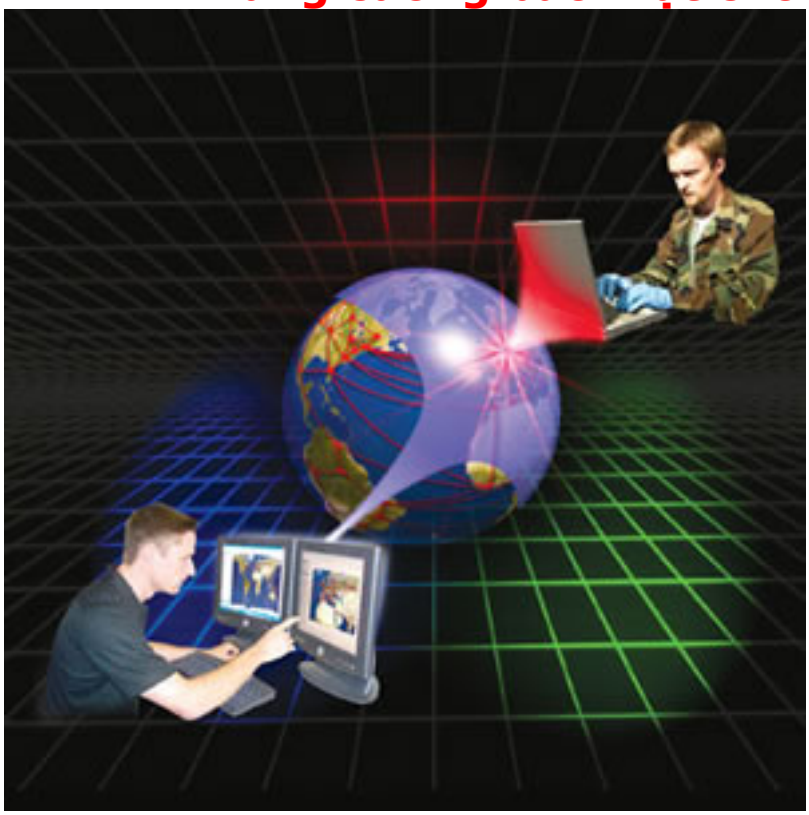
Tăng cường bảo mật cho mạng IP



Nội dung chính

****

Tăng cường Bảo mật cho mạng IP

Bảo mật mạng là một vấn đề rất rộng, có thể được xem xét ở mức dữ liệu (nơi mà những vấn đề về trộm gói tin và mã hóa dữ liệu có thể xảy ra), ở mức giao thức, và ở mức ứng dụng. Ngày càng có nhiều người kết nối Internet và các công ty ngày càng mở rộng mạng, vấn đề bảo mật cho mạng nội bộ trở nên khó khăn hơn. Công ty phải xác định khu vực nào của mạng nội bộ cần bảo vệ, tìm cách hạn chế người dùng truy cập tới những khu vực đó, xác định loại dịch vụ mạng nào cần sàng lọc để ngăn chặn những lỗ hổng bảo mật. Cisco Systems cung cấp rất nhiều tính năng ở tầng giao thức (protocol hay network layer) để
tăng cường bảo mật cho mạng IP. Những tính năng này bao gồm điều khiển hạn chế truy cập
tới routers và servers bằng console port, Telnet, Simple Network Management Protocol (SNMP),
Terminal Access Control System (TACACS), thẻ chứa mã người dùng và danh sách truy cập
Việc thiết lập kiến trúc của một firewal cũng sẽ được nói tới. Bài viết này chỉ nói đến những vấn đề
bảo mật ở mức network-layer, nhưng nếu bỏ qua những vấn đề bảo mật ở mức host-level cũng
sẽ rất nguy hiểm. Về những biện pháp bảo mật ở host-level bạn hãy xem hướng dẫn về các ứng dụng
của bạn, và danh sách liệt kê ở cuối bài viết này.

Tìm hiểu cách tiếp cận của Cisco với vấn đề bảo mật mạng

Khi người ta nói tới bảo mật, họ muốn chắc chắn rằng người dùng chỉ thực hiện được những việc
được cho phép, chỉ nhận được những thông tin được cho phép, và không thể gây ra hư hại với dữ
liệu, ứng dụng hay hệ điều hành của hệ thống
Từ bảo mật còn bao hàm nghĩa bảo vệ khỏi những tấn công ác ý từ bên ngoài. Bảo mật cũng liên

quan đến điều khiển hiệu ứng của các lỗi và sự cố thiết bị. Những gì có thể bảo vệ chống lại những
tấn công được tính toán kỹ lưỡng thì cũng ngăn chặn được những rủi ro ngẫu nhiên. Bài viết này
cung cấp những việc mà bạn có thể làm để tăng cường bảo mật cho mạng của bạn. Trước khi đi
vào chi tiết, sẽ rất có ích nếu bạn hiểu những khái niệm cơ bản không thể thiếu với bất cứ hệ thống nào
(*) Biết rõ kẻ thù
Ở đây muốn nói tới những kẻ tấn công. Hãy tìm hiểu xem ai muốn vượt qua các biện pháp bảo
mật của bạn, xác định động lực thúc đẩy họ. Xác định họ muốn làm gì và những hư hại họ có thể gây ra
cho hệ thống của bạn.
Các biện pháp bảo mật không thể ngăn chặn tuyệt đối các hành động không được phép, mà chỉ khiến
việc đó trở nên khó khăn hơn. Mục tiêu là khiến sự bảo mật của mạng vượt qua khả năng hay động lực
thúc đẩy kẻ tấn công.
(*) Tính toán chi phí
Các biện pháp bảo mật hầu hết đều làm giảm đi sụ tiện lợi. Bảo mật có thể khiến công việc đình trệ và tạo
thêm chi phí đào tạo và quản trị. Nó có thể đòi hỏi nhiều tài nguyên quan trọng cũng như những phần cứng
chuyên dụng.
Khi thiết kế các biện pháp bảo mật, bạn cần hiểu được chi phí của chúng, so sánh với lợi ích có thể có. Để
làm được như vậy bạn phải hiểu chi phí cho bản thân các biện pháp và chi phí cho những lỗ hổng bảo mật có
thể có.
(*) Những giả định của bạn
Mỗi hệ thống bảo mật đều có những giả định của nó. Ví dụ, bạn có thể giả sử rằng kẻ tấn công biết ít hơn
bạn, rằng họ dùng những phần mềm tiêu chuẩn. Hãy kiểm tra và đánh giá cẩn thận các giả định của bạn.
Mỗi giả định chưa được xem xét sẽ là một lỗ hổng bảo mật tiềm ẩn.
(*) Điều khiển các thông tin bí mật
Hầu hết bảo mật là dựa trên các thông tin bí mật, chẳng hạn như password và các khóa mã hóa.
Điều quan trọng nhất là hiểu được khu vực bạn cần bảo vệ. Những kiến thức nào sẽ giúp ai đó vượt qua
hệ thống của bạn ? Bạn phải bảo vệ cẩn thận với kiến thức đó. Càng nhiều thông tin bí mật, càng
khăn cho việc bảo vệ tất cả chúng. Hệ thống bảo mật chỉ nên thiết kế cho một giới hạn nhất định thông
tin cần giữ.
(*) Hãy nhớ đến yếu tố con người
Rất nhiều phương pháp bảo mật thất bại vì những người thiết kế không để ý đến

việc người dùng
nghĩ gì. Ví dụ, do chúng rất khó nhớ, password tạo 1 cách tự động thường thấy được ghi ở mặt dưới
bàn phím.Nếu các biện pháp bảo mật gây trở ngại cho việc sử dụng thiết yếu của hệ thống, những biện
pháp đó sẽ bị bỏ qua. Để đạt được ý muốn, bạn phải chắc chắn rằng người dùng có thể hoàn thành
công việc của họ, bạn phải làm cho họ hiểu được và chấp nhận sự cần thiết của bảo mật.
Người dùng nên có một sự hợp tác với hệ thống bảo mật, ít nhất ở mức độ nào đó.Password,
chẳng hạn, có thể nhận được bằng cách đơn giản gọi điên đến người dùng, giả làm người quản
trị. Nếu người dùng của bạn hiểu những vấn đề bảo mật và nếu họ hiểu lý do những biện pháp của
bạn, họ sẽ không khiến cho kẻ xâm nhập cảm thấy dễ dàng.
Ít nhất, người dùng nên được hướng dẫn không bao giờ đưa password hay thông tin bí mật qua
đường điện thoại hay email không được bảo vệ, cảnh giác với những câu hỏi qua điện thoại. Một vài
công ty đã lập ra những chương trình đào tạo về bảo mật thông thường cho nhân viên, nhân viên không
được truy cập Internet khi chưa hoàn thành chương trình này.
(*) Biết điểm yếu của bạn
Mọi hệ thống đều có điểm yếu. Bạn cần hiểu các điểm yếu trong hệ thống của bạn và cách khai thác
những điểm yếu đó. Bạn cũng nên biết khu vực có nguy cơ cao nhất và ngăn chặn sự truy cập đến đó.
Hiểu được những điểm yếu là bước đầu tiên đưa chúng thành những khu vực an toàn.
(*) Giới hạn phạm vi truy cập
Bạn nên đặt những giới hạn thích hợp trong hệ thống sao cho nếu kẻ xâm nhập có thể truy cập đến
một phần hệ thống, họ không thể tự động có quyền truy cập đến phần còn lại của hệ thống.
(*) Hiểu môi trường làm việc của bạn
Hiểu hệ thông của bạn hoạt động ra sao, biết được cái gì được mong đợi và cái gì không, quen với
việc các thiết bị thường được sử dụng thế nào, sẽ giúp bạn phát hiện những vấn đề bảo mật. Chú ý
đến những sự kiện không bình thường giúp bạn phát hiện kẻ xâm nhập trước khi chúng phá hoại hệ
thống. Những công cụ giám sát có thể giúp bạn phát hiện những sự kiện không bình thường đó.
(*) Giới hạn sự tin tưởng
Bạn nên biết chính xác bạn phần mềm nào bạn tin tưởng, và hệ thống bảo mật của bạn không nên
dựa trên giả định rằng tất cả các phần mềm không có lỗi

(*) Nhớ đến physical security
Truy cập một cách trực tiếp vào 1 máy tính (hay một router), một người kinh nghiệm có thể chiếm
toàn bộ điều khiển trên đó.Sẽ chẳng có ý nghĩa gì nếu cài đặt những phần mềm bảo mật khi quyền
sử dụng trực tiếp phần cứng không được quan tâm.
(*) Bảo mật ở khắp nơi
Hầu hết những thay đổi trong hệ thống của bạn có thể có ảnh hưởng đến bảo mật. Điều này đặc biệt
đúng khi một dịch vụ mới được tạo ra. Những nhà quản trị, lập trình, và người dùng phải luôn để ý đến
vấn đề bảo mật trong mỗi thay đổi họ tạo ra. Hiểu được khía cạnh bảo mật của mỗi thay đổi đòi hỏi
thực hành, khám phá mỗi dịch vụ có thể được sử dụng theo những cách nào.

Điều khiển truy cập tới Cisco Routers

Việc điều khiển truy cập tới Cisco routers của bạn là rất quan trọng. Bạn có thể điều khiển truy cập tới
routers sử dụng các phương pháp sau :
- Truy cập console
- Truy cập telnet
- Truy cập bằng Simple Network Management Protocol (SNMP)
- Điều khiển truy cập tới servers có những file cấu hình hệ thống
Bạn có thể bảo vệ 3 phương pháp đầu tiên bằng cách sử dụng tính năng của phần mềm router. Với mỗi
phương pháp, bạn có thể cho phép privileged access (truy cập với đặc quyền) hay nonprivileged access
(truy cập thông thường) đối với mỗi người dùng (hay nhóm người dùng). Nonprivileged access cho phép
người dùng theo dõi router nhưng không được thay đổi router. Privileged access cho người dùng toàn
quyền thay đổi cấu hìnhcho router. Với truy cập qua console port và Telnet, bạn có thể thiết lập 2 loại
password. Loại thứ nhất là password đăng nhập, cho phép nonprivileged access. Sau khi truy cập vào router,
người dùng có thể chuyển sang chế độ privileged bằng cách nhập password phù hợp. Ở chế độ privileged
người dùng có toàn quyền thay đổi thiết lập
Truy cập SNMP cho phép bạn đặt những chuỗi SNMP khác nhau cho cả nonprivileged và privileged access.
Nonprivileged access cho phép người dùng ở 1 host gửi đến router những thông điệp SNMP get-request
và SNMP get-next-request. Những thông điệp này được dùng để lấy thông tin từ router. Privileged access
cho phép người dùng gửi những thông điệp SNMP set-request để thay đổi cấu hìnhvà trạng thái hoạt động
của router.

Truy cập Console

Console là thiết bị đầu cuối gắn trực tiếp với router qua cổng console. Việc bảo mật được áp dụng với
console bằng cách buộc người dùng xác nhận bản thân qua password. Theo mặc định, không có password
đi kèm với console access.

Password cho chế độ nonprivileged
Bạn thiết lập password cho chế độ nonprivileged bằng cách đánh dòng lệnh sau vào file cấu hìnhcủa router.
Password phân biệt chữ hoa, chữ thường. Ở ví dụ, password là "1forAll"
line console 0
login
password 1forAll
Khi bạn đăng nhập vào router, sẽ nhận được thông báo login như sau
User Access Verification
Password:
Bạn phải nhập password "1forAll" để có quyền nonprivileged access đến router. Router sẽ trả lời như sau :
router>Dấu nhắc > báo hiệu đây là chế độ nonprivileged. Bây giờ bạn có thể dùng rất nhiều lệnh để xem thông tin
về hoạt động của router. Không bao giờ dùng "cisco", hay những biến thể khác như "pancho" cho password
của Cisco router. Đó sẽ là những password đầu tiên kẻ xâm nhập thử khi họ nhìn thấy dấu đăng nhập Cisco.

Password cho chế độ privileged
Thiết lập password cho chế độ privileged bằng cách đưa dòng lệnh sau vào file cấu hìnhcủa router. Trong ví
dụ này password là "san-tran".
enable-password san-fran
Để truy cập chế độ privileged, đánh lệnh sau:
router> enable
Password:
Gõ password "san-fran" để được privileged access tới router. Router trả lời như sau :
router#
Dấu nhắc # báo hiệu chế độ privileged. Ở chế độ privileged, bạn có thể đánh tất cả các lệnh để xem thông
tin và cấu hìnhcho router.

Giới hạn thời gian phiên làm việc
Đặt password đăng nhập và password enable có thể chưa đủ an toàn trong 1 số trường hợp. Giới hạn thời gian cho

một console không được điều khiển (mặc định 10 phút) cung cấp thêm một biện pháp an toàn.Bạn có thể
thay đổi giới hạn này bằng lệnh exec-timeout mm ss trong đó mm là số phút, ss là số giây. Lệnh sau thay
đổi giới hạn thành 1 phut 30 giây
line console 0
exec-timeout 1 30

Mã hóa password
Tất cả password trên router đều có thể xem được bằng lệnh xem cấu hìnhcủa router trong chế độ privileged.
Nếu bạn có quyền truy cập ở chế độ privileged , bạn có thể xem tất cả password ở dạng cleartext, theo mặc
định. Có một cách để giấu cleartext password. Lệnh password-encryption lưu các password dưới dạng mã
hóa.Tuy nhiên, nếu bạn quên password, để lấy lại quyền truy cập, bạn phải có quyền truy cập trực tiếp (physical access) đối với router.

Truy cập bằng Telnet

Bạn có thể truy cập theo chế độ nonprivileged hoặc privileged tới router thông qua Telnet. Giống như với
Console, sự bảo mật với Telnet có được khi người dùng xác nhận bản thân bằng password. Thực tế,
rất nhiều khái niệm tương tự mô tả ở phần "Console Access" ở trên cũng áp dụng cho truy cập Telnet.
Bạn phải nhập password để chuyển từ chế độ nonprivileged sang privileged, có thể mã hóa password, đặt
giới hạn thời gian cho phiên làm việc.

Password cho chế độ nonprivileged
Mỗi cổng Telnet của router được coi như một thiệt bị đầu cuối "ảo" (virtual terminal). Có tối đa 5 cổng
dành cho virtual terminal (VTY) trên router , cho phép 5 phiên làm việc Telnet đồng thời. Trên router, các
này đánh số từ 0 đến 4. Bạn có thể đặt nonprivileged password cho các cổng với lệnh cấu hình sau.Trong ví
dụ này, cổng virtual terminal từ 0 đến 4 sử dụng password "marin" :
line vty 0 4
login
password marin
Khi người dùng telnet đến IP của router, router trả lời tương tự như sau :
% telnet router
Trying ...
Connected to router
Escape character is '^]'
User Access Verification

Password:
Nếu người dùng nhập đúng nonprivileged password, dấu nhắc sau sẽ xuất hiện:
router>
Password cho chế độ privileged
Bây giờ người dùng đã có nonprivileged access và có thể chuyển sang chế độ privileged bằng cách gõ
lệnh enable giống như đối với Console Access.

Hạn chế truy cập Telnet đối với những địa chỉ IP cụ thể
Nếu bạn muốn chỉ những IP nhất định có thể dùng Telnet truy cập router, bạn phải dùng lệnh access-class nn in
để xác định danh sách truy cập (từ 1 đến 99). Lệnh cấu hình sau cho phép truy cập Telnet đến router từ các host
trong mạng 192.85.55.0:
access-list 12 permit 192.85.55.0 0.0.0.255
line vty 0 4
access-class 12 in

Hạn chế truy cập Telnet đối với các sản phẩm Cisco thông qua cổng TCP
Có thể truy cập tới 1 sản phẩm của Cisco thông qua Telnet đến những cổng TCP nhất định. Kiểu truy cập
Telnet thay đổi tùy theo những phiên bản phần mềm Cisco:
- Software Release 9.1 (11.4) và cũ hơn, 9.21 (3.1) và cũ hơn
- Software Release 9.1 (11.5) , 9.21 (3.2), 10.0 và mới hơn
Với Software Release 9.1 (11.4) và cũ hơn, 9.21 (3.1) và cũ hơn, có thể , theo mặc định, thiết lập kết nối TCP
tới sản phẩm của Cisco thông qua các cổng TCP trong Bảng 3-1

Bảng 3-1 : Cổng TCP truy cập Telnet tới các sản phẩm Cisco (các phiên bản cũ)
Cổng TCP Phương thức truy cập
7 Echo
9 Discard
23 Telnet (tới cổng VTY theo kiểu quay vòng)
79 Finger
1993 SNMP thông qua TCP
2001-2999 Telnet tới cổng hỗ trợ (auxiliary - AUX), cổng terminal (TTY), và cổng virtual terminal (VTY)
3001-3999 Telnet tới những cổng quay vòng (chỉ có thể khi đã được cấu hình với lệnh rotary)
4001-4999 Telnet (stream mode) , mirror của các cổng trong khoảng 2000
5001-5999 Telnet (stream mode), mirror của khoảng 3000 (chỉ khi đã cấu hình rotary)
6001-6999 Telnet (binary mode), mirror của khoảng 2000
7001-7999 Telnet (binary mode), mirror của khoảng 300 (chỉ khi đã cấu hình rotary)
8001-8999 Xremote (chỉ với communication servers)
9001-9999 Reverse Xremote (chỉ với communication servers)
10001-19999 Reverse Xremote rotary (chỉ với communication servers, khi đã cấu

hình rotary trước)

Chú ý : Vì Cisco routers không có đường TTY, thiết lập truy cập (trên communicaiton servers) tới các cổng
2002,2003,2004 và lớn hơn có thể cung cấp truy cập tới VTY (trên routers) tới các cổng tương ứng. Để cung
cấp truy cập tới các cổng TTY, bạn có thể tạo danh sách truy cập trong đó hạn chế truy cập đối với VTYs.
Khi thiết lập những nhóm quay vòng, luôn nhớ rằng có thể truy cập đến bất cứ cổng nào trong nhóm (trừ khi
có danh sách giới hạn truy cập).
Sau đây là ví dụ minh họa một danh sách truy cập từ chối truy cập đến cổng hỗ trợ (AUX) và chỉ cho phép truy cập
telnet từ địa chỉ 192.32.6.7 :
access-class 51 deny 0.0.0.0 255.255.255.255
access-class 52 permit 192.32.6.7
line aux 0
access-class 51 in
line vty 0 4
Chú ý : nếu lệnh ip alias được cho phép trên sản phẩm Cisco, mọi kết nối TCP tới bất cứ cổng nào cũng được
coi là hợp lệ. Có thể bạn sẽ muốn vô hiệu hóa lệnh này
Có thể bạn muốn tạo danh sách truy cập hạn chế truy cập tới sản phẩm Cisco qua cổng TCP.
đến router.
Với Software Release 9.1 (11.5), 9.21 (3.2), và bất cứ phiên bản nào của Software Release 10, những cải tiến
sau đã được thực hiện :
- Truy cập trực tiếp đến virtual terminal lines (VTYs) qua cổng trong các khoảng 2000,4000 và 6000 đã được vô
hiệu hóa theo mặc định
- Kết nối tới cổng echo và discard (7 và 9) có thể được vô hiệu hóa với lệnh no service tcp-small-servers
- Tất cả sản phẩm Cisco cho phép kết nối tới IP alias chỉ với cổng 23
Với những phiên bản sau này, Cisco router chấp nhận kết nối TCP qua các cổng mặc định trong Bảng 3-2

Bảng 3-2 : Cổng TCP cho truy cập Telnet tới các sản phẩm Cisco (những phiên bản sau)

Cổng TCP Phương thức truy cập
7 Echo
9 Discard
23 Telnet
79 Finger
1993 Cổng hỗ trợ (AUX)
4001 Cổng AUX (stream)
6001 Cổng AUX (binary)

Truy cập qua cổng 23 có thể bị hạn chế bằng cách tạo danh sách truy cập và gán nó cho một đường virtual terminal.
Truy cập qua cổng 79 có thể vô hiệu hóa bằng lệnh no service finger. Truy cập qua cổng 1993 có thể được kiểm
soát bằng danh sách truy cập SNMP. Truy cập qua cổng 2001,4001 và 6001 có thể được kiểm soát bằng 1 danh
sách truy cập đặt ở 1 cổng hỗ trợ (AUX)

Terminal Access Conroller Access Control System (TACACS)

Password chế độ nonprivileged và privileged được áp dụng cho mỗi người dùng truy cập router từ console port hay
Telnet. Ngoài ra, Terminal Access Controller Access Control System (TACACS) cung cấp 1 cách xác nhận mỗi
người dùng dựa trên từng cơ sở riêng biệt trước khi họ có thể có quyền truy cập vào router hay communication
server. TACACS được xây dựng ở Bộ quốc phòng mỹ và được mô tả trong Request For Comments (RFC) 1492.
TACACS được Cisco sử dụng để cho phép quản lý tốt hơn, xem ai có quyền truy cập tới router trong chế độ
nonprivileged và privileged .
Với TACACS enabled, router nhắc người dùng nhập username và password. Sau đó, router gọi TACACS server để
xác định password có đúng không. Một TACACS server thường chạy trên một trạm làm việc UNIX. Domain TACACS
servers có thể nhận được thông qua anonymous ftp đến ftp.cisco.com trong thư mục /pub. Sử dụng /pub/README
để tim tên file. Một server hỗ trợ TACACS đầy đủ có kèm trong CiscoWorks Version 3.
Lệnh cấu hình tacacs-server host xác định UNIX host chạy một TACACS server sẽ xác nhận lại yêu cầu gửi từ routers.
Bạn có thể đánh lệnh tacacs-server host nhiều lần để chỉ ra nhiều TACACS server cho một router.

Nonprivileged Access
Nếu tất cả server đều không sẵn sàng, bạn có thể bị khóa đối với router. Lúc này, lệnh cấu hình tacacs-server
last resort [password | succeed] cho phép bạn xác định xem có cho người dùng đăng nhập không cần password
(từ khóa succeed) hay buộc người dùng cung cấp password chuẩn (từ khóa password)
Các lệnh sau chỉ ra một TACACS server và cho phép đăng nhập nếu server gặp sự cố:
tacacs-server host 129.140.1.1
tacacs-server last-resort succeed

Buộc người dùng truy cập qua Telnet xác nhận bản thân qua lệnh cấu hìnhsau :
line vty 0 4
login tacacs

Privileged Access (truy cập với đặc quyền)
Phương pháp kiểm tra password này cũng có thể áp dụng với chế độ privileged dùng lệnh enable use-tacacs.
Nếu tất cả server đều không sẵn sàng tiếp nhận, lệnh cấu hìnhenable last-resort [succeed | password] cho biết
có để người dùng đăng nhập không cần password hay không. Nếu bạn dùng lệnh enable use-tacacs, bạn cũng
phải dùng lệnh tacacs-server authenticate enable. Lệnh tacacs-server extended cho phép thiết bị Cisco chạy
chế độ TACACS mở rộng. Hệ thống UNIX phải chạy extended TACACS daemon, có thể nhận được bằng anonymous
ftp tới ftp.cisco.com, tên file là xtacacsd.shar. Daemon này cho phép communication servers và những thiết bị
khác giao tiếp với hệ thống UNIX và cập nhật thông tin mà thiết bị đó gửi.
Lệnh username <user> password [0 | 7] <password> cho phép bạn lưu một danh sách user và password trong
thiết bị Cisco thay vì trên một TACACS server. Số 0 lưu password dạng cleartext trong file cấu hình. Số 7 lưu
ở dạng mã hóa. Nếu bạn không có một TACACS server và vẫn muốn xác định từng user bạn có thể dùng những
lệnh cấu hìnhsau :
username steve password 7 steve-pass
username allan password 7 allan-pass
Token Card Access (truy cập bằng thẻ)
Sử dụng TACACS cho routers và communication server, có thể hỗ trợ các loại key devices , hay token card.
Mã của TACACS server có thể thay đổi để hỗ trợ việc này mà không cần thay đổi cấu hình của router hay
communication server. Sự thay đổi này không thể trực tiếp từ Cisco
Hệ thống token card dựa trên một tấm thẻ bạn phải có để xác nhận bản thân. Bằng cách móc nối (hook)
với mã của TACACS server, các công ty thứ 3 (third-party) có thể cung cấp những dịch vụ này. Một trong
những sản phẩm như vậy là Enigma Logic SafeWord, ngoài ra còn có Security Dynamics SmartCard.

Simple Network Management Protocol (SNMP) Access

SNMP là một phương pháp khác dùng truy cập router. Với SNMP, bạn có thể thu thập thông tin hay cấu hình
routers. Thu thập thông tin với thông điệp get-request và get-next-request, cấu

hình routers với thông điệp
set-request. Mỗi thông điệp SNMP có một community string (chuỗi công cộng !), là 1 password ở dạng cleartext
được gửi trong mỗi gói tin giữa trung tâm điều khiển(management station) và router, nơi có chứa một SNMP agent.
Chuỗi SNMP được dùng để xác nhận các thông tin gửi đi giữa manager và agent. Chỉ khi manager gửi thông điệp
với community string đúng thì agent mới trả lời. SNMP agent trên router cho phép bạn thiết lập những community
string cho truy cập ở chế độ nonprivileged và privileged. Bạn có thể thiết lập community strings trên router thông qua
lệnh cấu hình snmp-server community <string> [RO | RW] [access-list].
Tuy nhiên, SNMP community strings được gửi ở dạng cleartext. Do đó, bất cứ ai có khả năng lấy được 1 gói tin nào
đó có thể sẽ tìm ra chuỗi này, có thể giả mạo người dùng sửa đổi routers qua SNMP. Vì vậy sử dụng lệnh no snmp-server
trap-authentication có thể ngăn chặn những kẻ xâm nhập bắt các thông điệp (gửi giữa SNMP managers và agents)
để tìm community strings.
Người ta đã cải tiến bảo mật của SNMP version 2 (SNMPv2) , được mô tả trong RFC 1446. SNMPv2 dùng thuật
toán MD5 để xác nhận giao tiếp giữa server và agent. MD5 xác nhận tính tương thích của dữ liệu, nguồn gốc cũng
như thời gian. Hơn nữa SNMPv2 có thể dùng chuẩn mã hóa dữ liệu DES để mã hóa thông tin.

Chế độ nonprivileged
Dùng từ khóa RO của lệnh snmp-server community để cung cấp truy cập nonprivileged tới routers qua SNMP.
Lệnh cấu hình sau làm agent trong router chỉ cho phép các thông điệp SNMP get-request và get-next-request,
được gửi đi với community string "public" :
snmp-server community pubic RO 1
Bạn có thể chỉ rõ danh sách địa chỉ IP được phép gửi thông điệp tới router bằng tùy chọn access-list với lệnh
snmp-server community. Ở ví dụ sau, chỉ hosts 1.1.1.1 và 2.2.2.2 được phép truy cập nonprivileged tới router
qua SNMP:
access-list 1 permit 1.1.1.1
access-list 1 permit 2.2.2.2
snmp-server community public RO 1

Chế độ privileged
Sử dụng từ khóa RW của lệnh snmp-server community để cung cấp truy cập privileged tới router qua SNMP.
Lệnh sau khiến agent trong router chỉ cho phép thông điệp SNMP set-request, được gửi với community string
là "private" :

snmp-server community private RW 1
Bạn có thể chỉ rõ danh sách IP được phép gửi thông điệp tới router bằng tùy chọn access-list của lệnh snmp-server
community. Ở ví dụ sau , chỉ có hosts 5.5.5.5 và 6.6.6.6 được phép truy cập privileged tới router qua SNMP :
access-list 1 permit 5.5.5.5
access-list 1 permit 6.6.6.6
snmp-server community private RW 1

Điều khiển việc truy cập đến các Servers chứa các file cấu hình

Nếu 1 router thường xuyên download file cấu hình từ một server Trivial File Transfer Protocol (TFTP) hay Maintenance
Operations Protocol (MOP), bất cứ ai có thể truy cập server này cũng có thể thay đổi file cấu hình của router trên server đó.
Communication servers có thể đươc cấu hình để chấp nhận một kết nối LAT (Local Area Transport).Protocol translator
và các translating router có thể chấp nhận kết nối X.29. Sự khác biệt về kiểu truy cập này cần được chú ý khi tạo
một kiến trúc firewall.

Thiết lập kiến trúc firewall của bạn

Một kiến trúc firewall là 1 mô hình tồn tại giữa bạn và thế giới bên ngoài nhằm bảo vệ bạn khỏi những kẻ xâm
nhập. Trong phần lớn tình huống, những kẻ xâm nhập được đại diện bởi mạng Internet và hàng ngàn mạng kết
nối với nó. Điển hình như một firewall dựa trên nhiều bộ máy khác nhau trong hình 3-1

Hình 3-1 : <không có>
Trong kiến trúc này, một router được nối với Internet (exterior router), buộc mỗi giao tiếp mạng đi vào application gateway (cổng ứng dụng).
Một router được nối với mạng nội bộ (interior router) chỉ tiếp nhận những gói tin từ cổng ứng dụng.
Cổng ứng dụng thiết lập policies (chính sách) đối với từng người dùng và từng ứng dụng. Hệ quả là nó điều
khiển được sử phân phát của các dịch vụ cả đến và đi từ mạng nội bộ. Ví dụ, chỉ một số người dùng được
phép giao tiếp với Internet, hay chỉ một số ứng dụng được phép thiết lập kết nối với bên ngoài. Nếu chỉ 1 ứng
dụng được phép gửi thư, chỉ những gói thư được đi qua router.

Điều khiển lưu thông trong mạng
Phần này sử dụng tình huống minh họa trong hình 3-2 để mô tả việc sử dụng

danh sách truy cập ngăn chặn lưu
thông dữ liệu đến và đi từ một firewall router và một firewall communication server

Hình 3-2 : <không có>
Trong bài viết này firewall router cho phép kết nối "đến" từ 1 hay nhiều server hay host. Một router được thiết kế hoạt
động như 1 firewall là điều ta mong muốn, vì nó định rõ mục đích của router là external gateway và tránh làm
phiền các router khác với nhiệm vụ này. Trong tình huống mạng nội bộ cần được cô lập, firewall router sẽ cung
cấp điểm cô lập mà không ảnh hưởng đến phần còn lại của mạng.

Cấu hình một Firewall Router

Trong cấu hình của firewall router dưới đây, subnet 13 của Class B là firewall subnet, trong khi đó subnet 14 cung
cấp kết nối Internet qua một nhà cung cấp dịch vụ :
interface ethernet 0
ip address B.B.13.1 255.255.255.0
interface serial 0
ip address B.B.14.1 255.255.255.0
router igrp
network B.B.0.0
Cấu hình đơn giản này không có sự bảo mật và cho phép tất cả mọi lưu thông từ thế giới bên ngoài đến mạng. Để
có sự bảo mật với firewall router, sử dụng danh sách truy cập và nhóm truy cập như mô tả dưới đây.

Xác định danh sách truy cập
Danh sách truy cập xác định những lưu thông thực tế sẽ được cho phép hay từ chối, trong khi đó 1 nhóm truy
cập áp dụng 1 danh sách truy cập nhất định cho 1 interface. Danh sách truy cập có thể dùng để từ chối kết nối
ẩn chứa mối nguy hại về bảo mật và cho phép tất cả các kết nối khác, hoặc cho phép những kết nối chấp nhận
được và từ chối tất cả kết nối còn lại. Đối với một firewall, cách thứ 2 là cách an toàn hơn.
Trong bài viết này, email và news đến được cho phép với 1 số hosts, nhưng FTP, Telnet và rlogin chỉ cho phép
những host nằm trong firewall subnet.Khoảng IP mở rộng (từ 100 đến 199) và các số cổng TCP hay UDP được
dùng để lọc lưu thông .Khi một kết nối sắp được hình thành cho email,Telnet, FTP,... nó sẽ cố mở một dịch

vụ ở một cổng xác định. Do đó bạn có thể lọc những kết nối đó bằng cách từ chối các gói tin tìm cách
sử dụng dịch vụ đó. Về danh sách của những dịch vụ và cổng thường gặp, xem phần "Lọc các dịch vụ
TCP và UDP" ở phần sau.
Một danh sách truy cập được gọi sau quyết định của router nhưng trước khi gói tin được gửi đến 1 interface.
Chỗ tốt nhất để xác định danh sách truy cập là tạo 1 file chứa các lệnh access-list, đặt file đó trong thư mục TFTP
mặc định và nạp file đó vào router.
Server chứa file đó fải chạy TFTP daemon và có kết nối TCP đến firewall router. Trước khi nạp, mọi xác định
trước đó của danh sách truy cập này được gỡ bỏ bằng lệnh no access-list 101
Lệnh access-list có thể được dùng để cho phép các gói tin trả về từ những kết nối được thiết lập trước đó. Với
từ khóa established, sẽ có sự phù hợp nếu gói TCP chứa acknowledgement (ACK) hay reset(RST) bits set.
access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 established
Nếu firewall routers nào chia sẻ mạng với 1 nhà cung cấp bên ngoài, bạn sẽ muốn cho phép truy cập từ các host
đó tới mạng của bạn. Trong bài viết này, nhà cung cấp bên ngoài có một cổng nối tiếp sử dụng firewall router
Class B địa chỉ (B.B.14.2) là địa chỉ nguồn như sau :
access-list 101 permit ip B.B.14.2 0.0.0.0 0.0.0.0 255.255.255.255
Ví dụ sau minh họa cách từ chối lưu thông từ 1 người dùng cố gắng che giấu một địa chỉ nội bộ của bạn với
bên ngoài (không dùng danh sách truy cập "đầu vào" 9.21) :
access-list 101 deny ip B.B.0.0 0.0.255.255 0.0.0.0 255.255.255.255
Lệnh sau cho phép Domain Name System (DNS) và Network Time Protocol (NTP) gửi yêu cầu và trả lời :
access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123
Lệnh sau từ chối cổng Network File Server (NFS) User Datagram Protocol (UDP) :
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2049
Lệnh sau từ chối OpenWindows ở cổng 2001 và 2002, từ chối X11 ở cổng 6001 và 6002 :
access-list 101 deny tcp 0.0.0.0 255.255.255.2550.0.0.0 255.255.255.255 eq 6001
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 6002
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2001
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2002

Lệnh sau cho phép Telnet đến communication server (B.B.13.2) :
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.2 0.0.0.0 eq 23
Lệnh sau cho phép FTP đến host ở subnet 13 :
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.100 0.0.0.0 eq 21
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.100 0.0.0.0 eq 20
Ở những ví dụ sau, mạng B.B.1.0 nằm trong mạng nội bộ.Các lệnh sau cho phép kết nối TCP và UDP tới các
cổng lớn hơn 1023 với những host hết sức giới hạn. Nhớ đừng để communication servers bộ dịch giao thức
(protocol translator) nằm trong danh sách này :
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.100 0.0.0.0 gt 1023
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.1.100 0.0.0.0 gt 1023
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.1.101 0.0.0.0 gt 1023
access-list 101 permit udp 0.0.0.0 255.255.255.255 B.B.13.100 0.0.0.0 gt 1023
access-list 101 permit udp 0.0.0.0 255.255.255.255 B.B.1.100 0.0.0.0 gt 1023
access-list 101 permit udp 0.0.0.0 255.255.255.255 B.B.1.101 0.0.0.0 gt 1023
Chú ý : chuẩn FTP sử dụng cổng >1023 cho kết nối dữ liệu của nó; do đó, cổng >1023 phải được mở. Chi tiết hơn
đọc phần "Cổng File Transfer Protocol (FTP) " ở phía dưới
Lệnh sau cho phép DNS truy cập tới DNS server(s) liệt kê bởi Network Information Center (NIC) :
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.100 0.0.0.0 eq 53
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.1.100 0.0.0.0 eq 53
Lệnh sau cho phép SMPT email theo chiều đến với 1 số máy :
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.13.100 0.0.0.0 eq 25
access-list 101 permit tcp 0.0.0.0 255.255.255.255 B.B.1.100 0.0.0.0 eq 25
Lệnh sau cho phép news transfer protocol (NNTP) server của mạng nội bộ nhận kết nối NNTP từ danh sách cho phép :
access-list 101 permit tcp 16.1.0.18 0.0.0.1 B.B.1.100 0.0.0.0 eq 119
access-list 101 permit tcp 128.102.18.32 0.0.0.0 B.B.1.100 0.0.0.0 eq 119
Lệnh sau cho phép Internet control message protocole (ICMP) cho thông điệp báo lỗi :
access-list 101 permit icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
Mỗi danh sách truy cập có ẩn câu lệnh "từ chối tất cả những thứ khác" ở cuối danh sách để chắc chắn các thuộc tính
không được đề cập đến sẽ bị từ chối.

Cổng File Transfer Protocol (FTP)
Hiện nay nhiều site chặn các phiên làm việc TCP từ ngoài vào nhưng cho phép kết nối ra ngoài. Vấn đề ở chỗ chặn kết
nối từ ngoài vào sẽ ngăn cản những chương trình FTP client truyền thống, vì những chương trình này dùng lệnh "PORT"
cho server biết chỗ để gửi file. Máy khách mở một kết nối "điều khiển" đến server, nhưng server sau đó sẽ mở một
kết nối "dữ liệu" ở một cổng nào đó (>1023) trên máy khách.
Rất may , còn có 1 cách khác cho phép máy khác mở một socket "dữ liệu" và cho phép bạn có cả firewall và FTP.
Máy khách gửi 1 lệnh PASV đến server, nhận lại một số hiệu cổng cho socket dữ

liệu, mở socket dữ liệu trên
cổng đó và bắt đầu gửi .
Để thực hiện phương pháp này, chương trình FTP client phải hỗ trợ lệnh PASV. Vấn đề duy nhất với phương pháp
này là nó không thực hiện được nếu server chặn luôn kết nối bất kỳ từ ngoài vào
Mã nguồn cho 1 chương trình FPT hoạt động được với firewall có thể nhận được bằng anonymous FTP tại ftp.cisco.com, file /pub/passive-ftp.tar.Z .Đây là phiên bản BSD 4.3 FTP có sửa chữa để hỗ trợ PASV.
Chú ý : Cẩn thận khi cung cấp dịch vụ anonymous FTP. Rất nhiều FTP server có lỗi ở khu vực này.

Áp dụng danh sách truy cập với các Interfaces
Sau khi danh sách truy cập được nạp vào router và lưu trên NVRAM, phải gán nó cho một interface phù hợp.
Trong bài viết này, lưu thông đến từ bên ngoài qua cổng nối tiếp 0 được lọc trước khi được đặt vào subnet 13
(ethernet 0). Do đó lệnh access-group , dùng 1 danh sách truy cập lọc các kết nối đến, phải được gán cho
Ethernet 0 như sau :
interface ethernet 0
ip access-group 101
Để điều khiển truy cập Internet từ mạng nội bộ, lập một danh sách truy cập và áp dụng nó với gói tin gửi đi trên
cổng nối tiếp 0 của router. Để làm được vậy, những gói tin gửi về từ các hosts sử dụng Telnet hay FTP phải
được cho phép truy cập đến firewall subnetwork B.B.13.0

Sàng lọc dịch vụ TCP và UDP
Vài cổng TCP và UDP thường gặp được liệt kê ở bảng 3-3

Bảng 3-3 : Một số cổng và dịch vụ TCP và UDP thường gặp
Dịch vụ Loại cổng Số cổng
FTP-Data TCP 20
FTP-Commands TCP 21
Telnet TCP 23
SMTP-Email TCP 25
TACACS UDP 49
DNS TCP và UDP 53
TFTP UDP 69
finger TCP 79
Sun Remote
Procedure Call(RPC) UDP 111
Network News
Transfer Protocol (NNTP) TCP 119
Network Time
Protocol (NTP) TCP và UDP 123
NeWS TCP 144
Simple Management

Network Protocol (SNMP) UDP 161
SNMP (traps) UDP 162
Border Gateway
Protocol (BGP) TCP 179
rlogin TCP 513
rexec TCP 514
talk TCP và UDP 517
ntalk TCP và UDP 518
Open Windows TCP và UDP 2000
Network File System (NFS) UDP 2049
X11 TCP và UDP 6000

Lời khuyên của CERT
Computer Emergency Response Team (CERT) khuyên nên lọc những dịch vụ trong bảng 3-4

Bảng 3-4 : Lời khuyên của CERT với các dịch vụ TCP, UDP và cổng

Dịch vụ Loại cổng Số cổng
DNS zone transfers TCP 53
TFTP daemon (tftpd) UDP 69
link TCP 87
Sun RPC TCP và UDP 1111
NFS UDP 2049
BSD UNIX các lệnh
bắt đầu bằng r- TCP từ 512 đến 514
line printer daemon (lpd) TCP 515
UNIX-to-UNIX copy
program daemon (uucpd) TCP 540
Open Windows TCP và UDP 2000
X Windows TCP và UDP 6000+

Phần lớn dịch vụ RPC không có số cổng cố định. Bạn nên tìm những cổng có dịch vụ này và chặn lại. Cisco
khuyên nên chặn tất cả cổng UDP trừ DNS nếu có thể.
Chú ý : Cisco khuyên bạn nên lọc dịch vụ finger ở cổng 79 để ngăn chặn người ngoài tìm hiểu cấu trúc thư
mục của người dùng và tên của host mà người dùng đăng nhập

danh sách truy cập "đầu vào"
Trong Software Release 9.21, Cisco giới thiệu khả năng gán danh sách truy cập "đầu vào" cho 1 interface. Điều này cho phép
người quản trị có thể lọc các gói tin trước khi chúng đi qua router. Trong nhiều trường hợp, danh sách truy cập "đầu vào"
và danh sách truy cập "đầu ra" đạt được những tính năng như nhau; tuy nhiên, danh sách truy cập "đầu vào" được ưa thích hơn
với 1 số người và có thể dùng để ngăn chặn một vài kiểu che giấu địa chỉ trong khi

danh sách truy cập "đầu ra" sẽ không
cung cấp đủ độ bảo mật.
Hình 3-3 minh họa 1 host đang bị đánh lừa. Ai đó ở bên ngoài đang mạo nhận rằng đến từ mạng 131.108.17.0.Router interface
cho rằng gói tin đến từ 131.108.17.0.Để tránh việc này, 1 input access list được áp dụng cho router interface đối với bên ngoài.
Nó sẽ chặn bất cứ gói tin nào từ ngoài vào với địa chỉ nguồn trong mạng nội bộ mà router biết (17.0 và 18.0)

Hình 3-3 : <không có>
Nếu bạn có nhiều mạng nội bộ nối với firewall router và router đang dùng bộ lọc "đầu ra", lưu thông giữa các mạng
nội bộ sẽ bị ảnh hưởng bởi bộ lọc. Nếu bộ lọc "đầu vào" chỉ được dùng với router interface với bên ngoài, mạng
nội bộ sẽ không bị ảnh hưởng đáng kể.
Chú ý : Nếu 1 địa chỉ sử dụng source routing, nó có thể gửi và nhận thông qua firewall router. Vì lý do này, bạn
nên vô hiệu hóa source routing trên router với lệnh no ip source-route

Cấu hình một Firewall Communication Server

Trong bài viết này, firewall communication server có 1 modem ở line 2

```
interface Ethernet 0
ip address B.B.13.2 255.255.255.0
!
access-list 10 deny B.B.14.0 0.0.0.255
access-list 10 permit B.B.0.0 0.0.255.255
!
access-list 11 deny B.B.13.2 0.0.0.0
access-list 11 permit B.B.0.0 0.0.255.255
!
line 2
login tacacs
location FireWallCS#2
!
access-class 10 in
access-class 11 out
!
modem answer-timeout 60
modem InOut
telnet transparent
terminal-type dialup
flowcontrol hardware
stopbits 1
rxspeed 38400
txspeed 38400
```

!
tacacs-server host B.B.1.100
tacacs-server host B.B.1.101
tacacs-server extended
!
line vty 0 15
login tacacs

Xác định danh sách truy cập
Trong ví dụ này, số hiệu mạng được dùng để cho phép hay từ chối truy cập;do đó khoảng IP chuẩn được sử dụng
(từ 1 đến 99). Với những kết nối từ bên ngoài đến modem lines, chỉ những gói tin từ những host trong mạng nội bộ Class B và những gói tin từ các host trong firewall subnetwork được cho phép:
access-list 10 deny B.B.14.0 0.0.0.255
access-list 10 permit B.B.0.0 0.0.255.255
Những kết nối đi chỉ được cho phép đến các hosts trong mạng nội bộ và communication server
access-list 11 deny B.B.13.2 0.0.0.0
access-list 11 permit B.B.0.0 0.0.255.255

Áp dụng danh sách truy cập với các đường kết nối
Áp dụng 1 danh sách truy cập với 1 đường kết nối bằng lệnh access-class. Trong bài viết này, sự hạn chế trong
danh sách truy cập 10 được áp dụng cho các kết nối đến với đường kết nối 2, sự hạn chế trong danh sách truy
cập 11 được áp dụng cho các kết nối đi với đường kết nối 2
line 2.
access-class 10 in
access-class 11 out

Sử dụng banners để tạo một thông báo
Ta có thể dùng cấu hình banner exec để tạo ra các thông báo, sẽ được hiện trong tất cả các kết nối. Ví dụ,
trên một communication server, bạn có thể đưa vào thông điệp sau :
banner exec ^C
If you have problems with the dial-in lines, please
send mail to helpdesk@CorporationX.com.
If you get the message "% Your account is expiring", please send mail with name and voicemail box to helpdesk@CorporationX.com, and
someone will contact you to renew your account.
Unauthorized use of these resources is prohibited.

Bảo vệ những dịch vụ ngoài chuẩn

Có rất nhiều dịch vụ ngoài chuẩn từ Internet. Trong trường hợp của 1 kết nối vào Internet, những dịch vụ này có
thể rất tinh vi và phức tạp. Ví dụ của những dịch vụ này là World Wide Web

(WWW), Wide Area Information
Service (WAIS), Gopher và Mosaic. Hầu hết những hệ thống này liên quan đến việc cung cấp thông tin cho
người dùng theo những cách tổ chức khác nhau, cho phép tim kiếm thông tin một cách có cấu trúc.
Phần lớn những hệ thống này có những giao thức riêng. Một vài trường hợp như Mosaic sử dụng nhiều
giao thức để nhận được thông tin. Bạn phải cẩn thận khi thiết kế một danh sách truy cập áp dụng với mỗi
dịch vụ. Trong nhiều trường hợp, các danh sách truy cập có liên quan đến nhau vì mối liên quan giữa các
dịch vụ.

Tổng kết

Mặc dù bài viết này minh họa cách sử dụng các tính năng ở mức network-layer của Cisco để tăng cường tính
bảo mật cho mạng IP, để có được sự bảo mật đúng nghĩa, bạn phải quan tâm đến tất cả hệ thống ở tất cả
các mức

Tài liệu tham khảo

Cheswick, B. and Bellovin, S. Firewalls and Internet Security. Addison-Wesley.
Comer, D.E and Stevens, D.L., Internetworking with TCP/IP. Volumes I-III. Englewood Cliffs, New Jersey:
Prentice Hall; 1991-1993.
Curry, D. UNIX System Security—A Guide for Users and System Administrators.
Garfinkel and Spafford. Practical UNIX Security.O'Reilly & Associates.
Quarterman, J. and Carl-Mitchell, S. The Internet Connection, Reading, Massachusetts: Addison-Wesley
Publishing Company; 1994.
Ranum, M. J. Thinking about Firewalls, Trusted Information Systems, Inc.
Stoll, C. The Cuckoo's Egg. Doubleday.
Treese, G. W. and Wolman, A. X through the Firewall and Other Application Relays.

Requests For Comments (RFCs)
RFC 1118. "The Hitchhiker's Guide to the Internet." September 1989.
RFC 1175. "A Bibliography of Internetworking Information." August 1990.
RFC1244. "Site Security Handbook." July 1991.
RFC 1340. "Assigned Numbers." July 1992.
RFC 1446. "Security Protocols for SNMPv2." April 1993.
RFC 1463. "FYI on Introducing the Internet—A Short Bibliography of Introductory Internetworking Readings
for the Network Novice." May 1993.
RFC 1492. "An Access Control Protocol, Sometimes Called TACACS." July 1993.

Internet Directories
Documents at gopher.nist.gov.

The "Computer Underground Digest" in the /pub/cud directory at ftp.eff.org.
Documents in the /dist/internet_security directory at research.att.com.