HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA VIỄN THÔNG

---*---**

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC

BẢO MẬT TRONG SSL VPN

Giảng viên hướng dẫn: TS. Nguyễn Tiến Ban

Sinh viên thực hiện : Võ Trọng Giáp

Lớp : D04VT1

Hà Nội - 2008

Mục lục

Mục lục ..... **i**

Danh mục hình vẽ ..... **iv**

Danh mục bảng biểu ..... **v**

Thuật ngữ viết tắt ..... **vi**

Lời nói đầu ..... **viii**

CHƯƠNG 1 GIỚI THIỆU VỀ SSL VPN **1**

1.1 Khái niệm về VPN ***1***

1.2. IPSec VPN và SSL VPN ***1***

1.2.1 IPSec VPN 1

1.2.2 SSL VPN 2

1.2.3 So sánh IPSec và SSL VPN 3

1.3 Khái niệm mạng tin cậy và mô hình kết nối SSL VPN ***4***

1.3.1. Khái niệm mạng tin cậy 4

1.3.2 Khái niệm vùng cách ly DMZ 4

1.3.3 Kết nối SSL VPN 5

1.4 Kết luận ***7***

Chương 2 HOẠT ĐỘNG CỦA SSL VPN **9**

2.1 Thiết bị và Phần mềm ***9***

2.2 Giao thức SSL ***10***

2.2.1 Lịch sử ra đời 10

2.2.2 Tổng quan công nghệ SSL 12

2.3 Thiết lập đường hầm bảo mật sử dụng SSL ***15***

2.3.1 Các đường hầm bảo mật 16

2.3.2 SSL và mô hình OSI 17

2.3.3 Truyền thông lớp ứng dụng 18

2.4 Công nghệ Reverse proxy ***18***

2.5 Truy cập từ xa SSL: Công nghệ Reverse proxy plus ***20***

2.5.1 Lưu lượng non-web qua SSL 20

2.5.2 Thiết lập kết nối mạng qua SSL 21

2.5.3 Công nghệ truy cập mạng với các ứng dụng Web 23

2.5.4 Applet 23

2.5.5 Truy cập từ xa tới nguồn tài nguyên file và tài nguyên khác....23
2.5.6 Các ứng dụng nội bộ cho phép truy nhập qua Internet....26
2.5.7 Giao diện truy nhập từ xa....29
2.5.8 Các công cụ quản trị....34
2.5.9 Hoạt động....34
2.6 Ví dụ phiên SSL VPN....37
2.7 Kết luận....38
CHƯƠNG 3: BẢO MẬT TRONG SSL VPN....39
3.1 Nhận thực và Xác thực....39
3.1.1 Nhận thực....39
3.1.2 Đăng nhập một lần....42
3.1.3 Xác thực....42
3.2 Các vấn đề bảo mật đầu cuối....43
3.2.1 Vấn đề dữ liệu nhạy cảm ở trong vùng không an toàn và giải pháp....43
3.2.2 Vấn đề công cụ tìm kiếm của nhóm thứ ba và giải pháp....48
3.2.3 Vấn đề người dùng quên đăng xuất và giải pháp....50
3.3.2 Vấn đề virus xâm nhập vào hệ thống mạng công ty qua SSL VPN....54
3.2.4 Vấn đề sâu xâm nhập vào mạng công ty qua SSL VPN và giải pháp....55
3.2.5 Vấn đề của các vùng không an toàn....57
3.2.6 Các hacker kết nối tới mạng công ty....59
3.2.7 Vấn đề rò rỉ thông tin mạng nội bộ và giải pháp....59
3.2.8 Đầu cuối tin cậy....61
3.2.9 Phân cấp truy cập dựa trên tình trạng điểm cuối....62
3.3 Vấn đề bảo mật phía máy chủ....64
3.3.1 Vấn đề tường lửa và các công nghệ bảo mật khác bị tấn công và giải pháp....64
3.3.2 Vấn đề yếu điểm của mức ứng dụng và giải pháp....68
3.3.3 Mã hóa....70
3.3.4 Cập nhật các máy chủ SSL VPN....70
3.3.5 So sánh Linux và Windows....70
3.3.6 Một vài khái niệm bảo mật khác của thiết bị SSL VPN....70
3.4 Kết luận....71
Chương 4 TRIỂN KHAI SSL VPN....73
4.1 Xác định yêu cầu....73

4.1.1 Mô hình truy nhập dữ liệu....73
4.1.2 Xác định nhu cầu của người dùng....73
4.2 Chọn lựa thiết bị SSL VPN phù hợp....75
4.2.1 Xác định mức độ truy cập phù hợp....76
4.2.2 Lựa chọn giao diện người dùng phù hợp....76
4.2.3 Quản lý mật khẩu từ xa....78
4.2.4 Sự tương thích của các chuẩn bảo mật....78
4.2.5 Platform....79
4.3 Xác định chức năng của SSL VPN sẽ được sử dụng....80
4.4 Xác định vị trí đặt máy chủ SSL VPN....81
4.4.1 Văn phòng....81
4.4.2 Vùng cách ly....82
4.4.3 Bên ngoài phạm vi tường lửa....84
4.4.4 Air Gap....85
4.4.5 Bộ tăng tốc SSL....86
4.5 Lên kế hoạch thực hiện....88
4.6 Đào tạo người dùng và nhà quản trị....89
4.7 Kết luận....89
Chương 5 MÔ PHỎNG SSL VPN....90
5.1 Giới thiệu....90
5.2 Thực hiện mô phỏng....91
5.2 Kết luận....96
Kết luận....97
Tài liệu tham khảo....98

Danh mục hình vẽ

Hình 1.1. Mô hình cơ bản VPN.....1
Hình 1.2. Mô hình DMZ.....5
Hình 1.3. Kết nối Client – SSL VPN hub.....6
Hình 1.4. Kết nối SSL VPN qua mạng không tin cậy.....7
Hình 2.1. Một số thiết bị SSL VPN.....10
Hình 2.2. Ví dụ về HTTPS.....11
Hình 2.3. Thuật toán mật mã đối xứng.....13
Hình 2.4. Thuật toán mật mã bất đối xứng.....14
Hình 2.5. Kết hợp hai thuật toán.....14
Hình 2.6. Đường hầm bảo mật.....16
Hình 2.7. Reverse proxy.....19
Hình 2.8. Gói tin mã hóa SSL.....22
Hình 2.9. Ổ đĩa từ xa.....24
Hình 2.10. Truy cập file.....25
Hình 2.11. Telnet.....25
Hình 2.12. Màn hình đăng nhập.....30
Hình 2.13. Cân bằng tải ở bên trong.....36
Hình 2.14. Cân bằng tải ở bên ngoài.....37
Hình 3.1. SSL VPN trong DMZ.....65
Hình 3.2. SSL VPN trong mạng nội bộ.....67
Hình 3.3. Bộ lọc lớp ứng dụng.....69
Hình 4.1. Máy chủ trong mạng nội bộ.....81
Hình 4.2. Máy chủ đặt trong DMZ.....83
Hình 4.3. Máy chủ ngoài phạm vi tường lửa.....84
Hình 4.4. AirGap.....86
Hình 4.5. Bộ tăng tốc SSL ở giữa DMZ và tường lửa.....87
Hình 4.6. Bộ tăng tốc đặt ở trong mạng nội bộ.....88
Hình 5.1. Mô hình mô phỏng.....90
Hình 5.2. Máy ảo ASA.....91

Hình 5.3. ASA trên VMware.....92
Hình 5.4. Cấu hình kết nối.....92
Hình 5.5. Cấu hình VMware network adapter.....93
Hình 5.6. Fidder 2.....93
Hình 5.7. Đăng nhập Cisco ASDM laucher.....93
Hình 5.8. Cisco ASDM 94
Hình 5.9. Cấu hình SSL VPN.....94
Hình 5.10. Thêm người dùng trong SSL VPN.....95
Hình 5.11. Đăng nhập đối với người dùng từ xa.....95
Hình 5.12. Màn hình làm việc người dùng từ xa.....95
Hình 5.13. Một số chức năng SSL VPN.....96

Danh mục bảng biểu

Bảng 3.1. Chính sách đối với các máy có độ tin cậy khác nhau.....63

Thuật ngữ viết tắt

Thuật ngữ	Tiếng Anh	Tiếng Việt
3DES	Triple Data Encryption Standard	Chuẩn mã hóa dữ liệu ba mức
ACL	Access Control List	Danh sách điều khiển truy cập
AES	Advanced Encryption Standard	Chuẩn mã hóa dữ liệu mở rộng
AH	Authentication Header	Mào đầu nhận thực
ASIC	Application Specific Integrated Circuit	Mạch tích hợp ứng dụng cụ thể
ASP	Active Server Page	Ngôn ngữ web động của Microsoft
ATM	Asynchronous Transfer Mode	Chế độ truyền không đồng bộ
CA	Certificate Authorities	Chứng thực nhận thực
CRM	Customer Relationship Management	Hệ thống quản lý khách hàng
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DMZ	Demilitarized Zone	Mạng biên
DNS	Domain Name System	Hệ thống quản lý tên miền
DoD	Department of Defense	Phòng bảo mật
DoS	Denial of Service	Tấn công từ chối dịch vụ
ESP	Encapsulating Security Payload	Đóng gói dữ liệu bảo mật
FPA	Forced Periodic Re-authentication	Bắt buộc nhận thực theo chu kỳ
FTP	File Transfer Protocol	Giao thức truyền file
GUI	Graphic User Interface	Giao diện đồ họa người dùng
HTTP	HyperText Transfer Protocol	Giao thức trình duyệt web
HTTPS	Hypertext Transfer Protocol over SSL	Giao thức HTTP qua SSL
ICMP	Internet Control Message Protocol	Giao thức bản tin điều khiển Internet
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập
IETF	Internet Engineering Task Force	Nhóm đặc trách về kỹ thuật Internet
IPSec	IP Security	Giao thức bảo mật Internet
ISAKMP	Internet Security Association and Key Management Protocol	Giao thức tổ hợp bảo mật Internet và quản lý khóa
KMV	Keyboard/Mouse/Video	Bàn phím/Chuột/Video
L2F	Layer-2 Forwarding	Giao thức chuyển tiếp lớp 2
L2TP	Layer-2 Tunneling Protocol	Giao thức đường hầm lớp 2
LAN	Local Area Network	Mạng cục bộ
LDAP	Lightweight Directory Access Protocol	Giao thức truy cập thư mục
LSP	Layered Service Provider	Dịch vụ phân lớp
MPLS	MultiProtocol Layer Switching	Chuyển mạch nhãn đa giao thức
NSP	Name Space Provider	Dịch vụ không gian tên
PCT	Private Communications Technology	Công nghệ giao tiếp cá nhân
PDA	Personal Data Assistants	Thiết bị trợ giúp cá nhân
PKI	Public Key Infrastructure	Cấu trúc khóa công cộng
POP	Point of Presence	Điểm kết nối

PPTP	Point to Point Tunneling Protocol	Giao thức đường hầm điểm-điểm
RADIUS	Remote Authentication Dial In User Service	Giao thức nhận thực từ xa
S-HTTP	Secure hypertext transfer protocol	Giao thức bảo mật HTTP
SMB	Small and Medium Business	Nhóm người dùng vừa và nhỏ
SNMP	Simple Network Management Protocol	Giao thức quản lý mạng đơn giản
SOHO	Small Office/Home Office	Văn phòng nhỏ / Nhà nhỏ
SSL	Secure Socket Layer	Lớp Socket bảo mật
SSO	Single Sign On	Đăng nhập một lần
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tải
UDP	User Datagram Protocol	Giao thức dữ liệu người dùng
URL	Uniform Resource Locator	Địa chỉ tham chiếu Internet
USB	Universal Serial Bus	Chuẩn kết nối tuần tự đa năng
VoIP	Voice over IP	Thoại qua Internet
VPN	Vitual Private Network	Mạng riêng ảo
XML	Extensible Markup Language	Ngôn ngữ đánh dấu mở rộng

Lời nói đầu

Ngày nay, sự phát triển của khoa học công nghệ đã làm thay đổi nhiều bộ mặt thương mại, đóng góp vào sự phát triển của kinh tế thế giới. Trong đó, công nghệ thông tin và truyền thông có một vai trò rất quan trọng.

Cùng với sự phát triển của thương mại, nhu cầu trao đổi thông tin giữa các chi nhánh ở các vùng khác nhau đã dẫn tới sự ra đời của công nghệ mạng riêng ảo VPN. Mạng VPN tận dụng được ưu điểm của cơ sở hạ tầng Internet sẵn có, thiết lập kết nối riêng ảo với chi phí rất thấp so với đường truyền kênh riêng. Vì vậy, VPN là một giải pháp tối ưu cho các doanh nghiệp.

Các giải pháp VPN phổ biến trước đây đều dựa trên nền IPSec. Tuy nhiên, giải pháp IPSec VPN có nhiều nhược điểm như người dùng phải cấu hình client, không tương thích với giao thức phân giải địa chỉ NAT, thực hiện kết nối mạng mà không quan tâm đến điểm kết nối. Do vậy, IPSec VPN thích hợp cho các kết nối vùng – vùng. Nhưng với sự phát triển của thương mại ngày nay, ngày càng nhiều công ty muốn nhân viên cũng như đối tác của họ có thể kết nối tới mạng nội bộ từ bất kỳ đâu. SSL VPN là một giải pháp toàn diện cho trường hợp này. SSL VPN đã trở thành một trong những giải pháp VPN hữu hiệu nhất, hiện nay, nó có thể hỗ trợ kết nối mạng, kết nối ứng dụng web, non-web,…

*Với đồ án **"Bảo mật trong SSL VPN"**, tôi hy vọng có thể góp phần tìm hiểu công nghệ VPN này, trong đó chú trọng đến hoạt động và các vấn đề bảo mật cũng như các giải pháp của SSL VPN.*

Nội dung của đồ án bao gồm 5 chương, với nội dung chính như sau:

***Chương 1** giới thiệu về VPN, các giải pháp IPsec VPN và SSL VPN, so sánh những ưu điểm của SSL VPN và IPsec VPN. Chương này cũng đưa ra khái niệm mạng tin cậy và vùng cách ly trong SSL VPN.*

***Chương 2** trình bày về phương thức hoạt động của SSL VPN, các công nghệ tiền thân của SSL VPN. Trong chương này cũng mô tả các thành phần dịch vụ của SSL VPN và các cải tiến quan trọng của công nghệ này.*

***Chương 3** đề cập đến các khái niệm và vấn đề bảo mật trong SSL VPN, cách giải quyết những vấn đề này, và phân tích ưu nhược điểm của chúng.*

***Chương 4** tập trung vào phương pháp xây dựng một mô hình SSL VPN cụ thể, nội dung của chương trình bày các giải pháp VPN khác nhau cho những điều kiện cụ thể.*

***Chương 5** giới thiệu chương trình mô phỏng SSL VPN, chương trình mô phỏng này sẽ giúp hiểu rõ hơn về cấu hình SSL VPN và những ưu điểm của SSL VPN so với các VPN truyền thống.*

Do còn nhiều mặt hạn chế về trình độ cũng như thời gian nên đồ án không thể tránh khỏi nhiều thiết sót, em rất mong nhận được ý kiến đóng góp của các thầy cô và bạn đọc.

Trong thời gian làm đồ án, em đã nhận được sự giúp đỡ rất nhiệt tình của các thầy cô giáo và đặc biệt là TS. Nguyễn Tiến Ban đã giúp đỡ em rất nhiều để em có thể hoàn thành được bản đồ án này.

Em xin chân thành cảm ơn!

Hà Nội, tháng 11 năm 2007

Sinh viên

Võ Trọng Giáp

CHƯƠNG 1 GIỚI THIỆU VỀ SSL VPN

1.1 Khái niệm về VPN

Định nghĩa cơ bản của VPN là một kết nối bảo mật giữa hai hoặc nhiều địa điểm qua một mạng công cộng. Cụ thể hơn VPN là một mạng dữ liệu cá nhân được xây dựng dựa trên một nền tảng truyền thông công cộng. VPN có thể cung cấp truyền dẫn dữ liệu bảo mật bằng cách tạo ra đường hầm dữ liệu giữa hai điểm, bằng cách sử dụng mã hóa để chắc chắn rằng không có hệ thống nào khác ngoài điểm cuối của nó có thể hiểu được dữ liệu. Hình 1.1 là một ví dụ cơ bản.

Hình 1.1. Mô hình cơ bản VPN

Người dùng từ xa sẽ kết nối tới Internet qua một nhà cung cấp dịch vụ, nhà cung cấp này có thể là VPNT, Viettel, EVN,… Hình trên mô tả khái niệm của VPN, VPN ẩn và mã hóa dữ liệu, do dó làm cho hacker không thể bắt được gói dữ liệu người dùng.

1.2. IPSec VPN và SSL VPN

1.2.1 IPSec VPN

IPSec sẽ mã hóa tất cả dữ liệu đi ra và giải mã dữ liệu vào, vì vậy nó có thể sử dụng một mạng công cộng, như Internet làm phương tiện trung chuyển. IPSec VPN thường tận dụng các giao thức lớp 3 của mô hình OSI, được thực hiện bởi các kỹ thuật khác nhau:

- Authentication Header (AH) hay mào đầu nhận thực.
- Encapsulating Security Payload (ESP) hay đóng gói dữ liệu bảo mật.

AH cung cấp hai cách để nhận thực, nó có thể thực hiện bởi phần cứng hoặc phần mềm, và trong nhiều trường hợp cung cấp khả năng nhận thực người dùng qua cặp nhận thực chuẩn – tên đăng nhập và mật khẩu. Nó cũng có thể nhận thực qua một Token, hoặc theo chuẩn X.509.

Giao thức ESP cung cấp khả năng mã hóa dữ liệu. Hầu hết thực hiện dựa trên các thuật toán hỗ trợ như DES (Data Encryption Standard – Chuẩn mã hóa dữ liệu), 3DES (Triple Data Encryption Standard – Chuẩn mã hóa dữ liệu ba mức), hoặc AES (Advanced Encryption Standard – Chuẩn mã hóa dữ liệu mở rộng). Trong hầu hết các trường hợp, IPSec sẽ thực hiện một quá trình bắt tay trong đó cần mỗi điểm đầu cuối trao đổi khóa và sau đó chấp nhận các chính sách bảo mật.

IPSec có thể hỗ trợ hai kiểu mã hóa:

- Transport: mã hóa phần dữ liệu của mỗi gói, nhưng phần header không được mã hóa. Thông tin định tuyến ban đầu trong gói tin không được bảo vệ khỏi nhóm người dùng không nhận thực.
- Tunnel: Mã hóa cả header và dữ liệu. Thông tin định tuyến ban đầu được mã hóa, và một chuỗi các thông tin định tuyến được thêm vào gói để định tuyến dữ liệu giữa hai điểm cuối.

IPSec hỗ trợ một giao thức gọi là ISAKMP/Oakley (Internet Security Association and Key Management Protocol/Oakley – Giao thức tổ hợp bảo mật Internet và quản lý khóa/Oakley). Giao thức này cho phép người nhận có được một khóa công cộng và nhận thực người gửi bằng cách sử dụng chữ ký kỹ thuật số. Quá trình đầu tiên của một hệ thống mật mã dựa trên khóa là trao đổi một khóa của một cặp khóa. Một khi các khóa được trao đổi, thì lưu lượng có thể được mã hóa. IPSec được mô tả trong nhiều RFC, bao gồm 2401, 2406, 2407, 2408, và 2409.

Nhược điểm của VPN dựa trên client (như IPSec) là cần phải cấu hình hoặc cài đặt một vài phần mềm đặc biệt. Có nhiều phần mềm được tích hợp sẵn VPN trong hệ điều hành (như Windows hay Linux), nhưng người dùng vẫn cần phải cấu hình client. Trong một vài trường hợp, thậm chí người dùng cần phải cài đặt cả chứng thực client. Thêm nữa, có thể phải dùng đến tường lửa, phần mềm diệt virus và một vài công nghệ bảo mật khác. Cấu hình cơ bản cho một IPSec VPN là một thiết bị hub ở trong tâm và một máy tính client từ xa. Khi kết nối được thiết lập thì sau đó một đường hầm được tạo ra qua mạng công cộng hoặc mạng riêng. Đường hầm mã hóa này sẽ bảo mật phiên truyền thông giữa hai các điểm cuối, và hacker sẽ không thể đọc được phiên truyền thông.

1.2.2 SSL VPN

Một phương thức khác để bảo mật dữ liệu qua Internet là SSL (Secure Socket Layer – Lớp socket bảo mật). SSL là một giao thức cung cấp khả năng mã hóa dữ liệu trên

mạng. SSL là một giao thức mạng có khả năng quản lý kênh truyền thông được bảo mật và mã hóa giữa server và client. SSL được hỗ trợ trong hầu hết các trình duyệt thông dụng như Internet Explorer, Netscape và Firefox. Một trong những chức năng chính của SSL là đảm bảo bí mật bản tin. SSL có thể mã hóa một phiên giữa client và server và do đó các ứng dụng có thể truyền và xác thực tên đăng nhập và mật khẩu mà không bị nghe trộm. SSL sẽ khóa các phiên nghe trộm dữ liệu bằng cách xáo trộn nó.

Một trong những chức năng quan trọng của SSL là khả năng cung cấp cho client và server có thể nhận thực được chúng qua việc trao đổi các chứng thực. Tất cả lưu lượng giữa SSL server và SSL client được mã hóa bằng cách sử dụng một khóa chia sẻ và một thuật toán mã hóa. Tất cả điều này được thực hiện qua quá trình bắt tay, nơi bắt đầu khởi tạo phiên. Một chức năng khác của giao thức SSL là SSL đảm bảo bản tin giữa hệ thống gửi và hệ thống nhận không bị giả mạo trong suốt quá trình truyền. Kết quả là SSL cung cấp một kênh bảo mật an toàn giữa client và server. SSL được thiết kế cơ bản cho việc bảo mật mà trong suốt đối với người dùng. Thông thường một người dùng chỉ phải sử dụng địa chỉ URL để kết nối tới một server hỗ trợ SSL. Server sẽ chấp nhận kết nối trên cổng TCP 443 (cổng mặc định cho SSL). Khi nó kết nối được tới cổng 443 thì quá trình bắt tay sẽ thiết lập phiên SSL.

Sự kết hợp của SSL và VPN tạo ra các ưu điểm sau:

- Sự kết hợp giữa kỹ thuật mã hóa SSL và công nghệ proxy làm cho việc truy cập tới ứng dụng Web và các ứng dụng công ty trở nên thực sự dễ dàng.
- Sự kết hợp của các công nghệ có thể cung cấp quá trình xác thực client và server với dữ liệu được mã hóa giữa các cặp client-sever khác nhau.
- Trên hết, là nó có thể thiết lập SSL VPN dễ dàng hơn nhiều so với thiết lập IPSec VPN.

Trong một vài trường hợp, việc thực thi SSL VPN tương tự như đối với IPSec. SSL VPN cũng cần phải có một số thiết bị hub. Các client cũng cần phải có một số phần mềm giao tiếp, được gọi là các trình duyệt hỗ trợ SSL. Hầu hết các máy tính đều có một trình duyệt hỗ trợ SSL, bao gồm cả một chứng thực SSL root từ CA (Certificate Authorities – Chứng chỉ nhận thực) công cộng. Thiết bị hub trung tâm và phần mềm client sẽ mã hóa dữ liệu qua một mạng IP. Quá trình này sẽ bảo mật dữ liệu chống các cuộc tấn công của hacker.

1.2.3 So sánh IPSec và SSL VPN

Thông thường IPSec VPN sẽ sử dụng một phần mềm chuyên biệt ở đầu cuối, thiết bị hub và client. Điều này cung cấp kết nối bảo mật cao. Mỗi điểm cuối cần một vài bước thiết lập cấu hình, và cần phải có nhiều sự can thiệp của con người vào quá trình xử lý.

SSL VPN thường không cần thiết phải có các phần mềm client đặc biệt. SSL VPN có toàn bộ chức năng bảo mật như IPSec VPN. Hơn nữa, nếu trình duyệt được cập nhật thường xuyên thì quá trình cấu hình được tự động xử lý.

Cả IPSec và SSL VPN có thể cung cấp truy nhập từ xa an toàn cho ứng dụng thương mại. Cả hai công nghệ này đều hỗ trợ nhiều giao thức nhận thực, bao gồm chứng thực X.509. Về cơ bản, IPSec không thể bị tất công, trừ khi sử dụng chứng thực. Server SSL VPN luôn luôn xác thực với một chứng thực số, SSL sẽ quyết định server đích nào được xác thực bằng CA tương ứng. SSL cung cấp khả năng mềm dẻo trong trường hợp giới hạn người dùng tin cậy hoặc rất khó để cài đặt chứng thực người dùng (ví dụ như các máy tính công cộng).

1.3 Khái niệm mạng tin cậy và mô hình kết nối SSL VPN

1.3.1. Khái niệm mạng tin cậy

Một mạng tin cậy của một công ty là một mạng mà công ty sử dụng để quản lý hoạt động. Trong nhiều trường hợp, một mạng tin cậy thường được định nghĩa như một vùng an toàn. Mạng tin cậy thường có các hệ thống đầu cuối, các trang web nội bộ, xử lý dữ liệu, tin nhắn nội bộ. Trong nhiều công ty, mạng tin cậy được cho phép trực tiếp tác động qua lại với các hệ thống mà không cần mã hóa. Có một vấn đề với định nghĩa trên là có quá nhiều mạng tin cậy được tạo ra bởi các công ty. Mạng tin cậy đôi khi không phải luôn đáng tin cậy. Tức là trong một số trường hợp mạng tin cậy không được tin cậy. Lý do là nó được kết nối quá nhiều tới bên ngoài. Do đó, trên thực tế là một mạng tin cậy được xem như một mạng mà các nhân viên nội bộ công ty sử dụng khi ở cơ quan hoặc ở đâu đó qua một đường truyền bảo mật.

1.3.2 Khái niệm vùng cách ly DMZ

DMZ (Demilitarized zone) là một mạng cách ly, được đặt như là một vùng đệm giữa một mạng tin cậy của công ty và các mạng không tin cậy (Internet luôn được xem như là một mạng không tin cậy). Mục đích ban đầu của DMZ sẽ ngăn chặn người dùng bên ngoài trực tiếp kết nối vào một mạng tin vậy. Hình 1.2 mô tả một DMZ thông thường.

Hầu hết các DMZ được cấu hình thông qua một tập hợp các luật được xác định bằng các chính sách và sau đó được thực hiện thông qua các thủ tục của công ty. Một trong các luật cơ bản là một cổng đơn lẻ (như cổng 80) không được DMZ cho phép truy cập. Vì vậy nếu bạn thử truy cập một ứng dụng trên một DMZ qua HTTP trên cổng 80 thì bạn sẽ không truy cập được. Đây chính là cách DMZ thực hiện, nó giữ lại các lưu lượng không tin cậy đang cố đi vào mạng tin cậy. DMZ sẽ lọc lưu lượng và giới hạn truy cập tới mạng tin cậy thông qua bộ lọc và quá trình nhận thực, và trong một vài trường hợp DMZ sẽ chặn toàn bộ lưu lượng nếu cần thiết. Dưới đây là một vài chức năng mà DMZ có thể thực hiện:

- Chặn các cuộc quét cổng vào mạng tin cậy.
- Chặn các truy cập vào mạng tin cậy qua một cổng TCP đơn lẻ.
- Chặn DOS (Denial of Service Attack – Tấn công từ chối dịch vụ).
- Quét vius, nội dung, kích cỡ các e-mail.
- Chặn các cuộc nghe trộm / thay đổi gói.

Hình 1.2. Mô hình DMZ

1.3.3 Kết nối SSL VPN

Vậy làm thế nào SSL VPN tích hợp vào trong cơ cấu mạng của công ty? Dưới đây là hai trường hợp của truy nhập SSL VPN.

- SSL VPN truy nhập tới các thiết bị được chọn qua một SSL VPN hub (truy nhập từ Internet).
- SSL VPN truy nhập tới một mạng chuyên biệt, sử dụng một SSL VPN hub nằm giữa mạng tin cậy và mạng chuyên biệt.

a) SSL VPN – Hub

Một trong những chức năng bảo mật chính của một DMZ là khả năng hủy kết nối IP ở nhiều điểm trong DMZ và mạng tin cậy. Hình 1.3 mô tả một kết nối từ một client qua Internet (không tin cậy) tới một SSL VPN hub trong một mạng tin cậy.

Lưu lượng được định tuyến vào DMZ, và sau đó bị dừng lại ở bộ định tuyến. Bây giờ, địa chỉ IP máy trạm được chuyển sang một địa chỉ IP DMZ, ví dụ 10.10.10.10. DMZ sau đó có thể thực hiện một vài nhận thực và cho phép lưu lượng định tuyến tới vùng tin cậy của DMZ. Tại điểm này, địa chỉ IP máy trạm có thể được chuyển sang một địa chỉ IP khác, như 192.168.10.12. Sau đó các gói tin sẽ được định tuyến vào thiết bị SSL VPN (hub).

SSL VPN sẽ thực hiện một vài kiểm tra thêm nữa trên lưu lượng dựa trên các luật và quá trình nhận thực. Nếu vượt qua thì lưu lượng có thể được định tuyến tới máy chủ bản tin HTTP. Ví dụ thực tế cho trường hợp này là một nhân viên đang trong thời kỳ nghỉ phép có thể truy cập e-mail nội bộ một cách an toàn mà không sợ bị lộ trước hacker.

b) SSL VPN – Mạng riêng

Hình 1.3. Kết nối Client – SSL VPN hub

Nhiều công ty thương mại sẽ có nhiều mạng riêng, các mạng riêng này có thể nối không chỉ trong một vùng nhỏ, mà có thể trải rộng trên toàn cầu. Trong nhiều trường hợp, các mạng riêng này sẽ kết nối với nhau qua các nhà cung cấp dịch vụ Internet ISP (Internet Service Provider). Cũng có nhiều công ty có nhiều mạng riêng ở cơ quan, nhưng chỉ có một điểm POP (Point of Presence – Điểm kết nối) tới Internet. Điều này sẽ đòi hỏi thêm một số chính sách bảo mật để giữ mạng an toàn, mỗi POP là một nơi để hacker có

thể truy cập vào mạng. Thêm nữa, không phải tất cả các nhân viên công ty là đáng tin cậy, một vài người có thể là mối đe dọa cho tài nguyên công ty. Và kết quả là, các công ty lớn thường để cho mạng tin cậy của mình trở thành không tin cậy, do có thể có truy cập không xác thực vào mạng riêng ở một vài điểm – không chỉ là ở các POP mà có thể từ ISP. Hình 1.4 mô tả SSL VPN có thể được sử dụng để cung cấp truy cập an toàn trong khi mạng không tin cậy.

Trong hình 1.4, người dùng cuối được đặt trong mạng tin cậy của công ty. Người dùng cuối có thể muốn được truy cập một trang web, tin nhắn hoặc máy chủ file của họ. Lưu lượng khởi tạo ở máy tính người dùng và sẽ được định tuyến qua một địa chỉ mạng tin cậy, ví dụ như 192.168.10.22. Các gói tin bị dừng ở các SSL VPN hub, ở thiết bị này, dữ liệu sẽ được chuyển tới dịch vụ web. Ngày nay, một công ty lớn có thể chắc chắn rằng dữ liệu của họ được bảo mật, không thể bị xem trộm bởi các hacker qua SSL VPN.

Hình 1.4. Kết nối SSL VPN qua mạng không tin cậy

1.4 Kết luận

Chương này giới thiệu về VPN, các phương thức IPSec VPN, SSL VPN và một số ưu nhược điểm của chúng. Trong nội dung chương cũng đưa ra khái niệm mạng tin cậy và DMZ, đây là các khái niệm cơ bản trong SSL VPN. Qua chương này, chúng ta có thể nhận

thấy các ưu điểm rõ ràng của SSL VPN so với IPSec VPN và đó cũng là lý do để SSL VPN phát triển mạnh mẽ trong thời gian qua.

Chương 2 HOẠT ĐỘNG CỦA SSL VPN

Các sản phẩm SSL VPN cho phép người dùng thiết lập các phiên truy cập từ xa an toàn từ trình duyệt kết nối Internet. Cho phép người dùng truy cập e-mail, hệ thống thông tin khẩn cấp, và nhiều tài nguyên mạng khác từ bất kỳ nơi nào. Mặc dù thiết bị SSL VPN thoạt nhìn rất đơn giản nhưng nó là một công nghệ phức tạp và tiên tiến.

Tại thời điểm hiện nay, không có một chuẩn nào cho công nghệ SSL VPN (trừ SSL, HTTP, và các thành phần khác của SSL VPN). Một vài SSL VPN của tổ chức thứ ba, chủ yếu mô tả các chức năng, không phải là các kỹ thuật cụ thể để thực hiện các chức năng đó. Với sự cạnh tranh cao trong thị trường SSL VPN, các nhà sản xuất thiết bị cũng không công khai các kỹ thuật bên trong sử dụng trong các sản phẩm. Tuy nhiên, mặc dù không có các thông tin từ nhà sản xuất, ta vẫn có thể hiểu được công nghệ SSL VPN. Tất cả các các đơn đặt hàng từ khác hàng đều yêu cầu cung cấp dịch vụ dựa trên truy cập web từ xa. Và kết quả là, các công nghệ cơ bản sử dụng trong các sản phẩm SSL VPN có nhiều đặc điểm chung.

2.1 Thiết bị và Phần mềm

Trong thị trường hiện nay, các sản phẩm bảo mật như SSL VPN thường được bán dưới dạng *thiết bị*, thiết bị thường được xem như là một hộp đen, có nghĩa là người quản trị mạng không cần thiết phải hiểu cách chúng thực hiện. Về lý thuyết, các thiết bị giảm chi phí trong việc cài đặt, cấu hình, và bảo trì một hệ thống công nghệ thông tin.

Mặc dù có một vài sự khác biệt trong các công nghệ bên trong, hầu hết các thiết bị bao gồm các máy tính chạy phần mềm SSL VPN trên một hệ điều hành. Do đó, đứng trên quan điểm bảo mật, thực chất không có các điểm khác biệt khi thực hiện SSL VPN bằng thiết bị so với SSL VPN bằng phần mềm, phần mềm này có thể được cài đặt trên các máy chủ của người mua.

Tuy nhiên, trên phương diện thực tế, các thiết bị thông thường được đóng gói cùng với hệ điều hành điều khiển, phần mềm SSL VPN và một vài cấu hình cơ bản. Kết quả là nó giảm được các sai sót của con người trong quá trình cài đặt và cấu hình thiết bị, và chắc chắc không có xung đột giữa phần cứng và phần mềm. Do đó trong nhiều trường hợp, thiết bị có nhiều ưu điểm bảo mật hơn phần mềm. Các tổ chức với các chuẩn dữ liệu trung tâm khuyến nghị rằng các máy chủ thích hợp với sản phẩm dựa trên phần mềm hơn, đây là một trường hợp đặc biệt khi mà người quản trị đã có kinh nghiệm trong các hệ thống phần cứng.

Hình 2.1 mô tả các thiết bị SSL VPN, từ trái qua phải là các thiết bị của Safenet, Juniper Networks và Whale Communications.

Hình 2.1. Một số thiết bị SSL VPN

Bất chấp nhiều có nhiều thiết bị khác nhau và hoạt động bên trong của chúng cũng khác nhau, công nghệ cơ bản của SSL VPN vẫn được xác định rõ ràng.

2.2 Giao thức SSL

Giao thức SSL là thành phần chính của công nghệ SSL VPN. Do đó, việc hiểu được SSL sẽ giúp chúng ta hiểu được cách làm việc của SSL VPN.

2.2.1 Lịch sử ra đời

Các trang web sử dụng giao thức HTTP (Hypertext Transfer Protocol – Giao thức truyền siêu liên kết). Bản thân HTTP không có mã hóa hay các biện pháp bảo vệ dữ liệu được truyền giữa người dùng và máy chủ web. Với sự phát triển của World Wide Web trong những năm đầu của thập kỷ 90, và sự mở rộng trong các hoạt động thương mại sử dụng web bao gồm truyền các thông tin bí mật qua mạng Internet, cần phải loại trừ khả năng bị nghe trộm bởi nhóm người không xác thực trên các cuộc giao tiếp giữa các máy tính qua mạng Internet.

Một vài công nghệ đã được phát triển để thực hiện điều này, tất cả chúng để sử dụng mã hóa để bảo vệ dữ liệu nhạy cảm. Giao thức chứng tỏ được những ưu điểm vượt trội và nó nhanh chóng trở thành chuẩn cho giao tiếp web an toàn là SSL.

SSL phiên bản 1.0 được giới thiệu trong trình duyệt Mosaic năm 1994, và phiên bản cải tiến (SSL phiên bản 2.0) được thương mại hóa vào cuối năm đó khi những người tạo ra Mosaic thành lập Netscape Communication và tích hợp vào trình duyệt Navigator của họ.

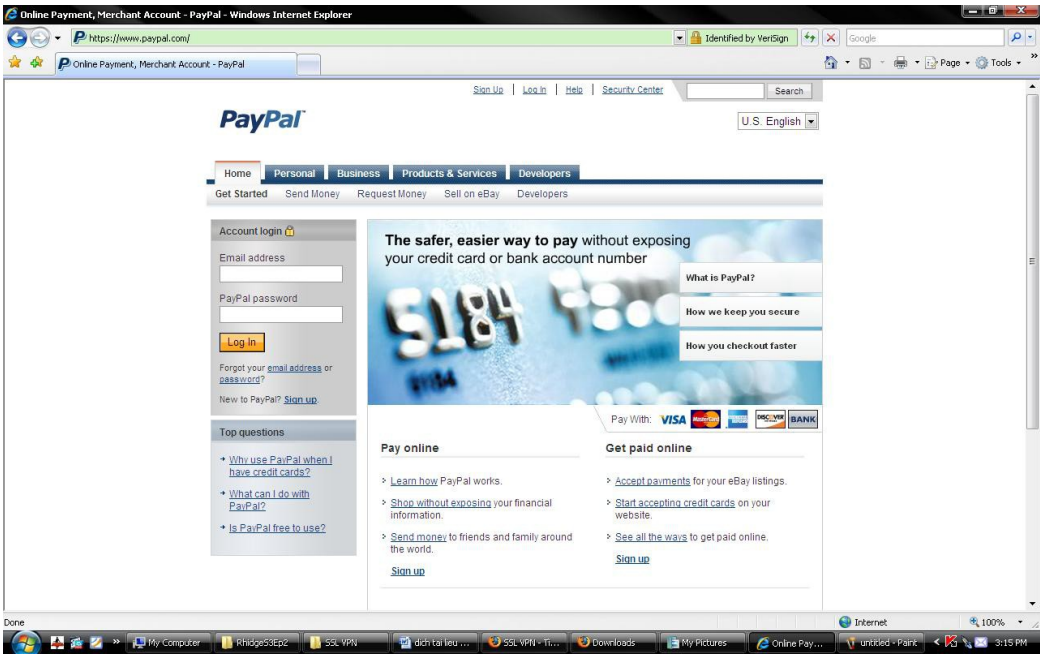
Và trong trường hợp này, bằng cách nhìn vào địa chỉ URL của trang web trong trình duyệt, người dùng có thể xác định trang web nào sử dụng SSL trong phiên giao tiếp. Các trang web mã hóa SSL có tiền tố là HTTPS trong khi trang web bình thường có tiền tố là HTTP. (Ngày nay, các trình duyệt thường thể hiện SSL dưới dạng biểu tượng, như một ống khóa hay một chìa khóa,…).

HTTPS là một giao thức web sử dụng SSL để mã hóa HTTP, nó được sử dụng rộng rãi cho các phiên truyền thông bảo mật. HTTPS không phải là S-HTTP, một giao thức mã hóa hai chiều phiên giao tiếp trang web, S-HTTP là một mở rộng của giao thức HTTP, được sử dụng hỗ trợ bảo mật dữ liệu truyền qua World Wide Web. S-HTTP được thiết kế

để truyền các bản tin một cách an toàn trong khi SSL được thiết kế để thiết lập một kết nối bảo mật giữa hai máy tính. S-HTTP đã cạnh tranh với HTTP trong những ngày đầu, nhưng về cơ bản đã thất bại so với HTTPS trong lĩnh vực thương mại điện tử (do không mã hóa các thông tin phiên), và đã không được sử dụng nữa.

Ngày nay, các máy chủ thường cung cấp dịch vụ web (HTTP) trên cổng 80 và lưu lượng web đã mã hóa SSL (HTTPS) trên cổng 443.

Hình 2.2 là một trang web đã mã hóa HTTPS. Lưu ý https ở đầu địa chỉ URL và biểu tượng ổ khóa ở cần phía trên bên phải của hình.



Hình 2.2. Ví dụ về HTTPS

Năm 1995, Microsoft đã đưa ra một phiên bản Internet Explorer, với một công nghệ mã hóa riêng gọi là PCT (Private Communications Technology – Công nghệ giao tiếp cá nhân). PCT có một vài ưu điểm so với SSL phiên bản 2.0. Tuy nhiên, ngay sau khi phiên bản Internet Explorer được đưa ra, Netscape đã đưa ra phiên bản SSL 3.0, bao gồm các ưu điểm của PCT, sau đó SSL 3.0 đã đưa truyền thông web bảo mật trong thương mại trở về với SSL.

Năm 1996, sự phát triển của World Wide Web trở thành một kênh thương mại lớn và công nghệ truyền thông trở nên được đảm bảo, với sự phát triển của SSL, tổ chức IETF (Internet Engineering Task Force – Nhóm đặc trách về kỹ thuật Internet) bắt đầu chuẩn hóa giao thức SSL. Năm 1999, IETF hoàn thành xong và thiết lập SSL như là một chuẩn của truyền thông web với tên gọi TLS (Transport Layer Security – Lớp bảo mật trung chuyển).

Bên cạnh việc bảo vệ dữ liệu thông qua mã hóa, SSL sử dụng kỹ thuật băm (hashing) để chắc chắn nội dung phiên giao tiếp không bị thay đổi trong suốt quá trình một máy tính gửi một tin nhắn và bên nhận đọc được nó.

Một giá trị băm là một số được tạo từ một chuỗi văn bản bằng cách áp dụng thuật toán toán học. Giá trị băm thường nhỏ hơn text và được tạo bởi một công thức, công thức này đảm bảo rằng giá trị văn bản nguồn khác nhau thì giá trị băm sẽ khác nhau. Công thức băm là một hàm một chiều, có nghĩa là không thể xác định đoạn văn bản ban đầu từ giá trị băm. Hashing là quá trình thực hiện công thức băm vào đoạn văn bản để đưa ra giá trị băm.

Cũng cần lưu ý rằng mặc dù thành công trên lĩnh vực bảo mật web, SSL VPN đã thất bại trên một lĩnh vực khác. Mục đích thứ hai của SSL là để tránh giả mạo website từ hacker trộm dữ liệu người dùng bằng cách giả mạo trang web mà người dùng muốn trao đổi tài chính. Mặc dù công nghệ SSL đã cho người dùng một phương thức để xác nhận nhận dạng máy chủ, nhưng sự phức tạp của nó đã làm cho phương thức này không được chấp nhận. Sau khi SSL trở nên phổ biến, được chuẩn hóa và triển khai rộng rãi, vấn đề các website giả mạo trở nên không thể chấp nhận được. Thuật ngữ *phishing* là một loại hình tội phạm trong đó người dùng bị lừa mất các thông tin bí mật vào tay các tổ chức mưu lợi. Hàng tháng, phishing làm thiệt hại khoảng hàng triệu đô la. Hiện nay, sự thiết hụt này của SSL là một vấn đề lớn cho thương mại trực tuyến dẫn tới việc thực thi SSL VPN.

SSL cũng có các kỹ thuật để xác thực máy trạm. Bằng cách tạo ra các chứng thực máy trạm, người dùng có thể chứng minh được mình đối với máy chủ. Mặc dù chức năng này của SSL hiếm khi được sử dụng, nó có tầm quan trọng lớn trong SSL VPN do nó cho phép máy chủ nhận diện mức độ tin tưởng của máy trạm.

Vậy tóm lại, SSL có các mục đích sau:

- Bảo mật truyền thông.
- Đảm bảo toàn vẹn dữ liệu.
- Xác thực máy chủ.
- Xác thực máy trạm.

2.2.2 Tổng quan công nghệ SSL

SSL sử dụng thuật toán mật mã (cryptography) để mã hóa dữ liệu, vì vậy chỉ có hai máy tính có khả năng đọc bản tin và hiểu được nó. Điều này gọi là bảo vệ dữ liệu tin cậy. SSL hỗ trợ nhiều thuật toán mật mã khác nhau, các thuật toán này có khả năng mã hóa nhiều phiên làm việc chuyên biệt dựa trên phiên bản SSL, chính sách bảo mật công ty và hạn chế của chính quyền.

Có hai loại thuật toán mật mã được sử dụng trong mỗi phiên SSL, đối xứng và bất đối xứng. Trong khi mật mã đối xứng được sử dụng để mã hóa tất cả các giao tiếp trong

một phiên SSL thì thuật toán mật mã bất đối xứng được sử dụng để chia sẻ khóa phiên đối xứng một cách an toàn giữa người dùng và SSL VPN.

a) Thuật toán mật mã đối xứng: đảm bảo tin cậy dữ liệu

Thuật toán đối xứng sử dụng cùng một khóa để mã hóa và giải mã, và do đó cả hai bên đối thoại cần phải chia sẻ khóa như hình 2.3. Quá trình xử lý thuật toán mật mã đối xứng cần ít vòng CPU hơn quá trình xử lý bất đối xứng. Tuy nhiên, thuật toán mật mã đối xứng có một nhược điểm lớn là làm thế nào một bên chia sẻ khóa bí mật với bên kia nếu như phải truyền qua môi trường Internet không tin cậy.

Hình 2.3. Thuật toán mật mã đối xứng

Một khóa là một đoạn dữ liệu (thường là một số lớn), nó giúp cho một thuật toán mật mã để mã hóa văn bản thông thường thành văn bản mật, hoặc để giải mã văn bản mật thành văn bản ban đầu. Sử dụng cùng một thuật toán với các khóa khác nhau thì sẽ cho ra kết quả khác nhau.

b) Thuật toán mật mã bất đối xứng: Đảm bảo tin cậy dữ liệu

Thuật toán mật mã bất đối xứng giải quyết vấn đề chuyển đổi khóa nói trên. Nó sử dụng một cặp khóa, một khóa gọi là khóa bí mật và một khóa gọi là khóa công cộng. Khóa công cộng không phải là bí mật và nó được chia sẻ tới tất cả trong khi khóa bí mật thì thuộc quyền sở hữu của một máy tính nào đó. Dữ liệu đã được mã hóa với một khóa chỉ có thể được mã hóa với khóa còn lại của cặp. Ví dụ, khi Tom muốn gửi một tin nhắn tới Joe và muốn chỉ có Joe mới có thể đọc được tin nhắn, Tom sẽ mã hóa tin nhắn với khóa công cộng của Joe. Và tin nhắn chỉ được mã hóa với khóa bí mật của Joe và chỉ có Joe xử

lý khóa này thì Joe mới đọc được tin nhắn. Tương tự, khi Joe trả lời lại cho Tom, anh ta sẽ mã hóa bản tin với khóa công cộng của Tom. Và chỉ có một khóa cần phải được chia sẻ trong kiểu thuật toán bất đối xứng này là các khóa công cộng, và các khóa công cộng này không phải là bí mật, vì vậy thuật toán bất đối xứng không gặp phải vấn đề chia sẻ khóa. Các khóa công cộng có thể dễ dàng được truyền đi qua mạng Internet như mô tả ở hình 2.4.

Hình 2.4. Thuật toán mật mã bất đối xứng

Tuy nhiên, thuật toán mật mã bất đối xứng cần một bộ xử lý phức tạp và không thể mã hóa khối lượng dữ liệu lớn. Nó không thể được sử dụng để mã hóa tất cả phiên SSL. Do đó, người ta đã nghĩ đến việc dùng thuật toán mật mã bất đối xứng để truyền khóa bí mật. Và SSL đã sử dụng ý tưởng này, SSL sử dụng thuật toán mật mã bất đối xứng để truyền khóa bí mật giữa người dùng đầu xa và máy chủ, và sau đó thực hiện thuật toán mật mã đối xứng để truyền dữ liệu trong suốt phiên làm việc SSL như hình 2.5.

Hình 2.5. Kết hợp hai thuật toán

c) Thuật toán mật mã bất đối xứng: Nhận thực máy chủ

Bên cạnh việc mã hóa, thuật toán mật mã cũng cung cấp khả năng nhận thực máy chủ. Nếu một người dùng mã hóa một bản tin với khóa bí mật của người đó, bất kỳ người dùng giải mã bản tin bằng cách sử dụng khóa công cộng của người gửi thì có thể đảm bảo được rằng bên gửi đúng là người gửi bản tin. Không có ai khác có khả năng tạo ra bản tin mà có thể được giải mã bởi khóa công cộng trừ người sở hữu khóa bí mật.

Chứng thực SSL là một kỹ thuật trong đó một máy chủ web có thể chứng thực nó đối với người dùng thông qua khóa công cộng mà máy chủ đưa tới. Một bên thứ ba sử dụng chứng thực theo cách đó để chứng minh tổ chức đó đúng thật sự là nó. Do đó, khi người dùng nhận được một chứng thực từ một công ty ABC và khi dùng khóa đó để giải mã giao tiếp thành công thì tương ứng với việc công ty đó là ABC. Điều này cho phép người dùng biết được họ đang giao tiếp với công ty ABC chứ không phải là giả mạo của công ty ABC. Một chứng thực SSL là phương tiện trong đó các máy chủ có thể truyền các khóa công cộng của họ tới người dùng ở lúc bắt đầu phiên SSL.

Như mô tả ở trên, mặc dù có khả năng nhận thực của SSL, phishing vẫn tồn tại phổ biến. Do đó, cần phải có khả năng chống lừa đảo của SSL. Trong suốt quá trình thiết lập một phiên giao tiếp SSL bảo mật, máy tính người dùng sẽ cảnh báo người dùng nếu chứng thực hết hạn, hoặc không tin cậy hoặc không phù hợp với máy chủ hoặc miền mà nó nhận được. Tuy nhiên, hầu hết người dùng không hiểu được các cảnh báo trên và thường nhấn OK hoặc Accept khi có hộp thoại về các vấn đề chứng thực.

d) Thuật toán mật mã: Nhận thực máy trạm

Như đã giới thiệu ở trên, SSL cung cấp khả năng nhận thực máy trạm thông qua chứng thực. Các máy trạm có một chứng thực đại diện để máy chủ có thể nhận thực được. Mặc dù SSL hiếm khi thực hiện hai công nghệ nhận thực này, chúng có ý nghĩa quan trọng đối với SSL VPN, cho phép máy chủ SSL VPN nhận diện máy trạm ở những mức độ tin cậy khác nhau.

e) Kích cỡ khóa

Ở thời điểm hiện tại, SSL thường mã hóa với khóa phiên có độ dài 128 bit ngẫu nhiên. Do đó, sẽ là không thực tế để sử dụng các công nghệ phần cứng để giải mã dữ liệu vớ độ dài khóa này thay vào đó người ta sử dụng máy tính. Trước đây, để đạt được các tiêu chuẩn của US Export, SSL thường được sử dụng với khóa 40 bit. Nhưng ngày nay, 40 bit không thể đủ mạnh để chống lại các chương trình giải mã và do đó không thể mã hóa các thông tin nhạy cảm.

2.3 Thiết lập đường hầm bảo mật sử dụng SSL

Bây giờ chúng ta đã hiểu SSL là gì và nó hoạt động như thế nào, bây giờ đồ án sẽ mô tả làm thế nào SSL cho phép chúng ta tạo ra các đường hầm.

2.3.1 Các đường hầm bảo mật

Một đường hầm bảo mật giữa các máy tính có thể được hiểu như một kênh bảo mật truyền thông giữa hai máy qua một môi trường không an toàn. Kênh bảo mật tương tự như một đường hầm dưới sông cho phép các phương tiện đi lại giữa hai điểm đầu cuối đường hầm và tránh các yếu tố môi trường như nước ảnh hưởng tới giao thông.

Đường hầm truyền thông cho phép giao tiếp giữa hai máy tính qua các mạng công cộng một cách an toàn, vì vậy các máy tính khác trên các mạng này không thể truy cập vào giao tiếp giữa hai máy tính này.

Tuy nhiên, không giống như ví dụ đường hầm dưới sông, đường hầm mạng không thực hiện một đường truyền vật lý giữa hai máy tính và các máy tính khác. Hơn nữa, kỹ thuật đường hầm máy tính có bao gồm mã hóa tất cả các giao tiếp giữa hai máy tính, vì vậy thậm chí nếu một máy tính khác nhận được phiên truyền thông thì nó cũng không thể giải mã được nội dung thật sự của bản tinh giữa hai máy tính như mô tả ở hình 2.6.

Hình 2.6. Đường hầm bảo mật

Kỹ thuật đường hầm không phải là khái niệm được giới thiệu với công nghệ SSL VPN. Nó được sử dụng trong một số công nghệ được triển khai trước đây, mà nổi tiếng là IPSec VPN.

Một đường hầm đã mã hóa giữa hai máy tính qua một mạng không tin cậy như Internet thường được gọi là VPN, do đó việc thiết lập một đường hầm kết nối hai máy tính này tương ứng với một kết nối VPN. Hai máy tính có thể giao tiếp với nhau mà không lo lắng các máy khác có thể đọc được phiên giao tiếp. Mặc dù không hoàn toàn tránh khỏi nguy cơ các gói tin bị bắt như trên đường truyền riêng chuyên biệt nhưng VPN qua mạng Internet được đánh giá cao về khả năng bảo mật và đã được chấp nhận như là một chuẩn truyền thông trong thương mại hiện nay.

SSL VPN tạo ra các đường hầm bảo mật bằng cách thực hiện hai chức năng sau:

- Bắt buộc người dùng phải nhận thực trước khi cho phép truy cập, vì vậy chỉ có các nhóm nhận thực mới được thiết lập đường hầm.
- Mã hóa tất cả lưu lượng truyền qua và tới người dùng bằng cách thực hiện đường hầm thực sự sử dụng SSL.

Quá trình thiết lập một đường hầm SSL cần nhiều chuyển đổi các thông tin cấu hình khác nhau giữa các máy tính ở đầu cuối của kết nối. Các thông tin chi tiết liên quan đến phiên truyền thông, các giao thức mã hóa, chuyển đổi khóa,… không được đề cập chi tiết trong đồ án này do giới hạn độ dài đồ án. Tuy nhiên, để hiểu được công nghệ SSL VPN, chúng ta cần phải hiểu một chút về giao thức SSL VPN và vị trí của SSL VPN trong mô hình OSI.

2.3.2 SSL và mô hình OSI

Năm 1984, tổ chức kết nối hệ thống mở Open System Interconnect, một nhóm chuyên đưa ra các tiêu chuẩn quốc tế, đưa ra một khung tóm tắt các công nghệ phân lớp trong việc giao tiếp các máy tính gọi là mô hình OSI.

Nó bao gồm bảy lớp:

- Lớp 7: Lớp ứng dụng
- Lớp 6: Lớp trình diễn
- Lớp 5: Lớp phiên
- Lớp 4: Lớp vận chuyển
- Lớp 3: Lớp mạng
- Lớp 2: Lớp liên kết dữ liệu
- Lớp 1: Lớp vật lý

Thông thường, đường hầm VPN được thực hiện ở lớp mạng hoặc lớp thấp hơn (ví dụ, IPSec thực hiện ở lớp mạng). Truy nhập từ xa được thực hiện để thiết lập kết nối mạng mã hóa giữa một nút mạng từ xa và một mạng bên trong, tạo ra kết nối từ xa mà các lớp trên lớp 4 không thể hiểu được. Các ứng dụng thực hiện được các chức năng khi người dùng ở cơ quan và khi họ ở một điểm từ xa, ngoại trừ rằng khi yêu cầu được chuyển xuống lớp dưới, chúng bị thay thế qua các kết nối mạng tương ứng ở các địa điểm xác định của người dùng. Thỉnh thoảng, kết nối là cục bộ và thỉnh thoảng nó bao gồm đường

hầm qua mạng Internet. Việc thiết lập các kết nối này cần phải cài đặt và cấu hình các phần mềm client trên máy tính người dùng. Phần mềm client này sẽ điều khiển đường hầm lớp mạng.

SSL VPN thì lại thực hiện khác. Nó thiết lập các kết nối sử dụng SSL, ở các chức năng lớp 4 và 5. Nó cũng đóng gói thông tin ở lớp 6 và 7 và giao tiếp ở lớp cao nhất của mô hình OSI. Ngày nay, một vài SSL VPN cũng có thể tạo đường hầm lớp mạng, và trở thành công nghệ truy cập VPN linh hoạt nhất.

Một điều quan trọng nữa là SSL không hoàn toàn là một giao thức web. Nó thực hiện ở lớp phiên và lớp vận chuyển của mô hình OSI và có thể thiết lập các đường hầm giao tiếp cho nhiều giao thức lớp ứng dụng và có thể được xếp trên lớp ứng dụng. Ví dụ, mặc dù SSL mã hóa phiên web (HTTPS), SSL cũng có thể mã hóa POP3 và FTP trong nhiều môi trường, cũng có thể sử dụng SSL để mã hóa tất cả các giao thức lớp ứng dụng.

2.3.3 Truyền thông lớp ứng dụng

Vì vậy tạo sao SSL VPN không sử dụng SSL để thiết lập đường hầm lớp mạng như IPSec thực hiện?

Một trong những ưu điểm chính của SSL VPN là khả năng truy cập tài nguyên từ bất kỳ máy tính nào hoặc thậm chí là bất kỳ thiết bị cầm tay nào, ở bất cứ nơi đâu. SSL VPN không thể thực hiện ở lớp mạng do có hai lý do sau:

- Giới hạn kỹ thuật của các thiết bị nhằm tránh việc thiết lập giao tiếp lớp mạng qua SSL, nhưng cho phép truy nhập lớp ứng dụng từ trình duyệt.
- Các chính sách bảo mật thường ngăn cản việc đính kèm các điểm Internet công cộng và xem các máy tính như nút mạng.

Việc thiết lập kết nối ở mức cao hơn của mô hình OSI có thể dẫn tới vấn đề chi phí và có một số các nhược điểm. Không có các chuẩn cho truyền thông lớp ứng dụng như đối với TCP, UDP, IP, IPSec và các giao thức mạng và giao tiếp lớp vận chuyển. Các ứng dụng độc lập không xác định được một chuẩn ngôn ngữ rộng rãi, các đặc điểm hoặc định dạng nên nó làm phức tạp thêm việc điều khiển giao tiếp tới các ứng dụng đầu cuối.

Sự khác nhau giữa giao tiếp lớp ứng dụng và giao tiếp lớp mạng dẫn tới một số vấn đề lớp trong bảo mật, các vấn đề này sẽ được trình bày trong chương sau.

2.4 Công nghệ Reverse proxy

Một trong những chức năng cơ bản nhất của SSL VPN là khả năng nhận các yêu cầu người dùng và truyền chúng qua các máy chủ nội bộ. Chức năng này gọi là Reverse proxying.

Nói một cách kỹ thuật, một máy chủ reverse proxy là một máy tính nằm giữa máy chủ web nội bộ và Internet, và xuất hiện như các máy trạm bên ngoài như là một máy chủ web thực thụ. Người dùng ngoài xem reverse proxy như là nó đang phục vụ các yêu cầu của họ trong khi trên thực tế, nó chỉ thay thế các yêu cầu của họ trước khi đưa tới các máy chủ khác nhau, các máy chủ này thường đặt trên mạng nội bộ. Tương tự như máy chủ thật sự trả lời reverse proxy, reverse proxy cũng trả lời người dùng. Reverse proxy thường là một phần của kế hoạch cân bằng lưu lượng, hay là một phần của kế hoạch bảo mật hoặc đơn giản chỉ là ẩn các máy chủ thực sự từ các người dùng do lý do bảo mật.

Các reverse proxy như mô tả ở hình 2.7, thực hiện như là một lối vào cấu trúc web của một tổ chức.

Hình 2.7. Reverse proxy

Các reverse proxy web thường dùng để tăng độ bảo mật của truy cập Internet trên nền web và cho kế hoạch cân bằng lưu lượng. Tuy nhiên, chúng không thỏa mãn được các yêu cầu của truy nhập từ xa. Chúng không thể đóng gói lưu lượng mạng client/server qua SSL, không thể biến nhiều ứng dụng nội bộ thành các ứng dụng có thể truy cập từ

Internet, không hỗ trợ truy cập an toàn tới các hệ thống file, và không hỗ trợ giao diện người dùng hướng đối tượng. Đó là những gì mà công nghệ SSL VPN có thể đạt được.

2.5 Truy cập từ xa SSL: Công nghệ Reverse proxy plus

Trong khi SSL VPN đã phát triển nhiều chức năng khác, thì ở mức cơ bản, nhiều máy chủ SSL VPN tận dụng công nghệ tương tự như reverse proxy để cho phép người dùng web yêu cầu và truyền các tài nguyên nội bộ. Tất nhiên, SSL VPN đã đưa thêm nhiều chức năng khác so với các chức năng của reverse proxy.

Vậy, những chức năng nào mà SSL VPN cải tiến so với reverse proxy và tại sao nó phải đưa thêm vào?

Có nhiều sự cải tiến, tất cả chúng đều cực kỳ quan trọng đối với truy cập từ xa, bao gồm:

- **Khả năng cho phép các ứng dụng web và ứng dụng non-web tận dụng đường hầm SSL**: Một reverse proxy web đơn giản chỉ cho phép truy cập các ứng dụng trên nền web, nhưng công nghệ SSL VPN cho phép một giải pháp truy cập từ xa toàn diện hơn, các ứng dụng khác cũng có thể sử dụng đường hầm để truy cập từ xa.
- **Khả năng cho phép truy cập từ xa tới file, máy in, và các tài nguyên khác**: Reverse proxy không có các chức năng này.
- **Khả năng chuyển các ứng dụng nội bộ thành có thể truy cập từ Internet**: Một vài ứng dụng nền web đơn giản không hoạt động qua reverse proxy, trong khi SSL VPN cho phép chúng hoạt động.
- **Khả năng cho phép người dùng sử dụng chương trình hướng đối tượng**: Thường các reverse proxy phục vụ yêu cầu dưới dạng không phải là giao diện người dùng.
- **Khả năng kết nối một thiết bị từ xa tới một mạng qua SSL**

Năm cải tiến trên cho phép công nghệ SSL VPN thực hiện chức năng truy cập từ xa hiệu quả hơn, thông qua cách hiểu chúng, chúng ta có thể hiểu được SSL VPN thực hiện như thế nào, do đó chúng ta sẽ tìm hiểu chi tiết từng cải tiến trên trong phần sau.

2.5.1 Lưu lượng non-web qua SSL

Như đã nói ở trên, một trong những cải tiến của SSL VPN so với reverse proxy là khả năng đường hầm hóa lưu lượng non-web qua SSL. Các ứng dụng non-web thường dựa vào phần mềm client và phần mềm này có thể giao tiếp với các máy chủ trên các cổng khác với cổng web. Do đó, phần mềm có thể tự động chọn các cổng và sử dụng các cổng khác nhau cho mỗi phiên làm việc. Các reverse proxy, thông thường hoạt động ở cổng 443 (HTTPS) và 80(HTTP) không thể điều khiển mỗi phiên giao tiếp, mà điều này là cực kỳ cần thiết đối với giải pháp truy cập từ xa.

Vậy làm thế nào để SSL VPN cho phép các phiên giao tiếp xảy ra trên một cổng SSL?

Mặc dù các sản phẩm khác nhau của SSL VPN không sử dụng cùng một phương pháp để đạt được mục đích này nhưng các phương pháp thường dùng là:

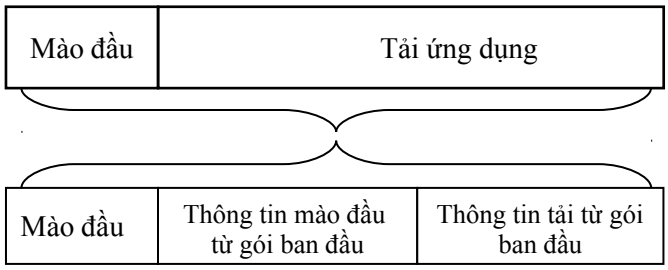
- **Chuyển lưu lượng tới các cổng đặc biệt**: SSL VPN gửi mã tới máy tính người dùng, mã này cho phép nó lắng nghe các yêu cầu tới các địa chỉ và cổng xác định, mà khi yêu cầu được tạo ra, nó sẽ chuyển nội dung các yêu cầu này tới máy chủ SSL VPN qua đường hầm SSL VPN, sau đó máy chủ SSL VPN căn cứ vào địa chỉ, cổng để chuyển tương ứng sẽ gửi lại các yêu cầu này tới địa chỉ cụ thể trong mạng nội bộ.
- **Chuyển dữ liệu qua các cổng động**: Một cách hữu hiệu khác là SSL VPN không đóng gói các giao tiếp ứng dụng. Thay vào đó, nó mở các cổng động trên tường lửa từ địa chỉ IP xác định của client tới địa chỉ chính nó. Cho phép phiên truyền thông có thể hoàn thành mà không cần tải bất kỳ mã nào tới máy trạm. Máy trạm chỉ đơn thuần giao tiếp tới máy chủ qua các cổng động. Mặc dù nó có thể là phương thức đơn giản nhất để thực hiện, nhưng nó sẽ dẫn tới các vấn đề bảo mật và thường không được sử dụng. Nó cũng có thể sử dụng ngoài SSL VPN và có thể làm chúng ta trệch hướng khi nghiên cứu về SSL VPN.
- **Tận dụng các thành phần của hệ điều hành cho phép truyền lưu lượng qua SSL VPN**: Ngày nay, hệ điều hành có thể cung cấp các công cụ có thể tận dụng để truyền lưu lượng. Ví dụ, trong môi trường Windows có NSP (Name Space Provider – Dịch vụ không gian tên) và LSP (Layered Service Provider – Dịch vụ phân lớp) có thể được sử dụng để định nghĩa lại đích cho các phiên truyền thông cụ thể. Sử dụng mỗi phương pháp này để thiết lập đường hầm cần nhiều yêu cầu dựa trên nhà sản xuất SSL VPN hơn là việc thiết lập kết nối mạng qua SSL VPN. Ở thời điểm này, nó cho phép khả năng cung cấp nhiều khả năng điều khiển truyền thông và bảo mật tốt hơn.
- **Tận dụng các dịch vụ đầu cuối**: Các ứng dụng chạy trên các máy chủ trong một mạng nội bộ, chỉ với thông tin bàn phím/chuột/video (Keyboard/Mouse/Video-KVM) chuyển tiếp qua cổng chuẩn SSL giữa người dùng máy tính và mạng nội bộ.
- **Thiết lập một kết nối mạng qua SSL.**

2.5.2 Thiết lập kết nối mạng qua SSL

Một kỹ thuật khác cho phép truy nhập từ xa tới các ứng dụng non-web qua một kết nối SSL là thiết lập một kết nối mạng qua SSL, điều này có nghĩa là, máy từ xa sẽ được gán một địa chỉ IP nội bộ, và xem như nó là một nút trên mạng nội bộ và được sử dụng như kiểu IPSec. Việc thiết lập các kết nối mạng qua SSL thỉnh thoảng được xem như là một chức năng của chính nó (và không chỉ là một phương thức cho phép truy cập tới các ứng dụng non-web).

Để thiết lập một kết nối, SSL VPN gửi một vài đoạn mã (thông thường là một ActiveX control hoặc một Java applet) tới máy tính người dùng và từ đó sẽ tạo một "adapter mạng ảo" trên máy tính người dùng. Sau đó gán địa chỉ mạng IP nội bộ cho máy, và sử dụng đường hầm SSL để thiết lập kết nối mạng giữa mạng nội bộ và nút từ xa. Các adapter mạng ảo có thể chuyển tiếp các giao thức mạng – như TCP, UDP, IP, ICMP,…

Toàn bộ gói tin mạng được mã hóa sử dụng SSL và đặt nó trong tải của một gói mới sử dụng giao thức TCP/IP thông thường như hình 2.8.



Hình 2.8. Gói tin mã hóa SSL

Có hai loại đường hầm mạng cơ bản có thể sử dụng:

- **Đường hầm hoàn chỉnh (full tunneling)**: Tất các các lưu lượng mạng được tạo trên máy tính người dùng (ví dụ TCP/IP, UDP/IP, IMCP,…) đều được gửi tới máy chủ SSL VPN. Máy chủ SSL VPN định tuyến lưu lượng được định trước tới hệ thống nội bộ tới các máy này, và gửi lưu lượng định trước tới Internet qua các cổng khác(các cổng sử dụng cho tất cả các lưu lượng hướng Internet trước từ tổ chức).
- **Đường hầm không hoàn chỉnh (split tunneling):** Máy tính người dùng gửi tất cả các lưu lượng tương ứng với SSL VPN (như lưu lượng tới các hệ thống nội bộ) qua đường hầm, nhưng định tuyến lưu lượng tới Internet qua các gateway bình thường.

Hơn nữa, các đường hầm loại SSL VPN có thể có hoặc có thể không kết nối trực tiếp hai đường:

- Kết nối trực tiếp hai đường: Kết nối mạng được thiết lập qua SSL trên cả hai đường, có nghĩa là từ người dùng tới máy chủ SSL VPN (và mạng của nó) và từ máy chủ SSL VPN (và mạng của nó) tới người dùng. Đây là loại đường hầm SSL VPN giống như kết nối mạng LAN khi họ ở cơ quan. Một người dùng có thể *ping* tới một máy khác trên mạng nội bộ, và một người quản trị mạng trên một mạng nội bộ có thể phân tích ping tới người dùng từ xa.
- Kết nối trực tiếp hai đường không hoàn chỉnh: Đường hầm không hoạt động thực sự như kết nối mạng trực tiếp hai đường, và một vài loại giao tiếp không thể khởi tạo từ bên của máy chủ SSL VPN. Một ví dụ là kết nối có thể cho phép TCP hoạt động hai chiều, nhưng không cho phép ICMP thực hiện từ máy chủ SSL VPN tới máy trạm. Vì vậy người dùng có thể ping một máy chủ trên mạng nội bộ, nhưng không máy tính nào trên mạng nội bộ có thể ping máy tính người dùng từ xa.

Thỉnh thoảng, các sản phẩm SSL VPN có khả năng truy cập nhiều hơn các công nghệ đã nói ở trên, trong trường hợp này, phương thức sử dụng thường được gọi là chế độ hoạt động. Ví dụ, một SSL VPN có thể cho phép truy cập loại ứng dụng cho Web, chuyển tiếp cổng để có nhiều truy cập hiệu quả hơn, và truy cập mức mạng cho người quản trị mạng. Đồ án sẽ mô tả các chế độ này trong phần bảo mật.

2.5.3 Công nghệ truy cập mạng với các ứng dụng Web

Cần phải lưu ý rằng một vài phương thức điều khiển truy cập từ xa tới các ứng dụng non-web kể trên (đường hầm mạng, chuyển tiếp cổng, và dịch vụ đầu cuối) có thể cũng được sử dụng để cung cấp truy cập từ xa tới các ứng dụng web. Tuy nhiên, việc sử dụng các công nghệ này để truy cập tới các ứng dụng nền web sẽ làm mất đi các ưu điểm của SSL VPN. Có thể truy cập web từ bất kỳ máy tính đơn giản nào với một trình duyệt web, trong khi các công nghệ điều khiển non-web cần công nghệ mạnh hơn ở máy trạm (ví dụ như khả năng chạy các applet, hệ điều hành mạnh hơn) và chỉ giới hạn trong một số hệ thống. Hơn nữa, việc thực hiện sử dụng giao tiếp web truyền thống sẽ tốt hơn là khi sử dụng các dịch vụ máy trạm để hiển thị nội dung của một trình duyệt web trên một máy chủ cơ quan. Sẽ là không khôn ngoan khi thiết lập kết nối giữa các máy không an toàn và mạng của bạn, thậm chí là một máy có thể chạy applet để thiết lập đường hầm qua SSL.

2.5.4 Applet

Sự cần thiết phải thiết lập đường hầm lưu lượng non-web qua SSL (và mong muốn thiết lập kết nối mạng qua SSL) đã dẫn tới khái niệm applet. Trong công nghệ SSL VPN, các applet tương ứng là các phần mã được sử dụng bởi SSL VPN để thực hiện nhiều tác vụ khác nhau trên các máy tính sử dụng để truy cập từ xa. Applet có thể điều khiển máy trạm lập đường hầm qua SSL, phân các yêu cầu tới các cổng IP cụ thể và chuyển tiếp tới đường hầm SSL, hoặc giao tiếp với các thành phần hệ điều hành.

Trong công nghệ SSL VPN, chúng ta sẽ thấy rằng các applet thực hiện rất nhiều chức năng, không chỉ là các chức năng trong công nghệ SSL VPN, mà cũng có thể thực hiện nhiều tác vụ bảo mật khác.

2.5.5 Truy cập từ xa tới nguồn tài nguyên file và tài nguyên khác

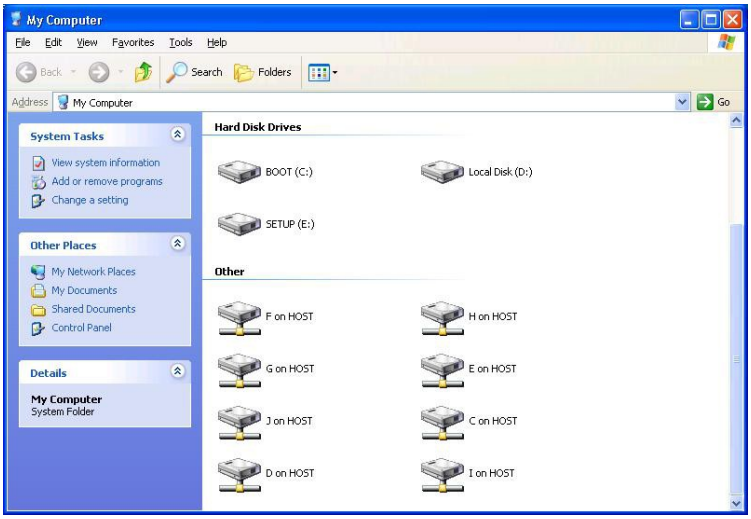
Trong công nghệ SSL VPN, có hai loại truy cập file cần phải quan tâm:

1. Mounting các ổ mạng từ xa
2. Giao diện truy cập file

a) Mounting ổ đĩa mạng từ xa

Mounting ổ đĩa mạng từ xa tương tự như khả năng một SSL VPN cho phép các người dùng từ xa truy cập tới các ổ đĩa mạng (bao gồm thư mục home) như là họ làm việc tại các cơ quan. Việc cho phép mount ổ đĩa từ xa phục vụ một mục đích khác là một vài

các ứng dụng có thể có nhiều liên kết file hoặc thư mục sử dụng chung một tên, và chỉ có thể sử dụng nếu có khả năng mount từ xa. Ví dụ như mounting cho phép người dùng truy cập các ổ đĩa F,G,H,.. từ Windows Explorer từ máy được sử dụng truy nhập SSL VPN như mô tả hình 2.9 (lưu ý biểu tượng ổ đĩa mạng).



Hình 2.9. Ổ đĩa từ xa

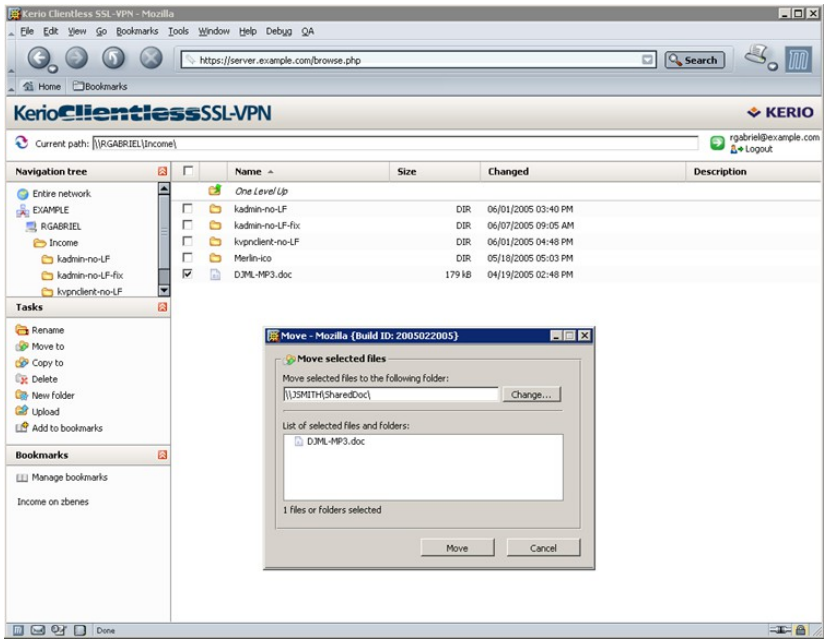
Chức năng này thường được thực hiện bởi một trong các phương thức đồ án đã mô tả ở trên là bằng cách thiết lập kết nối mạng qua SSL, chuyển tiếp lưu lượng SMB qua các cổng thích hợp.

b) Giao diện truy nhập file

SSL VPN thường sử dụng giao diện GUI cho truy cập file từ xa. Thông thường, người dùng có thể tải lên, tải xuống hoặc tìm các file trong một chia sẻ mạng xác định hoặc trên thư mục home của họ. Một giao diện file có thể tương tự như Windows Explorer hoặc khác biệt hoàn toàn so với các tiện ích hệ thống khác. Một ví dụ giao diện truy nhập file như hình 2.10.

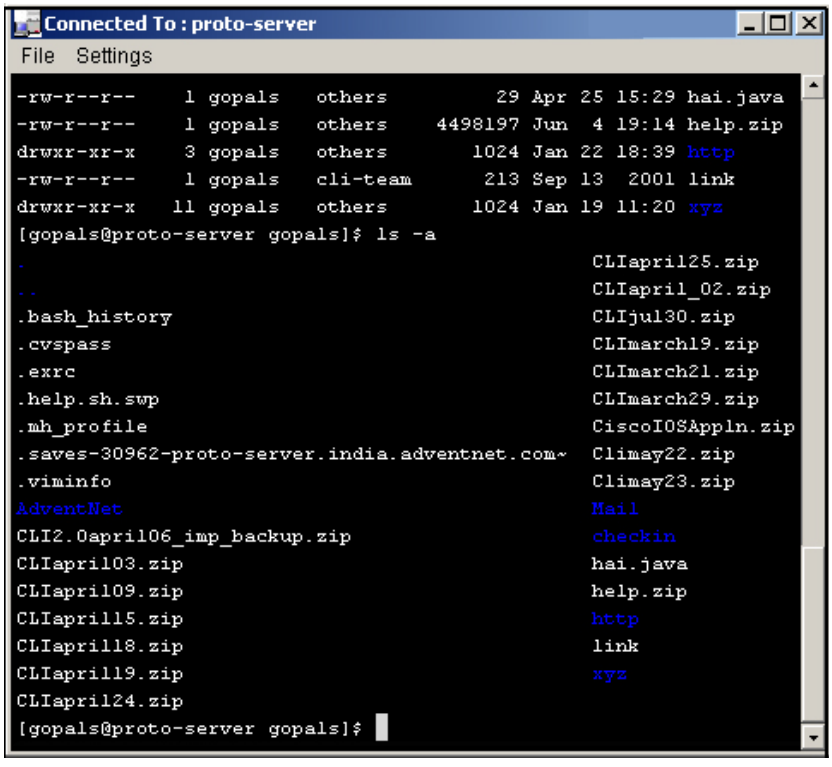
c) Truy cập Telnet và Host

SSL VPN cũng có thể cung cấp khả năng cho phép người dùng Telnet tới các hệ thống nội bộ, có thể thực hiện dựa trên tiện ích Telnet trên thiết bị truy nhập (ví dụ telnet.exe trên MS Windows) hoặc sử dụng một applet đặc biệt có khả năng truy cập SSL. SSL VPN thường cũng hỗ trợ phương pháp truy nhập sử dụng các giao thức Telnet-3270 hoặc Telnet-5250. Mỗi truy nhập cần một phần mềm truy nhập đặc biệt trên thiết bị đầu cuối hoặc có thể tải về các mã cần thiết từ máy chủ SSL VPN. Có thể truy nhập bằng cách thiết lập một kết nối mạng qua SSL và chuyển tiếp lưu lượng như là người dùng ở trong mạng nội bộ, hoặc chặn các yêu cầu cổng và chuyển tiếp như đã mô tả ở các chương trên.



Hình 2.10. Truy cập file

Hình 2.11 mô tả một phiên truy nhập telnet qua SSL VPN:



Hình 2.11. Telnet

d) Các tài nguyên máy in và tài nguyên mạng khác

Công nghệ SSL VPN có thể cho phép người dùng in trên các máy in ở cơ quan từ cách xa hàng ngàn cây số hoặc có thể gửi các bản fax qua các máy chủ fax của công ty.

Tương tự như trường hợp truy nhập file, SSL VPN tận dụng các công nghệ trên để có thể thực hiện điều đó.

e) Các dịch vụ đầu cuối

Một lĩnh vực được chú ý là các dịch vụ đầu cuối. Truy nhập từ xa tới các dịch vụ đầu cuối thường được cung cấp bởi hầu hết các SSL VPN và nó cũng được thực hiện như các ứng dụng non-web khác. Tuy nhiên, chú ý rằng một vài dịch vụ đầu cuối thường được coi như là các giải pháp truy nhập từ xa của chính nó. Nếu có một hệ thống khẩn cấp của một công ty được thực hiện qua các dịch vụ đầu cuối, thì người dùng có khả năng sử dụng từ xa nếu các dịch vụ đầu cuối được mở qua Internet.

Tất nhiên, nếu các dịch vụ đầu cuối có thể truy nhập được từ Internet, thì cần phải chắc chắn rằng chúng là an toàn. Điều này phụ thuộc vào việc thực hiện SSL VPN, các tường lửa ứng dụng, hoặc các công nghệ bảo mật khác để điều khiển truy nhập từ xa trong cơ cấu dịch vụ đầu cuối. Các dịch vụ đầu cuối không hiệu quả khi cung cấp truy nhập từ xa tới các ứng dụng web, mặc dù có thể được thực hiện được khi sử dụng một SSL VPN như là một cổng truy nhập từ xa và phục vụ các yêu cầu ứng dụng web, với các dịch vụ đầu cuối để điều khiển lưu lượng non-web.

Các dịch vụ đầu cuối (và các công nghệ liên quan) cũng có thể cho phép các người dùng truy nhập máy tính của họ (ở cơ quan) từ bất kỳ nơi đâu – đây là một nguyên nhân khác để đưa các loại dịch vụ đầu cuối vào loại truy cập từ xa.

2.5.6 Các ứng dụng nội bộ cho phép truy nhập qua Internet

Một trong những cải tiến chính so với công nghệ reverse proxy được giới thiệu bởi SSL VPN là khả năng chuyển đổi các ứng dụng nội bộ vào trong các hệ thống để chúng có thể được truy nhập qua internet. Đồ án đã giải thích làm thế nào các ứng dụng non-web có thể được mở rộng việc sử dụng qua mạng Internet. Bây giờ chúng ta sẽ xem xét đến các ứng dụng nền web.

Các ứng dụng nền web

Các ứng dụng cho phép một giao diện web và thường được truy nhập bằng một trình duyệt. Thoạt nhìn, việc cung cấp truy cập từ xa tới các ứng dụng trên nền SSL là một việc tương đối đơn giản – chỉ cần chuyển tất cả các lưu lượng HTTP thành lưu lượng HTTPS đã mã hóa SSL, nhưng đây không phải là trường hợp như vậy. Các ứng dụng web thiết kế cho sử dụng trên một mạng nội bộ nên thường bao gồm các phần mà thường hay tạo ra các vấn đề nghiêm trọng khi thiết kế một truy cập từ xa. Sau đây là một vài ví dụ:

- **Dải địa chỉ IP nội bộ**: Có nhiều dải địa chỉ cho IP nội bộ, và các địa chỉ này không thể định tuyến qua Internet (được định nghĩa trong RFC 1918). Các địa chỉ trong dải này, thường sử dụng NAT (Network Address Translation – Giao thức phân giải địa

chỉ) để chuyển đổi các địa chỉ có thể truy cập được bên ngoài tới địa chỉ sử dụng trong LAN. Mặc dù NAT là một công nghệ hữu dụng, việc sử dụng các địa chỉ mạng nội bộ có thể dẫn tới vấn đề khi một người muốn được cung cấp dịch vụ truy cập từ xa nền SSL. Bất kỳ máy chủ nào sử dụng địa chỉ IP nội bộ với các ứng dụng web sẽ không thể hoạt động từ xa. Các máy chủ NAT chỉ chuyển đổi địa chỉ trong các phần mào đầu của gói. Chúng không phân tích và dịch địa chỉ trong mã HTML hoặc XML của trang web. Vì vậy, một liên kết tới *http://192.168.1.2/page45.asp* sẽ được chuyển đổi bởi SSL VPN (với phương thức mã hóa SSL) thành *https://192.168.1.2/page45.asp* . Nhưng khi một liên kết được nhấp chuột từ xa, 192.168.1.2 sẽ không thể xác định được và người dùng sẽ nhận được một thông báo lỗi.

Các vùng địa chỉ không thể định tuyến trên Internet bao gồm:

1. Lớp A – từ 10.0.0.0 đến 10.255.255.255
2. Lớp B – từ 172.16.0.0 đến 173.31.255.255
3. Lớp C – từ 192.168.0.0 đến 192.168.255.255

- **Sử dụng các tên máy không đạt chuẩn**: Các máy tính được đặt trong một mạng nội bộ, tên của nó có thể truy cập cục bộ được, nhưng sẽ không truy cập được nó qua Internet nếu tên của nó không đạt chuẩn. Ví dụ, liên kết như *http://human-resource-server* có thể hoạt động khi người dùng ở máy tính cơ quan, nhưng không thể hoạt động qua Internet. Bất kỳ các ứng dụng nội bộ hoặc các bản tin e-mail nội bộ sẽ không hoạt động khi người dùng thử kết nối chúng từ xa.
- **Sử dụng tên máy chuẩn nhưng không phải là địa chỉ DNS công cộng hoặc có thể truy cập theo cách khác từ Internet**: Cùng với các tên máy không chuẩn, đây cũng là một trường hợp khác có thể khiến các ứng dụng không hoạt động. Ví dụ, *server5.josephesternberg.com* có thể là một tên máy chủ hoạt động trên mạng LAN của người dùng và tương ứng với đó là các chức năng trong một ứng dụng sẽ hoạt động tốt khi người dùng sử dụng chương trình qua một kết nối LAN wifi từ phòng khách. Nhưng bởi vì tên miền này không có trong bất kỳ máy chủ DNS nào ngoài mạng LAN của anh ta nên các truy cập từ xa tới địa chỉ này sẽ không thực hiện được.
- **Các liên kết được thực hiện dựa trên JavaScript, Java applets, ActiveX, Macromedia Flash**: Bởi vì chúng được thực hiện dựa trên các mã này, một vài liên kết không thể xuất hiện khi xem nguồn trang web của các ứng dụng và máy chủ SSL VPN. Do đó, nếu nó không được chuyển đổi thì một số thành phần của ứng dụng sẽ không hoạt động được.

Vậy thì làm thế nào để SSL VPN cho phép truy cập từ xa khi các ứng dụng có thành phần không hoạt động qua Internet?

Câu trả lời là nó sẽ chuyển đổi các thành phần nội bộ thành dạng có thể truy cập từ bên ngoài được. Các sản phẩm SSL VPN khác nhau thực hiện điều này khác nhau, dưới đây là một số phương thức thực hiện:

- **Truyền thông tin về thành phần nội bộ như là một tham số**: Khi thực hiện truyền, các liên kết trong thành phần nội bộ sẽ được chuyển sang định dạng URL sau: *https://SSL-VPN-NAME/somepage.html?RealLocation=InternalInformation*. Do lý do bảo mật, thông tin nội bộ sẽ được mã hóa trong nguồn của trang web được truy nhập.Vídụ:
  https://SSL-VPN-NAME/somepage.html?RealLocation=SomeEncrytedString
- **Thay đổi URL để thêm thông tin**: Thay vì truyền các thông tin như là một tham số, thông tin sẽ được thêm vào URL như là một thư mục thông tin. Ví dụ: *https://SSL-VPN-NAME/InternalInformation/somepage.html*. Tương tự như trên, nó có thể được mã hóa và trở thành
  https://SSL-VPN-NAME/EncryptedString/somepage.html
- **Thực hiện đường hầm như là ứng dụng non-web**: Một trong những nhược điểm của thực hiện chuyển đổi là các bộ máy chuyển đổi không phải là hoàn hảo. Một vài thành phần cần được chuyển đổi lại không được chuyển đổi hoặc không chuyển đổi chính xác. Ví dụ, các website có thể sử dụng các đoạn mã flash trong liên kết, nhưng nhiều SSL VPN không hiểu được các thành phần được xây dựng bên trong các đoạn mã này, và kết quả là nó không thể chuyển đổi được liên kết. Các applet Java có thể xây dựng theo nhiều cách khác nhau và do đó SSL VPN có thể sai sót một số thành phần khi thực hiện chuyển đổi.
  Một kỹ thuật đơn giản SSL VPN sử dụng để tránh vấn đề không chuyển đổi được là không chuyển đổi tất cả cùng một lúc, thay vào đó tận dụng kết nối mạng qua SSL cho các ứng dụng web. Máy tính người dùng từ xa trở thành một nút trong mạng nội bộ và có thể truy nhập bất kỳ ứng dụng nào – web hoặc non-web. Như đã trình bày ở trước, phương pháp này có thể mô phỏng hiệu quả kết nối IPSec, nhưng sử dụng đường hầm SSL thay vì IPSec. Ưu điểm của phương pháp này là chắc chắn các ứng dụng sẽ được truy cập từ xa mà không phải quan tâm đến sai sót trong việc chuyển đổi. Ở cùng một thời điểm, đường hầm giới hạn số máy tính mà nó có thể hỗ trợ truy cập an toàn. Điều này sẽ đưa ra một khái niệm bảo mật mới mà sẽ được giới thiệu ở chương sau.
- **Điều khiển các ứng dụng web phức tạp**: Như đã trình bày ở trước, loại truy cập dịch vụ đầu cuối có thể được sử dụng để điều khiển các ứng dụng web phức tạp nhưng cần giảm số các thiết bị có thể truy cập và do đó cũng làm giảm hiệu năng của nó.

Các SSL VPN thường chuyển đổi và tận dụng đường hầm lớp thấp để sử dụng cho các ứng dụng khi đường hầm không hoạt động.

Ngày nay, hầu hết các ứng dụng nền web đều không chỉ sử dụng HTML trên giao diện của nó mà sử dụng nhiều thành phần khác nữa, thường là Java hoặc ActiveX. Các công nghệ này mở rộng chức năng của trình duyệt web cả về phương diện giao diện và truyền thông. Mặc dù một vài applet Java và ActiveX không là vấn đề đối với SSL VPN

nhưng một vài applet khác thì khác. Thường các công nghệ này là nguyên nhân chính để sử dụng đường hầm lớp thấp hơn để truyền thông tin trang web.

2.5.7 Giao diện truy nhập từ xa

Cải tiến quan trọng thứ ba của SSL VPN so với reverse proxy là khả năng sử dụng dễ dàng đối với người sử dụng qua giao diện GUI. Một vài thành phần của giao diện người sử dụng sẽ được mô tả dưới đây:

a) Đăng nhập

Do là một lối vào cho doanh nhân vào doanh nghiệp, SSL VPN cần phải nhận thực trước khi cho phép truy nhập. Do đó, chúng không cho phép người dùng thiết lập các phiên và gửi các yêu cầu tới máy chủ nội bộ trừ khi người dùng được nhận thực.

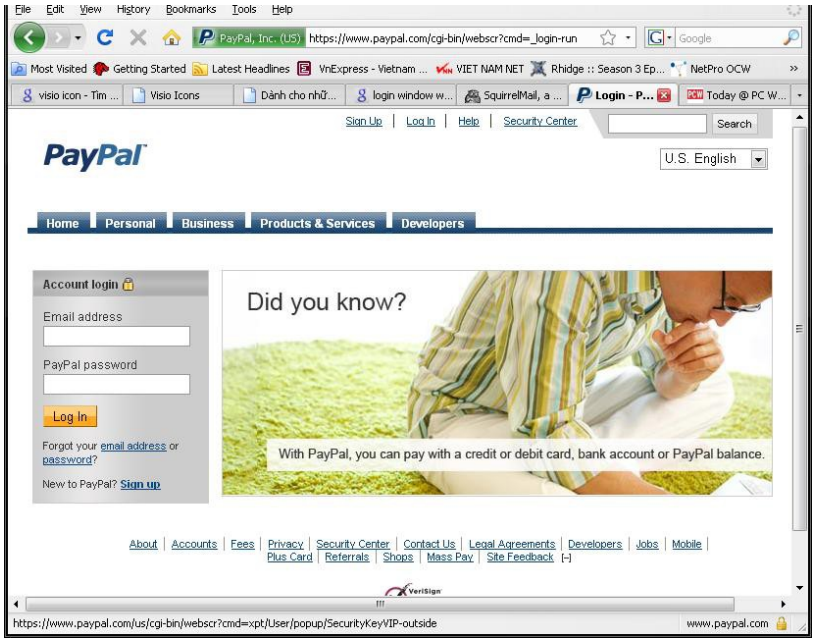
Mặc dù tên đăng nhập và mật khẩu là mẫu nhận thực thông thường nhất, SSL VPN thường hỗ trợ các phương pháp nhận thực khác cũng rất tốt. Phương thức của các tổ chức thứ ba đưa ra là giao diện RADIUS hoặc LDAP, giao diện này thường được sử dụng khi thực hiện SSL VPN. Các phương thức nhận thực khác bao gồm các hệ thống mật khẩu, các thẻ, các card thông minh, các thiết bị nhận thực USB, các chứng thực máy trạm, chứng thực sinh học, và nhận thực dựa trên PKI (Public Key Infrastructure – cấu trúc khóa công cộng). Các công nghệ nhận thực này thường tốt hơn là sử dụng tên đăng nhập và mật khẩu truyền thống. Tuy nhiên, cần lưu ý rằng các thiết bị nhận thực đặc biệt (như thẻ bài USB, bộ đọc vân tay) cần các thiết bị cụ thể, do đó người dùng sẽ không thể truy nhập từ xa trên các máy tính công cộng hoặc trên máy tính mượn.

Ngoài phương thức nhận thực, một điều quan trọng nữa là cho phép người dùng chỉ nhận thực một lần, hơn là bắt họ phải nhập vào các chứng thực mỗi lần truy nhập hệ thống nội bộ. Nhiều sản phẩm SSL VPN khác nhau sử dụng các phương thức khác nhau để thực hiện SSO (Single Sign On – Đăng nhập một lần), nhưng thường là một trong ba phương thức sau:

- Dựa trên khởi tạo đăng nhập người dùng, mật khẩu sẽ được gom lại từ người dùng cho mỗi lần đăng nhập hệ thống. Các chứng thực được lưu trữ trong một cơ sở dữ liệu trên thiết bị SSL VPN, và các đăng nhập sau tới SSL VPN, thì thiết bị SSL VPN có thể tự động cho phép người dùng vào hệ thống tương ứng với mật khẩu đã lưu trữ. Phương thức này có ưu điểm là cho phép thực hiện SSO đơn giản khi thiết lập, nhưng cũng có nhược điểm là cần phải bảo vệ cơ sở dữ liệu các chứng thực và vấn đề đồng bộ các cơ sở dữ liệu chứa thông tin nhận thực (ví dụ như cần phải giữ cho hai cơ sở dữ liệu này đồng bộ với nhau, để cho phép xóa người dùng trên nhiều cơ sở dữ liệu khi họ rời khỏi công ty).
- SSL VPN được tích hợp với cơ sở dữ liệu nhận thực và xác thực của tổ chức thứ ba. Chứng thực để truy nhập các hệ thống nội bộ được lưu giữ và bảo trì trong các

hệ thống tổ chức thứ ba, chứng thực này được lưu trữ ở đây trong suốt quá trình khởi tạo phiên SSL VPN của người dùng như đã mô tả ở trên, hoặc được nhập vào trong một cơ sở dữ liệu trước khi sử dụng SSL VPN. Dựa trên các truy cập các ứng dụng, SSL VPN rút các chứng thực từ cơ sở dữ liệu bên ngoài và tự động đăng nhập người dùng.

- SSL VPN không bảo trì bất kỳ thông tin chứng thực nào, nhưng nó gom lại tất cả các thông tin cần thiết trên trang đăng nhập khi người dùng đăng nhập. Phương thức quản lý này đơn giản hóa việc quản lý chứng thực và tránh được các vấn đề bảo mật, nhưng cần người dùng nhập nhiều mật khẩu mỗi lần họ xác thực.



Hình 2.12. Màn hình đăng nhập

Nhiều khi người ta sử dụng kết hợp các kỹ thuật trên. Ví dụ, một SSL VPN có thể lưu trữ và trích các mật khẩu cho hệ thống nội bộ từ một cơ sở dữ liệu, nhưng yêu cầu người dùng nhập thông tin nhận thực cho các hệ thống nhạy cảm hơn mỗi lần đăng nhập. Tương tự, một SSL VPN có thể thực hiện SSO cho hầu hết các hệ thống, nhưng yêu cầu đăng nhập (sau khi một người dùng đã đăng nhập vào SSL VPN) nếu người dùng đăng nhập vào một hệ thống nhạy cảm đặc biệt.

SSL VPN thường cho phép các trang web đăng nhập được tùy chỉnh, vì vậy chúng có thể xuất hiện trong các trang web khác của công ty. Các thành phần như logo công ty, cảnh báo truy nhập không nhận thực thường có trong một trang đăng nhập tổ hợp. Tất nhiên, nếu SSO cần gom các chứng thực trên trang đăng nhập thì trang web sẽ được tùy biến cho phù hợp.

b) Các trang chủ

Sau khi đăng nhập thành công vào một SSL VPN thì người dùng thường được dẫn tới một trang gọi là trang chủ hay trang portal hay trang menu, ở đây, họ có thể chọn các ứng dụng họ có thể truy nhập.

Các trang chủ và các thành phần của nó tùy thuộc vào sản phẩm SSL VPN. Nhưng thường có các thành phần sau đây:

- **Tên và logo công ty**: Thường được xác định khi cấu hình SSL VPN.
- **Menu ứng dụng**: Danh sách các ứng dụng mà từ đó người dùng có thể chọn ứng dụng họ muốn truy cập.
- **Bookmarks**: Các bookmark cá nhân cho mỗi người dùng, thường để truy cập vào các ứng dụng, file, thư mục và các tài nguyên khác. Người quản trị hệ thống có thể thiết lập các bookmark cho từng người dùng hoặc từng nhóm. Đôi khi người dùng cũng có thể tự thiết lập các bookmark của họ.
- **Giúp đỡ**: Các liên kết sau có thể là những tiện ích hữu dụng:
    - Liên kết tải các tiện ích hữu dụng. Ví dụ như môt liên kết để tải một chương trình xem văn bản Microsoft Word mà không cần phải cài đặt Office từ một máy khi họ sử dụng SSL VPN.
    - Một liên kết tới lịch ngày tháng cơ bản.
    - Liên kết tới chương trình tính toán.
- **Tin tức**: Tin tức hoặc các thông báo của công ty.
- **Truy nhập file**: Truy nhập tới một giao diện thân thiện người dùng từ đó có thể truy cập các file, hoặc có thể cung cấp khả năng mounting ổ đĩa mạng hoặc thư mục home, hoặc cả hai.
- **Không gian URL nội bộ**: Là một không gian trong có người dùng có thể nhập URL mà các URL này chỉ được sử dụng trong mạng nội bộ (ví dụ như chúng có trong danh sách DNS công cộng) và truy cập được nếu người dùng ở cơ quan của họ bằng cách sử dụng LAN.
- **Đồng hồ hoặc Timer**: Hiển thị thời gian của phiên SSL, là thời gian cho tới khi tiến hành nhận thực tiếp theo, hoặc thời gian tính từ hoạt động cuối của người dùng, hoặc thời gian còn lại cho tới khi tự ngắt kết nối (trong trường hợp người dùng không thực hiện bất kỳ tác vụ nào).
- **Toolbar:** Là một thanh các biểu tượng để dễ dàng truy cập vào nhiều chức năng SSL VPN khác nhau.
- **Giúp đỡ**: Truy cập tới sự giúp đỡ trực tuyến.

Tất nhiên, các trang chủ thường được tùy chỉnh cho phù hợp với từng sản phẩm SSL. Một vài chức năng chỉ có đối với người dùng độc lập, một vài chức năng thường chỉ có đối với người quản trị. Một vài sản phẩm SSL VPN cho phép những người quản trị không chỉ tùy biến trang chủ mà còn có thể mở rộng chức năng của chúng.

Khả năng tùy chỉnh: Hai thành phần mà SSL VPN thường cho phép tùy chỉnh là trang chủ và danh sách bookmark. Các mẫu và nội dung trang chủ thường được cấu hình

bởi người quản trị, các cấu hình có thể dựa trên người dùng, nhóm người dùng hoặc từng tổ chức của công ty. Điều này cho phép cung cấp linh hoạt các chức năng tương ứng với từng người dùng. Ví dụ, một kỹ sư đang làm việc trên văn phòng MIS có thể sử dụng Telnet và hệ thống điều khiển vé (Trouble-Ticket Tracking System), trong khi người sử dụng ở trên văn phòng tài chính thì có thể sử dụng Danh sách tài khoản có thể nhận (Accounts Receiveable) và Danh sách các tài khoản có thể chi trả (Accounts Payable). Các bookmark thường khác nhau đối với người dùng khác nhau.

Một vài tổ chức có các trang chủ riêng, và nếu máy chủ SSL VPN có đủ khả năng thực hiện, họ có thể tận dụng trang chủ chuẩn của họ thay vì trang chủ của nhà sản xuất thiết bị SSL VPN.

c) Các thanh công cụ (Toolbar)

Các toolbar thường xuất hiện ở bên trên hoặc bên trái màn hình SSL VPN trình duyệt, cung cấp cho người dùng dễ dàng chuyển đổi giữa các ứng dụng. Các toolbar cũng có thể có các thành phần truy nhập giúp đỡ trực tuyến, các ứng dụng giúp đỡ người dùng hoặc các thành phần đã mô tả ở trên trong phần trang chủ. Các toolbar cũng có thể được tùy biến bởi người dùng hoặc nhà quản trị.

d) Các ngôn ngữ

Có nhiều loại hỗ trợ ngôn ngữ:

- **Hỗ trợ các ứng dụng sử dụng các ký tự non-latin**: Nhiều tập đoàn đa quốc gia hoặc có nhiều chi nhánh thường có các ứng dụng hoặc dữ liệu mà không sử dụng ký tự latin, và các ký tự này cần phải được hỗ trợ bởi SSL VPN.
- **Giao diện người dùng đa ngôn ngữ**: Để thực hiện, người dùng thường muốn sử dụng thiết bị có hỗ trợ ngôn ngữ địa phương. Các tùy chọn ngôn ngữ có thể thực hiện tự động dựa vào chức năng ngôn ngữ của trình duyệt, hoặc có thể được thiết lập bởi người dùng, hoặc người quản trị. Các trang chủ, bản tin lỗi, toolbar,… đều có thể tùy biến ngôn ngữ cho phù hợp.
- **Tính tương thích với phiên bản ngôn ngữ khác**: Khả năng tải bất kỳ mã nào có thể tải về của SSL VPN (ví dụ applet) để chạy trên các phiên bản ngôn ngữ khác của hệ điều hành, cũng là khả năng của các công cụ quản trị để chạy trên các hệ điều hành.
- **Giao diện tiện ích quản trị đa ngôn ngữ**: Là khả năng cho phép các công cụ quản trị có các ngôn ngữ khác ngoài tiếng Anh.

e) So sánh nhiều cửa sổ và một cửa sổ

Một vài SSL VPN cho phép nhiều ứng dụng được mở trong một cửa sổ và cho phép người dùng sử dụng toolbar để chuyển đổi giữa chúng. Một phương pháp khác là mỗi cửa sổ độc lập cho mỗi chương trình. Mỗi phương pháp có các ưu điểm và nhược

điểm của chúng, nên sự lựa chọn chủ yếu phụ thuộc vào người dùng. Nhưng ngày nay, nhà sản xuất thiết bị hoặc người quản trị hệ thống SSL VPN thường lựa chọn phương pháp nào sẽ được chọn.

f) Nút logout

Một nút đăng xuất cho phép người dùng thoát ra ngoài SSL VPN bằng nhấp chuột. Sau khi người dùng thoát ra ngoài, phiên SSL sẽ bị hủy và truy nhập tới tất cả các ứng dụng sẽ bị hủy cho tới khi người dùng đăng nhập trở lại.

g) Giúp đỡ

Chức năng giúp đỡ trực tuyến có thể được truy cập từ công cụ SSL VPN, từ trang chủ, hoặc cả hai. Nó giúp đỡ trả lời các câu hỏi người dùng thường hỏi khi sử dụng SSL VPN, và cung cấp thông tin liên lạc tới dịch vụ giúp đỡ SSL VPN tại chỗ và dịch vụ giúp đỡ người dùng truy cập từ xa.

h) Giao diện người dùng dựa trên loại trình duyệt

Với sự phát triển nhanh chóng của các thiết bị PDA (Personal Data Assistants – thiết bị trợ giúp cá nhân) và các thiết bị cầm tay khác, khả năng truy cập các hệ thống và thông tin quan trọng từ bất kỳ đâu đã phát triển mạnh mẽ. Với sự phát triển của máy tính cầm tay và năng lực xử lý cho phép công nghệ SSL VPN cung cấp khả năng truy nhập từ các thiết bị có kích cỡ trong tầm tay. Do đó, ngày nay SSL VPN có thể hỗ trợ các thiết bị chạy trên hệ điều hành WindowsCE/PocketPC, PalmOS và Symbian OS.

Một chức năng quan trọng của SSL VPN là khả năng tùy chỉnh giao diện GUI dựa trên loại thiết bị sử dụng để truy cập. Điều này là do trình duyệt web trên thiết bị cầm tay không thể trình bày như một trình duyệt cỡ lớn thông thường được, bởi vậy khả năng tùy chỉnh là cần thiết. Hơn nữa, băng thông di động không thể đáp ứng nhanh như cố định đối với các bức ảnh lớn hoặc các loại dữ liệu đa phương tiện khác, thường thì SSL VPN giảm số lượng các bức ảnh và âm thanh để tối ưu hoạt động web trên thiết bị cầm tay.

SSL VPN hiện tại không thể cho phép mức độ truy cập của các thiết bị cầm tay như là các máy tính truyền thống. Mặc dù hầu hết SSL VPN đều hỗ trợ truy nhập tới các ứng dụng nền web từ các thiết bị nhỏ, nhưng do hạn chế về thiết bị, SSL VPN không thể hỗ trợ kết nối lớp mạng hoặc hỗ trợ kết nối tới các ứng dụng non-web. Khả năng mounting các ổ đĩa từ xa thường thì không thể thực hiện được mặc dù giao diện truy cập file vẫn thực hiện được. Một vài nhược điểm đã kể trên là do khả năng của các thiết bị cầm tay không thể chạy được hoàn toàn các ActiveX hoặc Java để thực hiện truy cập từ xa hoàn toàn. Tuy nhiên, với nhiều ứng dụng chính đều dựa trên nền giao diện web, khả năng truy cập tới các ứng dụng nền web từ thiết bị cầm tay rất hữu dụng đối với một tổ chức, công ty. Và với các thiết bị cầm tay thế hệ mới, các nhược điểm trên sẽ không còn tồn tại trong SSL VPN.

i) Cửa sổ trạng thái SSL VPN

Như là một phần của phần mềm mà SSL VPN sử dụng để điều khiển đường hầm cho phiên giao tiếp non-web qua SSL, cửa sổ trạng thái có thể được nhìn thấy trên máy trạm. Cửa sổ này có thể xác định địa chỉ IP nội bộ được gán cho máy tính người dùng (nếu kết nối mạng được thiết lập qua SSL), địa chỉ IP bên ngoài của máy tính, cổng nào được sử dụng và nội dung dữ liệu truyền tới mạng nội bộ, dung lượng dữ liệu đã truyền và một số thông tin cần thiết về máy người dùng và phiên SSL VPN.

Thông thường người dùng không cần phải để ý các thông tin này, thông tin này sẽ hỗ trợ cho người quản trị mạng khi phiên giao tiếp khó thực hiện hoặc có sai sót và họ muốn sửa chữa.

j) Giao diện WebMail

Một vài SSL VPN được trang bị giao diện e-mail nền web đơn giản (webmail) cho phép người dùng sử dụng để đọc và gửi e-mail mà không cần phải sử dụng các client e-mail lớn hoặc các hệ thống Webmail chuẩn như Microsoft Outlook Web Access hoặc Lotus iNotes. Giao diện Webmail hỗ trợ bởi SSL VPN thường thô sơ và có thể sử dụng được trên rất nhiều thiết bị. Điều này cho phép SSL VPN thực hiện truy cập web trên các thiết bị cầm tay và các trình duyệt cấp thấp khác, trên các thiết bị không thể cài đặt một ứng dụng e-mail tiêu chuẩn.Ở thời điểm được giới thiệu, SSL VPN Webmail rất được hoan nghênh.

2.5.8 Các công cụ quản trị

Tất cả sản phẩm SSL VPN có các công cụ quản trị của chính nó, một số công cụ dựa trên nền web và một số sử dụng các client và một số cho phép nhiều cấp độ tích hợp với mạng chung và các hệ thống quản trị máy tính qua giao thức SNMP (Simple Network Management Protocol – Giao thức quản lý mạng đơn giản). Một vài công cụ cũng tích hợp với SYSLOG để dễ dàng kiểm tra các hoạt động.

Như đã mô tả từ trước, SSL VPN thường là các máy tính chạy phần mềm. Do đó, một vài cấp độ quản lý phần mềm cho thiết bị là cần thiết, do đó người quản trị phải biết rõ hoạt động của hệ điều hành như Linux hoặc Windows, và cần phải thực hiện update một số miếng vá để chắc chắn SSL VPN đảm bảo được an toàn.

2.5.9 Hoạt động

Để cải thiện hoạt động, SSL VPN tận dụng các công nghệ sau:

- Tăng tốc SSL
- Nén lưu lượng HTTP
- Sử dụng bộ đệm
- Cân bằng tải

a) Tăng tốc SSL

Việc chạy các thuật toán phức tạp (bao gồm các thuật toán bất đối xứng) trên một máy tính sẽ ngốn nhiều thời gian xử lý của CPU. Do đó, quá trình xử lý SSL làm giảm hoạt động hệ thống. Một máy chủ SSL VPN có thể dùng các tài nguyên trên mào đầu SSL của nó thậm chí trước khi phục vụ cho bất kỳ truy cập nào. Quá trình xử lý SSL có thể làm giảm số yêu cầu người dùng (bao gồm một SSL VPN) có thể xử lý đồng thời.

Các bộ tăng tốc SSL giải phóng CPU khỏi quá trình xử lý SSL, giải phóng bộ xử lý để điều khiển được nhiều yêu cầu người dùng. Các bộ tăng tốc SSL thực hiện như là các card có thể thêm vào một máy chủ hoặc như là các thiết bị ngoại vi được đặt trên cùng một mạng như các máy chủ, ở đó, chúng điều khiển quá trình quá trình xử lý SSL. Một vài sản phẩm SSL VPN xem bộ tăng tốc SSL như là chức năng chuẩn của nó, một vài sản phẩm thì xem nó như là thành phần tùy chọn bổ sung, và một số khác hỗ trợ các thiết bị tăng tốc ngoại vi. Dù là thế nào thì bộ tăng tốc SSL cải thiện đáng kể hoạt động của một SSL VPN.

b) Nén lưu lượng HTTP

Các mã (HTML, XML, JavaScript, ASP,…) sử dụng trong các trang web thường có giao diện người dùng của chính nó tương tự như các ứng dụng web, hơn nữa nó sử dụng dữ liệu định dạng mã ASCII, định dạng này có thể được nén với tỉ lệ cao sử dụng các chuẩn nén. Bởi vì có nhiều người dùng có thể truy nhập SSL VPN qua các kết nối Internet chậm, việc nén lưu lượng HTTP cải thiện rất nhiều phương thức truy nhập từ xa qua SSL VPN.

Nhiều năm trước đây, các trang web và máy chủ cho phép mỗi phương pháp nén như là một phần của mã hóa và chức năng mã hóa được cung cấp trong chuẩn HTTP 1.1. Trong quá trình khởi tạo một phiên web, máy trạm sẽ trao đổi với máy chủ để thống nhất phương pháp nén sử dụng (thường là gzip). Nếu máy chủ web cũng hỗ trợ phương pháp nén, máy chủ sẽ bắt đầu gửi lưu lượng web tới trình duyệt. Khi máy chủ nhận được các dữ liệu này, nó giải nén và trình bày dữ liệu như thường. Quá trình xử lý tải trên máy chủ để nén dữ liệu và quá trình giải nén trên trình duyệt thường nhỏ hơn nhiều so với thời gian truyền dữ liệu khi không nén, và do đó, phương pháp nén lưu lượng HTTP cải thiện được đáng kể hoạt động SSL VPN.

c) Sử dụng bộ đệm

Các máy chủ SSL VPN có thể lưu giữ đệm các trang web hoặc trang thành phần thường được yêu cầu trong suốt phiên làm việc của một người dùng. Bằng cách đó, chúng có thể giảm số các giao tiếp nội bộ cần thiết để trả lời yêu cầu người dùng và do đó tăng hiệu quả hệ thống.

d) Cân bằng tải: IP Spraying

Một phương thức khác được sử dụng để tăng tốc hoạt động của SSL VPN là tận dụng nhiều thiết bị SSL VPN cùng hoạt động. Kỹ thuật chia nhỏ tải truy nhập đến nhiều hệ thống khác nhau gọi là cân bằng cải (load balancing) và khi được sử dụng, nó không chỉ cải thiện hoạt động mà còn đảm bảo khi đứt kết nối trên một máy chủ SSL VPN sẽ không làm ảnh hưởng đến toàn bộ các truy cập từ xa.

Trong một kiểu cân bằng tải thường được sử dụng, tất cả các thiết bị SSL VPN như là một máy chủ đơn lẻ với một tên và một địa chỉ IP đối với người dùng. Khi người dùng gửi yêu cầu tới SSL VPN này, bộ chia tải (phần mềm hoặc phần cứng) sẽ chia các yêu cầu HTTP dựa trên các SSL VPN thực. Mô hình chia tải này gọi là IP Spraying.

Hầu hết các SSL VPN xem cân bằng tải là một tùy chọn của thiết bị. Một vài thiết bị xem nó là một thành phần bên trong thiết bị vì thế các thiết bị SSL VPN có thể tự điều khiển cân bằng tải và định tuyến các yêu cầu sao cho thích hợp như hình 2.13.

Hình 2.13. Cân bằng tải ở bên trong

Thậm chí các sản phẩm đã có khả năng cân bằng tải vẫn có thể sử dụng thêm thiết bị cân bằng tải của hãng khác, thiết bị này được đặt trước các thiết bị SSL VPN như mô tả 2.14.

Hình 2.14. Cân bằng tải ở bên ngoài

e) Việc truy cập từ các trình duyệt cũ

Như chúng ta đã mô tả ở trên, cần phải có một phương pháp truy cập dành cho các thiết bị cầm tay và các thiết bị cũ.

Sự tăng nhanh của số lượng các trình duyệt web trong những năm cuối của thập kỷ 90 dẫn tới một vấn đề chung là có quá nhiều các trình duyệt cũ được sử dụng trên thế giới. Một vài các trình duyệt này không hỗ trợ hoặc hỗ trợ không hoàn chỉnh các yêu cầu kỹ thuật cho SSL VPN, và việc truy cập từ xa có thể bị hạn chế hoặc không thể thực hiện được. Bên cạnh vấn đề chạy các ActiveX và Java như đã mô tả, các trình duyệt cũ cũng có thể không hỗ trợ một vài thành phần GUI, hoặc thậm chí không hỗ trợ một số mức mã hóa SSL.

Truy cập từ các trình duyệt cũ cũng ảnh hưởng đến hoạt động của phiên làm việc SSL VPN. Ví dụ, nhiều trình duyệt không hỗ trợ nén qua luồng HTTP.

Thông thường, công nghệ SSL VPN thường được quảng cáo cho phép truy cập từ bất kỳ trình duyệt nào, nhưng thực sự đó là một cách thổi phồng những ưu điểm của công nghệ SSL VPN.

2.6 Ví dụ phiên SSL VPN

Bây giờ chúng ta sẽ mô tả các thành phần của SSL VPN thực hiện như thế nào, trong một phiên làm việc của người dùng:

1. Người dùng nhập URL của hệ thống truy cập từ xa SSL VPN vào trình duyệt. Trong ví dụ này là *http://remote.packtpub.com.*
2. Nếu người dùng truy nhập với một cổng không mã hóa (trong ví dụ này là HTTP ở cổng 80), SSL VPN sẽ chuyển tiếp nó tới cổng 443 và bắt đầu sử dụng mã hóa SSL cho tất cả giao tiếp với người dùng. Địa chỉ chuyển tiếp là

https://remote.packtpub.com. SSL VPN sẽ gửi tới người dùng một trang đăng nhập. (Trên thực tế, SSL VPN có thể thực hiện nhiều kiểm tra bảo mật trước khi gửi trang đăng nhập. Đồ án sẽ mô tả chi tiết ở chương sau.

3. Người dùng nhập chứng thực của họ (thông thường là tên đăng nhập và mật khẩu) tới SSL VPN.
4. Nếu chứng thực được chấp nhận, SSL VPN gửi trang chủ và tải về các mã ActiveX hoặc Java cần thiết để thiết lập đường hầm lưu lượng non-web qua SSL hoặc thiết lập kết nối mạng qua SSL.
5. Người dùng chọn một ứng dụng nền web sử dụng trang chủ và SSL VPN sẽ đưa người dùng vào hệ thống. SSL VPN dịch tất cả các giao tiếp từ hệ thống nội bộ trước khi chuyển tiếp chúng tới người dùng.
6. Khi người dùng nhấp chuột vào một liên kết trong ứng dụng, SSL VPN chuyển đổi liên kết từ định dạng bên ngoài thành dạng nội bộ và chuyển tiếp yêu cầu tới máy chủ tương ứng.
7. Khi cần phải có lưu lượng non-web từ máy trạm, phần mềm SSL VPN trên máy chủ người dùng đóng gói dữ liệu bằng cách sử dụng một trong các kỹ thuật đã mô tả ở trên và gửi nó qua kết nối SSL tới SSL VPN, ở đó nó sẽ khôi phục nó trở thành định dạng ban đầu và gửi nó tới mạng nội bộ.

2.7 Kết luận

Chương này đã trình bày về giao thức SSL và cách thiết lập VPN sử dụng SSL, đây là hoạt động cơ bản của SSL VPN. Chương này cũng giới thiệu các công nghệ tiền thân của SSL VPN, và qua đó hiểu rõ hơn bản chất của nó. Ngoài ra, trong nội dung chương cũng đề cập đến các dịch vụ, các thành phần của một SSL VPN điển hình, và từ đó nêu ra hoạt động của nó, các thành phần bổ sung cho hoạt động của nó.

Qua những nội dung đã trình bày, chúng ta có thể nhận thấy SSL VPN tận dụng các công nghệ tiên tiến để cho phép truy cập từ xa từ bất kỳ các trình duyệt nào. Chúng được trang bị để cho phép giao tiếp nền web và non-web, và sử dụng các công nghệ phức tạp để đạt được nhiều ưu điểm của cả hai loại lưu lượng này. Thậm chí SSL VPN có thể cho phép kết nối mạng từ xa.

Những ưu điểm của SSL VPN khiến cho nó phát triển mạnh. Tuy nhiên, SSL VPN vẫn tồn tại một số vấn đề về bảo mật sẽ được trình bày trong ở chương sau.

CHƯƠNG 3: BẢO MẬT TRONG SSL VPN

SSL VPN thực hiện như một gateway vào cấu trúc mạng của công ty, và do đó vấn đề bảo mật là một thành phần quan trọng của SSL VPN. Và khả năng bảo mật của thiết bị SSL VPN là một trong những yếu tố quan trọng để công ty sẽ chọn sản phẩm nào để thực hiện.

Bảo mật trong SSL VPN chia thành ba phần chính:

- **Nhận thực (Authentication) và xác thực (Authorization)**: Người dùng có thể truy cập tới các thông tin và hệ thống qua SSL VPN. Vì vậy, phải chắc chắn rằng chỉ có các người dùng nhận thực có thể truy cập tài nguyên qua SSL VPN và các người dùng độc lập chỉ có thể truy cập tới tài nguyên của họ được phép truy cập.
- **Bảo mật đầu cuối**: Bảo mật đầu cuối thường được biết đến như là bảo mật bên máy trạm (Client-Side Security) hoặc bảo mật bên trình duyệt (Browser-Side Security). Đây là một công nghệ thực hiện để tránh các vấn đề liên quan đến bảo mật xảy ra trên các thiết bị được sử dụng để truy nhập các tài nguyên qua SSL VPN. Một điều quan trọng nữa là không giống như các công nghệ truy cập từ xa trước đây, công nghệ SSL VPN cho phép truy cập từ các máy không được xem là an toàn và do đó, khái niệm điểm đầu cuối khác với khái niệm điểm đầu cuối trong các hệ thống truy cập từ xa trước đây.
- **Bảo mật bên máy chủ**: Bảo mật bên máy chủ, thường được gọi là bảo mật mạng (Network Security), tương ứng với việc bảo vệ nguồn tài nguyên nội bộ của công ty bao gồm bản thân máy chủ SSL VPN từ các cuộc tấn công từ máy tính nạn nhân.

Mặc dù đồ án sẽ mô tả khá chi tiết các lĩnh vực bảo mật trên, nhưng cần lưu ý là các sản phẩm SSL VPN thực hiện bảo mật rất là khác nhau. Mỗi sản phẩm không cần thiết phải có tất cả các chức năng trên, và tùy thuộc vào thiết kế sản phẩm và khả năng của nó, một vài vấn đề bảo mật được bỏ qua khi thực hiện thiết bị. Một điều dễ nhận thấy là một vài chức năng bảo mật mô tả dưới đây thường được thực hiện qua cách tích hợp các sản phẩm của hãng thứ ba với chức năng lõi SSL VPN được thực hiện bởi nhà sản xuất SSL VPN, đôi khi còn được thực hiện bởi người thực hiện. Phần sau của chương này mô tả các chức năng bảo mật với công nghệ SSL VPN và một vài cách thực hiện các chức năng này.

3.1 Nhận thực và Xác thực

Như đã mô tả ở trước, SSL VPN thường cần người dùng xác thực bản thân họ trước khi được phép truy cập vào tài nguyên nội bộ.

3.1.1 Nhận thực

Nhận thực thường thực hiện bằng một trong các cách sau:

- Một cái gì đó mà chỉ một người biết.
- Một cái gì đó mà chỉ một người có.
- Một cái gì đó mà chỉ người đó là (ví dụ như đặc điểm vật lý của người sử dụng).

Các sản phẩm SSL VPN hỗ trợ nhiều phương thức bảo mật khác nhau. Thông thường nhất, nhận diện người dùng thường sử dụng tên đăng nhập và một trong các nhân tố sau:

a) Mật khẩu

Người dùng được cấp một mật khẩu bí mật mà chỉ người dùng biết và nó kết hợp với thông tin nhận diện của người dùng (tên đăng nhập). SSL VPN so sánh mật khẩu với mật khẩu được lưu trữ trong cơ sở dữ liệu hoặc thực hiện thuật toán băm và so sánh với giá trị băm của mật khẩu với mật khẩu lưu trong cơ sở dữ liệu. Nếu hai giá trị này giống nhau, người dùng được xác thực.

b) Mật khẩu một lần

Người dùng được cấp một vài mật khẩu mà chỉ có thể dùng một lần. Sau khi người dùng nhập tên đăng nhập cùng với mật khẩu một lần, người dùng có thể đăng nhập hệ thống. Tuy nhiên, mật khẩu đặc biệt được sử dụng để truy cập sẽ không thể được dùng để truy cập ở các lần tiếp theo. Mật khẩu một lần được thực hiện bằng các cách sau:

- **Danh sách các mật khẩu một lần được xác định từ trước**: Một danh sách các mật khẩu một lần được tạo bởi hệ thống nhận thực và gửi tới người dùng khi họ ở cơ quan. Ở thời điểm người dùng muốn đăng nhập từ xa, người dùng sử dụng mật khẩu tiếp theo trong danh sách và xóa nó khỏi danh sách. Khi danh sách hết, một danh sách mới sẽ được tạo ra và gửi tới người dùng.
- **Phần cứng hoặc phần mềm có thể tạo ra mật khẩu một lần**: Các sản phẩm như Vasco DigiPass hoặc RSA SecurID khá phổ biến trong lĩnh vực này. Một thiết bị phần cứng nhỏ hoặc một phần của phần mềm chạy trên một máy tính cầm tay hoặc một máy tính xách tay được sử dụng để tạo ra một mật khẩu một lần bằng cách tính toán dựa trên thời gian hệ thống, một tổ hợp khóa, và thông tin khác. Máy chủ nhận thực có thông tin về tổ hợp khóa và có thể tạo mật khẩu người một lần giống như thế ở bất kỳ thời điểm nào mà người dùng thử kết nối. Giá trị của người dùng nhập vào được so sánh với giá trị được tạo bởi máy chủ nhận thực và nếu chúng trùng nhau, người dùng sẽ được phép truy nhập.
- **Trả lời dựa trên các hệ thống thẻ bài phần cứng hoặc phần mềm**: Máy chủ nhận thực đánh dấu người dùng với một số (hoặc một chuỗi các ký tự) mà người dùng nhập vào hệ thống phần mềm hoặc hệ thống thẻ bài phần cứng. Thẻ bài hoặc phần mềm sẽ tạo ra một mã dựa trên thông tin nhập vào. Mã này sẽ được gửi tới máy chủ nhận thực. Máy chủ so sánh giá trị nhận được với giá trị nó tự tạo ra dựa trên mã ban đầu và nếu trùng khớp thì người dùng được phép truy cập.

c) Thông tin sinh trắc học

Sinh trắc học là cách người ta dùng các đặc điểm sinh học của con người để nhận diện người dùng, phương pháp này thường không được dùng phổ biến trong truy nhập SSL VPN. Các bộ đọc sinh trắc thường không có ở nhiều nơi và do đó, nhận thực bằng sinh trắc học chỉ giới hạn ở một số địa điểm. Tuy nhiên, sinh trắc học có thể được sử dụng để nhận thực người dùng cho phiên đặc quyền, phương pháp tên đăng nhập và mật khẩu cho phép người dùng truy nhập, nhưng người dùng sử dụng phương pháp nhận thực sinh trắc họ sẽ được phép truy cập nhiều tài nguyên hơn. Khái niệm này sẽ được mô tả nhiều hơn ở phần sau của chương này.

d) Các chứng thực máy trạm

Các chứng thực máy trạm (là một ví dụ của trường hợp "một cái gì đó mà người dùng có") có thể được sử dụng để nhận thực người dùng vào SSL VPN. Tuy nhiên, cần phải lưu ý rằng việc sử dụng của họ thường bị giới hạn chỉ ở trên các máy tính mà cài đặt sẵn chứng thực. Rõ ràng là không thể sử dụng phương pháp này cho các trạm Internet công cộng, do các trạm này thường không cho phép người dùng truy nhập vào ổ đĩa mềm/CD hoặc USB. Hơn nữa, nếu chứng thực này chứng tỏ một một tài nguyên gì đó mà một người dùng có trong khi người khác không được phép có, sẽ là không thận trọng nếu cho phép tải một chứng thực lên một máy tính mượn hoặc máy tính công cộng, mà các máy tính này có thể dễ dàng bị các tổ chức khác sử dụng. Do đó, chứng thực máy trạm thường được sử dụng từ các thiết bị bảo mật đặc biệt.

e) Thẻ thông minh hoặc USB Token

Là các thiết bị vật lý nhỏ được thiết kế đặc biệt cho việc sử dụng với các hệ thống nhận thực, thường thì các chứng thực máy trạm hoặc mật khẩu đã mã hóa được lưu trữ trên các thiết bị này.

f) Nhận thực dựa trên hai nhân tố

Các sản phẩm SSL VPN thường cho phép sử dụng hai yếu tố nhận thực. Nhận thực dựa trên hai nhân tố tức là quá trình nhận thực sử dụng cả hai phương thức nhận thực khác nhau, ví dụ, cung cấp một mật khẩu mà chỉ người dùng biết và một mật mã từ một thẻ phần cứng mà chỉ có người dùng có. Nhận thực dựa trên hai nhân tố thường mạnh hơn nhận thực một nhân tố thông thường, tuy nhiên, một phương pháp nhận thực mạnh một nhân tố sẽ hiệu quả hơn là nhận thực hai nhân tố yếu.

Một điểm đáng chú ý là một vài người dùng đề nghị nhận thực dựa trên địa chỉ IP của thiết bị người dùng sử dụng để truy cập. Trong trường hợp công nghệ SSL VPN,thì điều này sẽ dẫn tới một vài vấn đề. Mục tiêu của SSL VPN là cung cấp một truy cập từ xa từ nhiều loại máy khác nhau. Do đó người quản trị không muốn giới hạn số máy tính mà từ đó người dùng có thể truy cập qua SSL VPN. Do đó, chúng ta không muốn sử dụng địa chỉ IP để sử dụng nhận diện người dùng. Người dùng có thể sử dụng SSL VPN từ một

máy tính mới hoàn toàn hoặc máy tính đã sử dụng trước đây. Họ cũng có thể sử dụng các máy tính công cộng hoặc máy tính mượn để thực hiện truy cập từ xa. Hơn nữa, sự phổ biến của NAT (Network Address Translation – Giao thức phân giải địa chỉ) dẫn tới trường hợp nhiều người dùng sử dụng các máy tính khác nhau trong cùng một mạng LAN, trong khi máy chủ SSL VPN thì lại hiểu học cùng một địa chỉ IP, và việc sử dụng rộng rãi DHCP và các giao thức gán địa chỉ IP động khác dẫn tới một vấn đề là địa chỉ IP có thể thay đổi dễ dàng giữa các phiên SSL VPN.

Bất chấp các vấn đề kể trên, địa chỉ IP có thể được sử dụng kết hợp với thông tin dựa trên máy tính để nhận diện các máy (sẽ được mô tả ở sau trong chương này). Ở cùng một thời điểm, rõ ràng rằng địa chỉ IP không thể sử dụng để nhận diện các người dùng của một SSL VPN.

3.1.2 Đăng nhập một lần

Như đã mô tả ở phần trên, SSL VPN thường cho phép khả năng đăng nhập một lần SSO (Single Sign On), điều này có nghĩa là không cần người dùng phải nhận thực cho một ứng dụng trong mọi phiên. Đúng hơn là họ tận dụng một vài kỹ thuật để gom các chứng thực mà người dùng đã nhập vào. Chi tiết về phương pháp này đã được mô tả chi tiết ở phần trên.

3.1.3 Xác thực

Trong công nghệ SSL VPN, xác thực đại diện cho khả năng một người dùng đã nhận thực được phép truy cập các ứng dụng cụ thể và đọc, thay đổi hoặc xóa các file hoặc dữ liệu cụ thể. Xác thực được thực hiện theo nhiều cách khác nhau:

a) Sự cho phép của hệ điều hành

Sự truy cập tới một vài ứng dụng hoặc file có thể được điều khiển bởi sự cho phép của hệ điều hành (ví dụ như danh sách điều khiển truy cập Access Control List hay ACL), nó định nghĩa người dùng nào có thể được truy cập tài nguyên cụ thể. Khi người dùng thử truy cập tài nguyên, hệ điều hành xác định tài nguyên nào họ được phép truy cập và không được phép truy cập, từ đó quyết định cho phép hay từ chối truy cập.

b) Sự cho phép của hệ thống file

Các máy tính có hệ thống file được truy cập có thể điều khiển truy nhập tới các thư mục và các file qua các ACL chuẩn hoặc các điều khiển file hệ thống khác được cho phép truy cập đúng tài nguyên của người dùng hoặc nhóm người dùng cụ thể. Hệ thống thường được thực hiện như là một phần của hệ điều hành, nhưng một vài trường hợp có thể là một gói bổ sung.

c) Sự cho phép của ứng dụng

Một vài ứng dụng cần phải xác thực trước khi cho phép truy cập. Dựa vào chức năng nhận diện người dùng trong ứng dụng, mà nó có thể cho phép hoặc chặn hoạt động của người dùng. Chức năng này không phân biệt người dùng từ xa hay người dùng trong cơ quan của họ.

d) Các giao diện hạn chế

Một SSL VPN cũng có thể chặn một người dùng khi họ truy cập một tài nguyên cụ thể bằng cách dựa trên giao diện hạn chế người dùng. Một giao diện hạn chế có thể được tận dụng qua SSL VPN để tránh người dùng thấy các công cụ mà họ không được sử dụng. Khi thực hiện giao diện hạn chế này sẽ giảm được các cuộc gọi giúp đỡ, người dùng sẽ không gọi và hỏi làm sao họ thấy các ứng dụng cụ thể nhưng không thể truy cập chúng.

e) Thông tin xác thực được quản lý bởi SSL VPN

Khi người dùng truy cập từ xa, quyền truy cập của họ có thể khác khi họ truy cập từ trong cơ quan. Hệ thống này được gọi là hệ thống truy cập phân cấp (Tiers-of-Access) (sẽ được mô tả trong phần sau của chương này). Khi thông tin xác thực khác với các phiên từ xa, dữ liệu liên quan tới người nào có thể truy cập từ xa thường được lưu trữ trong dữ liệu cục bộ của máy chủ SSL VPN. Người dùng không được phép truy nhập với các tài nguyên qua SSL VPN (thậm chí nếu họ có thể truy cập tài nguyên đó khi họ ở văn phòng) sẽ không được SSL VPN cho phép truy cập tài nguyên đó.

f) Cơ sở dữ liệu xác thực nhóm thứ ba

Một nơi có thể lưu trữ thông tin xác thực cho người dùng nội bộ và người dùng từ xa có thể được lưu trữ trong các cơ sở dữ liệu xác thực nhóm thứ ba. Các sản phẩm thực tế trong các năm gần đây đã được tích hợp các hệ thống này.

3.2 Các vấn đề bảo mật đầu cuối

Các vấn đề bảo mật đầu cuối bao gồm các vấn đề sau:

- Dữ liệu nhạy cảm ở trong vùng không an toàn
- Người dùng quên đăng xuất
- Các virus đến các mạng nội bộ qua SSL VPN
- Các đoạn mã độc hai tới mạng nội bộ qua đường hầm tạo bởi SSL VPN
- Các hacker truy nhập tới mạng tập đoàn bằng cách rẽ các mạng qua SSL VPN

3.2.1 Vấn đề dữ liệu nhạy cảm ở trong vùng không an toàn và giải pháp

3.2.1.1. Vấn đề

Trong suốt phiên truy nhập từ xa, người dùng có thể tải về các thông tin nhạy cảm tới thiết bị mà họ đang sử dụng để truy cập. Trong thời kỳ đầu của các công nghệ truy cập từ xa, mặc dù dữ liệu cá nhân được lưu trữ trên các thiết bị truy cập nhưng đó không phải

là vấn đề nghiêm trọng do người dùng chỉ có thể truy cập từ các thiết bị của công ty, thiết bị này được công ty cung cấp cho họ. Tuy nhiên, với sự phát triển của SSL VPN và người dùng bắt đầu truy cập tài nguyên của công ty từ các máy tính công cộng hoặc máy tính mượn, lưu trữ dữ liệu trên các thiết bị đó có thể dẫn tới các vấn đề bảo mật.

Một vài thông tin lưu trữ trên một thiết bị truy nhập có thể được lưu trữ tạm thời trên máy tính. Ví dụ, một người dùng tận dụng khả năng truy cập file của SSL VPN và tải về một bảng gì đó mà có thể lưu lại trên ổ đĩa. Nếu file này bao gồm các thông tin cá nhân, ví dụ như kế hoạch bán hàng trong một vài năm tới, thì tốt hơn hết là chúng ta nên xóa bảng này khi phiên truy cập kết thúc.

Vấn đề này là cực kỳ nghiêm trọng khi một số lượng lớn dữ liệu nhạy cảm được lưu trữ trên thiết bị truy nhập mà người dùng không hề biết.

a) Vấn đề bộ nhớ đệm trình duyệt

Để cải thiện hiệu quả hoạt động, các trình duyệt thường lưu trữ bản sao các trang web, ảnh và file đa phương tiện mà người dùng truy nhập. Bằng cách cho phép trình duyệt tải các thành phần nhanh hơn khi người dùng quay trở lại trang trước (hoặc thậm chí là trang khác mà có sử dụng các thành phần này). Tuy nhiên, điều đó cũng dẫn đến một vấn đề bảo mật cho người dùng SSL VPN, là người sử dụng tiếp theo có thể truy cập SSL VPN để cho phép tải các thông tin đã truy cập trong suốt phiên SSL VPN trước đó.

b) Vấn đề bộ nhớ đệm của các chương trình

Một vài ứng dụng không sử dụng các bộ nhớ đệm hệ thống chuẩn để lưu trữ dữ liệu tạm thời của chúng. Thay vào đó, chúng tận dụng các hệ thống bộ nhớ đệm của riêng chúng và lưu trữ ở những nơi khác trong hệ thống file nội bộ. Dữ liệu ghi trên các bộ nhớ đệm sẽ bị xóa khi kết thúc phiên làm việc SSL VPN. Phần này sẽ được mô tả chi tiết ở phần sau trong chương này, các công cụ nhóm thứ ba có thể được sử dụng để truy nhập một SSL VPN cũng có thể tạo các phiên bản bộ nhớ đệm của các file truy cập trong các bộ nhớ đệm của chúng.

c) Các file tạm thời: Xem các file đính kèm E-mail

Tương tự như vậy, các file tạm thời được tạo ra trên thiết bị truy nhập khi người dùng truy nhập file đính kèm e-mail qua một giao diện Webmail. Trong nhiều trường hợp, các file không tự động xóa bởi hệ thống e-mail khi người dùng kết thúc phiên làm việc – do đó người dùng tiếp theo có thể xem được nội dung của bất kỳ file đính kèm nào mà người dùng đã mở ra. Việc mã hóa các file đính kèm e-mail sẽ làm cho các file này là không thể đọc với nhóm thứ ba, thường không thể giải quyết được vấn đề này do có hai lý do sau:

- Các file được lưu đệm khi chúng được truy cập trong các ứng dụng truyền thống – như văn bản trong Microsoft Word. Điều này thường xảy ra sau khi chúng được giải mã.
- Khả năng giải mã hóa thường không có trong các giao diện Web-mail.

Mật khẩu bảo vệ tất cả các file đính kèm (ví dụ như khả năng sử dụng mật khẩu bảo vệ có trong Word, Excel,…) cũng không giải quyết được vấn đề này do:

- Không phải tất cả các ứng dụng cho phép bảo vệ dữ liệu qua mật khẩu.
- Cơ chế mật khẩu trong một số ứng dụng quá yếu, có thể dễ dàng bị bẻ khóa.
- Việc cần thiết phải bảo vệ tất cả các file đính kèm bằng mật khẩu là không thực tế, người dùng không thích sử dụng chúng trong tất cả các file.

Chúng ta cần một giải pháp tốt hơn đối với vấn đề bộ đệm các file đính kèm.

d) File tạm thời: Các cơ chế tải về và cơ chế khác

Vấn đề này đồng nhất với vấn đề file đính kèm – chỉ khác cách đưa thông tin ban đầu tới thiết bị truy nhập.

e) Nội dung các trường được nhớ cho chức năng AutoComplete

Khi người dùng điền các trường trong form trực tuyến, họ thường thấy các giá trị mà trình duyệt khuyến nghị, là các giá trị mà người dùng đã nhập trước đó. Điều này là do trình duyệt thường lưu đệm dữ liệu các trường để hỗ trợ trong các form trong tương lai. Một người dùng nhập một địa chỉ e-mail trên một trang web mà nội dung các form tương tự như trang web trước đây thì chức năng AutoComplete sẽ tự động điền vào các trường này bằng các giá trị trước đây. Tuy nhiên, như trường hợp nhớ đệm các thành phần web, chức năng này dẫn tới một vấn đề bảo mật đối với người dùng SSL VPN. Các dữ liệu mà người dùng nhập vào các trường trong suốt một phiên SSL VPN như số CMTND có thể bị người khác thấy.

f) URL được nhớ đệm do chức năng AutoComplete

Tương tự như nội dung được nhớ, các URL được truy cập bởi người dùng được lưu trữ đệm trên các thiết bị truy nhập. Điều này cho phép người dùng bắt đầu nhập một vài từ vào thanh địa chỉ và máy tính sẽ hỗ trợ các phần còn lại của địa chỉ, giúp cho người dùng thuận tiện không phải gõ lại nhiều lần. Cũng giống như trường hợp các trường form, điều này cũng có thể dẫn tới trường hợp các thông tin cá nhân trong URL có thể bị thấy bởi người khác. Đây cũng là một vấn đề cá nhân, nhiều người không muốn người khác biết về các tài nguyên mạng mà họ đã xem. Vì vậy các địa chỉ URL đã truy cập trong một phiên truy cập từ xa phải được xóa trong các máy tính công cộng hoặc máy tính mượn, để người khác không thể thấy.

g) Tạo cookie trong suốt các phiên người dùng

Cookie là một trường văn bản nhỏ được để trong thiết bị truy nhập trong suốt phiên web, nó cho phép các thông tin cụ thể được nhớ, như thông tin người dùng cho phiên làm việc đó hoặc phiên tiếp theo. Các cookie thường lưu trữ thông tin tên đăng nhập (và đôi khi là cặp nhận thực tên đăng nhập và mật khẩu) cho các website mà người dùng muốn truy nhập mà không cần phải nhập toàn bộ các thông tin đăng nhập mỗi lần họ muốn truy cập. Các cookie cũng thường được sử dụng để lưu trữ các tùy chọn, tùy biến cá nhân cho các trang web cụ thể. Do vậy, cookie có thể chứa thông tin nhạy cảm, và trong khi chúng tạo ra những ưu điểm lớn về hỗ trợ người dùng và cải thiện các chức năng thì chúng cũng dẫn tới vấn đề bảo mật khi chúng có thể bị mất trên các máy tính công cộng hoặc máy tính mượn khi phiên làm việc SSL VPN kết thúc.

h) Các bản ghi lưu giữ

Các trình duyệt thường hỗ trợ lưu giữ các trang web đã truy cập vì vậy người dùng có thể dễ dàng truy cập lại các trang này mà không cần phải truy cập lại. Nhưng các thông tin này cũng có thể dễ dàng bị mất khi người tiếp theo có thể xem được. Các thông tin này cũng chứa các thông tin nhạy cảm, do vậy cũng dễ dàng bị mất trên các máy tính công cộng hoặc máy tính mượn.

i) Các chứng thực người dùng được nhớ bởi trình duyệt

Một vài trình duyệt web cho phép người dùng nhớ các thông tin chứng thực như tên đăng nhập và mật khẩu, do đó người dùng sẽ không cần phải nhập bằng tay các thông tin này ở lần đăng nhập tiếp theo. Rõ ràng là khi người dùng SSL VPN trên máy tính mượn hoặc máy tính công cộng sẽ không muốn lưu trữ các thông tin như vậy trên thiết bị họ muốn truy cập. Tuy nhiên, nếu một người dùng sai sót và cho phép trình duyệt lưu trữ chứng thực của người đó thì sẽ dẫn tới một vấn đề bảo mật nghiêm trọng. Hơn nữa, một vài chứng thực được lưu trữ mà không hỏi người dùng! Ví dụ như hệ thống sử dụng phương pháp bảo mật HTTP đơn giản lưu trữ mật khẩu của người dùng trong suốt phiên làm việc (để tránh có hỏi người dùng nhập lại ID và mật khẩu đối với mỗi yêu cầu tới máy chủ). Các chứng thực này sẽ được lưu giữ mà cho tới khi trình duyệt tắt hoặc người dùng khác đăng nhập và nhập vào mật khẩu mới.

Rõ ràng rằng điều này sẽ dẫn tới các thông tin nhạy cảm có thể bị mất trên các thiết bị không đảm bảo khi người dùng kết thúc phiên SSL VPN của họ.

3.2.1.2 Giải pháp

Có nhiều cách để giải quyết các vấn đề dữ liệu nhạy cảm lưu trữ trên các thiết bị truy nhập, các sản phẩm SSL VPN khác nhau có cách giải quyết khác nhau. Tuy nhiên, hầu hết là các giải pháp sau:

- **Không làm gì cả**: Phương thức này là không thể chấp nhận đối với hầu hết các tổ chức, nhưng một vài sản phẩm SSL VPN cấp thấp không thể giải quyết được vấn đề dữ liệu ở thiết bị đầu cuối.
- **Cảnh báo người dùng**: Một vài thiết bị SSL VPN cấp thấp không làm gì để bảo vệ dữ liệu nhạy cảm nhưng cảnh báo người dùng nên đăng xuất hoặc loại bỏ các dữ liệu nhạy cảm của phiên làm việc. Phương pháp này thường không hiệu quả do:
    - Xóa bỏ thông tin bộ đệm không phải là một việc làm đơn giản – như đã mô tả ở trên, có nhiều vùng trong đó thông tin nhạy cảm được lưu trữ. Một người dùng cần phải có hiểu biết nhiều về kỹ thuật mới có thể xóa các thông tin này.
    - Thậm chí hiểu biết kỹ thuật của người dùng cũng không đủ để thực hiện xóa hết các thông tin nhạy cảm khỏi ổ cứng. Một lệnh hệ thống như Del hoặc rm là không đủ để bảo vệ các thông tin nhạy cảm khỏi các truy cập không phù hợp (sẽ được mô tả ở phần sau trong chương này).
    - Điều gì sẽ xảy ra nếu người dùng không bao giờ đăng xuất và không có cảnh báo nào xuất hiện?
- **Tận dụng lệnh NOCACHE**: Hầu hết các trình duyệt phổ biến hiện nay đều hiểu lệnh NOCACHE được gửi từ máy chủ web để không cho phép lưu đệm dữ liệu truy cập. Về mặt lý thuyết, nếu máy chủ SSL VPN thực hiện lệnh NOCACHE trên tất cả các trang dữ liệu nó gửi tới máy tính người dùng thì vấn đề dữ liệu nhạy cảm được lưu trữ đệm sẽ được giải quyết. Tuy nhiên, thực tế nó lại không giải quyết được vấn đề do một số lý do sau:
    - Không phải tất cả các trình duyệt hỗ trợ NOCACHE.
    - Một vài ứng dụng cần bộ nhớ đệm mới thực hiện được các chức năng của nó.
    - Việc loại bỏ bộ nhớ đệm sẽ dẫn tới giảm hiệu năng hệ thống và một vài ứng dụng cơ bản sẽ không thực hiện được, đặc biệt là trên đường truyền modem chậm.
    - Lệnh NOCACHE không tránh được việc lưu AutoComplete, lưu history và một số chức năng khác. Nó chỉ bắt trình duyệt không lưu đệm các thành phần web nhận được. Các file tạm thời vẫn được tạo ra khi mở file đính kèm e-mail và kết quả là các vấn đề bảo mật vẫn tồn tại.

Tuy có các nhược điểm nghiêm trọng trên, một vài SSL VPN cấp thấp vẫn dùng lênh NOCACHE để thực hiện bảo mật. Các giải pháp này có thể sử dụng cho các dự án cụ thể và trong các môi trường thực tế, nhưng nhìn chung, một trong hai phương pháp kể trên sẽ được sử dụng để xóa các dữ liệu nhạy cảm.

- **Xóa tất cả các dữ liệu bộ đệm sau phiên làm việc của người dùng**: Khi một người dùng kết thúc một phiên làm việc, SSL VPN sẽ xóa tất cả các thông tin bộ đệm được tạo ra trong suốt phiên làm việc đó. Một điều quan trọng là thông tin tạm thời cần phải được xóa khỏi thiết bị truy nhập không chỉ khi người dùng đăng xuất,

mà cả khi ngắt phiên làm việc và một số trường hợp các. Các phiên làm việc có thể kết thúc khi một trong các lý do sau:

- Người dùng đăng xuất
- Sau một khoảng thời gian mà người dùng không thực hiện gì cả
- Sau một thời gian định trước, hoặc sau khi xuất hiện sự kiện nhận thực lại (đã định trước) nhưng người dùng không thực hiện nhận thực thì phiên làm việc cũng tự động kết thúc
- Trình duyệt bị hỏng
- Trình duyệt tắt
- Hệ điều hành thiết bị truy nhập bị hỏng
- Hệ điều hành tắt hoặc khởi động lại
- Thiết bị truy nhập bị tắt do mất điện

Khi bất kỳ một trong các trường hợp trên xảy ra, SSL VPN cần phải xóa các thông tin nhạy cảm trên thiết bị truy nhập. Tuy nhiên, trong trường hợp hệ điều hành hỏng hoặc mất điện, thì việc xóa bỏ thông tin sẽ được thực hiện sau khi hệ thống khởi động lại.

- **Sử dụng không gian lưu trữ ảo mã hóa, không gian này sẽ bị xóa sau khi phiên làm việc kết thúc**: SSL VPN sử dụng một phần của bộ nhớ và ổ đĩa cứng (và bắt các công cụ khác trên thiết bị truy nhập phải sử dụng chúng) để lưu trữ tất cả các thông tin tạm thời cho phiên làm việc của người dùng. Nội dung của phần bộ nhớ và ổ đĩa này được mã hóa. Không gian lưu trữ ảo này có thể bị xóa khi kết thúc phiên làm việc, nhưng thậm chí nếu không bị xóa thì các thông tin này cũng rất khó bị mất vào tay các nhóm không nhận thực. Giải pháp này dường như là một giải pháp đơn giản để giải quyết vấn đề thông tin bộ đệm, nhưng không gian ảo này lại không tương thích với tất cả ứng dụng, đây là nhược điểm chính để phương pháp này không được thực hiện.

Các hệ điều hành mới tận dụng các hệ thống bộ nhớ ảo chứa các file swap. Cho phép người dùng có khả năng sử dụng nhiều hơn dung lượng bộ nhớ của máy tính, bộ nhớ này nằm trên ổ cứng. Vì vậy, trong trường hợp dữ liệu đệm bị xóa hoặc không gian lưu trữ ảo được sử dụng, thì có thể một vài thông tin nhạy cảm được lưu giữ trong file swap và có thể không bị xóa sau khi kết thúc phiên làm việc người dùng. Thông thường, người dùng khác không thể đọc được nó. Tuy nhiên, trong trường hợp cố ý đọc thì các chuyên gia điệp báo có thể đọc được thông tin nhạy cảm này.

3.2.2 Vấn đề công cụ tìm kiếm của nhóm thứ ba và giải pháp

3.2.2.1. Vấn đề

Một vấn đề bảo mật nữa là các công cụ tìm kiếm của nhóm thứ ba (ví dụ như Google Desktop Search Tool) chạy trên các máy tính sử dụng để truy nhập SSL có thể tạo

ra các phiên bản đệm của các trang web và các tài liệu đã truy cập trong suốt phiên làm việc SSL VPN.

Thậm chí các trang SSL đã mã hóa có thể được lưu trữ ở dạng không mã hóa! Điều này dẫn tới một vấn đề bảo mật nghiêm trọng thậm khi đối với người dùng sử dụng SSL VPN để xóa các dữ liệu tạm thời sau khi kết thúc mỗi phiên SSL VPN. Các dữ liệu được lưu đệm bởi các công cụ tìm kiếm – và thông tin chỉ mục được tạo bởi các công cụ này – có thể tiếp tục được lưu giữ ngay cả khi các thông tin trong bộ đệm bị xóa. Sẽ rất khó để xóa bộ nhớ đệm trong các công cụ tìm kiếm này và thường không thể xóa các bản ghi riêng lẻ từ bộ nhớ đệm. Điều cốt yếu là, các công cụ tìm kiếm có thể tạo các bộ nhớ của nó mà không thể truy nhập bởi SSL VPN.

3.2.2.2. Giải pháp

Có nhiều cách để giải quyết vấn đề trên:

- **Chặn truy nhập**: SSL VPN phải chặn truy nhập nếu xác định được các các công cụ tìm kiếm (hoặc công cụ tạo chỉ mục) chạy trên thiết bị truy nhập. Việc này sẽ giới hạn truy nhập, nhưng tránh được việc lưu đệm dữ liệu. Tất nhiên SSL VPN phải biết được công cụ tìm kiếm nào đang được sử dụng và làm thế nào để xác định nó.
- **Tắt chức năng tạo chỉ mục**: SSL VPN phải tắt chức năng tạo chỉ mục và khởi động lại nó khi kết thúc phiên làm việc SSL VPN. Tương tự như phương pháp trên, SSL VPN cần phải có những hiểu biết về các công cụ tìm kiếm.
- **Sử dụng không gian lưu trữ ảo đã mã hóa (có thể xóa được)**: Phiên SSL VPN không bao giờ lưu các file không mã hóa trên ổ đĩa – thay vào đó, nó sử dụng một không gian lưu trữ ảo, và sẽ xóa không gian này sau khi kết thúc phiên làm việc. Tuy nhiên, điều này không bảo vệ được dữ liệu đệm trước tất cả các công cụ tìm kiếm, và có thể không bảo vệ được các thông tin nhạy cảm bị ghi vào các công cụ tạo chỉ mục (thậm chí ngay cả trường hợp bản copy dữ liệu là không thể truy nhập được đối với công cụ tạo chỉ mục).

Các yêu cầu của văn phòng bảo vệ (DoD – Department of Defense)

Việc xóa các thông tin tạm thời khỏi thiết bị truy cập không phải là một nhiệm vụ đơn giản như việc gọi hệ điều hành xóa các file thông thường. Điều này là do ba lý do sau:

- Các hệ đều hành hiện nay đều có chức năng tránh việc xóa các thông tin quan trọng. Một trong số các chức năng này là "Trash Can" hoặc "Recycle Bin" mà thực chất sau khi xóa các file thì các file bị xóa sẽ được lưu trữ ở đây cho tới khi không gian mà chúng chiếm cần phải được giải phóng để lưu trữ các file khác. Bởi vì các file có thể được phục hồi từ những thư mục đặc biệt này và các công cụ phục hồi hệ

thống khác, SSL VPN không nên gọi các lệnh hệ điều hành Del để xóa các thông tin nhạy cảm trên các thiết bị truy nhập.

- Thậm chí khi Trash Can/Recycle Bin không được sử dụng, các hệ điều hành thường không xóa hẳn các file khỏi ổ đĩa khi chúng thực hiện "deleted". Thay vào đó, chúng xóa các liên kết tới file bị xóa trong calalog nội dung ổ đĩa, và do đó các file không truy cập được nữa mặc dù nội dung của nó vẫn được lưu dữ vật lý cho tới khi chúng bị ghi đè lên bởi dữ liệu mới. Trừ khi chúng bị ghi đè thì các file này vẫn có thể dễ dàng khôi phục bằng các phần mềm đặc biệt.
- Thậm chí khi bị xóa logic trong ổ đĩa và ghi đè bởi dữ liệu mới thì các vết tích điện tử thông tin ban đầu vẫn được giữ lại. Bằng cách sử dụng các công cụ đặc biệt, người ta vẫn có thể khôi phục được dữ liệu đã bị xóa. Để tránh được điều này thì các máy tính có thể ghi đè các dữ liệu đã bị xóa nhiều lần bằng các chuỗi ngẫu nhiên 1 và 0. Khi đã bị ghi lại ngẫu nhiên nhiều lần thì rất khó để có thể khôi phục được dữ liệu ban đầu.

Văn phòng bảo vệ liên bang Mỹ quy định tiêu chuẩn xóa file cần ít nhất là ba lần và thường thì file đã bị xóa không thể khôi phục. Một vài SSL VPN ngày này sử dụng tiêu chuẩn này khi sử dụng một trong hai phương thức trên để xóa dữ liệu tạm thời.

3.2.3 Vấn đề người dùng quên đăng xuất và giải pháp

3.2.3.1. Vấn đề

Một vấn đề nữa là người dùng quên đăng xuất (logout) phiên làm việc. Điều này thường xảy ra trong môi trường web, trong đó một người dùng có thể nhận thực ở một hệ thống và có thể sử dụng nó, nhưng sau đó lại duyệt một website khác mà không nhận ra rằng phiên làm việc đã nhận thực từ trước vẫn hoạt động. Các phiên làm việc này trên các máy tính rỗi có thể được sử dụng bởi người khác và họ thực hiện các mục đích xấu nhằm lấy các thông tin nhạy cảm. Vấn đề này không chỉ xảy ra ở công nghệ SSL VPN mà thường xảy ra ở tất cả các hệ thống nền web khác.

Để tránh vấn đề này thì các ứng dụng web thường đưa ra một thời gian tự động thoát hệ thống khi không có tác vụ nào thực hiện. Nếu nó xác định rằng không có tác vụ nào đang thực hiện bởi người dùng trong một thời gian định trước thì nó sẽ kết thúc phiên làm việc như là người dùng đăng xuất.

Thời gian tự động thoát hệ thống rõ ràng là rất cần thiết, nó bảo vệ các tổ chức khỏi các phiên làm việc bởi các nhóm không nhận thực sau khi người dùng hệ thống quên đăng xuất. Tuy nhiên, thời gian tự động thoát hệ thống này trong môi trường SSL VPN có thể dẫn tới một số rắc rối sau:

- Một SSL VPN tình cờ thoát phiên làm việc của người dùng và có thể dẫn tới hủy bỏ các công việc đang làm. Vấn đề này có thể là khi người dùng nhập các thông tin

vào form của trình duyệt, họ không truyền bất kỳ thông tin nào tới máy chủ SSL VPN cho tới khi họ thực sự gửi nó bằng cách nhấp chuột vào nút Submit. Và kết quả là nếu người dùng nhập form quá dài, SSL VPN có thể xác định rằng người dùng không làm gì cả trong một khoảng thời gian khá dài. Nếu thời gian này quá thời gian tự động thoát hệ thống mà người dùng vẫn không nhấp chuột nút Submit thì hệ thống sẽ tự động thoát ra. Điều này dẫn tới người dùng sẽ mất dữ liệu họ đang nhập (và tất cả những thứ khác trong phiên SSL VPN). Một kiểu khác của vấn đề này người dùng viết một e-mail quá dài và tương tự như trên, họ có thể mất dữ liệu e-mail họ đang viết dở.

- Một vài hoạt động không thực sự là người dùng đang làm (non-activity) có thể được xem như là hoạt động của người dùng, và phiên làm việc sẽ không bị kết thúc. Vấn đề trên là hoàn toàn có thể xảy ra, một vài chương trình có chức năng tự động refresh, điều đó có nghĩa là nó tự động cập nhật trang web trong một khoảng thời gian định trước. Ví dụ như, các phần mềm e-mail phổ biến thường có một thời gian định trước để cập nhật hộp thư của người dùng, và các ứng dụng quản lý thông tin cá nhân (PIM – Personal Information Manager) thường có một thời gian định trước để cập nhật lịch làm việc. Mặc dùng các chức năng trên rõ ràng là rất cần thiết nhưng nó dẫn tới vấn đề khi thực hiện chức năng tự động tắt phiên làm việc SSL. Các chức năng tự động cậm nhật này được thực hiện bằng cách chèn các mã vào trang web để trình duyệt thực hiện tự động gửi các yêu cầu cập nhật tới máy chủ, tuy nhiên, đối với máy chủ SSL VPN thì nó được xem như một hoạt động của người dùng. Tất cả máy chủ SSL VPN xem dữ liệu được truyền từ trình duyệt người dùng đến SSL VPN như là dấu hiệu để biết người dùng đang thực hiện tác vụ. Do đó, nếu các ứng dụng thực hiện chức năng tự động cập nhật thì chức năng tự động thoát khỏi hệ thống sau một thời gian của SSL VPN sẽ không thể thực hiện được, và các phiên làm việc này sẽ mãi được duy trì. (Vấn đề này cũng có thể xảy ra nếu một SSL VPN được sử dụng để thiết lập một kết nối dạng network qua SSL và sử dụng kỹ thuật tự động ping hoặc các kỹ thuật tương tự).
- Các phiên làm việc người dùng có thể mất trước khi hết thời gian timeout: Một số người xấu vẫn có một cơ hội trong đó họ có thể lợi dụng các phiên bị người dùng bỏ quên trước khi thời gian tự động đăng xuất hết. Các hệ thống timeout dựa trên phương thức đợi một khoảng thời gian xác định để thoát phiên làm việc. Điều này cho phép kẻ xấu sử dụng thiết bị đăng nhập trước khi khoảng thời gian kết thúc và do đó, chúng có thể sử dụng các phiên làm việc này như một người dùng bình thường.

3.2.3.2 Giải pháp

Một vài kỹ thuật được sử dụng trong SSL VPN để giải quyết các vấn đề nêu trên:

a) Thời gian timeout lâu

Trước khi tìm hiểu một vài kỹ thuật để giải quyết vấn đề trên, đồ án sẽ mô tả một phương pháp đơn giản nhưng không thể thực hiện được.

Một cách mà các nhà quản trị hệ thống có thể tránh vấn đề để người dùng hợp pháp làm phiền bởi thời gian timeout không hợp lý là tăng ngưỡng thời gian timeout lên, lâu hơn thời gian mà người dùng thường xử lý các tác vụ như là hoàn thành form hay là viết e-mail. Tuy nhiên thì phương pháp này có nhiều nhược điểm nghiêm trọng.

Việc cho phép các phiên làm việc rỗi bằng cách tăng thời gian timeout làm tăng nguy cơ các người dùng không nhận thực có thể truy cập trong khoảng thời gian mà phiên vẫn hoạt động khi máy tính không có người dùng. Hậu quả là thời gian timeout lâu làm mất đi mục đích ban đầu của chính nó.

Thứ hai, trong một môi trường web một người dùng có thể bắt đầu làm việc trên một form hoặc bản tin e-mal và sau đó xem các website khác, trong khi lại dự định thực hiện lại công việc ban đầu ở một thời điểm sau đó. Do đó, không thể xác định được thời gian bao lâu để viết một e-mail và các ước lượng là không thực tế.

Tất nhiên rằng, ngưỡng thời gian lâu sẽ không làm được gì để giải quyết vấn đề trên nếu các ứng dụng hỗ trợ chức năng tự động cập nhật.

Do đó, ngưỡng thời gian timeout lâu không được sử dụng để giải quyết các vấn đề bảo mật trên.

b) Các hệ thống timeout cảnh báo

Một cách thích hợp để đạt được vấn đề người dùng quên đăng xuất là sử dụng thời gian cảnh báo.

Các hệ thống thời gian cảnh báo là các hệ thống timeout dựa trên việc không hoạt động trong đó người dùng được nhận một cảnh báo trước khi tự động thoát khỏi hệ thống. Hai mức thời gian cảnh báo được sử dụng - một để cảnh báo người dùng sắp tự động thoát, và một để thoát hẳn phiên làm việc. Ví dụ là, một SSL VPN có thể được cấu hình để cảnh báo một người dùng cứ mỗi 8 phút không thực hiện gì cả và sau đó hai phút nếu người dùng vẫn không làm gì cả thì phiên làm việc sẽ bị ngắt. Trên thông báo có thể có một nút để người dùng có thể click vào để tạo cho người dùng một hoạt động (ví dụ, click OK để chấp nhận đã nhận bản tin cảnh báo). Nếu người dùng không phản hồi hoặc tạo ra một hoạt động khác thì phiên làm việc sẽ ngắt sau hai phút (vậy là sau 10 phút sẽ ngắt nếu không có bất kỳ hoạt động nào).

Cảnh báo có thể dưới dạng pop-up với dòng cảnh báo đơn giản: Bạn đang ở đây? Với các nút bấm Có và Không (hoặc thậm chí chỉ nút Có). Nếu người dùng trả lời, SSL VPN biết người dùng đang hoạt dộng và reset bộ đếm thời gian. Nếu người dùng không trả lời, thì trong khoảng thời gian định trước, phiên làm việc sẽ bị ngắt.

c) Buộc nhận thực lại theo chu kỳ

Buộc nhận thực lại theo chu kỳ (FPA – Forced Periodic Re-authentication) bắt buộc người dùng đã nhận thực phải nhập chứng thực của họ sau một khoảng thời gian định trước (được xác định bởi người quản trị) để tiếp tục được làm việc.

Kết hợp với các ngưỡng cấu hình đã đề cập trước, một SSL VPN hỗ trợ FPA cho phép một chức năng bảo mật khác đối với người dùng thường quên đăng xuất – nó cần người dùng nhập chứng thực của mình theo chu kỳ tùy thuộc vào mức độ hoạt động. Sau một thời gian xác định, người dùng sẽ được được yêu cầu chứng thực. Nếu người dùng nhập chứng thực, phiên làm việc sẽ khôi phục lại như lúc bắt đầu yêu cầu, thậm chí là có thể khôi phục khi người dùng đang nhập form dở, nếu người dùng không nhập chứng thực thì phiên làm việc sẽ kết thúc.

Mặc dù đây là một giải pháp không hoàn hảo cho lắm, nhưng FPA vẫn là cách tốt nhất để giải quyết vấn đề người dùng không nhận thực thử truy cập tới một phiên SSL VPN qua thiết bị truy cập không có người sử dụng và bắt đầu phiên làm việc bất hợp pháp trước khi thời gian timeout kết thúc. FPA không tránh được người dùng xấu thử truy cập, tương tự như SSL VPN không có cách nào để phân biệt người dùng không hợp pháp với người dùng trước đó cho tới khi FPA xảy ra. Tuy nhiên, nó giảm thiệt hại bằng cách giới hạn thời gian người dùng không hợp pháp có thể sử dụng phiên.

d) Bỏ qua các hoạt động giả mạo

Để các kỹ thuật timeout hoạt động chính xác trong một môi trường trong đó các máy tính tự động refresh các yêu cầu hoặc lưu lượng khác (các hoạt động này là không thể phân biệt được với hoạt động người dùng), SSL VPN cần phải có một số kỹ thuật trong đó nó biết được xử lý thế nào đối với lưu lượng được tự động tạo ra và bỏ qua các lưu lượng đó khi xác định được thời điểm cuối diễn ra hoạt động người dùng. Điều này có thể thực hiện bằng cách thêm vào cấu hình một chuỗi các danh sách yêu cầu sẽ bị bỏ qua khi kiểm tra yêu cầu người dùng. Trong trường hợp ứng dụng web (tạo ra hầu hết các vấn đề) thì thường khá đơn giản, và bởi vì thường có một giới hạn số các địa chỉ URL trên mỗi ứng dụng nên dễ dàng có thể tạo một danh sách các địa chỉ URL này. Đối với các ứng dụng non-web, việc xác định cấu tạo của các yêu cầu tự động refresh sẽ phức tạp hơn một ít, nhưng hoàn toàn có thể xác định được do các yêu cầu tự động thường khác xa so với các yêu cầu thực sự của người dùng.

e) Các ngưỡng Timeout

Như đã mô tả ở trên, điều quan trọng là các nhà quản trị SSL VPN cấu hình SSL VPN của họ như thế nào để có thể tận dụng được các cảnh báo, timeout, hoặc nhận thực lại. Một vài SSL VPN có giá trị mặc định cho các ngưỡng này, một vài SSL VPN thì lại không có, thậm chí một vài sản phẩm ban đầu còn không bật hệ thống timeout. Trong bất

kỳ trường hợp nào thì cấu hình của hệ thống timeout cũng cần phải được thiết lập lại cho phù hợp với chính sách công ty.

3.3.2 Vấn đề virus xâm nhập vào hệ thống mạng công ty qua SSL VPN

3.3.2.1. Vấn đề

Một vấn đề nữa là việc cho phép các truy cập từ xa từ các máy có thể dẫn tới việc các virus được truyền qua từ một máy tính tới mạng công ty. Khả năng tải lên các file tới các hệ thống file từ bất kỳ máy tính nào cũng làm tăng lên đáng kể khả năng file đó chứa một virus, và virus này sẽ nằm trong một máy tính của mạng công ty. Vấn đề này lại càng nghiêm trọng hơn trong trường hợp SSL VPN cho phép các truy cập từ xa tới e-mail, các hệ thống quản lý liên quan đến khách hàng CRM (Customer Relationship Management), và nhiều hệ thống khác, do các hệ thống này cho phép người dùng đính kèm các file vào bản tin hoặc cơ sở dữ liệu, hoặc có thể cho phép tải các file vào cơ sở dữ liệu công ty.

3.3.2.2. Giải pháp

Có nhiều giải pháp để giải quyết vấn đề virus qua SSL VPN. Nhưng có ba phương pháp thường dùng là:

- Kiểm tra việc sử dụng công nghệ chống virus trên máy trạm
- Chặn việc tải lên
- Thực hiện một hệ thống chống virus trên mạng nội bộ

a) Kiểm tra phần mềm chống virus trên thiết bị người dùng

Một phương pháp thông thường để tránh vấn để virus xâm nhập mạng công ty qua SSL VPN là máy chủ SSL VPN kiểm tra thiết bị người dùng xem tình trạng của phần mềm chống virus như thế nào trước khi cho phép truy cập một vài hoặc tất cả chức năng của SSL VPN. Quá trình kiểm tra có thể thực hiện để xác nhận rằng phần mềm chống virus được cài đặt, chạy, sử dụng dữ liệu cập nhật hay không,… Nếu các máy tính này đạt được các chuẩn mà công ty cho phép thì được phép truy cập, nếu toàn bộ hệ thống không đạt được các chuẩn thì có thể chỉ được truy cập tới một phần con của hệ thống qua SSL VPN, hoặc cấm tất cả các truy cập. Nếu một người dùng bị cấm, SSL VPN có thể mô tả lý do tại sao cấm truy cập trong đó nói rõ các phần mềm cần thiết (hoặc các bản cập nhật cần thiết) mà máy trạm phải cài đặt để có thể có quyền truy cập.

b) Cấm tải lên

Một phương pháp nữa được sử dụng để tránh các virus xâm nhập mạng công ty qua kết nối SSL VPN là cấm người dùng tải các file tới các mạng nội bộ từ các máy tính từ xa. Kiểu cấm này có thể là cấm hoàn toàn hoặc cấm trong phạm vi rộng và nó có thể được nới lỏng ra nếu máy tính người dùng sử dụng chương trình chống virus thích hợp.

c) Thực hiện chống virus trên mạng nội bộ

Phương pháp thứ ba được sử dụng để tránh virus xâm nhập vào mạng công ty qua kết nối SSL VPN là thực hiện các công nghệ chống virus trên mạng LAN của công ty. Việc chống virus này được thực hiện ở biên của SSL VPN.

Các file được tải lên từ một cửa sổ truy cập file SSL VPN cần phải được quét trên các máy chủ file trước khi chúng được thêm vào. Các file đính kèm vào các bản tin e-mail gửi từ một phiên SSL VPN cần phải thực hiện quét virus trên máy chủ e-mail.

Mặc dù phương pháp này về lý thuyết là có thể chống được tất cả các loại virus, nhưng nó nhiều nhược điểm. Các virus trong e-mail có thể được đính kèm dưới dạng mã hóa (để tránh bị các phần mềm chống virus của công ty phát hiện) hoặc có thể được gửi vào một máy chủ nội bộ và chạy trước khi hệ thống chống virus nội bộ có thể xác định và xóa chúng. Tuy nhiên, nhìn chung, đây là phương pháp tốt để tránh virus tấn công vào mạng nội bộ.

3.2.4 Vấn đề sâu xâm nhập vào mạng công ty qua SSL VPN và giải pháp

3.2.4.1. Vấn đề

Các virus và sâu thường bị nhầm lẫn với nhau, nhưng chúng không đồng nhất với nhau. Virus là các mã độc hại mà chúng có thể đính kèm bản thân nó vào một vài đoạn mã khác (host code) và được kích hoạt khi các đoạn mã này (host code) được chạy. Trong khi sâu là các chương trình độc lập mà không tìm cách để đính kèm nó vào các chương trình khác, thay vào đó, chúng tự nhân bản qua các kết nối mạng.

Do đó, vấn đề các loại sâu xâm nhập vào các mạng công ty qua kết nối SSL VPN khác với virus. Các hệ thống chống virus có thể chặn được một số loại sâu, nhưng do sâu không cần phải có hoạt động của con người để kích hoạt nó, và do chúng được kích hoạt nhanh hơn virus, do đó chúng gây ra nhiều nguy hiểm hơn đối với SSL VPN.

Một sâu nằm trên một máy tính được sử dụng để kết nối SSL VPN có thể có khả năng lợi dụng kết nối SSL VPN để tấn công vào mạng nội bộ của công ty. Bởi vì sâu không cần kích hoạt bởi con người. một thiết bị có thể bị nhiễm trong khi kết nối một phiên SSL VPN và qua đó lan nhiễm tới nhiều máy tính trên mạng nội bộ. Điều này có thể xảy ra trước khi các phần mềm chống virus có thể xác định ra chúng.

3.2.4.2. Giải pháp

Cài đặt một chính sách trong đó không cho phép truy cập từ các máy tính không an toàn có thể làm nhẹ bớt tác hại của sâu, nhưng việc thực hiện các luật này có thể làm giảm đi các chức năng của SSL VPN và làm giảm giá trị của SSL VPN. Hơn nữa, nó có thể tránh được truy cập của người dùng từ các máy tính không an toàn, nhưng lại không tránh

được các sâu từ các kết nối SSL VPN mức mạng. Điều này sẽ được mô tả chi tiết ở phần sau trong chương này.

Thêm nữa, có hai công nghệ cho phép chống sự xâm nhập của sâu là tường lửa cá nhân và tường lửa ứng dụng. Mặc dù hai công nghệ này có tên khá giống nhau nhưng chúng thực sự khác nhau.

Tường lửa cá nhân

Các gói phần mềm hoặc thiết bị này nằm trước các máy chủ (máy chủ này phục vụ nội dung cho các người dùng Internet). Chúng có các khả năng của reverse proxy, nhưng chúng chỉ phục vụ các hoạt động được chấp nhận. Có nhiều công nghệ được sử dụng trong tường lửa các nhân và sẽ là rất hữu ích khi nghiên cứu về bảo mật SSL VPN khi tìm hiểu kỹ các công nghệ này.

Bộ lọc dựa trên logic phủ định các yêu cầu người dùng

Bộ lọc logic phủ định làm việc tương tự như các bộ máy chống virus. Nó so sánh các yêu cầu đầu vào với dấu hiệu của các cuộc tấn công đã biết, bất kỳ yêu cầu mà trùng khớp với các dấu hiệu tấn công đã biết sẽ bị chặn khi kết nối với các máy chủ. Mặc dù bộ lọc dựa trên logic phủ định thực sự có hiệu quả trong việc tránh các cuộc tấn công đã biết, nó lại không cần thiết đối với bản thân SSL VPN, hay nó không mạnh khi đối đầu với các cuộc tấn công mới mà không có dấu hiệu trong cơ sở dữ liệu. Từ khi các cuộc tấn công zero day (tấn công vào các vùng không có bảo vệ, hoặc không được cập nhật) ngày càng tăng thì nhược điểm này ngày càng trở nên trầm trọng. Logic phủ định cần các hoạt động bảo trì thường xuyên, do các dấu hiệu cần phải được cập nhật liên tục.

Bộ lọc dựa trên logic khẳng định

Bộ lọc dựa trên logic khẳng định lại hoạt động theo cách khác. Tất cả các yêu cầu được so sánh với dấu hiệu của các yêu cầu an toàn sẽ được xử lý, điều đó có nghĩa là các loại giao tiếp được hỗ trợ tới các máy chủ được bảo vệ. Bất kỳ yêu cầu nào không phù hợp với các dấu hiệu đó sẽ bị chặn lại. Bộ lọc logic khẳng định cần cần nhiều công sức hơn bộ lọc logic phủ định (như các bộ lọc này cần phải được bật để nhận diện các yêu cầu phù hợp) nhưng cần ít bảo trì hơn các hệ thống phủ định, như không cần phải thường xuyên cập nhật. Hơn nữa, bộ lọc logic khẳng định có thể bảo vệ hệ thống khỏi các cuộc tấn công zero-day và các loại sâu mới, các cuộc tấn công không thể sử dụng các yêu cầu hợp pháp và do đó không thể vượt qua bộ lọc này.

Bộ lọc dựa trên các luật động

Công nghệ lọc động bao gồm quét động lưu lượng web đi ra, và thiết lập các chính sách thời gian thực, các chính sách này tương ứng với yêu cầu người dùng hiện tại. Trả lời yêu cầu người dùng sau đó thực hiện như bộ lọc logic khẳng định để chắc chắn chúng thỏa

mãn là một trả lời mong đợi. Thỉnh thoảng luật cho các trang web tĩnh được thiết lập trước (để tăng hiệu quả hệ thống). Mặc dù về lý thuyết nó là tối ưu nhưng bộ lọc động lại thất bại khi đối phó với nhiều vấn đề quan trọng và điều này làm cho nó không được ứng dụng thực tế. Một ví dụ, quá trình xử lý cần phân tích các trang web và chỉ ra các trả lời phù hợp có thể dẫn tới việc giảm hoạt động hệ thống. Hơn nữa, sẽ là rất khó để thành công tạo ra một tập hợp các luật đối với các ứng dụng biến đổi liên tục như ngày nay, và các luật này chỉ có thể chặn khoảng 99% các hoạt động có hại hoặc cho phép đạt được mức an toàn tương đối.

Kết hợp các phương thức

Sự kết hợp các phương thức kể trên có thể được sử dụng để kết hợp các ưu điểm và giảm nhược điểm của từng phương thức độc lập. Ví dụ, một bộ lọc có thể tận dụng các luật dựa trên logic khẳng định nhưng cho phép các luật đó bao gồm nhiều luật được thiết lập động trong suốt các phiên người dùng dựa trên cái gì đang được truy cập và ai đang yêu cầu truy cập. Tương tự, logic khẳng định có thể được sử dụng kết hợp với các luật logic phủ định. Trong SSL VPN, các ứng dụng tường lửa có thể đặt ở trên máy chủ SSL VPN hoặc đặt trên một proxy trước SSL VPN. Trong cả hai trường hợp, các tường lửa ứng dụng kiểm tra yêu cầu người dùng và trước khi chuyển tiếp dữ liệu tới quá trình xử lý SSL VPN, nó kiểm tra an ninh dữ liệu một cách nghiêm ngặt.

3.2.5 Vấn đề của các vùng không an toàn

Nhiều vấn đề khác liên quan đến truy cập từ các vùng không an toàn. Một vài chúng là vấn đề chung, trong khi cũng có một vài vấn đề chỉ SSL VPN mới có.

a) Phần mềm gián điệp

Phần mềm gián điệp là các phần mềm được cài đặt mà người dùng không được biết để theo dõi hoạt động của người dùng trên máy tính bị nhiễm. Thông tin mà phần mềm gián điệp thu thập được có thể được sử dụng cho các hoạt động phạm pháp như chiếm dụng số thẻ tín dụng và sử dụng nó để trả tiền, hoặc các mục đích khác như mua hàng trực tuyến và sử dụng chúng để quảng cáo hay nhiều mục đích thương mại khác. Trong bất kỳ trường hợp nào, điều quan trọng là ta phải để người dùng truy cập các hệ thống nhạy cảm mà các hoạt động của họ không bị theo dõi. Một vài SSL VPN có thể kiểm tra phần mềm gián điệp trên thiết bị truy nhập và một vài phần mềm chống virus có thể phát hiện phần mềm gián điệp . Tuy nhiên, việc kiểm tra các phần mềm gián điệp thường dựa trên dấu hiệu của các phần mềm gián điệp đã biết và một vài phương thức khác, và nó có nhiều yếu điểm. Do đó, tốt hơn là ta nên đưa ra các cảnh khi truy cập từ các máy tính có dấu hiệu bị nhiễm các phần mềm gián điệp.

b) Thiết bị ghi lại thao tác bàn phím

Một cách bọn xấu có thể thực hiện để lấy thông tin nhạy cảm từ người dùng là tận dụng các thiết ghi lại thao tác bàn phím trên các máy tính mà nạn nhân sử dụng. Có hai kiểu thiết bị ghi lại thao tác bàn phím được sử dụng ngày nay là phần cứng và phần mềm.

Phần cứng ghi lại thao tác bàn phím

Phần cứng ghi lại thao tác bàn phím là các thiết bị nhỏ được cắm vào một cổng bàn phím của máy tính (hoặc cổng USB nếu một bàn phím USB được sử dụng). Thiết bị đó thường giống như một dây cắm nhỏ hoặc một cáp mở rộng, lưu lại tất cả các thao tác bàn phím được gõ vào bộ nhớ đệm. Do đó, người cài đặt nó có thể lấy lại nó, tải các bản ghi tới máy tính, reset lại nó và cài đặt cho lần theo dõi tiếp theo.

Phương thức đơn giản nhất để chống lại phần cứng ghi lại thao tác bàn phím là kiểm tra máy tính xem thiết bị ghi lại có cài đặt trên nó không. Điều này là có thể khi ai đó cài đặt phần cứng này trên máy tính cá nhân, tuy nhiên điều này là không thích hợp khi người cài đặt nó làm việc ở các tiệm cafe internet hoặc tương tự như thế. Tất nhiên, nếu thông tin cá nhân bị lộ thì dẫn tới vấn đề cực kỳ nghiêm trọng.

Trong bất kỳ trường hợp nào, vấn đề của các phần cứng ghi lại bàn phím thường xảy ra trên các phiên truy nhập từ xa từ các vị trí công cộng. Là vấn đề chung của SSL VPN, IPSec VPN hoặc các công nghệ khác được sử dụng.

Phần mềm ghi lại thao tác bàn phím

Phần mềm ghi lại thao tác bàn phím là một kiểu của phần mềm gián điệp, chúng là các phần mềm ghi lạ các thao tác người dùng và tự động gửi thông tin đến người cài đặt. Giải pháp cho phần mềm này cũng tương tự như đối với phần mềm gián điệp.

c) Shoulder Surfing

Đây là một kiểu lừa đảo giống như xem thông tin bí mật từ phía sau của người sử dụng. Bọn xấu thường lợi dụng các địa điểm công cộng để có thể biết được các thông tin nhạy cảm.

d) Các máy quay phim đặt ở các máy tính

Các vụ lừa đảo shoulder surfing ngày càng tăng, giá thành các thiết bị giám sát và bảo mật cũng trở nên rẻ đi rất nhiều. Các máy quay phim có thể ghi lại các hành động của bất kỳ ai làm việc trong sân bay, hành lang khách sạn, hoặc thậm chí là cổng ra của công viên. Do đó, bất kỳ loại công nghệ truy cập từ xa nào được sử dụng (IPSec, SSL) thì nội dung của màn hình được sử dụng cần phải được bảo vệ khỏi bất kỳ thiết bị theo dõi nào. Thiết bị giám sát thỉnh thoảng được che giấu đi, thông tin cực kỳ nhạy cảm sẽ không được truy cập ở các địa điểm mà ở đó có lắp đặt các thiết bị như trên – thậm chí nếu người dùng

không thực sự phát hiện ra các thiết bị này. Như đã giới thiệu ở trên, dữ liệu cụ thể được truy cập sẽ phải phụ thuộc vào cấp độ cho phép của vấn đề an ninh.

e) Phát xạ điện từ

Một số người sử dụng các thông tin nhạy cảm một cách thông thường cũng dẫn tới một vấn đề đáng đề cập là phát xạ điện từ. Khi các thiết bị điện được sử dụng, chúng tạo ra các sóng điện từ phát xạ. Các chuẩn của các quốc gia là khác nhau (theo đó mức độ phát xạ được chấp nhận), nhưng bởi vì có thể mức độ phát xạ này là an toàn đối với con người, nhưng điều đó không có nghĩa là an toàn đối với dữ liệu. Nói tóm lại, bằng cách sử dụng các thiết bị đặc biệt, một người có thể chặn các phát xạ từ thiết bị máy tính và ghi lại các thông tin đang truyền trên hệ thống.

Có nhiều công nghệ có thể cô lập thiết bị máy tính khỏi các thiết bị nghe trộm kiểu này (ở Mỹ, các thiết bị cô lập cần phải đạt các tiêu chuẩn TEMPEST), nhưng các trạm Internet công cộng và các máy tính mượn thường không được bảo vệ theo cách này. Cũng như các máy tính xách tay của công ty khi sử dụng ở các điểm công cộng cũng không được bảo vệ theo cách này. Do đó, một người có thể sử dụng các công cụ đặc biệt để theo dõi máy tính người dùng mà không cần dùng kiểu shoulder surfing hoặc sử dụng máy quay phim. Vì vậy, các bí mật quân sự hoặc các thông tin cực kỳ nhạy cảm mà các tổ chức xấu muốn trộm không thể được truy cập từ các máy tính mà không được xem là an toàn ở các điểm mà một người khác có thể theo dõi thiết bị.

3.2.6 Các hacker kết nối tới mạng công ty

Một vấn đề nữa của truy cập SSL VPN là các tổ chức không nhận thực có thể truy cập tới một mạng công ty bằng cách kết nối cầu (bridging) tới mạng công ty qua máy tính người dùng SSL VPN. Một người dùng máy tính thường được kết nối tới một mạng nội bộ. Đồng thời, khi người dùng đang truy cập một phiên SSL VPN, máy tính có thể được kết nối tới một mạng công ty từ xa khác. Do đó, máy tính có thể đồng thời được kết nối tới hai mạng. Vì vậy có thể có trường hợp một người sử dụng một mạng (trong trường hợp của đồ án là mạng cục bộ LAN) để kết nối tới mạng công ty qua máy tính người sử dụng.

Cũng có một vấn đề bảo mật khác đối với mạng cục bộ hệ thống trên mạng máy chủ SSL VPN có thể kết nối tới mạng cục bộ qua đường hầm SSL VPN. Đây không phải là một vấn đề đối với tập đoàn cung cấp truy nhập SSL VPN, nhưng có thể phải chịu trách nhiệm pháp lý nếu SSL VPN bị lợi dụng kiểu này. Hơn nữa, vấn đề này có thể khiến các tổ chức cấm người dùng thiết lập kết nối SSL VPN tới các thiết bị của họ trừ khi các thiết bị không cho phép kết nối mức mạng. Điều này tương tự như trong công nghệ IPSec hiện tại.

3.2.7 Vấn đề rò rỉ thông tin mạng nội bộ và giải pháp

3.2.7.1. Vấn đề

Hacker chuẩn bị tấn công một mạng thường xem xét tài nguyên của mạng đó để xác định kiểu kỹ thuật tấn công nào đạt hiệu quả nhất. Sự hiểu biết về tên các máy, cấu trúc thư mục, địa chỉ IP,… của mạng nội bộ có thể hỗ trợ rất nhiều trong việc vượt qua hệ thống an ninh của mạng nội bộ.

Thật không may mắn là SSL VPN thường có lỗi trong việc cung cấp các thông tin như vậy tới các tổ chức bên ngoài. Như đã mô tả ở chương 2, một chức năng của SSL VPN là chuyển đổi thông tin nội bộ tới các định dạng dữ liệu mà bên ngoài có thể truy cập được. Sự chuyển đổi này thường khiến các thông tin nội bộ tránh được các tổ chức bên ngoài nhưng tham số (bao gồm các thông tin nội bộ) có thể được đọc bởi bất kỳ ai đang xem phiên SSL VPN. Điều này là đúng đối với các thành viên, các khách hàng hoặc khách hàng tương lai của công ty đang sử dụng SSL VPN.

3.2.7.2. Giải pháp

Giải pháp cho vấn đề này thực sự đơn giản, SSL VPN không cho phép các thông tin nội bộ được biểu diễn dưới dạng văn bản thông thường đối với các nhóm từ xa. Thông tin này được biểu diễn trong URL dưới dạng mã hóa, như tham số mã hóa hoặc lưu trữ trên máy chủ SSL VPN được mã hóa dưới dạng số thêm vào địa chỉ URL gửi tới người dùng. Một số giải pháp khác có thể được sử dụng để đạt được mục đích ẩn kiến trúc thông tin nội bộ khỏi người dùng bên ngoài.

3.2.7.3. In ấn và fax

Người dùng có thể sử dụng SSL VPN để in ấn trên các máy in cục bộ (ví dụ các máy in đặt tại nơi họ đang làm việc) hoặc có thể muốn in trên các máy in đặt trên văn phòng của họ (cục bộ tới SSL VPN). Các vấn đề bảo mật của kiểu này là:

Máy in cục bộ với người dùng

Có hai vấn đề đối với người dùng in trên máy in cục bộ là:

1. Nếu máy in chia sẻ được sử dụng, có thể một người dùng khác sẽ xem được bản in (thậm chí nhận bản in) trước người dùng. Thông tin nhạy cảm có thể bị các nhóm không nhận thực xem như kiểu này, và nếu các nhóm khác đọc các thông tin này mà không thực sự trộm chúng, người dùng có thể không bao giờ biết các thông tin này bị đưa ra ngoài.
2. Các hệ điều hành ngày nay nhóm (spool) dữ liệu trước khi gửi chúng tới các máy in – chúng lưu trữ một ảnh, ảnh này được in vào trong đĩa và sau đó chuyển đến máy in hơn là có các ứng dụng giao tiếp trực tiếp với máy in. Mặc dù quá trình nhóm dữ liệu làm cho hiệu quả in ấn cao hơn (các máy in có thể dễ dàng chia sẻ) và dễ sử dụng hơn (người dùng có thể trở lại làm việc trước khi quá trình in ấn xảy ra), nhưng điều này sẽ dẫn tới một số vấn đề bảo mật. Với SSL VPN vấn đề là thông tin nhạy cảm được in ra, nó được gói trong một ảnh

được lưu trữ trên máy tính không thuộc quyền quản lý của công ty. Người dùng có thể không biết được ai đã truy cập tới các ảnh này và nó được lưu trữ ở đâu. Do đó, thỉnh thoảng tốt hơn hết là tắt chức năng nhóm khi in các thông tin nhạy cảm qua SSL VPN.

Các máy in đặt cục bộ đối với máy chủ SSL VPN

Rõ ràng rằng, nhóm (spooling) không tạo ra vấn đề nào khi một người sử dụng một SSL VPN từ bên trong nội bộ văn phòng. (Nếu nhóm trong văn phòng không được bảo đảm, thì có một vấn đề nghiêm trọng đối với tất cả người sử dụng, không chỉ là người sử dụng SSL VPN). Tuy nhiên, vấn đề in ấn trong văn phòng khi người dùng thực sự ở xa là một vấn đề nghiêm trọng. Người dùng thực hiện in ấn không thể biết được ai đang đứng gần máy in và đơn giản cũng không biết ai đang ở bên trong văn phòng nhận được bản in này. Do đó, mặc dù chắc chắn phải sử dụng nhiều lần in ấn từ xa, nhưng người sử dụng phải cẩn thận khi thực hiện các tác vụ này.

3.2.7.4. Xóa file

Một vấn đề khác trong đó các chức năng hệ điều hành có thể dẫn tới vấn đề bảo mật của một phiên SSL VPN là xóa dữ liệu.

Trong nhiều trường hợp, các file mà người dùng kích hoạt sao chép từ các ổ đĩa từ xa (hoặc các nơi khác) tới một máy cục bộ sẽ không bị xóa khi người dùng kết thúc phiên SSL VPN và do đó người dùng cần phải chắc chắn xóa các file này.

Như đã mô tả ở trên, các hệ điều hành ngày nay thường không xóa dữ liệu khi người dùng xóa chúng. Thay vào đó, hệ điều hành thường sử dụng các thư mục đặc biệt để giữ dữ liệu cho tới khi cần không gian phải lưu trữ dữ liệu mới. Thậm chí khi các file bị ghi đè thì cũng không xóa hoàn toàn file. Để xóa file hoàn toàn thì người dùng phải thực sự xóa không gian đĩa này nhiều lần. Thường thì không dễ làm được điều này, nhưng mức độ của vấn đề này thường không quan trọng. Vấn đề lớn hơn đối với người dùng thông thường là bọn xấu có thể vào các thư mục rác để có thể thử phục hồi dữ liệu sử dụng các phần cứng đặc biệt.

3.2.8 Đầu cuối tin cậy

SSL VPN cho phép các công ty có khả năng cấu hình một số máy tính để chắc chắn chúng tin vậy, người dùng có thể sử dụng các thiết bị này để truy cập nhiều tài nguyên hơn so với các thiết bị thông thường. Các thiết bị tin cậy thường là các máy tính của công ty hoặc được quản lý bởi công ty, và thỉnh thoảng được biết như là các thiết bị điều khiển. Khi thiết bị tin cậy được sử dụng, thường thì các kiểm tra bảo mật là không cần thiết, ví dụ các file tạm thời không cần phải xóa trên các máy máy tính xách tay của công ty, các thông tin nhạy cảm (như các văn bản thương mại) được cố tình lưu lại. Ngưỡng thời gian timeout khác nhiều so với khi người dùng sử dụng thiết bị truy cập thông thường.

Các chứng thực thường được sử dụng để nhận diện máy tính là đáng tin cậy. Các nhà quản trị SSL VPN tạo ra các chứng thực đặc biệt cho các máy SSL VPN sẽ tin tưởng và các chứng thực này cài đặt trên các thiết bị tương ứng của người dùng. Mặc dù các chứng thực này thường được cài đặt bởi bản thân các nhà quản trị, SSL VPN cho phép người dùng yêu cầu các chứng thực trực tuyến, và cung cấp quá trình tải xuống và cài đặt tự động các chứng thực này một khi người quản trị mạng chấp nhận yêu cầu người dùng.

Cải tiến khả năng đầu cuối tin cậy bao gồm cả khả năng cho phép quét các thiết bị truy cập để lấy thông tin chứng thực máy trạm, chứng thực này được dùng để xác định mức độ tin cậy – ví dụ, xác định sự có mặt của một USB đặc biệt với nội dung cụ thể, một phần mềm cụ thể với cấu hình đặc biệt, hoặc một tổ hợp khóa registry được cấu hình với giá trị cụ thể. Mỗi một lần quét có thể được thực hiện thay thế hoặc kết hợp với việc kiểm tra chứng thực máy trạm. Tất nhiên, các mức độ tin cậy khác nhau sẽ có các chính sách khác nhau.

3.2.9 Phân cấp truy cập dựa trên tình trạng điểm cuối

SSL VPN được truy cập từ các máy tính như máy tính xách tay của công ty, máy tính ở nhà, trạm Internet công cộng, các thiết bị cầm tay. Tất cả sự khác nhau của các máy tính dẫn tới các mức bảo mật khác nhau và các mức tin cậy khác nhau, sự truy cập từ các thiết bị này chắc chắn phải không giống nhau. Ví dụ, không nên cho phép tải lên file từ một máy có dấu hiệu nhiễm virus, nhưng cho phép tải lên từ các máy an toàn như máy tính xách tay của công ty mà có phần mềm diệt virus cài đặt. Vậy thì mức truy cập nào mà SSL VPN cần phải cung cấp từ các thiết bị khác nhau?

Rõ ràng rằng không nên thực hiện phương pháp giới hạn với truy cập SSL VPN, mà thay vào đó là xác định mức bảo mật của thiết bị truy cập và tạo ra một phiên truy cập cụ thể với chính sách phù hợp. Mức độ truy cập tối đa có thể được từ một thiết bị cụ thể nào đó, người dùng thiết bị này có thể truy cập tối đa tới mạng công ty.

Các chính sách bảo mật công ty điều chỉnh thiết bị truy cập thường dựa trên tình trạng thiết bị để cho phép người dùng thực hiện các chức năng cụ thể. Trong ví dụ trước, một chính sách cho phép quá trình tải lên chỉ có thể thực hiện từ các thiết bị có chạy các phần mềm diệt virus. SSL VPN cũng có thể được thiết lập để thực hiện hoàn toàn các chính sách này và chặn truy cập từ các ứng dụng hoặc một phần ứng dụng cụ thể nếu không thỏa mãn các chính sách bảo mật.

Mức độ truy cập cho phép đối với một phiên làm việc cụ thể thường được xác định khi người dùng đăng nhập. Một applet nhỏ gửi tới thiết bị truy cập để thực hiện nó, xác định xem làm thể nào thiết bị thỏa mãn các tiêu chuẩn khác nhau được thiết lập bởi các nhà quản trị SSL VPN dựa trên các chính sách bảo mật của công ty. Nó cũng thử cài các mã liên quan đến bảo mật khác nhau vào các thiết bị truy cập và gửi báo cáo về máy chủ SSL VPN nếu thành công. Dựa trên việc thực hiện các applet, mức độ bảo mật của thiết bị

được thiết lập và mức độ truy cập cũng phụ thuộc vào đó. Cách khác là tận dụng các phần mềm đặt trước trên thiết bị truy cập để thực hiện kiểm tra. Quá trình kiểm tra môi trường bảo mật trên thiết bị truy cập gọi là kiểm tra host hoặc kiểm tra thiết bị truy cập.

Một điều quan trọng là điều khiển truy cập không chỉ có thể giới hạn toàn bộ ứng dụng mà có thể giới hạn chức năng trong một ứng dụng. Bảng 3.1 biểu diễn các chính sách đối với truy cập e-mail từ các thiết bị với các tình trạng bảo mật khác nhau.

Các thành phần ảnh hưởng lên mức độ truy cập của một người sử dụng bao gồm:

- **Phần mềm diệt virus**: Nó đang chạy? Phần mềm diệt virus nào đang được sử dụng? Phiên bản của nó? Ngày cập nhật của nó?
- **Tường lửa cá nhân:** Nó đang chạy? Tường lửa cá nhân nào đang được sử dụng? Phiên bản của nó? Chính sách nào đang có tác dụng?
- **Kỹ thuật nhận thực:** Một người dùng được hỗ trợ một tên đăng nhập và mật khẩu có thể được truy cập tài nguyên ít hơn một người dùng có một mật khẩu dùng một lần hoặc thẻ USB cắm vào máy tính để nhận thực,…
- **Hệ điều hành:** Hệ điều hành nào mà người sử dụng máy tính đang sử dụng?
- **Khóa Registry:** Các tổ hợp giá trị khóa cụ thể nào?
- **Các chứng thực máy trạm:** Một vài địa chỉ IP có thể được tin cậy (nếu như chúng ở trong mạng nội bộ).
- **Nhà cung cấp dịch vụ:** Có phải người dùng sử dụng dịch vụ của một nhà cung cấp cho phép các chức năng bảo mật khác nhau trong khi kết nối?

Bảng 3.1. Chính sách đối với các máy có độ tin cậy khác nhau

Tình trạng của thiết bị truy cập			**Điều khiển truy cập**			
Máy tin cậy	**Đã cài đặt phần mềm chống virus**	**Có khả năng xóa các file tạm thời**	**Cho phép người dùng đọc e-mail (văn bản)**	**Cho phép người dùng gửi e-mail (văn bản)**	**Cho phép người dùng mở file đính kèm**	**Cho phép người dùng gửi file đính kèm**
Không	Có	Có	Có	Có	Có	Có
Không	Có	Không	Có	Có	Không	Có
Không	Không	Có	Có	Có	Có	Không
Không	Không	Không	Có	Có	Không	Không
Có-Tin cậy mức 2	Có	Có/Không	Có	Có	Có	Có
Có-Tin cậy mức 2	Không	Có/Không	Có	Có	Có	Không
Có-Tin cậy mức 1	Có/Không	Có/Không	Có	Có	Có	Có

- **Các gói phần mềm chống phần mềm gián điệp:** Chúng đang chạy? Gói nào?

- **Các file tạm thời:** Các file tạm thời của SSL VPN thường được xóa trên máy tính này?

Nhà cung cấp dịch vụ điều khiển

Vì cả lý do bảo mật lẫn kinh tế, các công ty thường yêu cầu người dùng thực hiện tất cả các kết nối từ xa qua các nhà cung cấp viễn thông cụ thể. Các nhà cung cấp này có thể giảm bớt tỉ lệ kết nối đối với số người dùng lớn, hoặc cho phép thực hiện bắt buộc các chính sách cụ thể (như lọc các từ xấu hoặc chặn kết nối chia sẻ file ngang hàng). Một vài kỹ thuật SSL VPN có thể xác định thuộc tính kết nối người dùng, địa chỉ IP người dùng và các thông tin định tuyến và chặn các người dùng không sử dụng nhà cung cấp dịch vụ cần thiết khi truy cập tài nguyên công ty qua SSL VPN.

3.3 Vấn đề bảo mật phía máy chủ

Như vậy là ta đã biết các vấn đề bảo mật bên phía máy trạm, đồ án sẽ tiếp tục mô tả các vấn đề bảo mật phía máy chủ khi thực hiện SSL VPN. Bảo mật phía máy chủ bao gồm các vấn đề liên quan đến bảo vệ mạng nội bộ khỏi các hành động có hại bởi sự có mặt của SSL VPN và các kết nối của nó, và bảo vệ bản thân máy chủ SSL VPN.

3.3.1 Vấn đề tường lửa và các công nghệ bảo mật khác bị tấn công và giải pháp

3.3.1.1. Vấn đề

Đối với người dùng để giao tiếp với SSL VPN và đối với SSL VPN có thể chuyển tiếp các yêu cầu tới các hệ thống nội bộ, việc giao tiếp cần phải sử dụng giao thức TCP/IP (và có thể là UDP/IP và ICMP). Các tường lửa (chặn các cổng giao tiếp) cần phải được cấu hình để bảo vệ bởi SSL VPN, nhưng lại tạo ra các vấn đề bảo mật. Đồ án sẽ sử dụng hai tình huống thường xảy ra để mô tả kỹ hơn vấn đề này.

Trong một công ty có ý thức bảo mật, máy chủ SSL VPN sẽ không đặt ngoài tầm bảo vệ của tường lửa, nó sẽ được đặt trong một DMZ hoặc một mạng nội bộ.

a) SSL VPN trong một DMZ

Nếu SSL VPN được đặt trong một DMZ, tường lửa bên ngoài cho phép cổng 443 (và thường cũng là cổng 80) mở lưu lượng bên ngoài (bao gồm cả yêu cầu người dùng tới SSL VPN). Điều này bản thân nó không phải là một vấn đề bảo mật nghiêm trọng, tuy nhiên, trong trường hợp SSL VPN, đây là một vấn đề thực sự. Hình 3.1 mô tả một SSL VPN đặt trong một DMZ. Kiến trúc này sẽ tạo ra một số vấn đề bảo mật.

Bởi vì các đường hầm SSL VPN thực hiện các giao thức khác nhau qua các tường lửa bên ngoài và xây dựng lại chúng trong SSL VPN:

Hình 3.1. SSL VPN trong DMZ

- **Các khóa mã hóa SSL được lưu giữ trong một môi trường không an toàn (DMZ):** Nếu các khóa SSL bị tấn công, kẻ tấn công có thể giả dạng công ty. Kẻ tấn công có thể tận dụng các trò lừa đảo để trộm các thông tin nhạy cảm từ người dùng. Vì vậy tốt hơn hết là không nên đưa các khóa này vào vùng không an toàn hoặc nửa tin cậy.
- **Mã hóa được thực hiện trong một vùng không an toàn:** Việc truyền các thông tin nhạy cảm dưới dạng văn bản thông thường qua vùng mạng DMZ không an toàn có thể là mục tiêu cho các chương trình bắt gói tin. Do đó, trong kiến trúc trên, SSL VPN không cho phép mã hóa thực sự đầu cuối - đầu cuối, mà nó thực hiện mã hóa đầu cuối – một nửa đầu cuối (end-to-middle). Do đó nội dung của phiên SSL VPN được giải mã trong một vùng không an toàn bên ngoài mạng đích.
- **Các tường lửa bên ngoài bị gây hại bởi SSL VPN:** Nếu một người dùng từ xa được cho phép thiết lập kết nối mạng qua SSL, và sau đó người dùng cơ bản có thể truyền các giao thức yêu cầu trong các gói mạng (các gói này được truyền đường hầm trong giao thức HTTPS tới SSL VPN). Điều này có nghĩa là các giao thức bị chặn bởi các tường lửa bên ngoài có thể được thực

hiện qua đường hầm hóa trong HTTPS tới DMZ. Khi các nhà quản trị cấu hình các tường lửa bên ngoài để chặn các cổng cụ thể, cũng có nghĩa là không cho phép một dịch vụ cụ thể nào đó từ Internet, và cũng có nghĩa là họ muốn dịch vụ này phải bị chặn.

- **Các cổng cần phải được mở trong tường lửa bên trong:** Điều này tạo ra kết nối không cân bằng giữa DMZ và mạng nội bộ. Việc mở các cổng ảnh hưởng đến hiệu quả của tường lửa bên trong, làm lu mờ khoảng cách môi trường DMZ và Internet, và tạo ra các vấn đề bảo mật nghiêm trọng. Thêm nữa, việc mở các cổng này thường làm tổn hại đến các chính sách bảo mật.
- **Các nút từ xa có thể là các cầu nối đến các mạng khác:** Nếu một người dùng từ xa cho phép thiết lập kết nối mạng qua SSL VPN, thì có thể xảy ra trường hợp mạng nội bộ của người dùng có thể kết nối tới mạng nội bộ công ty qua thiết bị truy cập sử dụng kết nối SSL VPN. Đây là một vấn đề lớn ảnh hưởng đến kết cấu mạng.
- **Các nhóm bên ngoài có thể được cho phép trở thành các nút trong mạng công ty:** Hầu hết các công ty quan tâm đến bảo mật ngăn cấm bất kỳ máy tính nào không thuộc công ty trở thành một nút trong mạng của công ty. Nếu một SSL VPN được sử dụng đối với các văn phòng, các khách hàng và các khách hàng tương lai để cho phép truy cập tới tài nguyên công ty và nếu SSL VPN cho phép người dùng từ xa thiết lập kết nối mạng qua SSL VPN, chính sách này có thể không thể thực hiện được.

b) SSL VPN trên mạng nội bộ

Một trường hợp khác là đặt máy chủ SSL VPN trên mạng nội bộ mà không đặt trên DMZ.

Hình 3.2 mô tả một SSL VPN đặt trên một mạng nội bộ, sơ đồ này dẫn tới các vấn đề bảo mật nghiêm trọng, các vấn đề này khác với các vấn đề tạo bởi việc sử dụng mô hình dựa trên DMZ:

- **Toàn bộ kiến trúc tường lửa bị tấn công:** Các giao thức mà tường lửa hỗ trợ để chặn bị đường hầm hóa trong SSL tới mạng nội bộ. Tại thời điểm máy chủ SSL VPN tổ chức lại dịnh dang giao tiếp cho phù hợp, nội dung của phiên giao tiếp đã ở sẵn trong mạng nội bộ - trong khi chúng không thuộc nơi đó!
- **Các nhóm không nhận thực được phép gửi các gói mạng tới mạng nội bộ:** Các gói cần phải được gửi bởi người dùng từ xa tới mạng nội bộ thì người dùng phải được nhận thực. Hacker và sâu không được phép truy cập tới bất kỳ tài nguyên nào của công ty. Việc cho phép chúng truy cập có thể dẫn tới vấn đề tấn công từ chối dịch vụ DoS, map mạng công ty hoặc quét các điểm yếu bảo mật để trộm dữ liệu hoặc điều khiển các máy tính.

- **Bất kỳ hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System) dựa trên mạng ở trên DMZ sẽ không có hiệu quả:** Các IDS làm việc bằng cách quét các gói mạng khi chúng qua một mạng, việc đặt các IDS trên một DMZ là một kỹ thuật tốt để dừng lưu lượng xấu vào mạng công ty. Tuy nhiên, trong trường hợp một SSL VPN trên một mạng nội bộ, tất cả các yêu cầu được mã hóa với SSL VPN – nếu các yêu cầu qua DMZ ở dạng mã hóa thì các IDS sẽ không thể đọc được chúng. Và do đó, IDS sẽ không có tác dụng gì trong mạng.

Hình 3.2. SSL VPN trong mạng nội bộ

3.3.1.2. Giải pháp

Không có giải pháp đơn giản nào cho các vấn đề trên. Tuy nhiên, việc sử dụng các phương pháp dựa trên các công nghệ thích hợp có thể làm giảm nhẹ tác hại của các vấn đề kể trên.

Một máy chủ SSL VPN cần phải chắc chắn rằng nó kết hợp chính xác với các tường lửa bổ sung để tạo thành một kiến trúc mạng công ty. Do các vấn đề kể trên, việc sử dụng SSL như là một kỹ thuật đường hầm cho các kết nối mạng thực sự về cơ bản là còn nhiều việc phải xem xét.

Việc thiết lập một kết nối mạng qua SSL VPN cần phải được hoàn thành đối với các máy mà bạn sẽ cho phép kết nối tới mạng tập đoàn, như các máy tính của công ty. Thậm chí khi bạn cho phép các máy tính an toàn tuy cập tới mạng công ty theo cách này, cần phải biết được rằng các tường lửa cá nhân trên các máy tính này được biến đổi hiệu

quả vào trong tầm kiểm soát của tường lửa trong công ty, đây là một nhiệm vụ nó không được trang bị trước để thực hiện. Vì vậy, việc thiết lập một kết nối mạng qua SSL (đây là một chức năng mạnh của công nghệ SSL VPN) không phải là một ý tưởng tốt đứng trên quan điểm bảo mật.

May mắn thay, việc thiết lập một kết nối mạng qua SSL là không thường xuyên (và thường không được khuyến nghị).

Có thể đạt được truy cập tới các ứng dụng và file mà không cần thiết lập kết nối mức mạng. Việc cho phép truy cập thường an toàn hơn khi đường hầm hóa thông tin mạng và làm giảm nhẹ tác hại các vấn đề kể trên (trừ vấn đề địa chỉ IP nội bộ của một thiết bị đầu cuối).

Hơn nữa, nếu chỉ các lớp trên của mô hình OSI thực sự truyền tới SSL VPN, do đó có thể có các kiến trúc tường lửa thông thường thực hiện bảo mật mức mạng và SSL VPN thực hiện bảo mật lớp ứng dụng. SSL VPN có thể kiểm tra để chắc chắn rằng chỉ các giao thức ứng dụng cụ thể được sử dụng, và do đó chỉ các yêu cầu phù hợp với các giao thức này được phép qua.

Nhiều cách lọc truy cập được thực hiện. Ví dụ như:

- Ai có thể truy cập (ví dụ tên đăng nhập đã nhận thực: JosephSteinberg).
- Ứng dụng nào (ví dụ: Telnet).
- Trên máy chủ nảo (ví dụ: Máy chủ 1).
- Từ các thiết bị nào (ví dụ: Từ các thiết bị tin cậy và các máy tính với các tường lửa cá nhân và các chương trình chống virus).

Một vài tùy chọn tốt để thực hiện lưu trữ các chứng thực SSL trong một vùng không an toàn là:

- Sử dụng một bộ tăng tốc SSL, cho phép các chứng thực SSL được lưu trữ trong vùng an toàn của bộ tăng tốc.
- Sử dụng công nghệ Air Gap (sẽ được mô tả sau), nó cho phép di chuyển chứng thực tới mạng nội bộ được bảo vệ bởi Air Gap.
- Sử dụng công nghệ Air Gap kết hợp với một bộ tăng tốc SSL, làm tăng mức độ bảo vệ chứng thực.

3.3.2 Vấn đề yếu điểm của mức ứng dụng và giải pháp

3.3.2.1. Vấn đề

Các yếu điểm trong phần mềm máy chủ được chú ý nhiều trong một vài năm qua. Các lỗ hổng trong các sản phẩm khác nhau dẫn tới sự tăng nhanh của các sâu, và dẫn tới thiệt hại hàng tỉ đôla.

Hầu hết các SSL VPN tận dụng các máy chủ như là một phần của kiến trúc. Do đó, bất kỳ yếu điểm nào trên máy chủ web (hoặc bất kỳ ở đâu trong phần mềm SSL VPN) có thể dẫn tới các vấn đề bảo mật nghiêm trọng. Kỹ thuật hardening (là quá trình xử lý tối ưu cấu hình hệ thống để bảo mật hơn) một thiết bị SSL VPN có thể giải quyết thích hợp vấn đề này, tuy nhiên, hardening không bao giờ là hoàn hảo, và các thiết bị SSL VPN đã hardening vẫn có nhiều yếu điểm dễ bị tấn công. Hơn nữa, các yếu điểm này có thể ở trong hệ điều hành cơ bản của thiết bị.

Thậm chí nếu bản thân thiết bị SSL VPN vẫn bảo mật thì bởi vì nó gửi các yêu cầu người dùng tới các máy chủ nội bộ, nên các yếu điểm trong hệ thống nội bộ có thể được tận dụng bằng cách tấn công máy chủ SSL VPN, và thậm chí trong trường hợp máy chủ SSL VPN không bị tổn thương thì nó sẽ chuyển tiếp yêu cầu (các cuộc tấn công) tới các máy chủ nội bộ.

3.3.2.2. Giải pháp

Hình 3.3. Bộ lọc lớp ứng dụng

Để tránh SSL VPN trở thành nạn nhân cho các sâu, cần phải thực hiện các bộ lọc lớp ứng dụng. Bộ lọc có thể là sản phẩm của hãng thứ ba trên proxy đặt trước SSL VPN như mô tả trong hình 3.3 (dữ liệu truyền theo thứ tự A,B,C,D,E) hoặc có thể được tích hợp với bản thân máy chủ SSL VPN.

Việc lọc các yêu cầu gửi tới SSL VPN được xem như là một chức năng của máy chủ SSL VPN thực sự hoặc như là một chức năng của một tường lửa lớp ứng dụng (đặt trước SSL VPN) có thể giải quyết các vấn đề yếu điểm của lớp ứng dụng. Các loại khác

nhau của bộ lọc đã được mô tả ở trước và chúng có thể chặn các yêu cầu xấu từ SSL VPN yếu.

3.3.3 Mã hóa

Việc mã hóa được thực hiện khi thông tin bí mật được truyền qua Internet. Trong trường hợp các SSL VPN, SSL là công nghệ được tận dụng để mã hóa tất cả các giao tiếp. Ngày nay, các trình duyệt hầu hết đã hỗ trợ mã hóa 128 bit, có nhiều lý do để hầu hết các công ty đều chuyển sang mã hóa 128 bit được cung cấp bởi SSL. Thông tin chi tiết đã được mô tả trong chương 2.

3.3.4 Cập nhật các máy chủ SSL VPN

Một điểm nữa cần chú ý khi tìm hiểu SSL VPN là không có sản phẩm phần mềm (hoặc phần mềm chạy trên thiết bị) nào là hoàn hảo. Các bug (thường tạo ra các yếu điểm bảo mật) thường có trong các gói phần mềm ngày nay. SSL VPN không tránh khỏi ảnh hưởng bởi các lỗi lập trình, các sản phẩm SSL VPN có thể chứa các bug, các bug này cần phải được sửa bằng các gói cập nhật. Mỗi sản phẩm SSL VPN có một chuỗi các cập nhật theo thứ tự, như một vài sản phẩm cần các cập nhật trước trước khi thực hiện một gói cập nhật nào đó, một vài sản phẩm cho phép công nghệ tường lửa ứng dụng logic – khẳng định bên trong máy chủ SSL VPN làm giảm các yêu cầu cập nhật, một vài sản phẩm tận dụng các sản phẩm hãng thứ ba và cần các cập nhật của hãng thứ ba.

3.3.5 So sánh Linux và Windows

Các máy chủ SSL VPN ngày nay thường chạy trên Microsoft Windows Server hoặc các hệ điều hành máy chủ Linux. Mặc dù Microsoft đã nhận được nhiều lời khen ngợi về tính bảo mật của hệ điều hành và các sản phẩm phần mềm, nhưng Linux cũng phát triển mạnh trong thời gian gần đây và có nhiều lợi thế bảo mật.

3.3.6 Một vài khái niệm bảo mật khác của thiết bị SSL VPN

Các máy chủ SSL VPN thực hiện như là các cổng từ Internet đầy rẫy các kẻ nguy hiểm vào các môi trường được bảo vệ của công ty. Do đó, chúng phải có khả năng bảo vệ khỏi các cuộc tấn công bao gồm các kỹ thuật để chắc chắn bản thân chúng có khả năng phục hồi, củng cố bức tường bảo vệ. Cùng với các công nghệ đồ án đã mô tả ở trên, nhiều khái niệm đang quan tâm liên quan đến bảo mật máy chủ SSL VPN sẽ được mô tả trong các phần sau đây.

a) Hardening

Hardening là quá trình xử lý tối ưu cấu hình của một máy tính hoặc một mạng để chúng an toàn nhất có thể. Nó thường thực hiện tắt các dịch vụ không cần thiết, thay đổi các mặc định hệ điều hành, tắt các khả năng mạng không cần thiết, loại ra các truy cập từ

người dùng khi có người cần điều khiển thiết bị, và xóa các phần mềm không cần thiết. Nhiều SSL VPN được vận chuyển trên các máy tính tiền – hardened, thỉnh thoảng được gọi là các thiết bị (như đã mô tả ở trên). Hardening thường giảm độ nhạy cảm của một SSL VPN đối với các cuộc tấn công, và là một phương thức kinh tế hiện nay. Tuy nhiên, một điểm quan trọng cần nhận thấy là hardening không có khả năng phục hồi, nếu có một sai sót trong mã hệ điều hành, tất cả các thủ tục hardening có thể trở nên vô nghĩa.

b) Air Gap

Air Gap là một công nghệ tận dụng hai máy chủ - một đặt ở biên mạng nội bộ, ở trên tất cả các chứng năng SSL VPN chạy, và một đặt ở biên Internet. Giữa chúng có một bộ nhớ nhỏ. Máy chủ đặt ở biên Internet được hardened và chỉ chạy mã cho phép nhận các kết nối IP. Nó gửi tải ứng dụng từ các gói nó nhận được tới bộ nhớ nhỏ, từ đó máy chủ nội bộ đọc các yêu cầu vào. Air Gap cho phép bảo mật tốt hơn phương thức hardening đơn giản do chúng phục hồi kết nối mạng, giảm các vấn đề mức hệ điều hành, và tránh được các máy đã kết nối Internet thử nhận địa chỉ SSL VPN. Nhược điểm của Air Gap là nó có giá thành cao hơn hardening do nó cần hai máy chủ. Do đó, Air Gap thường phù hợp hơn với mạng lớn, trong đó vấn đề bảo mật được đặt lên hàng đầu.

c) Bảo vệ từ các hệ thống nội bộ và mạng nội bộ

Máy chủ SSL VPN cần phải được bảo vệ khỏi các tấn công từ người dùng nội bộ. Các mật khẩu là cần thiết để truy cập bất kỳ công cụ quản trị nào. Hơn nữa, tốt hơn là có một vài tường lửa cơ bản trên máy chủ SSL VPN để chống các sâu và phần mềm độc hại có thể tấn công từ mạng nội bộ và chặn chúng khỏi tấn công máy chủ SSL VPN.

d) ASIC

Các ASIC (Application – Specific Integrated Circuit – Mạch tích hợp ứng dụng cụ thể) là các chip được thiết kế để chạy các ứng dụng cụ thể. Chúng thường có trong ô tô và nhiều thiết bị điện tử, và bây giờ chúng xuất hiện trong một vài sản phẩm SSL. Nếu các chức năng bảo mật được tích hợp vào các chip ASIC, thì các chip này có thể tăng chức năng bảo mật web và giảm thiệt hại của SSL VPN khi bị tấn công.

3.4 Kết luận

Chương này đã trình bày các vấn đề về bảo mật trong SSL VPN, cụ thể là:

- Nhận thực, xác thực và đăng nhập một lần
- Khái niệm bảo mật đầu cuối
- Đầu cuối tin cậy và truy cập phân cấp
- Các vấn đề bảo mật phía máy chủ
- Sự cần thiết phải cập nhật máy chủ SSL VPN để có khả năng phục hồi trước các vụ tấn công

- Windows hay Linux là phù hợp với máy chủ SSL VPN

Qua những nội dung đã trình bày, chúng ta có thể thấy rằng SSL VPN đã gặp rất nhiều vấn đề bảo mật, có nhiều cách giải quyết khác nhau, mỗi cách giải quyết có những ưu điểm và nhược điểm riêng. Tuy vậy, nhìn chung có thể nhận thấy rằng SSL VPN là giải pháp toàn diện để giải quyết các vấn đề bảo mật đó.

Chương 4 TRIỂN KHAI SSL VPN

SSL VPN là một giải pháp hữu dụng nhưng không có nghĩa nó là công nghệ hoàn hảo phù hợp với tất cả các truy nhập từ xa cần thiết. Chương này sẽ mô tả các trường hợp có thể thực hiện một SSL VPN và các trường hợp mà IPSec được sử dụng sẽ phù hợp hơn.

4.1 Xác định yêu cầu

Công nghệ là công cụ được sử dụng để giúp con người thực hiện các mục đích, và do đó việc lựa chọn công nghệ cụ thể cần phải dựa trên các mục đích. Do đó, quan trọng là xác định mục tiêu của công ty hướng tới và dựa trên các yêu cầu đó, chọn công cụ kỹ thuật phù hợp. Trường hợp SSL VPN cũng như vậy.

4.1.1 Mô hình truy nhập dữ liệu

Truy nhập từ xa thường có hai mô hình chính: Site-to-Site và User-to-Site.

- **Site-to-Site:** Các công ty ở nhiều vùng khác nhau thường muốn ghép các mạng từ xa vào một mạng lớn. Thay vào việc chi tiền cho các liên kết đắt đỏ giữa các Site này, công ty có thể sử dụng công nghệ VPN để tạo kênh bảo mật qua Internet và do đó liên kết các site này lại. Kết nối VPN giữa các mạng nội bộ ở mỗi nơi thường được thực hiện bởi các phần mềm đặc biệt với các tường lửa ở mỗi site và được biết đến như là Site-to-Site VPN hoặc tường lửa tới tường lửa VPN. Công nghệ IPSec là một kiểu kết nối này, IPSec được sử dụng cho các kết nối này trong nhiều năm qua. Các nhà sản xuất SSL VPN đã không tập trung phát triển thị trường này trong thời gian đầu và ngày nay cũng chưa thể thỏa mãn được các yêu cầu kết nối Site-to-Site. Các công ty cần thực hiện kết nối Site-to-Site cần chọn lựa một công nghệ chuyển giao.
- **User-to-Site:** Truy nhập từ xa tới các tài nguyên như file, ứng dụng, cơ sở dữ liệu và các dịch vụ đầu cuối thường được gọi là kết nối User-to-Site. Công nghệ SSL VPN thường là một lựa chọn rất tốt khi các công ty thực hiện kết nối User-to-Site.

Bây giờ đồ án sẽ mô tả các bước thực hiện SSL VPN để thỏa mãn các yêu cầu User-to-Site.

4.1.2 Xác định nhu cầu của người dùng

SSL VPN phù hợp với truy cập từ xa User-to-Site. Nhưng truy cập nào mà người dùng muốn khi họ không ở công ty? Không có câu trả lời đơn giản nào cho câu hỏi này.

Các trường hợp khác nhau

Một vài người dùng kỹ thuật làm việc ở văn phòng MIS của một tập đoàn lớn có thể cần truy cập mức mạng do đó họ có thể ping các máy, trong khi một người bán hàng chỉ cần muốn truy cập từ xa tới hệ thống e-mail dựa trên web và hệ thống CRM của công ty. Chức năng mà một tổ chức thương mại cần và loại sản phẩm VPN công ty sẽ mua phụ thuộc nhiều vào mục đích sử dụng. Phần sau là một vài trường hợp thông thường và các khuyến nghị thực hiện:

- **Truy cập hoàn toàn mức mạng:** Nếu cần chỉ một nhóm người người dùng truy cập từ xa để truy cập hoàn toàn mức mạng như là họ ở văn phòng và việc truy cập chỉ thực hiện trên các máy tin cậy của công ty, một giải pháp dựa trên SSL đầu cuối là phù hợp. Một vài giải pháp có thể miễn phí (ít nhất là về phương diện đầu tư ban đầu), như các nhà sản xuất tường lửa/IPSec bắt đầu cho phép truy cập SSL như là một thành phần bổ sung của sản phẩm.
- **Truy cập từ xa tới e-mail:** Nếu người dùng thông thường cần truy cập từ xa tới e-mail mà không cần các ứng dụng khác, một giải pháp e-mail cụ thể có thể là một giải pháp phù hợp. Nhiều nhà sản xuất cho phép các sản phẩm của họ hỗ trợ chỉ chức năng này, và đương nhiên là giá của nó rẻ hơn nhiều so với SSL VPN đầy đủ. (Và thường thì nếu công ty muốn phát triển lên thì giải pháp trên có thể được phát triển thành SSL VPN đầy đủ).
- **Truy cập tới nhiều ứng dụng**: Nếu người dùng muốn truy cập tới nhiều ứng dụng hoặc nhiều file, thì dùng SSL VPN thông thường (được mô tả trong đồ án) là một giải pháp hữu hiệu.
- **Truy cập mức mạng đầy đủ đối với một số người dùng**: Nếu chỉ một số lượng nhỏ người dùng cần truy cập từ xa, và nhiều người dùng kỹ thuật cần truy cập mức mạng đầy đủ thì IPSec là một giải pháp lý tưởng. Một SSL VPN mức thấp có thể là một giải pháp tùy chọn.
- **Truy cập từ xa từ một số lượng các máy tính chỉ định**: Nếu truy cập từ xa chỉ được cho phép từ một số lượng nhỏ các máy tính xác định trước, thì cả IPSec VPN và SSL VPN đều là lựa chọn tốt. (SSL VPN thường tốt hơn nếu người dùng không giỏi lắm về kỹ thuật).
- **Truy cập đối với người dùng thương mại điện tử:** Nếu SSL VPN thực hiện như một công cụ cho không chỉ nhân viên mà cả người dùng thương mại điện tử - trong trường hợp khác hàng tương lai không nhận thực và khác hàng đều muốn truy cập tới các phần cụ thể thì một sản phẩm SSL VPN có các khả năng này (truy cập mức ứng dụng, tường lửa ứng dụng,…) là một lựa chọn tốt.
- **Các yêu cầu thương mại:** Nếu nhiều yêu cầu thương mại như cung cấp trang chủ truy cập từ xa cho nhân viên và cung cấp truy cập thương mại điện tử, trường hợp này thì nên sử dụng SSL VPN có khả năng cung cấp nhiều trang chủ SSL VPN độc lập.

- **Truy cập từ xa tới máy tính để bàn đối với một hoặc hai người dùng:** Nếu truy cập từ xa chỉ cần thiết đối với một hoặc hai người dùng và truy cập từ xa tới các máy tính của họ là chủ yếu thì việc sử dụng các phần mềm như GoToMyPC, pcAnywhere hoặc các sản phẩm khác tương tự sẽ tốt hơn nhiều là sử dụng một SSL VPN.

Tất nhiên là có nhiều khả năng có thể sử dụng tương ứng với nhiều yêu cầu khác nhau. Mỗi công ty cũng cần đối chiếu chức năng hiện tại của thiết bị và các chức năng sẽ phát triển trong tương lai của thiết bị để chọn lựa. Nói cách khác, một điểm quan trọng nữa là thiết bị đó hỗ trợ được các công việc thương mại cần thiết và các phiên bản tiếp theo của thiết bị sẽ hỗ trợ được các công việc thương mại trong tương lai.

Một thực tế quan trọng cần phải nhớ khi xác định các yêu cầu là người dùng thường không hiểu công nghệ chính họ đang sử dụng, nhưng họ thường biết việc của họ cần những gì. Vì vậy, trong khi một người dùng có thể suy nghĩ rằng anh ấy cần kết nối loại mạng cho hệ thống bởi vì nó luôn được thực hiện trong quá khứ (có nghĩa là trước đây anh ấy sử dụng kết nối loại mạng), trong khi có thể các ứng dụng sử dụng có thể cung cấp dịch vụ này mà không cần thiết lập kết nối mạng. Do đó, trong khi tìm hiểu người dùng cần các yêu cầu gì, thì phải giữ các công nghệ độc lập phù hợp với yêu cầu đó. Nói một cách khác, ta tìm hiểu tác vụ nào người dùng cần phải thực hiện chứ không phải họ nghĩ truy cập đó sẽ như thế nào.

4.2 Chọn lựa thiết bị SSL VPN phù hợp

Một SSL VPN là một đầu tư chiến lược và đầu tư theo yêu cầu thích hợp dẫn tới lựa chọn sản phẩm phù hợp. Ngày nay, các chức năng văn phòng của hầu hết các sản phẩm SSL VPN chính đã hội tụ lại với nhau. Điều này tạo ra một khung chung cho việc hình thành các dòng sản phẩm khác nhau của thiết bị. Tuy nhiên, không phải tất cả các trường hợp đều như vậy. Có nhiều chức năng có vẻ giống nhau và được phóng đại quá do tác hại của việc quảng cáo thương mại, chứ thực sự công nghệ sử dụng trong các sản phẩm khác nhau thường khác xa với chức năng được quảng cáo. Ưu điểm và nhược điểm của mỗi sản phẩm cần phải được so sánh với các yêu cầu của công ty trước khi quyết định sản phẩm nào và giải pháp nào được chấp nhận.

Tất nhiên là ta cũng phải tính toán đến yếu tố tin cậy của nhà sản xuất cho mỗi giải pháp, chẳng hạn bạn không muốn thực hiện công việc với một công ty phá sản hoặc đang bị điều tra bởi chính phủ.

Trong phần sau, đồ án sẽ mô tả rõ hơn và các nhân tố công ty cần xác định khi thực hiện một SSL VPN. Mặc dù không phải tất cả các nhân tố này áp dụng cho tất cả các công ty, chúng cũng rất thích hợp trong thực tế và có thể rất quan trọng trong việc xác định sự thành công của SSL VPN.

4.2.1 Xác định mức độ truy cập phù hợp

Rõ ràng, cần phải chắc chắn rằng sản phẩm được chọn sẽ cung cấp loại truy cập cần thiết. Việc xác định các ứng dụng và chức năng bạn muốn làm việc từ xa cũng rất quan trọng:

- Làm việc thực sự qua SSL VPN.
- Làm việc tất cả qua SSL VPN (tất cả các chức năng trong một ứng dụng làm việc).
- Làm việc qua SSL VPN từ các loại thiết bị bạn khuyến nghị người dùng sử dụng.
- Làm việc ở mức bạn yêu cầu họ thực hiện như vậy (ví dụ, ở mức ứng dụng vì vậy họ có thể sử dụng an toàn ở các thiết bị không tin cậy).

Nói một cách khác, quan trọng là phải chắc chắn rằng sản phẩm SSL VPN có thể đưa đến các chức năng bạn muốn có.

Nhiều SSL VPN đáp ứng được tất cả các chức năng bạn muốn có, nhưng có thể không cho phép tổng hợp các chức năng này như bạn cần để làm việc. Ví dụ, một SSL VPN có thể cho phép các ứng dụng được truy cập ở mức ứng dụng, và cho phép truy cập file, nhưng có thể không cho phép truy cập file ở mức ứng dụng. Việc xác định sản phẩm bạn mua có thể cung cấp các chức năng tổng hợp mà bạn cần là rất quan trọng.

Như đã mô tả ở trên, các yêu cầu thương mại cần phải tổng hợp lại mà không cần quan tâm đến công nghệ sử dụng để thực hiện các yêu cầu đó. Một ứng dụng cụ thể có thể có khả năng nhận thực người dùng khi họ ở văn phòng, nhưng các truy cập này có thể không phù hợp (do các chính sách bảo mật) đối với người dùng từ xa. Đôi khi, các truy cập này có thể thực hiện – nhưng chỉ là một phần nào đó của chương trình. Thỉnh thoảng, các truy cập cần phải được cung cấp tới ứng dụng, nhưng một vài chức năng trong chương trình lại không thực hiện được. Do đó, như đã mô tả trong chương 3, cần thiết phải có một vài cấp độ truy cập để phù hợp với chính sách bảo mật. Nếu chính sách của bạn điều khiển truy cập được cấp độ hóa thì bạn cần phải chắc chắn rằng SSL VPN bạn chọn có thể thực hiện phương pháp đó.

Một lưu ý quan trọng nữa là thỉnh thoảng một ứng dụng không làm việc qua một SSL VPN ở mức ứng dụng có thể dễ dàng thay đổi cách thực hiện của nó. Điều này là đặc biệt đúng trong trường hợp các menu Flash, các ứng dụng Java đơn giản, và các nơi mà thay đổi các mã này với một ngôn ngữ thay đổi luân phiên.

4.2.2 Lựa chọn giao diện người dùng phù hợp

Mặc dù tất cả các SSL VPN đều có giao diện đồ họa người dùng, nhưng các giao diện này lại khác nhau. Nhiều điểm quan trọng cần chú ý khi chọn giải pháp SSL VPN bao gồm:

- **Hỗ trợ truy cập từ thiết bị cầm tay:** Sự tăng lên của số lượng người dùng truy cập tài nguyên công ty từ các thiết bị cầm tay chạy trên các hệ điều hành như PalmOS, PocketPC, hoặc Sysbiam. Hầu hết các nhà sản xuất SSL VPN đều nói rằng sản phẩm của họ sẽ cho phép truy cập từ các thiết bị cầm tay. Tuy nhiên, công ty muốn thực hiện một SSL VPN cần phải kiểm tra xem SSL VPN đó thực hiện truy cập tốt từ các thiết bị từ xa cụ thể như thế nào, bởi vì không phải tất cả các SSL VPN làm việc với tất cả các thiết bị từ xa.
- **Sự linh hoạt của GUI:** Được xây dựng dựa trên GUI chuẩn giữa các sản phẩm SSL VPN, và chọn một chuẩn cho một nhóm cụ thể hoặc công ty. Một GUI tối ưu thường cho phép người dùng làm việc với một giao diện đơn giản như khi SSL VPN được cài đặt, nhưng cũng có thể được tùy biến. Khả năng thay dổi giao diện người dùng thường là một nhân tố rõ rệt của việc phân cấp người dùng. Người dùng của tất cả các sản phẩm SSL VPN sử dụng trình duyệt để truy cập từ xa. Một vài thành phần của giao diện là cố định qua các sản phẩm. Còn nữa, mặc dù khá giống nhau, giao diện xuất hiện thực sự trong trình duyệt rất khác nhau giữa các sản phẩm, cũng như độ linh hoạt và tùy chỉnh cung cấp cho người quản trị và người dùng. Hầu hết các SSL VPN cho phép các thành phần cơ bản của GUI có thể tùy biến được, ví dụ như màu nền của trang chủ, logo của công ty tải trên trang web, bookmark của người dùng. Tuy nhiên, sự thay đổi cơ bản của giao diện chuẩn không làm thay đổi cách làm việc của người dùng. Nếu một số lượng lớn người dùng sử dụng SSL VPN, và đương nhiên là cần có nhiều giao diện khác nhau tương ứng với từng nhóm người. Hệ thống phải luôn cho phép khả năng người dùng làm việc theo cách mà họ làm việc ở văn phòng và không hạn chết họ theo nghĩa thực hiện giao diện không thân thiện hoặc không hiệu quả. Hơn nữa, do cần thiết phải truy cập từ các thiết bị cầm tay, ta cần phải xác định xem SSL VPN có thể tối ưu giao diện cho thiết bị cầm tay với giao diện nhỏ được hay không.
- **Hỗ trợ nhiều ngôn ngữ:** Hỗ trợ nhiều ngôn ngữ là rất quan trọng trong các công ty đa quốc gia và các môi trường khác trong đó sử dụng nhiều ngôn ngữ. Nhiều nhân tố cần phải được xác định:
    - Nó có là SSL VPN động với nhiều ngôn ngữ trên giao diện người dùng, ngôn ngữ của một phiên làm việc cụ thể dựa trên cấu hình trên thiết bị truy cập.
    - Các công ty ở các nước không sử dụng tiếng Anh có thể không cần phải hỗ trợ nhiều ngôn ngữ mà chỉ cần hỗ trợ ngôn ngữ địa phương của họ. Các công ty mà thực hiện công việc thương mại của họ ở nhiều nước khác nhau thì tất nhiên cần hỗ trợ giao diện đa ngôn ngữ.
    - Nếu người dùng sử dụng bộ chữ non-Latin, hoặc dữ liệu non-Latin để truy cập thì phải chắc chắn SSL VPN có hỗ trợ các truy cập như vậy.

  - Tất nhiên, nếu một công ty thực hiện công việc thương mại của họ trên một vùng mà chỉ nói một ngôn ngữ thì tất nhiên là chức năng đa ngôn ngữ sẽ là không cần thiết và không cần phải kiểm tra.
- **Đăng nhập một lần bảo mật:** Nếu công ty của bạn lên kế hoạch thực hiện đăng nhập một lần bảo mật thì bạn phải chắc chắn rằng sản phẩm bạn dùng phải hỗ trợ SSO. Chức năng của SSO đã được mô tả ở các chương trước. Hãy chắc chắn rằng SSL VPN cho phép loại nào bạn cần đối với các yêu cầu thương mại và tích hợp nó.
- **Tích hợp trang chủ đang tồn tại:** Nếu công ty của có một trang chủ đang tồn tại, sẽ là tốt hơn nếu trang chủ ở cơ quan đang tồn tại cũng giống như trang chủ khi truy cập từ xa. Người dùng có thể thực hiện các công việc của họ như ở cơ quan và làm giảm bớt các yêu cầu giúp đỡ từ người dùng.

4.2.3 Quản lý mật khẩu từ xa

Các mật khẩu nên thường xuyên thay đổi, việc sử dụng một mật khẩu trong một thời gian dài có thể dẫn tới bị lộ và mất tác dụng.

Tuy nhiên truy nhập SSL VPN lại có một số vấn đề với việc quản lý mật khẩu. Một công ty bắt buộc người dùng của họ thường xuyên thay đổi mật khẩu, nếu không mật khẩu sẽ hết tác dụng thì người dùng đang sử dụng chương trình tại thời điểm mật khẩu hết tác dụng sẽ bị khóa tất cả các ứng dụng và file của họ.

Do đó, các công ty cần đầu tư SSL VPN cần xác định khi nào họ muốn có chức năng quản lý mật khẩu từ xa. Nếu họ thực hiện chức năng đó, họ cũng cần phải xác định xem SSL VPN có hỗ trợ chức năng đó hay không.

Một SSL VPN cho phép quản lý mật khẩu từ xa phải cảnh báo người dùng khi mật khẩu của họ sắp hết hạn và cho phép người dùng thay đổi mật khẩu sử dụng trình duyệt.

Các công ty sử dụng hai nhân tố nhận thực như là cơ chế điều khiển truy nhập cần phải chắc chắn rằng SSL VPN hỗ trợ cập nhật hệ thống nhận thực. Ví dụ, trong trường hợp cơ chế nhận thực dựa trên thẻ bài tận dụng máy chủ lưu trữ PIN (như là RSA SecurID) thì SSL VPN phải cho phép quản lý từ xa với các mã PIN kết hợp với các thẻ bài.

4.2.4 Sự tương thích của các chuẩn bảo mật

Tất cả các SSL VPN cho phép chức năng bảo mật, nhưng các chức năng bảo mật là khác nhau đối với các sản phẩm khác nhau. Việc đưa ra kết hoạch phù hợp để tính toán xem sản phẩm sử dụng có phù hợp với chính sách bảo mật của công ty hay không là rất quan trọng. Công nghệ SSL VPN và bảo mật của nó đã được mô tả ở phần trên của đồ án, dưới đây là các câu hỏi mà công ty phải trả lời được trước khi chọn sản phẩm SSL VPN:

- **Kết nối và khả năng kết nối:** Có phải SSL VPN bắt buộc bạn phải thực hiện một kết nối mạng từ bất kỳ máy tính không phải của công ty tới mạng nội bộ? Nó dựa vào các kết nối mạng để thực hiện bất kỳ các công việc quan trọng? Nếu công ty chặn các kết nối mạng thì các ứng dụng có thể hoạt động từ xa? Còn chuyển tiếp cổng thì như thế nào - ứng dụng nào sẽ hoạt động nếu chuyển tiếp cổng bị tắt?
- **Tích hợp với IDS:** Có phải SSL VPN tích hợp tốt với IDS (Hệ thống phát hiện xâm nhập)? Nó có hỗ trợ IDS dựa trên host trên máy chủ SSL VPN?
- **Tường lửa:** SSL VPN cho phép chặn các giao thức trong phạm vi tường lửa để đường hầm vào trong công ty. Nếu có, ở đâu sẽ bị chặn? Sẽ cần một tường lửa để cài đặt trên thiết bị SSL VPN?
- **Tường lửa ứng dụng:** SSL VPN cung cấp tường lửa ứng dụng, mà nó có thể chặn tất cả các yêu cầu không được xem là an toàn? Hoặc chỉ đơn giản kiểm tra định dạng HTML phù hợp (trong trường hợp các sâu và hacker có thể xâm nhập vào mạng công ty và tấn công hệ thống nội bộ)?
- **Timeout và tắt phiên làm việc:** SSL VPN cho phép thời gian timeout khi người dùng quên tắt phiên làm việc? Người dùng có được cảnh báo khi tắt phiên làm việc?
- **Đệm hóa dữ liệu:** SSL VPN đệm hóa dữ liệu từ thiết bị truy cập trong một môi trường bảo mật hoặc đơn giản là xóa nó (trong trường hợp tránh các nhóm không nhận thực có thể khôi phục nó) Nó xóa thông tin được lưu trữ trong các vùng không chuẩn? Nếu vùng bộ nhớ ảo được sử dụng thì tất cả các ứng dụng từ xa cần phải sử dụng bộ nhớ ảo này?
- **Kiểm tra và chứng thực:** SSL VPN đã được chứng thực bởi tổ chức kiểm tra bảo mật độc lập? Họ đã kiểm tra bảo mật thiết bị SSL VPN (bao gồm các vấn đề bên máy trạm) hoặc đơn giản là khả năng phục hồi của thiết bị khi bị một loại tấn công cụ thể nào đó? Sản phẩm đã được kiểm tra với một môi trường tương tự công ty bạn?

4.2.5 Platform

a) Phần cứng

Một vài loại SSL VPN ở dưới dạng thiết bị, trong khi một vài loại khác thì ở dưới dạng phần mềm mà cần phải cài đặt vào máy tính dẫn đến vấn đề lựa chọn loại nào phù hợp hơn (và lựa chọn các thành phần trong thiết bị nữa). Một thiết bị thì cài đặt đơn giản hơn và một vài công ty thích sử dụng một nhà cung cấp phần cứng chuẩn và cấu hình máy chủ để quản lý đơn giản. Trong bất kỳ trường hợp nào, chắc chắn rằng SSL VPN bạn chọn cho phép một platform tương thích trong một thời gian dài.

b) Hệ điều hành

Như đã mô tả trong chương 3, nhiều phiên bản khác nhau của Windows và Linux thường được sử dụng trong hầu hết các máy chủ SSL VPN. Về cơ bản, tốt hơn là chọn một SSL VPN chạy trên một hệ điều hành mà người quản trị đã tương thích với nó, và dựa trên các công cụ quản trị và điều khiển chuẩn mà công ty đã sử dụng.

c) Kết nối mạng

Ngày nay, SSL VPN thường sử dụng kết nối 100BaseT hoặc 1000BaseT (hay Gigabit Ethernet). Tuy nhiên, thực tế là phải bắt buộc các công ty đều có kết nối Internet cùng một tốc độ. Bởi vậy, 100BaseT thường hỗ trợ nhiều dung lượng dữ liệu hơn. Nút cổ chai trong SSL VPN thường không có trong kết nối từ máy chủ tới mạng, và do đó tốc độ của NIC sẽ liên quan nhiều đến hoạt động của SSL VPN.

Một ngoại lệ là nếu SSL VPN được sử dụng nội bộ (ví dụ người dùng trên mạng nội bộ sẽ truy cập hệ thống qua SSL VPN). Trong trường hợp này thì băng thông của máy chủ cũng rất quan trọng.

4.3 Xác định chức năng của SSL VPN sẽ được sử dụng

SSL VPN cho phép rất nhiều chức năng, một vài chức năng là không cần thiết đối với một môi trường cụ thể. Việc quyết định các chức năng nào mà công ty cần sử dụng để trực tiếp thỏa mãn các yêu cầu là rất quan trọng. Một vài trường hợp thông thường đã được mô tả ở phần trên của chương này. Dưới đây là một vài điểm cần lưu ý:

1. Truy cập mức ứng dụng có thể sử dụng cho các truy cập thông thường. Khi các ứng dụng cho phép một giao diện web, giao diện web đó cần phải được cho phép sử dụng qua SSL VPN.
2. Việc sử dụng truy cập loại dịch vụ đầu cuối đối với truy cập các ứng dụng có các giao diện web là không hiệu quả. Nó cũng làm giảm hoạt động và tạo ra các giới hạn không cần thiết đối với ứng dụng.
3. Quá trình đường hầm mạng có thể được sử dụng đối với người dùng cấp cao từ các điểm tin cậy, nhưng phải được tắt khi truy cập từ các máy tính không an toàn. Trong trường hợp này, chỉ nên dùng chuyển tiếp cổng.
4. Một khi Telnet được cho phép, thì cần phải giới hạn đối với mỗi người dùng, mỗi tài nguyên và mỗi điểm đích (ví dụ, Joe chỉ có thể Telnet từ máy tính xách tay của anh ấy đến máy chủ 1, 2, 3, 4).
5. Quá trình đường hầm và chuyển tiếp cổng không bao giờ được sử dụng theo kiểu "band-aid" – điều đó khiến các chương trình ở mức ứng dụng vì một vài lý do nào đó lại không hoạt động ở mức ứng dụng với một sản phẩm SSL VPN cụ thể nào đó (ví dụ, các ứng dụng web phức tạp sử dụng cho khách hàng truy cập).
6. Bộ nhớ cache phải bị xóa trên tất cả các máy tính.
7. Các ngưỡng timeout trên máy tin cậy cần phải được đặt lâu hơn trên máy không tin cậy.

4.4 Xác định vị trí đặt máy chủ SSL VPN

Như đã mô tả ở chương 3, việc đặt vị trí của SSL VPN liên quan nhiều đến việc thực hiện bảo mật.

Bây giờ đồ án sẽ mô tả những điểm hợp lý và không hợp lý khi đặt máy chủ ở một số nơi khác nhau trong kiến trúc mạng công ty thông thường.

4.4.1 Văn phòng

Một vị trí mà SSL VPN có thể đặt trong mạng nội bộ được mô tả trong hình 4.1.

Hình 4.1. Máy chủ trong mạng nội bộ

a) Ưu điểm

- Không có các cổng ngoài một cho SSL (và có thể có một cổng cho HTTP thông thường) cần được mở trong bất kỳ tường lửa nào.
- Giải mã lưu lượng SSL được thực hiện trong văn phòng.
- Các khóa SSL được lưu trữ trong một mạng an toàn.

b) Nhược điểm

- **Làm hư hỏng kiến trúc tường lửa:** Nó có thể làm hỏng toàn bộ kiến trúc tường lửa. Các giao thức mà tường lửa hỗ trợ để chặn bị đường hầm hóa sử dụng SSL trên tất cả các đường tới mạng nội bộ. Tại thời điểm máy chủ SSL VPN khôi phục lại định dạng ban đầu, nội dung của các phiên giao tiếp đã nằm trong mạng nội bộ mà trong khi nó không thuộc mạng này.

- **Mạng dựa trên IDS trên DMZ trở thành không tác dụng:** Bất kỳ mạng nào dựa trên các IDS trên DMZ sẽ mất tác dụng. Các IDS hoạt động bằng cách quét các gói mạng khi chúng đi qua mạng – việc đặt các IDS trên một DMZ là một công nghệ hữu ích để dừng lưu lượng xấu tới mạng công ty. Tuy nhiên, trong trường hợp một SSL VPN trên mạng nội bộ, tất cả các yêu cầu được mã hóa với SSL. Nếu các yêu cầu truyền qua DMZ ở dạng mã hóa, IDS sẽ không thể đọc được. Và do đó, IDS sẽ không thể phân biệt được người dùng và các cuộc tấn công.
- **Tự do truy cập tới mạng nội bộ:** Nếu máy chủ SSL VPN bị tấn công bởi một hacker hoặc sâu, các nhóm không nhận thực có thể tự do truy cập tới mạng nội bộ mà máy chủ SSL VPN kết nối được.
- **Các nút từ xa thực hiện như một cầu nối tới mạng khác:** Các nút từ xa có thể trở thành các cầu nối tới mạng khác như đã mô tả. Nếu một người dùng được cho phép thết lập một kết nối mạng qua SSL, thì có thể tất cả người dùng trên mạng nội bộ của máy đó có thể kết nối tới mạng nội bộ. Điều này làm ảnh hưởng nghiêm trọng đến kiến trúc công ty.
- **Các nhóm không nhận thực được phép gửi các gói mạng tới mạng nội bộ:** Vì một số lý do nào đó, công ty có thể cho phép các truy cập vi phạm các chính sách bảo mật. Từ đó, hacker và sâu có thể có truy cập tới bất kỳ tài nguyên nào của công ty. Dẫn tới các cuộc tấn công từ chối dịch vụ DoS, map mạng công ty, quét các điểm yếu và từ đó ăn trộm dữ liệu hoặc điều khiển các máy tính nội bộ,…

4.4.2 Vùng cách ly

Người ta thường đặt một máy chủ SSL VPN trong một DMZ như trong hình 4.2.

a) Ưu điểm

- Các giao thức không cần thiết có thể bị chặn bởi tường lửa bên trong.
- Chỉ các nhóm nhận thực có thể truy cập tài nguyên nội bộ, các nhóm không nhận thực sẽ bị chặn ở DMZ.
- IDS dựa trên mạng có thể đồng thời làm việc trên DMZ và các mạng nội bộ.
- Việc sử dụng một DMZ cho phép một phương thức phân lớp để bảo mật.

b) Nhược điểm

- **Các khóa SSL được duy trì trong một vùng không an toàn:** Nếu các khóa SSL bị tấn công, kẻ tấn công có thể giả dạng công ty. Tội phạm có thể tận dụng các thủ thuật lừa đảo để trộm thông tin nhạy cảm từ người dùng. Vì vậy tốt hơn hết là không nên đặt các khóa trong vùng không an toàn hoặc nửa an toàn.

- **Giải mã được thực hiện trong một vùng không an toàn:** Do việc truyền các thông tin nhạy cảm dưới dạng văn bản thông thường trên vùng DMZ không an toàn, nên các thông tin này có thể bị bắt lại bởi các phần mềm bắt gói tin. Do đó, SSL VPN sẽ không thể thực hiện được chức năng mã hóa đầu cuối – đầu cuối, mà chỉ là đầu cuối – nửa đầu cuối, tức là nội dung của phiên SSL được giải mã trong vùng không an toàn bên ngoài mạng đích.

Hình 4.2. Máy chủ đặt trong DMZ

- **SSL VPN làm hỏng các tường lửa bên ngoài:** Nếu một người dùng từ xa được cho phép thiết lập kết nối mạng qua SSL, người dùng có thể truyền bất kỳ giao thức nào bằng cách nhúng các gói mạng trong HTTPS. Điều này có nghĩa là các giao thức đó không thể bị chặn bởi tường lửa bên ngoài khi chúng đường hầm hóa trong HTTPS tới DMZ. Các nhà quản trị thiết lập tường lửa bên ngoài để chặn một cổng cụ thể để tắt một dịch vụ cụ thể nào đó. Việc cho phép giao tiếp này phá vỡ các bức tường bảo mật là một vấn đề quan trọng và thường ảnh hưởng đến chính sách bảo mật công ty.
- **Một số cổng cần phải được mở trên tường lửa nội bộ:** Điều này cho phép một số loại giao tiếp không thích hợp giữa DMZ và mạng nội bộ. Việc mở các cổng này làm tổn hại đến hiệu quả của tường lửa nội bộ, làm lu mờ biên giới giữa DMZ và Internet, và tạo ra các vấn đề bảo mật nghiêm trọng.
- **Các nút từ xa có thể thực hiện như một cầu nối tới mạng khác:** Các nút từ xa có thể trở thành các cầu nối tới mạng khác như đã mô tả ở trên. Nếu một người dùng được cho phép thết lập một kết nối mạng qua SSL, thì có

thể tất cả người dùng trên mạng nội bộ của máy đó có thể kết nối tới mạng nội bộ.

- **Các nhóm bên ngoài có thể trở thành các nút trên mạng công ty:** Hầu hết các công ty quan tâm đến bảo mật đều không muốn bất kỳ máy tính nào không phải của công ty trở thành một nút của mạng công ty. Nếu một SSL VPN được sử dụng cho các thành viên, các khách hàng, và các khác hàng tương lại để truy cập tài nguyên công ty, và nếu SSL VPN cho phép người dùng từ xa thiết lập kết nối mạng qua SSL, thì chính sách này sẽ bị tổn hại (và vấn đề này sẽ dẫn tới một loạt các vấn đề nghiêm trọng).
- **Truy cập để tấn công các máy chủ nội bộ:** Nếu một hacker hoặc sâu tấn công máy chủ SSL VPN, các nhóm xấu có thể truy cập tới một máy tính và từ đó tiến hành tấn công các máy chủ nội bộ.

4.4.3 Bên ngoài phạm vi tường lửa

Hình 4.3. Máy chủ ngoài phạm vi tường lửa

Một vị trí có thể của SSL VPN là phía bên ngoài phạm vi tường lửa

a) Ưu điểm

- Các giao thức không mong muốn sẽ không thể tới công ty – thậm chí không đến được cả DMZ.
- Các nhóm không nhận thực không thể tới DMZ của công ty hoặc mạng nội bộ của nó.
- Các hệ thống IDS dựa trên mạng có thể hoạt động trên cả DMZ và các mạng nội bộ.

b) Nhược điểm

- **SSL VPN không được bảo vệ khỏi các cuộc tấn công mức mạng:** Trừ khi SSL VPN có tường lửa mức mạng, việc đặt nó trong một môi trường không an toàn như trên sẽ dẫn tới các vấn đề nghiêm trọng.
- **Các khóa SSL được lưu trữ trong vùng không an toàn:** Như đã mô tả ở phần DMZ, hoàn cảnh này cũng khiến các khóa không được lưu trữ trong vùng an toàn, thậm chí còn ở vùng tồi tệ hơn – Internet.
- **Các cổng cần phải mở trên tường lửa:** Điều này cho phép một số loại giao tiếp không thích hợp giữa DMZ và mạng nội bộ. Việc mở các cổng này làm tổn hại đến hiệu quả của tường lửa nội bộ, làm lu mờ biên giới giữa DMZ và Internet, và tạo ra các vấn đề bảo mật nghiêm trọng.

4.4.4 Air Gap

Air Gap và các công nghệ tương tự giúp giải quyết được một số vấn đề bảo mật đã được nêu ra trước đây. Air Gap sử dụng hai máy chủ để phục vụ các yêu cầu SSL VPN, một kết nối tới mạng nội bộ và một tới DMZ. Máy chủ bên ngoài nhận các yêu cầu người dùng, trong khi máy chủ bên trong thực hiện tất cả các quá trình SSL VPN và các chức năng bảo mật. Giữa hai máy tính, không có kết nối mạng nào nhưng có một bộ nhớ chia sẻ giữa chúng, bộ nhớ này chỉ có thể truy cập bởi một máy chủ tài một thời điểm.

Trong hình 4.4, một Air Gap chuyển đổi máy tính nào có thể truy nhập bộ nhớ tại thời điểm hiện tại.

a) Ưu điểm

Công nghệ Air Gap duy trì một kết nối giữa Internet và các máy chủ nội bộ, và cho phép một số cải tiến so với kiểu DMZ chuẩn thông thường đã được mô tả ở trên.

- Nó chắc chắn rằng bất kỳ máy nào có thể tới mạng nội bộ bằng một kết nối mức mạng trong khi người dùng không tin cậy không thể truy cập tới. Thậm chí nếu máy chủ SSL VPN bên ngoài bị tấn công bởi các hacker và các sâu thì các nhóm này vẫn không thể kết nối tới hệ thống nội bộ.
- SSL VPN khó bị tấn công hơn do yếu điểm của hệ điều hành không thể bị lợi dụng trên máy chủ nội bộ.
- Các khóa SSL được duy trì trong vùng mạng nội bộ an toàn hoặc trên vùng DMZ an toàn hơn mà không cần mở các cổng giao tiếp cho quá trình giao tiếp liên quan đến mã hóa SSL.
- Các cổng không được mở trên các tường lửa đã kết nối tới Internet.

Hình 4.4. AirGap

b) Nhược điểm

Nhược điểm chính của công nghệ Air Gap là nó đắt hơn và phức tạp hơn kiến trúc thông thường. Và do vậy, Air Gap phù hợp hơn cho các công ty lớn hoặc vừa quan tâm đến bảo mật, và không thích hợp đối với các công ty nhỏ.

4.4.5 Bộ tăng tốc SSL

Việc giải thoát một bộ xử lý SSL trên cùng một mạng cũng là một trường hợp thực hiện SSL. Hình 4.5 mô tả một ví dụ giải thoát quá trình xử lý SSL từ bên ngoài phạm vi tường lửa tới DMZ.

Tuy nhiên, sử dụng bộ tăng tốc SSL cũng có thể tác động đến kiến trúc mạng. Ví dụ, việc giải phóng quá trình giải mã SSL từ một vùng không an toàn tới một bộ xử lý SSL nội bộ sẽ tạo nên nhiều hiệu quả khác nhau. Các ví dụ trong trường hợp này bao gồm:

- Giải phóng xử lý SSL khỏi phạm vi tường lửa tới DMZ.
- Giải phóng quá trình xử lý SSL từ DMZ tới văn phòng.
- Giải phóng SSL từ DMZ bên ngoài tới DMZ bên trong.

Trong tất cả các trường hợp thì đều có những ưu điểm và nhược điểm chung.

Hình 4.6 mô tả giải phóng xử lý SSL từ DMZ tới văn phòng.

a) Ưu điểm

Việc giải mã sẽ thực hiện ở một môi trường an toàn hơn. Các khóa SSL được lưu trữ trong một môi trường an toàn hơn.

b) Nhược điểm

Tuy nhiên thì nó cũng có những nhược điểm. Giao tiếp giữa máy chủ SSL VPN trên vùng ít an toàn hơn và bộ tăng tốc trong môi trường an toàn hơn thì các cổng giao tiếp phải được mở, điều đó có nghĩa là mô hình bảo mật phân lớp sẽ bị yếu đi.

Hình 4.5. Bộ tăng tốc SSL ở giữa DMZ và tường lửa

Hình 4.6. Bộ tăng tốc đặt ở trong mạng nội bộ

4.5 Lên kế hoạch thực hiện

Mặc dù không có danh sách các công việc để tiến hành chuẩn bị thực hiện SSL VPN nhưng phần sau sẽ đưa ra một danh sách các yêu cầu cần chú ý trong giai đoạn thiết kế:

- **Các địa chỉ IP có thể kết nối từ bên ngoài:** Công nghệ bảo mật như NAT có thể cho phép một địa chỉ IP nội bộ được sử dụng. Nếu công nghệ Air Gap được sử dụng, thì cũng cần một địa chỉ cho mỗi máy chủ. Nếu các máy chủ SSL VPN được sử dụng kết hợp với bộ cân bằng tải thì địa chỉ IP ảo (có thể truy cập Internet) sẽ được xem như địa chỉ IP thực của máy chủ.
- **Tên DNS có thể kết nối từ bên ngoài:** Nếu bộ cân bằng tải được sử dụng thì tên DNS để kết nối SSL VPN cần phải được xem như là các tên DNS của các máy chủ SSL VPN thực sự.
- **Dải địa chỉ IP và tên DNS của các hệ thống nội bộ:** Bạn cũng cần phải biết dải địa chỉ IP và nên DNS của bất kỳ hệ thống nội bộ mà bạn muốn cung cấp truy cập từ xa. Nếu SSL VPN bạn đang sử dụng không có các module chương trình mà tự động cấu hình các cập thì đối với mỗi ứng dụng bạn cần phải biết cổng sử dụng cho ứng dụng đó nữa.
- **Nhận thực truy cập và các hệ thống thư mục người dùng:** Bạn cũng cần cấu hình nhận thực và hệ thống thư mục người dùng để SSL VPN giao tiếp.
- **Địa chỉ IP tăng tốc SSL bên ngoài:** Địa chỉ IP cho bất kỳ bộ tăng tốc SSL VPN bên ngoài sẽ được sử dụng bởi SSL VPN để tăng độ tin cậy hoặc hiệu

năng hệ thống cần phải đực xác định. Nếu một bộ tăng tốc SSL được cài đặt vào máy chủ SSL VPN, bạn phải theo đúng chỉ dẫn tích hợp bộ tăng tốc.

- **Các chính sách bảo mật:** Bao gồm tất cả các chính sách để truy cập.
- **Các yếu tố vật lý:** Bao gồm:
  - Không gian Rack cắm ở sau phòng máy tính hoặc trung tâm dữ liệu.
  - Cáp mạng
  - Cáp nguồn
  - Bộ ổn định và lưu trữ điện

4.6 Đào tạo người dùng và nhà quản trị

Việc đào tạo cho người dùng và nhà quản trị là rất quan trọng đối với sự thành công của bất kỳ công nghệ nào. Do sự phổ biến của các trình duyệt nên SSL VPN cũng không mất quá nhiều chi phí cho việc đào tạo này.

4.7 Kết luận

Trong chương này, đồ án mô tả làm thế nào để lên kế hoạch thực hiện một SSL VPN. Nội dung chương bao gồm các vấn đề:

- Xác định các yêu cầu thương mại
- Chọn sản phẩm SSL VPN phù hợp
- Xác định vị trí thiết bị
- Thực hiện SSL VPN

Qua những nội dung đã trình bày, chúng ta có thể nhận thấy rằng tùy vào điều kiện của các công ty, chi nhánh mà chúng ta có thể thực hiện SSL VPN theo nhiều cách khác nhau. Sự khác nhau có thể là ở chủng loại thiết bị, sơ đồ thiết bị và thậm chí có thể là các giải pháp khác ngoài SSL VPN như IPSec VPN, phần mềm,…

Chương 5 MÔ PHỎNG SSL VPN

5.1 Giới thiệu

Trong các phần trước, chúng ta đã xem xét một số khía cạnh của SSL VPN, bao gồm hoạt động và các vấn đề bảo mật cũng như cách giải quyết trong SSL VPN. Chương này sẽ giới thiệu chương trình mô phỏng một SSL VPN, để qua đó có thể thấy rõ hơn ưu điểm của SSL VPN.

Kịch bản mô phỏng được thể hiện trên hình 5.1:

Hình 5.1. Mô hình mô phỏng

Trong đó ASA là thiết bị Router dòng 5500 của Cisco, thiết bị này được cải tiến từ PIX (firewall), nó hỗ trợ IPSec VPN và SSL VPN. Phần quan trọng nhất của chương trình mô phỏng này cũng chính là việc mô phỏng hoạt động thiết bị đó.

Hiện nay, phần mềm mô phỏng ASA mới được phát triển gần đây, các nhóm phát triển đều tập trung giả lập môi trường Bios của thiết bị ASA thật, để từ đó chạy các IOS của ASA thật. Các môi trường này đều được viết từ ngôn ngữ lập trình C++ nên thường chọn hệ điều hành Linux để chạy (một điều cần chú ý nữa là ASA được phát triển từ Bộ định tuyến, mà bộ định tuyến thì đươc phát triển từ máy tính chạy Unix). Vì vậy, để mô phỏng ASA, chúng ta có 2 hướng chính:

- Thứ nhất là sử dụng hệ điều hành Windows, và chạy chương trình mô phỏng Qemu, thực chất của chương trình này là tạo ra một môi trường Linux ảo trên Windows.
- Thứ hai là sử dụng hệ điều hành Linux thật để chạy IOS.

Đối với cách thứ nhất thì có nhược điểm là Qemu có quá nhiều lỗi khi giả lập Linux trên Windows, và đặc biệt không thể bật được chức năng Webvpn (tên khác của SSL VPN). Đối với cách thứ hai thì mô phỏng tốt ASA với đầy đủ các chức năng quan trọng, nhưng nhược điểm là chúng ta cần phải có máy tính khác để telnet vào và quản lý nó. Bởi vậy, em sử dụng cả hai phương pháp trên, chạy Linux trên máy ảo để chạy ASA.

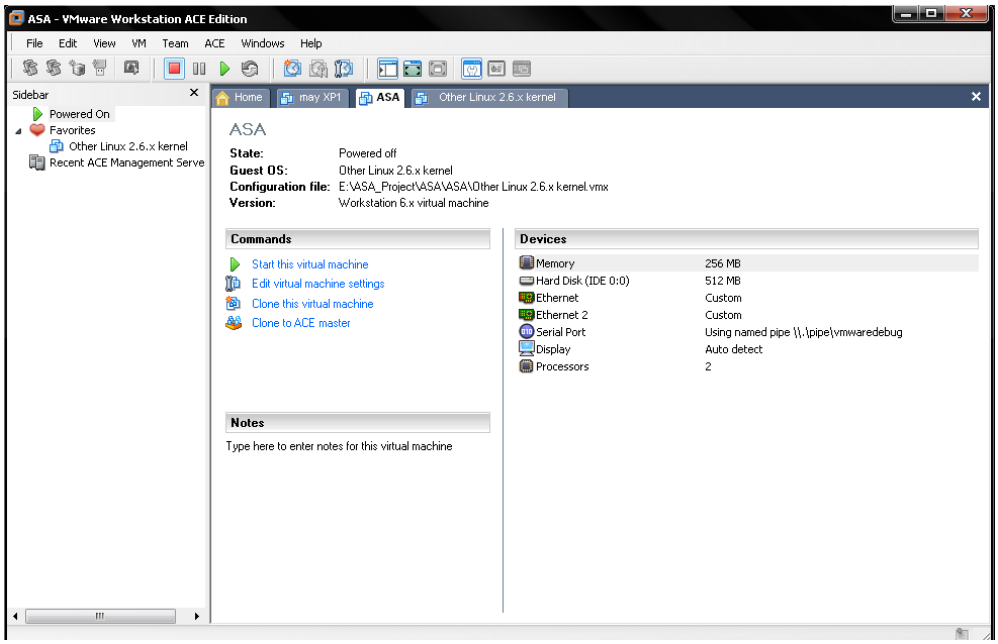
Các phần mềm sử dụng trong phần mô phỏng này bao gồm:

- **VMware**: Đây là phần mềm mô phỏng máy ảo chạy hệ điều hành thật, đặc biệt, VMware có các Switch ảo để hỗ trợ kết nối với máy tính thật, switch thật.
- **CiscoSDM**: Đây là phần mềm quản lý thiết bị của Cisco, với phần mềm này, việc quản lý SSL VPN và các chức năng khác của thiết bị sẽ dễ dàng hơn rất nhiều. Phần mềm này chạy trên Java.
- **Fiddler 2**: Đây là phần mềm thay đổi bản tin web, các gói tin HTTP và HTTPS đều phải qua phần mềm này, mục đích của phần mềm này là trả lời các bản tin yêu cầu phiên bản của CiscoSDM tới ASA, trong khi ASA không thể trả lời được các yêu cầu này (do nó là mô phỏng, không có đoạn Bios chứa đoạn mã phiên bản ASA). Phần mềm này chạy trên Java.
- **SolarWind TFTP server**: Để tạo một máy chủ TFTP trên máy tính, mục đích là tải trình điều khiển ASDM lên ASA.
- **Putty**: Là chương trình telnet, hỗ trợ telnet, SSH,…

Chương trình mô phỏng thiết bị 5520 của Cisco, chạy ASA phiên bản 8.02 với trình điều khiển ASDM phiên bản 6.02.

5.2 Thực hiện mô phỏng

Đầu tiên, tạo máy ảo với phần mềm VMware như hình 5.2:

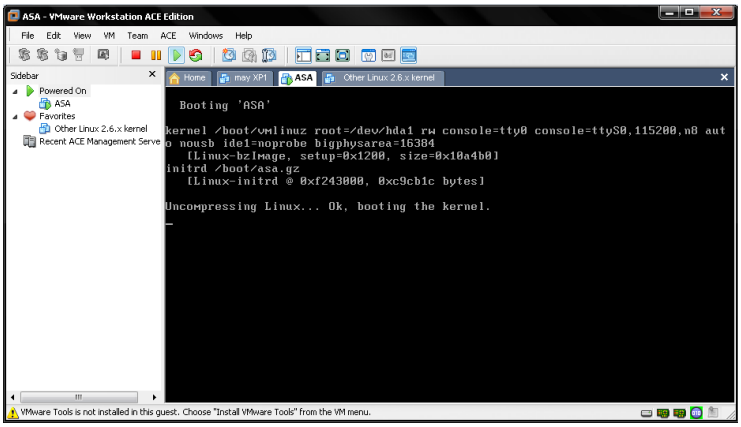


Hình 5.2. Máy ảo ASA

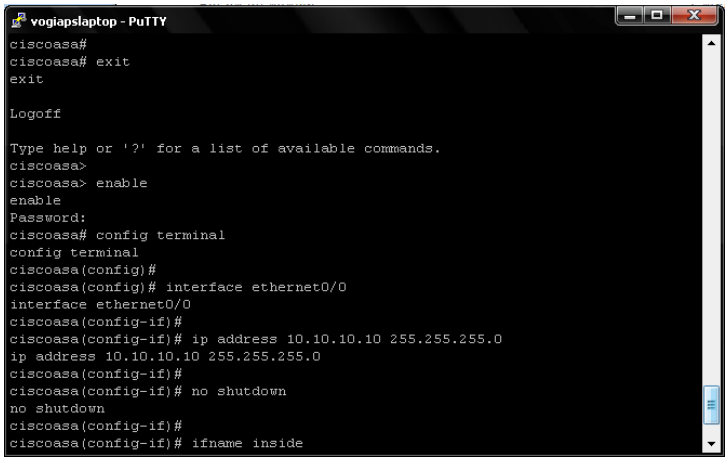
Có 3 kết nối tới máy tính này, tương ứng với 3 kết nối của thiết bị ASA, Ethernet kết nối tới máy tính qua Switch ảo VMnetwork 5. Ethernet 2 và Serial đều là kết nối tùy chọn, có thể sử dụng cho nhiều kết nối khác, kết nối Serial sử dụng pine.

Sau đó ta chạy máy ảo này, kết quả như hình 5.3.

Sau đó chạy VMware gateway để kết nối với ASA. Dùng Putty để telnet tới ASA, địa chỉ 127.0.0.1 port 567. Từ cửa sổ Telnet ta tiến hành cấu hình các cổng để kết nối tới máy tính thật qua cổng Ethernet, bật chức năng http server (qua lệnh *http server enable, http 0.0.0.0 0.0.0.0 inside)* , cấu hình tftp server (*qua lệnh tftp-server inside 10.10.10.230 asdm-602.bin*), cấu hình username và password quản lý (qua lệnh *username admin password admin privilege 15),* như hình 5.4.



Hình 5.3. ASA trên VMware



Hình 5.4. Cấu hình kết nối

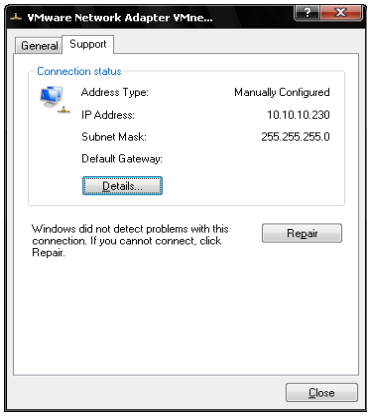
Trên giao diện VMware network adapter ta cũng tiến hành gán địa chỉ IP (hình 5.5):

Sau đó, chạy TFTP server, tiến hành copy trình điều khiển asdm-602.bin vào bộ nhớ flash của ASA (qua lệnh *copy flash tftp*).

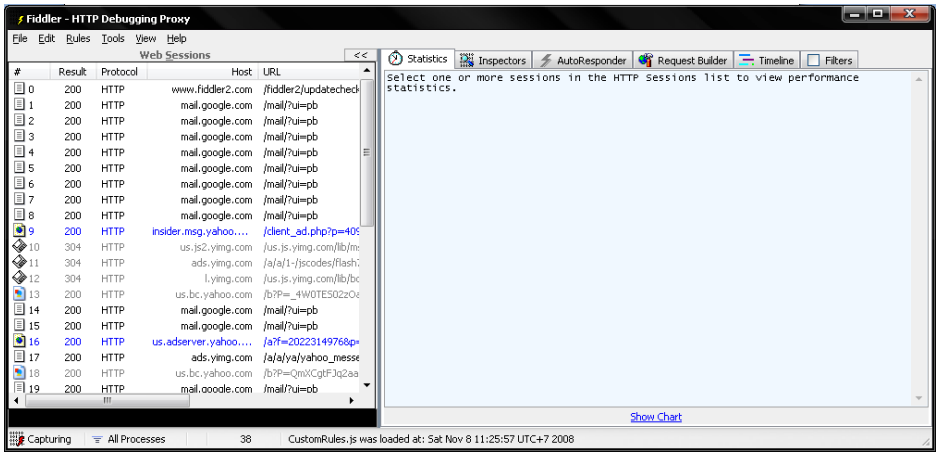
Sau đó, chạy Fiddler 2, thêm đoạn mã trả lời phiên bản vào luật của nó:

static function OnBeforeResponse(oSession: Session)
{
If
(oSession.url.EndsWith("/admin/exec/show+version/show+curpriv/perfmon+interval+10/show+asdm+sessions/show+firewall/show+mode/changeto+system/show+admin-context"))

```
{
 oSession.utilDecodeResponse();
  oSession.utilReplaceInResponse('Hardware:   ','Hardware:   ASA5520,');
}
```



Hình 5.5. Cấu hình VMware network adapter

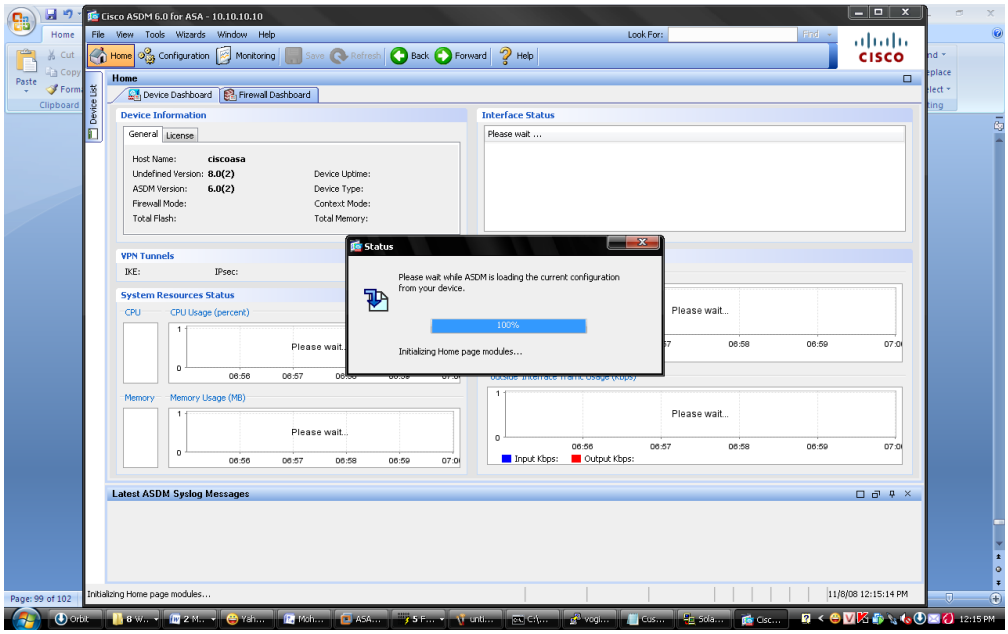


Hình 5.6. Fidder 2

Chạy CiscoSDM tới địa chỉ cổng Ethernet của ASA như trong hình 5.7

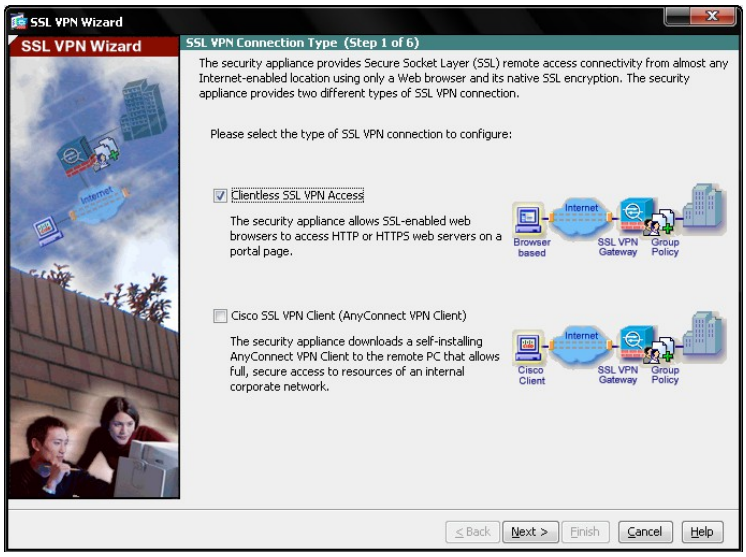
Hình 5.7. Đăng nhập Cisco ASDM laucher

Ta vào được Cisco ASDM laucher như hình 5.8.



Hình 5.8. Cisco ASDM

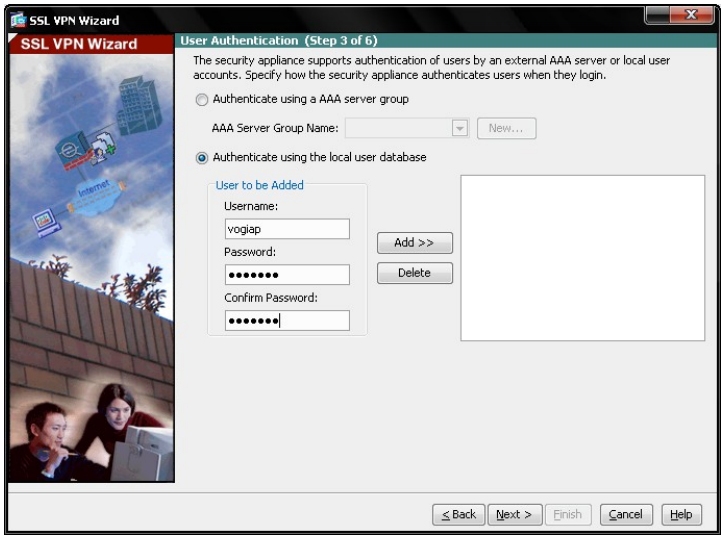
Qua ASDM laucher, ta tiến hành cấu hình SSL VPN:



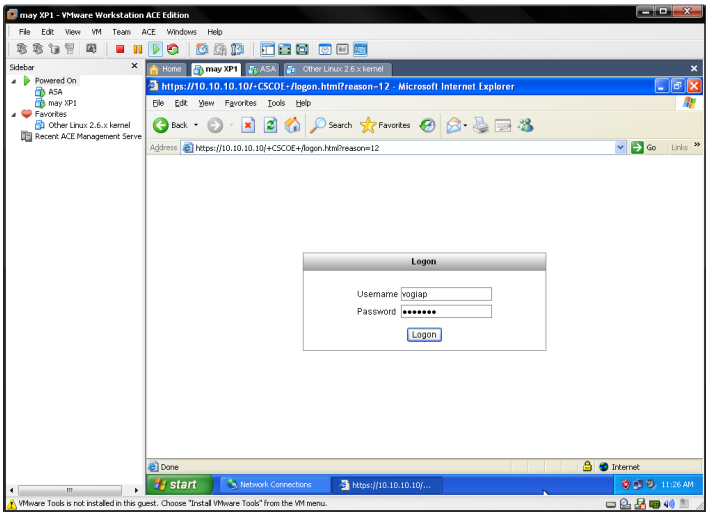
Hình 5.9. Cấu hình SSL VPN

Có nhiều bước trong cấu hình, trong đó có bước cấu hình nhận thực (hình 5.10):

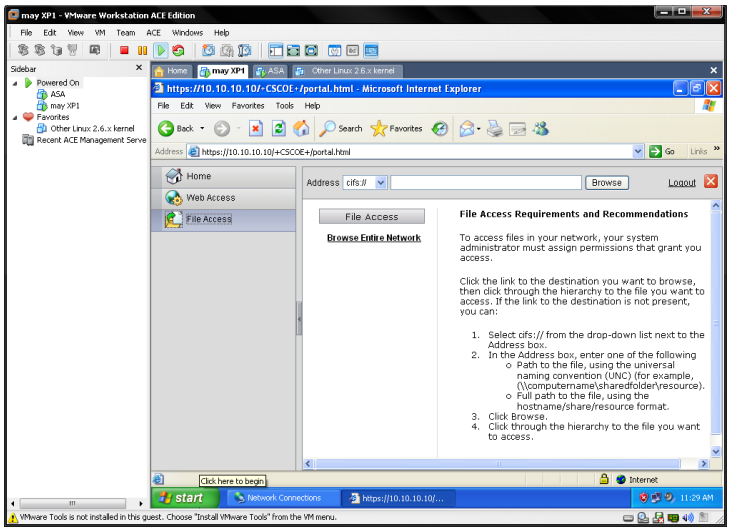
Sau đó tiến hành đăng nhập từ một trình duyệt web trên một máy tính kết nối mạng, ta sẽ có trang chủ. Ở đây em dùng trình duyệt Internet Explorer trên Windows XP chạy trên máy ảo VMware, ta sẽ được kết quả như hình 5.11. Sau khi đăng nhập, ta sẽ có phiên làm việc như hình 5.12.



Hình 5.10. Thêm người dùng trong SSL VPN

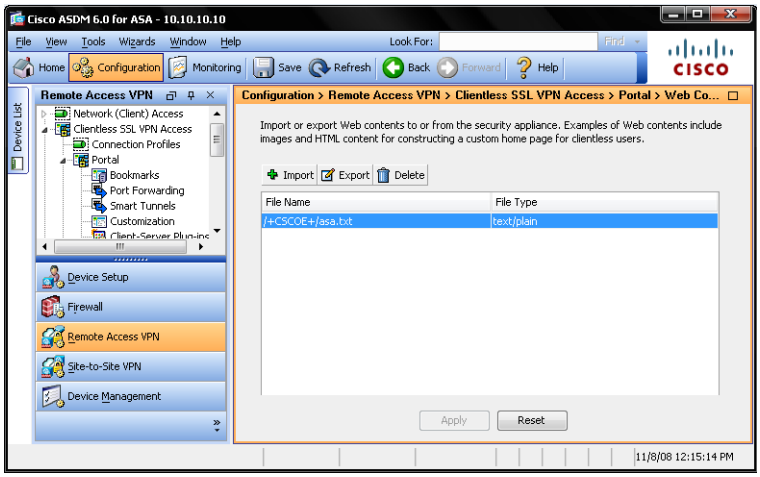


Hình 5.11. Đăng nhập đối với người dùng từ xa



Hình 5.12. Màn hình làm việc người dùng từ xa

Như vậy, ta đã tiến hành mô phỏng thành công SSL VPN, ngoài ra, với Cisco ASDM, ta còn có thể có rất nhiều chức năng quản lý, như thêm trang web, thêm công việc, thêm file,… cho truy cập SSL VPN từ xa. Hình 5.13 mô tả một số chức năng:



Hình 5.13. Một số chức năng SSL VPN

5.2 Kết luận

Chương này trình bày về các bước mô phỏng SSL VPN chạy trên ISO thật của Cisco, đây là một số bước chính trên thực tế sẽ được tiến hành khi xây dựng SSL VPN cho một doanh nghiệp. Qua đó, chúng ta có thể thấy rõ, đối với một người dùng truy cập từ xa thì ta chỉ cần trình duyệt kết nối mạng, gõ địa chỉ URL của công ty, đăng nhập là hoàn toàn có thể làm các công việc hàng ngày, đây là một trong những ưu điểm mạnh mẽ nhất để cho SSL VPN trở thành một trong những công nghệ được quan tâm nhất hiện nay trong lĩnh vực kết nối VPN.

Kết luận

Công nghệ SSL VPN là một công nghệ đã được áp dụng ở nhiều nước, đã mang lại nhiều lợi ích cho các doanh nghiệp. Nó tận dụng được các ưu điểm về giá thành, sự linh hoạt và quản trị để trở thành một trong những công nghệ VPN phổ biến nhất hiện nay. Trong tương lai, SSL VPN sẽ được tiếp tục phát triển và ngày càng hoàn thiện hơn, nên ứng dụng của nó trong tương lai sẽ là trong nhiều lĩnh vực hơn, hiệu quả hơn, bảo mật hơn,…

Đồ án này đã tìm hiểu về hoạt động và các vấn đề bảo mật của SSL VPN. Nội dung chính đồ án đã trình bày bao gồm:

- *Khái niệm về VPN và SSL VPN, đưa ra một số khái niệm liên quan đến SSL VPN. Qua đó chúng ta có thể nhận thấy ưu điểm của công nghệ này.*
- *Giao thức SSL và việc sử dụng SSL để tạo nên VPN, các công nghệ tiền thân của SSL VPN. Hoạt động của SSL VPN, các cải tiến quan trọng trong SSL VPN, các dịch vụ trong SSL VPN và các thành phần của nó. Qua đó chúng ta có thể có một cái nhìn sâu hơn về hoạt động của SSL VPN.*
- *Phương pháp bảo mật trong SSL VPN, các khái niệm, và vấn đề bảo mật xảy ra với SSL VPN cũng như cách giải quyết các vấn đề này. Qua đó chúng ta có thể hiểu rõ hơn về bảo mật trong SSL VPN*
- *Các bước cần tiến hành để xây dựng một SSL VPN cho một môi trường cụ thể, qua đó đưa ra các giải pháp cho từng môi trường cụ thể.*
- *Tiến hành mô phỏng SSL VPN, đây là một chương trình mô phỏng khá sát với thực tế do tất cả các thành phần đều chạy trên hệ điều hành thật. Qua đó mô tả một cách trực quan các ưu điểm rõ rệt của SSL VPN.*

Do các ưu điểm rõ rệt của nó, giải pháp SSL VPN không ngừng được cải tiến trong thời gian gần đây. Bởi vậy, hướng nghiên cứu tiếp theo của đồ án là tìm hiểu các cải tiến mới được đưa ra trong thời gian gần đây. Ngoài ra, hướng phát triển chương trình mô phỏng sẽ là sử dụng các công cụ trong mô phỏng để xây dựng một SSL VPN toàn diện hơn, với nhiều dịch vụ hơn,…

Cuối cùng, em xin cảm ơn sự quan tâm của các thầy cô giáo đối với đồ án, và đặc biệt xin gửi lời cám ơn chân thành và sâu sắc tới thầy giáo Nguyễn Tiến Ban đã đóng góp ý kiến và giúp đỡ em rất nhiều trong thời gian làm đồ án.

Hà nội, tháng 11 năm 2008

Võ Trọng Giáp

Tài liệu tham khảo

[1]. SSL VPN, Understanding, evaluting, and planning secure, web-based remote acess. Joseph Steiberg and Timothy Speed. Packt Publishing, 2005.

[2]. SSL Remote Access VPNs, Jazib Frahim and Qiang Huang. Cisco Press, 2008.

[3]. SSL and TLS Essentials, Stephen Thomas. Wiley Computer Publishing John Wiley & Sons, Inc, 2000.

[4]. Cisco Security Appliance Command Line Configuration Guide, chapter 34: Configuring Easy VPN Services on the ASA 5505, Cisco Press, 2005.

[5]. Jupiter Networks Secure Access SSL VPN. Syngress Publishing, Inc, 2007