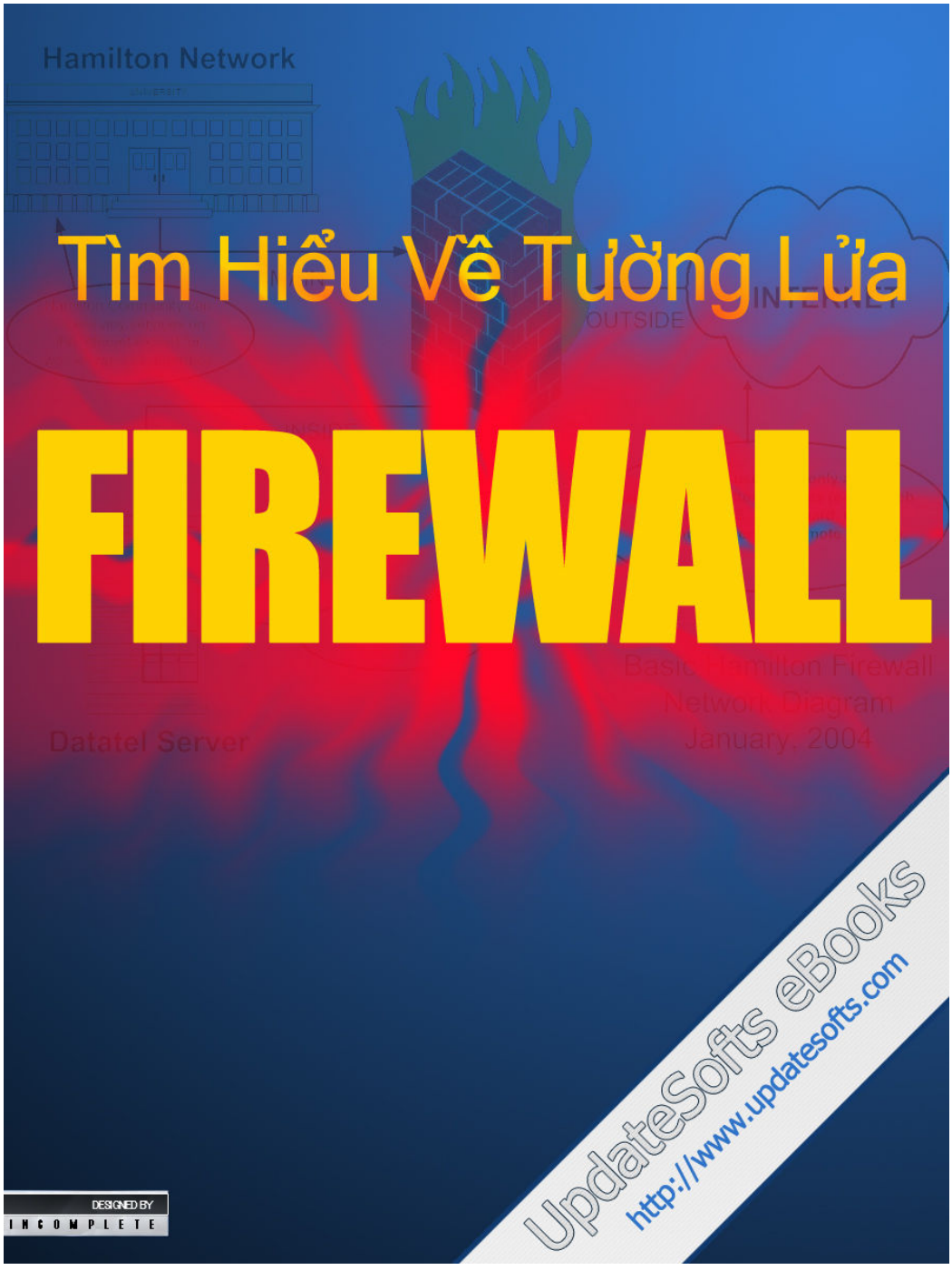

Hamilton Network
Tìm Hiểu Về Tường Lửa
FIREWALL
OUTSIDE
Datatel Server
January, 2004
UpdateSofts eBooks
http://www.updatesofts.com
DESIGNED BY
INCOMPLETE

M•c l•c

1. An toàn thông tin trên mạng

1.1 Tại sao cần có Internet Firewall

Hiện nay, khái niệm mạng toàn cầu - Internet không còn mới mẻ. Nó đã trở nên phổ biến tới mức không cần phải chú giải gì thêm trong những tạp chí kỹ thuật, còn trên những tạp chí khác thì tràn ngập những bài viết dài, ngắn về Internet. Khi những tạp chí thông thường chú trọng vào Internet thì giờ đây, những tạp chí kỹ thuật lại tập trung vào khía cạnh khác: an toàn thông tin. Đó cùng là một quá trình tiến triển hợp logic: khi những vui thích ban đầu về một siêu xa lộ thông tin, bạn nhất định nhận thấy rằng không chỉ cho phép bạn truy nhập vào nhiều nơi trên thế giới, Internet còn cho phép nhiều người không mời mà tự ý ghé thăm máy tính của bạn.

Thực vậy, Internet có những kỹ thuật tuyệt vời cho phép mọi người truy nhập, khai thác, chia sẻ thông tin. Những nó cũng là nguy cơ chính dẫn đến thông tin của bạn bị hư hỏng hoặc phá huỷ hoàn toàn.

Theo số liệu của CERT(Computer Emegency Response Team - "Đội cấp cứu máy tính"), số lượng các vụ tấn công trên Internet được thông báo cho tổ chức này là ít hơn 200 vào năm 1989, khoảng 400 vào năm 1991, 1400 vào năm 1993, và 2241 vào năm 1994. Những vụ tấn công này nhằm vào tất cả các máy tính có mặt trên Internet, các máy tính của tất cả các công ty lớn như AT&T, IBM, các trường đại học, các cơ quan nhà nước, các tổ chức quân sự, nhà băng... Một số vụ tấn công có quy mô khổng lồ (có tới 100.000 máy tính bị tấn công). Hơn nữa, những con số này chỉ là phần nổi của tảng băng. Một phần rất lớn các vụ tấn công

không được thông báo, vì nhiều lý do, trong đó có thể kể đến nỗi lo bị mất uy tín, hoặc đơn giản những người quản trị hệ thống không hề hay biết những cuộc tấn công nhằm vào hệ thống của họ.

Không chỉ số lượng các cuộc tấn công tăng lên nhanh chóng, mà các phương pháp tấn công cũng liên tục được hoàn thiện. Điều đó một phần do các nhân viên quản trị hệ thống được kết nối với Internet ngày càng đề cao cảnh giác. Cũng theo CERT, những cuộc tấn công thời kỳ 1988-1989 chủ yếu đoán tên người sử dụng-mật khẩu (UserID-password) hoặc sử dụng một số lỗi của các chương trình và hệ điều hành (security hole) làm vô hiệu hệ thống bảo vệ, tuy nhiên các cuộc tấn công vào thời gian gần đây bao gồm cả các thao tác như giả mạo địa chỉ IP, theo dõi thông tin truyền qua mạng, chiếm các phiên làm việc từ xa (telnet hoặc rlogin).

1.2 Bạn muốn bảo vệ cái gì?

Nhiệm vụ cơ bản của Firewall là bảo vệ. Nếu bạn muốn xây dựng firewall, việc đầu tiên bạn cần xem xét chính là bạn cần bảo vệ cái gì.

1.2.1 Dữ liệu của bạn

Những thông tin lưu trữ trên hệ thống máy tính cần được bảo vệ do các yêu cầu sau:

- Bảo mật: Những thông tin có giá trị về kinh tế, quân sự, chính sách vv... cần được giữ kín.
- Tính toàn vẹn: Thông tin không bị mất mát hoặc sửa đổi, đánh tráo.
- Tính kịp thời: Yêu cầu truy nhập thông tin vào đúng thời điểm cần thiết.

Trong các yêu cầu này, thông thường yêu cầu về bảo mật được coi là yêu cầu số 1 đối với thông tin lưu trữ trên mạng. Tuy nhiên, ngay cả khi những thông tin này không được giữ bí mật, thì những yêu cầu về tính toàn vẹn cũng rất quan trọng. Không một cá nhân, một tổ chức nào lãng phí tài nguyên vật chất và thời gian để lưu trữ những thông tin mà không biết về tính đúng đắn của những thông tin đó.

1.2.2 Tài nguyên của bạn

Trên thực tế, trong các cuộc tấn công trên Internet, kẻ tấn công, sau khi đã làm chủ được hệ thống bên trong, có thể sử dụng các máy này để phục vụ cho mục đích của mình như chạy các chương trình dò mật khẩu người sử dụng, sử dụng các liên kết mạng sẵn có để tiếp tục tấn công các hệ thống khác vv...

1.2.3 Danh tiếng của bạn

Như trên đã nêu, một phần lớn các cuộc tấn công không được thông báo rộng rãi, và một trong những nguyên nhân là nỗi lo bị mất uy tín của cơ quan, đặc biệt là các công ty lớn và các cơ quan quan trọng trong bộ máy nhà nước. Trong trường hợp người quản trị hệ thống chỉ được biết đến sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công các hệ thống khác, thì tổn thất về uy tín là rất lớn và có thể để lại hậu quả lâu dài.

1.3 Bạn muốn bảo vệ chống lại cái gì?

Còn những gì bạn cần phải lo lắng. Bạn sẽ phải đương đầu với những kiểu tấn công nào trên Internet và những kẻ nào sẽ thực hiện chúng?

1.3.1 Các kiểu tấn công

Có rất nhiều kiểu tấn công vào hệ thống, và có nhiều cách để phân loại những kiểu tấn công này. ở đây, chúng ta chia thành 3 kiểu chính như sau:

1.3.1.1 Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm được quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò cặp tên người sử dụng-mật khẩu. Đây là phương pháp đơn giản, dễ thực hiện và không đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Kẻ tấn công có thể sử dụng những thông tin như tên người dùng, ngày sinh, địa chỉ, số nhà vv.. để đoán mật khẩu. Trong trường hợp có được danh sách người sử dụng và những thông tin về môi trường làm việc, có một trương trình tự động hoá về việc dò tìm mật khẩu này. một trương trình có thể dễ dàng lấy được từ Internet để giải các mật khẩu đã mã hoá của các hệ thống unix có tên là *crack*, có khả năng thử các tổ hợp các từ trong một từ điển lớn, theo những quy tắc do người dùng tự định nghĩa. Trong một số trường hợp, khả năng thành công của phương pháp này có thể lên tới 30%.

Phương pháp sử dụng các lỗi của chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được tiếp tục để chiếm quyền truy

nhập. Trong một số trường hợp phương pháp này cho phép kẻ tấn công có được quyền của người quản trị hệ thống (*root* hay *administrator*).

Hai ví dụ thường xuyên được đưa ra để minh hoạ cho phương pháp này là ví dụ với chương trình sendmail và chương trình rlogin của hệ điều hành UNIX.

Sendmail là một chương trình phức tạp, với mã nguồn bao gồm hàng ngàn dòng lệnh của ngôn ngữ C. Sendmail được chạy với quyền ưu tiên của người quản trị hệ thống, do chương trình phải có quyền ghi vào hộp thư của những người sử dụng máy. Và Sendmail trực tiếp nhận các yêu cầu về thư tín trên mạng bên ngoài. Đây chính là những yếu tố làm cho sendmail trở thành một nguồn cung cấp những lỗ hổng về bảo mật để truy nhập hệ thống.

Rlogin cho phép người sử dụng từ một máy trên mạng truy nhập từ xa vào một máy khác sử dụng tài nguyên của máy này. Trong quá trình nhận tên và mật khẩu của người sử dụng, rlogin không kiểm tra độ dài của dòng nhập, do đó kẻ tấn công có thể đưa vào một xâu đã được tính toán trước để ghi đè lên mã chương trình của rlogin, qua đó chiếm được quyền truy nhập.

1.3.1.2 Nghe trộm

Việc nghe trộm thông tin trên mạng có thể đưa lại những thông tin có ích như tên-mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa vỉ giao tiếp mạng (Network Interface Card-NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng.

Những thông tin này cũng có thể dễ dàng lấy được trên Internet.

1.3.1.3 Giả mạo địa chỉ

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (*source-routing*). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong với một địa chỉ IP giả mạo (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong), đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

1.3.1.4 Vô hiệu hoá các chức năng của hệ thống (denial of service)

Đây là kểu tấn công nhằm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó thiết kế. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng. Ví dụ sử dụng lệnh *ping* với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

1.3.1.5 Lỗi của người quản trị hệ thống

Đây không phải là một kiểu tấn công của những kẻ đột nhập, tuy nhiên lỗi của người quản trị hệ thống thường tạo ra những lỗ hổng cho phép kẻ tấn công sử dụng để truy nhập vào mạng nội bộ.

1.3.1.6 Tấn công vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác. Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi. Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

1.3.2 Phân loại kẻ tấn công

Có rất nhiều kẻ tấn công trên mạng toàn cầu – Internet và chúng ta cũng không thể phân loại chúng một cách chính xác, bất cứ một bản phân loại kiểu này cũng chỉ nên được xem như là một sự giới thiệu hơn là một cách nhìn rập khuôn.

1.3.2.1 Người qua đường

Người qua đường là những kẻ buồn chán với những công việc thường ngày, họ muốn tìm những trò giải trí mới. Họ đột nhập vào máy tính của bạn vì họ nghĩ bạn có thể có những dữ liệu hay, hoặc bởi vì họ cảm thấy thích thú khi sử dụng máy tính của người khác, hoặc chỉ đơn giản là họ không tìm được một việc gì hay hơn để làm. Họ có thể là người tò mò nhưng không chủ định làm hại bạn. Tuy nhiên, họ thường gây hư hỏng hệ thống khi đột nhập hay khi xoá bỏ dấu vết của họ.

1.3.2.2 Kẻ phá hoại

Kẻ phá hoại chủ định phá hoại hệ thống của bạn, họ có thể không thích bạn, họ cũng có thể không biết bạn nhưng họ tìm thấy niềm vui khi đi phá hoại.

Thông thường, trên Internet kẻ phá hoại khá hiếm. Mọi người không thích họ. Nhiều người còn thích tìm và chặn đứng những kẻ phá hoại. Tuy ít nhưng kẻ phá hoại thường gây hỏng trầm trọng cho hệ thống của bạn như xoá toàn bộ dữ liệu, phá hỏng các thiết bị trên máy tính của bạn...

1.3.2.3 Kẻ ghi điểm

Rất nhiều kẻ qua đường bị cuốn hút vào việc đột nhập, phá hoại. Họ muốn được khẳng định mình thông qua số lượng và các kiểu hệ thống mà họ đã đột nhập qua. Đột nhập được vào những nơi nổi tiếng, những nơi phòng bị chặt chẽ, những nơi thiết kế tinh xảo có giá trị nhiều điểm đối với họ. Tuy nhiên họ cũng sẽ tấn công tất cả những nơi họ có thể, với mục đích số lượng cũng như mục đích chất lượng. Những người này không quan tâm đến những thông tin bạn có hay những đặc tính khác về tài nguyên của bạn. Tuy nhiên để đạt được mục đích là đột nhập, vô tình hay hữu ý họ sẽ làm hư hỏng hệ thống của bạn.

1.3.2.4 Gián điệp

Hiện nay có rất nhiều thông tin quan trọng được lưu trữ trên máy tính như các thông tin về quân sự, kinh tế... Gián điệp máy tính là một vấn đề phức tạp và khó phát hiện. Thực tế, phần lớn các tổ chức không thể phòng thủ kiểu tấn công này một cách hiệu quả và bạn có thể chắc rằng đường liên kết

với Internet không phải là con đường dễ nhất để gián điệp thu lượm thông tin.

1.4 Vậy Internet Firewall là gì?

1.4.1 Định nghĩa

Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hoả hoạn. Trong công nghệ mạng thông tin, Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn. Cũng có thể hiểu rằng Firewall là một cơ chế để bảo vệ mạng tin tưởng (trusted network) khỏi các mạng không tin tưởng (untrusted network).

Internet Firewall là một thiết bị (phần cứng+phần mềm) giữa mạng của một tổ chức, một công ty, hay một quốc gia (Intranet) và Internet. Nó thực hiện vai trò bảo mật các thông tin Intranet từ thế giới Internet bên ngoài.

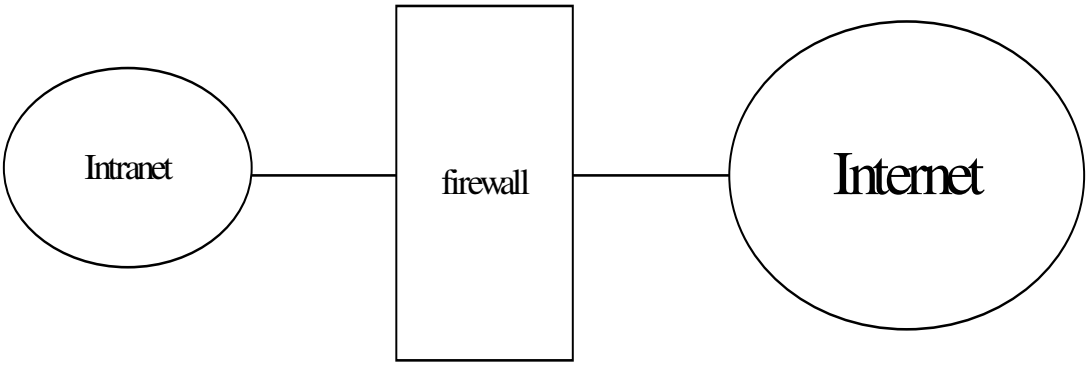
1.4.2 Chức năng

Internet Firewall (từ nay về sau gọi tắt là firewall) là một thành phần đặt giữa Intranet và Internet để kiểm soát tất cả các việc lưu thông và truy cập giữa chúng với nhau bao gồm:

- Firewall quyết định những dịch vụ nào từ bên trong được phép truy cập từ bên ngoài, những người nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong, và cả những dịch vụ nào bên ngoài được phép truy cập bởi những người bên trong.

- Để firewall làm việc hiệu quả, tất cả trao đổi thông tin từ trong ra ngoài và ngược lại đều phải thực hiện thông qua Firewall.
- Chỉ có những trao đổi nào được phép bởi chế độ an ninh của hệ thống mạng nội bộ mới được quyền lưu thông qua Firewall.

Sơ đồ chức năng hệ thống của firewall được mô tả như trong hình 2.1



Hình 2.1 Sơ đồ chức năng hệ thống của firewall

1.4.3 Cấu trúc

Firewall bao gồm:

- Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router.
- Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ. Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

Chúng ta sẽ đề cập kỹ hơn các hoạt động của những hệ này ở phần sau.

1.4.4 Các thành phần của Firewall và cơ chế hoạt động

Một Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:

- Bộ lọc packet (packet-filtering router)
- Cổng ứng dụng (application-level gateway hay proxy server)
- Cổng mạch (circuite level gateway)

1.4.4.1 Bộ lọc gói tin (Packet filtering router)

1.4.4.1.1 Nguyên lý:

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua Firewall thì điều đó có nghĩa rằng Firewall hoạt động chặt chẽ với giao thức liên mạng TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS...) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ để có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các *packet* và những con số địa chỉ của chúng.

Bộ lọc packet cho phép hay từ chối mỗi *packet* mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc *packet* hay không. Các luật lệ lọc *packet* này là dựa trên các thông tin ở đầu mỗi *packet* (packet header), dùng để cho phép truyền các packet đó ở trên mạng. Đó là:

- Địa chỉ IP nơi xuất phát (IP Source address)

- Địa chỉ IP nơi nhận (IP Destination address)
- Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)
- Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)
- Cổng TCP/UDP nơi nhận (TCP/UDP destination port)
- Dạng thông báo ICMP (ICMP message type)
- giao diện packet đến (incomming interface of packet)
- giao diện packet đi (outcomming interface of packet)

Nếu luật lệ lọc packet được thoả mãn thì *packet* được chuyển qua firewall. Nếu không *packet* sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) được phép mới chạy được trên hệ thống mạng cục bộ.

1.4.4.1.2 Ưu điểm

- Đa số các hệ thống firewall đều sử dụng bộ lọc *packet*. Một trong những ưu điểm của phương pháp dùng bộ lọc packet là chi phí thấp vì cơ chế lọc *packet* đã được bao gồm trong mỗi phần mềm router.
- Ngoài ra, bộ lọc *packet* là trong suốt đối với người sử dụng và các ứng dụng, vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả.

1.4.4.1.3 Hạn chế:

Việc định nghĩa các chế độ lọc *packet* là một việc khá phức tạp, nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ Internet, các dạng *packet header*, và các giá trị cụ thể mà họ có thể nhận trên mỗi trường. Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển.

Do làm việc dựa trên *header* của các *packet*, rõ ràng là bộ lọc *packet* không kiểm soát được nội dung thông tin của *packet*. Các *packet* chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

1.4.4.2 Cổng ứng dụng (application-level gateway)

1.4.4.2.1 Nguyên lý

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service (dịch vụ đại diện). Proxy service là các bộ chương trình đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quản trị mạng không cài đặt chương trình proxy cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

Một cổng ứng dụng thường được coi như là một pháo đài (bastion host), bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đảm bảo an ninh của một bastion host là:

- Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ thống (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào Operating System, cũng như là đảm bảo sự tích hợp firewall.

- Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.

- Bastion host có thể yêu cầu nhiều mức độ xác thực khác nhau, ví dụ như user password hay smart card.

- Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một sồ các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

- Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của giao thông qua nó, mỗi sự kết nối, khoảng thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.

- Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ môt proxy đang có vấn đề.

Ví dụ: Telnet Proxy

Ví dụ một người (gọi là outside client) muốn sử dụng dịch vụ TELNET để kết nối vào hệ thống mạng qua môt bastion host có Telnet proxy. Quá trình xảy ra như sau:

1. Outside client telnets đến bastion host. Bastion host kiểm tra password, nếu hợp lệ thì outside client được phép vào giao diện của Telnet proxy. Telnet proxy cho phép một tập nhỏ những lệnh của Telnet, và quyết định những máy chủ nội bộ nào outside client được phép truy nhập.

2. Outside client chỉ ra máy chủ đích và Telnet proxy tạo một kết nối của riêng nó tới máy chủ bên trong, và chuyển các lệnh tới máy chủ dưới sự uỷ quyền của outside client. Outside client thì tin rằng Telnet proxy là máy chủ thật ở bên trong, trong khi máy chủ ở bên trong thì tin rằng Telnet proxy là client thật.

1.4.4.2.2 Ưu điểm:

- **Cho phép** người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.
- Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.
- Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.
- Luật lệ filltering (lọc) cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

1.4.4.2.3 Hạn chế:

Yêu cầu các users biến đổi (modìy) thao tác, hoặc modìy phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Ví dụ, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước đê nối với máy chủ chứ không phải là một bước thôi. Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet.

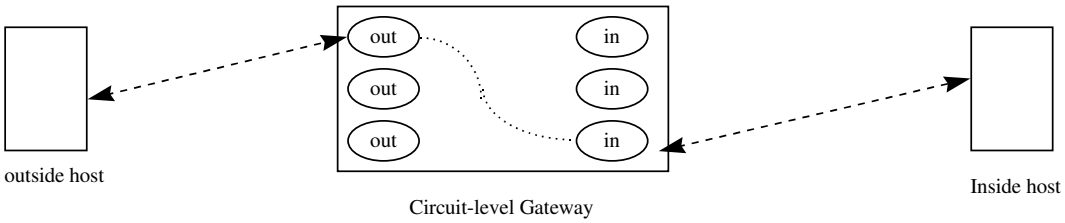
1.4.4.3 Cổng vòng (circuit-Level Gateway)

Cổng vòng là một chức năng đặc biệt có thể thực hiện đươc bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.

Hình 2.2 minh hoạ một hành động sử dụng nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục Telnet nào.Cổng vòng làm việc như một sợi dây,sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên, vì sự kết nối này xuất hiện từ hệ thống firewall, nó che dấu thông tin về mạng nội bộ.

Cổng vòng thường được sử dụng cho những kết nối ra ngoài, nơi mà các quản trị mạng thật sự tin tưởng những người dùng bên trong. Ưu điểm lớn nhất là một bastion host có thể được cấu hình như là một hỗn hợp cung cấp Cổng ứng dụng cho những kết nối đến, và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các dịch vụ Internet, trong khi vẫn cung cấp

chức năng bức tường lửa để bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.



Hình 2.2 Cổng vòng

1.4.5 Những hạn chế của firewall

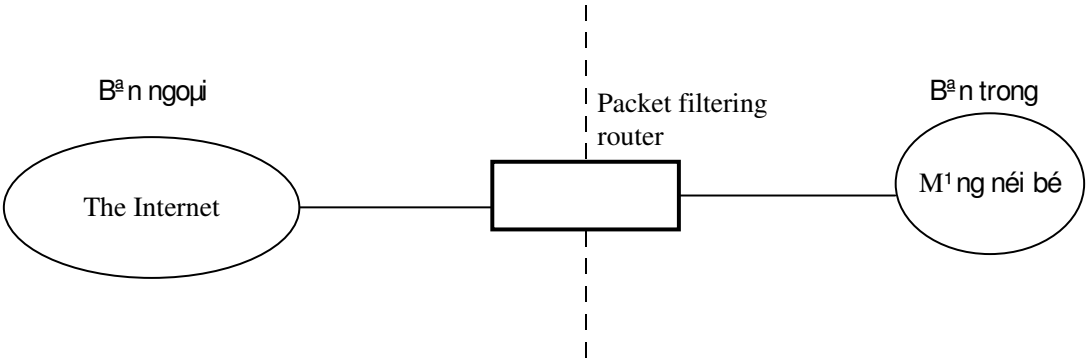
- Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.
- Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, firewall không thể chống lại một cuộc tấn công từ một đường dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.
- Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-driven attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.
- Một ví dụ là các virus máy tính. Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các

virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của firewall.

1.4.6 Các ví dụ firewall

1.4.6.1 Packet-Filtering Router (Bộ trung chuyển có lọc gói)

Hệ thống Internet firewall phổ biến nhất chỉ bao gồm một packet-filtering router đặt giữa mạng nội bộ và Internet (Hình 2.3). Một packet-filtering router có hai chức năng: chuyển tiếp truyền thông giữa hai mạng và sử dụng các quy luật về lọc gói để cho phép hay từ chối truyền thông. Căn bản, các quy luật lọc đựơc định nghĩa sao cho các host trên mạng nội bộ được quyền truy nhập trực tiếp tới Internet, trong khi các host trên Internet chỉ có một số giới hạn các truy nhập vào các máy tính trên mạng nội bộ. Tư tưởng của mô cấu trúc firewall này là tất cả những gì không được chỉ ra rõ ràng là cho phép thì có nghĩa là bị từ chối.



Hình 2.3 Packet-filtering router

Ưu điểm:

- giá thành thấp (vì cấu hình đơn giản)

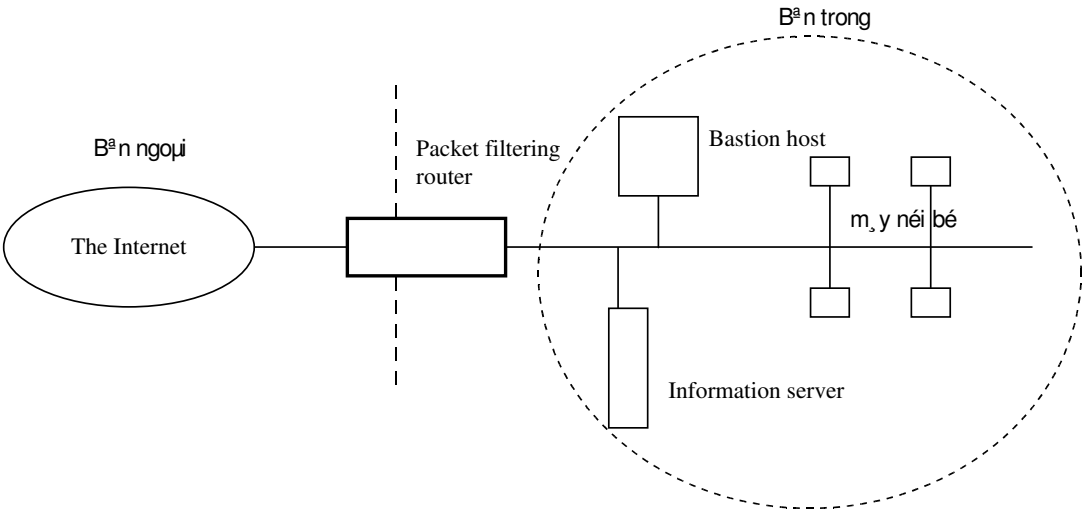
- trong suốt đối với người sử dụng

Hạn chế:

- Có tất cả hạn chế của một packet-filtering router, như là dễ bị tấn công vào các bộ lọc mà cấu hình được đặt không hoàn hảo, hoặc là bị tấn công ngầm dưới những dịch vụ đã được phép.
- Bởi vì các packet được trao đổi trực tiếp giữa hai mạng thông qua router , nguy cơ bị tấn công quyết định bởi số lượng các host và dịch vụ được phép. Điều đó dẫn đến mỗi một host được phép truy nhập trực tiếp vào Internet cần phải được cung cấp một hệ thống xác thực phức tạp, và thường xuyên kiểm tra bởi người quản trị mạng xem có dấu hiệu của sự tấn công nào không.
- Nếu một packet-filtering router do một sự cố nào đó ngừng hoạt động, tất cả hệ thống trên mạng nội bộ có thể bị tấn công.

1.4.6.2 Screened Host Firewall

Hệ thống này bao gồm một packet-filtering router và một bastion host (hình 2.4). Hệ thống này cung cấp độ bảo mật cao hơn hệ thống trên, vì nó thực hiện cả bảo mật ở tầng network(packet-filtering) và ở tầng ứng dụng (application level). Đồng thời, kẻ tấn công phải phá vỡ cả hai tầng bảo mật để tấn công vào mạng nội bộ.



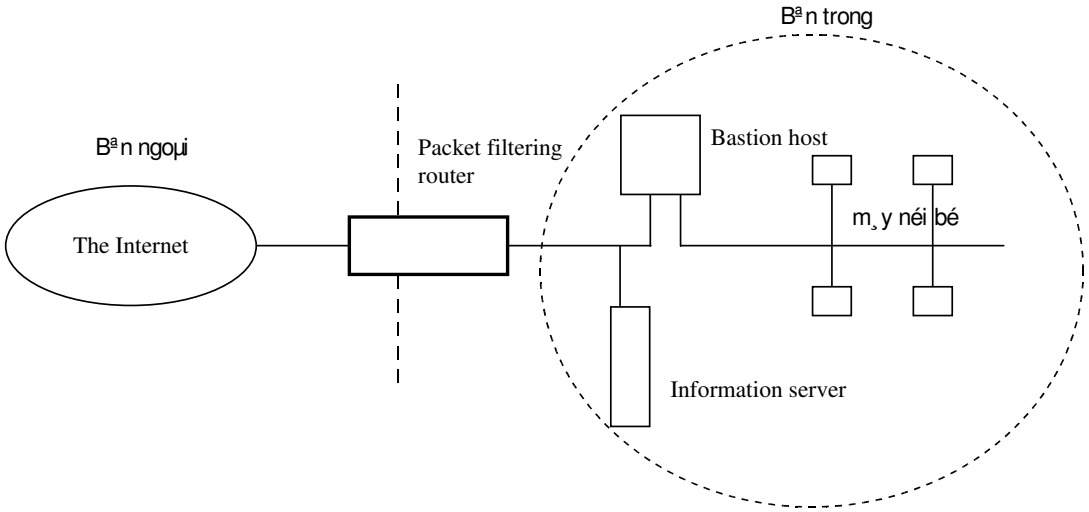
Hình 2.4 Screened host firewall (Single- Homed Bastion Host)

Trong hệ thống này, bastion host được cấu hình ở trong mạng nội bộ. Qui luật filtering trên packet-filtering router được định nghĩa sao cho tất cả các hệ thống ở bên ngoài chỉ có thể truy nhập bastion host; Việc truyền thông tới tất cả các hệ thống bên trong đều bị khoá. Bởi vì các hệ thống nội bộ và bastion host ở trên cùng một mạng, chính sách bảo mật của một tổ chức sẽ quyết định xem các hệ thống nội bộ được phép truy nhập trực tiếp vào bastion Internet hay là chúng phải sử dụng dịch vụ proxy trên bastion host. Việc bắt buộc những user nội bộ được thực hiện bằng cách đặt cấu hình bộ lọc của router sao cho chỉ chấp nhận những truyền thông nội bộ xuất phát từ bastion host.

Ưu điểm:

Máy chủ cung cấp các thông tin công cộng qua dịch vụ Web và FTP có thể đặt trên packet-filtering router và bastion. Trong trường hợp yêu cầu độ an toàn cao nhất, bastion host có thể chạy các dịch vụ proxy yêu cầu tất cả các user cả trong và ngoài truy nhập qua bastion host trước khi nối với máy chủ. Trường hợp không yêu cầu độ an toàn cao thì các máy nội bộ có thể nối thẳng với máy chủ.

Nếu cần độ bảo mật cao hơn nữa thì có thể dùng hệ thống firewall dual-home (hai chiều) bastion host (hình 2.5). Một hệ thống bastion host như vậy có 2 giao diện mạng (network interface), nhưng khi đó khả năng truyền thông trực tiếp giữa hai giao diện đó qua dịch vụ proxy là bị cấm.



Hình 2.5 Screened host firewall (Dual- Homed Bastion Host)

Bởi vì bastion host là hệ thống bên trong duy nhất có thể truy nhập được từ Internet, sự tấn công cũng chỉ giới hạn

đến bastion host mà thôi. Tuy nhiên, nếu như người dùng truy nhập được vào bastion host thì họ có thể dễ dàng truy nhập toàn bộ mạng nội bộ. Vì vậy cần phải cấm không cho người dùng truy nhập vào bastion host.

1.4.6.3 Demilitarized Zone (DMZ - khu vực phi quân sự) hay Screened-subnet Firewall

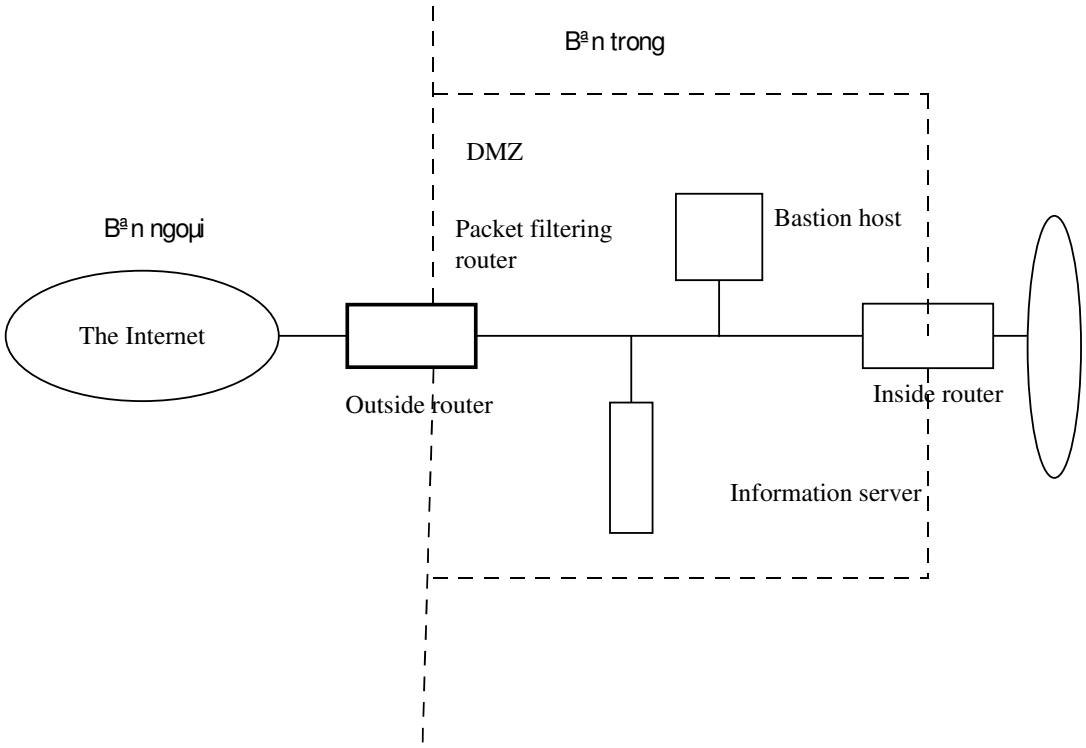
Hệ thống này bao gồm hai packet-filtering router và một bastion host (hình 2.6). Hệ thống firewall này có độ an toàn cao nhất vì nó cung cấp cả mức bảo mật : network và application trong khi định nghĩa một mạng "phi quân sự". Mạng DMZ đóng vai trò như một mạng nhỏ, cô lập đặt giữa Internet và mạng nội bộ. Cơ bản, một DMZ được cấu hình sao cho các hệ thống trên Internet và mạng nội bộ chỉ có thể truy nhập được một số giới hạn các hệ thống trên mạng DMZ, và sự truyền trực tiếp qua mạng DMZ là không thể được.

Với những thông tin đến, router ngoài chống lại những sự tấn công chuẩn (như giả mạo địa chỉ IP), và điều khiển truy nhập tới DMZ. Nó cho phép hệ thống bên ngoài truy nhập chỉ bastion host, và có thể cả information server. Router trong cung cấp sự bảo vệ thứ hai bằng cách điều khiển DMZ truy nhập mạng nội bộ chỉ với những truyền thông bắt đầu từ bastion host.

Với những thông tin đi, router trong điều khiển mạng nội bộ truy nhập tới DMZ. Nó chỉ cho phép các hệ thống bên trong truy nhập bastion host và có thể cả information server. Quy luật filtering trên router ngoài yêu cầu sử dung dich vụ proxy bằng cách chỉ cho phép thông tin ra bắt nguồn từ bastion host.

Ưu điểm:

- Kẻ tấn công cần phá vỡ ba tầng bảo vệ: router ngoài, bastion host và router trong.
- Bởi vì router ngoài chỉ quảng cáo DMZ network tới Internet, hệ thống mạng nội bộ là không thể nhìn thấy (invisible). Chỉ có một số hệ thống đã được chọn ra trên DMZ là được biết đến bởi Internet qua routing table và DNS information exchange (Domain Name Server).
- Bởi vì router trong chỉ quảng cáo DMZ network tới mạng nội bộ, các hệ thống trong mạng nội bộ không thể truy nhập trực tiếp vào Internet. Điều nay đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ proxy.



Hình 2.6 Screened-Subnet Firewall

2. Các dịch vụ Internet

Như đã trình bày ở trên, nhìn chung bạn phải xác định bạn bảo vệ cái gì khi thiết lập liên kết ra mạng ngoài hay Internet: dữ liệu, tài nguyên, danh tiếng. Khi xây dựng một Firewall, bạn phải quan tâm đến những vấn đề cụ thể hơn: bạn phải bảo vệ những dịch vụ nào bạn dùng hoặc cung cấp cho mạng ngoài (hay Internet).

Internet cung cấp một hệ thống các dịch vụ cho phép người dùng nối vào Internet truy nhập và sử dụng các thông tin ở trên mạng Internet. Hệ thống các dịch vụ này đã và đang được bổ sung theo sự phát triển không ngừng của Internet. Các dịch vụ này bao gồm World Wide Web (gọi tắt là WWW hoặc Web), Email (thư điện tử), Ftp (file transfer protocols - dịch vụ chuyển file), telnet (ứng dụng cho phép truy nhập máy tính ở xa), Archie (hệ thống xác định thông tin ở các file và directory), finger (hệ thống xác định các user trên Internet), rlogin(remote login - vào mạng từ xa) và một số các dịch vụ khác nữa.

2.1 World Wide Web - WWW

WWW là dịch vụ Internet ra đời gần đây nhất, nhưng phát triển nhanh nhất hiện nay. Web cung cấp một giao diện vô cùng thân thiện với người dùng, dễ sử dụng, vô cùng thuận lợi và đơn giản để tìm kiếm thông tin. Web liên kết thông tin dựa trên công nghệ hyper-link (siêu liên kết), cho phép các trang Web liên kết với nhau trực tiếp qua các địa chỉ của chúng. Thông qua Web, người dùng có thể :

- Phát hành các tin tức của mình và đọc tin tức từ khắp nơi trên thế giới
- Quảng cáo về mình, về công ty hay tổ chức của mình cũng như xem các loại quảng cáo trên thế giới, từ kiếm việc làm, tuyển mộ nhân viên, công nghệ và sản phẩm mới, tìm bạn, vân vân.
- Trao đổi thông tin với bè bạn, các tổ chức xã hội, các trung tâm nghiên cứu, trường học, vân vân
- Thực hiện các dịch vụ chuyền tiền hay mua bán hàng hoá
- Truy nhập các cơ sở dữ liệu của các tổ chức, công ty (nếu như được phép)

Và rất nhiều các hoạt động khác nữa.

2.2 Electronic Mail (Email hay thư điện tử).

Email là dịch vụ Internet được sử dụng rộng rãi nhất hiện nay. Hâu hết các thông báo ở dạng text (văn bản) đơn giản, nhưng người sử dụng có thể gửi kèm theo các file chứa các hình ảnh như sơ đồ, ảnh . Hệ thống email trên Internet là hệ thống thư điện tử lớn nhất trên thế giới, và thường được sử dụng cùng với các hệ thống chuyển thư khác.

Khả năng chuyển thư điện tử trên Web có bị hạn chế hơn so với các hệ thống chuyển thư điện tử trên Internet, bởi vì Web là một phương tiện trao đổi công cộng, trong khi thư là một cái gì đó riêng tư. Vì vậy, không phải tất cả các Web brower đều cung cấp chức năng email. (Hai browser lớn nhất hiện nay là Netscape và Internet Explorer đều cung cấp chức năng email).

2.3 Ftp (file transfer protocol hay dịch vụ chuyển file)

Ftp là một dịch vụ cho phép sao chép file từ một hệ thống máy tính này đến hệ thống máy tính khác ftp bao gồm thủ tục và chương trình ứng dụng, và là một trong những dịch vụ ra đời sớm nhất trên Internet.

Fpt có thể được dùng ở mức hệ thống (gõ lệnh vào *command-line*), trong Web browser hay một số tiện ích khác. Fpt vô cùng hữu ích cho những người dùng Internet, bởi vì khi sục sạo trên Internet, bạn sẽ tìm thấy vô số những thư viện phần mềm có ích về rất nhiều lĩnh vực và bạn có thể chép chúng về để sử dụng.

2.4 Telnet và rlogin

Telnet là một ứng dụng cho phép bạn truy nhập vào một máy tính ở xa và chạy các ứng dụng ở trên máy tính đó. Telnet là rất hữu ích khi bạn muốn chạy một ứng dụng không có hoặc không chạy được trên máy tính của bạn, ví dụ như bạn muốn chạy một ứng dung Unix trong khi máy của bạn là PC. Hay bạn máy tính của bạn không đủ mạnh để chạy một ứng dụng nào đó, hoặc không có các file dữ liệu cần thiết.

Telnet cho bạn khả năng làm việc trên máy tính ở xa bạn hàng ngàn cây số mà bạn vẫn có cảm giác như đang ngồi trước máy tính đó.

Chức năng của rlogin(remote login - vào mạng từ xa) cũng tương tự như Telnet.

2.5 Archie

Archie là một loại thư viện thường xuyên tự động tìm kiếm các máy tính trên Internet, tạo ra một kho dữ liệu về danh sách các file có thể nạp xuống (downloadable) từ Internet. Do đó, dữ liêu trong các file này luôn luôn là mới nhất.

Archie do đó rất tiện dụng cho người dùng để tìm kiếm và download các file. Người dùng chỉ cần gửi tên file, hoặc các từ khoá tới Archie; Archie sẽ cho lại địa chỉ của các file có tên đó hoặc có chứa những từ đó.

2.6 Finger

Finger là một chương trình ứng dụng cho phép tìm địa chỉ của các user khác trên Internet. Tối thiểu, finger có thể cho bạn biết ai đang sử dụng một hệ thống máy tính nào đó, tên login của người đó là gì.

Finger hay được sử dụng để tìm địa chỉ email của bè bạn trên Internet. Finger còn có thể cung cấp cho bạn nhiều thông tin khác, như là một người nào đó đã login vào mạng bao lâu. Vì thế finger có thể coi là một người trợ giúp đắc lực nhưng cũng là mối hiểm hoạ cho sự an toàn của mạng.

3. Hệ thống Firewall xây dựng bởi CSE

Bộ chương trình Firewall 1.0 của CSE được đưa ra vào tháng 6/1998. Bộ chương trình này gồm hai thành phần:

- Bộ lọc gói tin – IP Filtering
- Bộ chương trình cổng ứng dụng – proxy servers

Hai thành phần này có thể hoạt động một cách riêng rẽ. Chúng cũng có thể kết hợp lại với nhau để trở thành một hệ thống firewall hoàn chỉnh.

Trong tập tài liệu này, chúng tôi chỉ đề cập đến bộ chương trình cổng ứng dụng đã được cài đặt tại VPCP.

3.1 Tổng quan

Bộ chương trình proxy của CSE (phiên bản 1.0) được phát triển dựa trên bộ công cụ xây dựng Internet Firewall TIS (Trusted Information System) phiên bản 1.3. TIS bao gồm một bộ các chương trình và sự đặt lại cấu hình hệ thống để nhằm mục đích xây dựng một Firewall. Bộ chương trình được thiết kế để chạy trên hệ UNIX sử dụng TCP/IP với giao diện socket Berkeley.

Việc cài đặt bộ chương trình proxy đòi hỏi kinh nghiệm quản lý hệ thống UNIX, và TCP/IP networking. Tối thiểu, người quản trị mạng firewall phải quen thuộc với:

- việc quản trị và duy trì hệ thống UNIX hoạt động
- việc xây dựng các package cho hệ thống

Sự khác nhau khi đặt cấu hình cho hệ thống quyết định mức độ an toàn mạng khác nhau. Người cài đặt firewall phải hiểu rõ yêu cầu về độ an toàn của mạng cần bảo vệ, nắm chắc những rủi ro nào là chấp nhận được và không chấp nhận được, thu lượm và phân tích chúng từ những đòi hỏi của người dùng.

Bộ chương trình proxy được thiết kế cho một số cấu hình firewall, trong đó các dạng cơ bản nhất là dual-home gateway (hình 2.4), screened host gateway(hình 2.5), và screened subnet gateway(hình 2.6). Như chúng ta đã biết, trong những cấu trúc firewall này, yếu tố căn bản nhất là bastion host, đóng vai trò như một người chuyển tiếp thông tin (forwarder), ghi nhật ký truyền thông, và cung cấp các dịch vụ. Duy trì độ an toàn trên bastion host là cực kỳ quan trọng, bởi vì đó là nơi tập trung hầu hết các cố gắng cài đặt một hệ thống firewall.

3.2 Các thành phần của bộ chương trình proxy:

Bộ chương trình proxy gồm những chương trình bậc ứng dụng (application-level programs), hoặc là để thay thế hoặc là được cộng thêm vào phần mềm hệ thống đã có. Bộ chương trình proxy có những thành phần chính bao gồm:

- Smap: dịch vụ SMTP(Simple Mail Tranfer Protocol)
- Netacl: dịch vụ Telnet, finger, và danh mục các điêu khiển truy nhập mạng
- Ftp-Gw: Proxy server cho Ftp
- Telnet-Gw: Proxy server cho Telnet
- Rlogin-Gw: Proxy server cho rlogin
- Plug-Gw: TCP Plug-Board Connection server (server kết nối tức thời dùng thủ tục TCP)

3.2.1 Smap: Dịch vụ SMTP

SMTP được xây dựng bằng cách sử dụng cặp công cụ phần mềm smap và smapd. Có thể nói rằng SMTP chống lại sự đe doạ tới hệ thống, bởi vì các chương trình mail chạy ở mức độ hệ thống để phân phát mail tới các hộp thư của user.

Smap và smapd thực hiện điều đó bằng cách cô lập chương trình mail, bắt nó chạy trên một thư mục dành riêng (restricted directory) qua chroot (thay đổi thư mục gốc), như một user không có quyền ưu tiên. Mục đích của smap là cô lập chương trình mail vốn đã gây ra rất nhiều lỗi trên hệ thống. Phần lớn các công việc xử lý mail thường được

thực hiện bởi chương trình sendmail. Sendmail không yêu cầu một sự thay đổi hay đặt lại cấu hình gì cả. Khi một hệ thống ở xa nối tới một cổng SMTP, hệ điều hành khởi động smap. Smap lập tức chroot tới thư mục dành riêng và đặt user-id ở mức bình thường (không có quyền ưu tiên). Bởi vì smap không yêu cầu hỗ trợ bởi một file hệ thống nào cả, thư mục dành riêng chỉ chứa các file do smap tạo ra. Do vậy, bạn không cần phải lo sợ là smap sẽ thay đổi file hệ thống khi nó chroot. Mục đích duy nhất của smap là đối thoại SMTP với các hệ thống khác, thu lượm thông báo mail, ghi vào đĩa, ghi nhật ký, và thoát.

Smapd có trách nhiệm thường xuyên quét thư mục kho của smap và đưa ra các thông báo đã được xếp theo thứ tự (queued messages) tới sendmail để cuối cùng phân phát. Chú ý rằng nếu sendmail được đặt cấu hình ở mức bình thường, và smap chạy với uucp user-id (?), mail có thể được phân phát bình thường mà không cần smapd chạy với mức ưu tiên cao. Khi smapd phân phát một thông báo, nó xoá file chứa thông báo đó trong kho.

Theo ý nghĩa này, sendmail bị cô lập, và do đó một user lạ trên mạng không thể kết nối với sendmail mà không qua smap. Tuy nhiên, smap và smapd không thể giải quyết vấn đề giả mạo thư hoặc các loại tấn công khác qua mail. Smap có kích thước rất nhỏ so với sendmail (700 dòng so với 20,000 dòng) nên việc phân tích file nguồn để tìm ra lỗi đơn giản hơn nhiều.

3.2.2 Netacl: công cụ điều khiển truy nhập mạng

Chúng ta đã biết rằng inetd không cung cấp một sự điều khiển truy nhập mạng nào cả: nó cho phép bất kỳ một hệ

thống nào trên mạng cũng có thể nối tới các dịch vụ liệt kê trong file *inetd.conf*.

Netacl là một công cụ để điều khiển truy nhập mạng, dựa trên địa chỉ network của máy client, và dịch vụ được yêu cầu. Vì vậy một client (xác định bởi địa chỉ IP hoặc hostname) có thể khởi động telnetd (một version khác của telnet) khi nó nối với cổng dịch vụ telnet trên firewall.

Thường thường trong các cấu hình firewall, netacl được sử dụng để cấm tất cả các máy trừ một vài host được quyền login tới firewall qua hoặc là telnet hoặc là rlogin, và để khoá các truy nhập từ những kẻ tấn công.

Độ an toàn của netacl dựa trên địa chỉ IP và/hoặc *hostname*. Với các hệ thống cần độ an toàn cao, nên dụng địa chỉ IP để tránh sự giả mạo DNS. Netacl không chống lại được sự giả địa chỉ IP qua chuyển nguồn (source routing) hoặc những phương tiện khác. Nếu có các loại tấn công như vậy, cần phải sử dụng một router có khả năng soi những packet đã được chuyển nguồn (screening source routed packages).

Chú ý là netacl không cung cấp điều khiển truy nhập UDP, bởi vì công nghệ hiện nay không đảm bảo sự xác thực của UDP. An toàn cho các dịch vụ UDP ở đây đồng nghĩa với sự không cho phép tất cả các dịch vụ UDP.

Netacl chỉ bao gồm 240 dòng mã C (cả giải thích) cho nên rất dễ dàng kiểm tra và hiệu chỉnh. Tuy nhiên vẫn cần phải cẩn thận khi cấu hình nó.

3.2.3 Ftp-Gw: Proxy server cho Ftp

Ftp-Gw là một proxy server cung cấp điều khiển truy nhập mạng dựa trên địa chỉ IP và/hoặc hostname, và cung cấp

điều khiển truy nhập thứ cấp cho phép tuỳ chọn khoá hoặc ghi nhật ký bất kỳ lệnh ftp nào. Đích cho dịch vụ này cũng có thể tuỳ chọn được phép hay khoá. Tất cả các sự kết nối và byte dữ liệu chuyển qua đều bị ghi nhật kí lại.

Ftp-Gw tự bản thân nó không đe doạ an toàn của hệ thống firewall, bởi vì nó chạy chroot tới một thư mục rỗng, không thực hiện một thủ tục vào ra file nào cả ngoài việc đọc file cấu hình của nó. Kích thước của Ftp-gw là khoảng 1,300 dòng. Ftp gateway chỉ cung cấp dịch vụ ftp, mà không quan tâm đến ai có quyền hay không có quyền kết xuất (export) file. Do vậy, việc xác định quyền phải được thiết lập trên gateway và phải thực hiện trước khi thực hiện kết xuất (export) hay nhập (import) file. Ftp gateway nên được cài đặt dựa theo chính sách an toàn của mạng. Bộ chương trình nguồn cho phép người quản trị mạng cung cấp cả dịch vụ ftp và ftp proxy trên cùng một hệ thống.

3.2.4 Telnet-Gw: Proxy server cho Telnet

Telnet-Gw là một proxy server cung cấp điều khiển truy nhập mạng dựa trên địa chỉ IP và/hoặc hostname, và cung cấp sự điều khiển truy nhập thứ cấp cho phép tuỳ chọn khoá bất kỳ đích nào. Tất cả các sự kết nối và byte dữ liệu chuyển qua đều bị ghi nhật ký lại. Mỗi một lần user nối tới telnet-gw, sẽ có một menu đơn giản của các chọn lựa để nối tới một host ở xa.

Telnet-gw không phương hại tới an toàn hệ thống, vì nó chạy chroot đến môt thư mục dành riêng (restricted directory). File nguồn bao gồm chỉ 1,000 dòng lệnh. Việc xử lý menu là hoàn toàn diễn ra ở trong bộ nhớ, và không

có môt subsell hay chương trình nào tham dự. Cũng không có việc vào ra file ngoài việc đọc cấu hình file. Vì vậy, telnet-gw không thể cung cấp truy nhập tới bản thân hệ thống firewall.

3.2.5 Rlogin-Gw: Proxy server cho rlogin

Các terminal truy nhập qua thủ tục BSD rlogin có thể được cung cấp qua rlogin proxy. rlogin cho phép kiểm tra và điêu khiển truy nhập mạng tương tự như telnet gateway. Rlogin client có thể chỉ ra một hệ thống ở xa ngay khi bắt đầu nối vào proxy, cho phép hạn chế yêu cầu tương tác của user với máy (trong trường hợp không yêu cầu xác thực).

3.2.6 Sql-Gw: Proxy Server cho Oracle Sql-net

Thông thường, việc khai thác thông tin từ CSDL Oracle được tiến hành thông qua dịch vụ WWW. Tuy nhiên để hỗ trợ người sử dụng dùng chương trình *plus33* nối vào máy chủ Oracle, bộ firewall của CSE được đưa kèm vào chương trình Sql-net proxy. Việc kiểm soát truy nhập được thực hiệu qua tên máy hay địa chỉ IP của máy nguồn và máy đích.

3.2.7 Plug-Gw: TCP Plug-Board Connection server

Firewall cung cấp các dịch vụ thông thường như Usernet news. Người quản trị mạng có thể chọn hoặc là chạy dịch vụ này trên bản thân firewall, hoặc là cài đặt một proxy server. Do chạy news trực tiếp trên firewall dễ gây lỗi hệ thống trên phần mềm này, cách an toàn hơn là sử dụng proxy. Plug-gw được thiết kế cho Usernet News.

Plug-gw có thể được đặt cấu hình để cho phép hay từ chối một sự kết nối dựa trên địa chỉ IP hoặc là hostname. Tất cả sự kết nối và các byte dữ liệu chuyển qua đều được ghi nhật ký lại.

3.3 Cài đặt

Bộ cài đặt gồm 2 đĩa mềm 1.44 Mb, R1 và R2. Mỗi bộ cài đặt đều có một số *Serial number* khác nhau và chỉ hoạt động được trên máy có *hostname* đã xác định trước. Việc cài đặt được tiến hành bình thường bằng cách dùng lệnh *custom*.

Khi cài đặt, một người sử dụng có tên là *proxy* được đăng ký với hệ thống để thực hiện các chức năng quản lý proxy. Người cài đặt phải đặt mật khẩu cho user này.

Một thư mục */usr/proxy* được tự động thiết lập, trong đó có các thư mục con:

- *bin* để chứa các chương trình thực hiện
- *etc* để chứa các tệp cấu hình Firewall và một số ví dụ các file cấu hình của hệ thống khi chạy với Firewall như *inetd.conf, services*, *syslog.conf*
- *log* để chứa các tệp nhật ký
- *report* để chứa các tệp báo cáo sau này.

Việc đặt cấu hình và quản trị CSE Firewall đều thông qua các chức năng trên *menu* khi *login* vào máy Firewall bằng tên người sử dụng là *proxy.* Sau khi cài đặt nên đổi tên những tệp hệ thống và lưu lại trước khi đặt cấu hình:

- */etc/inetd.conf*
- */etc/services*
- */etc/syslog.conf.*

3.4 Thiết lập cấu hình:

3.4.1 Cấu hình mạng ban đầu

Với Firewall host-base Chúng ta có thể chắc chắn vào việc mạng được cài đặt theo một chính sách an toàn được lựa chọn nhằm ngăn cản mọi luồng thông tin không mong muốn giữa mạng được bảo vệ và mạng bên ngoài. Điều này có thể được thực hiện bởi screening router hay dual-home gateway. Thông thường, các thiết bị mạng đều sử dụng cơ chế an toàn cài đặt trên router nơi mà mọi liên kết đều phải đi qua.

Một điều cần quan tâm là trong khi đang cài đặt, những máy chủ công khai (Firewall bastion host) có thể bị tấn công trước khi cơ chế an toàn của nó được cấu hình hoàn chỉnh để có thể chạy được. Do đó, nên cấu hình tệp *inetd.conf* để cấm tất cả các dịch vụ mạng từ ngoài vào và sử dụng thiết bị đầu cuối để cài đặt.

Tại thời điểm đó, chúng ta có thể quy định những truy nhập giữa mạng được bảo vệ và mạng bên ngoài nào sẽ bị khoá. Tuỳ theo mục đích, chúng ta có thể ngăn các truy nhập tuỳ theo hướng của chúng. Chương trình cũng cần được thử nghiệm kỹ càng trước khi sử dụng. Nếu cần thiết có thể dùng chương trình */usr/proxy/bin/netscan* để thử kết nối tới tất cả máy tính trong mạng con để kiểm tra. Nó sẽ cố gắng thử lọt qua Firewall theo mọi hướng để chắc chắn rằng các truy nhập bất hợp pháp là không thể xảy ra. Ngăn cấm truy nhập vào ra là cái chốt trong cơ chế an toàn của Firewall không nên sử dụng nếu nó chưa được cài đặt và thử nghiệm kỹ lưỡng.

3.4.2 Cấu hình cho Bastion Host

Một nguyên nhân cơ bản của việc xây dựng Firewall là để ngăn chặn các dịch vụ không cần thiết và các dịch vụ không nắm rõ. Ngăn chặn các dịch vụ không cần thiết đòi hỏi người cài đặt phải có hiểu biết về cấu hình hệ thống. Các bước thực hiện như sau:

- Sửa đổi tệp */etc/inetd.conf, /etc/services, /etc/syslog.conf, /etc/sockd.conf*.
- Sửa đổi cấu hình hệ diều hành, loại bỏ những dịch vụ có thể gây lỗi như NFS, sau đó rebuild kernel.

Việc này được thực hiện cho tới khi hệ thống cung cấp dịch vụ tối thiểu mà người quản trị tin tưởng. Việc cấu hình này có thể làm đồng thời với việc kiểm tra dịch vụ nào chạy chính xác bằng cách dùng các lệnh *ps* và *netstat.* Phần lớn các server được cấu hình cùng với một số dạng bảo mật khác, các cấu hình này sẽ mô tả ở phần sau. Một công cụ chung để thăm dò các dịch vụ TCP/IP là */usr/proxy/bin/portscan* có thể dùng để xem dịch vụ nào đang được cung cấp. Nếu không có yêu cầu đặc biệt có thể dùng các file cấu hình nói trên đã được tạo sẵn và đặt tại */usr/proxy/etc* khi cài đặt, ngược lại có thể tham khảo để sửa đổi theo yêu cầu.

Toàn bộ các thành phần của bộ Firewall đòi hỏi được cấu hình chung (mặc định là */usr/proxy/etc/netperms*). Phần lớn các thành phần của bộ Firewall được gọi bởi dịch vụ của hệ thống là *inetd*, khai báo trong /etc/inetd.conf tương tự như sau:

ftp	stream	tcp	nowait	root	/usr/proxy/bin/netacl	ftpd
ftp-gw	stream	tcp	nowait	root	/usr/proxy/bin/ftp-gw	ftp-gw
telnet-a	stream	tcp	nowait	root	/usr/proxy/bin/netacl	telnetd
telnet	stream	tcp	nowait	root	/usr/proxy/bin/tn-gw	tn-gw
login	stream	tcp	nowait	root	/usr/proxy/bin/rlogin-gw	rlogin-gw
finger	stream	tcp	nowait	nobody	/usr/proxy/bin/netacl	fingerd
http	stream	tcp	nowait	root	/usr/proxy/bin/netacl	httpd
smtp	stream	tcp	nowait	root	/usr/proxy/bin/smap	smap

Chương trình netacl là một vỏ bọc TCP (TCP Wrapper) cung cấp khả năng điều khiển truy cập cho những dịch vụ TCP và cũng sử dụng một tệp cấu hình với Firewall.

Bước đầu tiên để cấu hình netacl là cho phép mạng nội bộ truy nhập có giới hạn vào Firewall, nếu như nó cần thiết cho nhu cầu quản trị. Tuỳ thuộc vào TELNET gateway tn-gw có được cài đặt hay không, quản trị có thể truy cập vào Firewall qua cổng khác với cổng chuẩn của telnet (23). Bởi vì telnet thường không cho phép chương trình truy cập tới một cổng không phải là cổng chuẩn của nó. Dịch vụ proxy sẽ chạy trên cổng 23 và telnet thực sự sẽ chạy trên cổng khác ví dụ dịch vụ có tên là telnet-a ở trên (Xem file *inetd.conf* ở trên). Có thể kiểm tra tính đúng đắn của netacl bằng cách cấu hình cho phép hoặc cấm một số host rồi thử truy cập các dịch vụ từ chúng.

Mỗi khi netacl được cấu hình, TELNET và FTP gateway cần phải được cấu hình theo. Cấu hình TELNET gateway chỉ đơn giản là coi nó như một dịch vụ và trong *netacl.conf* viết một số miêu tả hệ thống nào có thể sử dụng nó. Trợ giúp có thể được cung cấp cho người sử dụng khi cần thiết. Việc cấu hình FTP proxy cũng như vậy. Tuy nhiên, FTP có

thể sử dụng cổng khác không giống TELNET. Rất nhiều các FTP client hỗ trợ cho việc sử dụng cổng không chuẩn.

Dịch vụ rlogin là một tuỳ chọn có thể dùng và phải được cài đặt trên cổng ứng dụng của bastion host (cổng 512) giao thức rlogin đòi hỏi một cổng đặc biệt, một quá trình đòi hỏi sự cho phép của hệ thống UNIX. Người quản trị muốn sử dụng cơ chế an toàn phải cài đặt thư mục cho proxy để nó giới hạn nó trong thư mục đó.

Smap và smapd là các tiến trình lọc thư có thể được cài đặt sử dụng thư mục riêng của proxy để xử lý hoặc sử dụng một thư mục nào đó trong hệ thống. Smap và smapd không thay thế sendmail do đó vẫn cần cấu hình sendmail cho Firewall. Việc này không mô tả trong tài liệu này.

3.4.3 Thiết lập tập hợp quy tắc

Khi cấu hình cho proxy server và chương trình điều khiển truy cập mạng điều cần thiết là thiết lập chính xác tập quy tắc để thể hiện đúng với mô hình an toàn mong muốn. Một cách tốt để bắt đầu cấu hình Firewall là để mọi người trong mạng sử dụng tự do các dịch vụ đồng thời cấm tất cả mọi người bên ngoài. Việc đặt cấu hình cho firewall không quá rắc rối, vì nó được thiết kế để hỗ trợ cho mọi hoàn cảnh. Tệp tin */usr/proxy/etc/netperms* là CSDL cấu hình và quyền truy nhập (configuration/permissions) cho các thành phần của Firewall: netacl, smap, smapd, ftp-gw, tn-gw, http-gw, và plug-gw. Khi một trong các ứng dụng này khởi động, nó đọc cấu hình và quyền truy nhập của nó từ netperms và lưu trữ vào một CSDL trong bộ nhớ.

File *configuration/permissions* được thiết lập thành những quy tắc, mỗi quy tắc chứa trên một dòng. Phần đầu tiên của

mỗi quy tắc là tên của ứng dụng, tiếp theo là dấu hai chấm (":"). Nhiều ứng dụng có thể dùng chung một quy tắc với tên ngăn cách bởi dấu phảy. Dòng chú thích có thể chèn vào file cấu hình bằng cách thêm vào đầu dòng ký tự '#'.

3.4.3.1 Thiết lập tập hợp các quy tắc cho dịch vụ HTTP, FTP

Việc thiết lập cấu hình cho các dịch vụ HTTP, FTP là tương tự như nhau. Chúng tôi chỉ đưa ra chi tiết về thiết lập cấu hình và quy tắc cho dịch vụ FTP.

```
#Example ftp gateway rules:
#--------------------------------
ftp-gw:        denial-msg          /usr/proxy/etc/ftp-deny.txt
ftp—gw:        welcome-msg         /usr/proxy/etc/ftp-welcome.txt
ftp-gw:        help-msg            /usr/proxy/etc/ftp-help.txt
ftp-gw:        permit-hosts     10.10.170.* -log {retr stor}
ftp-gw:        timeout 3600
```

Trong ví dụ trên, mạng 10.10.170 được cho phép dùng proxy trong khi mọi host khác không có trong danh sách, mọi truy cập khác đều bị cấm. Nếu một mạng khác muốn truy cập proxy, nó nhận được một thông báo từ chối trong */usr/proxy/etc/ftp-deny.txt* và sau đó liên kết bị ngắt. Nếu mạng được bảo vệ phát triển thêm chỉ cần thêm vào các dòng cho phép.

```
ftp-gw:        permit-hosts  16.67.32.* -log {retr stor}
```

or

```
ftp-gw:        permit-hosts  16.67.32.* -log {retr stor}
ftp-gw:        permit-hosts  10.10.170.* -log {retr stor}
```

Mỗi bộ phận của Firewall có một tập các tuỳ chọn và cờ được mô tả trong manual page riêng của phần đó. Trong ví dụ trên, Tuỳ chọn -log {retr stor} cho phép FTP proxy ghi lại nhật ký với tuỳ chọn *retr* và *stor*.

3.4.3.2 Anonymous FTP

Anonymous FTP server đã được sử dụng trong hệ điều hành UNIX từ lâu. Các lỗ hổng trong việc bảo đảm an toàn (Security hole) thường xuyên sinh ra do các chức năng mới được thêm vào, sự xuất hiện của bug và do cấu hình sai. Một cách tiếp cận với việc đảm bảo an toàn cho anonymous FTP là sử dụng netacl để chắc chắn FTP server bị hạn chế trong thư mục của nó trước khi được gọi. Với cấu hinh như vậy, khó khăn cho anonymous FTP làm tổn hại đến hệ thống bên ngoài khu vực của FTP.

Dưới đây là một ví dụ sử dụng netacl để quyết định giới hạn hay không giới hạn vùng sử dụng của FTP đối với mỗi liên kết. Giả sử là mạng được bảo vệ là 192.5.12

```
netacl-ftpd:    hosts 192.5.12.*        -exec /etc/ftpd
netacl-ftpd:    hosts unknown           -exec /bin/cat /usr/proxy/etc/noftp.txt
netacl-ftpd:    hosts *                 -chroot /ftpdir -exec /etc/ftpd
```

Trong ví dụ này, người dùng nối với dịch vụ FTP từ mạng được bảo vệ có khả năng FTP bình thường. Người dùng kết nối từ hệ thống khác domain nhận được một thông báo rằng họ không có quyền sử dụng FTP. Mọi hệ thống khác kết nối vào FTP đều sử dụng với vùng file FTP. Điều này có một

số thuận lợi cho việc bảo đảm an toàn. Thứ nhất, khi kiểm tra xác thực, ftpd kiểm tra mật khẩu của người sử dụng trong vùng FTP, cho phép người quản trị đưa ra "account" cho FTP. Điều này cần thiết cho những người không có account trong bastion host cung cấp sự kiểm tra và xác thực nó còn cho phép quản trị sử dụng những điểm mạnh của ftpd cho dù nó chứa một số lỗ hổng về an toàn.

3.4.3.3 Telnet và rlogin

Nói chung truy cập tới bastion host nên bị cấm, chỉ người quản trị có quyền login. Thông thường để khi chạy proxy, chương trình telnet và rlogin không thể chạy trên các cổng chuẩn của chúng. Có 3 cách giải quyết vấn đề này:

- Chạy telnet và rloggin proxy trên cổng chuẩn với telnet và rlogin trên cổng khác và bảo vệ truy cập tới chúng bằng netacl
- Cho phép login chỉ với thiết bị đầu cuối.
- Dùng netacl để chuyển đổi tuỳ thuộc vào điểm xuất phát của kết nối, dựa trên proxy để thực hiện kết nối thực sự.

Cách giải quyết cuối cùng rất tiện lợi nhưng cho phép mọi người có quyền dùng proxy để login vào bastion host. Nếu bastion host sử dụng xác thực mức cao để quản lý truy cập của người dùng, sự rủi ro do việc tấn công vào hệ bastion host sẽ được giảm thiểu. để cấu hình hệ thống trước hết, tất cả các thiết bị được nối vào hệ thống qua netacl và dùng nó gọi các chương trình server hay proxy server tuỳ thuộc vào nơi xuất phát của kết nối.

Người quản trị muốn vào bastion host trước hết phải kết nối vào netacl sau đó ra lệnh kết nối vào bastion host. Việc này

đơn giản vì một số bản telnet và rlogin không làm việc nếu không được kết nối vào đúng cổng.

```
netacl-telnetd:     permit-hosts     127.0.0.1      -exec /etc/telnetd
netacl-telnetd:     permit-hosts     myaddress      -exec /etc/telnetd
netacl-telnetd:     permit-hosts     *              -exec /usr/proxy/bin/tn-gw
netacl-rlogin:      permit-hosts     127.0.0.1      -exec /etc/rlogin
netacl-rlogin:      permit-hosts     myaddress      -exec /etc/rlogin
netacl-rlogin:      permit-hosts     *              -exec /usr/proxy/bin/rlogin-gw
```

3.4.3.4 Sql-net proxy

Giả thiết là có hai CSDL STU nằm trên máy 190.2.2.3 và VPCP nằm trên máy 190.2.0.4.

Để cấu hình cho *sql-net proxy*, phải tiến hành các bước như sau:

3.4.3.4.1 Cấu hình trên firewall

- Đặt cấu hình cho tệp netperms như sau:

```
#Oracle proxy for STU Database
ora_stu1:       timeout 3600
ora_stu1:       port 1521 * -plug-to 190.2.2.3 -port 1521
ora_stu2:       timeout 3600
ora_stu2:       port 1526 * -plug-to 190.2.2.3 -port 1526

#Oracle proxy for VBPQ Database
```

ora_vpcp1: timeout 3600

ora_vpcp1: port 1421 * -plug-to 190.2.0.4 -port 1521

ora_vpcp2: timeout 3600

ora_vpcp2: port 1426 * -plug-to 190.2.0.4 -port 1526

- Đặt lại tệp */etc/services* như sau:

#Oracle Proxy for STU Database

ora_stu1 1521/tcp oracle proxy

ora_stu2 1526/tcp oracle proxy

#Oracle Proxy for VBPQ Database

ora_vpcp1 1421/tcp oracle proxy

ora_vpcp2 1426/tcp oracle proxy

- Đặt lại tệp */etc/inetd.conf* như sau:

#Oracle Proxy for VBPQ Database

ora_stu1 stream tcp nowait root /usr/proxy/bin/plug-gw ora_stu1

ora_stu2 stream tcp nowait root /usr/proxy/bin/plug-gw ora_stu2

#Oracle Proxy for VBPQ Database

ora_vpcp1 stream tcp nowait root /usr/proxy/bin/plug-gw ora_vpcp1

ora_vpcp2 stream tcp nowait root /usr/proxy/bin/plug-gw ora_vpcp2

- Đặt lại tệp */etc/syslog.conf* như sau:

#Logfile for Sql-gw

"sql-gw" /usr/proxy/log/plug-gw

3.4.3.4.2 Cấu hình trên máy trạm

- Đặt lại tệp *oracle_home\network\admin\tnsnames.ora* như sau:

```
#Logfile for Sql-gw
stu.world =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = tcp.world)
        (PROTOCOL = TCP)
        (Host = firewall)
        (Port = 1521)
      )
      (ADDRESS =
        (COMMUNITY = tcp.world)
```

```
        (PROTOCOL = TCP)
        (Host = firewall)
        (Port = 1526)
      )
    )
    (CONNECT_DATA = (SID = STU)
    )
  )

vpcp.world =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS =
        (COMMUNITY = tcp.world)
        (PROTOCOL = TCP)
        (Host = firewall)
        (Port = 1421)
      )
      (ADDRESS =
        (COMMUNITY = tcp.world)
        (PROTOCOL = TCP)
        (Host = firewall)
        (Port = 1426)
      )
    )
    (CONNECT_DATA = (SID = ORA1)
```

)

)

Bạn có thể dễ dàng mở rộng cho nhiều CSDL khác nằm trên nhiều máy khác nhau.

3.4.3.5 Các dịch vụ khác

Tương tự như trên là các ví dụ cấu hình cho các dịch vụ khác khai báo trong file *netperms:*

```
#  finger gateway rules:
# ---------------------
netacl-fingerd: permit-hosts 190.2.* ws1 -exec /etc/fingerd
netacl-fingerd: deny-hosts * -exec /bin/cat /usr/proxy/etc/finger.txt
#  http gateway rules:
# ---------------------
netacl-httpd: permit-hosts * -exec /usr/proxy/bin/http-gw
http-gw:        timeout 3600
#http-gw:       denial-msg      /usr/proxy/etc/http-deny.txt
#http-gw:       welcome-msg     /usr/proxy/etc/http-welcome.txt
#http-gw:       help-msg        /usr/proxy/etc/http-help.txt
http-gw:        permit-hosts 190.2.* 10.* 192.2.0.* -log { all }
http-gw:        deny-hosts 220.10.170.32 ws1
http-gw:        default-httpd hpnt
#
#  smap (E-mail) rules:
```

```
# ----------------------
smap, smapd:    userid root
smap, smapd:    directory /usr/spool/mail
smapd:          executable /usr/proxy/bin/smapd
smapd:          sendmail /usr/lib/sendmail
smap:           timeout 3600
#
```

Ngoài ra, trong CSE Firewall còn có dịch vụ socks để kiểm soát các phần mềm ứng dụng đặc biệt như Lotus Notes. Cần phải thêm vào các file cấu hình hệ thống như sau:

File */etc/services:*

```
socks          1080/tcp
```

File */etc/inetd.conf:*

```
 socks          stream    tcp     nowait     root        /etc/sockd          sockd
```

Cấu hình và quy tắc cho dịch vụ này nằm ở file */etc/sockd.conf*, chỉ có hai từ khoá cần phải quan tâm là permit và deny để cho phép hay không các host đi qua, dịch vụ này không kết hợp với dịch vụ xác thực. Địa chỉ IP và Netmask đặt trong file này giống như với lệnh dẫn đường *route* của UNIX.

```
permit  190.2.0.0 255.255.0.0
permit  10.10.170.50 255.255.255.255
permit  10.10.170.40 255.255.255.255
permit  10.10.170.31 255.255.255.255
deny    0.0.0.0 0.0.0.0 : mail -s 'SOCKD: rejected -- from %u@%A to host %Z
(service %S)' root
```

3.4.4 Xác thực và dịch vụ xác thực

Bộ Firewall chứa chương trình server xác thực được thiết kế để hỗ trợ cơ chế phân quyền. Authsrv chứa một cơ sở dữ liệu về người dùng trong mạng, mỗi bản ghi tương ứng với một người dùng, chứa cơ chế xác thực cho mỗi anh ta, trong đó bao gồm tên nhóm, tên đầy đủ của người dùng, lần truy cập mới nhất. Mật khẩu không mã hoá (Plain text password) được sử dụng cho người dùng trong mạng để việc quản trị được đơn giản. Mật khẩu không mã hoá không nên dùng với những người sử dụng từ mạng bên ngoài. Authsrv được chạy trên một host an toàn thông thường là bastion host. Để đơn giản cho việc quản trị authsrv người quản trị có thể sử dụng một shell *authmsg* để quản trị cơ sở dữ liệu có cung cấp cơ chế mã hoá dữ liệu.

Người dùng trong 1 cơ sở dữ liệu của authsrv có thể được chia thành các nhóm khác nhau được quản trị bởi quản trị nhóm là người có toàn quyền trong nhóm cả việc thêm, bớt người dùng. Điều này thuận lợi khi nhiều tổ chức cùng dùng chung một Firewall.

Để cấu hình authsrv, đầu tiên cần xác định 1 cổng TCP trống và thêm vào một dòng vào trong inetd.conf để gọi authsrv mỗi khi có yêu cầu kết nối. Authsrv không phải một tiến trình deamon chạy liên tục, nó là chương trình được gọi mỗi khi có yêu cầu và chứa một bản sao CSDL để tránh rủi ro. Thêm authsrv vào inet.conf đòi hỏi tạo thêm điểm vào trong */etc/services.* Vì authsrv không chấp nhận tham số, mà phải thêm vào inetd.conf và services các dòng như sau:

Trong */etc/services:*

authsrv 7777/tcp

Trong */etc/inetd.conf:*

authsrv stream tcp nowait root /usr/proxy/bin/authsrv authsrv

Cổng dịch vụ dùng cho authsvr sẽ được dùng để đặt cấu hình cho các ứng dụng client có sử dụng dịch vụ xác thực. Dịch vụ xác thực không cần áp dụng cho tất cả các dịch vụ hay tất cả các client.

#Example ftp gateway rules:

ftp-gw:	authserver	local host 7777
ftp-gw:	denial-msg	/usr/proxy/etc/ftp-deny.txt
ftp-gw:	welcome-msg	/usr/proxy/etc/ftp-welcome.txt
ftp-gw:	help-msg	/usr/proxy/etc/ftp-help.txt
ftp-gw:	permit-host	192.33.112.100
ftp-gw:	permit-host	192.33.112.* -log {retr stor} -auth {stor}
ftp-gw:	permist-host	* -authall
ftp-gw:	timeout	36000

Trong ví dụ trên, xác thực dùng với FTP proxy. Dòng đầu tiên định nghĩa địa chỉ mạng cổng dịch vụ của chương trình xác thực. Dòng permist-host cho thấy một trong số sự mềm dẻo của hệ thống xác thực, một host được lựa chọn để không phải chịu cơ chế xác thực, người dùng từ host này có thể truy cập tự do tới mọi dịch vụ của proxy. Permist-host thứ 2 đòi hỏi xác thực mọi hệ thống trong mạng 192.33.112 muốn truyền ra ngoài với -auth {store} những thao tác của FTP sẽ bị khoá tới khi người dùng hoàn thành việc xác thực

với server. Khi đó, lệnh được mở khoá và người dùng có thể vào hệ thống. Ví dụ cuối định nghĩa mọi người có thể nối với server nhưng trước hết họ phải được xác thực.

Authsrv server phải được cấu hình để biết máy nào được cho phép kết nối. Điều này cấm tất cả những cố gắng truy nhập bất hợp pháp vào server từ những server không chạy những phần mềm xác thực. Trong Firewall authsrv sẽ chạy trên bastion host cùng với proxy trên đó. Nếu không có hệ thống nào đòi hỏi truy cập, mỗi client và server coi "local host" như một địa chỉ truyền thông. Cấu hình authsrv định nghĩa nó sẽ vận hành CSDL và client hỗ trợ.

#Example authhsrv rules:

authsrv:	database	/usr/proxy/bin/authsrv.db
authsrv:	permit-host	localhost
authsrv:	permit-host	192.5.214..32

Trong ví dụ trên, đường dẫn tới CSDL định nghĩa và 2 host được nhận ra. Chú ý CSDL ở trên trong hệ thống được bảo vệ hoặc được bảo vệ nghiêm ngặt bởi cơ chế truy cập file. Bảo vệ CSDL rất quan trọng do đó nên để CSDL trên bastion host. Lối vào thứ 2 là một ví dụ về client sử dụng mã hoá DES trong khi truyền thông với authsrv. Khoá mã chứa trong tệp cấu hình đòi hỏi file cấu hình phải được bảo vệ. Nói chung, việc mã hoá là không cần thiết. Kết quả của việc mã hoá là cho phép quản trị có thể quản lý cơ sở dữ liệu xác thực từ trạm làm việc. Luồng dữ liệu duy nhất cần phải bảo vệ là khi người quản trị mạng đặt lại mật khẩu qua

mạng cục bộ, hay khi quản lý cơ sở dữ liệu xác thực qua mạng diện rộng.

Duy trì CSDL xác thực dựa vào 2 công cụ authload và authdump để load và dump CSDL xác thực. Người quản trị nên chạy authdump trong crontab tạo bản sao dạng ASCII của CSDL để tránh trường hợp xấu khi CSDL bị hỏng hay bị xoá.

Authsrv quản lý nhóm rất mềm dẻo, quản trị có thể nhóm người dùng thành nhóm dùng "group wiz", người có quyền quản trị nhóm có thể xoá, thêm, tạo sửa bản ghi trong nhóm, cho phép hay cấm người dùng, thay đổi password của mật khẩu của user trong nhóm của mình. Quản trị nhóm không thay đổi được người dùng của nhóm khác, tạo ra nhóm mới hay thay đổi quan hệ giữa các nhóm. Quản trị nhóm chỉ có quyền hạn trong nhóm của mình. Việc này có ích đối với tổ chức có nhiều nhóm làm việc cùng sử dụng Firewall.

Tạo một người sử dụng bằng lệnh "adduser"

adduser mrj 'Marcus J. Ranum'

Khi một user record mới được tạo nó chưa được hoạt động và người sử dụng chưa thể login. Trước khi người sử dụng login, quản trị mạng có thể thay đổi mật khẩu và số hiệu nhóm của người sử dụng đó

group users mjr

password "whumpus" mjr

proto SecurID mjr

enable mjr

Khi một user record tạo ra bởi người quản trị nhóm, nó thừa hưởng số hiệu nhóm cũng như giao thức xác thực. User record có thể xem bởi lệnh "display" hay "list".

Ví dụ một phiên làm việc với Authmsg:

%-> authmgs

Connected to server

authmgr-> **login**

Username: **wizard**

Challenge "200850" : 182312

Logged in

authmgs-> disp wizard

Report for user wizard (Auth DBA)

Last authenticated: Fri Oct 8 17:11:07 1993

Authentication protocol: Snk

Flags: WIZARD

authmgr-> **list**

Report for user in database

user	group	longname	flags	proto	last
wizard	users	Auth DBA	y W	Snk	Fri Oct 8 17:02:56 1993
avolio	users	Fred Avolio	y	passwd	Fri Sep 24 10:52:14 1993
rnj	users	Robert N. Jesse	y	passwd	Wed Sep 29 18:35:45 1993
mjr	users	Marcus J. Ranum	y	none	ri Oct 8 17:02:10 1993

authmgr-> adduser dalva "Dave dalva"

ok - user added initially disable

authmgr-> enable dalva

enabled

authmgr-> group dalva users

set group

authmgr-> proto dalva Skey

changed

authmgr-> disp dalva

Report for user dalva, group users (Dave Dalva)

Authentication protocol: Skey

Flags: none

authmgr-> password dalva

Password: #######

Repeat Password: #######

ID dalva s/key is 999 sol32

authmgr-> **quit**

Trong ví dụ trên quản trị nối vào authsrv qua mạng sử dụng giao diện authmsg sau khi xác thực user record hiển thị thời gian xác thực. Sau khi login, list CSDL user, tạo người dùng, đặt password, enable và đưa vào nhóm.

Khởi tạo CSDL Authsrv:

authsrv

-administrator mode-

authsrv# **list**

Report for user in database

user group longname flags proto last

--- ----- -------- ----- ----- ---

authsrv# adduser admin ‘Auth DBA’

ok - user added initially disable

authsrv# enable admin

enabled

authsrv# superwiz admin

set wizard

authsrv# proto admin Snk

changed

authsrv# pass ‘160 270 203 065 022 034 232 162’ admin

Secret key changed

authsrv# **list**

Report for user in database

user group longname flags roto last

--- ----- -------- ----- ---- ---

admin Auth DBA y W Snk never

authsrv# **quit**

Trong ví dụ, một CSDL mới được tạo cùng với một record cho người quản trị. Người quản trị được gán quyền, gán protocol xác thực.

3.4.5 Sử dụng màn hình điều khiển CSE Proxy:

Sau khi cài đặt xong, khi login vào user *proxy* màn hình điều khiển sẽ hiện nên menu các chức năng để người quản trị có thể lựa chọn.

PROXY SERVICE MENU

1 Configuration

2 View TELNET log

3 View FTP log

4 View HTTP log

5 View E-MAIL log

6 View AUTHENTICATE log

7 View FINGER log

8 View RLOGIN log

9 View SOCKD log

a Report

b Authentication

c Change system time

d Change password

e Shutdown

q Exit

Select option> _

Con số hay chữ cái đầu tiên thể hiện phím bấm để thực hiện chức năng. Sau khi mỗi chức năng thực hiện xong xuất hiện

thông báo Press ENTER to continue rồi chờ cho tới khi phím Enter được bấm để trở lại màn hình điều khiển chính.

3.4.5.1 1 Configuration

Chức năng này cho phép soạn thảo trực tiếp tới file cấu hình của proxy. Trong file này chứa các quy tắc của các dịch vụ như netacl, ftp-gw, tn-gw... Cú pháp của các quy tắc này đã được mô tả ở phần trên. Sau khi sử đổi các quy tắc chọn chức năng Save thì các quy tắc mới sẽ lập tức được áp dụng.

Chú ý: Bộ soạn thảo văn bản để soạn thảo file cầu hình có các phím chức năng tương tự như chức năng soạn thảo của Turbo Pascal 3.0. (Các chức năng cần thiết đều có thể thấy trên Status Bar ở dòng cuối cùng của màn hình). Đối với một số trường hợp bộ soạn thảo này không hoạt động thì chương trình soạn thảo *vi* của UNIX sẽ được dùng để thay thế.

3.4.5.2 2 View TELNET log

Chức năng xem nội dung nhật ký của tn-gw. Nhật ký ghi lại toàn bộ các truy nhập qua proxy đối với dịch vụ tn-gw. Đối với các dịch vụ khác như ftp-gw, http-gw đều dược ghi lại nhật ký và có thể theo dõi bởi các chức năng tương tự (Xem các mục dưới đây).

3.4.5.3 3 View FTP log

Chức năng xem nội dung nhật ký của ftp-gw.

3.4.5.4 4 View HTTP log

Chức năng xem nội dung nhật ký của http-gw.

3.4.5.5 5 View E-MAIL log

Chức năng xem nội dung nhật ký của dịch vụ email.

3.4.5.6 6 View AUTHENTICATE log

Chức năng xem nội dung nhật ký của dịch vụ xác thực.

3.4.5.7 7 View FINGER log

Chức năng xem nội dung nhật ký của finger.

3.4.5.8 8 View RLOGIN log

Chức năng xem nội dung nhật ký của rlogin-gw.

3.4.5.9 9 View SOCKD log

Chức năng xem nội dung nhật ký của sockd.

3.4.5.10 a Report

Chức năng làm báo cáo thống kê đối với tất cả các dịch vụ trong một khoảng thời gian nhất định.

Đầu tiên màn hình sẽ hiện lên một lịch để chọn khoảng thời gian muốn làm báo cáo. Sau khi tính toán xong báo cáo. Người sử dụng sẽ phải chọn một trong các đầu ra của báo cáo gồm : xem (đưa ra màn hình), save (ra đĩa mềm) hay print (in ra máy in gắn trực tiếp với máy server). Nếu muốn in từ các máy in khác ta có thể đưa ra đĩa mềm rồi in các tệp đó từ các trạm làm việc.

Fri May 8 10:39:13 1998

Apr							May							Jun						
S	M	Tu	W	Th	F	S	S	M	Tu	W	Th	F	S	S	M	Tu	W	Th	F	S
	1	2	3	4				1	2						1	2	3	4	5	6

5 6 7 8 9 10 11 3 4 5 6 7 8 9 7 8 9 10 11 12 13

12 13 14 15 16 17 18 10 11 12 13 14 15 16 14 15 16 17 18 19 20

19 20 21 22 23 24 25 17 18 19 20 21 22 23 21 22 23 24 25 26 27

26 27 28 29 30 24 25 26 27 28 29 30 28 29 30

31

From date (dd/mm[/yy]) (08/05/98):**01/05/98**

To date (dd/mm[/yy]): (08/05/98):**05/05/09**

Calculating...

View, save to MS-DOS floppy disk or print report (v/s/p/q)? **v**

3.4.5.11 b Authentication

Chức năng này gọi *authsrv* để quản trị người sử dụng và chức năng xác thực cho người đó. *authrv* đã được mô tả khá rõ ràng ở trên.

authsrv# **list**

Report for users in database

user	group	longname	status	proto	last
dalva	cse		n	passw	never
ruth	cse		y	passw	never

authsrv#

3.4.5.12 c Change system time

Chức năng đổi thời gian hệ thống. Chức năng này có tác dụng điều chỉnh chính xác giờ của hệ thống. Bởi vì giờ hệ thống có ảnh hưởng quan trọng tới độ chính xác của nhật ký. Giúp cho người quản trị có thể theo dõi đúng các truy nhập tới proxy.

Dòng nhập thời gian sẽ như dưới đây. Ngày tháng năm có thể không càn nhập nhưng cần chú ý tới dạng của số đưa vào. Dưới đây là ví dụ đổi giờ thành 11 giờ 28.

Current System Time is Fri May 08 10:32:00 HN 1998

Enter new time ([yymmdd]hhmm): **1128**

3.4.5.13 d Change password

Chức năng đổi mật khẩu của *user proxy.*

3.4.5.14 e Shutdown

Chức năng *shut down* toàn bộ hệ thống. Chức năng này được dùng để tắt máy một cách an toàn đối với người sử dụng.

3.4.5.15 q Exit

Chức năng này *logout* khỏi màn hình điều khiển *proxy*.

3.4.6 Các vấn đề cần quan tâm với người sử dụng

Với người sử dụng, khi dùng CSE Proxy cần phải quan tâm đến các vấn đề sau:

3.4.6.1 Với các Web Browser

Cần phải đặt chế độ proxy để chúng có thể truy nhập đến các trang Web thông qua proxy.

Trong **Microsoft Internet Explore** (version 4.0) ta phải chọn View -> Internet option -> Connection -> Proxy Server và đặt chế độ Access the Internet using a proxy, đặt địa chỉ IP và port của proxy vào.

Trong **Netscape Nevigator** (version 4.0) ta phải chọn Edit ->Preferences -> Advanced -> Proxies và đặt địa chỉ proxy và cổng dịch vụ (port) (80) qua phần Manual proxy configuration.

3.4.6.2 Với người sử dụng telnet,

Nếu không được đặt chức năng xác thực thì quá trình như sau:

$ telnet vectra

Trying 192.1.1.155...

connect hostname [serv/ port]

connect to vectra.

Escape character is'^]'.

Vectra.sce.gov.vn telnet proxy (version V1.0) ready:

tn-gw -> **help**

Valid commands are: (unique abbreviations may be used)

connect hostname [serv/ port]

telnet hostname [serv/ port]

x-gw [hostname/ display]

help/ ?

quit/ exit

password

tn-gw -> c 192.1.1.1

Trying 192.1.1.1 port 23...

SCO Openserver ™ Release 5 (sco5.cse.gov.vn) (ttysO)

Login: **ngoc**

password: **#######**

...

$

Nếu có dùng chức năng xác thực, thì sau khi máy proxy trả lời:

Vectra.sce.gov.vn telnet proxy (version V1.0) ready:

Nhắc ta phải đưa vào tên và mật khẩu để thực hiện xác thực:

Username: **ngoc**

password: **#######**

Login accepted

tn-gw ->

3.4.6.3 Đối với người dùng dịch vụ FTP

Nếu có dùng chức năng xác thực thì quy trình như sau:

$ftp vectra

Connected to vectra.

220 -Proxy first requres authentication

220 Vectra.sce.gov.vn FTP proxy (version V1.0) ready:

Name (vectra: root): **ngoc**

331 Enter authentication password for ngoc

Password: #######

230 User authenticated to proxy

ftp>user ngoc@192.1.1.1

331 -(----GATEWAY CONNECTED TO 192.1.1.1----)

331-(220 sco5.cse,gov.vn FTP server (Version 2.1 WU(1)) ready.)

331 Password required for ngoc.

Password:

230 User ngoc logged in.

ftp>

...

ftp>bye

221 Goodbye.

$

Còn nếu không sử dụng chức năng xác thực thì đơn giản hơn:

$ftp vectra

Connected to vectra.

220 Vectra.sce.gov.vn FTP proxy (version V1.0) ready:

Name (vectra: root): **ngoc@192.1.1.1**

331 -(----GATEWAY CONNECTED TO 192.1.1.1----)

331-(220 sco5.cse,gov.vn FTP server (Version 2.1 WU(1)) ready.)

331 Password required for ngoc.

Password:

230 User ngoc logged in.

ftp>

...

ftp>bye

221 Goodbye

$

Nếu sử dụng chương trình **WS_FTP trên Window của Ipswitch, Inc** thì cần phải đặt chế độ Use Firewall ở trong phần Advanced khi ta cấu hình một phiên nối kết. Trong phần Firewall Informatic ta sẽ đưa địa chỉ IP của proxy vào phần Hostname, tên người dùng và mật khẩu (UserID và Password) cho phần xác thực trên proxy và cổng dịch vụ (21). Đồng thời phải chọn kiểu USER after logon ở phần Firewall type.