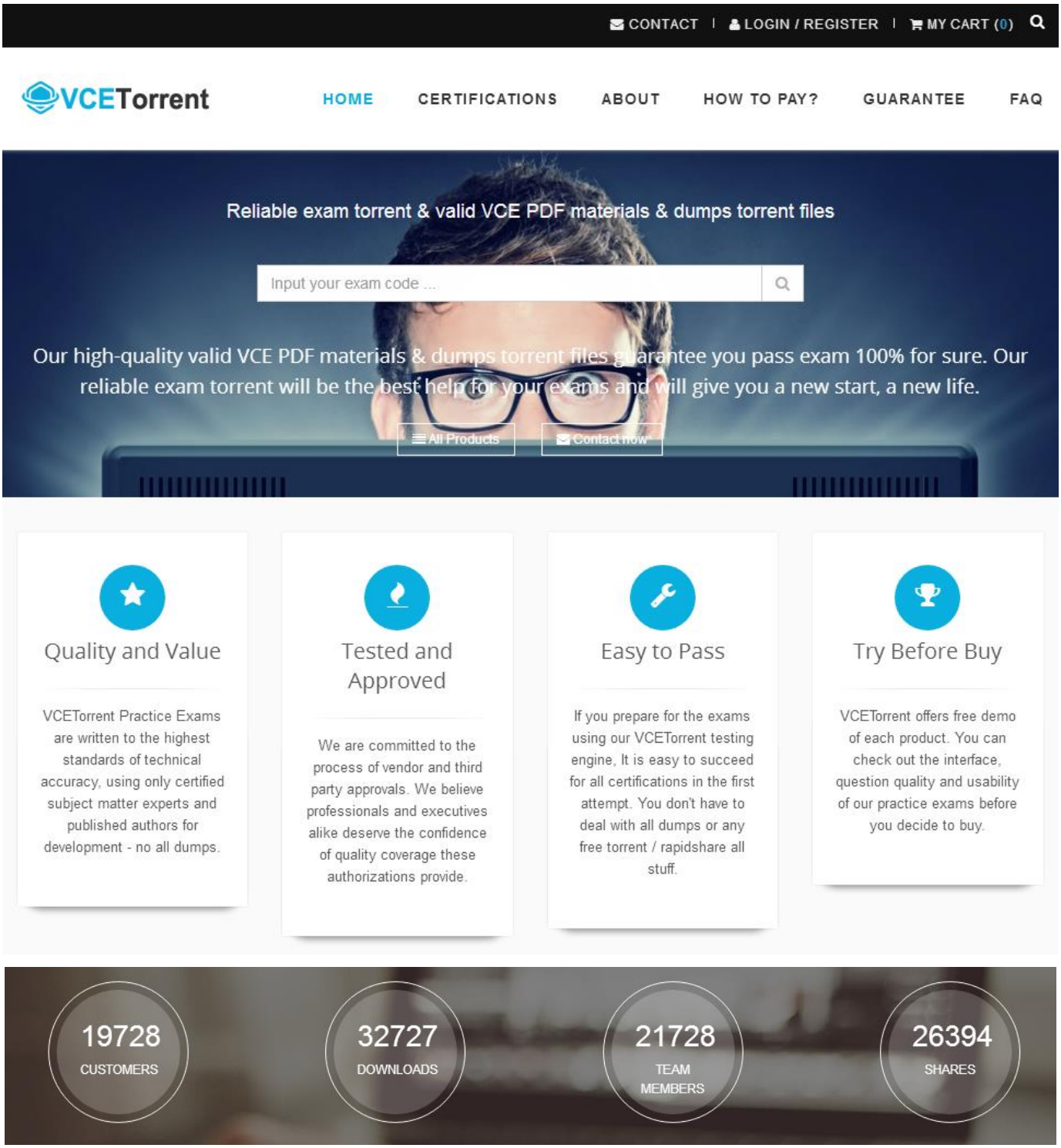
VCETorrent



http://www.vcetorrent.com

Reliable exam torrent & valid VCE PDF materials & dumps torrent files

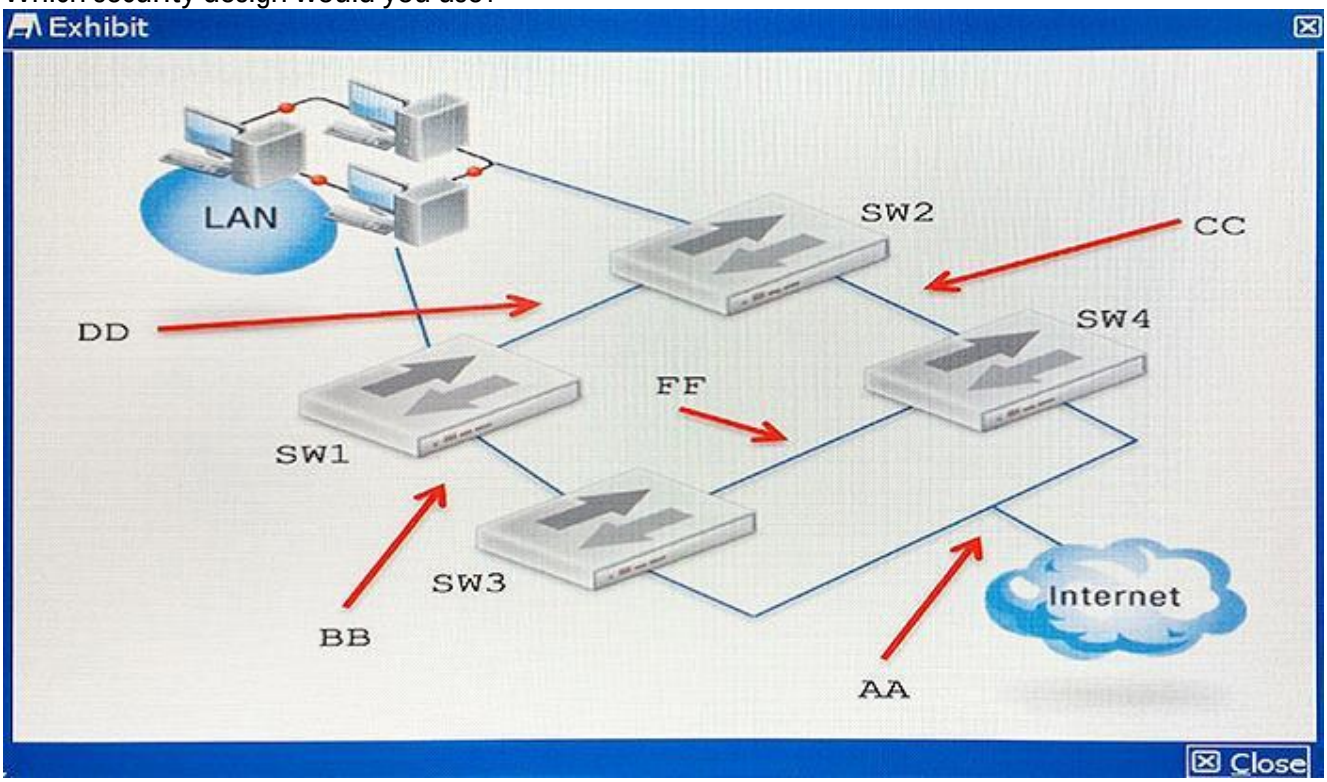
Exam : **NSE8**

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

Vendor : Fortinet

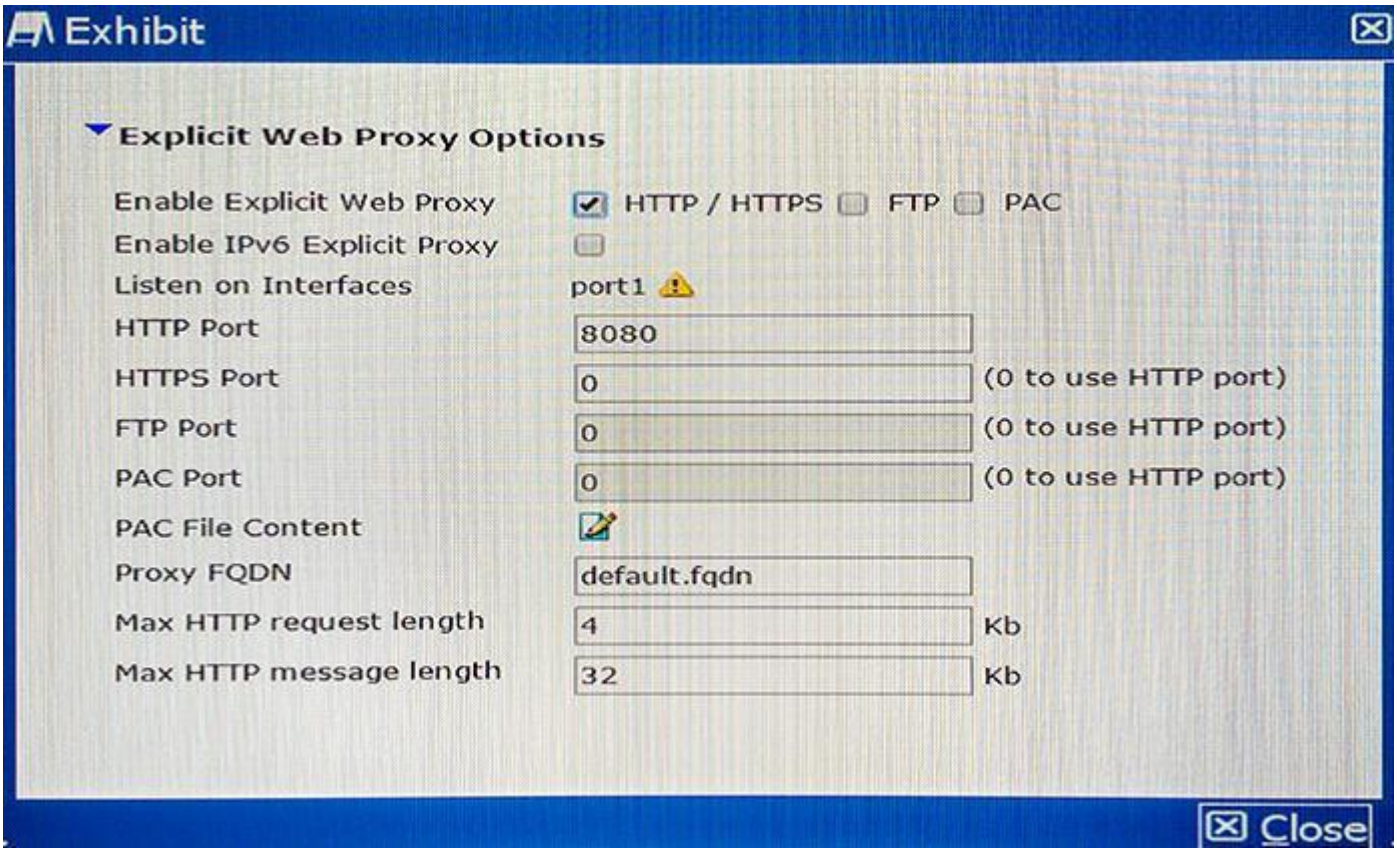
Version : DEMO

NO.1 A customer wants to secure the network shown on the exhibit with a full redundancy design.
Which security design would you use?



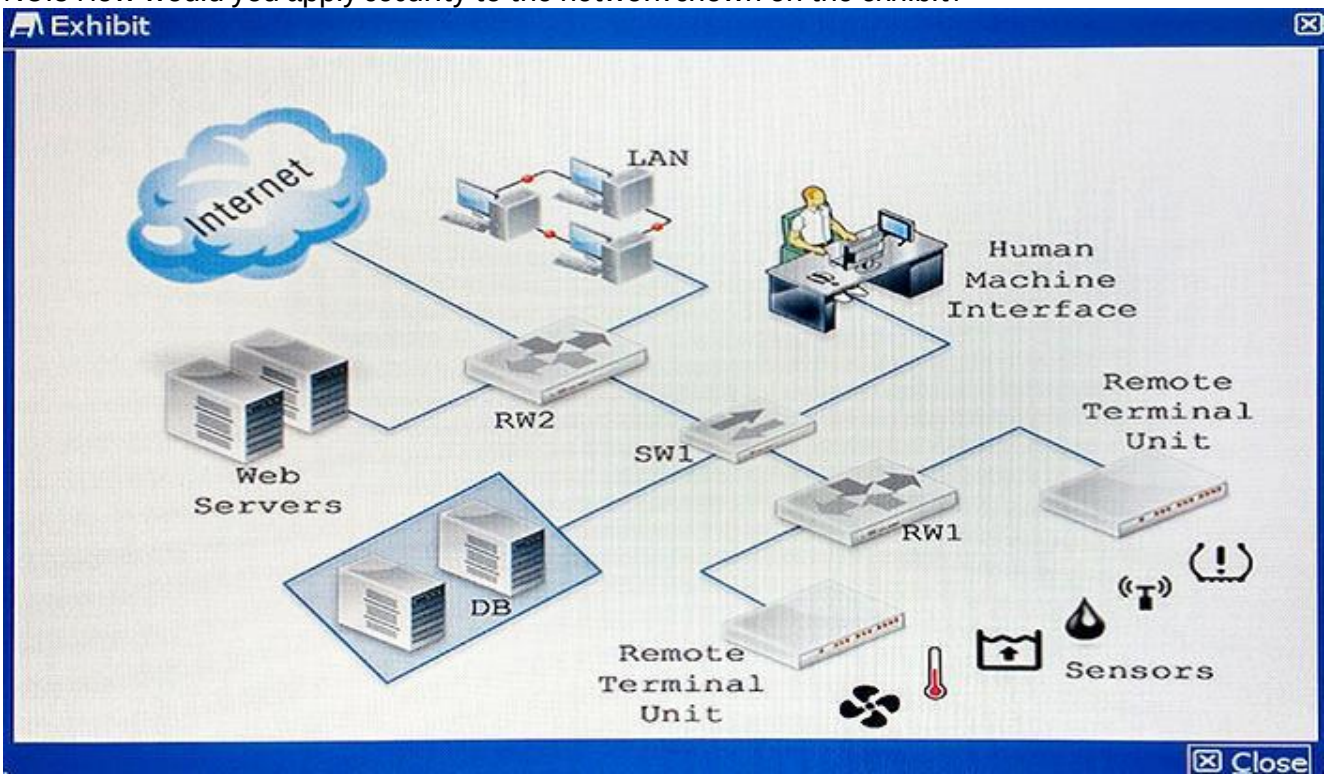
A. Place a Forti Gate FGCP Cluster between DD and AA, then connect it to SWI, SW2, SW3, and SW4.
B. Place a Forti Gate FGCP Cluster between BB and CC, then connect it to SWI, SW2, SW3, and SW4.
C. Place a Forti Gate FGCP Cluster between BB and AA, then connect it to SWI, SW2, SW3, and SW4.
D. Place a Forti Gate FGCP Cluster between DD and FF, then connect it to SWI, SW2, SW3, and SW4.
Answer: A

NO.2 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 1 72.16.10.254.
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

NO.3 How would you apply security to the network shown on the exhibit?



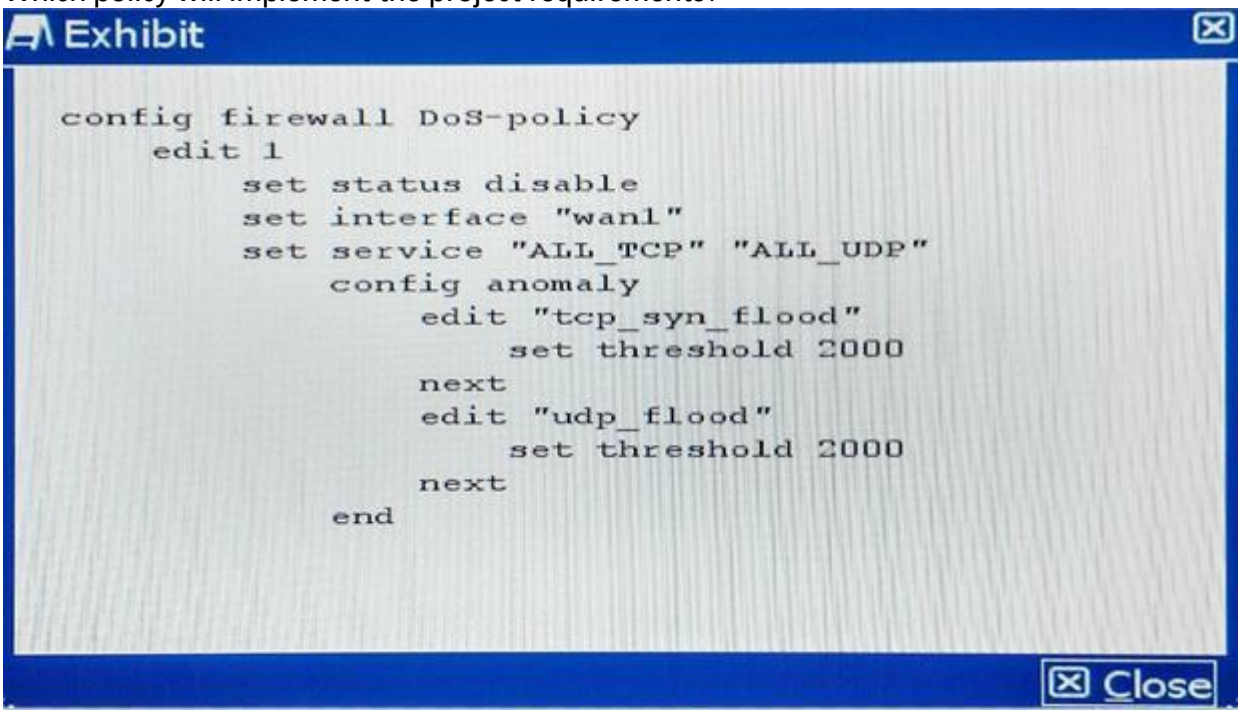
A. Replace RW1 with a ruggedized FortiGate and RW2 with a normal FortiGate. Enable industrial category on the application control Place a FortiGate to secure Web servers. Configure IPsec to secure
sensors data. Place a ruggedized FortiAP to provide Wi-Fi to the sensors.
B. Replace RW1 with a normal FortiGate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

NO.4 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.
Answer: B

NO.5 A cafe offers free Wi-Fi. Customers' 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".
Answer: B

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
```

A. Option A

B. Option B

C. Option C
D. Option D
Answer: B,D