

Bảo mật mạng máy tính



Bảo mật mạng máy tính



- Bảo mật mạng máy tính với các thiết bị
- Bảo mật mạng máy tính với các giao thức
- Bảo mật mạng máy tính với các phần mềm
- Một số quy tắc và chú ý

Thiết bị mạng



- Mô hình sử dụng HUB, SWITCH
- Thiết bị firewall cứng

SWITCH - HUB



- Mô hình truyền tin trên HUB
 - Mô hình vật lý dạng hình sao
 - Mô hình logic là mạng BUS
 - Các gói tin được truyền lần lượt đến các đầu mạng
 - Thiết bị mạng tự nhận dạng gói tin cần để xử lý
 - Những vấn đề
 - Tăng lưu lượng mạng
 - Khả năng bị nghe lén trong mạng
 - Giả mạo địa chỉ IP
 - Không ngăn chặn được địa chỉ, công nghi ngờ

SWITCH – HUB (t)



- Mô hình truyền tin trên SWITCH
 - Mô hình vật lý dạng hình sao
 - Mô hình logic là mạng sao
 - Mạng tự học thông tin MAC, địa chỉ IP, Port (physics)
 - Tạo bảng ánh xạ truyền
 - Cho phép cấu hình đến từng cổng (port)
 - Phân tải, lưu lượng
 - Những vấn đề
 - Giảm bớt lưu lượng mạng
 - Xác định nguồn gửi
 - Tạo được các VLAN
 - Việc đặt lại các bảng SWITCH có thể lợi dụng tấn công

SWITCH – HUB (t)



- So sánh
 - SWITCH nhiều điểm lợi hơn
 - Lưu lượng
 - Giảm bớt nghe lén
 - Có thể phân biệt dải địa chỉ giảm bớt giả mạo địa chỉ IP
 - Cấu hình giảm bớt các tấn công trên các cổng mạng
 - Nhật ký
 - Nguy cơ
 - Bị đánh chiếm bảng SWITCH tạo nguy cơ tấn công man-in-the-middle
 - Xu hướng: sử dụng SWITCH thay thế cho các HUB

ROUTER



- Sử dụng để chuyển mạng
 - Chuyển các gói mạng khác nhau
 - Thực hiện tìm đường cho các gói tin
- Tính năng
 - Giảm lưu lượng mạng không cần thiết
 - Kết nối giữa các mạng, mạng con
 - Thực hiện về băng thông
- Kết hợp
 - Kết hợp với log
 - Kết hợp với firewall

Wireless Access point



- Phát các tín hiệu mạng không dây
 - Cung cấp dịch vụ
 - Đặt mật khẩu
 - Đặt các điều kiện lọc
 - Tích hợp một số dịch vụ khác: firewall, ...

Wireless Access point (t)



☐ **Disable Security**

☐ **WEP**

Type: Automatic ▼

WEP Key Format: Hexadecimal ▼

Key Selected	WEP Key	Key Type
Key 1: <input checked="" type="radio"/>	<input type="text"/>	Disabled ▼
Key 2: <input type="radio"/>	<input type="text"/>	Disabled ▼
Key 3: <input type="radio"/>	<input type="text"/>	Disabled ▼
Key 4: <input type="radio"/>	<input type="text"/>	Disabled ▼

☐ **WPA/WPA2**

Version: Automatic ▼

Encryption: Automatic ▼

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: (in second, minimum is 30, 0 means no update)

Wireless Access point (t)



Wireless MAC Filtering

Wireless MAC Filtering: **Disabled**

Enable

Filtering Rules

- ☒ **Allow** the stations not specified by any enabled entries in the list to access.
- ☐ **Deny** the stations not specified by any enabled entries in the list to access.

ID	MAC Address	Status	Description	Modify
----	-------------	--------	-------------	--------

Add New...

Enable All

Disable All

Delete All

Firewall cứng



- Bản chất của Firewall cứng
 - Kiểm soát được gói tin ở mức 1
 - Kiểm soát được cổng (port mềm)
 - Kiểm soát được địa chỉ IP
 - Không kiểm soát về mặt nội dung truyền (mã độc)
 - Log các lưu lượng mạng
 - Tốc độ xử lý, sử dụng CPU của thiết bị
 - Bảo vệ toàn bộ mạng thông qua thiết bị
 - Thiết bị chuyên biệt
 - Tích hợp vào các router, switch trong hệ thống

Firewall cứng (t)



- Bảo vệ
 - Ngăn chặn các địa chỉ IP đến, đi nghi ngờ
 - Ngăn chặn một số dịch vụ (cổng)
 - Chặn thiết bị thông qua địa chỉ MAC
 - Với tích hợp với dịch vụ mức cao hơn có thể:
 - Quản lý về nội dung đơn giản

Static Route

Static Route

Disable ▾

IP Address

Subnet Mask

Gateway

Metric

Interface

LAN ▾

Apply

Refresh

Show Route Table

Static Route Table

Index	Destination IP Address	Subnet Mask	Gateway	Metric	Interface	Delete
-------	------------------------	-------------	---------	--------	-----------	--------

Hình ảnh router (t)



Media Bandwidth Management

Media Bandwidth Management

Active

Disable ▾

Automatic Uplink Speed

Enable ▾

Manual Uplink Speed

(Kbps)

Automatic Downlink Speed

Enable ▾

Manual Downlink Speed

(Kbps)

Media Bandwidth Management Rules

Address Type

IP ▾

Protocol

TCP ▾

Local IP Address

~

Port

~ (1~65535)

Mode

Guaranteed minimum bandwidth ▾

Uplink Bandwidth

(Kbps)

Hình ảnh router (t)



Denial of Service

☐ Enable DoS Prevention

- | | |
|---|---|
| <input type="checkbox"/> Whole System Flood: SYN | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> Whole System Flood: FIN | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> Whole System Flood: UDP | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> Whole System Flood: ICMP | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> TCP/UDP PortScan | <input type="text" value="Low"/> (Sensitivity) |

- | | |
|--|--|
| <input type="checkbox"/> Per-Source IP Flood: SYN | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> Per-Source IP Flood: FIN | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> Per-Source IP Flood: UDP | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> Per-Source IP Flood: ICMP | <input type="text" value="0"/> (Packets/Second) |
| <input type="checkbox"/> Enable Source IP Blocking | <input type="text" value="5"/> Block time (sec), 0 means no drop |

- ☐ ICMP Smurf
- ☐ IP Land
- ☐ IP Spoof
- ☐ IP TearDrop
- ☐ PingOfDeath

Hình ảnh router(t)



Content Filter

Keyword Blocking Settings

Enable URL keyword Blocking

Disable ▾

Keyword

Add

Refresh

Keyword List

Index	Active	Keyword	Delete
-------	--------	---------	--------

Hình ảnh router



- Quick Setup
- QSS
- + Network
- + Wireless
- + DHCP
- + Forwarding
- Security
 - Basic Security
 - Advanced Security
 - Local Management
 - Remote Management
- Parental Control
- + Access Control
- + Static Routing
- + Bandwidth Control
- + IP & MAC Binding
- Dynamic DNS

Firewall	
SPI Firewall:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VPN	
PPTP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
L2TP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPSec Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ALG	
FTP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
TFTP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
H323 ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/>	

Hình ảnh router



Advanced Security

Packets Statistics Interval (5 ~ 60): Seconds

DoS Protection: ☒ Disable ☐ Enable

☐ Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 ~ 3600): Packets/s

☐ Enable UDP-FLOOD Filtering

UDP-FLOOD Packets Threshold (5 ~ 3600): Packets/s

☐ Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): Packets/s

☐ Ignore Ping Packet From WAN Port

☐ Forbid Ping Packet From LAN Port

Save

Blocked Dos Host List

Thiết bị phần cứng



- Các thiết bị mạng
 - Có hệ thống nhật ký và phân tích
 - Thường tích hợp thêm firewall
 - Tích hợp thêm các chức năng xác thực và dịch vụ bảo mật mở rộng
 - Phân tích và chống lại một số mô hình tấn công
 - Cần tìm hiểu và khai thác phù hợp

Giao thức bảo mật



- Một số giao thức
 - Sử dụng IPSec
 - Sử dụng SSL
- Đặc điểm
 - Thực hiện tạo phiên và mã hóa, xác thực theo phiên
 - Có kiểm soát lại theo thời gian
 - Mã hóa thông tin gửi

Giao thức bảo mật (t)



- Chống các loại hình tấn công phiên
- Chống tấn công nghe lén

Dịch vụ bảo mật



- Sử dụng VPN
 - Thực tế dịch vụ IPSec
 - Sử dụng hạ tầng internet

Các phần mềm chuyên dụng



- Firewall
- Anti virus
- Internet security

Các phần mềm chuyên dụng (t)

- Firewall
 - Sử dụng các tính năng của firewall cơ bản
 - Kết hợp với các lớp ở mức trên
 - Kiểm tra được nội dung
 - Kiểm tra được tiến trình liên quan
 - Có thể kiểm soát được tấn công liên quan đến firewall
 - Kết hợp kiểm soát trojan và backdoor
 - Ngăn chặn được một số nội dung đơn giản

Các phần mềm chuyên dụng (t)

- Phần mềm diệt virus – anti virus
 - Mô hình phát hiện
 - So sánh mẫu
 - So sánh thông minh
 - Mô hình kiểm tra
 - Kiểm tra thụ động
 - Kiểm tra trực tuyến (kiểm tra thời gian thực)

Các phần mềm chuyên dụng (t)

- Phần mềm diệt virus – anti virus
 - Kiểm tra các loại mã độc
 - Virus
 - Worm
 - Trojan
 - Spyware
 - rookit

Các phần mềm chuyên dụng (t)

- Phần mềm diệt virus – anti virus
 - Kiểm tra dựa cơ sở dữ liệu
 - Sức mạnh dựa vào cơ sở dữ liệu
 - Tối ưu về thời gian thực hiện

Các phần mềm chuyên dụng (t)

- Phần mềm diệt internet security
 - Sự kết hợp giữa một số tính năng
 - Firewall
 - Anti virus
 - Và kiểm soát các tiến trình mạng

Mô hình máy chủ xác thực



- Sử dụng proxy - ISA server (Internet Security and Acceleration Server)
 - Kết hợp firewall cùng với proxy
 - Tăng cường khả năng xác thực, xác nhận người dùng
 - Kiểm soát mạng nội bộ và mạng bên ngoài
 - Ngăn chặn được trao đổi trong ngoài tránh các tấn công trực tiếp
 - Kiểm soát được nội dung truyền của

Mô hình máy chủ xác thực (t)

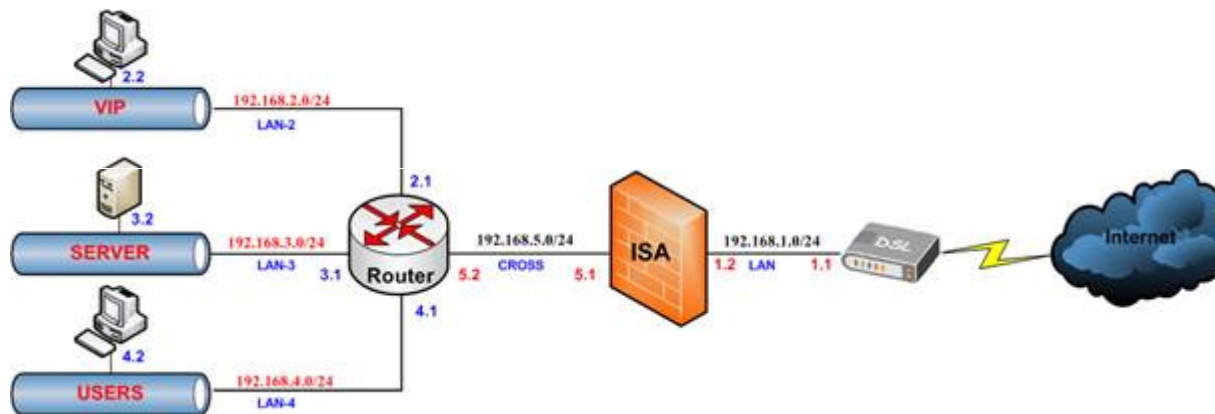
- Sử dụng proxy - ISA server (Internet Security and Acceleration Server)
 - Chống được tấn công trực diện vào máy tính mạng
 - Đảm bảo xác thực kết nối
 - Ngăn chặn được những kết nối không phép:
 - Back door, trojan
 - Ngăn chặn một phần phát tán mã độc
 - Nhật ký và nhật ký nội dung
 - Tấn công xã hội
 - Nhân viên xấu

Mô hình máy chủ xác thực (t)

- Sử dụng proxy - ISA server (Internet Security and Acceleration Server)
 - Hỗ trợ kết nối làm việc ngoài an toàn hơn
 - Nguy cơ bị tấn công và kiểm soát proxy server

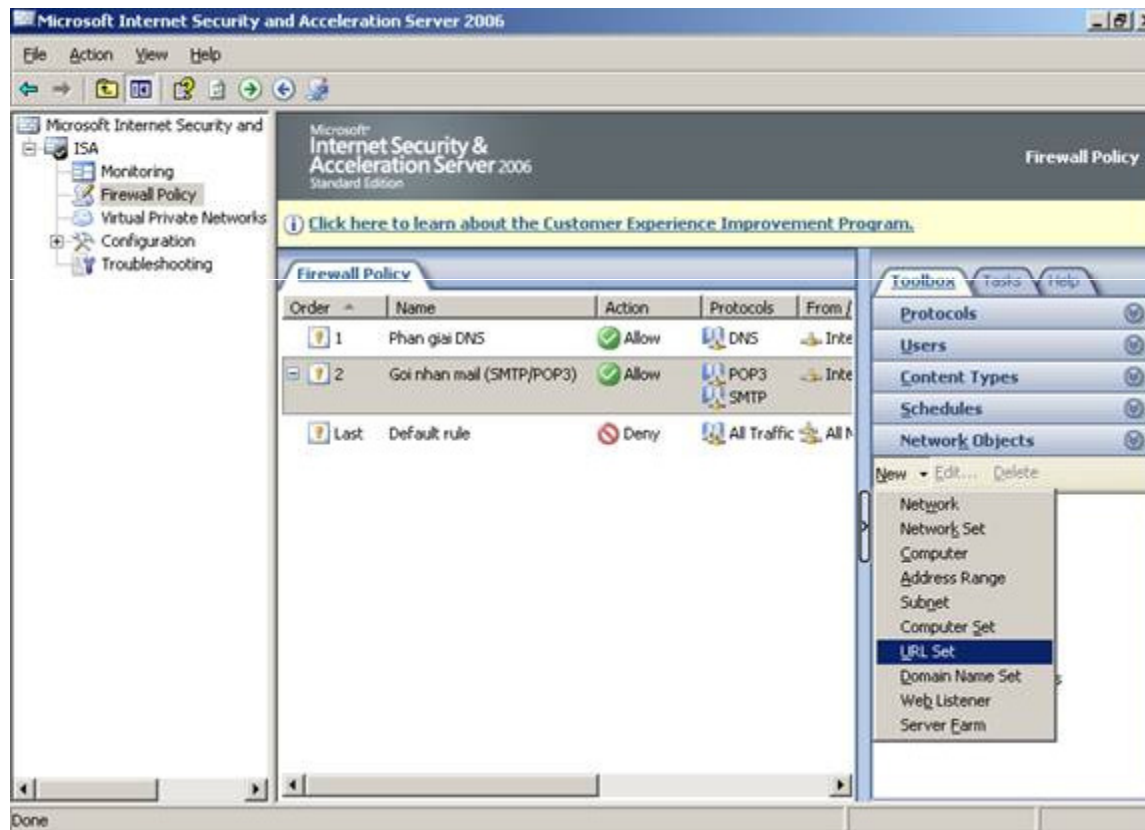
Mô hình máy chủ xác thực (t)

- <http://nhatnghe.com/tailieu/nnlab/bai%20lab%206.htm>



Mô hình máy chủ xác thực (t)

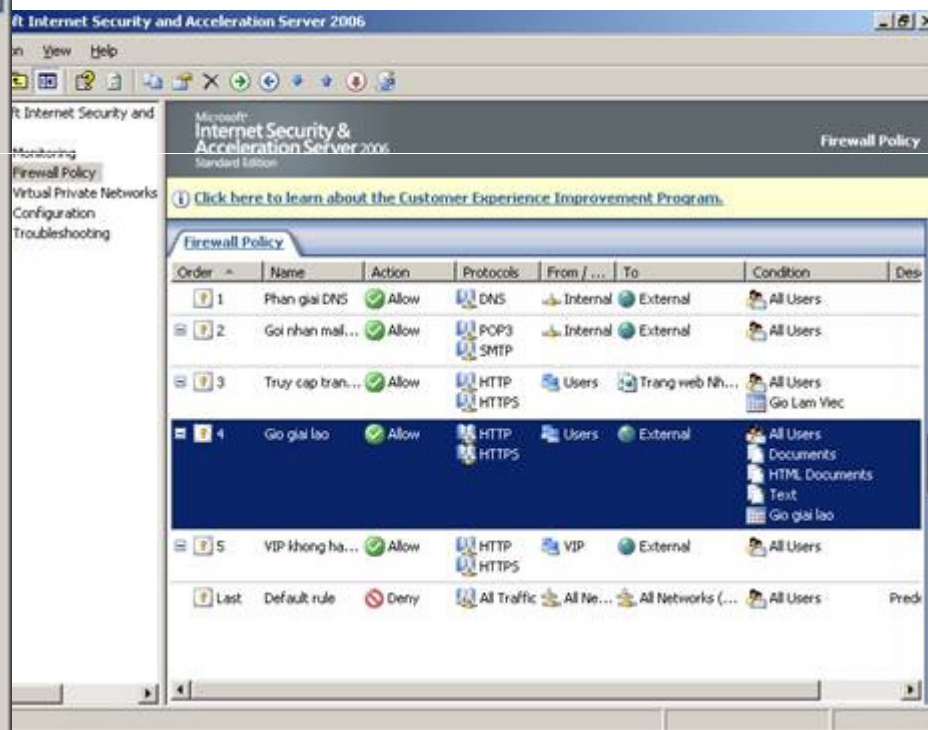
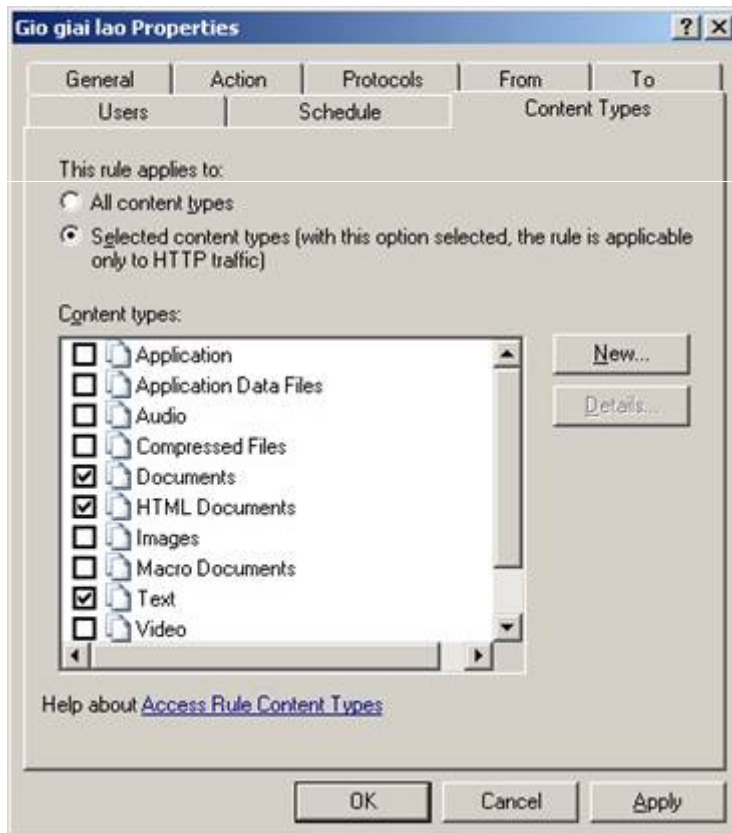
- Thêm quy tắc



Mô hình máy chủ xác thực (t)

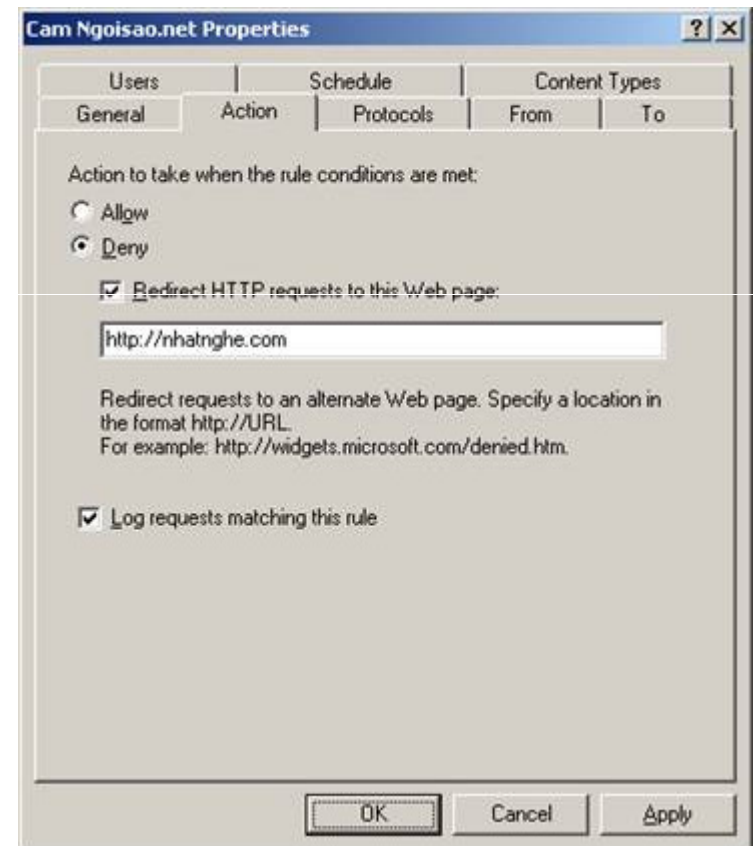
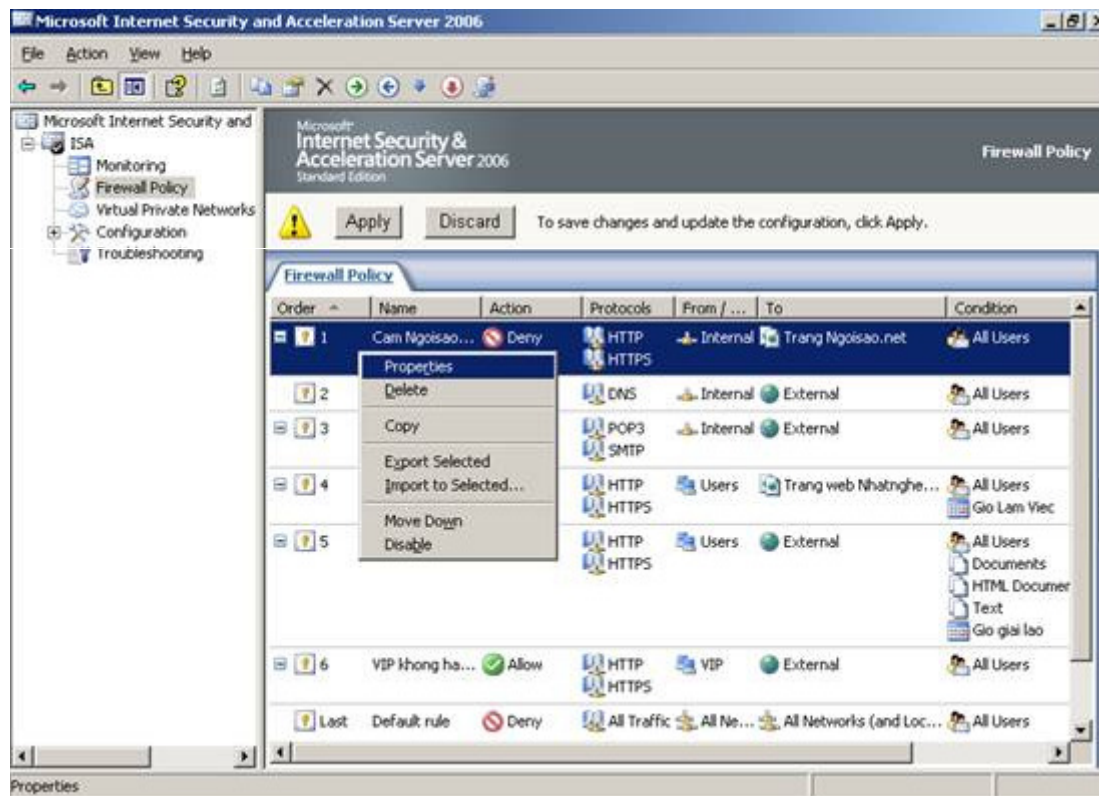


Cấm một số nội dung



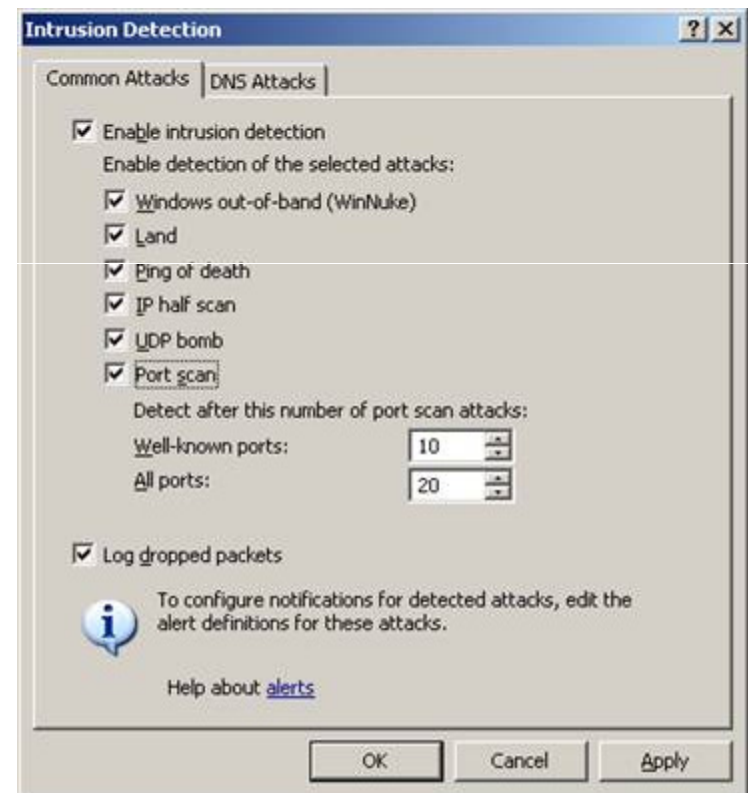
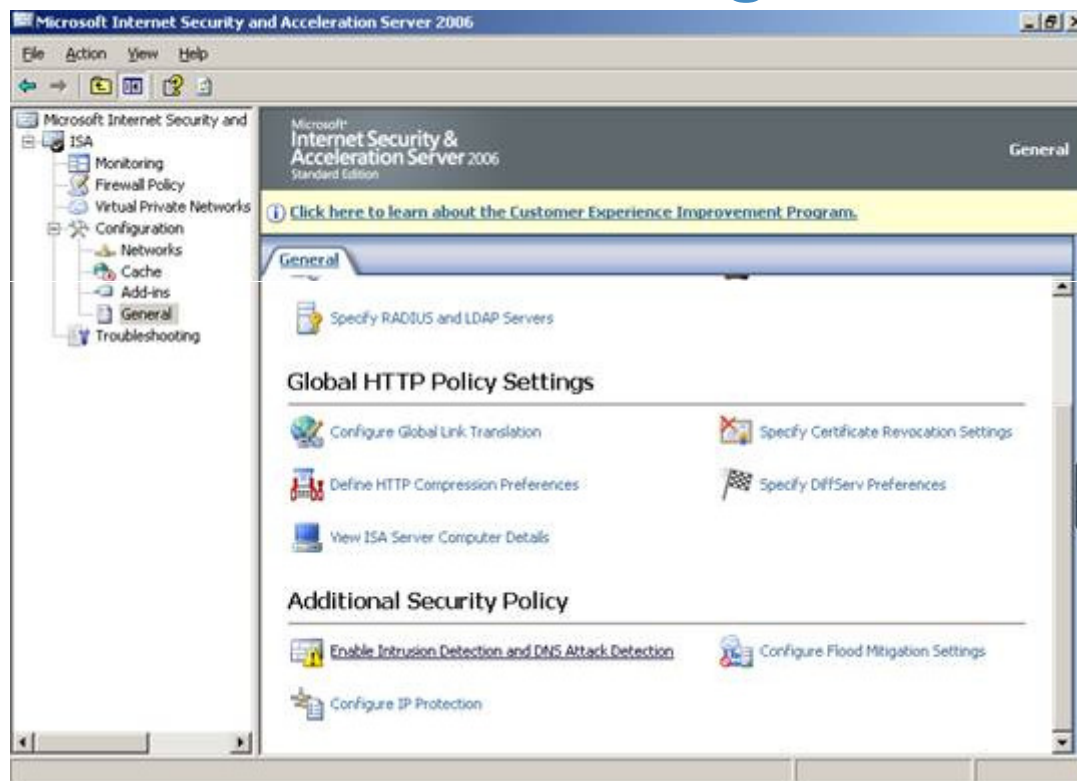
Mô hình máy chủ xác thực (t)

- Chuyển đổi trang



Mô hình máy chủ xác thực (t)

- Phát hiện tấn công



Công cụ phân tích mạng



- Sử dụng các hệ thống log
- Sử dụng các phần mềm phân tích chuyên dụng

Công cụ phân tích mạng (t)



- Hệ thống log: firewall, internet security, proxy, router, ...
 - Phân tích các hoạt động mạng
 - Các máy tính tiến trình
 - Đưa ra nhận định kiểm tra trên hệ thống
- Hệ thống phần mềm
 - Phần mềm bắt gói tin
 - Phân tích lưu lượng hoạt động
 - Tiến trình hoạt động
 - Nội dung hoạt động
 - Định hướng của tấn công

Công cụ phân tích mạng (t)

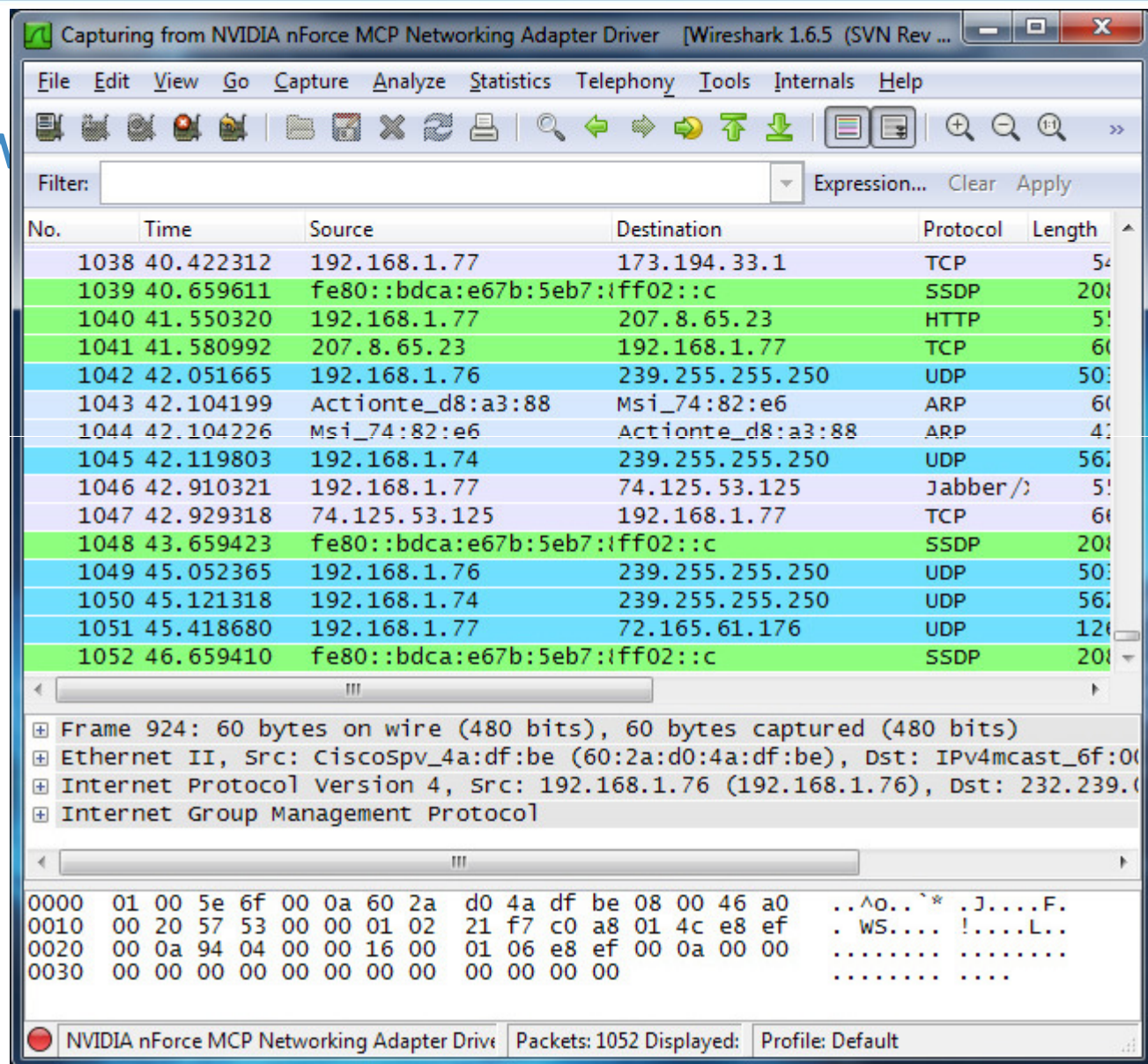


- Phần mềm bắt gói tin
 - wireshark
- Một số phần mềm tấn công mạng
 - Nmap
 - Nessus

Công cụ phân tích mạng (t)



- Hình ảnh w



Sử dụng các quy trình



- Quy tắc về đặt mật khẩu
- Quy tắc về sử dụng mạng
- Quy tắc về sử dụng máy tính
- Quy tắc về ứng xử trong tình huống cố định
 - Nghi ngờ virus
 - Nghi ngờ tấn công
 - Nghi ngờ về mất mát dữ liệu
- Quy tắc về thiết lập thông số hệ thống mạng cho các thành viên quản trị

Trình bày



- Bảo mật mạng máy tính với các thiết bị
- Bảo mật mạng máy tính với các giao thức
- Bảo mật mạng máy tính với các phần mềm
- Một số quy tắc và chú ý