CHƯƠNG 7
BẢO MẬT: FIREWALL, PROXY SERVER VÀ ROUTER

ThS. Trần Bá Nhiệm
Website:
sites.google.com/site/tranbanhiem
Email: tranbanhiem@gmail.com

Nội dung

- Giới thiệu
- Xây dựng hệ thống mạng từ đầu
- Xây dựng hệ thống mạng doanh nghiệp
- Tunneling trong mạng doanh nghiệp
- Vấn đề cần tránh khi xây dựng hệ thống mạng

Giới thiệu

- Thảo luận các vấn đề thực tế khi thiết lập một mạng
- Nhìn nhận việc thiết kế/xây dựng hệ thống mạng dưới lăng kính lập trình
- Chia làm 2 phần:
  - Giải thích cách tạo một mạng tự chủ, các máy độc lập
  - Nghiên cứu các thiết bị trung gian có vai trò quan trọng trong mạng Internet: gateways, router, firewall,…

Xây dựng hệ thống mạng từ đầu

- Chọn kiến trúc mạng
- 3 kiểu kết nối vật lý chính: UTP, BNC, wireless
- UTP được dành cho dạng cấu trúc star. Trong mạng nhỏ thì một máy tính dùng modem hoặc thiết bị khác kết nối với ISP, các máy khác dùng chung kết nối này. Với mạng lớn thì 1 router kết nối trực tiếp với đường dây tới ISP

Xây dựng hệ thống mạng từ đầu

- BNC dùng cho kiến trúc bus. Hiện nay ít được sử dụng
- Người dùng sẽ mong đợi một cơ chế chia sẻ file trên mạng. Để hạn chế quyền truy xuất nên chú ý đến Permissions

Thiết lập VPN

- Virtual Private Network (VPN) cho phép các client từ xa truy xuất an toàn vào mạng LAN
- Việc thiết kế sẽ bảo đảm người dùng từ xa "trong suốt" đối với việc truy xuất đó để chia sẻ file, dùng máy in chung,…
- VPN hoạt động trên giao thức PPTP hoặc L2TP

Xây dựng hệ thống mạng thương mại

- Trong thực tế hiện nay, việc cấp phát cho mỗi người dùng một địa chỉ public để truy cập trực tiếp vào Internet là việc không thể làm được (do khan hiếm địa chỉ)
- Khắc phục: nhóm người dùng kết nối với gateway, từ đó có kết nối trực tiếp đến Internet

Xây dựng hệ thống mạng thương mại

- Gateway là từ tổng quát chỉ thiết bị kết nối giữa mạng LAN và Internet
- Gateway có thể là một máy tính hoặc thiết bị chuyên dụng hoạt động độc lập
- Proxy và router chính là các gateway
- Proxy là dạng phần mềm chạy trên một máy tính
- Router là thiết bị phần cứng chuyên dụng hoạt động độc lập

Router

- Proxy có nhược điểm về hiệu suất hoạt động
- Router xử lý ở mức gói tin (packet) nên tốc độ xử lý vượt trội so với proxy. Nó hướng các gói đến đúng hướng, thay vì gửi một cách mù quáng đến router kế tiếp
- Router gần như “trong suốt” đối với các client nên độ linh hoạt cao hơn

Router

- Router phải có ít nhất 2 interface, trong đó chắc chắn có 1 dùng để nối tiếp đến mạng WAN(kết nối nối ISP). Mỗi port LAN có thể được nối vào 1 máy tính hoặc hub, switch.
- Các vấn đề cần thu thập từ ISP:
  - Địa chỉ IP cố định được phép dùng
  - IP của default gateway
  - Subnet mask?
  - Primary và secondary DNS

Router

- Mỗi máy tính nằm sau router phải được thiết lập địa chỉ default gateway và DNS server của nó đến giá trị gateway

Firewall

- Firewall thực hiện chức năng kiểm soát dòng dữ liệu đi vào và đi ra khỏi mạng LAN với tốc độ xử lý rất cao
- Firewall có thể được hiện thực bằng phần mềm hoặc phần cứng

Proxy

- Proxy có thể là phương án được xem xét nếu ta chỉ có kinh phí ít hoặc số lượng host truy cập nhỏ
- Proxy sẽ làm chậm tốc độ truy cập tương đối rõ
- Thiết kế bằng cách sử dụng 1 máy tính đóng vai trò proxy, chia sẻ kết nối Internet của nó cho các máy khác trong mạng

Proxy

- Tất cả các máy khác cần phải biết địa chỉ IP của máy proxy.
- Cách thiết lập trong IE: Tools→Internet Options→Connections→LAN Settings→Use a proxy server
- 2 dạng proxy:
  - Proxy mức ứng dụng
  - Proxy mức mạch điện tử

Proxy

- Proxy mức ứng dụng thông thường chấp nhận chỉ 1 giao thức như HTTP
- Proxy mức mạch điện tử có thể chấp nhận bất kỳ giao thức nào trên IP. Phổ biến thuộc loại này là SOCKS (xem RFC 1928)
- Để dùng SOCKS client phải chứng thực chính nó

NAT

- Network address translator (NAT)
- NAT chuyển đổi địa chỉ IP từ private thành public khi gói tin đi ra khỏi mạng LAN, ghi nhận vào bảng chuyển đổi NAT
- Khi gói tin phản hồi đến, NAT sẽ tra trong bảng chuyển đổi và biết được IP private để chuyển đến đúng host bên trong

NAT

- NAT được phát triển bởi hãng CISCO, nhưng hiện đã trở thành chuẩn Internet (xem RFC 1631)
- Static NAT là kiểu mà mỗi địa chỉ private đều có địa chỉ public tương ứng, điều đó có nghĩa là mỗi máy tính đều phân biệt được đối với mạng ngoài, nhưng chưa được phép truy cập đến

NAT

- Dynamic NAT là kiểu mà mọi địa chỉ private được ánh xạ đến 1 địa chỉ public duy nhất, khác nhau bởi tham số bổ sung là local port
- NAT cần lưu thông tin gói tin đã gửi ra
- Một mạng có 100 máy có thể tạo ra 6 triệu phiên làm việc đồng thời

Tunneling trong mạng doanh nghiệp

- Nếu khách hàng đã có mạng hoạt động nhưng ứng dụng không làm việc được trên đó thì không thể bỏ qua vấn đề này được
- Tình huống có thể: ví dụ như các ứng dụng hội thảo trực tuyến không làm việc được ở sau một firewall, thì khi đó có 3 phương án giải quyết:
  - chuyển server ra ngoài firewall

Tunneling trong mạng doanh nghiệp

  - thiết lập port chuyển qua tunnel đến firewall (hoặc router)
  - dữ liệu được tung lên một máy chủ proxy để tránh firewall
- Hai phương án đầu có thể triển khai trên cùng server
- Phương án sau phải thuê server độc lập chuyên dụng và có thể lập trình được trên đó

Proxy tunneling

- Không giống như router, các proxy không ‘trong suốt” đối với client.
- Cần phải chỉnh sửa code để tham chiếu đến proxy
- Khai báo và sử dụng proxy thông qua lớp WebProxy và HTTPWebRequest

Proxy tunneling

```
WebProxy myProxy= new
WebProxy("proxyserver",8080);
myProxy.BypassProxyOnLocal = true;
String url = "http://www.yahoo.com";
HttpWebRequest request =
(HttpWebRequest)HttpWebRequest.Create(
url);
request.Proxy = myProxy;
```

Firewall tunneling

- Nếu firewall được thiết lập block tất cả các cổng, thì sau đó bạn có thể thay đổi firewall cho phép truy cập vào cổng yêu cầu.
- Truy cập firewall thông qua địa chỉ web: http://192.168.1.1 hoặc tương tự, hoặc thông qua kết nối serial
- Một số router cho phép thiết lập cổng được chuyển dữ liệu thẳng mà không qua firewall

Firewall tunneling

- Tổng quát, nếu không muốn truy cập vào firewall hoặc muốn cung cấp một giải pháp thân thiện người dùng thì ràng buộc dữ liệu trên 1 proxy. Máy tính ở sau firewall sẽ mở kết nối TCP với proxy, dữ liệu từ client đến proxy được chuyển qua kết nối đó. Đây là kỹ thuật mà các ứng dụng Instant Messenger dùng

Phòng tránh

- Phòng tránh luôn luôn là cách tốt hơn để xảy ra sự cố rồi mới tìm cách chữa trị
- Một số vấn đề cần phòng tránh bao gồm:
  - Xung đột port
  - Vấn đề cấp phát IP động

Xung đột port

- Nếu phần mềm không thể chạy trên port mặc định của nó, ta hãy nghĩ đến việc chuyển sang port khác, hoặc nhắc nhở cho người dùng chuyển sang port khác. Nếu không ta có thể gặp 2 vấn đề:
  - Người dùng sẽ chắc chắn chạy phần mềm dùng trùng port với bạn và họ không muốn ngừng phần mềm đó

Xung đột port

- Firewall có thể đã được thiết lập để cho phép lưu thông qua một số port, thậm chí trong trường hợp người dùng phần mềm không dùng nhưng ISP của họ thì có
- Các client đang chờ kết nối vào ứng dụng cần phải biết port đã thay đổi. Bạn đơn giản chỉ cần hiển thị hộp thoại và cho phép người dùng nhập vào port mới, hoặc có thể dùng 1 DNS request để biết server đang lắng nghe trên port nào

Vấn đề cấp phát IP động

- Đây là vấn đề khá thường gặp phải
- Các ứng dụng thường mắc sai lầm là giả định địa chỉ IP cục bộ tĩnh trong suốt hoạt động của nó
- Cách giải quyết là dùng cơ chế theo dõi IP
- Phần mềm "không IP" có thể dùng kiểu ánh xạ một địa chỉ IP động từ DNS name
- Khi post 1 địa chỉ IP cần bảo đảm là địa chỉ public. Địa chỉ như 192.168.0.1 cho client không phải là ý tưởng tốt đối với thế giới bên ngoài

Bài tập

- Đọc và nghiên cứu các tài liệu về RFC được giới thiệu trong chương
- Vận dụng khả năng cài đặt hệ thống ảo trên máy tính để hiện thực cơ chế hoạt động của các thiết bị router, firewall,…