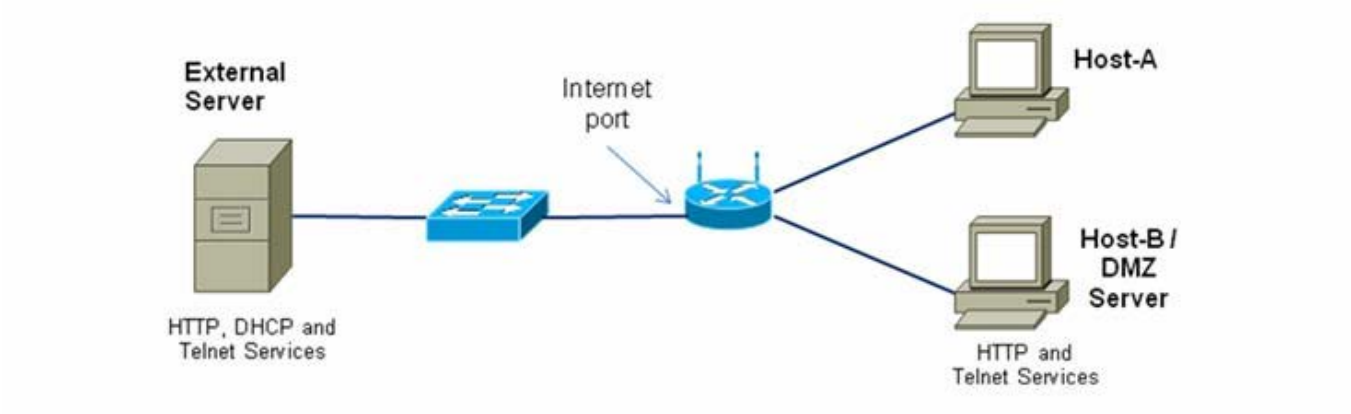
Lab 6
Cấu hình chính sách truy cập và thiết lập DMZ



I. Mục tiêu

- Đăng nhập đến thiết bị nhiều chức năng và các cài đặt bảo mật.
- Cài đặt chính sách truy cập Internet dựa vào địa chỉ IP và các dịch vụ mạng qua PortNumber (http, ftp,..)
- Cài đặt một DMZ cho truy cập Server với IP tĩnh.
- Cài đặt cổng chuyển tiếp để giới hạn chỉ truy cập đến dịch vụ HTTP.
- Sử dụng các đặc tính của Linksys WRT300N

II. Chuẩn bị

Cần các tài nguyên sau:

- Linksys WRT300N Hoặc thiết bị khác với cấu hình mặc định
- Username và Password truy cập vào thiết bị.
- Máy tính chạy Windows XP/ Windows 7 để cấu hình qua Linksys Web.
- Máy tính bên trong đóng vai trò như Server trong DMZ và cung cấp dịch vụ HTTP và Telnet.
- Server bên ngoài đóng vai trò như ISP và Internet với các cấu hình DHCP, HTTP và Telnet.
- Cáp kết nối PC, Linksys WRT300N hoặc các thiết bị tích hợp và switches

III. Nội dung

Lab này cung cấp hướng dẫn cho việc cấu hình bảo mật cho thiết bị đa chức năng Linksys WRT 300N (Các thiết bị khác cũng cấu hình tương tự). Linksys WRT 300N cung cấp Firewall dựa vào phần mềm để bảo vệ bên trong, các máy khách cục bộ bởi các tấn công từ bên ngoài. Kết nối từ các host bên trong tới các đích bên ngoài có thể được lọc dựa vào địa chỉ IP, các Website và ứng dụng đích. Linksys có thể được cấu hình tạo 1 miền DMZ để kiểm soát truy cập tới Server từ các host bên ngoài.

Lab chia làm 2 phần

- Phần 1 – Cấu hình chính sách truy cập.
- Phần 2 – Cấu hình thiết lập DMZ.

Phần 1 – Cấu hình chính sách truy cập

Bước 1: Xây dựng mạng và cấu hình các máy

a. *Kết nối máy tới cổng switch trên thiết bị đa năng như trong hình vẽ. Host-A được điều khiển sử dụng truy cập Linksys ở dạng Web. Host-B khởi tạo là máy test sau này trở thành DMZ server.*

b. *Cấu hình IP cho cả 2 máy. Kiểm tra Host-A được cấu hình là DHCP client. Gán 1 địa chỉ IP tĩnh tới Host-B trong dải 192.168.1.x với subnet mask là 255.255.255.0. Default gateway là địa chỉ cổng internal của Linksys.*

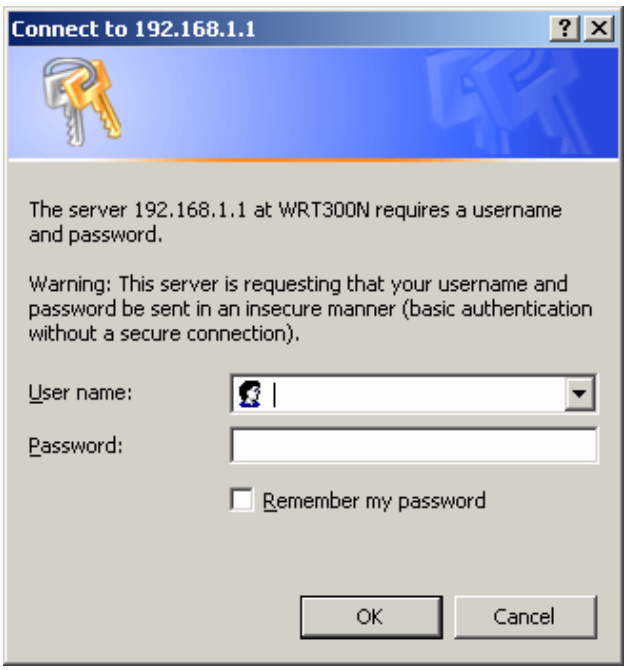
c. *Dùng lệnh ipconfig /all để lấy thông tin về địa chỉ IP của các máy cho dưới đây.*

Host	***IP Address***	***Subnet Mask***	***Default Gateway***
Host-A			
Host-B / DMZ			
External Server			

Bước 2: Đăng nhập vào Linksys

a. *Để truy cập vào Linksys vào trình duyệt Web và gõ vào địa chỉ IP bên trong của Linksys 192.168.1.1.*

b. *Sử dụng username và password để truy cập vào Linksys*



c. *Thiết bị đa chức năng nên được cấu hình để nhận IP từ DHCP từ bên ngoài. Màn hình mặc định sau khi đăng nhập vào thiết bị đa chức năng là Setup > Basic Setup.*

Kiểu kết nối Internet là gì?

_____

d. *Giá trị IP address mặc định bên trong và subnet mask của thiết bị đa chức năng.*

_____

e. *Kiểm tra thiết bị đa chức năng đã nhận IP bên ngoài từ DHCP server bằng cách click vào Status > Router tab.*

f. *Địa chỉ IP bên ngoài và subnet mask được gán tới thiết bị đa chức năng.*

_____

Bước 3: Xem thiết lập tường lửa trên thiết bị đa chức năng.

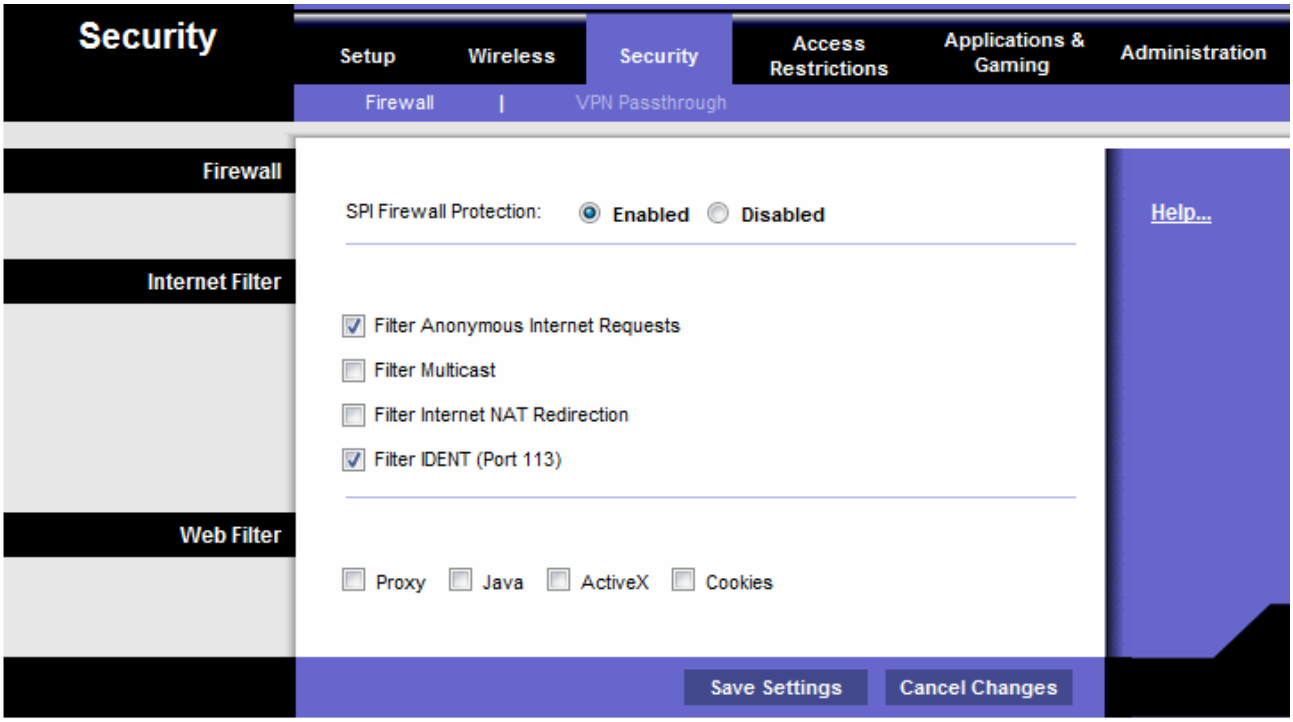
a. *Linksys WRT300N cung cấp tường lửa cơ bản và sử dụng dịch chuyển địa chỉ (NAT Network Address Translation). Thêm vào nó cung cấp tường lửa chức năng sử dụng SPI để phát hiện và ngăn chặn các gói tin từ Internet.*

b. *Từ màn hình chính, click vào* ***Security*** *tab để xem* ***Firewall*** *và* ***Internet Filter*** *trạng thái. Trạng thái của Firewall đã bảo vệ SPI chưa?* _____

c. *Mục* ***Internet Filter*** *nào đã được chọn?* _____

d. *Nhấn vào* ***Help*** *để tìm hiểu thêm về thiết lập. Lợi ích của filtering IDENT là gì?*

_____

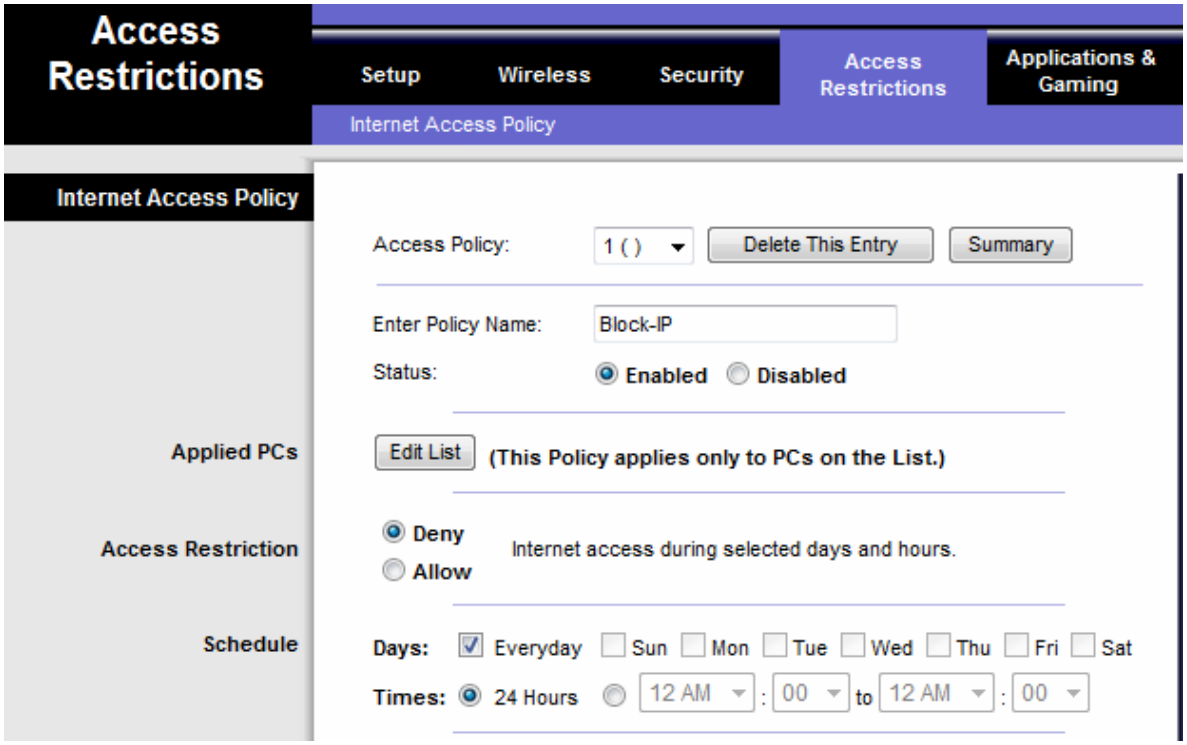


Bước 4: Cài đặt hạn chế truy cập Internet dựa vào địa chỉ IP

Thiết bị đa chức năng có thể kiểm soát các người dùng bên trong có thể ra ngoài Internet từ mạng cục bộ. Bạn có thể tạo một chính sách truy cập Internet để cho phép hoặc từ chối các máy tính chỉ định bên trong truy cập Internet dựa vào địa chỉ IP, địa chỉ MAC và các tiêu chuẩn khác.

a. *Từ màn hình chính, click vào* ***Access Restrictions*** *để định nghĩa* ***Access Policy 1****.*

b. *Trong mục Enter Policy Name (tên chính sách) gõ vào* ***Block-IP****. Trong mục Status chọn* ***Enabled*** *để cho phép chính sách, Chọn* ***Deny*** *để ngăn chặn truy cập Internet từ 1 IP cụ thể.*



c. *Click vào nút* ***Edit List*** *và gõ vào địa chỉ IP của Host-B. Click vào* ***Save Settings*** *và* ***Close****.*

Click ***Save Settings*** *để ghi lại Internet Access Policy 1 – Block IP.*

d. *Kiểm tra chính sách bằng cách truy cập tới Web server bên ngoài từ Host-B. Mở trình duyệt web và gõ vào địa chỉ IP của Server bên ngoài. Có thể truy cập được không ?.*

_____

e. *Thay đổi trạng thái của Block-IP Policy tới* ***Disabled*** *và click vào* ***Save Settings****. Bạn có thể truy cập Server bây giờ không?* _____

Bước 5: Cài đặt chính sách truy cập Internet dựa vào ứng dụng

Bạn có thể tạo chính sách truy cập Internet để ngăn chặn các máy tính cụ thể từ việc sử dụng các giao thức trên Internet.

a. *Từ màn hình GUI , click vào mục Access Restrictions để định nghĩa chính sách truy cập Internet.*

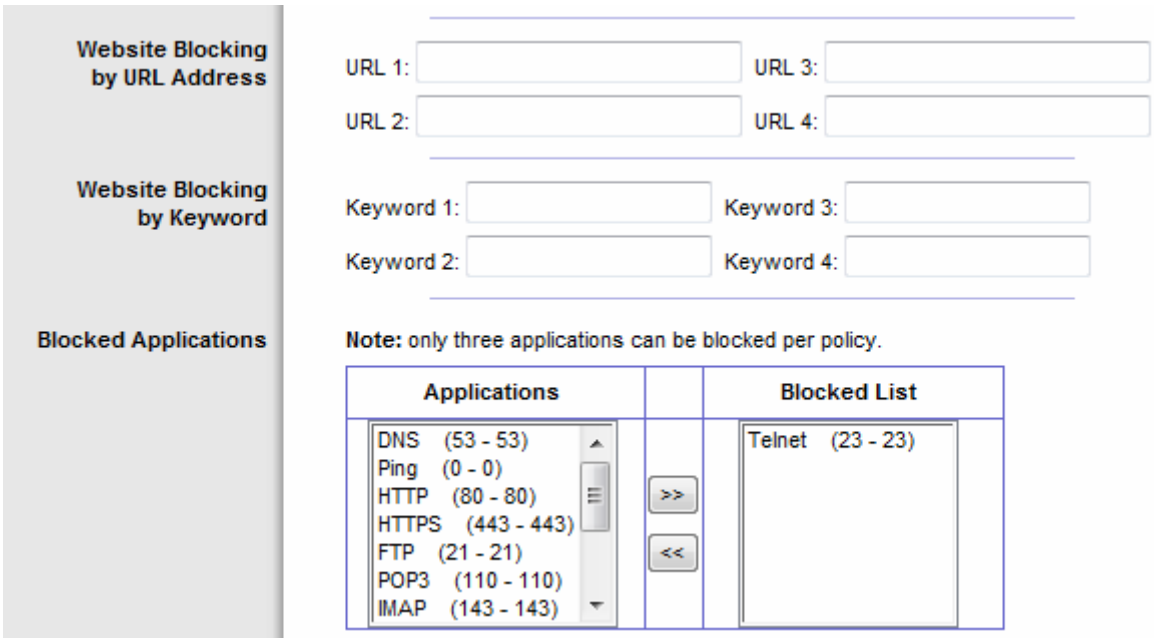
b. *Gõ vào Block-Telnet vào mục* ***Enter Policy Name****. Chọn* ***Enabled*** *để cho phép chính sách, và sau đó cho phép truy cập Internet từ 1 địa chỉ IP cụ thể miễn là nó không phải một trong các dịch vụ bị block.*

c. *Click vào Edit List và gõ vào IP của Host-B. Click* ***Save Settings*** *và sau đó click* ***Close.***

Các ứng dụng và các giao thức khác có bị block hay không?

_____

d. *Chọn chương trình* ***Telnet*** *từ danh sách các ứng dụng có thể bị khóa và sau đó click vào nút có 2 mũi tên để đưa vào danh sách* ***Blocked List****. Click* ***Save Settings****.*



e. *Kiểm tra chính sách bằng mở cửa sổ MS-DOS sử dụng* ***Start > All Programs > Accessories > Command Prompt.***

f. *Ping địa chỉ IP của server bên ngoài từ Host-B bằng câu lệnh* ***ping command****.*

Có thể ping được không? _____

g. *Telnet tới địa chỉ IP của Server bên ngoài từ Host-B sử dụng telnet A.B.C.D (Khi đó A.B.C.D là địa chỉ*
của Server).

Bạn có thể telnet đến Server được không? _____

Phần 2 – Cấu hình DMZ trên thiết bị đa chức năng

Bước 1: Cài đặt một DMZ đơn giản

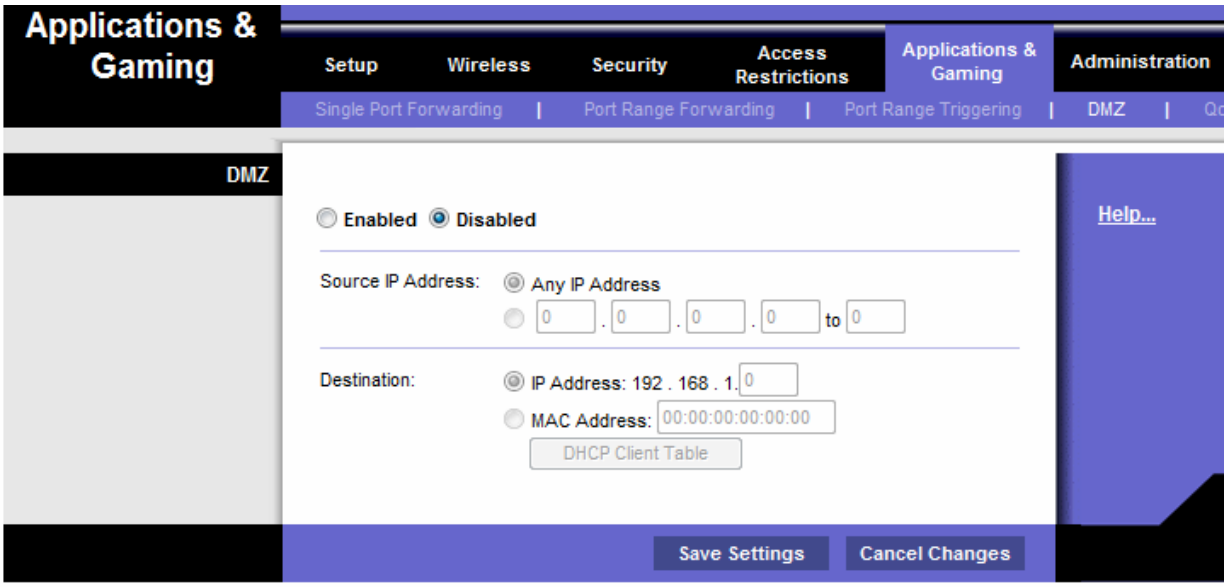
Thỉnh thoảng cần thiết để cho phép truy cập tới 1 máy tính từ Internet trong khi việc bảo vệ các máy tính khác trong mạng LAN. Để hoàn thành công việc này, bạn cần cài đặt một vùng DMZ mà cho phép truy cập tới bất kỳ cổng và các dịch vụ chạy trên server cụ thể. Bất kỳ các yêu cầu tạo cho các dịch vụ tới các địa chỉ bên ngoài của thiết bị đa chức năng sẽ được chuyển một lần nữa đến server cụ thể.

a. *Host-B sẽ đóng vai trò như DMZ server và sẽ chạy dịch vụ HTTP và Telnet servers. Kiểm tra Host-B có địa chỉ IP tĩnh hoặc, Host-B được cấp phát địa chỉ IP động.*

b. *Từ màn hình chính,click vào* ***Applications & Gaming*** *và clik vào* ***DMZ.***

b. *Click* ***Help*** *để học về DMZ. Cho các lý do cài đặt DMZ?*

_____
_____
_____



d. *DMZ mặc định là disabled. Chọn Enabled để cho phép DMZ. Để Source IP Address là Any IP Address, và gõ vào địa chỉ IP của Host-B trong Destination IP address. Click Save Settings.*

e. *Kiểm tra truy cập cơ bản đến DMZ server bằng cách ping từ server bên ngoài tới địa chỉ bên ngoài của thiết bị. Sử dụng lệnh* ***ping –a*** *để xác nhận là thực tế DMZ server phản ứng lại.*
Bạn có thể ping DMZ server hay không?.
_____

f. *Kiểm tra truy cập HTTP tới DMZ server bằng cách mở trình duyệt Web trên server bên ngoài và tập chung vào địa chỉ IP đầu External của thiết bị. Thử các bước tương tự từ trình duyệt Web trên Host-A tới Host-B bằng việc sử dụng địa chỉ bên trong.*

Bạn có thể truy cập trang Web hay không? _____

g. *Kiểm tra truy cập Telnet bằng việc mở MS-DoS tương tự bước 5. Telnet tới địa chỉ IP phía ngoài của thiết bị bằng cách sử dụng lệnh* **telnet** A.B.C.D *(A.B.C.D là địa chỉ phía ngoài của thiết bị).*

Bạn có thể Telnet với Server được không? _____

Bước 3: Cài đặt host với single port forwarding

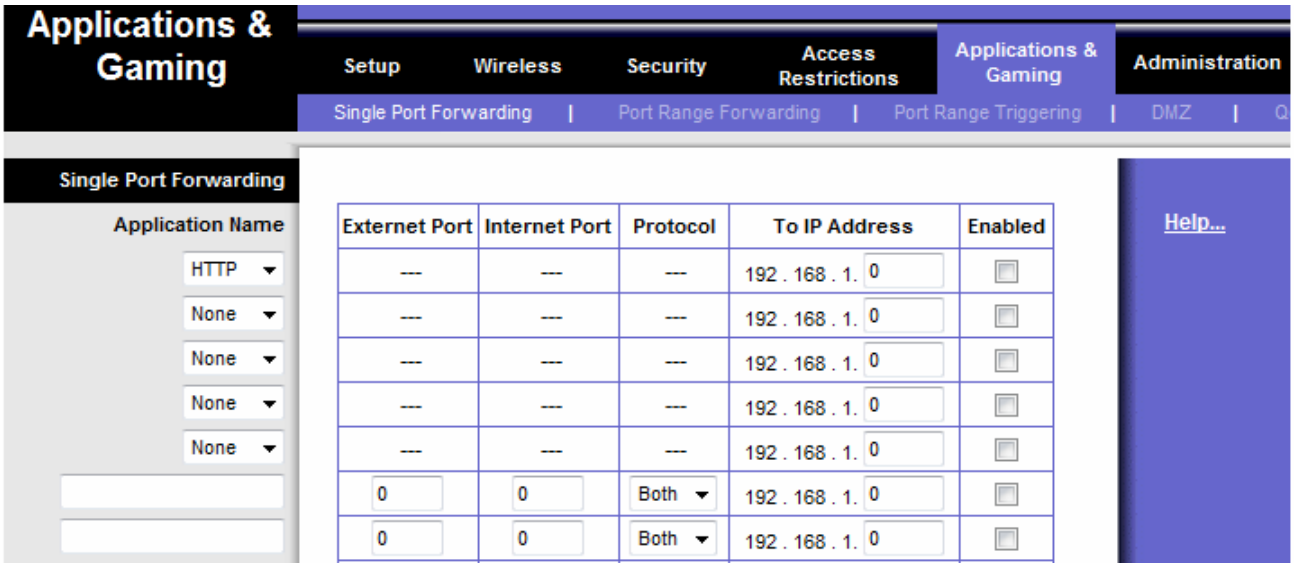
Việc cài đặt hosting DMZ trong bước 6 cho phép mở truy cập tới tất cả các port và các dịch vụ chạy trên Server như là HTTP, FTP và Telnet. Nếu 1 host được sử dụng cho 1 chức năng cụ thể, như là dịch vụ FTP hoặc Web, truy cập nên được giới hạn tới các dịch vụ cung cấp. Single port forwarding có thể hoàn thành công việc này và an ninh hơn là DMZ cơ bản, bởi vì nó chỉ mở những cổng cần thiết. Trước khi hoàn thành bước này, vô hiệu hóa thiết lập DMZ cho bước 1.

Host-B là server các cổng của nó được chuyển tiếp, nhưng truy cập bị giới hạn chỉ với giao thức HTTP(web).

a. *Từ màn hình chính, click vào* ***Applications & Gaming****, và sau đó click* ***Single Port Forwarding*** *để chỉ rõ các ứng dụng và các số hiệu cổng (port numbers).*

b. *Click vào Menu dưới tên* ***Application Name*** *và chọn* ***HTTP****. Đây là giao thức Web server cổng 80.*

c. *Trong hàng đầu tiên* ***To IP Address****, gõ vào địa chỉ IP của Host-B and chọn* ***Enabled****. click* ***Save Settings****.*



d. *Kiểm tra truy cập HTTP đến host DMZ bằng cách mở trình duyệt server bênngoài và trỏ vào địa chỉ bên ngoài của thiết bị. Thử tương tự trên Host-A đến Host-B.*

Bạn có thể truy cập trang Web không ? _____

e. *Kiểm tra truy cập Telnet bằng cách mở bằng câu lệnh như bước 5. Cố gắng thử Telnet tới địa chỉ IP bên ngoài của thiết bị sử dụng lệnh telnet A.B.C.D trong đó A.B.C.D là địa chỉ IP bên ngoài của thiết bị.*

Bạn có thể Telnet tới Server được không? _____

Bước 3: Khôi phục cấu hình mặc định của thiết bị

a. *Click vào* ***Administration > Factory Defaults****.*

b. *Click vào* ***Restore Factory Defaults*** *tất cả các cấu hình sẽ bị mất.*

Phần 3 – Giảng viên giao thêm bài cho sinh viên

IV. Thang điểm đánh giá

Bài	Điểm	Ghi chú
Phần 1	5	
Phần 2	2	
Phần 3	3	