CÀI ĐẶT VÀ CẤU HÌNH ISA SERVER FIREWALL 2004 - CHƯƠNG 1

Trong thực tế hiện nay bảo mật thông tin đang đóng một vai trò thiết yếu chứ không còn là "thứ yếu" trong mọi hoạt động liên quan đến việc ứng dụng công nghệ thông tin. Tôi muốn nói đến vai trò to lớn của việc ứng dụng CNTT đã và đang diễn ra s&o

Trong thực tế hiện nay bảo mật thông tin đang đóng một vai trò thiết yếu chứ không còn là "thứ yếu" trong mọi hoạt động liên quan đến việc ứng dụng công nghệ thông tin. Tôi muốn nói đến vai trò to lớn của việc ứng dụng CNTT đã và đang diễn ra sôi động, không chỉ thuần túy là những công cụ (Hardware, software), mà thực sự đã được xem như là giải pháp cho nhiều vấn đề. Khởi động từ những năm đầu thập niên 90, với một số ít chuyên gia về CNTT, những hiểu biết còn hạn chế và đưa CNTT ứng dụng trong các hoạt động sản xuất, giao dịch, quản lý còn khá khiêm tốn và chỉ dừng lại ở mức công cụ, và đôi khi tôi còn nhận thấy những công cụ "đắt tiền" này còn gây một số cản trở, không đem lại những hiệu quả thiết thực cho những Tổ chức sử dụng nó.

Và những ai "chộn rộn" nhất thì lại tự hỏi mình "mua cái thiết bị để làm gì nhĩ ?! nó không sản xuất ra được sản phẩm, và nó cũng chẳng giúp công việc giấy tờ giảm bớt là bao, liệu chúng ta đã tổn hao một số tiền vô ích?!.."" . Không đâu xa những nước láng giềng khu vực như

Thailand,

Singapore, những nền kinh tế mạnh trong khu vực và đang trên đà phát triển mạnh mẽ. Nhận thức được sự ưu việt của ứng dụng CNTT, và từ rất sớm họ đã đem CNNT áp dụng vào mọi hoạt động, không chỉ sản xuất, giao dịch, quản lý mà CNTT được mang đến mọi nhà, mọi người

. Và họ cũng học thành thục những kĩ năng để giải quyết và điều khiển công việc rất sáng tạo từ các "vũ khí" tân thời này. Đâu đó trong trích đoạn "Con đường Phía trước" của Bill Gates có nói đến giá trị to lớn của thông tin trong thế kỉ 21, một kỉ nguyên thông tin đích thực. Thực thể quý giá "phi vật chất" này, đang dần trở thành một đối tượng được săn lùng, được kiểm soát gắt gao, và cũng là bệ phóng cho tất cả những quốc gia muốn phát triển một cách mạnh mẽ, nhanh chóng và "bền vững". Cần có những hệ thống mạnh mẽ nhất để kiểm soát thông tin, sáng tạo thông tin và đem những thông tin này vào ứng dụng một cách có hiệu quả. Thế giới bước trong thế kĩ 21 dùng bàn đạp CNTT để tạo lực bẩy và cũng là để dẫn đường cho các hoạt động, cho mọi người xích lại gần nhau hơn, khiến cho những cách biệt Địa Lý không còn tồn tại, dễ dàng hiểu nhau hơn và trao đổi với nhau những gì có giá trị nhất, đặc biệt nhất.

Ứng dụng công nghệ thông tin một cách có hiệu quả và "bền vững", là tiêu chí hàng đầu của nhiều quốc gia hiện nay, Việt Nam không là ngoại lệ. Xét trên bình diện một doanh nghiệp khi ứng dụng CNTT vào sản xuất, kinh doanh cũng luôn mong muốn có được điều này. Tính hiệu quả là điều bắt buộc, và sự "bền vững" cũng là tất yếu. Dưới góc nhìn của một chuyên gia về bảo mật hệ thống, khi triển khai một hệ thống thông tin và xây dựng được cơ chế bảo vệ chặt chẽ, an toàn, như vậy là góp phần duy trì tính "bền vững" cho hệ thống thông tin của doanh nghiệp đó. Và tất cả chúng ta đều hiểu rằng giá trị thông tin của doanh nghiệp là tài sản vô giá. Không chỉ thuần túy về vật chất, những giá trị khác không thể đo đếm được như uy tín của họ với khách hàng sẽ ra sao, nếu những thông tin giao dịch với khách hàng bị đánh cắp, rồi sau đó bị lợi dụng với những mục đích khác nhau..Hacker, attacker, virus, worm, phishing, những khái niệm này giờ đây không còn xa lạ, và thực sự là mối lo ngại hàng đầu của tất cả các hệ thống thông tin (PCs, Enterprise

Networks, Internet, etc..). Và chính vì vậy, tất cả những hệ thống này cần trang bị những công cụ đủ mạnh, am hiểu cách xử lý để đối phó với những thế lực đen đáng sợ đó. Ai tạo ra bức tường lửa đủ mạnh này để có thể "thiêu cháy" mọi ý đồ xâm nhập?! Xin thưa rằng trước hết đó là ý thức sử dụng máy tính an toàn của tất cả mọi nhân viên trong một Tổ chức, sự am hiểu tinh tường của các Security Admin trong Tổ chức đó, và cuối cùng là những công cụ đắc lực nhất phục vụ cho "cuộc chiến" này. Đó là các Firewall, từ Personal Firewall bảo vệ cho từng Computer cho đến các Enterprise Firewall có khả năng bảo vệ toàn hệ thống Network của một Tổ chức. Và Microsoft ISA Server 2004 là một Enterprise Firewall như thế ! Một sản phẩm tốt và là người bạn tin cậy để bảo vệ an toàn cho các hệ thống thông tin.

CHƯƠNG 1: Triển khai hạ tầng Network với những Service thiết yếu

Cuốn sách được trình bày theo thực tế triển khai ISA Server 2004 trong mô hình Network của một Tổ chức. Nội dung của sách gói gọn trong các vấn đề cấu hình hệ thống ISA Server 2004 trở thành một Firewall mạnh mà vẫn đáp ứng được các yêu cầu sử dụng các Service từ xa, phục vụ cho cả các ISA Clients bên trong truy cập các Service bên ngoài (Internet), lẫn các Client bên ngoài (Internet Clients) cần truy cập các Service bên trong Network Tổ chức.

Firewalls luôn là một trong các loại thiết bị Network cấu hình phức tạp nhất và duy trì hoạt động của nó để bảo vệ Network cũng gặp không ít thử thách cho các Security Admin. Cần có những kiến thức cơ bản về TCP/IP và các Network Services để hiểu rõ một Firewall làm việc như thế nào. Tuy nhiên cũng không nhất thiết phải trở thành một chuyên gia về hạ tầng Network (Network Infrastructure) mới có thể sử dụng được ISA Server 2004 như một Network Firewall.

Chương này sẽ mô tả các vấn đề sau:

• Giúp bạn hiểu các tính năng có mặt trên ISA Server 2004 • Cung cấp những lời khuyên cụ thể khi dùng tài liệu để cấu hình ISA Server 2004 Firewall • Mô tả chi tiết thực hành triển khai (ISA SERVER 2004 Lab Configuration)

Hiểu các tính năng trên ISA Server 2004

ISA Server 2004 được thiết kế để bảo vệ Network, chống các xâm nhập từ bên ngoài lẫn kiểm soát các truy cập từ bên trong Nội bộ Network của một Tổ chức. ISA Server 2004 Firewall làm điều này thông qua cơ chế điều khiển những gì có thể được phép qua Firewall và những gì sẽ bị ngăn chặn. Chúng ta hình dung đơn giản như sau: Có một quy tắc được áp đặt trên Firewall cho phép thông tin được truyền qua Firewall, sau đó những thông tin này sẽ được "Pass" qua, và ngược lại nếu không có bất kì quy tắc nào cho phép những thông tin ấy truyền qua, những thông tin này sẽ bị Firewall chặn lại.

ISA Server 2004 Firewall chứa nhiều tính năng mà các Security Admin có thể dùng để đảm bảo an toàn cho việc truy cập Internet, và cũng bảo đảm an ninh cho các tài nguyên trong Nội bộ Network . Cuốn sách cung cấp cho các Security Admin hiểu được những khái niệm tổng quát và dùng những tính năng phổ biến, đặc thù nhất trên ISA Server 2004, thông qua những bước hướng dẫn cụ thể (Steps by Steps)

Firewalls không làm việc trong một môi trường "chân không", vì đơn giản là chúng ta triển khai Firewall để bảo vệ một cái gì đó, có thể là một PC, một Server hay cả một hệ thống Network với nhiều Service được triển khai như Web, Mail, Database….

Chúng ta sẽ có một hướng dẫn đầy đủ về việc triển khai các Service cần thiết cho hoạt động Network của một Tổ chức. cách thức cài đặt và cấu hình những Service này như thế nào. Và điều tối quan trọng là Network và các Service phải được cấu hình đúng cách trước khi triển khai Firewall. Điều này giúp chúng ta tránh được những vấn đề phiền toái nảy sinh khi triển khai ISA Server 2004.

Các Network Services và những tính năng trên ISA Server 2004 sẽ được cài đặt và cấu hình gồm:

• Cài đặt và cấu hình Microsoft Certificate Services (Service cung cấp các Chứng từ kĩ thuật số phục vụ nhận dạng an toàn khi giao dịch trên Network) • Cài đặt và cấu hình Microsoft Internet Authentication Services (RADIUS) Service xác thực an toàn cho các truy cập từ xa thông qua các remote connections (Dial-up hoặc VPN) • Cài đặt và cấu hình Microsoft DHCP Services (Service cung cấp các xác lập TCP/IP cho các node trên Network) và WINS Services (Service cung cấp giải pháp truy vấn NETBIOS name của các Computer trên Network) • Cấu hình các WPAD entries trong DNS để hỗ trợ chức năng Autodiscovery (tự động khám phá)) và Autoconfiguration (tự động cấu hình) cho Web Proxy và Firewall clients. Rất thuận lợi cho các ISA Clients (Web và Firewall clients) trong một Tổ chức khi họ phải mang Computer từ một Network (có một ISA Server) đến

Network khác (có ISA Server khác) mà vẫn tự động phát hiện và làm việc được với Web Proxy Service và Firewall Service trên ISA Server này . • Cài đặt Microsoft DNS server trên Perimeter Network server (Network chứa các Server cung cấp trực tuyến cho các Clients bên ngoài, nằm sau Firewall, nhưng cũng tách biệt với LAN)• Cài đặt ISA Server 2004 Firewall software • Back up và phục hồi thông tin cấu hình của ISA Server 2004 Firewall • Dùng các mô hình mẫu của ISA Server 2004 (ISA Server 2004 Network Templates) để cấu hình Firewall • Cấu hình các loại ISA Server 2004 clients • Tạo các chính sách truy cập (Access Policy) trên ISA Server 2004 Firewall • Publish Web Server trên một Perimeter Network • Dùng ISA Server 2004 Firewall đóng vai trò một Spam filtering SMTP relay (trạm trung chuyển e-mails, có chức năng ngăn chặn Spam mails) • Publish Microsoft Exchange Server services (hệ thống Mail và làm việc cộng tác của Microsoft, tương tự Lotus Notes của IBM) • Cấu hình ISA Server 2004 Firewall đóng vai trò một VPN server• Tạo kết nối VPN theo kiểu site to site giữa hai Networks

Trước khi thực hành cấu hình ISA Server 2004 Firewall, phải nhận thức rõ ràng : Đây là một hệ thống ngăn chặn các cuộc tấn công từ Internet và một Firewall với cấu hình lỗi sẽ tạo điều kiện cho các cuộc xâm nhập Network. Với những lý do này, điều quan trọng nhất các Security Admin quan tâm đó là Làm thế nào để cấu hình Firewall đảm bảo an toàn cho việc truy cập Internet .

Với cấu hình mặc định của mình ISA Server 2004 ngăn chặn tất cả lưu thông vào, ra qua Firewall.

Rõ ràng đây là một cấu hình chủ động, an toàn nhất mà Admin có thể yên tâm ngay từ đầu khi vận hành ISA Server. Và sau đó để đáp ứng các yếu cầu hợp pháp truy cập các Service khác nhau của Internet (ví dụ như web, mail, chat, download, game online v.vv..), Security Admin sẽ cấu hình để ISA Server 2004 có thể đáp ứng các yêu cầu được phép trên.

Các Securty Admin luôn được khuyến cáo: Hãy tạo các cuộc kiểm tra cấu hình ISA Server 2004 trong phòng Lab, trước khi đem các cấu hình này áp dụng thực tế. Chúng ta sẽ được hướng dẫn cấu hình ISA Server 2004 Firewall đúng cách, chính xác thông qua giao diện làm việc rất gần gũi của ISA Server 2004. Có thể có những sai lầm khi thực hiện Lab, nhưng các Admin không qua lo lắng vì chắc rằng các attackers không thể lợi dụng những lỗ hỗng này (trừ khi Lab Network được kết nối với Internet..). Trên Lab điều quan trọng nhất là hiểu đúng các thông số đã cấu hình, cho phép sai phạm và các Admin rút ra kinh ghiệm từ chính những “mistakes” này.

LAB hướng dẫn cấu hình ISA Server 2004 Firewall

Chúng ta sẽ dùng một Network Lab để mô tả những khả năng và những nét đặc trưng của ISA Server 2004. Các Admin khi thực hành nên xây dựng một Test Lab tương tự như mô hình chỉ ra dưới đây (tất cả các thông số sử dụng). Nếu các Security Admin không có đủ các thiết bị thật như Test Lab này, có thể dùng mô hình giả lập, đến từ các Virtual Software như

Microsoft’s Virtual PC software (hoặc VMWare) để tạo mô hình Lab ảo.

Xem thêm về Virtual PC tại Website: http://www.microsoft.com/windowsxp/virtualpc/

Trong phần này, chúng ta sẽ xem xét:

• Hướng dẫn cấu hình Network cho ISA Server 2004 • Cài đặt Windows Server 2003 , và sau đó nâng (dcpromo) Computer này lên thành một Domain controller (máy chủ kiểm soát toàn hoạt động của Domain) • Cài đặt Exchange Server 2003 trên Domain controller này và cấu hình thành một Outlook

Web Access Site dùng phương thức xác thực cơ bản (Basic authentication)

Sơ đồ Network triển khai ISA Server 2004

Mô hình Network Lab – 7Computers.

Tuy nhiên Network Lab không yêu cầu cả 7 Computers này chạy cùng một thời điểm

Điều này tạo điều kiện dễ dàng cho Lab đặc biệt là Lab ảo.

Mô hình Network của Tổ chức này có một Local Network (Network cục bộ LAN) và một Remote Network. Mỗi Network có một ISA Server 2004 chắn phía trước đóng vai trò Firewall. Tất cả các Computers trên Local Network đều là thành viên của Domain MSFirewall.org, và domain này bao gồm luôn cả ISA Server 2004 Firewall computer. Tất cả các Computers còn lại không là thành viên của Domain này.

Trên lab Network, Network Card ngoài (External interfaces) của các ISA Server 2004 Firewalls có kết nối cho phép truy cập Internet. Các Admin nên tạo các thông số cấu hình giống nhau để có thể Test các kết nối thực sự đến Internet từ phía Clients nằm sau ISA Server 2004 Firewalls.

Nếu chúng ta dùng phần mềm giả lập thì lưu ý rằng, chúng ta phải set-up đến 3 Virtual Networks trên Test Lab. Đó là các Vitual Networks: Domain Controller nằm trên Internal Network, TRIHOMELAN1 Computer nằm trên Perimeter Network và REMOTECLIENT virtual Network thứ ba.

Lưu ý với Lab ảo: Chắc chắn một điều là trên các Virtual Networks này bố trí các Computers trên các Virtual Switches khác nhau, để ngăn chặn các thông tin tràn ngập theo kiểu Ethernet broadcast traffic, điều này có thể gây nên những kết quả không mong muốn trên Lab ảo..

Cài đặt và cấu hình Domain Controller trên Internal Network
Một Computer khác hơn so với ISA Server 2004 Firewall computer, có quyền lực quản trị toàn Domain nội bộ đó là Domain Controller . Microsoft xây dựng mô hình Domain dưới sự kiểm soát của Active Directory Service và Domain Controller là công cụ kiểm soát Domain đó. (quản lý tất cả các Clients và Servers cung cấp Service trong Domain như Web, Mail, Database server và kể cảISA Servers)

Trong Lab này chúng ta sẽ cấu hình một Windows Server 2003 domain controller, và triển khai luôn các Service như: DNS, WINS, DHCP, RADIUS, Microsoft Exchange Server 2003 trên chính Domain controller này.

Các giai đoạn tiến hành:

• Cài đặt Windows Server 2003 • Cài đặt và cấu hình DNS service • Nâng Computer này lên thành Domain controller

Cài đặt Windows Server 2003

Tiến hành các bước sau trên Computer sẽ đóng vai trò Domain Controller

1. Đưa đĩa CD cài đặt vào CD-ROM, khởi dộng lại Computer. Cho phép boot từ CD 2. Chương trình Windows setup bắt đầu load những Files phục vụ cho việc cài đặt. Nhấn Enter khi mà hình Welcome to Setup xuất hiện 3. Đọc những điều khoản về License trên Windows Licensing Agreement , dùng phím PAGE DOWN để xem hết sau đó nhấn F8 để đồng ý với điều khoản 4. Trên Windows Server 2003, Standard Edition Setup xuất hiện màn hình tạo các phân vùng lôgic (Partition) trên đĩa cứng, trước hết tạo Partition dùng cho việc cài đặt Hệ Điều hành. Trong Test Lab này, toàn bộ đĩa cứng sẽ chỉ làm một Partition. Nhấn ENTER. 5. Trên Windows Server 2003, Standard Edition Setup, chọn Format the partition using the NTFS file system Nhấn ENTER. 6. Chương trình Windows Setup tiến hành định dạng (format) đĩa cứng, sẽ chờ ít phút cho tiến trình này hoàn thành 7. Computer sẽ tự Restart khi tiến trình copy File vào đĩa cứng hoàn thành8. Computer sẽ restart lại trong giao diện đồ họa (graphic interface mode). Click Next trên trang Regional and Language Options 9. Trên trang Personalize Your Software, điền Tên và Tổ chức của Bạn Ví dụ : Name: Nis.com.vn
Organization: Network Information Security Vietnam
10. Trên trang Product Key điền vào 25 chữ số của Product Key mà bạn có và click Next. 11. Trên trang Licensing Modes chọn đúng option được áp dụng cho version Windows Server 2003 mà bạn cài đặt. Nếu cài đặt Licence ở chế độ per server licensing, hãy đưa vào số connections mà bạn đã có License. Click Next.

12. Trên trang Computer Name và Administrator Password điền tên của Computer trong Computer

Name text box. Theo các bước trong xây dựng Test Lab này, thì Domain controller/Exchange Server trên cùng Server và có tên là EXCHANGE2003BE, tên này được điền vào Computer Name text box. Điền tiếp vào mục Administrator password và xác nhận lại password tại mục Confirm password (ghi nhớ lại password administrator cẩn thận, nếu không thì bạn cũng không thể log-on vào Server cho các hoạt động tiếp theo). Click Next. 13. Trên trang Date and Time Settings xác lập chính xác Ngày, giờ và múi giờ Việt

Nam (nếu các bạn ở Việt

Nam). Click Next. 14. Trên trang Networking Settings, chọn Custom settings option. 15. Trên trang Network Components, chọn Internet Protocol (TCP/IP) entry trong Components và click Properties. 16. Trong Internet Protocol (TCP/IP) Properties dialog box, xác lập các thông số sau: IP address: 10.0.0.2. Subnet mask: 255.255.255.0. Default gateway: 10.0.0.1 (chú ý Default Gateway 10.0.0.1 này cũng là IP address của Internal Card trênISA Server). Preferred DNS server: 10.0.0.2.

17. Click Advanced trên Internet Protocol (TCP/IP) Properties dialog box. Trong Advanced TCP/IP Settings dialog box, click WINS tab. Trên WINS tab, click Add. Trong TCP/IP WINS Server dialog box, điền 10.0.0.2 và click Add. 18. Click OK trong Advanced TCP/IP Settings dialog box. 19. Click OK trong Internet Protocol (TCP/IP) Properties dialog box. 20. Click Next trên trang Networking Components. 21. Chấp nhận lựa chọn mặc định môi trường Network là Workgroup (chúng ta sẽ tạo môi trường Domain sau, đưa máy này trở thành một Domain controller và cũng là thành viên của Domain (là một member server, vì trên Server này còn cài thêm nhiều Server Service khác ngoài Active Directory Service).Click Next. 22. Tiến trình cài đặt được tiếp tục và khi Finish, Computer sẽ tự khởi động lại 23. Log-on lần đầu tiên vào Windows Server 2003 dùng password mà chúng ta đã tạo cho tài khoản Administrator trong quá trình Setup. 24. Xuất hiện đầu tiên trên màn hình là trang Manage Your Server, bạn nên check vào Don't display this page at logon checkbox và đóng cửa sổ Window lại

Cài đặt và cấu hình DNS

Bước kế tiếp là cài đặt Domain Naming System (DNS) server trên chính Computer này (EXCHANGE2003BE). Điều này là cần thiết vì Active Directory Service hoạt động trên Domain Controller, kiểm soát toàn Domain yêu cầu phải có DNS server service phục vụ cho nhu cầu truy vấn tên -hostname, đăng kí các record (A, PTR, SRV records v.v..). Chúng ta sẽ cài DNS server và sau đó sẽ nâng vai trò Computer này lên thành một Domain Controller, và DNS server này sẽ phục vụ cho toàn Domain.

Tiến hành các bước sau để cài đặt DNS server

1. Click Start, Control Panel. Click Add or Remove Programs. 2. Trong Add or Remove Programs, click Add/Remove Windows Components 3. Trong Windows Components, xem qua danh sách Components và click Networking Services entry. Click Details. 4. Check vào Domain Name System (DNS) checkbox và click OK. 5. Click Next trong Windows Components. 6. Click Finish trên

Completing the Windows Components Wizard. 7. Đóng Add or Remove Programs

DNS server đã được cài đặt, Admin cần đưa vào DNS Server các thông số cụ thể phục vụ cho hoạt động truy vấn tên, cụ thể là sẽ tạo ra hai vùng Forward và Reverse lookup zones. Tiến hành các bước sau để cấu hình DNS server:

1. Click Start và sau đó click Administrative Tools. Click DNS2. Trong bảng làm việc của DNS (DNS console), mở rộng server name (EXCHANGE2003BE), sau đó click trên Reverse Lookup Zones. Right click trên Reverse Lookup Zones và click New Zone. 3. Click Next trên Welcome to the New Zone Wizard. 4. Trên Zone Type , chọn Primary zone option và click Next. 5. Trên Reverse Lookup Zone Name page, chọn Network ID option và Enter 10.0.0 vào text box. Click Next. 6. Chấp nhận chọn lựa mặc định trên Zone File page, và click Next. 7. Trên Dynamic Update page, chọn Allow both nonsecure and secure dynamic updates option. Click Next. 8. Click Finish trên Completing the New Zone Wizard page.

Kế tiếp chúng ta tạo Forward lookup zone cho Domain mà Computer này sẽ là Domain Controller.

Tiến hành các bước sau

1. Right click Forward Lookup Zone và click New Zone. 2. Click Next trên Welcome to the New Zone Wizard page. 3. trên Zone Type page, chọn Primary zone option và click Next.
4. Trên Zone Name page, điền tên của forward lookup zone trong Zone name text box. Trong ví dụ này tên của zone là MSFirewall.org, trùng với tên của Domain sẽ tạo sau này. Đưa MSFirewall.org vào text box. Click Next. 5. Chấp nhận các xác lập mặc định trên Zone File page và click Next. 6. Trên Dynamic Update page, chọn Allow both nonsecure and secure dynamic updates. Click Next. 7. Click Finish trên Completing the New Zone Wizard page.

8. Mở rộng Forward Lookup Zones và click vào MSFirewall.org zone. Right click trên MSFirewall.org và Click New Host (A).

9. Trong New Host dialog box, điền vào chính xác EXCHANGE2003BE trong Name (uses parent domain name if blank) text box. Trong IP address text box, điền vào 10.0.0.2. Check vào Create associated pointer (PTR) record checkbox. Click Add Host. Click OK trong DNS dialog box thông báo rằng (A) Record đã được tạo xong. Click Done trong New Host text box.

10. Right click trên MSFirewall.org forward lookup zone và click Properties. Click Name Servers tab. Click exchange2003be entry và click Edit.

11. Trong Server fully qualified domain name (FQDN) text box, điền vào tên đầy đủ của Domain controller computer là exchange2003be.MSFirewall.org. Click Resolve. Sẽ nhận thấy, IP address của Server xuất hiện trong IP address list. Click OK.

12. Click Apply và sau đó click OK trên MSFirewall.org Properties dialog box.

13. Right click trên DNS server name EXCHANGE2003BE , chọn All Tasks. Click Restart.

14. Close DNS console.

Giờ đây Computer này đã sẵn sàng để nâng vai trò lên Thành một Domain controller trong Domain MSFirewall.org

Tiến hành các bước sau để tạo Domain và nâng server này thành Domain Controller đầu tiên của Domain (Primary Domain Controller)

Cài đặt Primary Domain Controller

1. Click Start và click Run .

2. Trong Run dialog box, đánh lệnh dcpromo trong Open text box và click OK.

3. Click Next trên Welcome to the Active Directory Installation Wizard page.

4. Click Next trên Operating System Compatibility page.

5. Trên Domain Controller Type page, chọn Domain controller for a new domain option và click Next.

6. Trên Create New Domain page, chọn Domain in a new forest option và click Next.

7. Trên New Domain Name page, điền tên đầy đủ của Domain (Full DNS name) MSFirewall.org text box và click Next.

8. Trên NetBIOS Domain Name page (NetBIOS name của Domain nhằm support cho các Windows OS- như các dòng Windows NT và WINDOWS 9x đời cũ, khi các Client này muốn giao dịch với Domain), chấp nhận NetBIOS name mặc định

Trong ví dụ này là MSFIREWALL. Click Next.

9. Chấp nhận các xác lập mặc định trên Database and Log Folders page và click Next.

10. Trên Shared System Volume page, chấp nhận vị trí lưu trữ mặc định và click Next.

11. Trên DNS Registration Diagnostics page, chọn I will correct the problem later by configuring DNS manually (Advanced). Click Next.

12. Trên Permissions page, chọn Permissions compatible only with Windows 2000 or Windows Server 2003 operating system option. Click Next.

13. Trên Directory Services Restore Mode Administrator Password page (chế độ phục hồi cho Domain Controller khi DC này gặp phải sự cố,

Khi DC offline, vào chế độ troubleshoot này bằng cach1 Restart Computer, chọn F8), điền vào Restore Mode Password và sau đó Confirm password. (Các Admin không nên nhầm lẫn Password ở chế độ này với Domain Administrator Password, điều khiển hoạt động của DCs hoặc Domain). Click Next.

14. Trên Summary page, click Next.

15. Bây giờ là lúc Computer cần Restart để các thông số vừa cài đặt Active

16. Click Finish trên Completing the Active Directory Installation Wizard page, hoàn thành việc cài đặt.

17. Click Restart Now trên Active Directory Installation Wizard page.

18. Log-on vào Domain Controller dùng tài khoản Administrator sau khi đã Restart.

Cài đặt và cấu hình Microsoft Exchange trên Domain Controller

Computer đã sẵn sàng cho việc cài đặt Microsoft Exchange. Trong phần này chúng ta sẽ tiến hành những bước sau:

• Cài đặt các Service IIS World Wide Web, SMTP và NNTP services

• Cài đặt Microsoft Exchange Server 2003

• Cấu hình Outlook Web Access WebSite

Tiến hành các bước sau để cài World Wide Web, SMTP và NNTP services:

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

2. Trong Add or Remove Programs, click Add/Remove Windows Components
3. Trên Windows Components page, chọn Application Server entry trong Components page. Click Details.

4. Trong Application Server dialog box, check vào ASP.NET checkbox. Chọn Internet Information Services (IIS) entry và click Details.

5. Trong Internet Information Services (IIS) dialog box, check vào NNTP Service checkbox. Check tiếp SMTP Service checkbox. Click OK.

6. Click OK trong Application Server dialog box.

7. Click Next trên Windows Components page.

8. Click OK vào Insert Disk dialog box.

9. Trong Files Needed dialog box, đưa đường dẫn đến Folder I386 trên CD cài đặt Windows Server 2003 trong copy file từ text box. Click OK.

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

11. Close Add or Remove Programs .

Tiến hành các bước sau cài Microsoft Exchange:

1. Đưa Exchange Server 2003 CD vào CD-ROM, trên autorun page, click Exchange Deployment Tools link nằm dưới Deployment heading.

2. Trên Welcome to the Exchange Server Deployment Tools page, click Deploy the first Exchange 2003 server link.
3. Trên Deploy the First Exchange 2003 Server page, click New Exchange 2003 Installation link.

4. Trên New Exchange 2003 Installation page, kéo xuống cuối trang.Click Run Setup now link.

5. Trên Welcome to the Microsoft Exchange Installation Wizard page, click Next.

6. Trên License Agreement page, chọn I agree option và click Next.

7. Chấp nhận các xác lập mặc định trên Component Selection page và click Next.

8. Chọn Create a New Exchange Organization option trên Installation Type page và click Next.

9. Chấp nhận tên mặc định trong Organization Name text box trên Organization Name page, và click Next.

10. Trên Licensing Agreement page, chọn I agree that I have read and will be bound by the license agreement for this product và click Next.

11. Trên Installation Summary page, click Next.

12. Trong Microsoft Exchange Installation Wizard dialog box, click OK.

13. Click Finish trên on the Completing the Microsoft Exchange Wizard page khi cài đặt hoàn thành.

14. Đóng tất cả cửa sổ đang open.

Exchange Server đã được cài đặt và giờ đây Admin có thể tạo các mailboxes cho Users. Bước kế tiếp là cấu hình Outlook Web Access site và chỉ dùng phương thức xác thực duy nhất là Basic Authentication. Đối với các quản trị Mail Server thì đây là một cấu hình quan trọng (nhưng tất nhiên không bắt buộc) khi muốn cho phép truy cập từ xa (remote access) vào OWA site. Sau đó, chúng ta sẽ yêu cầu một Website Certificate (Chứng từ số Website) cho OWA site và publish OWA site dùng quy tắc Web Publishing Rule trênISA Server, thông qua rule này, sẽ cho phép remote users truy cập vào OWA site.

Tiến hành các bước sau để cấu hình OWA site dùng phương thức xác thực duy nhất Basic authentication:

1. Click Start, chọn Administrative Tools. Click Internet Information Services (IIS) Manager.

2. Trong Internet Information Services (IIS) Manager console, mở rộng server name, mở rộng WebSites node và mở Default Web Site.

3. Click trên Public node và sau đó right click. Click Properties.

4. Trong Public Properties dialog box, click Directory Security tab.

5. Trên Directory Security tab, click Edit trong khung Authentication and access control.

6. Trong Authentication Methods dialog box, đảm bảo không check vào (remove) Integrated Windows authentication checkbox. Click OK.

7. Click Apply và click OK.

8. Click trên Exchange node và right click. Click Properties.

9. Trên Exchange Properties dialog box, click Directory Security tab.

10. Trên Directory Security tab, click Edit trong Authentication and access control

11. Trong Authentication Methods dialog box, đảm bảo không check vào (remove) Integrated Windows authentication checkbox. Click OK.

12. Click Apply, click OK trong Exchange Properties dialog box.

13. Click trên ExchWeb node,sau đó right click. Click Properties.

14. Trong ExchWeb Properties dialog box, click Directory Security tab.

15. Trên Directory Security tab, click Edit trong khung Authentication and access control
16. Trong Authentication Methods dialog box, không check (remove) vào Enable anonymous access checkbox. Sau đó check vào Basic authentication (chú ý dùng phương thức xác thực này, password được gửi đi dưới dạng clear text) checkbox. Click Yes trong IIS Manager dialog box và Admin nhận được thông báo rằng password được gửi đi hoàn toàn không mã hóa (clear). Trong Default domain text box, đưa vào tên Internal Network domain, chính là MSFIREWALL. Click OK.

17. Click Apply trong ExchWeb Properties dialog box. Click OK trong Inheritance Overrides dialog box. Click OK trong ExchWeb Properties dialog box.

18. Right click Default Web Site và click Stop. Right click lại Default Web Site và click Start.

Kết luận:

Trong sách hướng dẫn cấu hình ISA Server 2004 này chúng ta đã thảo luận những mục tiêu và những phương thức, để có thể nắm bắt triển khai và cấu hình ISA sao cho hiệu quả nhất. Sách hướng dẫn cũng cung cấp cho các bạn phương pháp giải quyết vấn đề theo từng bước cụ thể. Chương một này tập trung vào việc xây dựng một cơ sở hạ tầng Network (Network Infrastructure) theo mô hình Microsoft Active Directory Domain trên máy chủ Winndows server 2003 Domain Controller, và triển khai các Service khác liên quan đến hạ tầng Network như WINS, DNS, và các Service gia tăng như Web, Mail.. Chương kế tiếp trình bày cách thức cài đặt một Microsoft Certificate Services trên Domain Controller Computer.

(Hết chương 1 mời các bạn tiếp tục theo dõi chương 2 sẽ được phát hành trong vài ngày tới)
Ho Viet Ha Owner Network Information Security Vietnam, Inc. http://nis.com.vn Email: networksecurity@nis.com.vn