Kết nối dịch vụ mạng riêng với Internet

Phạm Huy Hoàng - SoICT/HUST
hoangph@soict.hust.edu.vn

ONE LOVE. ONE FUTURE.

1

Kết nối dịch vụ cơ bản của Private Network với Internet

- Kết nối tầng giao vận & các dịch vụ
- Qui hoạch public server trong mạng private
- Dịch vụ IP cơ bản: DNS, Mail, FTP
- Qui hoạch vùng máy chủ trong mạng riêng

2

Dịch vụ IP cơ bản (nhắc lại)

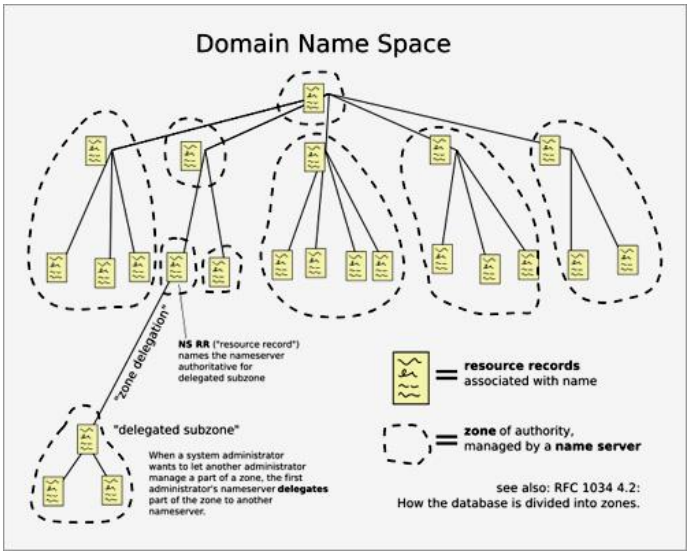
Dịch vụ	Giao thức tầng ứng dụng	Giao thức tầng giao vận
domain name	DNS	UDP
e-mail	SMTP	TCP
remote terminal access	Telnet	TCP
Web	HTTP	TCP
file transfer	FTP	TCP
streaming multimedia	giao thức riêng (e.g. RealNetworks)	TCP or UDP
Internet telephony	giao thức riêng (e.g., Vonage,Dialpad)	thường là UDP

Nhắc lại các khái niệm dịch vụ DNS

- Tên miền: định danh trên tầng ứng dụng cho các nút mạng
  - Trên Internet được quản lý tập trung
  - Quốc tế: ICANN
  - Việt Nam: VNNIC
- DNS (Domain Name System): hệ thống tên miền gồm các máy chủ quản lý thông tin tên miền và cung cấp dịch vụ DNS
- Vấn đề phân giải tên miền sang địa chỉ IP
  - Người sử dụng dùng tên miền để truy cập dịch vụ
  - Máy tính và các thiết bị mạng không sử dụng tên miền mà dùng địa chỉ IP khi trao đổi dữ liệu
- Làm thế nào để chuyển đổi tên miền sang địa chỉ IP?

Không gian tên miền

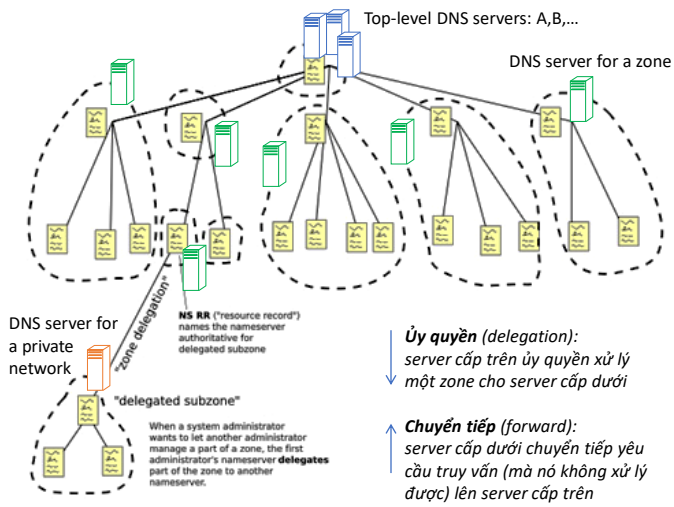
- Kiến trúc : hình cây
  - Root: Nút gốc
  - Chia thành các zone
- Mỗi nút là một tập hợp các bản ghi mô tả tên miền tương ứng với nút đó. Ví dụ:
  - SOA
  - NS
  - A
- Các tên miền "mới"
  - Top level
  - daotao.ai
  - zalo.me



Hình ảnh từ: Wikipedia

Internet DNS servers & private DNS server

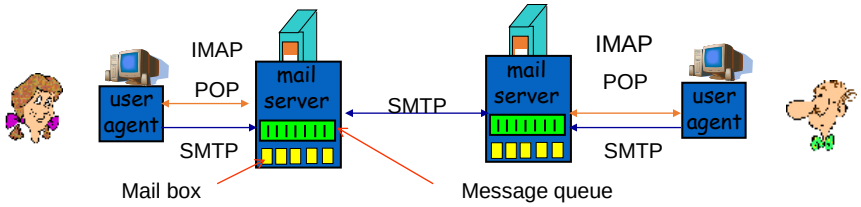
- Dịch vụ tên miền Internet đang được cung cấp bởi sự kết hợp của các top-level DNS servers và các DNS servers của các zone
- Mạng nội bộ bổ sung DNS server để xử lý các tên miên nội bộ
- Khai báo "forward" để xử lý truy vấn tên miền Internet (mà server nội bộ không có khả năng)
- Xin "delegate" zone private để server cấp trên ủy quyền dữ liệu zone private này cho server nội bộ
- Cần cơ chế xác thực giữa server private với server cấp trên trực tiếp



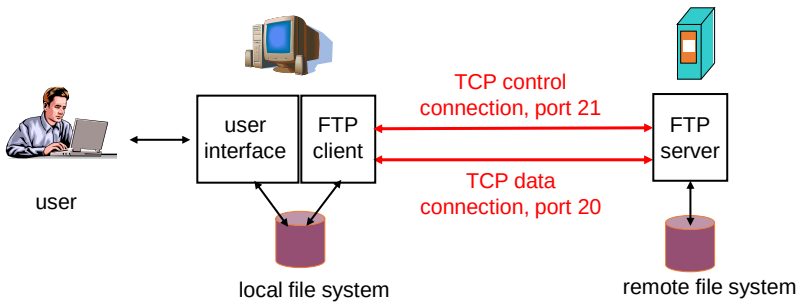
Dịch vụ thư điện tử (Email)

- MUA (Mail User Agent)
  - Lấy thư từ máy chủ
  - Gửi thư đến máy chủ
  - VD: Outlook, Thunderbird…
- MTA (Mail Transfer Agent): :
  - Chứa hộp thư đến của NSD (mail box)
  - Hàng đợi để gửi thư đi
  - VD: Sendmail, MS Exchange…

- Giao thức:
  - Chuyển thư: SMTP-Simple Mail Transfer Protocol
  - Nhận thư
    - POP – Post Office Protocol
    - IMAP – Internet Mail Access Protocol



Dịch vụ truyền file: File Transfer Protocol (FTP)

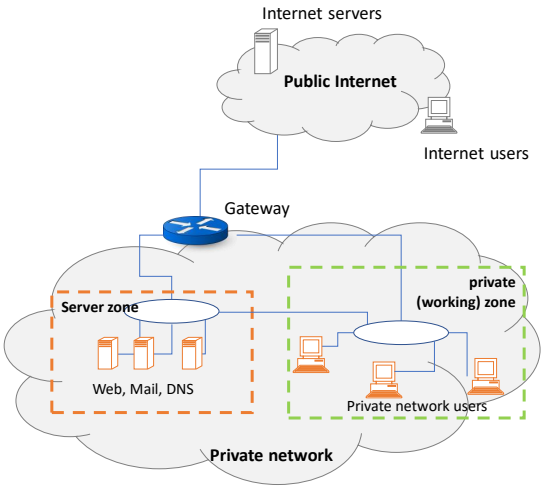


- Mô hình Client-server
- Trao đổi file giữa các máy
- Sử dụng TCP, cổng dịch vụ 20, 21

- Điều khiển Out-of-band :
  - Lệnh của FTP : cổng 21
  - Dữ liệu: cổng 20
- Người dùng phải đăng nhập trước khi truyền file
- Một số server cho phép người dùng với tên là anonymous

Qui hoạch public server trong mạng private

- Private servers được qui hoạch trong một vùng riêng của mạng private, gọi là server zone
- Truy nhập đến private servers:
  - Từ người dùng trong mạng private (theo đường nội bộ, an toàn, tin cậy)
  - Từ người dùng trên Internet (không an toàn, không tin cậy)
  - Từ các server trên Internet (an toàn, tin cậy)
- Truy nhập đến các public Internet servers:
  - Từ người dùng trong mạng private
  - Từ các server trong mạng private



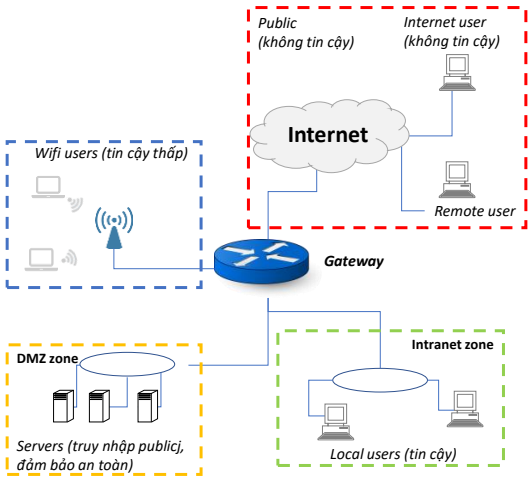
Đảm bảo an toàn mạng nội bộ

- Qui hoạch các vùng an toàn trong mạng nội bộ
- Tường lửa (firewall)
- Phát hiện & chống xâm nhập (IDS, IPS)

Thiết kế mạng IP (handout) – Phạm Huy Hoàng – ĐHBK Hà Nội
Tham khảo: https://users.soict.hust.edu.vn/hoangph/textbook/toc.html

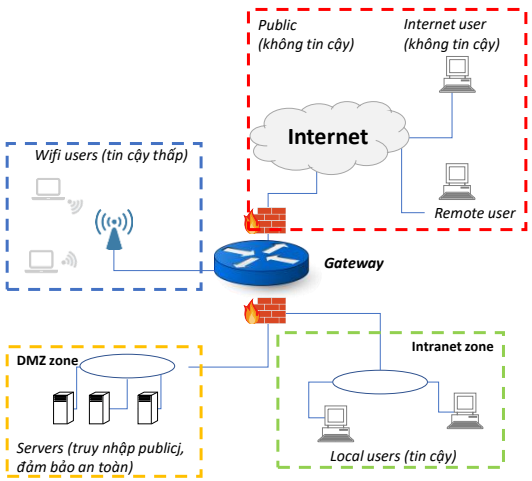
Qui hoạch các vùng mạng nội bộ

- Mục đích
  - "Nhóm" các trạm làm việc để xử lý đảm bảo an toàn cùng nhau
  - Các trạm làm việc trong cùng nhóm có nguy cơ bảo mật như nhau
  - Nhóm "không dây", nhóm "máy chủ", nhóm "trạm làm việc an toàn", v.v..
- Phương pháp chia nhóm thông thường:
  - "Green": các trạm làm việc tin cậy, kết nối có dây, kiểm soát tối đa (ra/vào mạng, cài đặt phần mềm, virus, v.v..)
  - "Orange": còn gọi là DMZ, vùng truy nhập tranh chấp giữa private và public. Nơi kết nối server
  - "Blue": vùng wifi. Không kiểm soát kết nối mạng vật lý
  - "Red": vùng public, không tin cậy



Tường lửa (Firewall)

- Đặt tại vị trí kiểm soát được kết nối giữa các vùng đã qui hoạch
- Đặc biệt quan tâm đến vùng Green và Red
- Tùy vào thiết kế hình trạng của mạng nội bộ để quyết định vị trí đặt tường lửa
  - Phía ngoài Gateway, kết nối với public Internet
  - Kết nối giữa vùng Green và DMZ
- Nguyên tắc hoạt động
  - Luật kiểm soát giao thông giữa các vùng: cho phép (grant) hoặc cấm (deny)
  - Mặc định cấm + các luật cho phép
  - Mặc định cho phép + các luật cấm

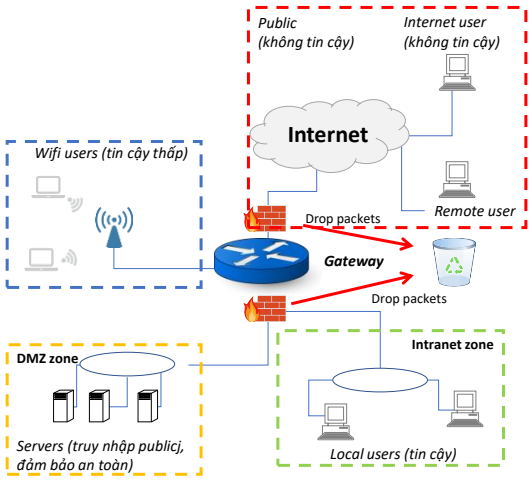


Các loại tường lửa

- Tường lửa kiểu cổng lọc gói tin (packet filtering gateway)
  - Đơn giản nhất nhưng vẫn hiệu quả ➔ phổ biến nhất
  - Luật kiểm soát truy nhập dựa trên các trường dữ liệu của gói tin: địa chỉ (nguồn/đích), loại giao thức, cổng truy nhập, v.v..
  - Đảm bảo hiệu năng ➔ không kiểm tra nội dung gói tin ➔ bài toán lạm dụng giao thức
- Tường lửa dựa trên trạng thái (stateful inspection firewall)
  - Khái niệm trạng thái (state) hay ngữ cảnh (context) của dòng giao thông
  - Bài toán chống quét cổng (trinh sát)
  - Ghi nhớ dòng dữ liệu (gói tin) & phát hiện nghi vấn: gửi đi từ một địa chỉ, tần suất gửi gói tin vượt ngưỡng, kết nối liên tục đến hoàng loạt cổng, v.v..
- Tường lửa kiểu bảo vệ (guard)
  - Hoạt động giống như một proxy ở tầng ứng dụng: nhận gói tin, kiểm soát, tạo gói tin mới, nhận kết quả, tạo gói tin kết quả trả về cho người yêu cầu
  - Kiểm soát chi tiết, loại bỏ hầu như mọi rủi ro
  - Great Firewall of China: https://en.wikipedia.org/wiki/Great_Firewall
- Tường lửa cá nhân (personal firewall)
  - Ứng dụng chạy trên máy trạm cần được bảo vệ
  - Có thể được cung cấp như một cấu phần của hệ điều hành

Tường lửa: Thiết lập luật giữa các vùng

	Direction		Status
Red	→	Firewall	Closed, Use external access
Red	→	Orange	Closed. Use port forwarding
Red	→	Blue	Closed. Use port forwarding or VPN
Red	→	Green	Closed. Use port forwarding or VPN
Orange	→	Firewall	Closed, No DNS nor DHCP for Orange
Orange	→	Red	Open
Orange	→	Blue	Closed, use DMZ pinholes
Orange	→	Green	Closed, use DMZ pinholes
Blue	→	Firewall	Closed, no access for Blue
Blue	→	Red	Closed, no access for Blue
Blue	→	Orange	Closed, no access for Blue
Blue	→	Green	Closed, use DMZ pinholes or VPN
Green	→	Firewall	Open
Green	→	Red	Open
Green	→	Orange	Open
Green	→	Blue	Open

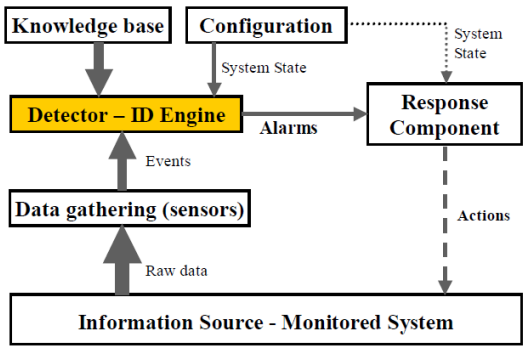


Hệ thống phát hiện & chống xâm nhập IDS/IPS

- Tại sao cần hệ thống phát hiện xâm nhập?
  - Tường lửa tạo cảm giác yên tâm cho mạng nội bộ nhưng chưa quyết triệt để các vấn đề tấn công mạng.
  - Sự cố bảo mật gây ra bởi các trạm bên trong (vùng Blue & Green)
- Intrusion Detection System (IDS):
  - Theo dõi các hoạt động trên mạng, phát hiện sớm nghi ngờ hoặc các hoạt động có khả năng gây hại (như hệ thống báo khói trong tòa nhà)
  - Xử lý nghi ngờ không nằm trong phạm vi của IDS
- IDS phản ứng nhanh:
  - Tự động chuyển sang chế độ bảo vệ: cách ly thành phần nghi ngờ nhiễm độc, ngăn chặn truy cập tài nguyên, v.v..
  - IDS bổ sung chức năng bảo vệ (Protection) thay vì chỉ phát hiện (Detection) ➔ IPS

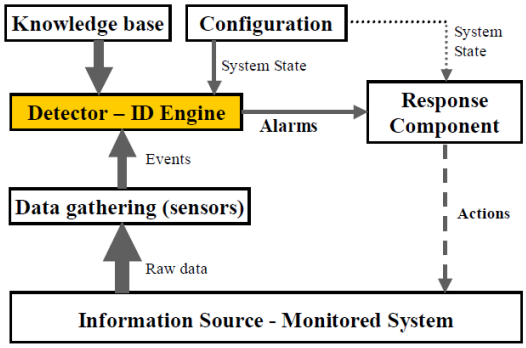
Kiến trúc IDS

- Các thành phần cơ bản của IDS:
  - Data gathering: thu thập thông tin (sensors) từ hệ thống cần giám sát
  - Detector – ID Engine: xử lý dữ liệu từ hệ thống sensor để phát hiện truy nhập khả nghi
  - Response Component: xử lý truy nhập khả nghi, có thể là cảnh báo người quản trị hoặc can thiệp ngay để ngăn chặn (chức năng Protection của IPS)
  - Knowledge base (database): thông tin hỗ trợ Detector xử lý dữ liệu sensor phát hiện truy nhập
  - Configuration: cấu hình cho Detector tùy theo trạng thái hệ thống (system state)
- Cơ chế phát hiện truy nhập
  - Signature-based: dựa trên dấu hiệu nhận biết
  - Abnomal-based: dựa trên hành vi bất thường



Phân loại IDS

- Information source
  - Host based
  - Network based
  - Application Logs
  - Wireless networks
  - Sensor Alerts
- Analysis strategy
  - Anomaly Detection
  - Misuse Detection
- Time Aspects
  - Real-time prediction
  - Off-line prediction
- Architecture
  - Centralized
  - Distributed & heterogeneous
- Response
  - Active response
  - Passive reaction

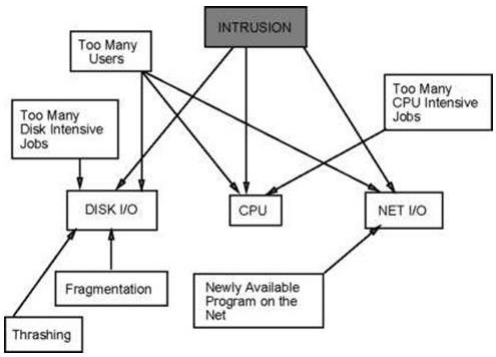


IDS dựa trên dấu hiệu nhận biết

- Chủ yếu dựa trên thông tin các trường header trong gói tin (IP, ICMP, TCP, v.v..). Ví dụ nhận biết có truy nhập ssh từ bên ngoài:
  - alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"incoming SSH connection!"; flags:S; sid:10000;)
- Cũng có thể dựa trên nội dung. Ví dụ nhận biết một trạm thuộc vùng Green truy nhập đến danh sách terrorism:
  - alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"terrorism contact!"; content:"terrorism"; nocase; sid:10003;)
- Xây dựng các luật nhận biết không đơn giản, có sự tham gia của cộng đồng. Ví dụ sau là một luật nhận biết có truy nhập khai thác lỗ hổng bảo mật ssh đã được cộng đồng phát hiện và chia sẻ luật xử lý:
  - alert tcp $EXTERNAL_NET any -> $HOME_NET $SSH_PORTS (msg:"INDICATOR-SHELLCODE ssh CRC32 overflow filler"; flow:to_server,established; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; fast_pattern:only; metadata:policy max-detect-ips drop, ruleset community; reference:bugtraq,2347; reference:cve,2001-0144; reference:cve,2001-0572; classtype:shellcode-detect; sid:1325; rev:14;)

IDS dựa trên hành vi bất thường

- IDS dựa trên dấu hiệu nhận biết chỉ phát hiện được các tấn công có dấu hiệu đã được khai báo. Kỹ thuật này cũng chỉ áp dụng được với các tấn công dấu hiệu cố định.
- IDS dựa trên hành vi bất thường hướng đến xử lý các tồn tại của IDS dựa trên đấu hiệu nhận biết. Cơ chế là dựa trên mô hình thống kê mô tả trạng thái bình thường và so sánh với dữ liệu sensor để phát hiện bất thường



Tham khảo thực hành IDS/IPS

- Snort: IDS dựa trên dấu hiệu nhận biết:
  - https://users.soict.hust.edu.vn/hoangph/textbook/ch05-3.html
- IPS: Snort + IPFire:
  - https://users.soict.hust.edu.vn/hoangph/textbook/ch05-4.html