

CÀI ĐẶT VÀ CẤU HÌNH ISA SERVER FIREWALL 2004 - CHƯƠNG 2 CÀI ĐẶT CERTIFICATE SERVICES

Microsoft Certificate Services có thể được cài đặt trên Domain controller của internal Network và cung cấp các Certificates cho các Hosts trong Internal Network domain, cũng như các Hosts không là thành viên của Internal Network domain. Chúng ta sẽ sử dụng Certificates

Microsoft Certificate Services có thể được cài đặt trên Domain controller của internal Network và cung cấp các Certificates cho các Hosts trong Internal Network domain, cũng như các Hosts không là thành viên của Internal Network domain. Chúng ta sẽ sử dụng Certificates trong nhiều kịch bản khác nhau, các công việc cần hoàn thành:

- Cho phép ISA Server 2004 Firewall cung cấp kênh để hỗ trợ L2TP/IPSec VPN protocol, tạo liên kết site-to-site VPN.
- Cho phép ISA Server 2004 Firewall cung cấp kênh để hỗ trợ L2TP/IPSec VPN protocol, tạo điều kiện cho VPN client thực hiện kết nối từ một Remote Location (site)
- Cho phép remote users có thể truy cập đến Outlook Web Access site, phương thức bảo mật mạnh SSL-to- SSL bridged connections.
- Publish secure Exchange SMTP và POP3 services lên Internet Certificates cho phép dùng SSL/TLS security. SSL (Secure Sockets Layer) protocol, là một giao thức lớp session (layer) có khả năng mã hóa dữ liệu truyền giữa client và server.

SSL security hiện được xem là chuẩn cung cấp an toàn cho các remote access đến các Websites. Ngoài ra, certificates còn có thể được dùng để xác nhận các đối tượng tham gia các kết nối VPN , bao gồm VPN clients và VPN servers (phương pháp này gọi là xác thực cả hai chiều- mutual Authentication)

Trong phần này chúng ta sẽ đề cập đến các tiến trình sau:

- Cài đặt Internet Information Services 6.0 để hỗ trợ Certificate Authority's Web

Enrollment (nhận các Certificates từ CA server thông qua hình thức đăng kí trên CA'sWeb)

- Cài đặt Microsoft Certificate Services ở chế độ

Enterprise CA

Cài đặt Internet Information Services 6.0

Certificate Authority's Web enrollment site sử dụng Internet Information Services World

Wide Publishing Service. Bởi vì chúng ta đã cài IIS Web services , trong chương 1 khi tiến hành cài Exchange 2003 hỗ trợ Outlook Web Access site, nên sẽ không cần cài lại IIS service. Tuy nhiên, bạn nên xác nhận lại WWW Publishing Service đã được Enabled, trước khi tiến hành cài

Enterprise CA.

Thực hiện các bước sau để xác nhận WWW Publishing Service đang chạy trên domain controller:

1. Click Start chọn Administrative Tools. Click Services
2. Trong Services console, click Standard tab phía dưới. Kéo xuống danh sách và double-click vào World Wide Web Publishing Service .
3. Trong World Wide Web Publishing Server Properties dialog box, xác nhận Startup type là Automatic, và trạng thái vận hành của service là Started.

4. Click Cancel và đóng Services console.

Như vậy WWW Publishing Service đã vận hành, bước tiếp theo là cài đặt

Enterprise CA software.

Cài đặt Certificate Services ở chế độ Enterprise CA

Microsoft Certificate Services sẽ được cài đặt ở chế độ này trên chính domain controller. Có những thuận lợi khi cài CA ở chế độ

Enterprise mode (ngược lại với Standalone mode) bao gồm:

- Chứng từ gốc của CA (root CA certificate) được tự động đưa vào vùng lưu trữ Certificate của Trusted Root Certification Authorities (certificate store) trên tất cả các máy thành viên của Domain (domain member). Các Computer thành viên của Domain khi dùng các giao dịch cần Certificates để nâng cao tính an toàn, có thể dễ dàng tìm các nhà cung cấp hợp pháp- CA servers, trong Trusted Root Certification Authorities trên Computer của mình.

- Các Clients này cũng dễ dàng dùng Certificates MMC snap-in (tại RUN, type mmc, chọn File, Add/Remove snap-in, Add, chọn Certificates), và dễ dàng dùng snap-in này để yêu cầu certificates từ CA Servers hoặc từ CA's Websites

- Tất cả các Computer trong Domain có thể được phân chia Certificates đồng loạt thông qua tính năng Active Directory autoenrollment feature

Lưu ý rằng không nhất thiết phải cài CA ở

Enterprise mode. Bạn có thể cài CA ở chế độ Standalone mode, nhưng trong Lab này chúng ta sẽ không đề cập standalone mode hoặc làm thế nào để xin cấp certificate từ một

Standalone CA

Tiến hành các bước sau để cài đặt

Enterprise CA trên Domain Controller EXCHANGE2003BE

1. Click Start, Control Panel. Click Add or Remove Programs.

2. Trong Add or Remove Programs, click Add/Remove Windows Components

3. Trên Windows Components page, kéo danh sách xuống và check vào Certificate Services checkbox. Click Yes trong Microsoft Certificate Services dialog box, thông báo rằng informing "you may not change the name of the machine or the machine's domain membership while it is acting as a CA". Như vậy là rất rõ ràng Bạn không thể thay đổi Computer Name hoặc thay đổi tư cách thành viên Domain của Computer này, sau khi đã cài CA service. Click Yes.

4. Click Next trên Windows Components page.

5. Trên CA Type page, chọn

Enterprise root CA option và click Next.

6. Trên CA Identifying Information page, điền tên cho CA server này trong Common name của CA text box. Nên dùng tên dạng DNS host name của domain controller. Tham khảo về cấu hình DNS hỗ trợ ISA Server

<http://www.tacteam.net/isaserverorg/isabokit/9dnssupport/9dnssupport.htm>

Trong text box này các bạn điền vào NetBIOS name của domain controller là EXCHANGE2003BE. Click

Next.

7. Nếu Computer này trước đây đã cài đặt một CA, bạn sẽ được hỏi "you wish to overwrite the existing key", ghi đè lên các khóa đã tồn tại. Còn nếu bạn đã triển khai các CA khác trên Network có thể không nên overwrite các khóa hiện tại. Và nếu đây là CA đầu tiên, có thể chấp nhận overwrite the existing key. Trong ví dụ này chúng ta trước đó đã chưa cài CA trên Computer vì vậy không nhìn thấy dialog box thông báo như trên

8. Trong Certificate Database Settings page, dùng vị trí lưu trữ mặc định cho Certificate Database và Certificate database log text boxes. Click Next.

9. Click Yes trong Microsoft Certificate Services dialog box, bạn nhận được thông báo phải restart Internet

Information Services. Click Yes để stop service. Service sẽ được restart automatic.

10. Click OK trong Insert Disk dialog box. Trong Files Needed dialog box, đưa đường dẫn đến I386 folder trong Copy file from text box và click OK.

11. Click Finish trên Completing the Windows Components Wizard page.

12. Đóng Add or Remove Programs.

Tại thời điểm này

Enterprise CA có thể cấp phát certificates cho các Computer khác trong Domain thông qua autoenrollment, Certificates mmc snap-in, hoặc qua Web enrollment site. Trong hướng dẫn cấu hình ISA Server 2004

này, chúng ta sẽ cấp phát một Web site certificate cho OWA Web site và cũng cấp phát các Computer certificates cho ISA Server 2004 Firewall computer và cho các external VPN

client và VPN gateway (VPN router) machine.

Kết luận:

Trong phần này chúng ta đã thảo luận về việc dùng một CA- Certificate Authority và làm thế nào để cài đặt một

Enterprise CA trên Domain controller trong internal Network. Và tiếp theo chúng ta sẽ dùng Enterprise CA để cấp Computer Certificates cho các VPN clients và servers, cũng cấp luôn một Web site certificate cho Exchange Server's Outlook Web Access Web site.

(Mời các bạn đón đọc chương 3)

Đã phát hành: Cài đặt và cấu hình ISA Server Firewall 2004 - Chương 1

Ho Viet Ha - Owner Network Information Security Vietnam, Inc. <http://nis.com.vn>

Email: networksecurity@Nis.com.vn