NSE8$^{Q\&As}$

Fortinet Network Security Expert 8 Written (800)

Pass Fortinet NSE8 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/nse8.html

100% Passing Guarantee
100% Money Back Assurance

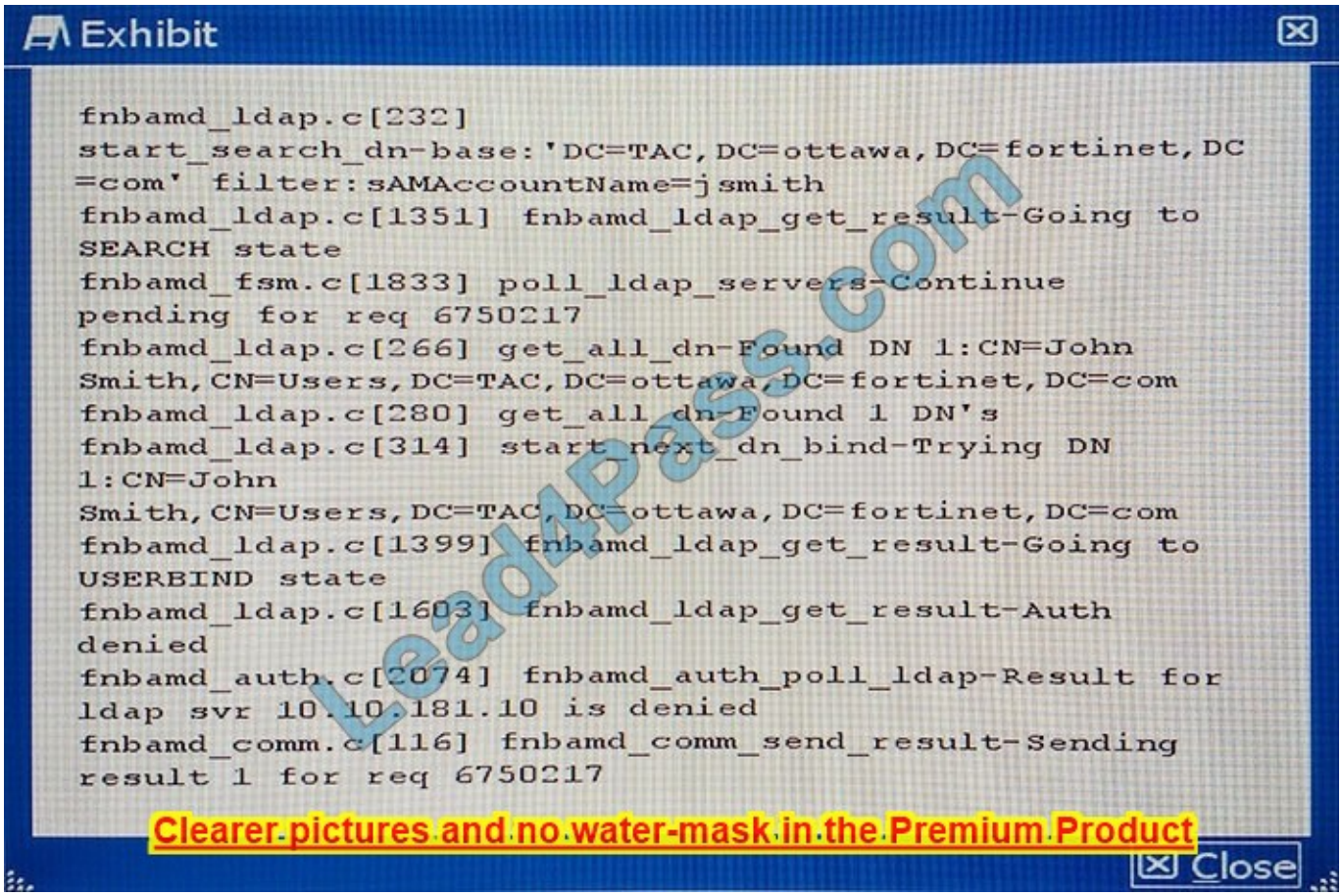
Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

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 2

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.

-

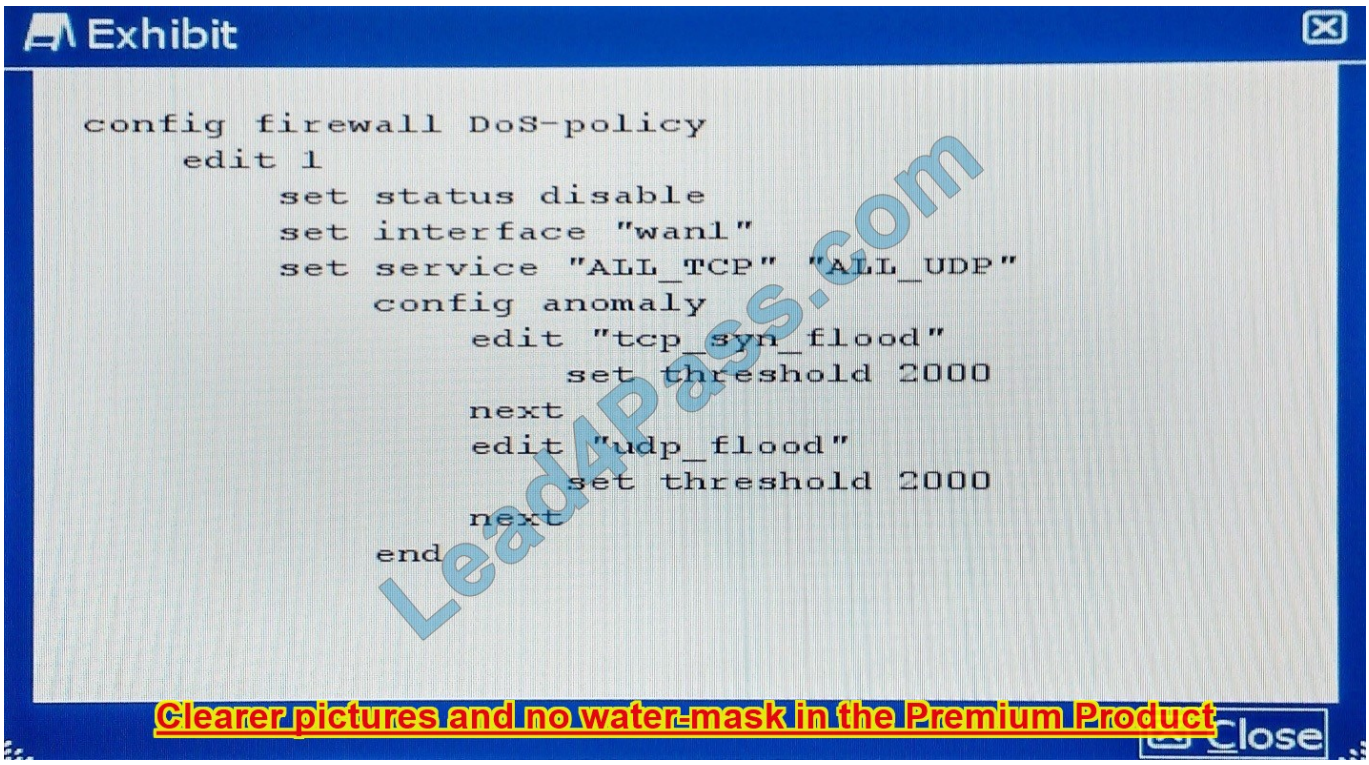
The tcp_syn_flood attacks are to be recorded and blocked.

-

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
```

A. B.

C.

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 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

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
```


Correct Answer: BD

BandD 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 3

A customer wants to implement a RADIUS Single Sign On (RSSO) solution for multiple FortiGate devices. The customer\\'s network already includes a RADIUS server that can generate the logon and logoff accounting records. However, the

RADIUS server can send those records to only one destination.

What should the customer do to overcome this limitation?

A. Send the RADIUS records to an LDAP server and add the LDAP server to the FortiGate configuration.

B. Send the RADIUS records to an RSSO Collector Agent.

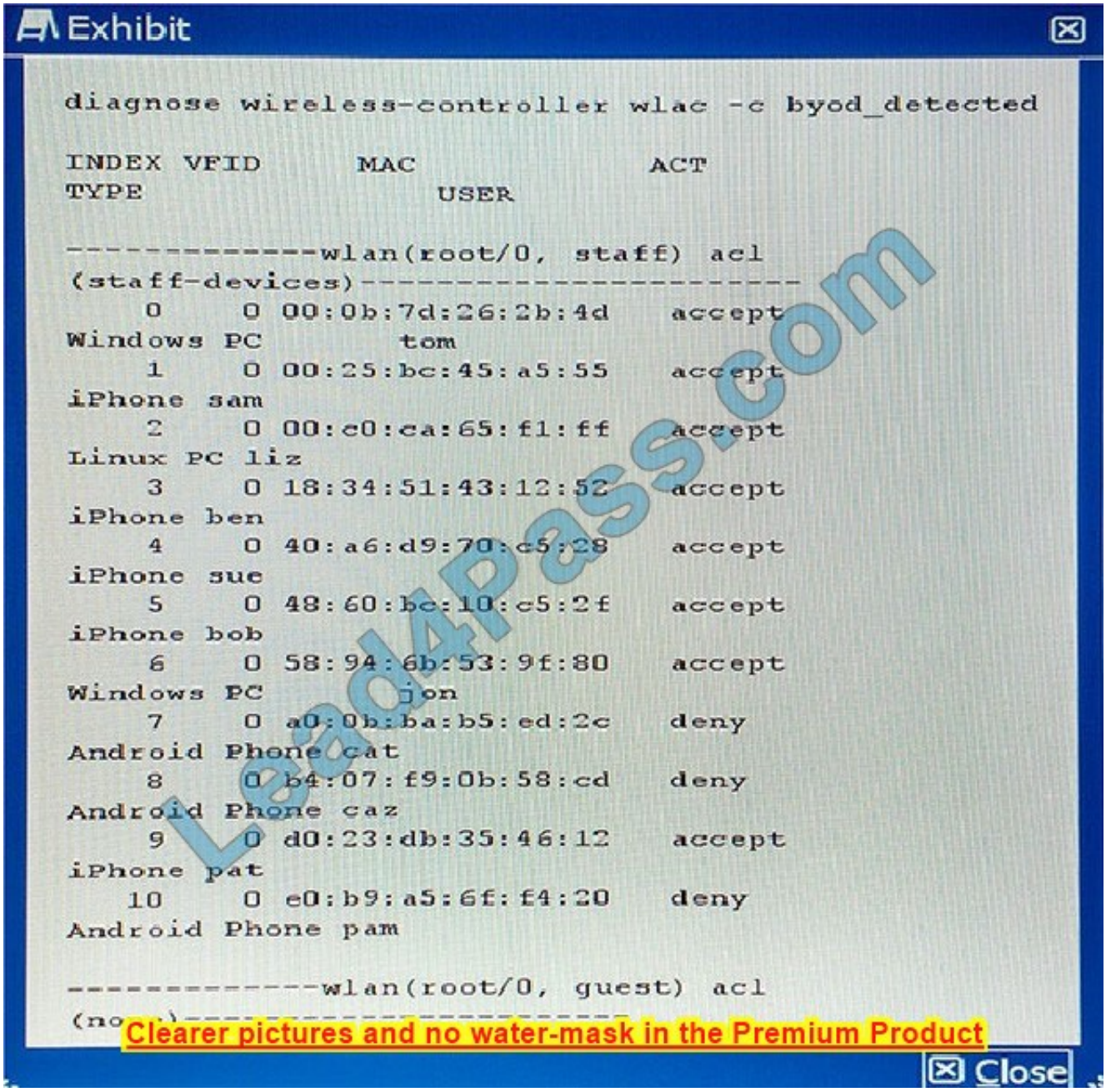
C. Send the RADIUS records to one of the FortiGate devices, which can replicate them to the other FortiGate units.

D. Use the RADIUS accounting proxy feature available in FortiAuthenticator devices.

Correct Answer: B

References: http://docs.fortinet.com/uploaded/files/1937/fortigate-authentication-52.pdf

QUESTION 4



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

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.

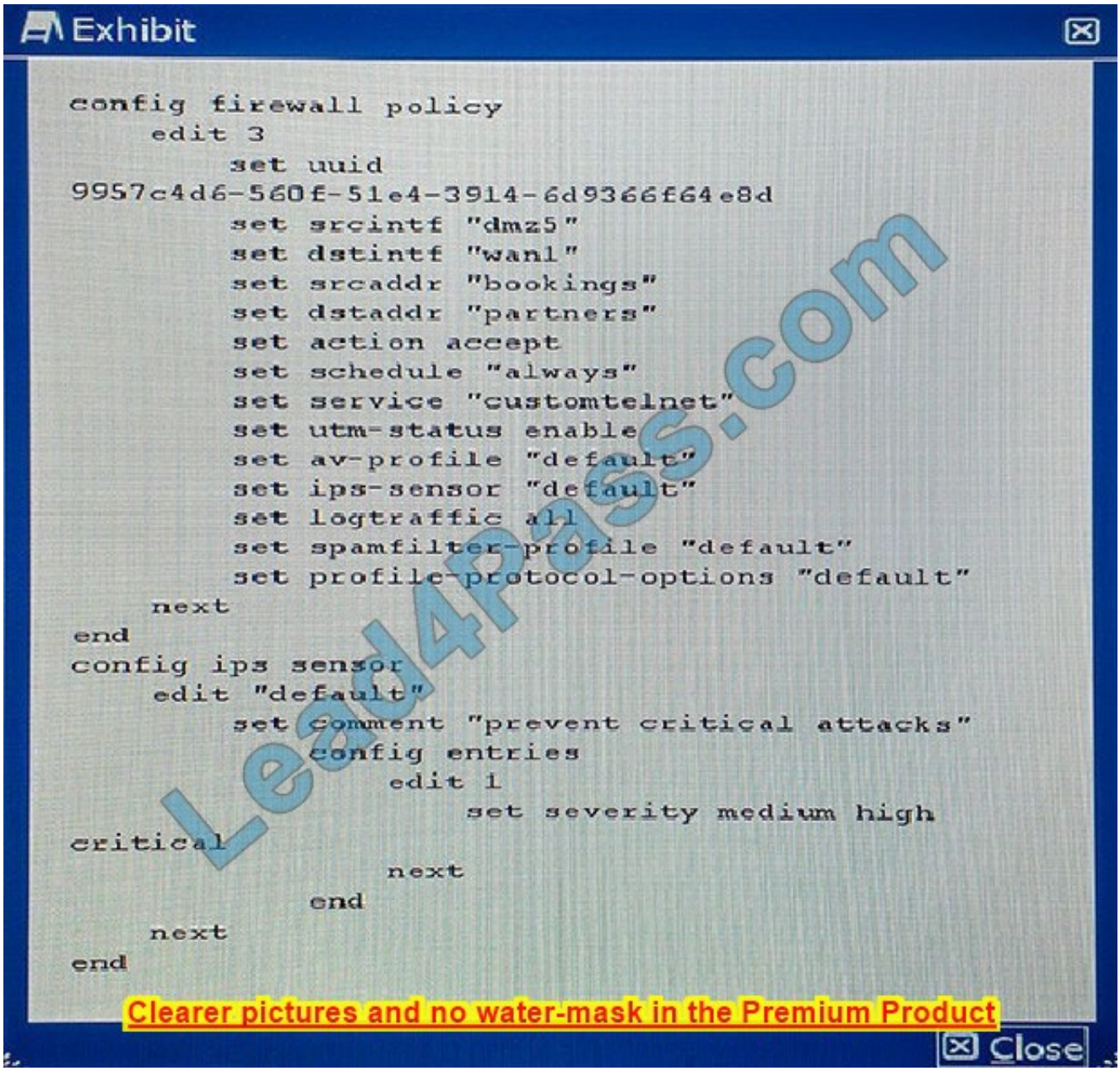
E. The "src-vis" process is active on the staff wireless network VAP interface.

Correct Answer: A

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

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.



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