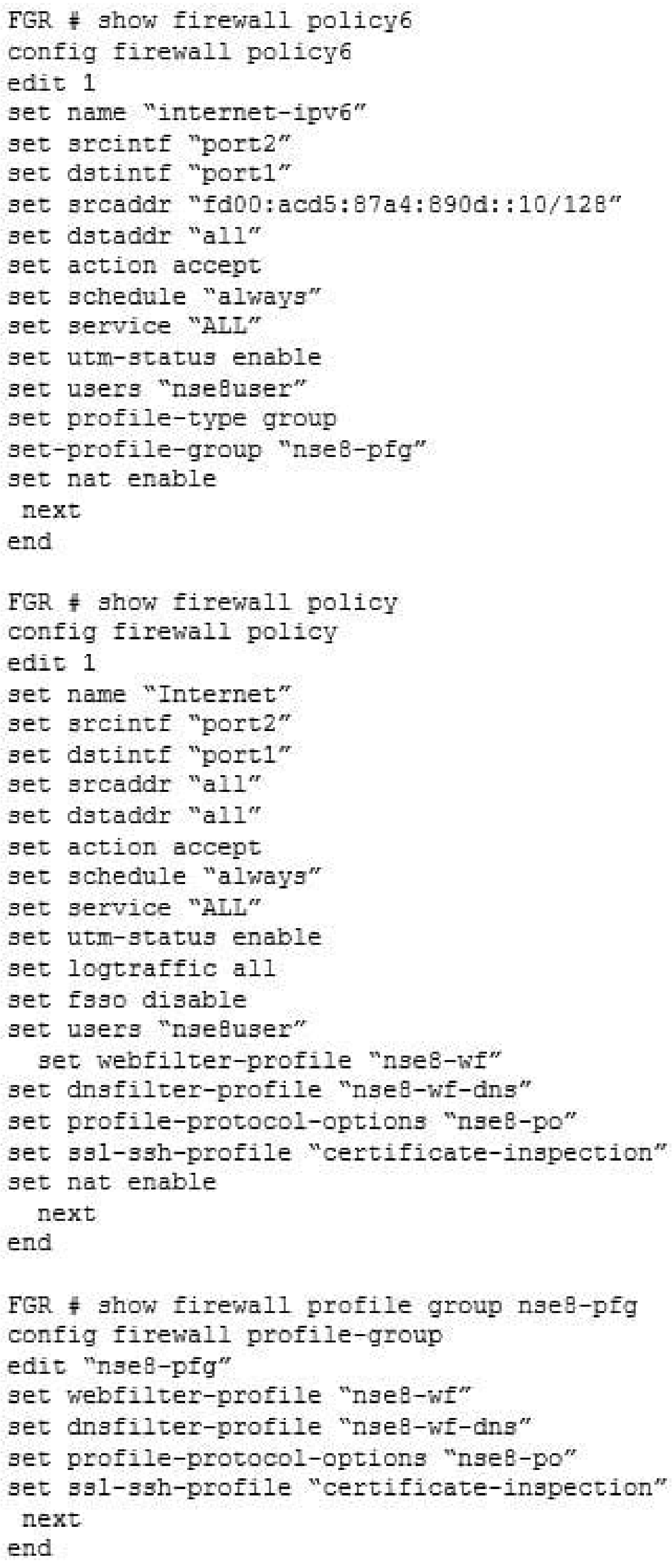
NSE8_810$^{Q\&As}$

Fortinet Network Security Expert 8 Written Exam (810)

QUESTION 1

Click the Exhibit button. Referring to the exhibit, which two statements are true? (Choose two.)



```
FGR # show firewall policy6
config firewall policy6
edit 1
set name "internet-ipv6"
set srcintf "port2"
set dstintf "port1"
set srcaddr "fd00:acd5:87a4:890d::10/128"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set users "nse8user"
set profile-type group
set-profile-group "nse8-pfg"
set nat enable
 next
end

FGR # show firewall policy
config firewall policy
edit 1
set name "Internet"
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set logtraffic all
set fsso disable
set users "nse8user"
  set webfilter-profile "nse8-wf"
set dnsfilter-profile "nse8-wf-dns"
set profile-protocol-options "nse8-po"
set ssl-ssh-profile "certificate-inspection"
set nat enable
  next
end

FGR # show firewall profile group nse8-pfg
config firewall profile-group
edit "nse8-pfg"
set webfilter-profile "nse8-wf"
set dnsfilter-profile "nse8-wf-dns"
set profile-protocol-options "nse8-po"
set ssl-ssh-profile "certificate-inspection"
 next
end
```

A. The IPv4 traffic for nse8user is filtered using the DNS profile.

B. The IPv6 traffic for nse8user is filtered using the DNS profile.

C. The IPv4 policy is allowing security profile groups.

D. The Web traffic for nse8user is being filtered differently in IPv4 and IPv6.

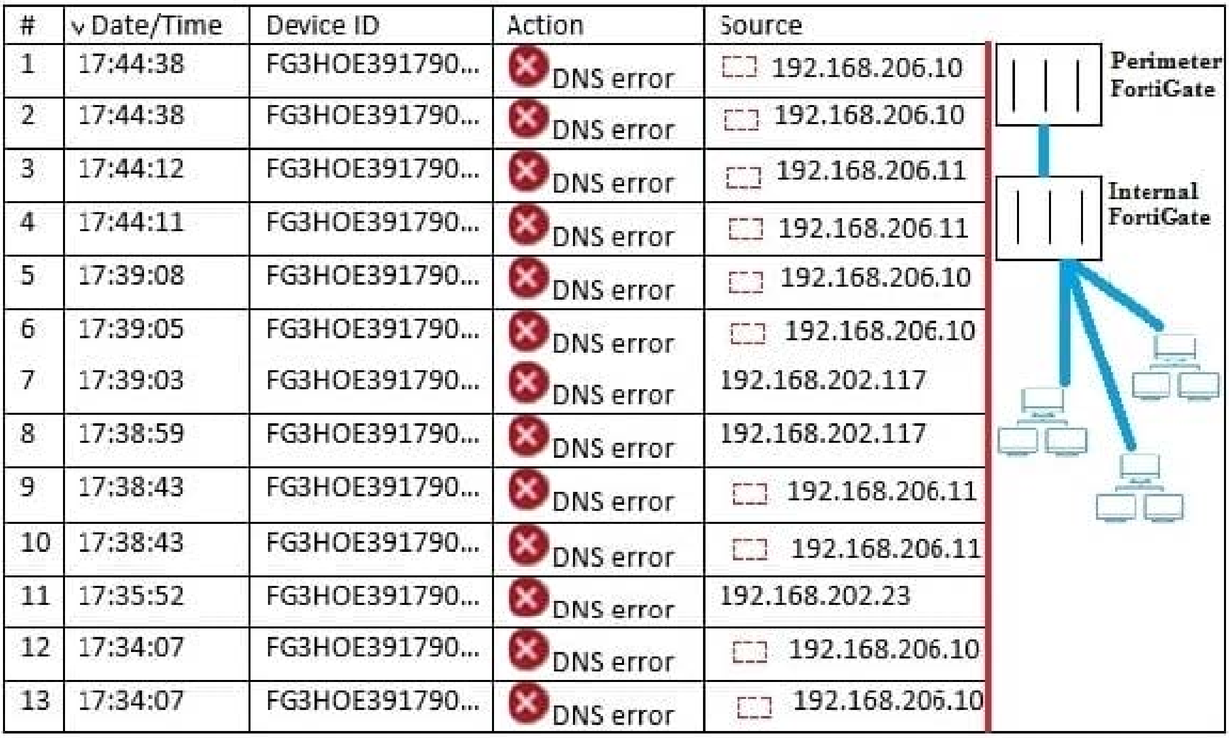
Correct Answer: AD

QUESTION 2

Exhibit

Click the Exhibit button.

You have deployed several perimeter FortiGates with internal segmentation FortiGates behind them. All FortiGate devices are logging to FortiAnalyzer. When you search the logs in FortiAnalyzer for denied traffic, you see numerous log messages, as shown in the exhibit, on your perimeter FortiGates only.



#	∨ Date/Time	Device ID	Action	Source
1	17:44:38	FG3HOE391790...	✖ DNS error	192.168.206.10
2	17:44:38	FG3HOE391790...	✖ DNS error	192.168.206.10
3	17:44:12	FG3HOE391790...	✖ DNS error	192.168.206.11
4	17:44:11	FG3HOE391790...	✖ DNS error	192.168.206.11
5	17:39:08	FG3HOE391790...	✖ DNS error	192.168.206.10
6	17:39:05	FG3HOE391790...	✖ DNS error	192.168.206.10
7	17:39:03	FG3HOE391790...	✖ DNS error	192.168.202.117
8	17:38:59	FG3HOE391790...	✖ DNS error	192.168.202.117
9	17:38:43	FG3HOE391790...	✖ DNS error	192.168.206.11
10	17:38:43	FG3HOE391790...	✖ DNS error	192.168.206.11
11	17:35:52	FG3HOE391790...	✖ DNS error	192.168.202.23
12	17:34:07	FG3HOE391790...	✖ DNS error	192.168.206.10
13	17:34:07	FG3HOE391790...	✖ DNS error	192.168.206.10

Which two actions would reduce the number of these log messages? (Choose two.)

A. Apply an application control profile lo the perimeter FortiGates that does not inspect DNS traffic to the outbound firewall policy.

B. Configure the internal ForbGates to communicate to ForpGuard using port 8888.

C. Disable DNS events logging horn ForirGate In the config log fortianalyser filter section.

D. Remove DNS signature*