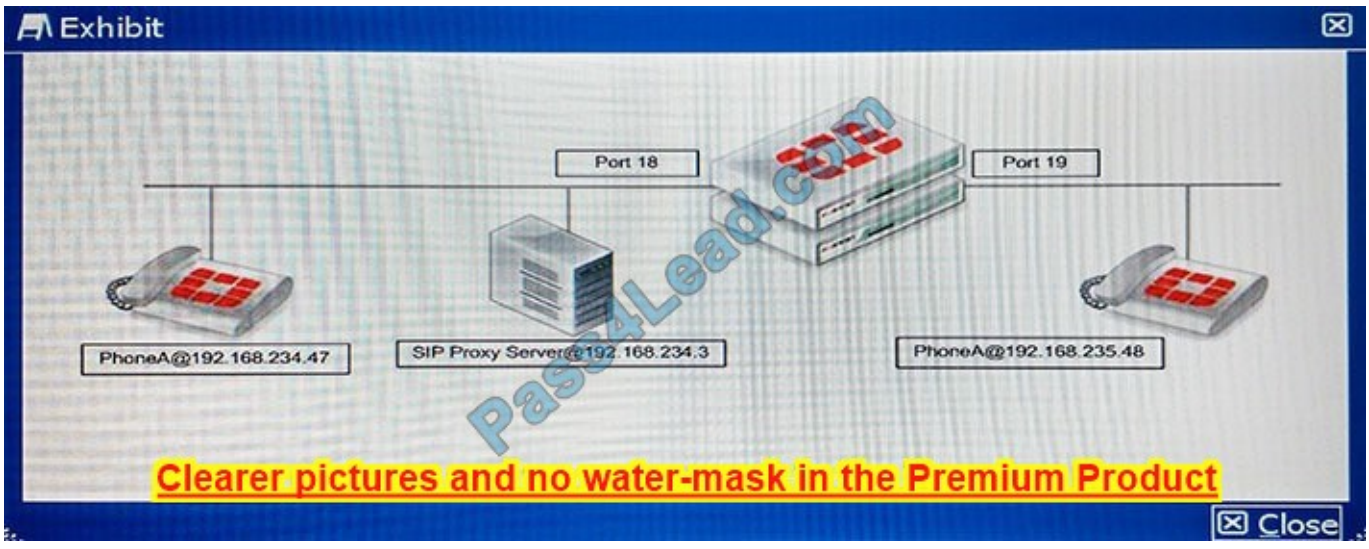

D.

Correct Answer: D

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

---

QUESTION 6



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
```

e

A. B. C. D.

Correct Answer: C

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

---

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.

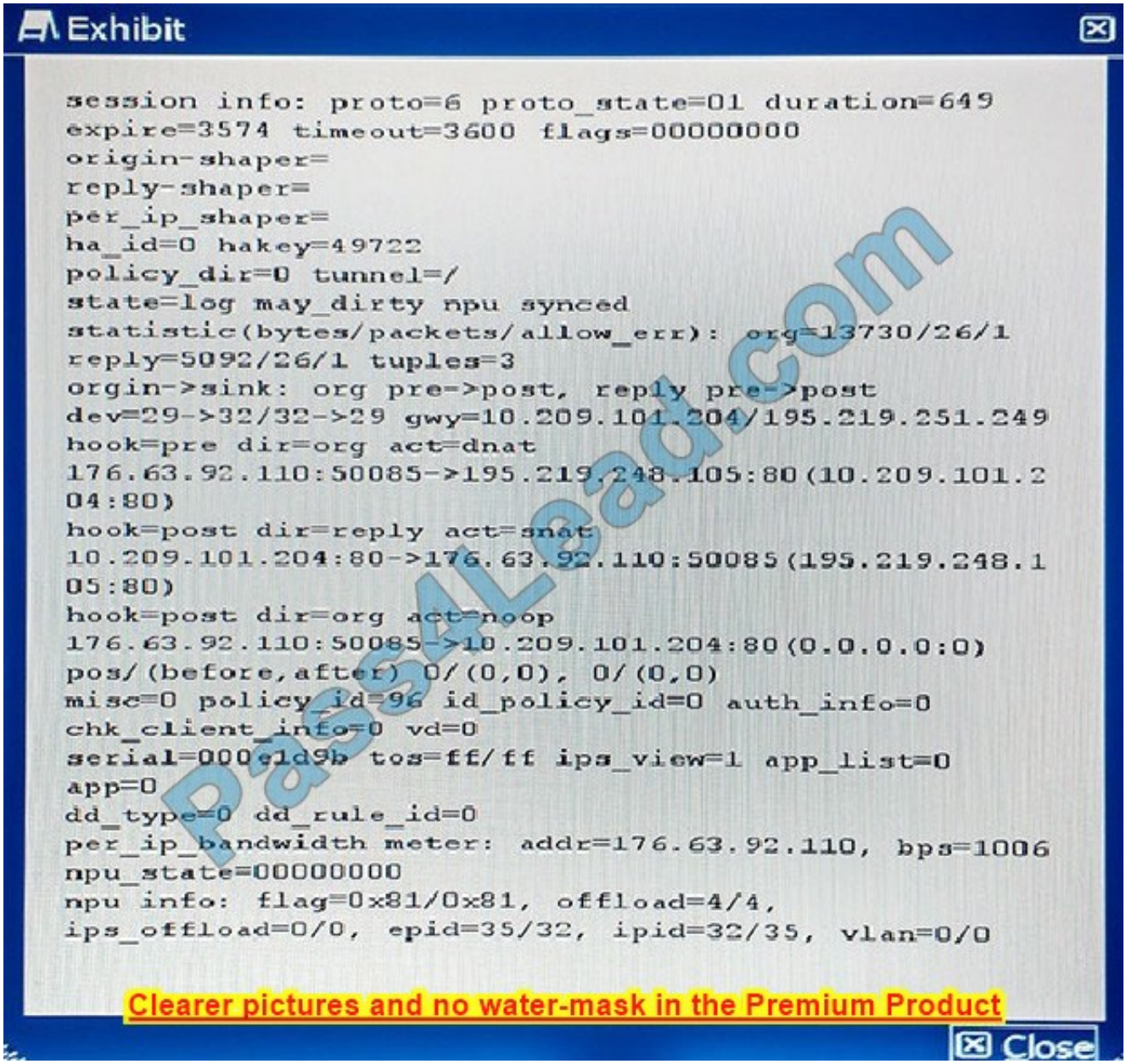
B. RADIUS authentication with each user\\'s IP address stored in a Vendor Specific Attribute (VSA).

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.

Correct Answer: D

QUESTION 8



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

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.

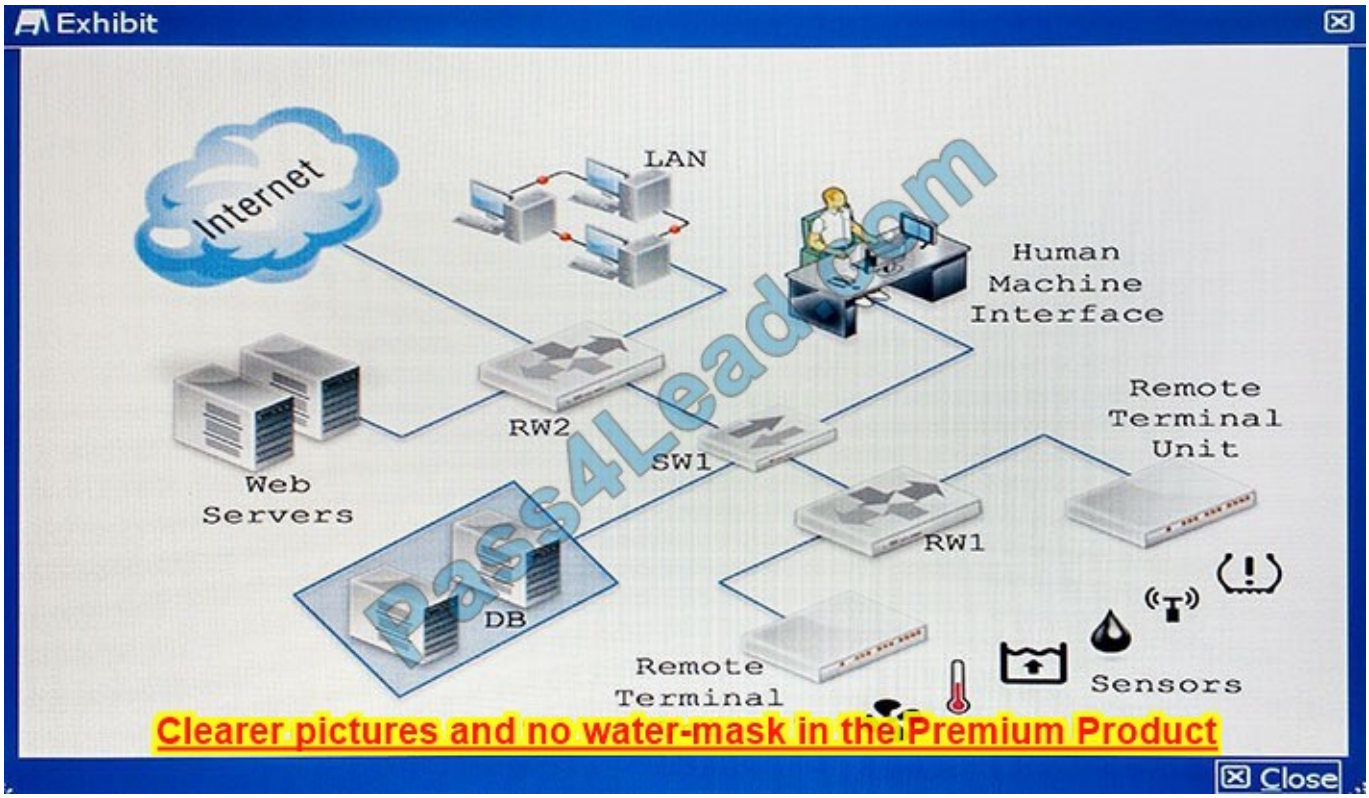
D. No QoS is applied to this traffic.

E. The traffic goes through a VIP applied to policy 96.

Correct Answer: B

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

QUESTION 9



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

A. Replace RW1 with a ruggedized FortiGate and RW2 with a normal FortiGate. Enable industrial category on the application control. Place a FortiGate to secure Web servers. Configure IPsec to secure sensors data. Place a ruggedized FortiAP to provide Wi-Fi to the sensors.

B. Replace RW1 with a normal FortiGate and RW2 with a ruggedized FortiGate. Enable industrial category on the application control. Place a FortiGate to secure Web servers. Configure IPsec to secure sensors data. Place a FortiAP to provide Wi-Fi to the sensors.

C. Replace RW1 with a normal FortiGate and RW2 with a ruggedized FortiGate. Enable industrial category on the Web filter. Place a FortiWeb to secure Web servers. Configure IPsec to secure sensors data. Place a ruggedized FortiAP to provide Wi-Fi to the sensors.

D. Replace RW1 with a normal FortiGate and RW2 with a ruggedized FortiGate. Enable industrial category on the application control. Place a FortiWeb to secure Web servers. Configure IPsec to secure sensors data. Place a ruggedized FortiAP to provide Wi-Fi to the sensors.

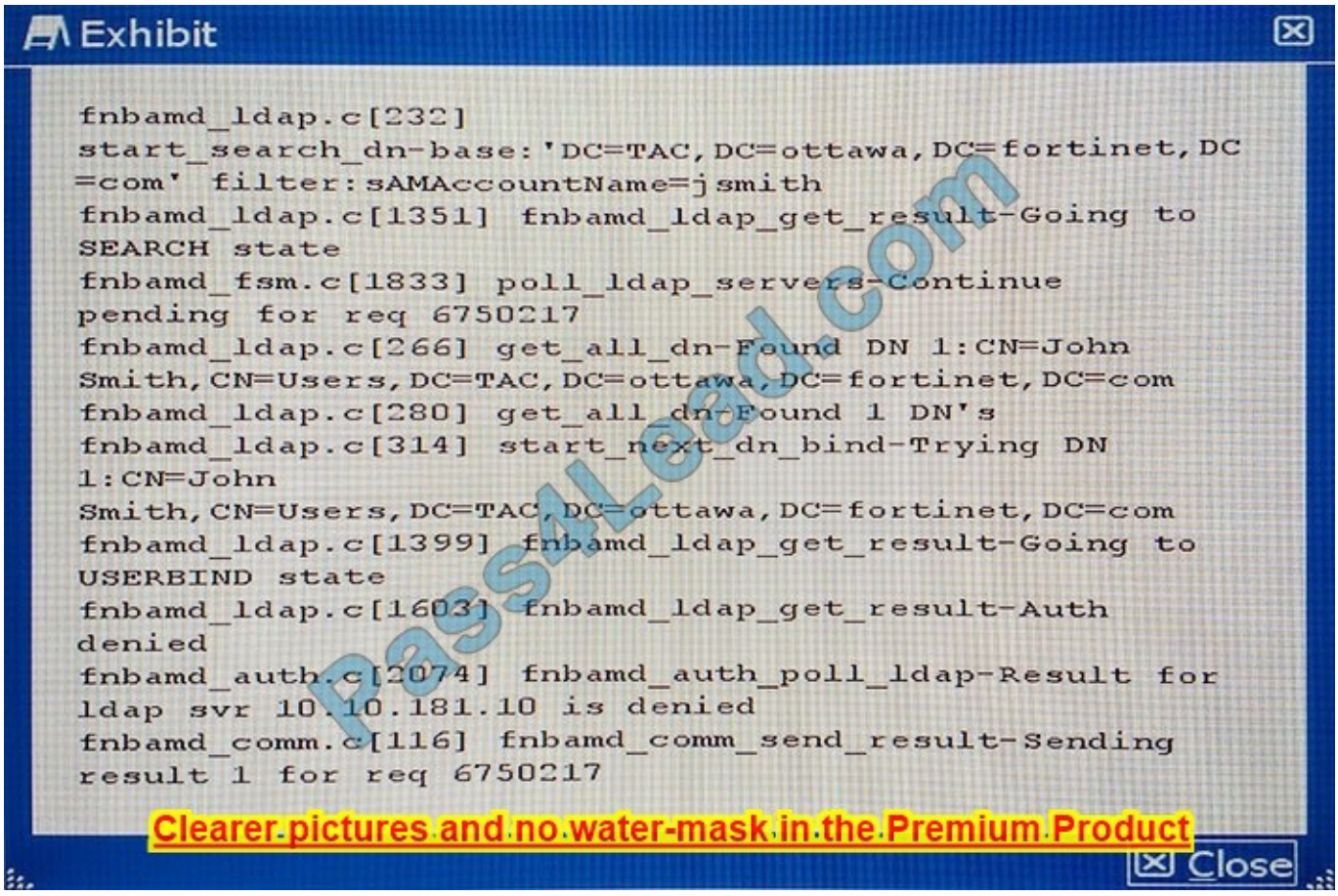
Correct Answer: D

QUESTION 10

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.

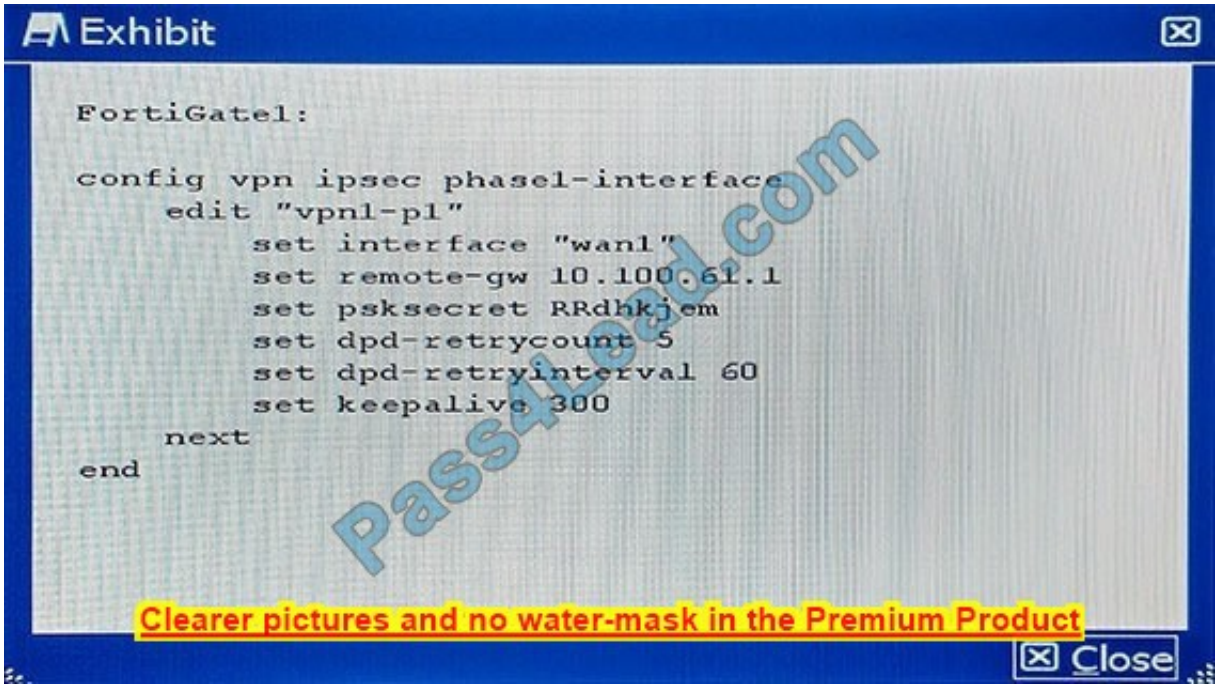
D. The user, John Smith, is using an incorrect password.

Correct Answer: A

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

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.



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

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

QUESTION 12

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

Correct Answer: C

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: