BẢO VỆ THƯ MỤC DÙNG CHUNG VỚI IPSEC

Giải pháp VLAN (Virtual LAN) thường được triển khai để cách ly các máy tính nối mạng nhưng trong thực tế nhiều đơn vị không có điều kiện trang bị switch hỗ trợ VLAN. Trong trường hợp này, dùng IPSec là giải pháp hữu hiệu để bảo vệ tài nguyên mạng chẳng hạn như

Giải pháp VLAN (Virtual LAN) thường được triển khai để cách ly các máy tính nối mạng nhưng trong thực tế nhiều đơn vị không có điều kiện trang bị switch hỗ trợ VLAN. Trong trường hợp này, dùng IPSec là giải pháp hữu hiệu để bảo vệ tài nguyên mạng chẳng hạn như thư mục dùng chung.Trong mô hình ví dụ có 2 nhóm máy tính, gọi là nhóm 1 và nhóm 2. Ta sẽ thực hiện cấu hình IPSec để chỉ có các máy tính ở trong cùng 1 nhóm có thể truy cập thư mục dùng chung của nhau.Để truy cập thư mục dùng chung, hệ điều hành XP/2000/2003 dùng giao thức TCP port 139 và port 445. Như vậy ta sẽ tạo 1 policy để lọc các cổng này. 1. Tạo mới và cấu hình IP Secutity Policy cho máy tính đầu tiên Bước 1: Chọn Start, Run và gõ MMC, nhấn Enter để mở trình Microsoft Manangement Console.Bước 2: Trong cửa sổ Console, chọn File, rồi chọn Add/Remove Snap-in.Bước 3: Trong hộp thoại mới mở, nhấn Add. Trong hộp thoại Add Stanalone Snap-in ta chọn IP Security Policy Management rồi nhấn Add.

Bước 4: Trong hộp thoại Select Computer or Domain ta chọn Local computer rồi nhấn Finish.

Bước 5: Tiếp theo nhấn Finish -> Close, rồi OK để trở về màn hình của MMCBước 6: Nhấn phải chuột vào mục IP Security Policies on Local Computer và chọn Create IP Security Policy. Nhấn Next để tiếp tục.

Bước 7: Tiếp theo, gõ tên của Policy cần tạo vào ô name, ví dụ "Lọc cổng 445 và 139". Nhấn Next để tiếp tục.

Bước 8: Chọn Activate the default response rule, rồi nhấn Next. Tiếp theo, tại Default Response Rule Authentication Method, bạn chọn Use this string to protect the key exchange (preshared key) và gõ vào "1234". Nhấn Next để tiếp tục.

Bước 9: Chọn Edit properties, rồi nhấn Finish để hoàn tất.

Bước 10: Trong hộp thoại "Lọc cổng 445 và 139", bạn bỏ mục chọn ở phần và nhấn Add. Tiếp tục, bạn chọn Next và chọn This rule does not specify a tunnel. Nhấn Next, chọn All Connection, rồi nhấn Next; bạn chọn Use this string to protect the key exchange (preshared key) và gõ vào "1234". Nhấn Next để tiếp tục.

Bước 11: Trong hộp thoại IP Filter List, bạn chọn Add. Tại mục name, bạn gõ vào tên của danh sách, ví dụ "Cổng 445, 139 ra - vào" (nên đặt tên cho dễ nhớ). Nhấn Add, rồi Next -> Next để tiếp tục.

Bước 12: Trong hộp thoại IP Filter Wizard, bạn gõ mô tả vào ô Description, ví dụ "445 ra". Nhấn Next để tiếp tục.Bước 13: Tại mục IP Traffic Source Address bạn chọn My IP Address. Nhấn Next để tiếp tục.Tại mục IP Traffic Destination Address bạn chọn Any IP Address. Nhấn Next để tiếp

tục.Tại mục Select a protocol type bạn chọn TCP. Nhấn Next để tiếp tục.Tại mục hộp thoại IP Protocol Port bạn chọn To this port và gõ vào giá trị 445.Nhấn Next rồi Finish để hoàn tất.

Bước 14: Lặp lại từ bước 12 đến bước 13 thêm 3 lần nữa với các tham số như sau:- Lần 1:* Descripton : Cổng 445 vào* Source Address : My IP Address* Destination Address: Any IP Address* Protocol Type: TCP* IP Protocol Port: Chọn From this port giá trị 445- Lần 2:* Descripton: Cổng 139 ra* Source Address: My IP Address* Destination Address: Any IP Address* Protocol Type: TCP* IP Protocol Port: Chọn To this port giá trị 139- Lần 3:* Descripton: Cổng 139 vào* Source Address: My IP Address* Destination Address: Any IP Address* Protocol Type: TCP* IP Protocol Port: Chọn From this port giá trị 139Kết thúc ta thu được kết quả như hình. Nhấn OK để tiếp tục.Bước 15: Trong hộp thoại Security Rile Wizard, ta chọn mục Cổng 445, 139 ra - vào. Nhấn Next để tiếp tục.

Bước 16: Tại hộp thoại Filter Action ta chọn mục Require Security. Nhấn Edit để thay đổi tham số của Filter Action.

Bước 17: Trong hộp thoại Require Security Properties, ta chọn mục Use session key perfect forward secrecy (PFS). Nhấn OK để quay trở lại rồi nhấn Next để tiếp tục.

Bước 18: Tiếp theo trong hộp thoại Authentication Method, bạn chọn Use this string to protect the key exchange (preshared key) và gõ vào "1234".Bạn có thể dùng chuỗi khác phức tạp hơn, tuy nhiên phải nhớ rằng các máy tính trong cùng 1 nhóm sẽ có preshared key giống nhau.Tại hộp thoại này còn có 2 mục trên chúng ta không chọn có ý nghĩa như sau:- Active Directory default (Kerberos V5 protocol): Chỉ chọn khi máy tính của bạn là thành viên được đăng nhập vào máy chủ (Windows Server 2000/2003) có cài Active Directory (hay còn gọi tắt là AD). Kerberos V5 là giao thức được mã hóa dữ liệu sử dụng giữa các user nằm trong AD.- Use a certificate from this certification authority (CA): Sử dụng phương thức xác thực dựa trên Certificate Authority (CA). Muốn dùng phương thức này, bạn cần kết nối đến một máy chủ có cài Certificate Service để thực hiện yêu cầu và cài đặt CA dùng cho IPSec.Nhấn Next tiếp tục, rồi Finish để trở về.Bước 19: Trong hộp thoại Edit Rule Properties bạn chọn mục "Cổng 445, 139 ra - vào" và nhấn Apply rồi OK để trở về.Bước 20: Nhấn phải chuột vào mục IP Security Policy vừa tạo (Lọc cổng 445 và 139) và chọn Assign.2. Sao chép IP Security cho máy tiếp theoTa có thể tiến hành 20 bước trên cho máy 2, rồi máy 3. Tuy nhiên, như vậy sẽ rất mất thời gian và có thể xảy ra nhầm lẫn dẫn đến không thể liên lạc được với nhau. Ta dùng công cụ netsh để thực hiện thao tác Export IPsec Policy để xuất policy ra 1 file, sau đó nhập (Import) file này vào máy tính khác. Cách thực hiện như sau:Bước 1: Chuẩn bịChọn Start, Run và gõ cmd và ấn Enter. Tại dấu nhắc của DOS ta gõ lệnh sau để tạo ra thư mục Ipsec ở ổ đĩa C:md C:\Ipsec Bước 2: Xuất IPSec policy ra file có tên Loc445va139.ipsec Gõ lệnh sau:netsh ipsec static exportpolicy file = c:\Ipsec\Loc445va139 (phần mở rộng ipsec do netsh tự thêm vào)Bước 3: Nhập IPSec Policy từ file Loc445va139.ipsec Chép file Loc445va139.ipsec vào thư mục C:\IPsec ở máy 2 và gõ lệnh sau:netsh ipsec static importpolicy file = c:\Ipsec\Loc445va139.ipsecTại máy 2, tiếp tục các bước từ 1 đến 5 ở mục 1, để có được màn hình quản lý IP Security Management. Nhấn phải chuột vào mục IP Security Policy (Lọc cổng 445 và 139) và chọn Assign.Tiếp tục bước 3 với máy 3.3. Thực hiện với nhóm 2Đối với máy 4, 5 trong nhóm 2, ta tiến hành tương tự với nhóm 1 như đã trình bày ở trên. Tuy nhiên giá trị

preshared key phải khác là giá trị của nhóm 1. Nguyễn Đắc TiếnEmail: tiennd@yahoo.com