CÔNG TY CP ĐẦU TƯ PHÁT TRIỂN CÔNG NGHỆ ỨNG DỤNG TOÀN CẦU HYPERLOGY

HƯỚNG DẪN
CẤU HÌNH FORTIGATE FIREWALL

Hà nội 10/2007

Mục lục

1. Giới thiệu FortiGate

1.1. Các giao diện của FortiGate

Console:
Ta có thể truy cập giao diện dòng lệnh (Command Line Interface-CLI) của FortiGate thông qua kết nối giữa cổng Serial của 1 máy tính quản trị với cổng Serial của FortiGate .
Internal:
Đây là giao diện kết nối với mạng LAN của đơn vị .Dựa trên thiết kế của mạng để cấu hình các thông số như IP, DHCP,DNS Server ...
WAN:
Đây là giao diện kết nối với mạng Internet thông qua Modem (Lease Line,ADSL)
DMZ
Đây là giao diện kết nối với vùng mạng cần độ bảo mật cao ,hạn chế các truy cập từ bên ngoài Internet ,LAN... dựa trên các chính sách (Policy) do người quản trị đặt ra.Các máy chủ như Mail Server,Web Server.. thường đặt ở trong vùng này.
USB:
Đây là giao diện dùng để backup,restore,upgrade Firmware cho FortiGate .Ngoài ra nó còn dùng để kết nối với modem dial-up làm đường dự phòng cho kết nối ra Internet.

1.2. Các đèn báo hiệu

Hiển thị trạng thái của FortiGate : nguồn,trạng thái của các Interface
Power : có các trạng thái sau:
Nhấp nháy : FortiGate đang khởi động
Xanh : FortiGate đang hoạt động bình thường
Tắt : FortiGate tắt nguồn
Internal,WAN.DMZ có các trạng thái sau :
Xanh : cáp đấu nối đúng đã sử dụng, thiết bị đấu nối đến đã bật.
Nhấp nháy : mạng đang hoạt động trên Interface này.
Tắt : chưa có kết nối
Link : Nếu xanh là mạng đang hoạt động ở tôc độ 100Mbps

2. Cấu hình FortiGate

2.1. Các cách truy nhập cấu hình FortiGate

FortiGate hỗ trợ các phương thức truy nhập và cấu hình sau:

- Console:
- http:
- https:
- telnet:
- ssh:
- snmp:

2.2. Lần đầu tiên cấu hình FortiGate

Lần đầu tiên được đưa và sử dụng, FortiGate có cấu hình do nhà sản xuất đặt sẵn bao gồm:

- Mode hoạt động mặc định: NAT
- Tên và Password truy nhập mặc định: admin/trống

- Địa chỉ IP mặc định của các giao diện :
  Internal : 192.168.1.99/24
  WAN1 : 192.168.100.99/24
  WAN2 : 192.168.101.99/24
  DMZ : 10.10.10.1/24
- Giao thức cho phép truy nhập mặc định: telnet, http, https,

2.3. Các bước cấu hình

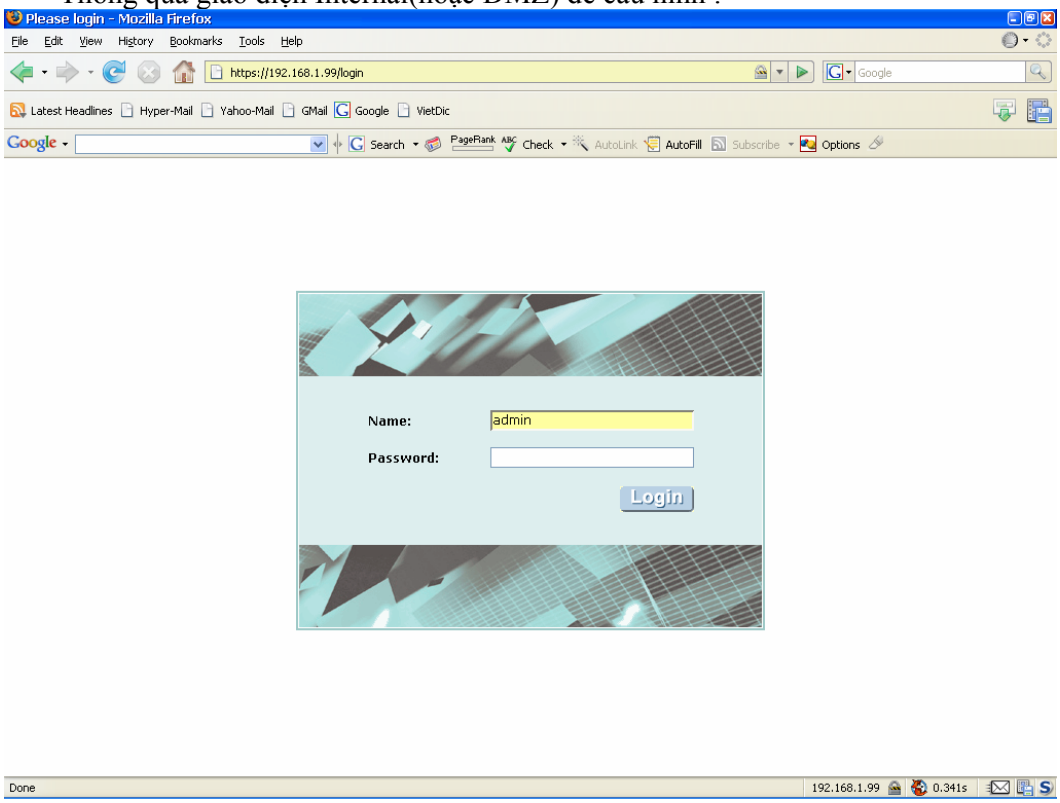
Cấu hình FortiGate cần tuân theo các bước sau:

- Cấu hình mode hoạt động của FortiGate:
- Cấu hình các giao diện
- Cấu hình DHCP
- Cấu hình các địa chỉ và vùng địa chỉ
- Cấu hình các dịch vụ
- Cấu hình các Protection profile
- Cấu hình các Policy
- Cấu hình Virtual IP
- Cấu hình dịch vụ AntiVirus
- Cấu hình dịch vụ AntiSpam
- Cấu hình dịch vụ IPS
- Cấu hình dịch vụ Web filter
- Cấu hình ghi log

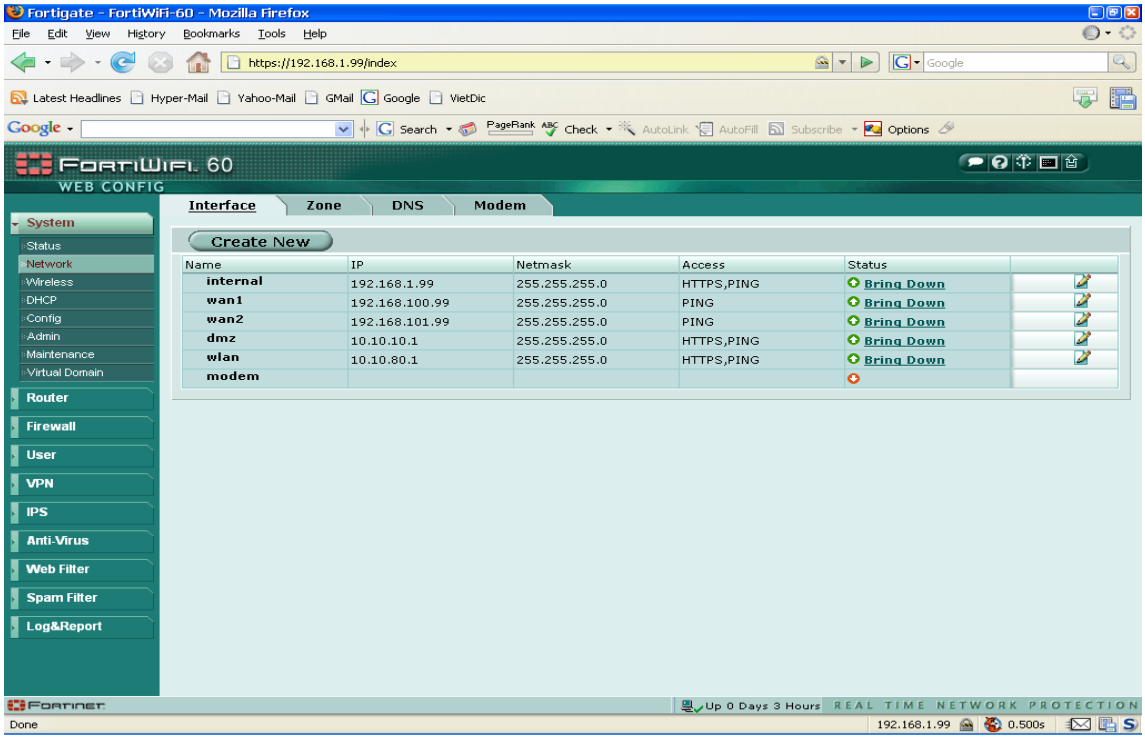
2.4. Cấu hình mode hoạt động của FortiGate

Trên giao diện web : https

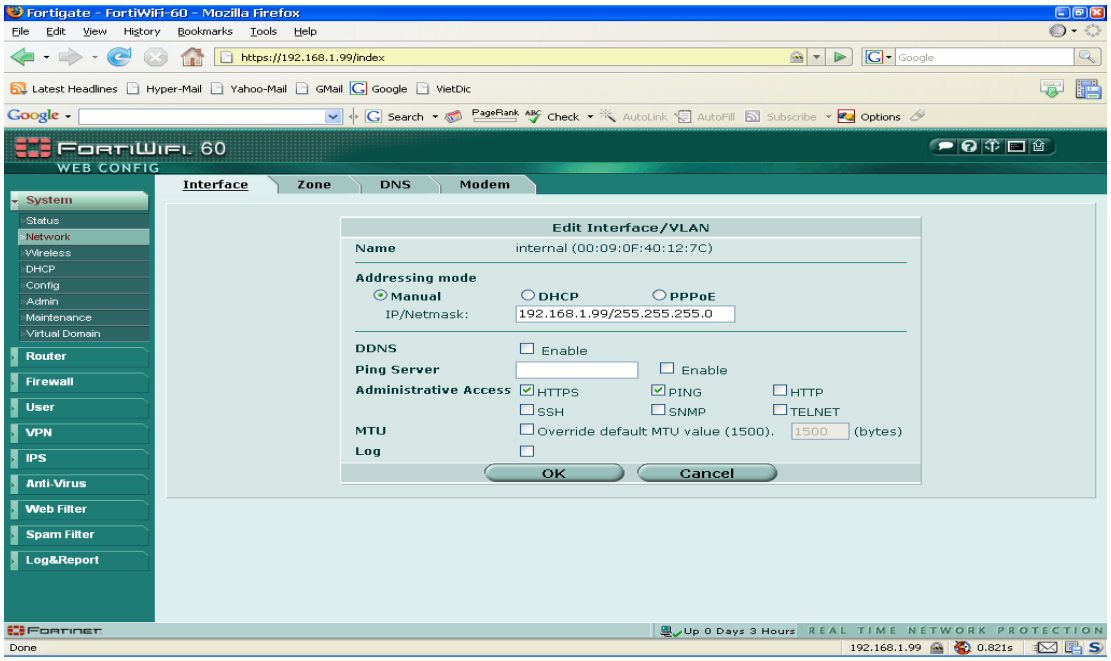
Thông qua giao diện Internal(hoặc DMZ) để cấu hình :



Tên truy cập : admin
Mật khẩu : để trống
Chọn "Login" , sau đó chọn System – Network



Tại cột Access hiển thị cho ta thấy các Mode được phép hoạt động trên từng giao diện. Muốn thay đổi Mode của từng giao diện ,tại cuối dòng của giao diện cần đổi Mode ta chọn nút để thay đổi Mode theo yêu cầu.



Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.5. Cấu hình các giao diện

Trên giao diện web: http, https

Chọn "Login" , sau đó chọn System – Network. Chọn giao diện cần thay đổi

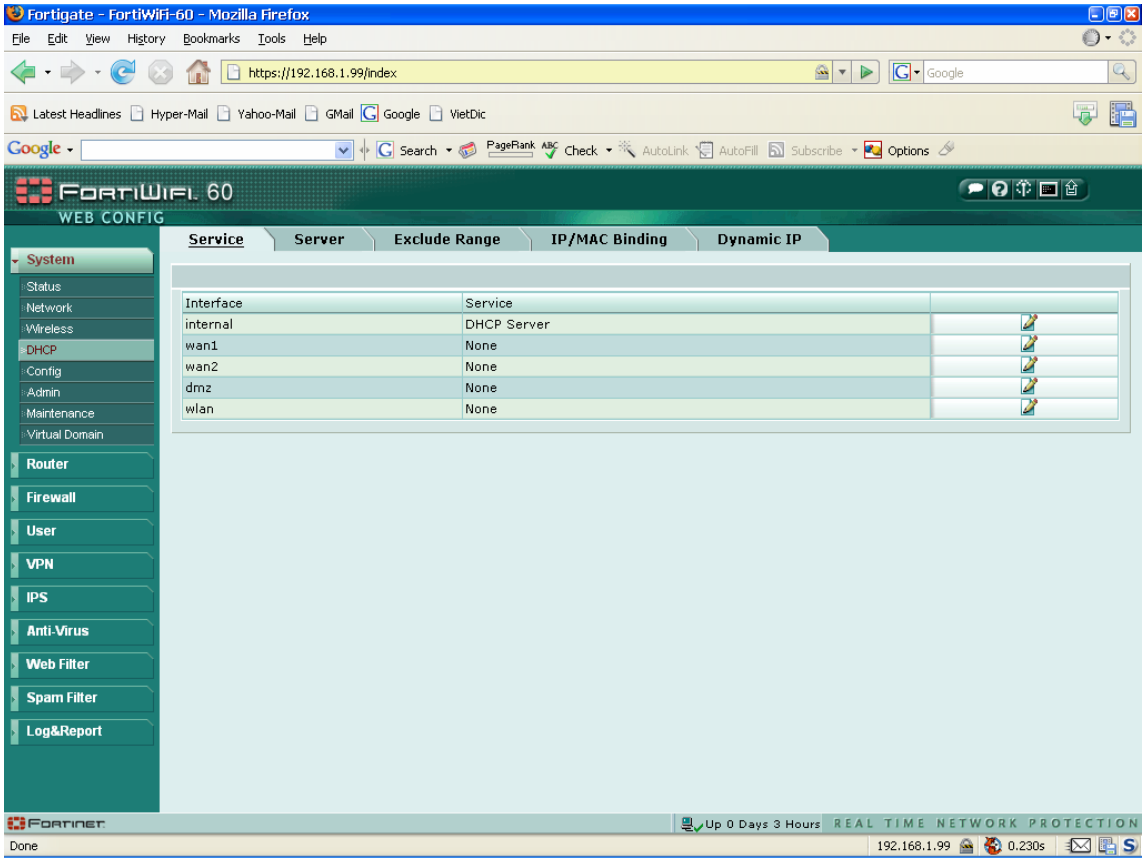
Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

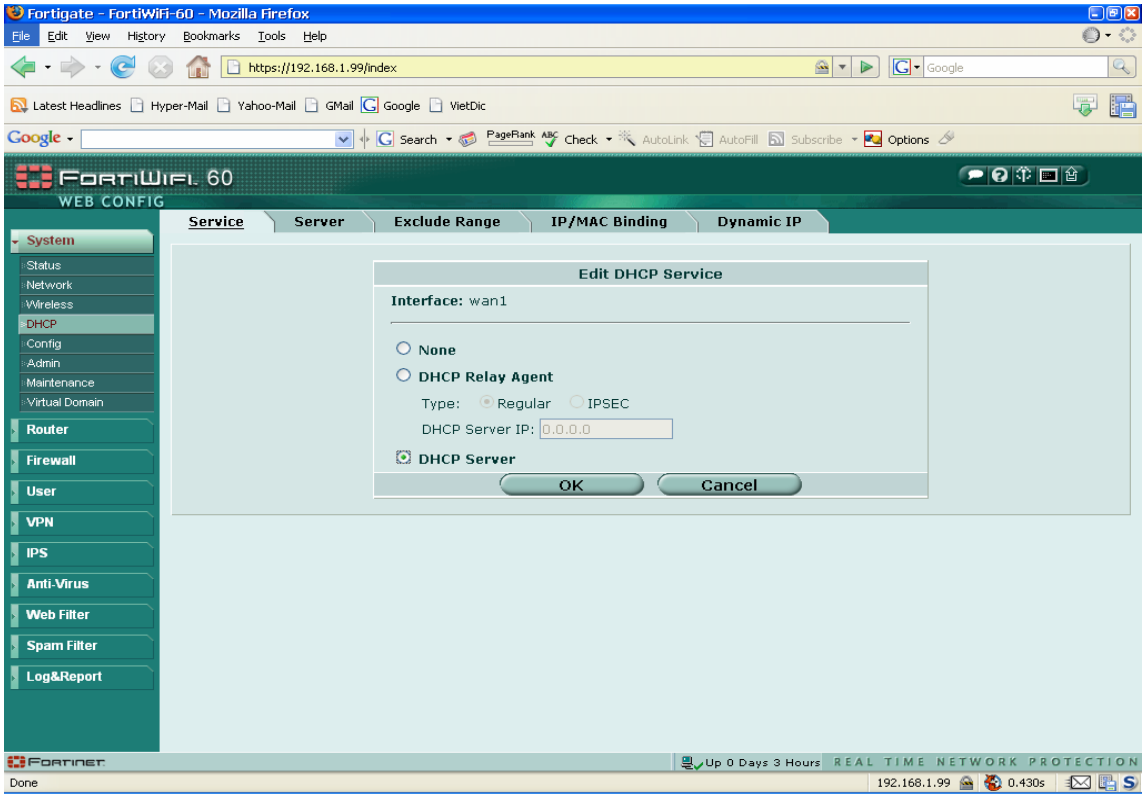
2.6. Cấu hình DHCP

Trên giao diện web: http, https

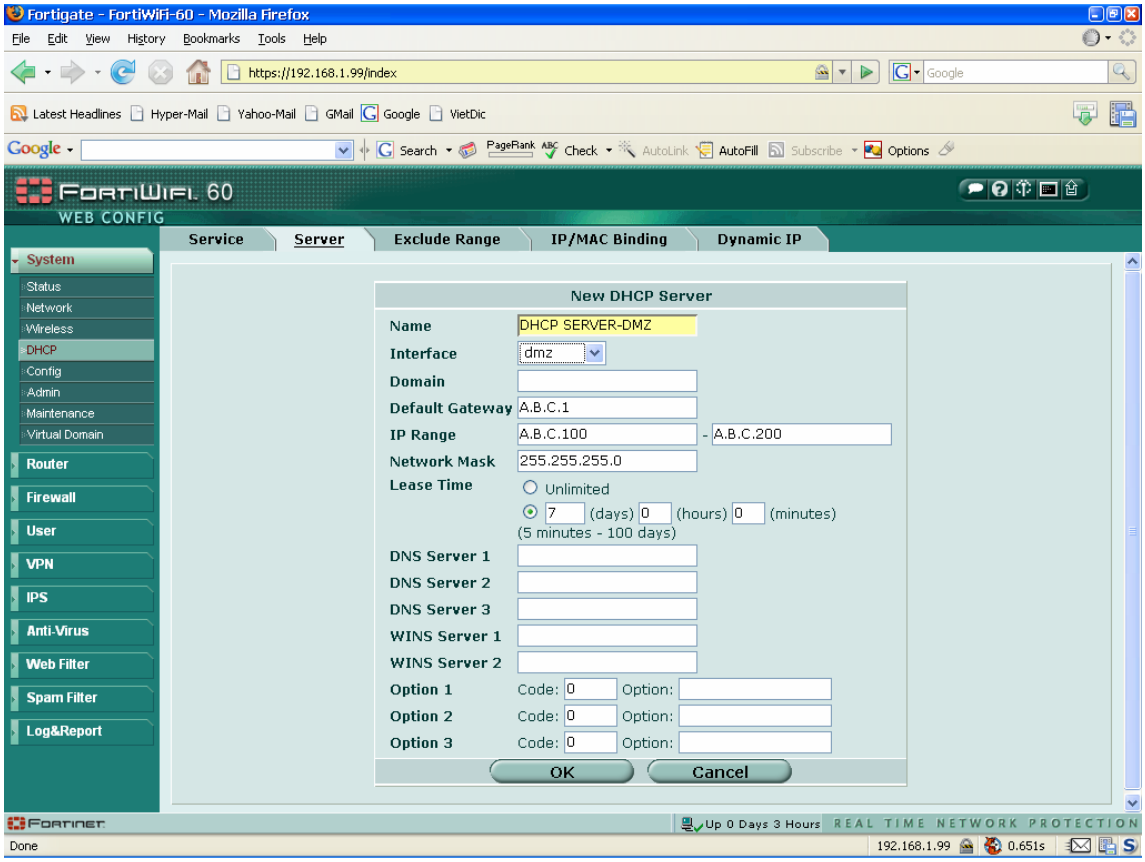
Chọn "Login" , sau đó chọn System – DHCP.Chọn giao diện cần thay đổi trong "Service"



Sau đó thay đổi tham số theo yêu cầu :



Tiếp đến chọn "Server", "Creat New" giao diện cần cấu hình DHCP:



Các tùy chọn DNS Server ,WINS Server...

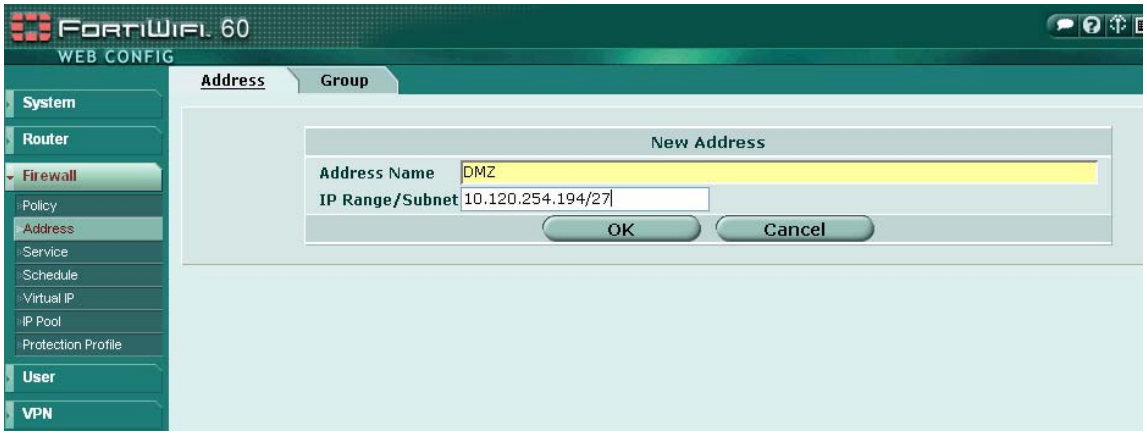
Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

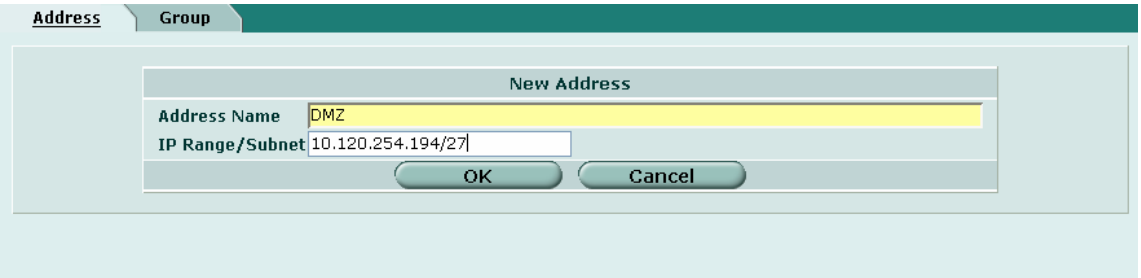
2.7. Cấu hình các địa chỉ và vùng địa chỉ

Trên giao diện web: http, https

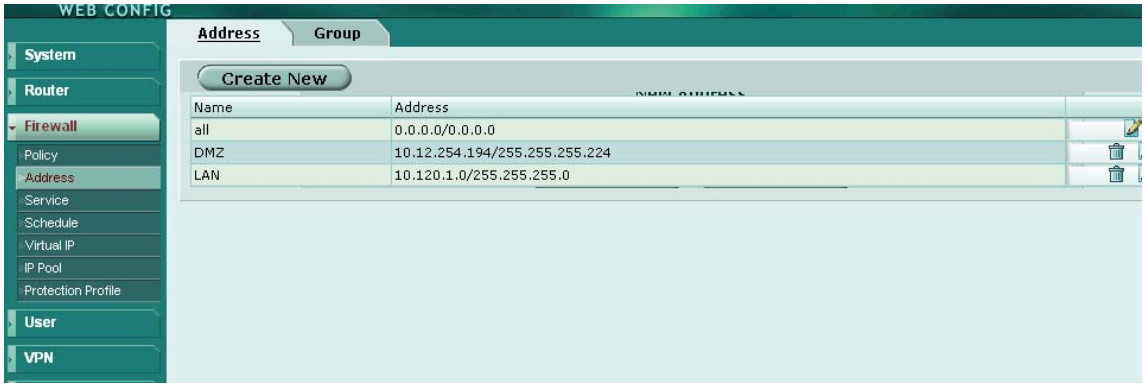
Login vào hệ thống ,chọn "Firewall" – "Address"



Chọn "Creat New" để định nghĩa các vùng : DMZ,LAN,...



Ví dụ :



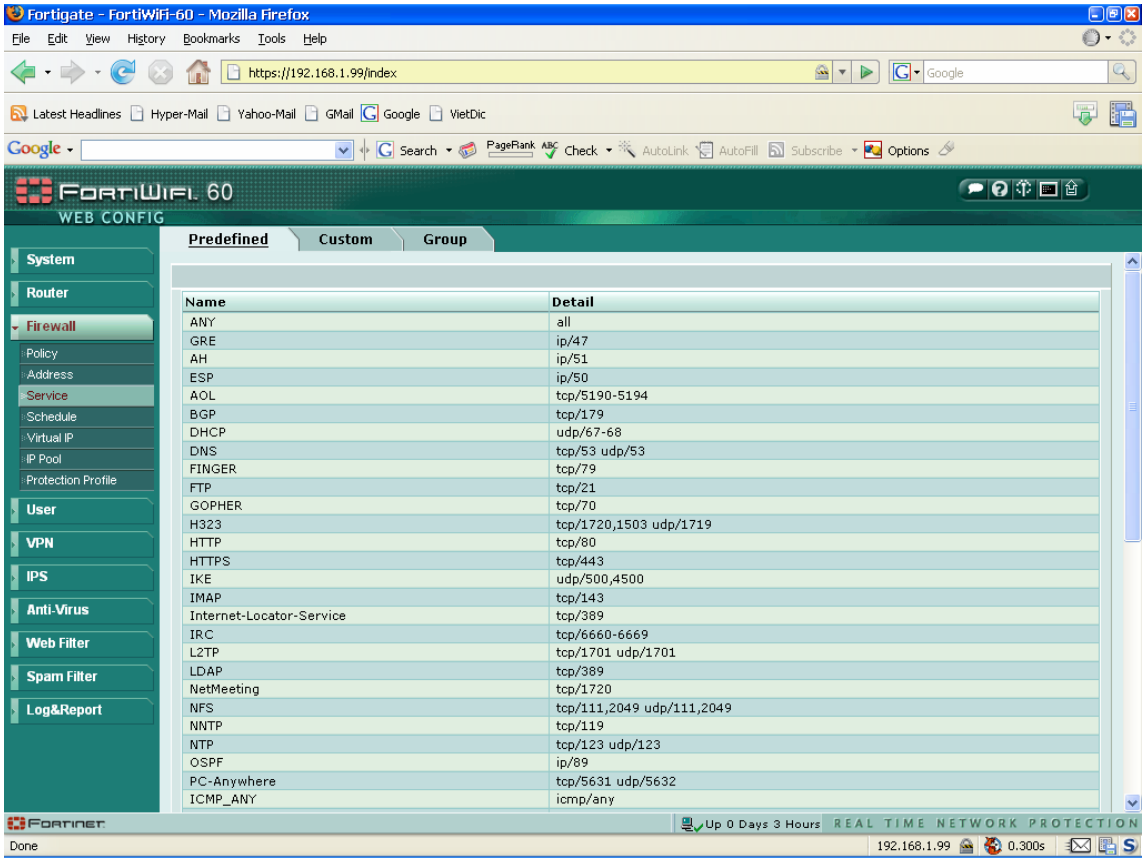
Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

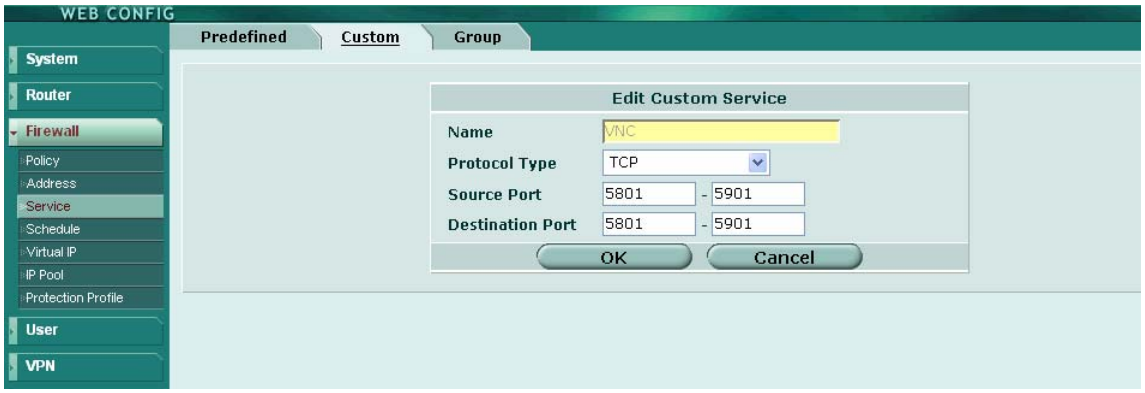
2.8. Cấu hình các dịch vụ

Trên giao diện web: http, https

Login vào hệ thống ,chọn "Firewall" – "Service"

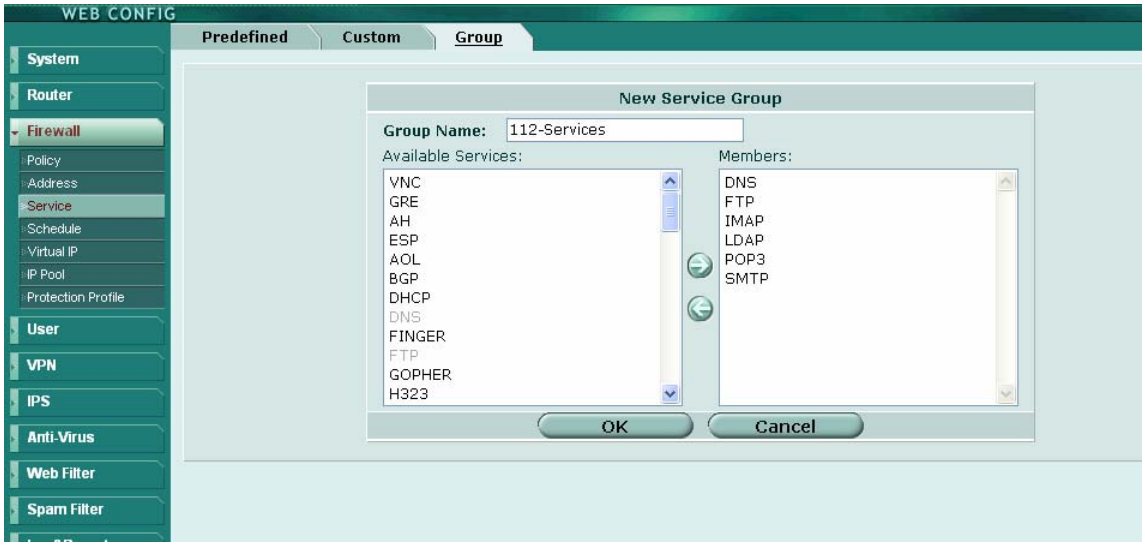


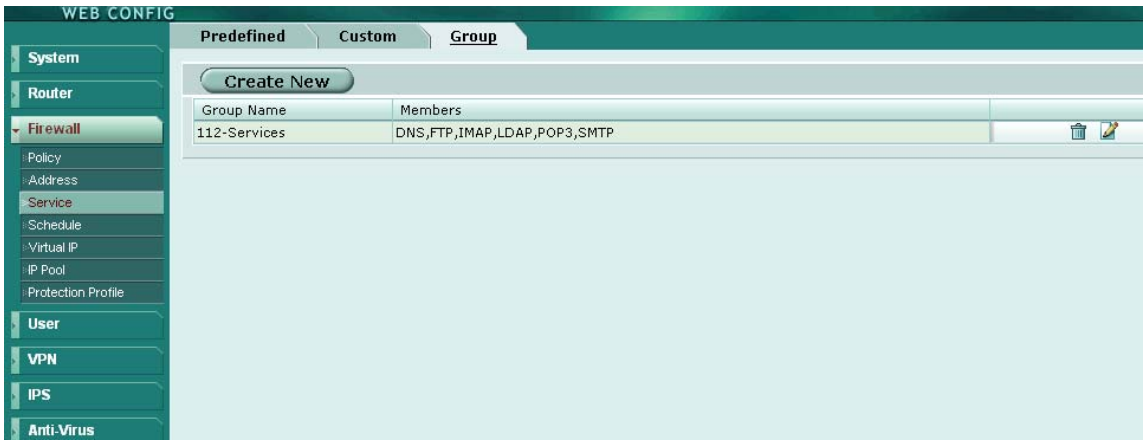
Predefined : Đây là các dịch vụ đã được định nghĩa trước với các tên tương ứng.
Custom : Nếu ta muốn định nghĩa thêm các dịch vụ theo yêu cầu . Ví dụ :



Khi đó ta sẽ thấy :

Nếu muốn nhóm lại 1 số dịch vụ để dễ dàng hơn khi tạo các Policy , ta có thể tạo 1 nhóm các dịch vụ và có thể tạo 1 Policy cho toàn bộ các dịch vụ trong nhóm này. 1 nhóm các dịch vụ này có thể bao gồm các dịch vụ **Predefined và Custom.**





Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.9. Cấu hình các Protection profile

Trên giao diện web: http, https

Việc sử dụng protection profiles để áp dụng các thiết lập bảo vệ khác nhau cho luồng thông tin mà được điều khiển bởi các policy của FortiGate. Mục đích :

- Cấu hình chống Virus cho các giao thức HTTP,FTP,IMAP,POP3,SMTP.
- Cấu hình lọc Web cho HTTP
- Cấu hình chống Spam cho IMAP,POP3,SMTP
- Cho phép chống xâm nhập (IPS- Intrusion Prevention System) cho tất cả các dịch vụ.

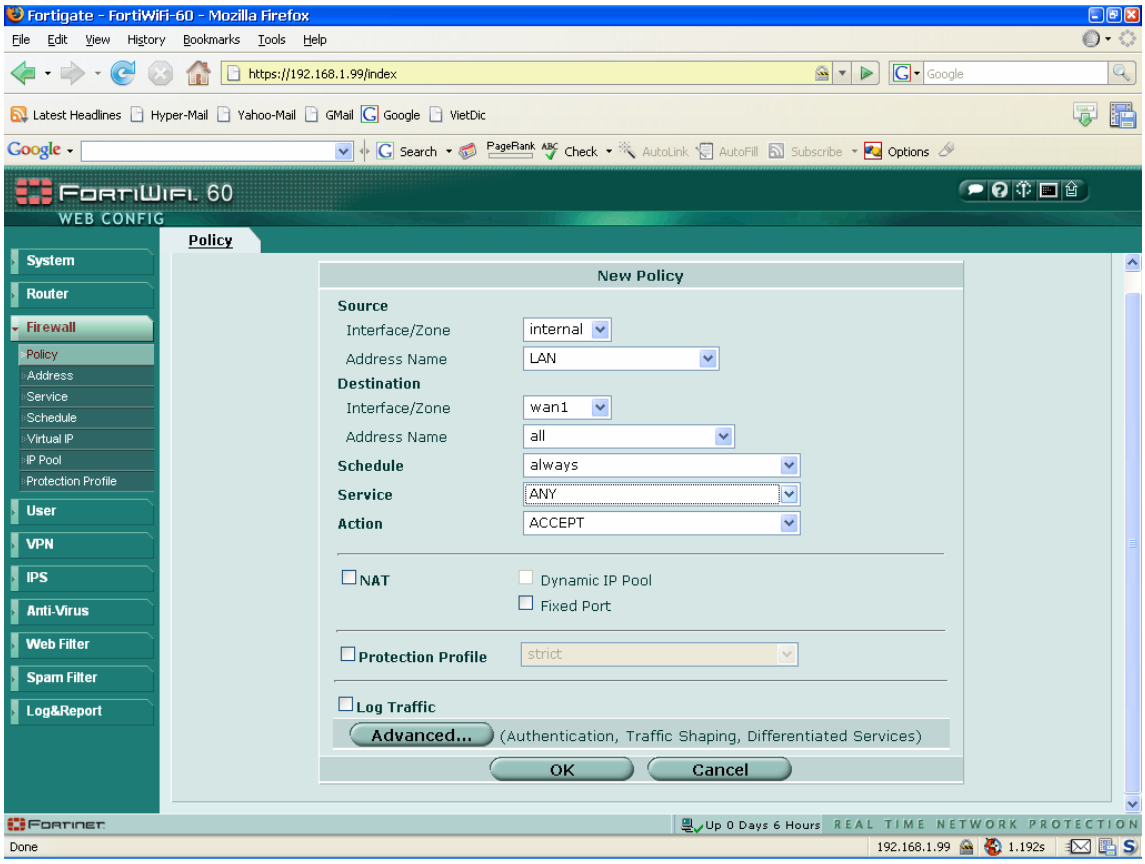
Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.10. Cấu hình các Policy

Trên giao diện web: http, https

Login vào hệ thống ,chọn "Firewall" – "Policy"



Source :

Interface/Zone :Giao diện nguồn

Address Name: tên của địa chỉ nguồn (địa chỉ được định nghĩa ở trên)

Destination :

Interface/Zone :Giao diện đích

Address Name :tên của địa chỉ đích (địa chỉ được định nghĩa ở trên)

Service : dịch vụ cần để lập Policy
Action :

ACCEPT : chấp nhận các kết nối phù hợp với Policy.Ta cũng có thể cấu hình NAT, protection profiles, log traffic, traffic shaping, authentication, và các dịch vụ khác nữa.

DENY : từ chối các kết nối phù hợp với Policy.

ENCRYPT : Chọn mã hóa để tạo policy này là 1 VPN IPSec (chấp nhận các gói tin IPSec).

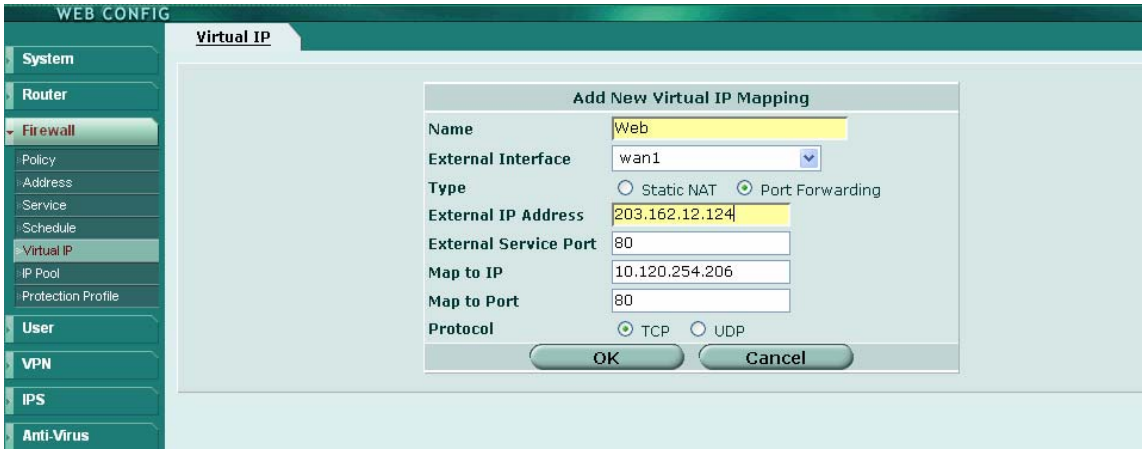
Như ví dụ trên ta sẽ có :

Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.11. Cấu hình Virtual IP

Trên giao diện web: http, https



Name : Tên gợi nhớ cho dịch vụ ta cần đặt
External Interface: Giao diện Wan mà ta cần ánh xạ vào.
Type

Static NAT : Ánh xạ từ 1 địa chỉ Wan vào 1 địa chỉ Private

Port Forwarding :Ánh xạ từ 1 port của địa chỉ Wan vào 1 port của địa chỉ Private

External IP Address : Địa chỉ Wan của giao diện

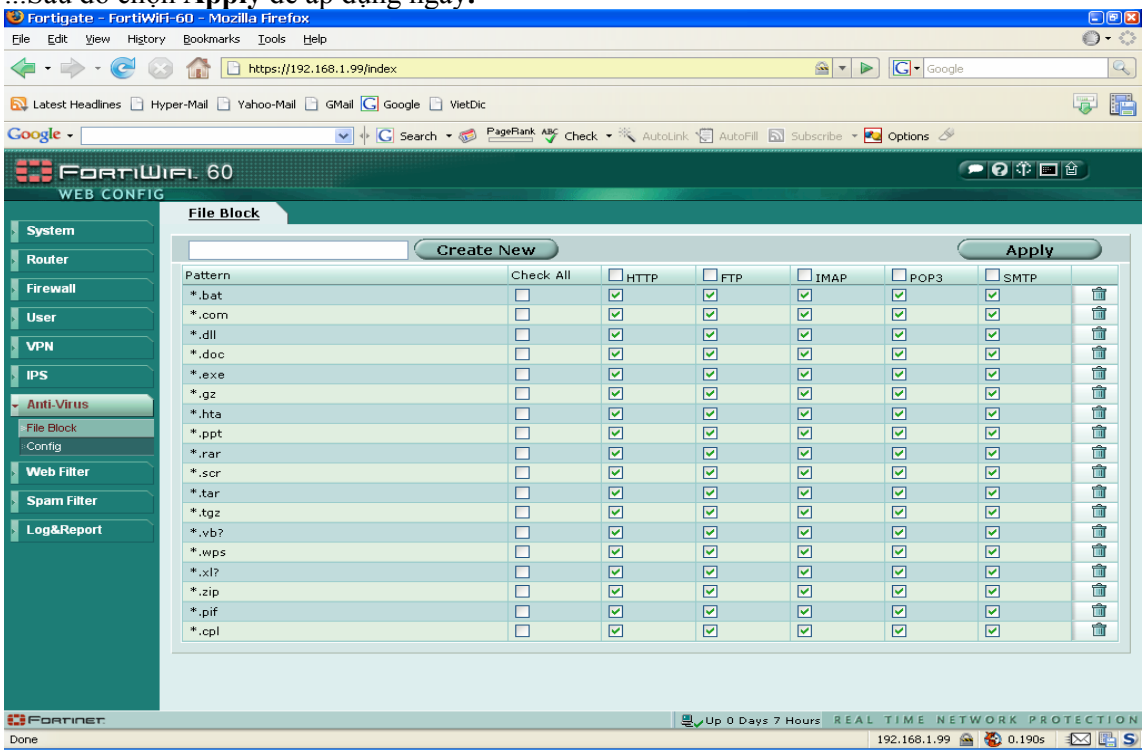
External Service Port : cổng dịch vụ của địa chỉ Wan
Map to IP : Địa chỉ IP Private cần ánh xạ đến
Map to Port :cổng dịch vụ của Địa chỉ IP Private cần ánh xạ đến
Protocol : Giao thức sử dụng
Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

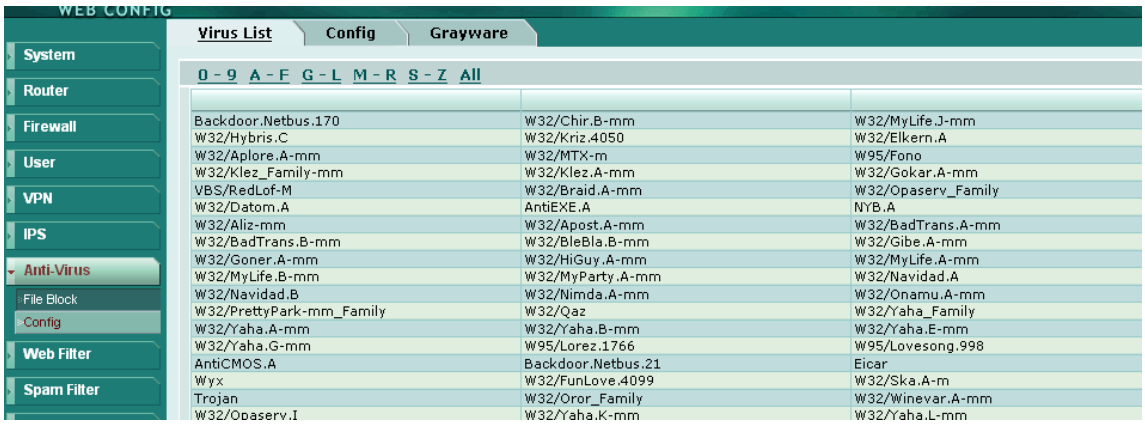
2.12. Cấu hình dịch vụ AntiVirus

Trên giao diện web: http, https
Login vào hệ thống ,chọn "Antivirus"

-File Block : ta có thể lựa chọn các định dạng File mẫu ,giao thức nào cần kiểm tra để ngăn chúng lại. Ta cũng có thể định nghĩa các định dạng File khác bằng cách tạo mới ...Sau đó chọn **Apply** để áp dụng ngay**.**



-Config : ta có thể thấy danh sách các mẫu Virus đaz được cập nhật vào.



Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.13. Cấu hình dịch vụ AntiSpam

Trên giao diện web: http, https
Login vào hệ thống ,chọn "Spam Filter"

Fortiguard_AntiSpam

Đây là 1 dịch vụ bảo vệ và chống Spam cho Email (FortiShield).Nó có nhiệm vụ kiểm tra các địa chỉ nguồn và URL của Email đến ,nếu có trong danh sách Blacklist ở trên FortiShield Server thì sẽ chặn việc gửi thư này.Bạn muốn sử dụng dịch vụ này thì phải đăng ký với nhà cung cấp.

IP address

Đây là địa chỉ IP nguồn mà ta cần kiểm tra (có thể là 1 địa chỉ hay 1 dải địa chỉ).Nếu phù hợp thì Protection Profile tương ứng được thi hành,nếu không phù hợp thì chuyển sang lọc Spam tiếp theo

Email address

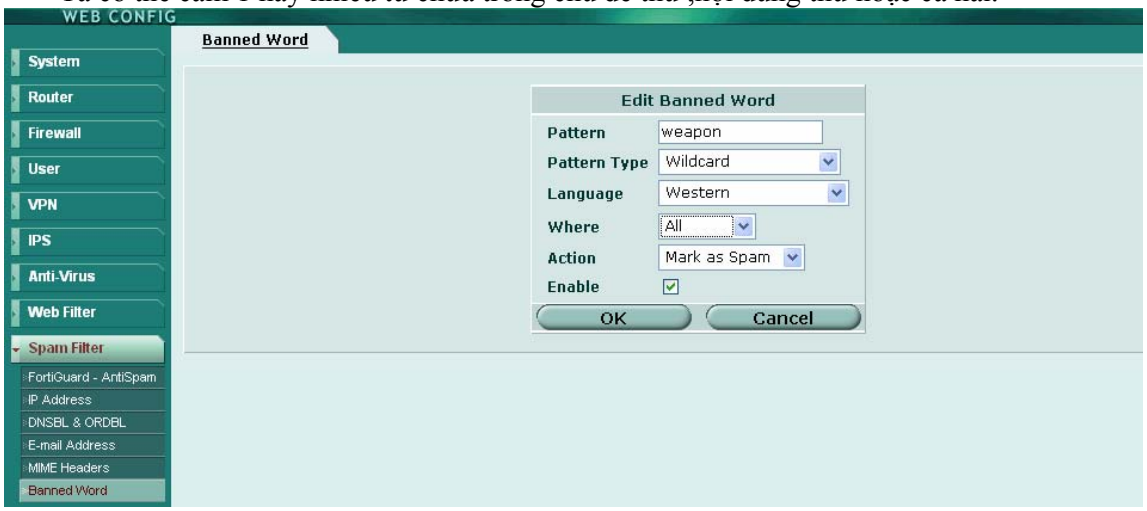
Đây là việc lọc Email theo địa chỉ cụ thể của người gửi hoặc toàn bộ Email của 1 domain nào đó.Ta có thể đánh dấu mỗi địa chỉ Email là "clear" hay "spam".

MIME (Multipurpose Internet Mail Extensions)

MIME thêm vào Email để mô tả kiểu nội dung ,mã hóa nội dung.Việc Spammer thay đổi các tham số này có thể làm cho bộ lọc Virus và Spam bị đánh lừa.Ta có thể sử dụng danh sách MIME Headers để đánh dấu Email từ các chương trình thư rác(chắc chắn) hay cùng với kiểu nội dung mà phổ biến các spam message hay dùng.

Banned Word

Ta có thể cấm 1 hay nhiều từ chứa trong chủ đề thư ,nội dung thư hoặc cả hai.



Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.14. Cấu hình dịch vụ IPS

Trên giao diện web: http, https
Login vào hệ thống ,chọn "IPS"
Predefine:

Đây là tập hợp các signature(dấu hiệu đặc trưng) được định nghĩa trước ,phân loại các loại dựa trên kiểu tấn công .Ngầm định các nhóm dấu hiệu này được kích hoạt ,1 số trong các nhóm khác thì không .Ta cũng có thể tạo ra các signature bằng tùy chọn Custom (Đặt tên,dấu hiệu,hành động , có ghi Log hay không ...)

Anormaly

Danh sách phát hiện các dấu hiệu anormaly chỉ được cập nhật khi Update Firmware.

Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.15. Cấu hình dịch vụ Web filter

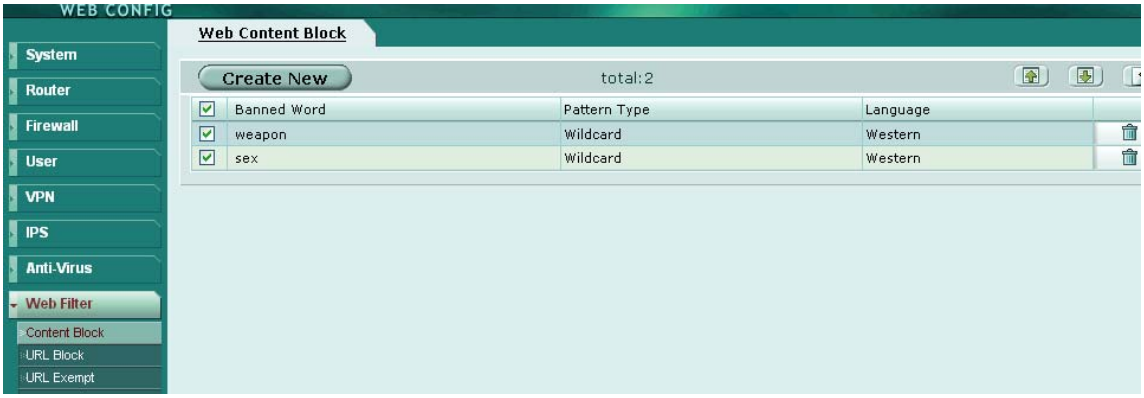
Cung cấp cấu hình truy nhập để thiết lập cho Web Filtering khi tạo 1 Protection profile cho firewall.

Trên giao diện web: http, https

Login vào hệ thống ,chọn "Web Filtering"

Content Block

Khóa trang Web có chứa những từ bị cấm ,có thể là 1 từ hoặc 1 chuỗi ký tự (text) có độ dài lên tới 80 ký tự. Số từ bị cấm cao nhất trong damh sách là 32.



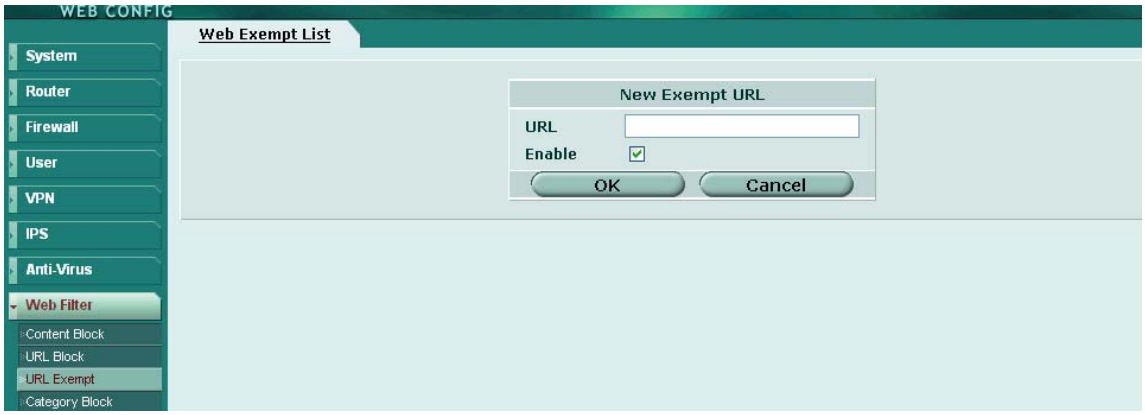
URL Block

Ta có thể thêm vào các URL hoặc 1 số các URL được quảng bá công khai sẵn có để cấm truy cập .Các mục có thể vào URL block list :

- Các URL đầy đủ
- Địa chỉ IP
-Từng phần riêng rẽ của các URL để cấm các sub-domain

URL Exempt

Ta có thể cấu hình cụ thể các URL được phép truy cập từ Web filtering.Các URL trong danh sách Exempt không bị quét Virus.

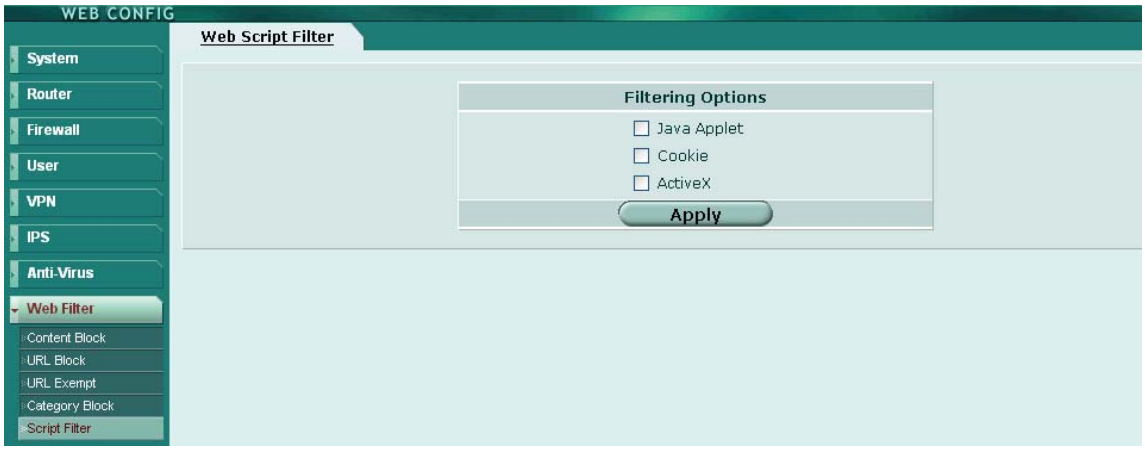


Category Block

Đây là dịch vụ có license tương tự FortiShield

Script Filter

Cho phép lọc Java Applet,Cookie và Active X



Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

2.16. Cấu hình ghi log

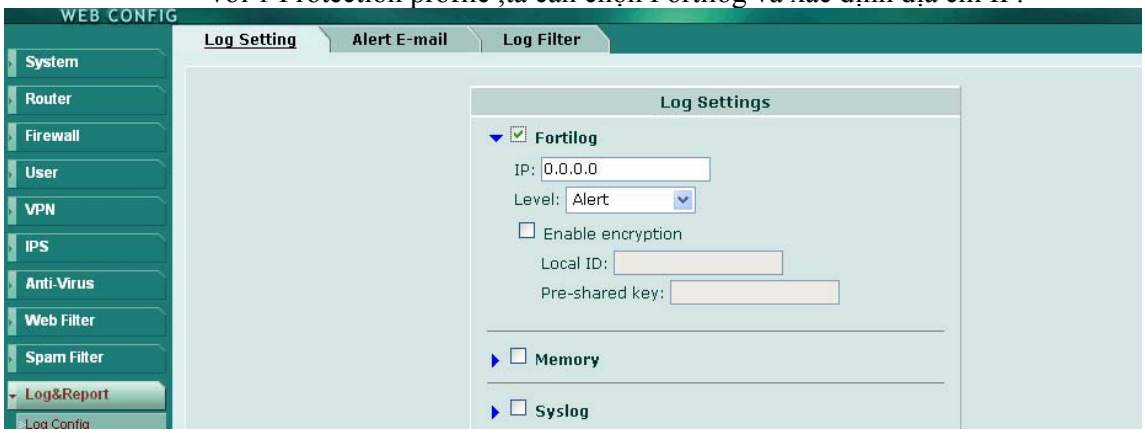
Trên giao diện web: http, https

Login vào hệ thống ,chọn "Log & Report"

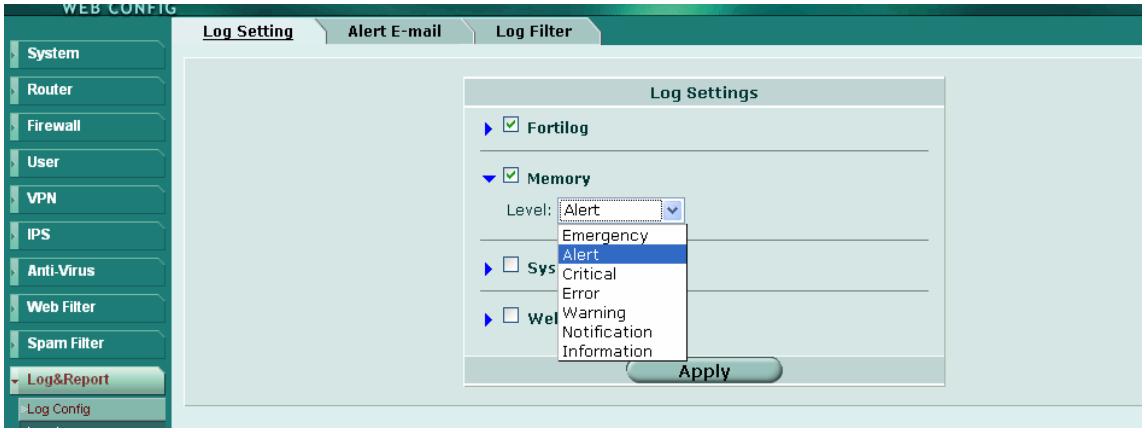
Log Config :

Ta có thể kích hoạt và cấu hình lưu trữ các log-message tới 1 hay nhiều nơi sau :

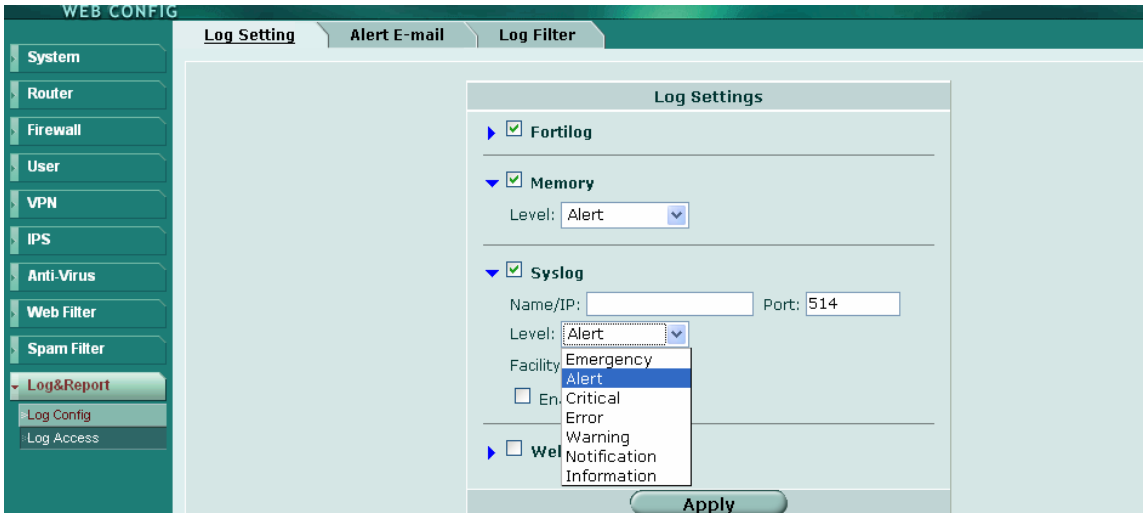
FortiLog : là 1 thiết bị phân tích và quản lý log, có thể tổng hợp với các FortiGate khác hoặc các loại firewall khác.Để thiết lập lưu trữ nội dung với 1 Protection profile ,ta cần chọn Fortilog và xác định địa chỉ IP.



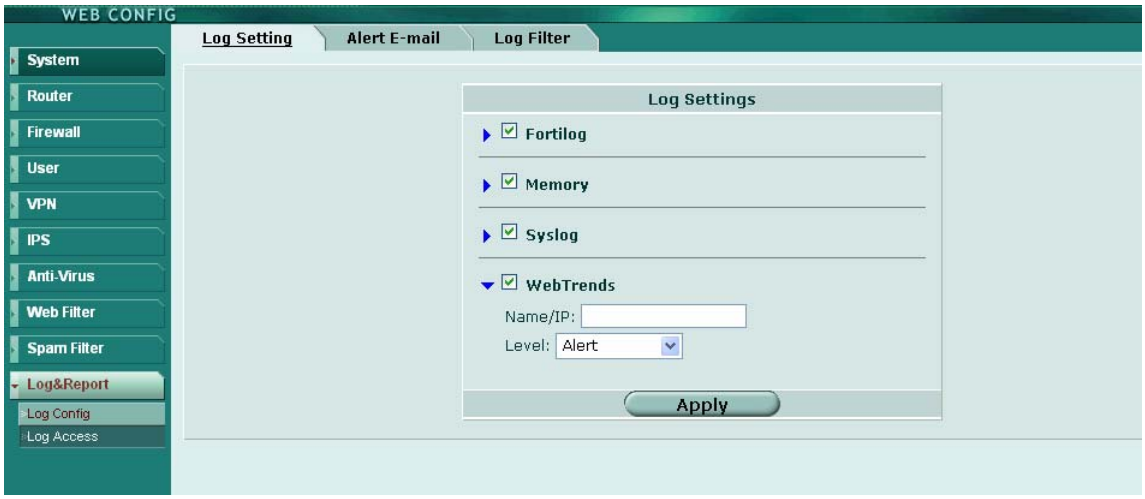
Memory : Quản lý thông tin bộ nhớ hệ thống của FortiGate .Lưu lượng và content log không được lưu lại bộ nhớ đệm. Khi bộ nhớ đầy ,các thông cũ nhất sẽ bị ghi đè . Tất cả các mục của Log sẽ bị xóa khi hệ thống khởi động lại. "Level" là lựa chọn cách thức cảnh báo .



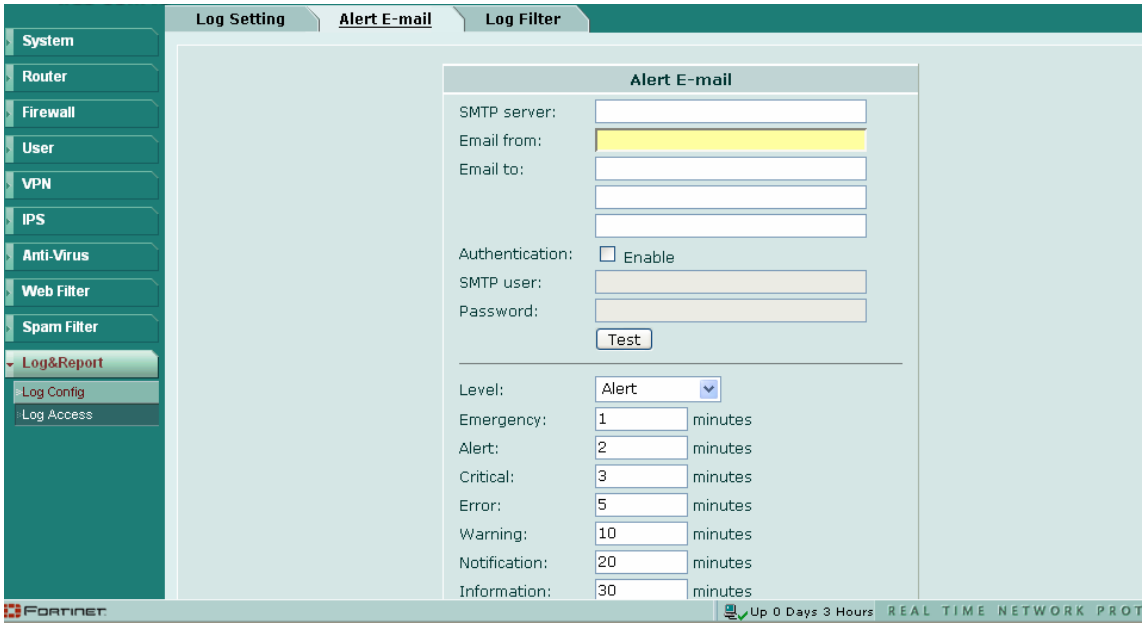
Syslog : 1 Remote Computer chạy làm máy chủ Syslog.(tên hoặc địa chỉ IP,port)



Web Trend : 1 Remote Computer chạy NetIQ WebTrends – máy chủ báo cáo thông tin firewall .

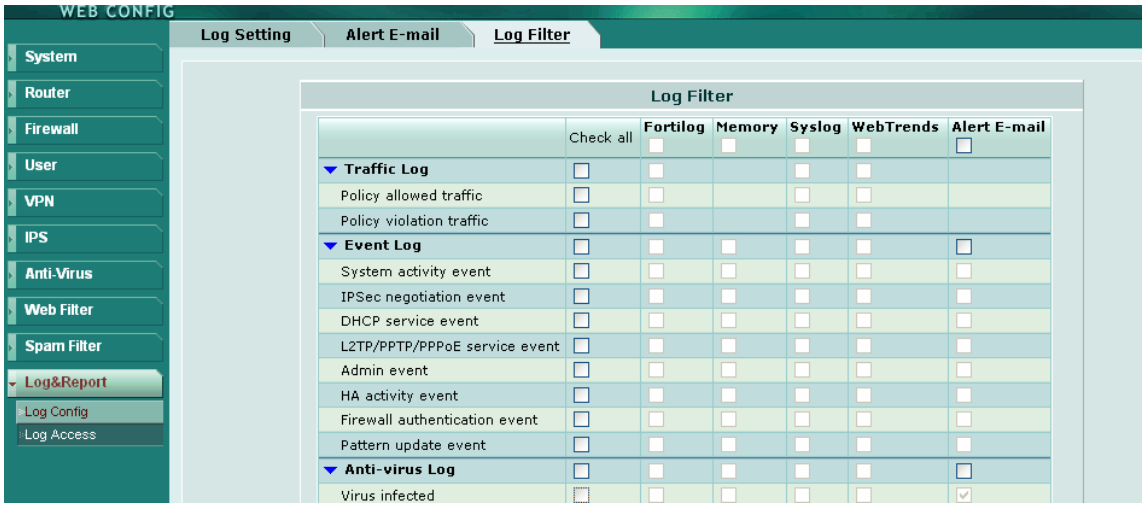


Alert E-Mail : Chỉ rõ ra Mail server và người nhận cho các thông báo thư và các mức độ, tần suất của các thông báo.



SMTP Server : tên và địa chỉ của SMTP Server cho các thông báo.
Email from : Địa chỉ người gửi
Email to : Địa chỉ người nhận thông báo
Authentication : thiết lập xác thực SMTP
SMTP user :
Password :
Level : Thiết lập mức độ cảnh báo, chu kỳ đợi trước khi gửi thông báo cảnh báo

Log Filter : Cấu hình cho các log filter : lưu tại đâu, lưu loại nào (traffic log,event log...)



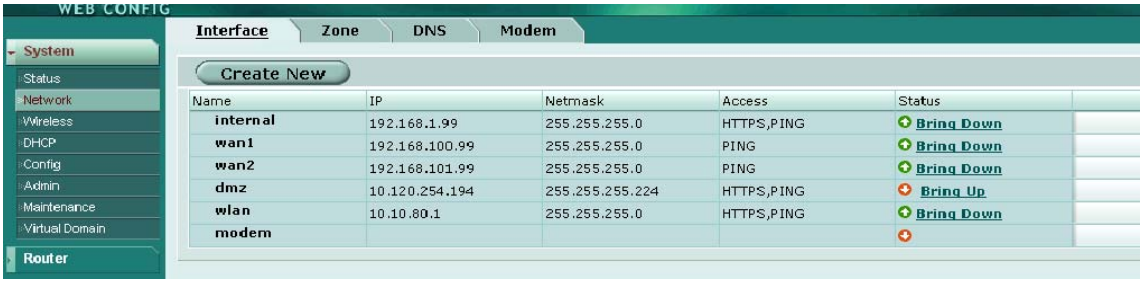
Console, telnet, ssh

Tham khảo thêm trong tài liệu hoặc trên trang web:
http://kc.forticare.com/

3. Kiểm tra hoạt động của FortiGate

3.1. Kiểm tra cấu hình giao diện

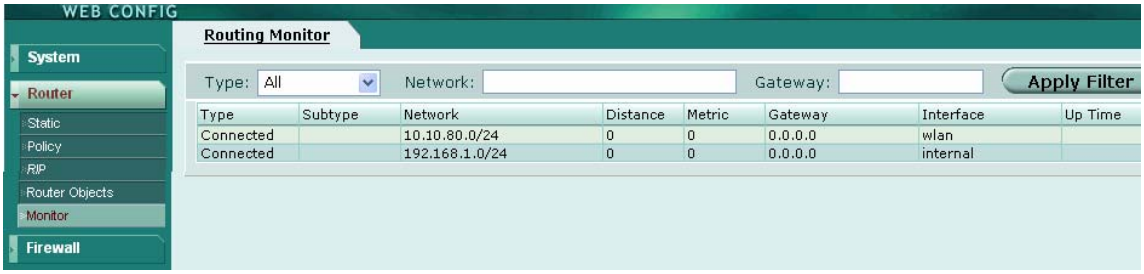
Muốn kiểm tra cấu hình của các giao diện , ta login vào hệ thống ,chọn System-Network



Nếu 1 giao diện nào đánh dấu xanh có nghĩa là giao diên đó đã "up",màu đỏ có nghĩa là giao diện đó bị "down".Muốn bật giao diện đó ta bấm vào "Bring up"

3.2. Kiểm tra cấu hình định tuyến

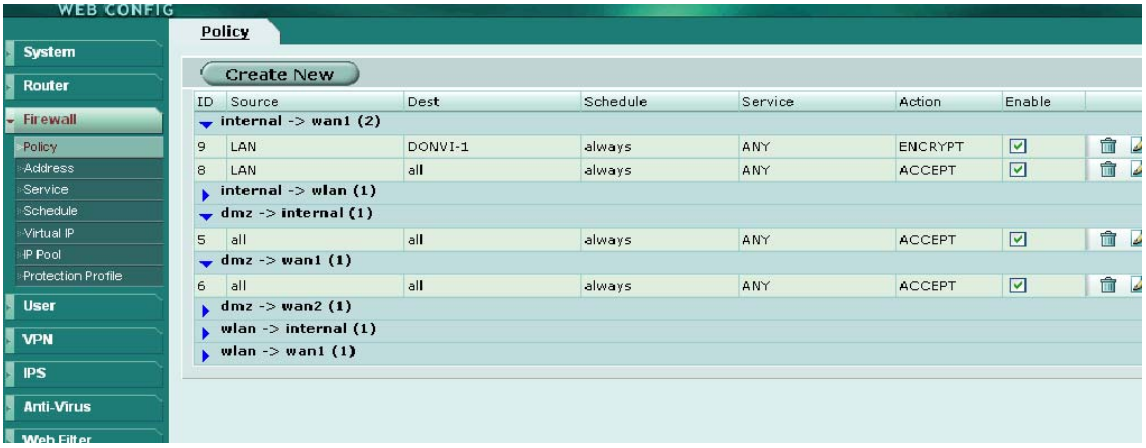
Login vào hệ thống ,chọn "Router" – "Monitor"



Type :cho biết các định tuyến của kiểu được chọn cụ thể
Network : cho biết các định tuyến của mạng cụ thể
Gateway : cho biết các định tuyến của mạng sử dụng 1 gateway cụ thể
Apply Filter : Áp dụng các định tuyến theo tiêu chuẩn được chỉ rõ
Up time : thời gian mà định tuyến đã sẵn sàng

3.3. Kiểm tra cấu hình Policy

Muốn kiểm tra cấu hình của các giao diện , ta login vào hệ thống ,chọn "Fire wall" – "Policy". Các Policy được tạo ra tùy theo mô hình mạng cụ thể. Lưu ý các yêu cầu ,kết nối giữa các vùng để đưa ra các Policy hợp lý. Với các Policy có Action là "Encrypt" thì có độ ưu tiên cao hơn Action "Accept".Vì vậy, ta luôn đặt chúng lên trước trong cùng 1 Policy (không phụ thuộc vào số thứ tự ở cột ID mà chỉ phụ thuộc thứ tự từ trên xuống dưới trong 1 Policy).



3.4. Kiểm tra hoạt động của mạng

Sau khi thiết lập xong các thông số theo mô hình mạng ,yêu cầu cụ thể , ta lần lượt kiểm tra kết nối giữa các vùng. Dùng các lệnh như Ping , Telnet đến các địa chỉ ,cổng cụ thể để kiểm tra các Policy.

4. Theo dõi hoạt động

4.1. Màn hình Status

Ta login vào hệ thống, chọn "System"-"Status".

System Status : cho biết thời gian đã hoạt động của firewall, đồng hồ hiện tại của hệ thống

Unit Information : cho biết tên của thiết bị ,Firmware version , FortiGuard AV Definitions, FortiGuard Intrution Definitions ,Serial Number,Operation Mode

Recent Virus Detections : chỉ rõ thời gian-nguồn-đích-dịch vụ-tên Virus quét được

Interface Status : cho biết tình trạng của toàn bộ các giao diện của hệ thống (IP,trạng thái...)

System Resource : tình trạng của CPU,bộ nhớ ,số lượng các session đang active, việc sử dụng mạng ...

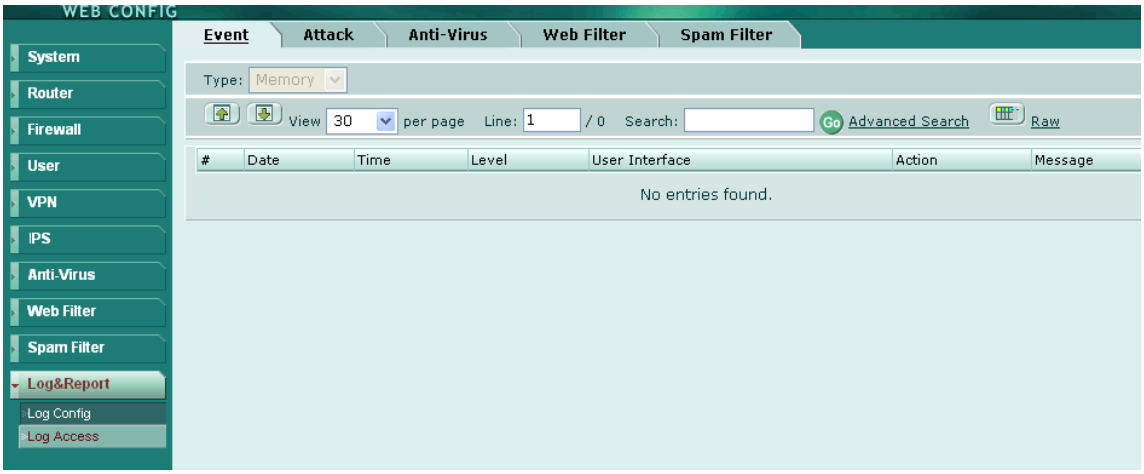
Automatic Refresh Interval : lựa chọn để điều khiển chu kỳ cập nhật hiển thị tình trạng của hệ thống

Refresh : Cập nhật hiển thị tình trạng của hệ thống bằng tay

Recent Intrusion Detections : phát hiện sự tấn công hiện thời.

4.2. Theo dõi log

Login vào Hệ thống , chọn "Log & Report"-"Log Access"



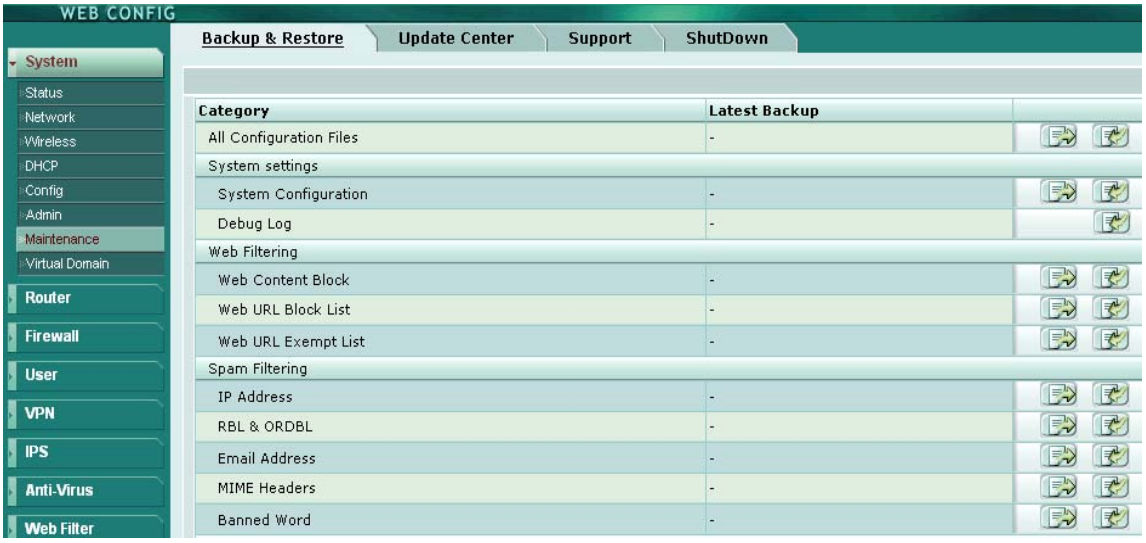
Ta có thể theo dõi các Event ,Attack,Anti-Virus,Web Filter,Spam Filter.Và có thể tìm kiếm các thông tin (Log Search) trong khoảng thời gian ta yêu cầu ,từ khóa cần tìm ...

5. Sao lưu và phục hồi cấu hình

5.1. Sao lưu và phục hồi cấu hình

FortiGate hỗ trợ việc sao lưu và phục hồi cấu hình 1 cách đơn giản và thuận tiện.

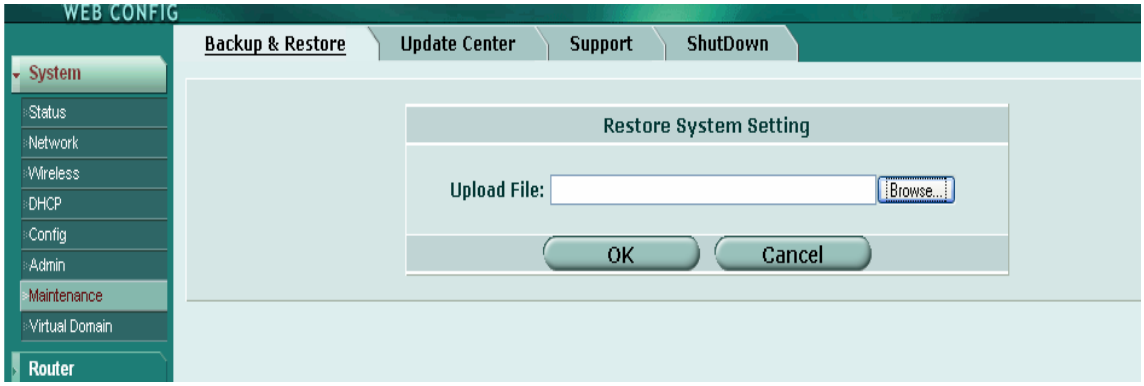
Login vào hệ thống ,chọn "System"-"Maintenance"



Muốn lưu cấu hình hiện tại của hệ thống ta chọn System Configuration- Back up

Ta chọn vào nút  (sẽ hiển thị "Backup") , sau đó sẽ có hướng dẫn lưu cấu hình-đặt tên cho file backup này.

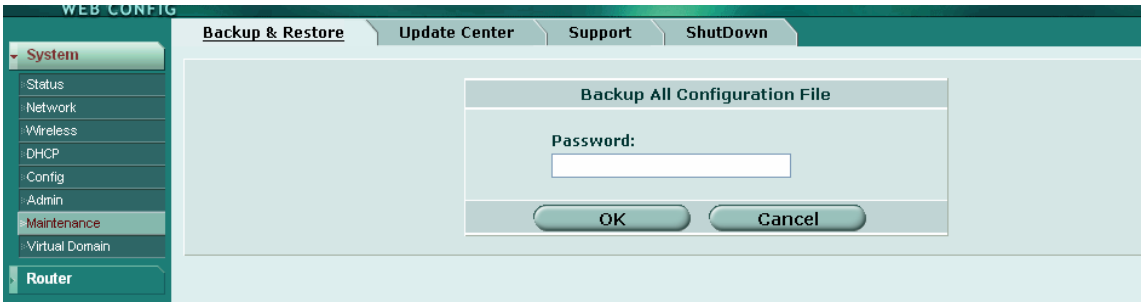
Muốn phục hồi 1 cấu hình đã lưu, ta chọn vào nút  (sẽ hiển thị "Restore") .Tiếp đến Browse đến nơi lưu file cấu hình , rồi nhấn OK.Sau khi phục hồi xong nên khởi động lại Hệ thống.



5.2. Sao lưu và phục hồi toàn bộ

Muốn lưu cấu hình hiện tại của hệ thống ta chọn dòng All Configgguration Files.Ta chọn vào nút  (sẽ hiển thị "Backup")

Sau đó nhập mật khẩu cho file cấu hình này. Tiếp đến ta chọn nơi lưu cấu hình này.



Muốn phục hồi 1 cấu hình đã lưu, ta chọn vào nút  (sẽ hiển thị "Restore") .Nhập mật khẩu của cấu hình khi sao lưu và Browse đến nơi chứa file cấu hình đó ,sau đó nhấn OK. Sau khi phục hồi xong nên khởi động lại Hệ thống.