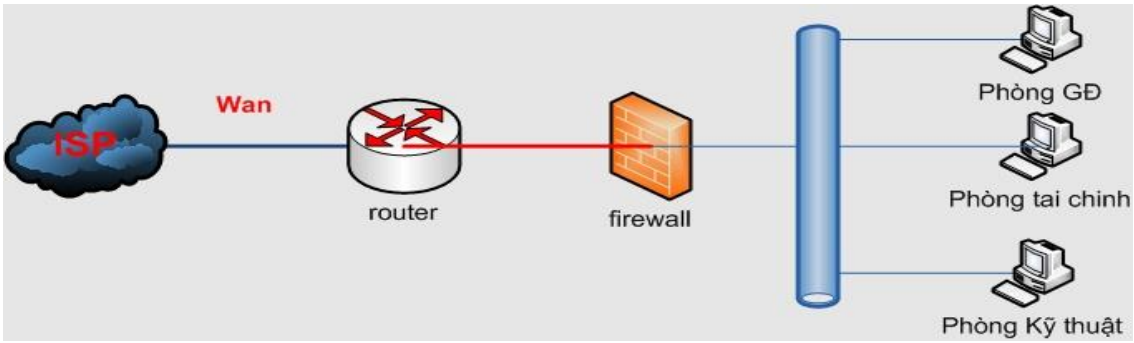
Bài thực hành số 2: An toàn mạng có dây

Nội dung yêu cầu: Xây dựng Firewall và IDS để bảo vệ mạng có dây

Phần 1 (5 điểm): Xây dựng mô hình Firewall



Mô tả hệ thống

1. **Một máy cài win server 2k3 (2k8) làm router: tạo 3 vlan gồm: phòng Giám Đốc, Phòng Kế Hoạch, Phòng Kỹ Thuật (có thể dùng 512 MB ram).**
2. **Một máy cài win server 2k3 (2k8) + isa 2k6: quản lý kết nối với internet và bảo vệ mạng nội bộ (có thể dùng 512MB ram).**
3. **Một máy cài win xp làm client: làm máy test (dùng 128MB ram).**

Máy router

Interface name	IP address	Subnet Mask	Default gateway	DNS
Cross (to Firewall)	192.168.5.2	255.255.255.0	192.168.5.1	
Lan_1	192.168.2.1	255.255.255.0		
Lan_2	192.168.3.1	255.255.255.0		
Lan_3	192.168.4.1	255.255.255.0		

Máy client

Interface name	IP address	Subnet Mask	Default gateway	DNS
Lan_1	192.168.2.2	255.255.255.0	192.168.2.1	8.8.8.8
Lan_2	192.168.3.3	255.255.255.0	192.168.3.1	8.8.8.8
Lan_3	192.168.4.2	255.255.255.0	192.168.4.1	8.8.8.8

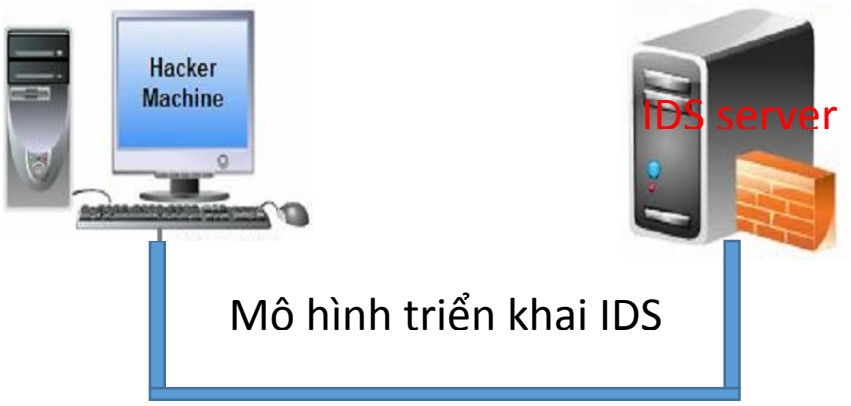
Máy Firewall

Interface name	IP address	Subnet Mask	Default gateway	DNS
Cross (to isp)	10.0.0.46	255.255.255.0	10.0.0.221	8.8.8.8
Lan_4 (to router)	192.168.5.1	255.255.255.0		

Yêu cầu:

1. Kiểm tra Default Rule
2. Tạo rule truy vấn DNS để phân giải tên miền
3. Tạo rule cho phép các user thuộc nhóm Manager truy cập Internet không hạn chế
4. Tạo rule cho phép các user thuộc nhóm Staff chỉ được phép truy cập 1 số trang web trong giờ hành chánh
5. Tạo rule cho phép các user thuộc nhóm Staff được truy cập web trong giờ giải lao, ngoại trừ trang ngoisao.net
6. Tạo rule cho phép user có thể kết nối mail yahoo bằng Outlook Express
7. Không cho nghe nhạc trực tuyến, cấm chat Yahoo Messenger, cấm download file có đuôi .exe
8. Cấm truy cập một số trang web, nếu truy cập sẽ tự động chuyển đến trang web cảnh cáo của công ty
9. Tạo VPN client to site cho phép remote user kết nối vào mạng nội bộ

Phần 2 (5điểm): Xây dựng hệ thống phát hiện xâm nhập với Snort IDS



Mô tả hệ thống

Máy IDS server:

- Sử dụng hệ điều hành: Centos, Ubuntu, Suse,…
- Cài đặt Mysql
- Cài đặt Snort IDS
- Cài đặt Base

Máy tấn công

Sử dụng Backtrack để tấn công, kiểm tra khả năng hoạt động của Snort IDS

Yêu cầu:

Cài đặt snort IDS và sử dụng web Base để kiểm tra khi có các cuộc tấn công.

- **Lưu ý:**

- Sinh viên sử dụng tên mình đặt mật khẩu ví dụ: sinh viên A tên Mai Vân Phương Vũ có password: vumvp
- Sử dụng các hệ điều Window, backtrack, Vmware,..
- Thực hiện report từng cá nhân, không thực hiện nhóm. Chụp hình hay quay phim lại
- Nghiêm cấm sao chép.