LAB 9. Firewall

I. Yêu cầu:

- Hiểu được khái niệm và vai trò của Firewall.
- Nắm được một số kỹ thuật cấu hình Rule Firewall bằng dòng lệnh trong Windows.
- Biết cách cấu hình chặn ứng dụng bằng Group Policy
- Biết cách sao lưu và phục hồi dữ liệu.

II. Tóm tắt lý thuyết:

- Một số khái niệm Firewall:
  - Inbound rules: các rule kiểm soát truy xuất từ ngoài vào trong
  - Outbound rules: các rule kiểm soát truy xuất từ trong ra ngoài
  - Connection Security rules: các rule bảo mật kết nối giữa các host
  - Monitoring: các rule theo dõi các sự kiện xảy ra
  - Việc thiết lập firewall rule có thể dựa trên ứng dụng cụ thể (program), port xác định (port), giao thức hoặc các dịch vụ hệ điều hành, địa chỉ ip máy gửi hay nhận.
  - Các firewall rule có thể thiết lập để chặn kết nối (block the connection), cho phép kết nối (allow the connection), chỉ cho phép các kết nối đã được chứng thực (allow the connection if it is secure).
  - Có thể chặn việc thi hành các ứng dụng bằng Group Policy (AppLocker).
- **Các lệnh sử dụng**: netsh firewall, netsh advfirewall
- Cấu hình Firewall:

  Cú pháp: netsh firewall [-r RemoteMachine]
  Các tùy chọn:

add	- Thêm cấu hình Firewall.
delete	- Xóa cấu hình Firewall.
set	- cập nhật thiết đặt cấu hình firewall.
show	- hiển thị cấu hình firewall.
dump	- hiển thị script cấu hình

  Cú pháp: netsh advfirewall [options]
  Các tùy chọn:

show	- hiển thị profile hay các thuộc tính tòan cục.
dump	- hiển thị script cấu hình advanced firewall
set	- đặt các chính sách bảo mật toàn cục
reset	- đặt lại chính sách bảo mật thành chính sách mặc định
export	- export chính sách bảo mật hiện hành ra 1 tập tin
import	- import 1 tập tin lưu chính sách bảo mật vào kho chính sách hiện hành
monitor	- chuyển vào chế độ kiểm soát firewall
firewall	- chuyển vào chế độ cấu hình firewall

mainmode - chuyển vào chế độ cấu hình chính advfirewall

Một số lệnh con:

Netsh advfirewall firewall [options]

- add: thêm 1 inbound hay outnound firewall rule
- delete: xóa tất cả các firewall rules phù hợp
- dump: hiển thị script cấu hình
- set: đặt các giá trị thuộc tính mới cho 1 rule đang tồn tại

- Sao lưu và phục hồi dữ liệu: sử dụng tiện ích Windows Server backup trên Widnows Server 2008 hay backup trên Windows XP.

III. Chuẩn bị

- Bài LAB sử dụng 1 máy Windows 7 và 1 máy Windows XP thuộc mạng 192.168.10.0
- Bảo đảm đường truyền đã thông.
- Đổi password của Administrator máy Windows 7 là win7@123
- Đổi password của Administrator máy Windows XP là winxp@123

IV. Triển khai

1. **Cấu hình Firewall** trên máy Windows 7.
   a. Cho phép truy xuất ip từ xa "192.168.0.2":
   ```
   netsh advfirewall firewall set rule name="allow80" new remoteip=192.168.0.2
   ```
   b. Cho phép nhóm "Remote Desktop":
   ```
   netsh advfirewall firewall set rule group="remote desktop" new enable=yes
   ```
   c. Cho phép truy xuất ra bằng giao thức UDP qua các port local:
   ```
   Set rule name="Allow port range" dir=out protocol=udp localport=5000-5020 action=allow
   ```
   d. Thêm 1 rule inbound không đóng gói bảo mật cho tiện ích browser.exe:
   ```
   netsh advfirewall firewall add rule name="allow browser" dir=in program="c:\programfiles\browser\browser.exe" security=authnoencap action=allow
   ```
   e. Thêm 1 rule outbound cho port 80:
   ```
   netsh advfirewall firewall add rule name="allow80" protocol=TCP dir=out localport=80 action=block
   ```
   f. Thêm 1 rule inbound có bảo mật và mã hóa các lưu lượng TCP qua port 80:
   ```
   netsh advfirewall firewall add rule name="Require Encryption for Inbound TCP/80" protocol=TCP dir=in localport=80 security=authdynenc action=allow
   ```
   g. Thêm 1 rule inbound cho trình browser.exe với yêu cầu bảo mật:
   ```
   netsh advfirewall firewall add rule name="allow browser" dir=in program="c:\program files\browser\browser.exe" security=authenticate action=allow
   ```
   h. Thêm 1 rule outbound cho phép giao thức UDP sử dụng các port local 5000-5010:

```
Add rule name="Allow port range" dir=out protocol=udp
localport=5000-5010 action=allow
```

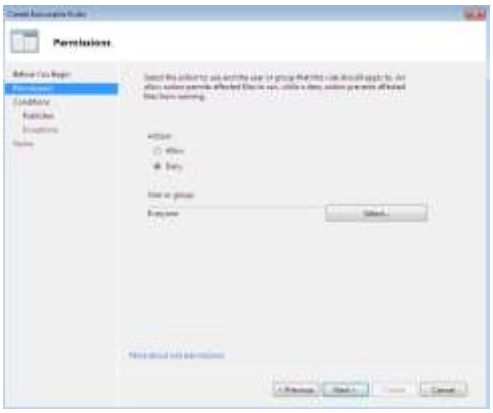
i. Hiển thị tất cả các rule inbound:

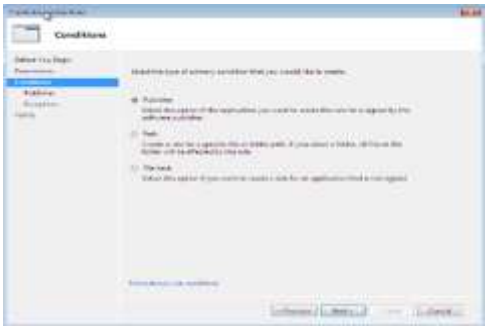
```
netsh advfirewall firewall show rule name=all dir=in
type=dynamic
```

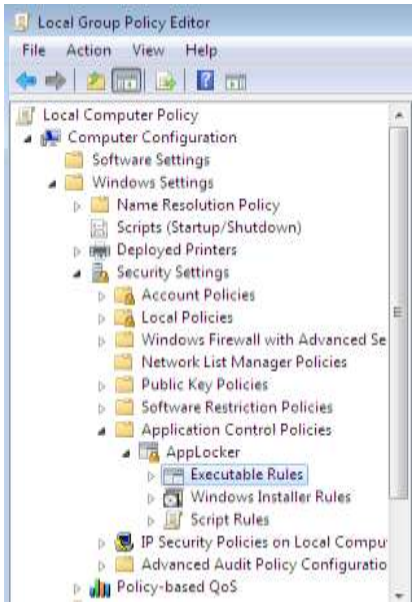
j. Hiển thị tất cả các thiết đặt cho tất cả các rule inbound có tên "allow browser":

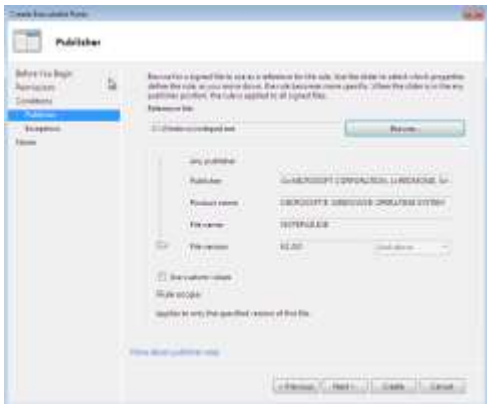
```
netsh advfirewall firewall show rule name="allow browser"
verbose
```

k. Chặn việc thi hành ứng dụng Remote Desktop Connection bằng AppLocker. Gpedit.msc. Click phải executable rules > Create new rule

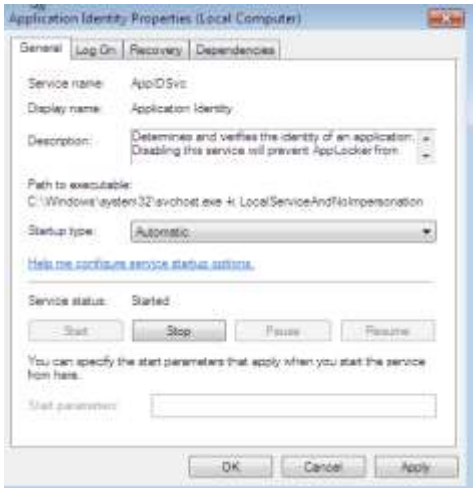








Services.msc



2. **Sao lưu và phục hồi dữ liệu**:
   - Sao lưu thông tin hệ thống
   - Sao lưu dữ liệu trong ổ đĩa D:
   - Phục hồi dữ liệu trên ổ đĩa D:

V. Bài tập. Triển khai lại bài lab trên một máy Windows Server 2008.

a. Cấm người dùng ping vào máy
b. Cấm người dùng sử dụng máy Windows 7 truy cập dịch vụ Web (http)
c. Cấm người dùng sử dụng Yahoo