

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG
KHOA CÔNG NGHỆ THÔNG TIN



ĐỒ ÁN TỐT NGHIỆP

NGÀNH: CÔNG NGHỆ THÔNG TIN

Họ và tên: Vũ Quốc Anh

Giảng viên hướng dẫn: ThS. Nguyễn Như Chiến

Hải Phòng - 2023

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG
KHOA CÔNG NGHỆ THÔNG TIN

**TÌM HIỂU, THỬ NGHIỆM HỆ THỐNG VPN DỰA
TRÊN OPENSWAN**

**ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY
NGÀNH: CÔNG NGHỆ THÔNG TIN**

**Họ và tên: Vũ Quốc Anh
Giảng viên hướng dẫn: ThS. Nguyễn Như Chiến**

Hải Phòng - 2023

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG
KHOA CÔNG NGHỆ THÔNG TIN

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên: Vũ Quốc Anh

Mã SV: 1912101008

Lớp: CT2301C

Ngành: Công nghệ thông tin

Tên đề tài: Tìm hiểu, thử nghiệm hệ thống VPN dựa trên OpenSwan

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

a. Nội dung

- Tìm hiểu về công nghệ IPSec.
- Tìm hiểu về gói phần mềm OpenSwan.
- Thực hiện cài đặt gói phần mềm OpenSwan trên hai sever (cài hệ điều hành Centos) và cấu hình sao cho hai mạng subnet ở phía sau hai server có thể kết nối được với nhau.

b. Các yêu cầu cần giải quyết

- Hiểu về công nghệ IPSec và tầm quan trọng của nó trong việc truyền tải dữ liệu trên mạng.
- Cài đặt và cấu hình thành công được gói phần mềm OpenSwan theo mô hình Site-to-Site.

2. Các tài liệu, số liệu cần thiết

Tài liệu tiếng việt

1. *Giáo trình An toàn mạng riêng ảo*, “Học viện Kỹ thuật Mật mã”.

Tài liệu tiếng anh

2. Dave Kosiur. *Building and Managing Virtual Private Networks*. 1998.
3. Jon C. Snader. *VPNs Illustrated: Tunnels, VPNs, and IPSec*. 2005
4. Paul Wouters, Ken Bantoft. *Building and Integrating Virtual Private Networks with OpenSwan*. 2006.
5. James S. Tiller. *A Technical Guide to IPSec Virtual Private Networks*. 2000
6. Naganand Doraswamy, Dan Harkins. *IPSec: The New Security Standard for the Internet, Intranets and Virtual Private networks, Second Edition*. 2003

3. Địa điểm thực tập tốt nghiệp

- Công ty Cổ phần hạ tầng Viễn thông CMC.

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Họ và tên : Nguyễn Như Chiến

Học hàm, học vị : Thạc sĩ

Cơ quan công tác : Học Viện Kỹ Thuật Mật Mã

Nội dung hướng dẫn : Nội dung hướng dẫn: “Nghiên cứu, thử nghiệm hệ thống VPN dựa trên OpenSwan”

Chương 1 - Bộ phần mềm OpenSwan: Trình bày tổng quan về VPN, giao thức IPsec VPN và giới thiệu bộ phần mềm OpenSwan: lịch sử, các thành phần của bộ phần mềm OpenSwan.

Chương 2 - Triển khai hệ thống VPN dựa trên OpenSwan: Trình bày thực nghiệm triển khai mô hình VPN Remote access dựa trên gói cài đặt bộ phần mềm OpenSwan.

Chương 3 - Phân tích và tùy biến mã nguồn OpenSwan: Trình bày về cấu trúc thư mục mã nguồn và phân tích các module của bộ phần mềm OpenSwan. Thực hiện tùy biến mã nguồn bộ phần mềm OpenSwan.

Chương 4 - Thử nghiệm: Trình bày thực nghiệm triển khai mô hình VPN site to site được biên dịch từ mã nguồn gốc và mã nguồn đã tùy biến của bộ phần mềm OpenSwan.

Đề tài tốt nghiệp được giao ngày 07 tháng 11 năm 2022

Yêu cầu phải hoàn thành xong trước ngày 18 tháng 2 năm 2023

Đã nhận nhiệm vụ ĐTTN

Đã giao nhiệm vụ ĐTTN

Sinh viên

Giảng viên hướng dẫn

Vũ Quốc Anh

ThS. Nguyễn Như Chiến

Hải Phòng, ngày tháng..... năm 2022

TRƯỞNG KHOA

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN TỐT NGHIỆP

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN TỐT NGHIỆP

Họ và tên giảng viên: Nguyễn Như Chiến

Đơn vị công tác: Trường Đại học Quản lý và Công nghệ Hải Phòng

Họ và tên sinh viên: Vũ Quốc Anh

Ngành: Công nghệ thông tin

Nội dung hướng dẫn: **Nghiên cứu, thử nghiệm hệ thống VPN dựa trên OpenSwan.**

1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp

Trong thời gian thực hiện đề án tốt nghiệp, sinh viên Vũ Quốc Anh đã có nhiều cố gắng, chủ động, có thái độ làm việc nghiêm túc. Mặc dù có những hạn chế nhất định về trình độ chuyên môn và đặc biệt là khoảng cách địa lý giữa sinh viên và thầy hướng dẫn nhưng sinh viên luôn tự tìm tòi, tiếp thu ý kiến thầy hướng dẫn, khảo sát thu thập tài liệu và khắc phục khó khăn để hoàn thành đề án đầy đủ các nội dung đăng ký trong đề cương và đúng tiến độ đề ra.

2. Đánh giá chất lượng của đề án/khóa luận (so với nội dung yêu cầu đã đề ra trong nhiệm vụ Đ.T. T.N trên các mặt lý luận, thực tiễn, tính toán số liệu...)

Đề án được trình bày rõ ràng trong 67 trang A4 bao gồm các ký hiệu chữ viết tắt, danh mục bảng biểu, danh mục hình vẽ, mục lục, lời nói đầu, nội dung 3 chương đề án, kết luận và tài liệu tham khảo. Nội dung đề án bảo đảm tính khoa học, chặt chẽ và logic đối với đề tài. Đề án tìm hiểu tổng quan về bộ phần mềm OpenSwan, triển khai hệ thống VPN dựa trên OpenSwan, phân tích biên dịch được mã nguồn và có thực nghiệm. Tuy nhiên phần thực nghiệm chưa kết nối được giữa hai server Hà Nội và Hải Phòng để lấy được dữ liệu thực.

3. Ý kiến của giảng viên hướng dẫn tốt nghiệp

Đạt

Không đạt

Điểm: 8,7 (tám phẩy bảy)

Hải Phòng, ngày 16 tháng 2 năm 2023

Giảng viên hướng dẫn

(Ký và ghi rõ họ tên)

ThS. Nguyễn Như Chiến

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN CHĂM PHẢN BIỆN

Họ và tên giảng viên:

Đơn vị công tác: Trường Đại Học Quản Lý và Công Nghệ Hải Phòng

Họ và tên sinh viên: Vũ Quốc Anh

Ngành: Công nghệ thông tin

Đề tài tốt nghiệp: Nghiên cứu, thử nghiệm hệ thống VPN dựa trên OpenSwan.

3. Ý kiến của giảng viên chăm phản biện

Được bảo vệ

Không được bảo vệ

Điểm:.....

Hải Phòng, ngày 25 tháng 10 năm 2022

Giảng viên chăm phản biện

(Ký và ghi rõ họ tên)

LỜI CẢM ƠN

Em xin chân thành cảm ơn tất cả các thầy, các cô trong trường Đại học Quản Lý và Công Nghệ Hải Phòng, những người đã nhiệt tình giảng dạy và truyền đạt những kiến thức quý báu trong suốt thời gian em học tập tại trường, để em có thể hoàn thành tốt đề án tốt nghiệp này.

Đặc biệt em xin chân thành cảm ơn thầy giáo ThS. Nguyễn Như Chiến, người đã trực tiếp hướng dẫn em tận tình, chỉ dạy em trong suốt quá trình làm đề án tốt nghiệp.

Tuy có nhiều cố gắng trong quá trình học tập cũng như trong thời gian thực hiện đề án tốt nghiệp nhưng không thể tránh khỏi những thiếu sót, em rất mong nhận được sự góp ý quý báu của tất cả các thầy, các cô cũng như tất cả các bạn để đề án tốt nghiệp của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng, ngày 10 tháng 12 năm 2022

Sinh viên

Vũ Quốc Anh

LỜI CAM ĐOAN

Em xin cam đoan rằng đề tài này được tiến hành một cách minh bạch, công khai. Mọi thứ được dựa trên sự cố gắng cũng như sự nỗ lực của bản thân cùng với sự giúp đỡ của thầy Nguyễn Như Chiến.

Các số liệu và kết quả nghiên cứu được đưa ra trong đề án là trung thực và không sao chép hay sử dụng kết quả của bất kỳ đề tài nghiên cứu nào tương tự. Nếu như phát hiện rằng có sự sao chép kết quả nghiên cứu đề những đề tài khác bản thân em xin chịu hoàn toàn trách nhiệm.

Hải Phòng, ngày 10 tháng 12 năm 2022

Sinh viên

(Ký và ghi rõ họ tên)

Vũ Quốc Anh

MỤC LỤC

CHƯƠNG 1. BỘ PHẦN MỀM OPENSWAN	1
1.1. Tổng quan về VPN.....	1
1.2. Các dạng VPN.....	8
1.3. Ưu điểm và nhược điểm của VPN	10
1.4. Giới thiệu về OpenSwan	10
1.5. Kết luận chương 1	17
CHƯƠNG 2. TRIỂN KHAI HỆ THỐNG VPN DỰA TRÊN OPENSWAN	18
2.1. Mô hình triển khai VPN.....	18
2.2. Cài đặt phần mềm OpenSwan.....	18
2.3. Triển khai thực nghiệm VPN Remote Access	19
2.4. Kết nối và kiểm tra kết nối.....	22
2.5. Kết luận chương 2	27
CHƯƠNG 3. PHÂN TÍCH VÀ TÙY BIẾN MÃ NGUỒN OPENSWAN	28
3.1. Cấu trúc thư mục mã nguồn	28
3.2. Phân tích các module mã nguồn bộ phần mềm OpenSwan	29
3.3. Tùy biến mã nguồn OpenSwan	30
3.4. Kết luận chương 3	35
CHƯƠNG 4. THỰC NGHIỆM.....	36
4.1. Thực nghiệm 1: Triển khai hệ thống VPN từ mã nguồn OpenSwan	36
4.2. Thực nghiệm 2: Triển khai hệ thống VPN từ mã nguồn OpenSwan đã tùy biến ...	47
4.3. Kết luận chương 4	51
KẾT LUẬN	53
TÀI LIỆU THAM KHẢO	54

DANH MỤC CHỮ VIẾT TẮT

AES	Advanced Encryption Standard
AH	Authentication Header
ATM	Asynchronous Transfer Mode
CA	Certificate Authority
CPU	Central Processing Unit
CRL	Certificate Revocation List
DC	Domain Controller
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
ESP	Encapsulation Security Payload
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HMAC	Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ICV	Integrity Check Value
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest Algorithm 5
CHAP	Challenge Handshake Authentication Protocol

MTU	Maximum Transmission Unit
NAT	Network Address Translation
OSI	Open Systems Interconnection Reference Model
PAM	Pluggable Authentication Module
PC	Personal Computer
PPTP	Point to Point Tunneling Protocol
PSK	Pre-Shared Key
RFC	Request For Comments
SA	Security Associations
SAD	Security Association Database
SHA	Secure Hash Algorithm
SKIP	Simple Key Internet Protocol
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
SPI	Security Parameter Index
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Networks

LỜI NÓI ĐẦU

Ngày nay, Internet đã phát triển mạnh về mặt mô hình cho đến công nghệ, đáp ứng các nhu cầu của người sử dụng. Internet đã được thiết kế để kết nối nhiều mạng khác nhau và cho phép thông tin chuyển đến người sử dụng một cách thuận tiện. Các thông tin trao đổi trên Internet cũng đa dạng cả về nội dung và hình thức, trong đó có rất nhiều thông tin cần bảo mật cao bởi tính kinh tế, tính chính xác và độ tin cậy của nó. Bên cạnh đó, những dịch vụ mạng ngày càng có giá trị, yêu cầu phải đảm bảo tính ổn định và an toàn cao. Tuy nhiên, các hình thức phá hoại mạng cũng trở nên tinh vi và phức tạp hơn, do đó đối với mỗi hệ thống, nhiệm vụ bảo mật đặt ra cho người quản trị là hết sức quan trọng và cần thiết.

Sự phát triển về quy mô của các công ty tổ chức cùng với việc áp dụng công nghệ thông tin vào các hoạt động đặt ra yêu cầu kết nối các chi nhánh và trung tâm thành một hệ thống duy nhất. Bên cạnh giải pháp thuê đường truyền riêng với chi phí lắp đặt và vận hành cao đó là giải pháp mạng riêng ảo (VPN - Virtual Private Network), với mô hình mới này, chúng ta không phải đầu tư thêm nhiều về cơ sở hạ tầng mà các tính năng như bảo mật và độ tin cậy vẫn được đảm bảo đồng thời có thể quản lý riêng được sự hoạt động của mạng này. VPN cho phép người sử dụng làm việc tại nhà riêng, trên đường đi hoặc các văn phòng chi nhánh có thể kết nối an toàn đến máy chủ của tổ chức bằng cơ sở hạ tầng được cung cấp bởi mạng công cộng. Nó cũng có thể đảm bảo an toàn thông tin giữa đại lý, nhà cung cấp và các đối tác kinh doanh với nhau trong môi trường truyền thông rộng lớn. Trong nhiều trường hợp VPN cũng giống như WAN (Wire Area Network), tuy nhiên đặc tính quyết định của VPN là chúng có thể dùng mạng công cộng mà vẫn đảm bảo tính riêng tư và tiết kiệm chi phí. Song song với những lợi ích mà VPN đem lại còn tồn tại những nguy cơ mất an toàn mạng, do đó phải lựa chọn ra một giải pháp phù hợp với mỗi môi trường mạng cụ thể. Hiện nay có nhiều công nghệ VPN nhưng để lựa chọn công nghệ nào tốt nhất thì rất khó vì còn tùy thuộc vào mỗi hệ thống triển khai. Nhận thấy công nghệ IPSec VPN rất hữu dụng và phù hợp với nhiều hệ thống mạng cũng như hỗ trợ nhiều thiết bị và mô hình triển khai nên em chọn làm đề tài **“Nghiên cứu, thử nghiệm hệ thống VPN dựa trên OpenSwan”** nhằm nghiên cứu về IPSec và cách thức thực hiện triển khai IPSec VPN trên Linux sử dụng sản phẩm mã nguồn mở là bộ phần mềm OpenSwan để đảm bảo an toàn mạng.

Nội dung đề án được triển khai thành bốn chương như sau:

Chương 1 - Bộ phần mềm OpenSwan: Trình bày tổng quan về VPN, giao thức IPSec VPN và giới thiệu bộ phần mềm OpenSwan: lịch sử, các thành phần của bộ phần mềm OpenSwan.

Chương 2 - Triển khai hệ thống VPN dựa trên OpenSwan: Trình bày thực nghiệm triển khai mô hình VPN Remote access dựa trên gói cài đặt bộ phần mềm OpenSwan.

Chương 3 - Phân tích và tùy biến mã nguồn OpenSwan: Trình bày về cấu trúc thư mục mã nguồn và phân tích các module của bộ phần mềm OpenSwan. Thực hiện tùy biến mã nguồn bộ phần mềm OpenSwan.

Chương 4 - Thực nghiệm: Trình bày thực nghiệm triển khai mô hình VPN site to site được biên dịch từ mã nguồn gốc và mã nguồn đã tùy biến của bộ phần mềm OpenSwan.

CHƯƠNG 1. BỘ PHẦN MỀM OPENSWAN

1.1. Tổng quan về VPN

1.1.1. Khái niệm VPN

Mạng riêng ảo là mạng sử dụng mạng công cộng (như Internet, ATM/Frame Relay của các nhà cung cấp dịch vụ) làm cơ sở hạ tầng để truyền thông tin nhưng vẫn đảm bảo là một mạng riêng và kiểm soát được truy nhập. Nói cách khác, VPN được định nghĩa là liên kết của tổ chức được triển khai trên một hạ tầng công cộng với các chính sách như là trong một mạng riêng.

1.1.2. Giao thức IPSec trong VPN

IPSec (Internet Protocol Security) là sự kết hợp của các chuẩn được định nghĩa trong RFC 2406, giao thức IPSec cho phép chứng thực, kiểm tra tính toàn vẹn dữ liệu, điều khiển truy cập và đảm bảo bí mật dữ liệu. Hoạt động tại tầng 3 của mô hình OSI.

IPSec bảo đảm tính tin cậy, tính toàn vẹn và tính xác thực của dữ liệu khi qua mạng IP (Internet Protocol) công cộng. Nó sử dụng hai giao thức để điều khiển quá trình xác thực và mã hóa tiêu đề gói IP:

- Xác thực tiêu đề AH (Authentication Header): AH đảm bảo tính toàn vẹn cho tiêu đề gói tin và dữ liệu
- Đóng gói tải tin an toàn ESP (Encapsulation Security Payload): thực hiện mã hóa và đảm bảo tính toàn vẹn cho gói dữ liệu nhưng không bảo vệ tiêu đề cho gói IP như AH.

IPsec sử dụng giao thức trao đổi khóa IKE (Internet Key Exchange) để thỏa thuận liên kết an toàn SA (Security Association) giữa hai thực thể và trao đổi các thông tin khóa. IKE cần được sử dụng phần lớn trong các ứng dụng thực tế để đem lại sự truyền tải thông tin an toàn trên diện rộng.

1.1.2.1. Cấu trúc bảo mật của IPSec

IPSec là một kiến trúc an toàn dựa trên chuẩn mở, nó có các đặc trưng sau:

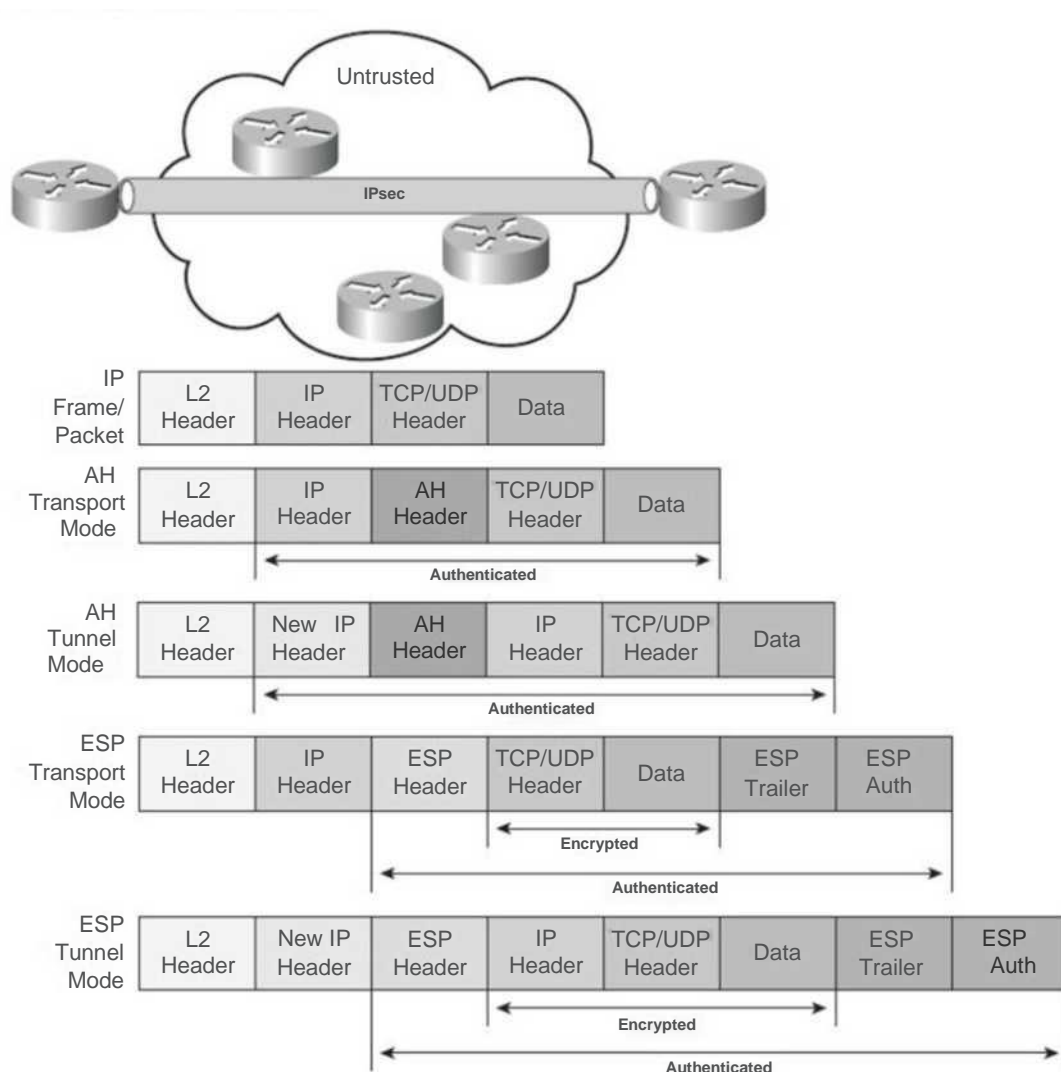
- Cung cấp tính xác thực, mã hóa, toàn vẹn dữ liệu và bảo vệ sự phát lại.
- Cung cấp khả năng tạo và tự động làm mới các khóa mật mã một cách an toàn.
- Sử dụng các thuật toán mật mã mạnh để cung cấp tính bảo mật.
- Cung cấp khả năng xác thực dựa trên chứng thư số.
- Điều chỉnh các thuật toán mật mã và các giao thức trao đổi khóa.
- Cung cấp tính năng an toàn cho các giao thức đường hầm truy cập từ xa như L2TP, PPTP.

IPSec là một phần bắt buộc của IPv6, có thể được lựa chọn khi sử dụng IPv4. Trong khi các chuẩn đã được thiết kế cho các phiên bản IP giống nhau, phổ biến hiện nay là áp dụng và triển khai trên nền tảng IPv4. IPSec được định nghĩa

từ RFC 1825 đến 1829 và được phổ biến vào năm 1995. Năm 1998, được nâng cấp với các phiên bản RFC 2401-2412, nó không tương thích với chuẩn 1825-1829. Trong tháng 12 năm 2005, thế hệ thứ ba của IPSec được mô tả trong RFC 4301-4309.

1.1.2.2. Chế độ làm việc của IPSec

IPSec có 2 chế độ làm việc là giao vận (transport) và đường hầm (tunnel). 2 chế độ làm việc này được chỉ ra trong Hình 1.1: sau:



Hình 1.1: Xử lý gói tin IP ở chế độ giao vận và chế độ đường hầm

a. Chế độ giao vận (Transport Mode)

Chế độ giao vận cho phép bảo vệ các giao thức lớp trên và một số trường trong IP Header. Trong chế độ này, AH Header hoặc ESP Header được chèn vào sau IP Header và trước một giao thức lớp trên như TCP hoặc UDP. Chế độ giao vận thường được sử dụng bởi các Host chứ không được sử dụng bởi Gateway.

Chế độ giao vận có ưu điểm là chỉ thêm vào gói IP ban đầu một số ít bytes, nhược điểm của chế độ này là nó cho phép các thiết bị trong mạng nhìn thấy địa chỉ nguồn và đích của gói tin và có thể thực hiện một số xử lý (ví dụ như

phân tích lưu lượng) dựa trên thông tin của tiêu đề IP. Tuy nhiên, nếu dữ liệu được mã hóa bởi ESP thì sẽ không biết được thông tin cụ thể bên trong gói IP là gì. Theo IETF thì chế độ giao vận chỉ có thể được sử dụng khi hai hệ thống đầu cuối IP-VPN có thực hiện IPSec.

b. Chế độ đường hầm (Tunnel Mode)

Trong chế độ đường hầm, một gói tin IP khác được thiết lập dựa trên gói tin IP cũ. Header của gói IP cũ mang địa chỉ nguồn và đích cuối cùng, còn Header của gói IP mới mang địa chỉ để định tuyến trên Internet. Trong chế độ này, gói tin được bảo vệ toàn bộ bao gồm cả IP Header.

Ưu điểm của chế độ đường hầm là bảo vệ toàn bộ gói IP và các địa chỉ cá nhân trong IP Header, nhược điểm là việc xử lý các gói tin sẽ trở nên khó khăn hơn.

1.1.2.3. Các thành phần bên trong IPSec

a. Giao thức xác thực tiêu đề AH

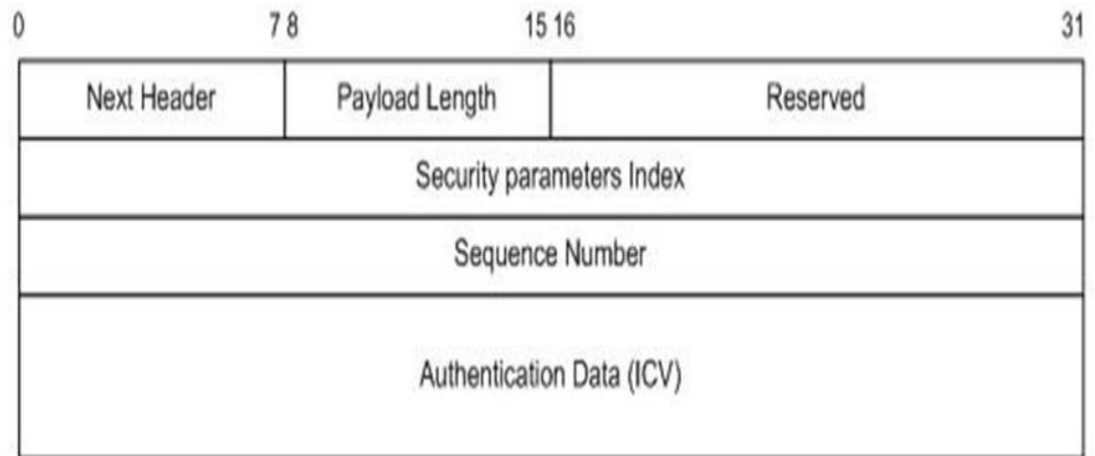
Giao thức xác thực tiêu đề AH sẽ thêm một tiêu đề vào gói IP. Như tên gọi của nó, tiêu đề này phục vụ cho việc xác thực gói dữ liệu IP gốc tại người nhận cuối cùng, tiêu đề này giúp nhận biết bất kỳ sự thay đổi nào về nội dung của gói dữ liệu bởi người dùng không mong muốn trong khi truyền, tuy nhiên AH không đảm bảo tính tin cậy.

Để tạo một AH, một giá trị mã thông điệp cần xác thực qua hàm băm (HMAC) được tạo tại người gửi. Giá trị băm này được tạo trên cơ sở của SA, SA xác định trình tự giao dịch sẽ được áp dụng cho gói dữ liệu. Mã kết quả được gắn kèm vào gói dữ liệu sau tiêu đề IP gốc. Tại người nhận cuối, HMAC được giải mã và được dùng để thiết lập việc xác thực người gửi cũng như tính toàn vẹn của thông điệp.

AH không mang lại sự tin cậy trong một giao dịch. Nó chỉ thêm một tiêu đề vào gói IP, phần còn lại của nội dung gói dữ liệu không được can thiệp đến. Hơn nữa, AH không bảo vệ bất kỳ trường nào trong tiêu đề IP vì một trong số đó có thể thay đổi trong quá trình truyền, chỉ có địa chỉ IP nguồn và địa chỉ IP đích là những trường mà không thay đổi trong quá trình truyền được bảo vệ bởi AH. Giao thức AH có các đặc trưng cơ bản như sau:

- Cung cấp tính toàn vẹn dữ liệu và bảo vệ chống phát lại
- Sử dụng mã xác thực thông điệp được băm (HMAC), dựa trên chia sẻ bí mật
- Nội dung các gói tin không được mã hoá
- Không sử dụng các trường changeable IP header để tính toán giá trị kiểm tra tính toàn vẹn (IVC)

AH Header bao gồm các trường như trong Hình 1.2 sau:



Hình 1.2: Các trường trong AH Header

- Next Header: Trường này dài 8 bits, chứa chỉ số giao thức IP
 - + Trong chế độ đường hầm, Payload là gói tin IP, giá trị Next Header được cài đặt là 4.
 - + Trong chế độ giao vận, Payload luôn là giao thức ở Transport Layer. Nếu giao thức lớp Transport là TCP thì trường giao thức trong IP là 6. Nếu giao thức lớp transport là UDP thì trường giao thức trong IP là 17.
- Payload Length: Trường này chứa chiều dài của AH Header.
- Reserved: Giá trị này được dành để sử dụng trong tương lai(cho đến thời điểm này nó được biểu thị bằng các chỉ số 0).
- Security Parameters Index (SPI): Mỗi đầu cuối của một kết nối IPSec tùy ý chọn giá trị SPI. Hoạt động này chỉ được dùng để nhận dạng cho kết nối. Bên nhận sử dụng giá trị SPI cùng với địa chỉ IP đích và loại giao thức IPSec (trong trường hợp này là AH) để xác định chính sách liên kết an toàn SA được dùng cho gói tin.
- Sequence Number: Chỉ số này tăng lên 1 cho mỗi AH Datagram khi một host gửi có liên quan đến chính sách SA. Giá trị bắt đầu của bộ đếm là 1, chuỗi số này không bao giờ được phép ghi đè lên là 0.
- Authentication Data: Trường này chứa giá trị ICV (Integrity Check Value). Trường này luôn là bội của 32-bit và phải được đệm vào nếu chiều dài của ICV trong các bytes chưa đầy.

b. Giao thức trao đổi khóa IKE (Internet Key Exchange)

Trong IPSec sử dụng giao thức trao đổi khóa IKE (Internet Key Exchange). Giao thức IKE được thiết kế ra để cung cấp 5 khả năng:

- Cung cấp những phương tiện cho hai bên về sự thống nhất những giao thức,

thuật toán và những khoá để sử dụng.

- Đảm bảo trao đổi khoá đến đúng người dùng.
- Quản lý khoá sau khi được chấp nhận.
- Đảm bảo rằng sự điều khiển và trao đổi khoá là an toàn.
- Cho phép sự chứng thực động giữa các đối tượng ngang hàng.

Giao thức IKE có các đặc tính sau:

- Các khoá tự phát sinh và những thủ tục nhận biết.
- Tự động làm mới lại khoá.
- Giải quyết vấn đề một khoá.
- Mỗi một giao thức an toàn (AH, ESP) có một không gian chỉ số an toàn của chính mình.
- Gắn sẵn sự bảo vệ.

Trước khi IPSec gửi xác nhận hoặc mã hoá dữ liệu IP, giữa bên gửi và bên nhận phải thống nhất về giải thuật mã hoá và khoá mã hoá hoặc những khoá để sử dụng. IPSec sử dụng giao thức IKE để tự thiết lập những giao thức đàm phán về những khoá sử dụng cho việc mã hoá, thuật toán sử dụng.

- Liên kết an toàn SA (Security Association)

Dịch vụ bảo mật liên kết giữa hai hay nhiều thực thể để thỏa thuận truyền thông an toàn được gọi là liên kết an toàn SA (Security Association).

Liên kết an toàn là một kết nối đơn hướng, nghĩa là với mỗi cặp truyền thông A và B nào đó có ít nhất hai SA (một từ A tới B và một từ B tới A). Khi lưu lượng cần truyền trực tiếp hai chiều qua VPN, giao thức trao đổi khóa IKE thiết lập một cặp SA trực tiếp và sau đó có thể thiết lập thêm nhiều SA khác, mỗi SA có một thời gian sống riêng. SA được nhận dạng duy nhất bởi ba thành phần gồm có:

- + Chỉ số thông số an toàn SPI (Security Parameters Index)
- + Địa chỉ IP đích
- + Chỉ thị giao thức an toàn (AH hay ESP)

Về nguyên tắc, địa chỉ IP đích có thể là một địa chỉ đơn hướng (Unicast), địa chỉ quảng bá (Broadcast) hoặc địa chỉ nhóm (Multicast). Tuy nhiên, cơ chế quản lý SA của IPSec hiện nay chỉ được định nghĩa cho những SA đơn hướng.

Liên kết an toàn cũng có hai kiểu là giao vận và đường hầm, phụ thuộc vào giao thức sử dụng. SA kiểu giao vận là một liên kết an toàn giữa hai trạm hoặc được yêu cầu giữa hai hệ thống trung gian dọc trên đường truyền. Trong trường hợp khác, SA kiểu giao vận cũng có thể được sử dụng để hỗ trợ IP-in-IP hay đường hầm GRE. SA kiểu đường hầm là một SA cơ bản được ứng dụng tới một đường hầm IP. SA giữa hai cổng an toàn là một SA kiểu đường hầm điển hình, giống như một SA giữa một trạm và một cổng an toàn. Tuy nhiên trong

những trường hợp mà lưu lượng đã được định hình từ trước như những lệnh SNMP, công an toàn làm nhiệm vụ như trạm và kiểu giao vận được cho phép.

- Cơ sở dữ liệu liên kết an toàn

Có hai cơ sở dữ liệu liên quan đến an toàn là:

- + Cơ sở dữ liệu chính sách an toàn SPD (Security Policy Database)
- + Cơ sở dữ liệu liên kết an toàn SAD (Security Association Database)

SPD chỉ ra những dịch vụ an toàn được đề nghị cho lưu lượng IP, phụ thuộc vào những yếu tố như nguồn, đích, chiều đi ra hay đi vào. Nó chứa đựng một danh sách những lối vào chính sách tồn tại riêng rẽ cho lưu lượng đi vào và đi ra. Các lối vào này có thể xác định một vài lưu lượng không qua xử lý IPSec, một vài phải được loại bỏ và còn lại thì được xử lý bởi IPSec. Các lối vào này là tương tự như firewall hay bộ lọc gói.

SAD chứa thông số về mỗi SA bao gồm khóa AH hay ESP, số trình tự, kiểu giao thức và thời gian sống của SA. Đối với xử lý đi ra, một lối vào SPD trở tới một lối vào trong SAD và SAD sẽ quyết định SA nào được sử dụng cho gói. Đối với xử lý đi vào, SAD được tham khảo để quyết định gói được xử lý tiếp.

- Hoạt động trao đổi khóa IKE

Kết nối IPSec chỉ được hình thành khi SA đã được thiết lập. Tuy nhiên, bản thân IPSec không có cơ chế để thiết lập liên kết an toàn. Chính vì vậy, IETF đã chọn phương án chia quá trình thiết lập kết nối IPSec ra thành hai phần:

- + IPSec cung cấp việc xử lý ở mức gói.
- + IKMP (Internet Key Management Protocol) chịu trách nhiệm thoả thuận các liên kết an toàn.

Sau khi cân nhắc một số phương án, trong đó có IKE, SKIP (Simple Key Internet Protocol) và Photuis, IETF đã quyết định chọn IKE là chuẩn để cấu hình SA cho IPSec.

Một đường hầm IPSec-VPN được thiết lập giữa hai bên qua các bước sau đây:

Bước 1: Quyết định lưu lượng nào cần được quan tâm bảo vệ tại một giao diện yêu cầu thiết lập phiên thông tin IPSec.

Bước 2: Thương lượng chế độ chính (Main mode) hoặc chế độ linh hoạt (Aggressive mode) sử dụng IKE, kết quả là tạo ra liên kết an toàn IKE (IKE SA) giữa các bên IPSec.

Bước 3: Thương lượng chế độ nhanh (Quick mode) sử dụng IKE, kết quả là tạo ra hai IPSec SA giữa các bên IPSec.

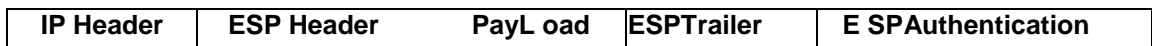
Bước 4: Dữ liệu bắt đầu truyền qua đường hầm mã hóa sử dụng kỹ thuật đóng gói ESP hay AH hoặc cả hai.

Bước 5: Kết thúc đường hầm IPSec-VPN (nguyên nhân có thể là do IPSec SA kết thúc, hết hạn hoặc bị xóa).

c. Giao thức đóng gói tải tin an toàn ESP

Mục đích chính của ESP là cung cấp sự tin cậy thêm vào xác thực người gửi và xác minh tính toàn vẹn của dữ liệu trong khi truyền. ESP mã hoá nội dung của gói dữ liệu bằng cách dùng các thuật toán mã hoá, như đã xác định bởi SA. Một số thuật toán được sử dụng bởi ESP bao gồm: thuật toán DES-CBC, thuật toán CAST-128, thuật toán IDEA và thuật toán 3DES, thuật toán AES, ... Các thuật toán xác thực thường được dùng tương tự như trong AH là HMAC - MD5 và HMAC-SHA.

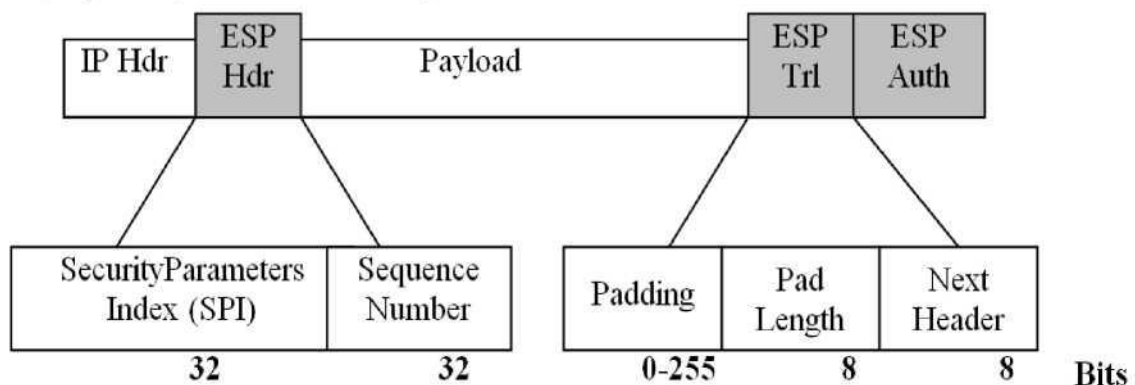
Như đã so sánh, AH mang lại tính xác thực và toàn vẹn dữ liệu đối với gói dữ liệu IP. ESP rất mạnh trong nhóm mã hoá. Nó cũng không chiếm dụng nhiều CPU. Kết quả là nó nhanh hơn AH. Nhưng 24 byte mà nó thêm vào gói dữ liệu có thể làm chậm việc phân đoạn về tính toán thông lượng như trong Hình 1.3 gói tin IP sau khi đã mã hóa.



Hình 1.3: Gói tin IP sau khi tiêu đề ESP và Trailer ESP được thêm vào

- Khuôn dạng gói dữ liệu ESP

Khuôn dạng của gói ESP phức tạp hơn so với khuôn dạng của AH, nó không chỉ gồm ESP header mà còn ESP trailer và ESP Authentication data. Dữ liệu Payload được đặt giữa ESP Header và ESP Trailer như trong Hình 1.4



Hình 1.4: Khuôn dạng gói ESP

Các trường trong ESP:

- + Security Parameters Index (SPI): Là một số 32 bit bất kỳ, cùng với địa chỉ IP đích và giao thức an toàn, ESP cho phép nhận dạng duy nhất SA của gói dữ liệu này. Giá trị SPI = 0 để chỉ ra chưa có SA nào tồn tại.
- + Sequence Number: Giống như AH, trường sequence number chứa một giá trị đếm tăng dần để chống lặp lại. Mỗi SA được lựa chọn thì giá trị của trường này bắt đầu là 0.
- + Payload Data: Trường có độ dài biến đổi chứa dữ liệu mô tả trong Next Header. Payload Data là trường bắt buộc và được mã hoá bởi các thuật toán mã hoá, các thuật toán mã hoá này được lựa chọn ngay

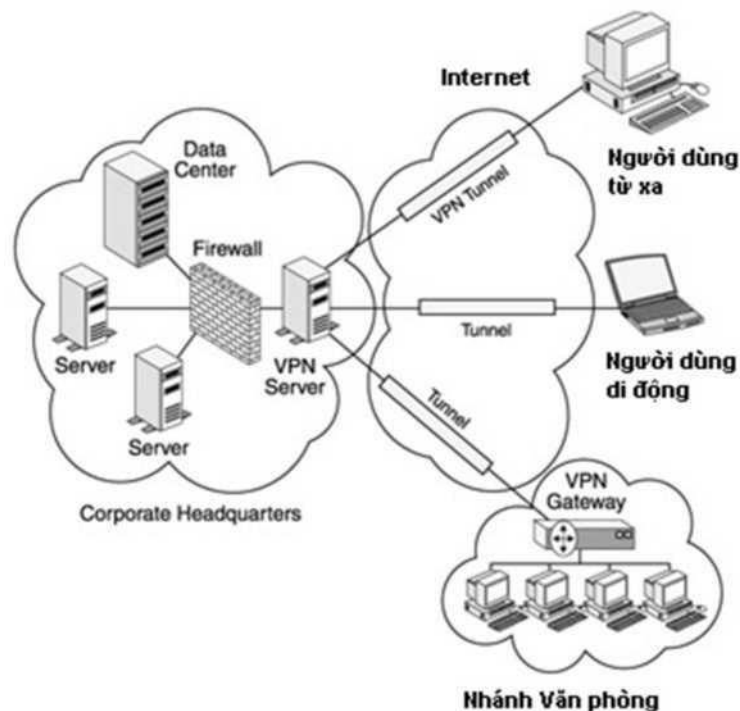
khi thiết lập SA. Trường Next Header có độ dài bằng một số nguyên lần 1 byte.

- + Padding: Trường padding được thêm vào để đoạn dữ liệu được mã hoá là một số nguyên lần của một khối các byte. Ngoài ra trường còn dùng để che dấu độ dài thực của Payload.
- + Pad Length: Xác định số byte padding đã thêm vào (0 đến 225)
- + Next Header: Là trường 8 bit bắt buộc, nó chỉ ra kiểu dữ liệu trong Payload Data.
- + Authentication Data: Trường có độ dài biến đổi chứa giá trị ICV được tính cho gói ESP từ SPI đến Next Header. Authentication là trường không bắt buộc, được thêm vào nếu dịch vụ Authentication được lựa chọn cho SA đang xét. Các thuật toán để tính ICV là các thuật toán hàm băm một chiều MD5 hoặc SHA giống với AH.

1.2. Các dạng VPN

1.2.1. VPN Remote Acces

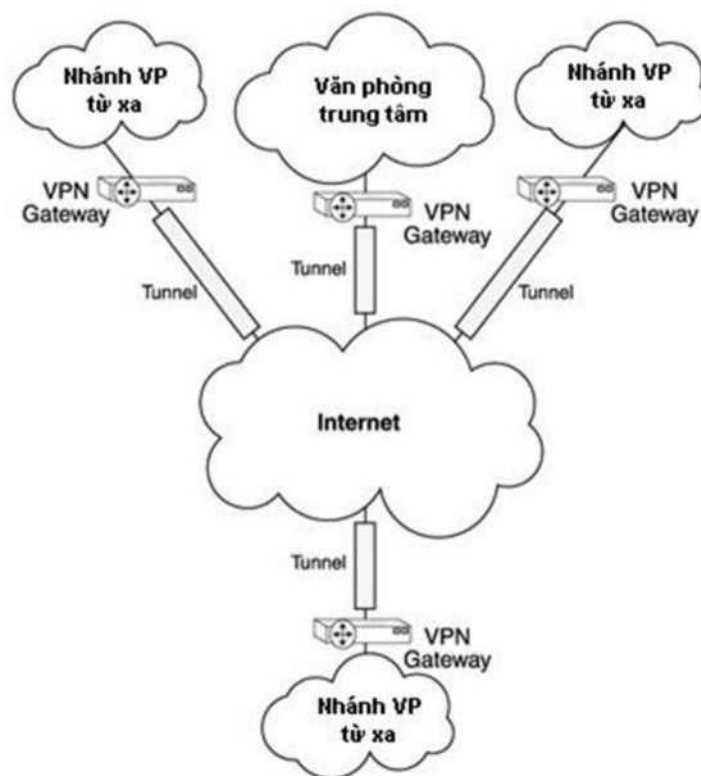
VPN Remote Access cho phép người dùng truy cập bất cứ lúc nào bằng remote, mobile, và các thiết bị truyền thông của nhân viên các chi nhánh kết nối đến tài nguyên mạng của công ty. Đặc biệt là những người dùng thường xuyên di chuyển hoặc các chi nhánh văn phòng nhỏ mà không có kết nối thường xuyên đến mạng Intranet của công ty. Nhằm đáp ứng nhu cầu truy cập dữ liệu và ứng dụng cho người dùng ở xa, bên ngoài công ty thông qua Internet. Ví dụ khi người dùng muốn truy cập vào cơ sở dữ liệu hay các máy chủ file, gửi nhận email từ các máy chủ mail nội bộ của công ty.



Hình 1.5: Mô hình VPN Remote Access

1.2.2. VPN Intranet

VPN Intranet hay còn gọi là VPN cục bộ là một mô hình tiêu biểu của VPN Site-to-Site, mô hình kết nối này được sử dụng để tạo liên kết bảo mật giữa các địa điểm khác nhau của một công ty hay doanh nghiệp. Nó liên kết trụ sở chính với các văn phòng chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối riêng nhưng luôn được mã hóa bảo mật. Điều này cho phép tất cả các điểm có thể truy nhập an toàn các nguồn dữ liệu được phép trong toàn công ty như trong Hình 1.6 dưới đây:

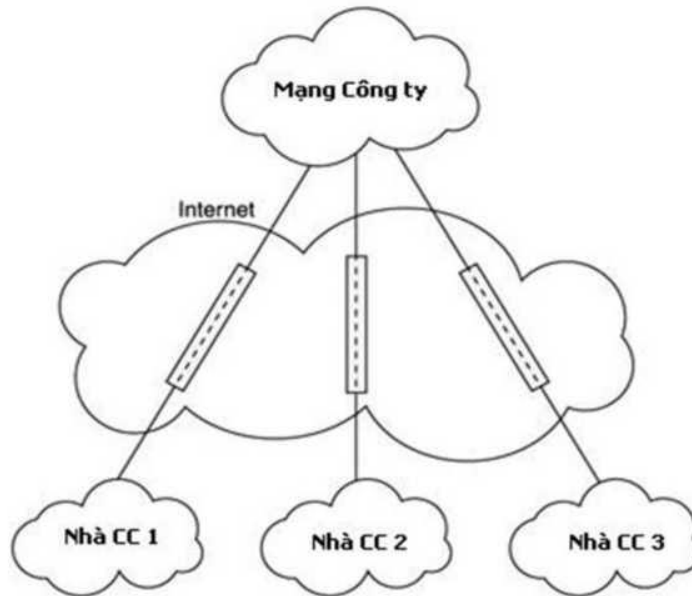


Hình 1.6: Mô hình VPN Intranet

VPN Intranet cung cấp những đặc tính của mạng WAN như khả năng mở rộng, tính tin cậy và hỗ trợ nhiều kiểu giao thức khác nhau với chi phí thấp nhưng vẫn đảm bảo tính mềm dẻo.

1.2.3. VPN Extranet

VPN Extranet liên kết các khách hàng, các nhà cung cấp, hay cộng đồng người sử dụng vào mạng Intranet của một tổ chức trên nền hạ tầng mạng công cộng sử dụng các đường truyền thuê bao như trong Hình 1.7



Hình 1.7: Mô hình VPN Extranet

Giải pháp này cũng cung cấp các chính sách như trong mạng riêng của một tổ chức nhưng đảm bảo tính bảo mật, tính ổn định. VPN Extranet thường sử dụng các kết nối dành riêng và thêm vào các lớp bảo mật để xác thực và giới hạn truy cập trên hệ thống.

1.3. Ưu điểm và nhược điểm của VPN

1.3.1. Ưu điểm

- Chi phí để triển khai thấp.
- Tính bảo mật cao với việc sử dụng các giao thức xác thực và mã hóa dữ liệu
- Tính mở rộng và linh hoạt trong kết nối.
- Hỗ trợ nhiều giao thức.
- Giảm chi phí vận hành quản lý, thiết lập, nâng cao kết nối, bảo mật, nâng cấp dễ dàng, hiệu suất băng thông.

1.3.2. Nhược điểm

- Phụ thuộc nhiều vào chất lượng mạng công cộng (Internet). Dẫn đến việc gói tin có thể được gửi đi chậm hoặc thất thoát trong quá trình truyền tin.
- Phụ thuộc vào nhà cung cấp dịch vụ ISP.
- Do độ phức tạp của các thuật toán mã hoá sẽ gây những khó khăn cho quá trình xác thực. Thêm vào đó, việc nén dữ liệu diễn ra chậm chạp. Do phải truyền dữ liệu thông qua Internet, nên khi trao đổi các dữ liệu lớn như các gói dữ liệu truyền thông, phim ảnh, âm thanh sẽ rất chậm.

1.4. Giới thiệu về OpenSwan

OpenSwan là phần mềm mã nguồn mở dùng triển khai IPSec VPN dựa

trên giao thức IPsec chuẩn RFC 2401. Được hỗ trợ trên nhiều bản phân phối linux khác nhau: Red Hat, Debian, SuSE, Slackware và Gentoo, v.v. Nó là một nhánh mở của dự án FreeS/WAN. Dự án FreeS/WAN được thành lập bởi doanh nhân John Gilmore, là dự án đầu tiên thực hiện IPsec trong mã nguồn mở cụ thể là trong hệ điều hành Linux.

OpenSwan hỗ trợ cho hầu hết các phần mở rộng (RFC + dự thảo IETF) liên quan đến IPsec, bao gồm các giao thức IKEv2, chứng thư số X.509, NAT Traversal, v.v.

1.4.1. Lịch sử của OpenSwan

Trong khi IETF vẫn đang trong quá trình thiết kế giao thức IPsec, doanh nhân John Gilmore đã thu nhập dự án FreeS/WAN. FreeS/WAN đứng thế cho mạng diện rộng bảo mật. Mục tiêu cuối cùng của dự án là làm cho IPsec trở thành chế độ hoạt động mặc định cho toàn bộ Internet. Phiên bản 1.0 đã được phát hành cho Linux vào tháng 4 năm 1999 dưới giấy phép GPL và làm việc trên nhân Linux 2.0.36.

Tháng 9 năm 2000, Ken Bantoft đã tạo ra Super FreeS/wan để cung cấp một phiên bản vá của FreeS/wan dễ sử dụng mà trong đó đã có tất cả các tính năng cần thiết cho người dùng VPN và có khả năng tương thích.

Mùa hè năm 2003, các tình nguyện viên Châu Âu và một số thành viên của dự án FreeS/wan dẫn đầu bởi Pau Wouters đã gặp và nói chuyện với John Gilmore tại trại hè Chaos Computer Club gần Berlin trên cơ sở đó tháng 11 năm 2003 Openswan được phát hành bởi Xelerance, một công ty mới thành lập cho việc tiếp tục phát triển của một thực hiện IPsec miễn phí cho Linux. Dự án đã được công bố và phiên bản cuối cùng của Free/WAN, với sự hỗ trợ Klips cho nhân Linux 2.6, đã được phát hành.

Phiên bản mới nhất của Openswan là 2.6.48 phát hành vào ngày 06 tháng 06 năm 2016.

1.4.2. Thành phần của OpenSwan

1.4.2.1. Pluto

Openswan có daemon IKE linh hoạt và tính năng phong phú nhất được gọi là Pluto. Mặc cho mọi người có thể dễ dàng bị nhầm lẫn khi đọc các log messages, nhưng Pluto vẫn cực kỳ chính xác. Nó thậm chí còn được sử dụng như một tài liệu tham khảo khi thực hiện thử nghiệm daemon IKE thương mại hóa.

Mỗi đêm, các dự án Openswan chạy một bộ kiểm tra hồi quy hằng đêm trên tất cả các mã, bao gồm Pluto. Nếu một thay đổi mã phá vỡ bất kỳ chức năng nào nó sẽ tự động báo cáo vào ngày hôm sau trên danh sách gửi thư hằng đêm. Ngoài ra còn có các bài kiểm tra xem gói tin cần phải được giảm đã thực sự bị giảm hay chưa, các bài kiểm tra khác về chứng nhận X.509, chuỗi CA không an toàn, chức năng NAT Traversal, phát hiện Peer Dead và nhiều thử nghiệm khác. Các bộ kiểm tra được vận chuyển với mã nguồn trong các thư mục con thử nghiệm, bất cứ ai cũng có thể chạy các phần mềm thử nghiệm trên hệ thống của mình và nó là một công cụ rất hữu ích nếu người sử dụng đang viết các bản vá lỗi của riêng mình hoặc mở rộng cho Openswan. Pluto có tính năng khởi động lại mạnh mẽ trong trường hợp thất bại bất ngờ. Bằng cách này, một lỗi duy nhất mà có xảy ra Pluto sẽ không tải lại toàn bộ mạng của người dùng.

Pluto có chức năng trao đổi, thiết lập kênh an toàn với nhiều tính năng thực hiện:

- Đơn giản hóa các phương thức nâng cao cho các cấu hình của đường hầm.
- Tuân theo RFC (AH, ESP, transport và tunnel mode).
- Hỗ trợ NAT-Traversal.
- Opportunistic Encryption (dựa trên khóa công khai trong DNS/DNSSEC) với DHCP tích hợp.
- Hỗ trợ RoadWarrior nâng cao (client trên IP động).
- Khả năng thực thi các scripts tùy biến trên một cơ sở cho mỗi người dùng hoặc mỗi đường hầm.
- Khóa RSA sig (khóa công khai được quy định trực tiếp).
- Sử dụng chứng thư số X.509, CAs, và xử lý CA trung gian.
- Certificate Revocation List (CRL) - danh sách thu hồi chứng thư động được truy xuất bằng cách sử dụng FTP, HTTP, hoặc LDAP.
- Phát hiện kết nối ngang hàng bị chết (Dead Peer Detection).
- XAUTH - Extended Authentication: hỗ trợ xác thực máy chủ và máy khách.
- Hỗ trợ chế độ Aggressive tương thích.
- Hỗ trợ ModeConfig.
- Hỗ trợ xác thực tập trung PAM - Pluggable Authentication Module.
- Hỗ trợ giao thức L2TP trên Windows.
- Smartcard và phần cứng khác hỗ trợ token (Secure ID, eToken, ...).

- Hỗ trợ cho việc triển khai quy mô lớn (hàng ngàn đường hầm đồng thời trên phần cứng PC).
- Mã nguồn là rất linh hoạt được chuyển trên nhiều nền tảng Linux (MIPS, ARM, Sparc, Alpha) từ Linux 2.0 đến 2.6, và Windows 2000 / XP.
- Làm việc với nhiều loại IPsec stack (Klips và Netkey).

Pluto hoạt động như IKE. Pluto chạy như một daemon trên một nút mạng. Hiện nay, nút mạng này phải có một hệ thống Linux chạy Klips hoặc Netkey của IPsec, hoặc một FreeBSD/NetBSD/MacOSX chạy KAME của IPsec.

Thực thi IKE trên một nút mạng cụ thể, giao tiếp với một thực thể IKE khác sử dụng gói tin UDP, vì vậy phải có một tuyến giữa các nút cho mỗi hướng. IKE có thể được triển khai trên một nút mạng để đàm phán SA cho nút mạng đó. IKE tạo ra một đường hầm xác thực và mã hóa sau đó là thỏa thuận SA cho IPsec, các thông số SA này sẽ được lưu trong cơ sở dữ liệu của SA là SAD.

Một IPsec SA dùng 2 cơ sở dữ liệu. Security Association Database (SAD) nắm giữ thông tin 1 liên quan đến mỗi SA. Thông tin này bao gồm thuật toán khóa, thời gian sống của SA, và chuỗi số tuần tự cơ sở dữ liệu thứ hai của IPsec SA, Security Policy Database (SPD), nắm giữ thông tin về các dịch vụ bảo mật kèm theo với một danh sách thứ tự chính sách các điểm vào và ra. Giống như firewall rules và packet filters. Các thực thể này định nghĩa lưu lượng nào phải được xử lý và lưu lượng nào bị bỏ qua theo từng chuẩn của IPsec.

1.4.2.2 Klips

Klips lần đầu tiên có trong IPsec stack cho Linux. Các phiên bản ban đầu chạy trên Linux 2.0 và các phiên bản mới nhất đã được hỗ trợ trên Linux 2.2 cho đến Linux 2.6. Nó được sử dụng duy nhất cho Linux Ipsec Stack trong hơn một năm.

Klips được viết lại giữa phiên bản FreeS/WAN 1.99 và phiên bản 2.x. Một số chức năng của nó được phát triển mạnh đến nay và được tái cấu trúc. Các mã 2.x cũng giới thiệu hệ thống kiểm tra hồi quy (regression). Mỗi một tính năng của Klips đều được kiểm tra trong các bài kiểm tra nightly regression. Các phiên bản 2.x còn là cơ sở cho OpenSwan 2.x.

Klips có chức năng thực hiện việc mã hóa các gói IP theo công nghệ IPsec.

a. IPsecX interface.

Kể từ khi Klips có sẵn các mã netfilter trong nhân Linux, nó đã tìm ra một cách mới để móc nối vào các hạt nhân và các mạng lưới stack. Các giải pháp tạo

ra các thiết bị ảo, các thiết bị IPsecX, và áp dụng một thủ thuật định tuyến để gửi các gói tin vào các thiết bị ảo. Ưu điểm là lưu lượng của gói tin rất rõ ràng. Một gói tin đã được mã hóa đi vào các thiết bị ethX. Nó phát hiện ra rằng đây là một gói IPsec, và nó được gửi đến các mã Klips để được xử lý. Klips giải mã gói tin, và đặt các gói giải mã trên thiết bị ipsecX. Như vậy, các gói tin sẽ đi qua tất cả các Linux iptables trên mỗi một interface, cho phép các luật tường lửa riêng biệt được thực hiện cho mã hóa và giải mã các gói tin. Điều này làm cho các luật tường lửa được viết rất dễ dàng và được coi là một trong những tính năng chính của Klips.

b. First Packet Caching.

Một tính năng quan trọng là bộ nhớ đệm (Caching) của các gói dữ liệu mạng khi mà một đường hầm PS được tạo ra. Bởi vì với bộ nhớ đệm này, đường hầm có thể dễ dàng được thiết lập bật và tắt mà không có bất kỳ mất mát nào về gói tin. Vì vậy mà việc mất mát gói tin không còn là vấn đề đáng lo ngại, nhưng hãy chú ý nếu mất đi một vài gói tin đầu sẽ dẫn đến một sự chậm trễ đáng kể.

c. Path MTU Discovery

Một tính năng khác của Klips là nó hỗ trợ đầy đủ Path MTU Discovery (RFC 1191). Path MTU Discovery mô tả một phương pháp để xác định đơn vị truyền tối đa (MTU) của một gói tin.

Path MTU Discovery (PMTUD) là một kỹ thuật được tiêu chuẩn hóa về mạng máy tính để xác định kích thước đơn vị truyền tải tối đa (MTU) trên mạng giữa hai giao thức Internet (IP) của các hosts với nhau, thông thường với mục tiêu tránh phân mảnh gói IP. PMTUD ban đầu được dành cho các bộ định tuyến trong Internet Protocol Version 4 (IPv4). Tuy nhiên, hiện nay tất cả các hệ điều hành hiện đại đã sử dụng nó trên các thiết bị đầu cuối.

Path MTU Discovery tìm ra kích thước lớn nhất của gói tin mà có thể được xử lý bởi tất cả các router trung gian giữa hai máy tính. Máy tính khởi tạo sẽ bắt đầu gửi các gói tin nhỏ, nhưng một khi nó đã được nhận một cách chính xác ở phía bên kia, thì nó sẽ tăng dần kích thước gói tin. Tại một điểm nào đó, hoặc là điểm kết thúc, hoặc là một máy ở giữa mà đang chuyển tiếp các gói tin, sẽ có một gói tin không thể gửi xa hơn được nữa bởi vì nó quá lớn. Nó sẽ drop gói tin và gửi lại một thông báo cho máy chủ đang gửi tin. Đây là một gói ICMP “Destination Unreachable” (không thể gửi tới đích), trong đó có chứa một thông điệp “Datagram Too Big” (gói dữ liệu quá lớn). Tại Máy gửi sẽ nhận được gói tin

ICMP đó, nó đọc giá trị 'Next-Hop MTU', và sử dụng gói tin có kích thước nhỏ hơn để thay thế.

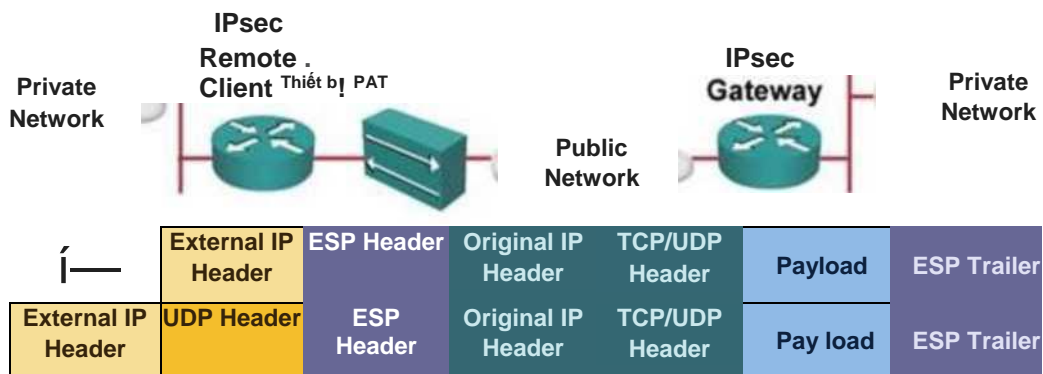
d. NAT Traversal

Đây là một trường hợp đặc biệt của NAT động, NAT traversal được sử dụng trong Linux. Với NAT traversal nhiều địa chỉ IP được ẩn đi dưới một địa chỉ duy nhất, nó tương phản với NAT động, chỉ có một kết nối cho một IP duy nhất tại một thời điểm. Trong NAT traversal nhiều kết nối đến cùng một IP sẽ được phân chia thông qua TCP Port.

NAT traversal còn được gọi là UDP đóng gói lưu lượng truy cập để có thể đến đích chỉ định khi một thiết bị không có một địa chỉ công cộng. Điều này thường là trường hợp nếu ISP đóng vai trò như NAT, hoặc các giao diện bên ngoài của tường lửa được kết nối với một thiết bị có kích hoạt NAT.

Cũng như IPSec cung cấp bảo mật, NAT traversal cũng cung cấp tính xác thực và toàn vẹn. Địa chỉ nhúng của máy chủ trong IP Payload không phù hợp với địa chỉ nguồn của gói tin IKE khi đó nó được thay thế bằng địa chỉ của thiết bị NAT. Điều này có nghĩa là phá vỡ tính xác thực. Vì vậy, khi các thiết bị NAT làm thay đổi các gói dữ liệu điều đó sẽ gây mất tính toàn vẹn và xác thực.

Trong một số trường hợp tùy thuộc vào mức độ mã hóa, lưu lượng và đặc biệt là các tiêu đề được mã hóa khi sử dụng ESP trong IPSec. Các thiết bị NAT không thể thay đổi các tiêu đề được mã hóa đến các địa chỉ riêng của mình. Trong khi đó, các thiết bị NAT ở giữa phá vỡ tính xác thực, tính toàn vẹn và trong một số trường hợp không thể làm bất cứ điều gì ở tất cả các gói tin. Rõ ràng các thiết bị NAT và IPSec là không tương thích với nhau, và để giải quyết vấn đề này NAT traversal đã được phát triển NAT traversal sẽ thêm một tiêu đề UDP mà gói gọn tiêu đề IPSec ESP bên trong. Nhưng gói UDP mới này là không được mã hóa và được coi là giống như một gói tin UDP bình thường, các thiết bị NAT có thể thực hiện các thay đổi cần thiết và xử lý gói tin. NAT traversal trên cũng giải quyết việc kiểm tra tính xác thực và toàn vẹn được chỉ ra trong Hình 1.8



Hình 1.8: NAT Traversal giúp hỗ trợ các gói tin đã được mã hoá có thể đi qua các thiết bị PAT

Trường hợp NAT traversal được sử dụng ở một hoặc cả hai cùng xác định với nhau rằng họ đang sử dụng NAT traversal, sau đó các cuộc đàm phán IKE chuyển sang sử dụng UDP port 4500. Các dữ liệu được gửi và xử lý bằng cách sử dụng IPsec trên UDP, mà đã được xử lý bởi NAT traversal. Đầu tiên nó nhận gói tin IPsec chưa đóng gói từ gói UDP và sau đó xử lý lưu lượng như một gói tin IPsec tiêu chuẩn.

Ba cổng đặc biệt phải được mở trên thiết bị NAT cho VPN làm việc một cách chính xác là UDP port 4500 (sử dụng cho NAT-T), UDP port 500 (sử dụng cho IKE) và giao thức IP 50 (ESP).

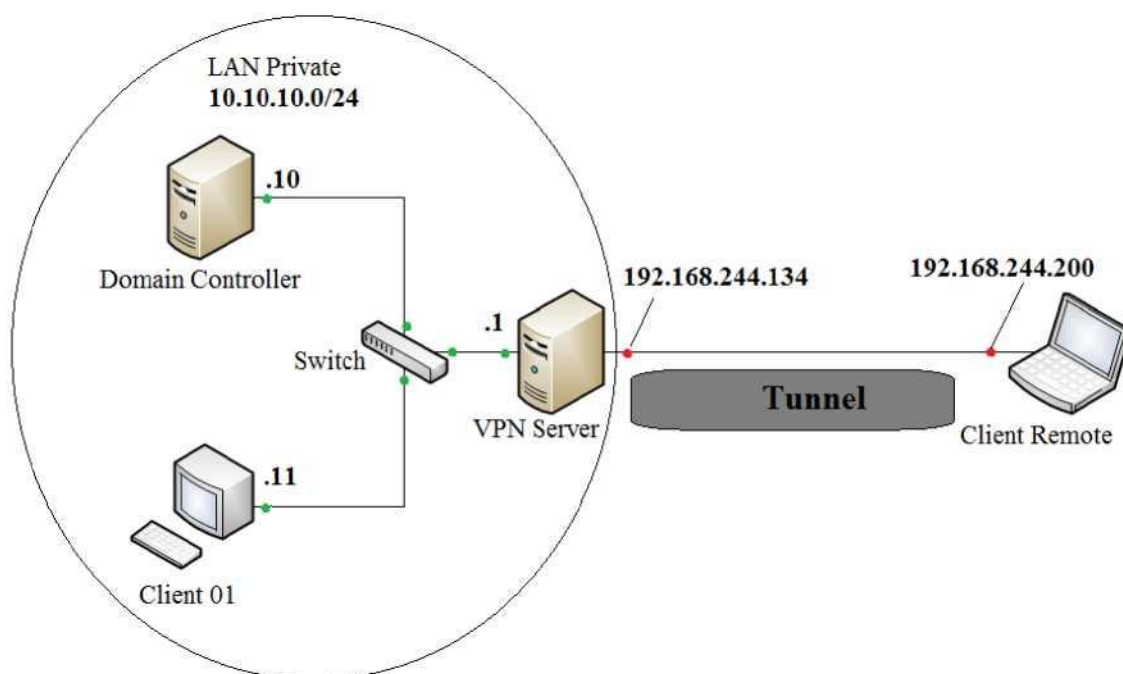
1.5. Kết luận chương 1

Chương 1 đã giới thiệu tổng quan về VPN, các mô hình VPN hiện nay cũng như ưu nhược điểm của VPN. Trình bày một cách chi tiết về giao thức IPsec VPN để từ đó lựa chọn phần mềm phù hợp triển khai IPsec VPN. Giới thiệu về bộ phần mềm OpenSwan, lịch sử hình thành và thành phần chính. Qua đây, chúng ta có thể thấy được việc sử dụng công nghệ VPN triển khai cho hệ thống mạng của các công ty, tổ chức là hết sức cần thiết. Với nhiều mô hình triển khai VPN và những ưu điểm của nó mang lại. Trong chương 1 của đề án đã chỉ ra giao thức IPsec VPN nhằm bảo đảm tính tin cậy, tính toàn vẹn và tính xác thực của dữ liệu khi qua mạng IP (Internet Protocol) công cộng và giới thiệu tổng quan về bộ phần mềm OpenSwan nhằm mục đích triển khai IPsec VPN. Việc lựa chọn sử dụng bộ phần mềm OpenSwan cho triển khai IPsec VPN những ưu điểm sau: bộ phần mềm OpenSwan là phần mềm mã nguồn mở, hỗ trợ trên nhiều bản phân phối linux, hỗ trợ cho hầu hết các phần mở rộng liên quan đến IPsec. Và để minh chứng cho những lý thuyết đã nêu ra trong chương 1 của đề án các phần tiếp theo trong đề án sẽ thực nghiệm trên cơ sở lý thuyết đó.

CHƯƠNG 2. TRIỂN KHAI HỆ THỐNG VPN DỰA TRÊN OPENSWAN

2.1. Mô hình triển khai VPN

Mô hình kết nối này cho phép người dùng ở xa kết nối tới mạng nội bộ của công ty, tổ chức. Cụ thể trong đề án tốt nghiệp sẽ sử dụng IPSec VPN xác thực người dùng bằng MS-CHAPv2 để kết nối và đảm bảo an toàn cho việc truyền dữ liệu giữa người dùng ở xa và mạng nội bộ của công ty, tổ chức qua môi trường mạng công cộng Internet. Sử dụng mô hình triển khai như trong Hình 2.1



Hình 2.1: Mô hình triển khai VPN Remote Access

Các thành phần hệ thống.

- 1 Máy chủ DC (Domain controller): Winserver 2003: 10.10. 10.10
- 1 Máy chủ VPN: CentOS 7 có 2 giao diện card mạng.
 - + Card public: 192.168.244.134
 - + Card private: 10.10.10.1
- 1 Máy Client: Win 7: 10 .10 .10. 11
- Máy Client Remote access: Win 7: 192.168.244.200

2.2. Cài đặt phần mềm OpenSwan

- Cài đặt gói OpenSwan trên CentOS 7 server 14.04

Sử dụng lệnh: apt-get install openswan

- Thực hiện bật chức năng IP Forwarding:

Sử dụng lệnh: echo 1 > /proc/sys/net/ipv4/ip_forward

- Sau đó restart IPsec: /etc/init.d/ipsec restart

- Để kiểm tra trạng thái của gói OpenSwan sử dụng lệnh: ipsec verify

```
root@localhost qa123:~# Ipsec verify
Checking your system to see if IPsec got installed and started correctly
Version check and Ipsec on-path
Linux Openswan U2.6.38/K3.19.0-25-generlc (netkey)
Checking for IPsec support In kernel
SAREF kernel support
NETKEY: Testing XFRM related proc values
      [OK]
      [OK]
Checking that pluto Is running
Pluto listening for IKE on udp 500
Pluto listening for NAT-T on udp 4500
Two or more Interfaces found, checking IP forwarding and MAS
QUERADEInG [OK]
Checking for 'tp' command
Checking /bin/sh Is not /bin/dash
Checking for 'tptables' command
Opportunistic Encryption Support ]
```

Trạng thái ipsec như trong Hình 2.2 sau

Hình 2.2: Trạng thái của gói OpenSwan

Trạng thái phần mềm được kiểm tra ở đây cho thấy đối với gói cài đặt OpenSwan chức năng mã hóa được hỗ trợ ở đây là Netkey. Netkey có chức năng và nguyên ký hoạt động cũng tương tự như Klips xong không được hỗ trợ nhiều cho IPv4, các tài liệu về Netkey cũng không có nhiều do nó đang được nhà phát triển sử dụng để hỗ trợ trên IPv6.

Như vậy gói phần mềm OpenSwan đã được cài thành công.

2.3. Triển khai thực nghiệm VPN Remote Access

Thiết lập các file cấu hình cho hệ thống VPN Remote Access

2.3.1. Cấu hình file ipsec.conf: nano /etc/ipsec.conf

```
version 2 # Conforms to second version of ipsec.conf specification
config setup
dumpdir=/var/run/pluto/
#Thư mục khởi tạo Pluto để thực hiện quá trình thiết lập kênh an toàn
nat_traversal=yes
#Bật hỗ trợ Nat-Traversal
```

```
virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12  
,%v6:fd00::/8,%v6:fe80::/10
```

```
#Những dải mạng nội bộ được hỗ trợ
```

```
protostack=netkey
```

```
# Quyết định giao thức stack được sử dụng
```

```
conn L2TP-PSK-NAT
```

```
rightsubnet=vhost: %priv
```

```
also=L2TP-PSK-noNAT
```

```
# Sử dụng giao thức L2TP với kiểu kết nối là Presharekey có hỗ trợ  
NAT. Các thông số tùy chỉnh được lấy ở dưới (L2TP-PSK-noNAT)
```

```
conn L2TP-PSK-noNAT
```

```
authby=secret
```

```
# Kiểu sử dụng là chia sẻ khóa bí mật sử dụng hệ mật RSA
```

```
pfs=no
```

```
# Disable pfs
```

```
auto=add
```

```
# Tải các kết nối và đáp ứng một yêu cầu gửi đến
```

```
keyingtries=3
```

```
# Số lần cố gắng thỏa thuận kết nối conn
```

```
ikelifetime=8h
```

```
# Thời gian tối đa trao đổi khóa và thiết lập kênh truyền
```

```
keylife=1h
```

```
# Thời gian sống của key
```

```
type=transport
```

```
# Kiểu giao thức truyền
```

```
Left=192.168.244.134
```

```
# Địa chỉ IP public của VPN Server
```

```
leftprotoport= 17/1701
```

```
# Cổng kết nối
```

```
right=%any
```

```
# Địa chỉ bên ngoài kết nối vào
```

```
rightprotoport=17/%any
```

```
# Cổng kết nối
```

2.3.2. Cấu hình file ipsec.secrets: nano /etc/ipsec.secrets

```
Include /var/lib/openswan/ipsec.secrets.inc
```

```
192.168.244.134 %any: PSK "123456"
```

```
# Khóa bí mật được thiết lập
```

2.3.3. Cấu hình file xl2tpd.conf: nano /etc/xl2tpd/xl2tpd.conf

```
[global]
```

```
Ipssec saref = no
```

```
debug tunnel = yes
```

```
debug avp = yes
```

```
debug packet = yes
```

```
debug network = yes
```

```
debug state = yes
```

```
[Ins default]
```

```
ip range = 10.10.10.100-10.10.10.150
```

```
# Dải địa chỉ dùng để cấp cho Client khi thực hiện VPN remote access vào
```

```
local ip = 10.10.10.1
```

```
# Địa chỉ card nội bộ (private) của máy chủ VPN
```

```
require chap = yes
```

```
refuse pap = yes
```

```
require authentication = yes
```

```
ppp debug = yes
```

```
pppoptfile = /etc/ppp/options.xl2tpd
```

```
length bit = yes
```

2.3.4. Cấu hình file options.xl2tpd : nano /etc/ppp/options.xl2tpd

```
refuse-mschap-v2
```

```
refuse-mschap
ipcp-accept-remote
ms-dns 8.8.8.8
ms-dns 8.8.4.4
asyncmap 0
auth
lock
hide-password
noccip
modem
dump
logfile /var/log/xl2tpd.log
logfd 2
idie 1800
mtu 1410
mru 1410
name thaonb4
password "Pa$$w0rd"
# Username và password để truy cập VPN
```

2.4. Kết nối và kiểm tra kết nối

Khởi động lại 2 giao thức: ipsec và xl2tp

`/etc/init.d/ipsec restart`, trạng thái khởi động như trong Hình 2.3

```
root@localhost qa123:~# /etc/init.d/ipsec restart ipsec_setup: stopping Openswan
IPsec... Ipsecsetup: starting Openswan IPsec U2.6.38/K3.19.0-25-generic...
ipsec_setup: multiple Ip addresses, using 192.168.244.134 on ethe root@localhost
qa123:~# I
```

Hình 2.3: Trạng thái khởi động lại của giao thức ipsec

`/etc/init.d/xl2tpd restart`, trạng thái khởi động như trong Hình 2.4

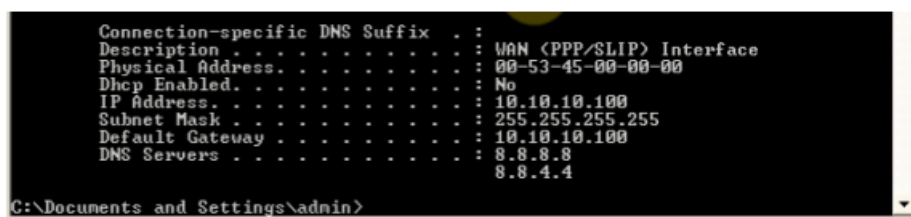
```
root@localhost qa123:~# /etc/init.d/xl2tpd restart Restarting Xl2tpd: Xl2tpd.
```

Hình 2.4: Trạng thái khởi động lại của giao thức L2T

Trên máy remote access thực hiện kết nối tới VPN server với thiết lập kết nối là L2TP như trong Hình 2.5

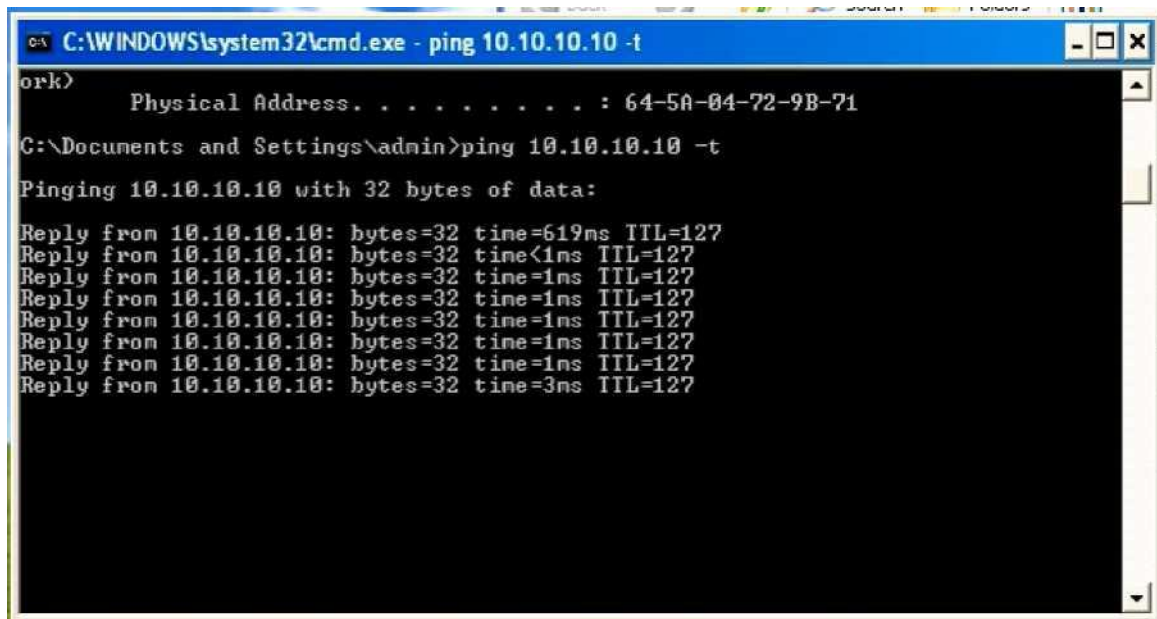


Hình 2.5: Kết nối remote access tới VPN sever erver
Sau khi kết nối thành công máy remote access sẽ được cấp 1 địa chỉ ip trong dải địa chỉ ip đã được thiết lập trên VPN server như trong Hình 2.6



Hình 2.6: Địa chỉ ip được cấp cho Client sau khi kết nối tới VPN Server

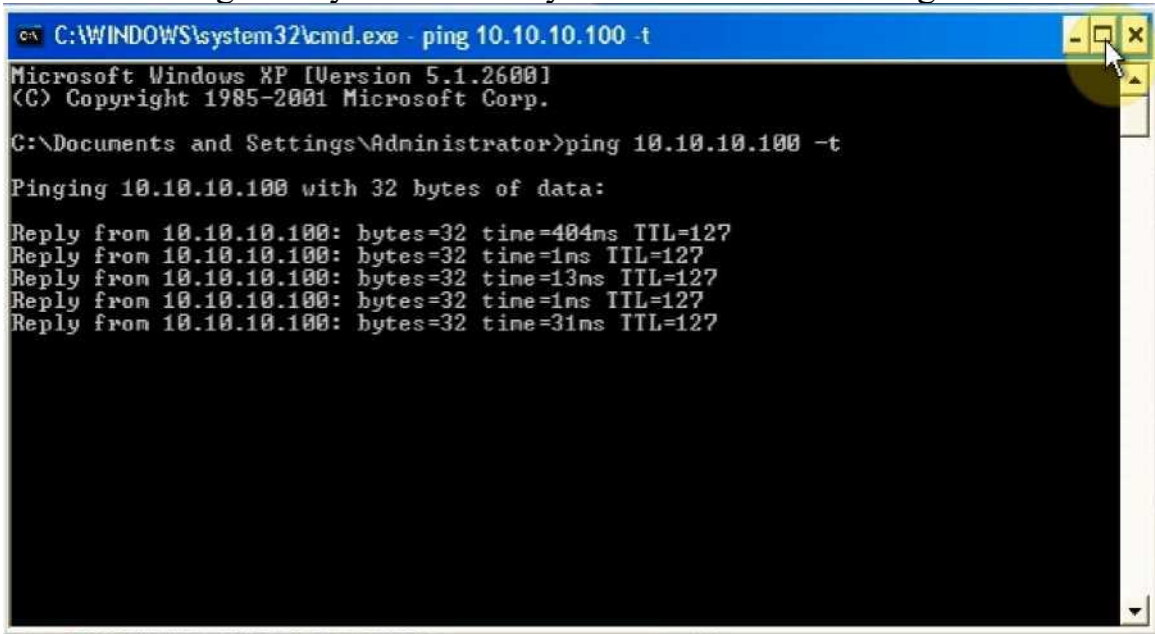
Kiểm tra Ping tới máy DC trong mạng LAN như trong Hình 2.7



```
C:\WINDOWS\system32\cmd.exe - ping 10.10.10.10 -t
ork>
Physical Address. . . . . : 64-5A-04-72-9B-71
C:\Documents and Settings\admin>ping 10.10.10.10 -t
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=619ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=3ms TTL=127
```

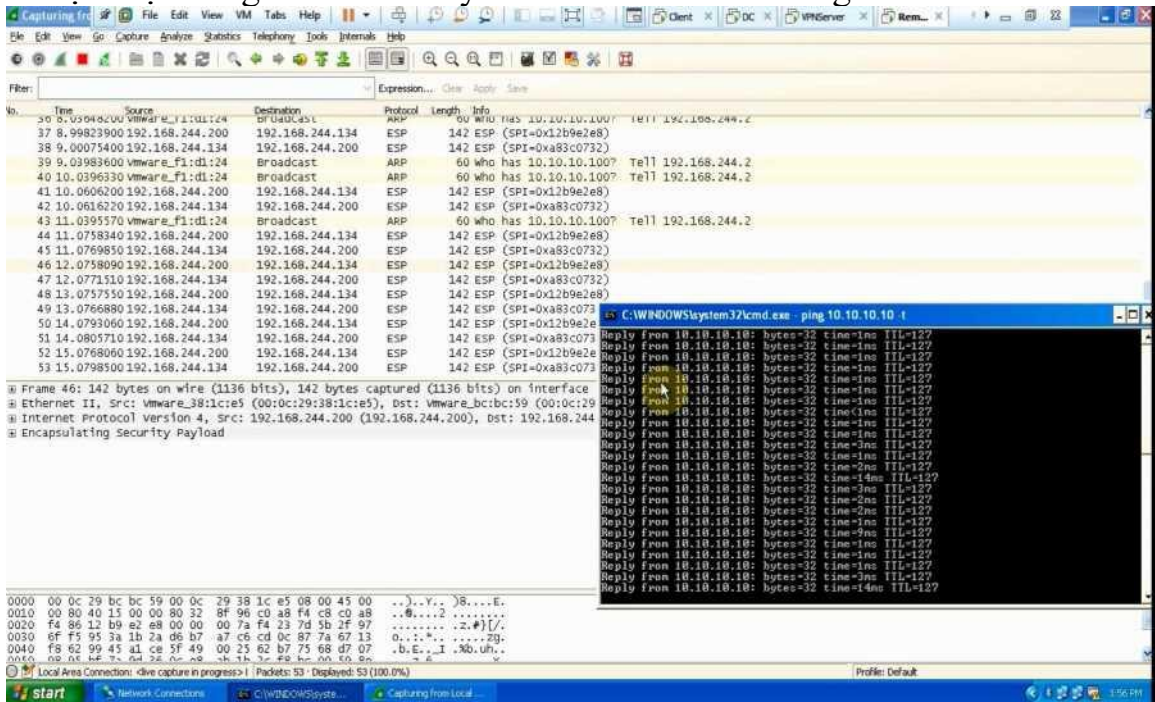
Hình 2.7: Kết quả kết nối từ máy remote access tới máy domain controller

Kiểm tra Ping từ máy client tới máy remote access như trong Hình 2.8



Hình 2.8: Kiểm tra Ping từ máy Client tới máy remote access

Thực hiện bắt gói tin trên máy remote access như trong Hình 2.9



Hình 2.9: Thực hiện bắt gói tin trên máy remote access

Thực hiện bắt gói tin trên máy remote access cho thấy các gói tin khi đi ra ngoài mạng nội bộ đã được mã hóa ESP. Do vậy mà máy remote access và vùng mạng nội bộ bên trong có thể liên lạc và trao đổi dữ liệu với nhau mà không cần quan tâm đến vấn đề bảo mật.

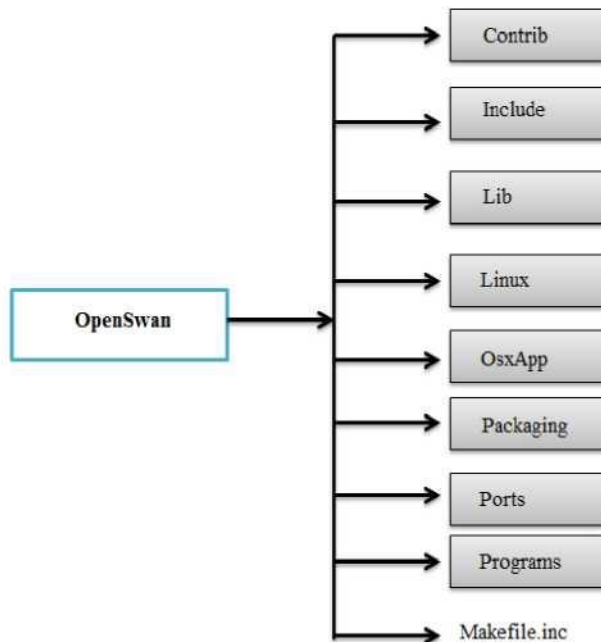
2.5. Kết luận chương 2

Chương 2 thực nghiệm mô hình VPN Remote Access sử dụng giao thức IPSec VPN với hỗ trợ là phần mềm OpenSwan. Bằng việc cài đặt gói OpenSwan trực tiếp từ gói hỗ trợ. Kết nối thành công với 2 giao thức IPSec và L2TP đảm bảo rằng khi người sử dụng kết nối tới một mạng nội bộ của 1 công ty hay tổ chức thì hoàn toàn được bảo mật. Các gói tin ra ngoài internet đã được mã hóa hoàn toàn và đường hầm mã hóa trong suốt với người sử dụng, do đó mà khách hàng hay nhân viên khi kết nối vào có thể trao đổi thông tin, dữ liệu một cách an toàn. Trên đây là những bước triển khai ban đầu được thực hiện dựa trên cơ sở lý thuyết của chương 1, trong những chương tiếp theo của đề án sẽ đi nghiên cứu sâu hơn về mã nguồn bộ phần mềm OpenSwan.

CHƯƠNG 3. PHÂN TÍCH VÀ TÙY BIẾN MÃ NGUỒN OPENSWAN

3.1. Cấu trúc thư mục mã nguồn

Mã nguồn bộ phần mềm OpenSwan có một số thư mục chính như trong Hình 3.1



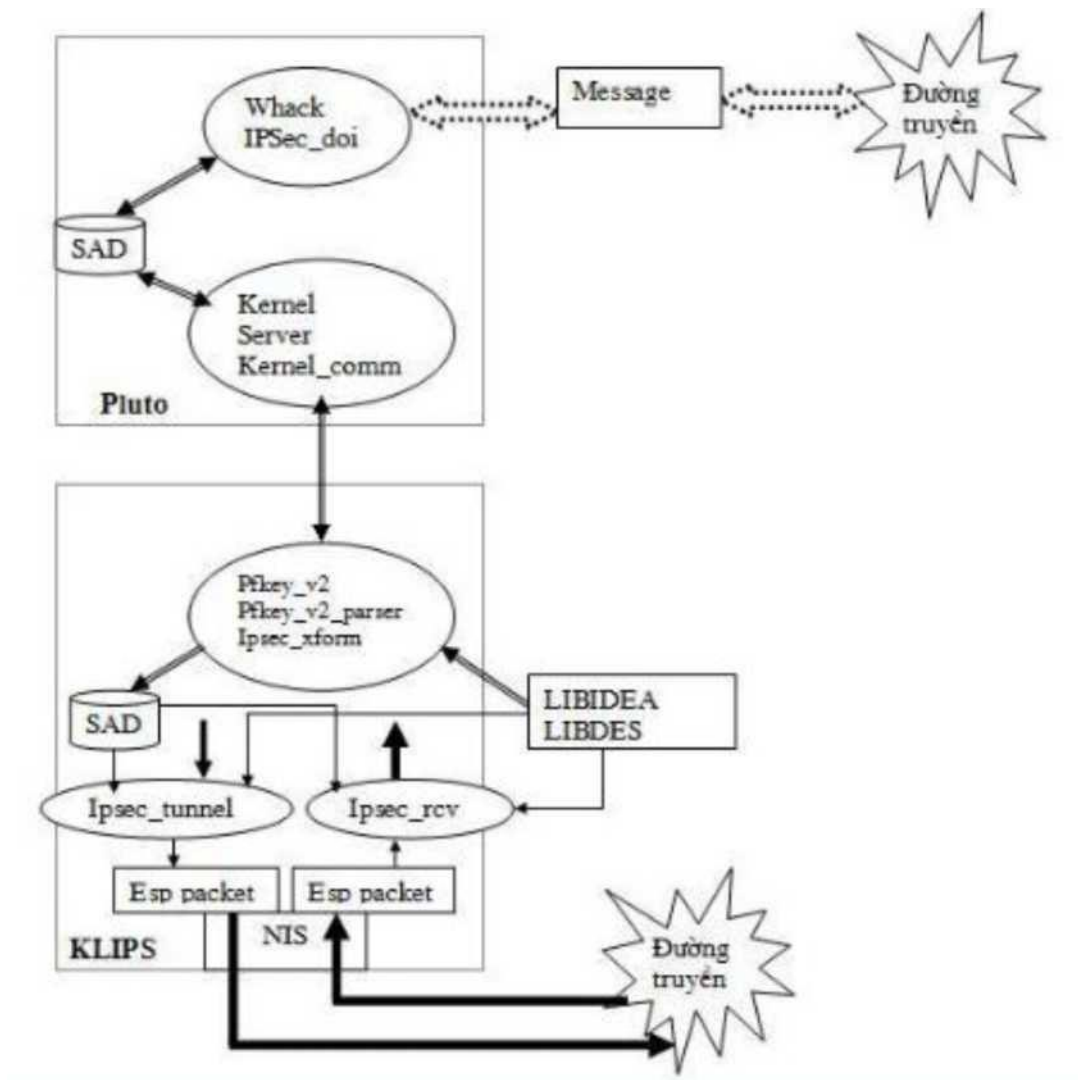
Hình 3.1: Cấu trúc thư mục chính trong mã nguồn bộ phần mềm OpenSwan

Trong đó:

- Thư mục Contrib: chứa các đóng góp của người dùng và sự đa dạng các loại mã trong việc phát triển.
- Thư mục Include: chứa nhân của mã nguồn OpenSwan và các thư viện của bộ phần mềm OpenSwan.
- Thư mục Lib: Gồm có các hàm thành phần và các thư viện như mã hóa, ipsec config, ipsec policy.
- Thư mục Linux: Thư mục chứa mã nguồn và thư viện để thực thi ipsec trên hệ điều hành Linux.
- Thư mục OsxApp: Được hỗ trợ riêng cho Mac OS X.
- Thư mục Packaging: Định nghĩa các giá trị thông số hoạt động của IPsec.
- Thư mục Ports: Định nghĩa các thông số hệ thống.
- Thư mục Programs: các hàm chính thực thi các file cấu hình và biên dịch.
- File Makefile.inc: File thực thi mã nguồn.

3.2. Phân tích các module mã nguồn bộ phần mềm OpenSwan

Các module chính của mã nguồn bộ phần mềm OpenSwan hoạt động theo như trong Hình 3.2 dưới đây



Hình 3.2: Sơ đồ hoạt động của các modul

Khi gói tin đi vào đường truyền sẽ được chuyển tới miền thực thi của Pluto tại đây Pluto sẽ có nhiệm vụ xác thực và thiết lập kênh an toàn cụ thể như sau:

Pluto sử dụng 2 file Whack.h và Whack.c sẽ có nhiệm vụ là tạo giao diện để thực hiện các lệnh Pluto cũng như các tiến trình của module Whack, tiếp theo đó module IPSec_doi thực hiện việc trao đổi các thông tin với các gateway khác để thực hiện các quá trình thỏa thuận các SA an toàn, trong module này, nó cũng thực hiện việc xác thực các gateway mã hóa bằng việc sử dụng khóa chia sẻ trước hay hệ mật khóa công khai sau đó dữ liệu được đưa tới CSDL liên kết an

toàn SAD tại đây SAD sẽ được tham chiếu để quyết định xem gói dữ liệu sẽ được xử lý tiếp theo, gói tin được chuyển tới miền thực hiện việc trao đổi các thông tin giữa Pluto và Klips với 3 module chính: Kernel, Server, Kernel_comm, gói tin được đưa tới Klips, Klips sử dụng module Pfkey_v2 và Pfkey_v2_parser để giao tiếp và trao đổi thông tin với Pluto sau đó gói tin sẽ được module Ipsec_xfrom kết hợp với các thư viện DES, IDEA và các thông tin đã thỏa thuận tại Pluto chuyển xuống để tạo ra các khóa an toàn cho phiên liên lạc, gói tin được chuyển tới SAD để quyết định các thông tin mã hóa hay giải mã sau đó được module Ipsec_tunnel mã hóa và đóng gói gửi vào đường truyền. Ở chiều ngược lại module Ipsec_rcv sẽ giải mã gói tin với các thông số đã được quyết định bởi SAD rồi đưa vào đường truyền.

3.3. Tùy biến mã nguồn OpenSwan

Một số thực hiện cho việc tùy biến mã nguồn:

- Sửa nội dung các hàm đã có
- Thêm hàm mới
- Tối giản mã nguồn với việc bỏ đi các hàm không cần thiết

Để dễ dàng hơn trong việc triển khai và vận hành hệ thống VPN, đồ án sẽ thực hiện việc sửa nội dung các hàm đã có bằng cách viết hóa một số ký tự truyền vào và phần kiểm tra trạng thái giao thức IPSec.

3.3.1. Viết hóa ký tự truyền vào

Việc cấu hình IPSec VPN phụ thuộc phần lớn vào file cấu hình ipsec.conf nó nằm trong thư mục /etc (thư mục chứa các file cấu hình), những tùy chọn, ký tự trong file ipsec.conf đều được tham chiếu đến mã nguồn OpenSwan đã biên dịch. Trong đó có những tùy chọn, ký tự mặc định và những tùy chọn, tự yêu cầu người sử dụng gần được truyền vào để thực hiện IPSec VPN.

Những thông số cấu hình trong file ipsec.conf thể được chia thành 3 phần:

- config setup

Những thông số cấu hình ở mức thiết lập ban đầu như: bật hỗ trợ NAT Traversal, tùy chọn những dải mạng nội bộ được hỗ trợ hay quyết định chức năng mã hóa...

- conn %default

Những tùy chọn mặc định cho việc thiết lập các kết nối

- conns

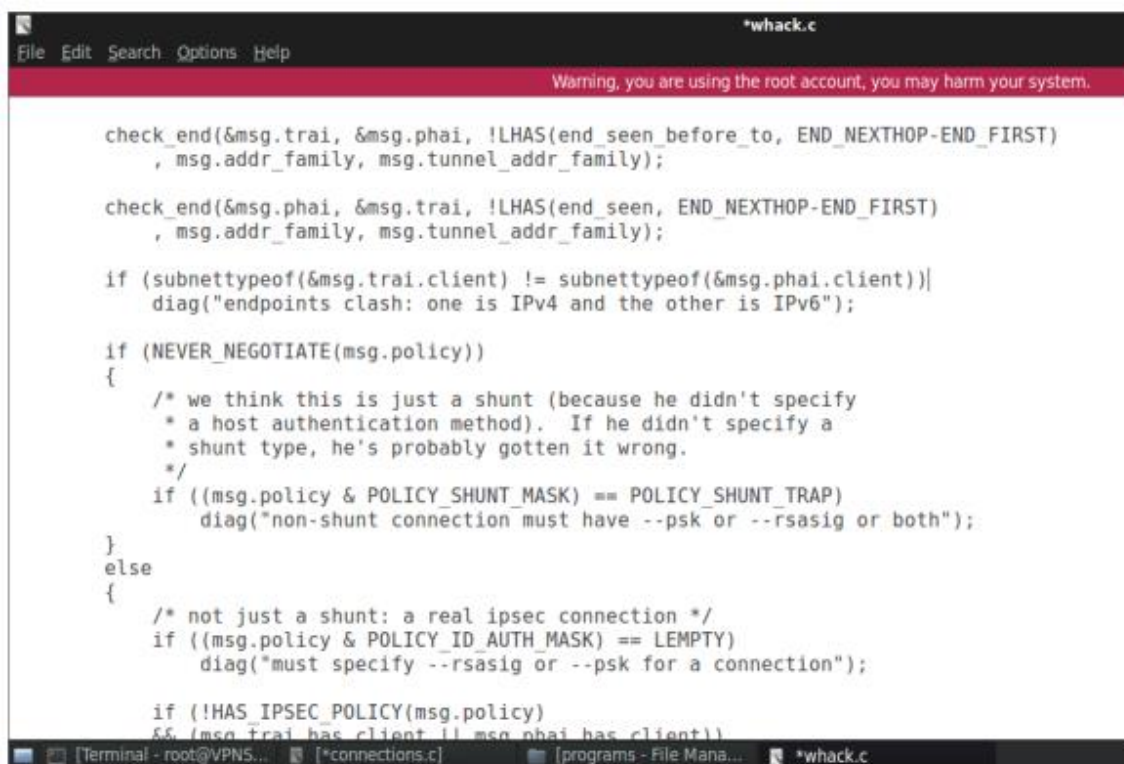
Những thông số truyền vào từ người dùng cho việc thiết lập các kết nối

Để dễ dàng hơn trong việc thiết lập các kết nối, đồ án sẽ trình bày về việc viết hóa những tham số truyền vào trong file cấu hình ipsec.conf. Bằng cách sửa đổi mã nguồn bộ phần mềm OpenSwan tìm kiếm và thay thế một số ký tự trong những file thực thi có phần đuôi là .c và .h của mã nguồn bộ phần mềm OpenSwan. Những file thực thi này được lưu chủ yếu tại thư mục programs của mã nguồn. Những ký tự được thay thế như sau:

- Ký tự “traí” thay thế cho ký tự “left” trong mã nguồn
- Ký tự “phụ” thay thế cho ký tự “subnet” trong mã nguồn
 - Ký tự “phái” thay thế cho ký tự “right” trong mã nguồn

Ví dụ về một số file trong thư mục mã nguồn đã được sửa đổi nội dung:

- File whack.c trong thư mục programs/pluto được thay thế với 2 ký tự “traí” và “phái” tương ứng với 2 ký tự “left” và “right” trong mã nguồn như trong Hình 3.3



```
*whack.c
Warning, you are using the root account, you may harm your system.

check_end(&msg.traí, &msg.phái, !HAS(end_seen_before_to, END_NEXTHOP-END_FIRST)
, msg.addr_family, msg.tunnel_addr_family);

check_end(&msg.phái, &msg.traí, !HAS(end_seen, END_NEXTHOP-END_FIRST)
, msg.addr_family, msg.tunnel_addr_family);

if (subnettypeof(&msg.traí.client) != subnettypeof(&msg.phái.client))
diag("endpoints clash: one is IPv4 and the other is IPv6");

if (NEVER_NEGOTIATE(msg.policy))
{
/* we think this is just a shunt (because he didn't specify
* a host authentication method). If he didn't specify a
* shunt type, he's probably gotten it wrong.
*/
if ((msg.policy & POLICY_SHUNT_MASK) == POLICY_SHUNT_TRAP)
diag("non-shunt connection must have --psk or --rsasig or both");
}
else
{
/* not just a shunt: a real ipsec connection */
if ((msg.policy & POLICY_ID_AUTH_MASK) == EMPTY)
diag("must specify --rsasig or --psk for a connection");

if (!HAS_IPSEC_POLICY(msg.policy)
&& (msg.traí.has_client || msg.phái.has_client))
```

Hình 3.3: Sửa đổi nội dung file whack.c trong mã nguồn

- File connections.c trong thư mục programs/pluto được thay thế với ký tự “phu” tương ứng với ký tự “subnet” trong mã nguồn như Hình 3.4 sau



```
File Edit Search Options Help
Warning, you are using the root account, you may harm your system.

if (routed(sr->routing)
&& addrinphu(our_client, &sr->this.client)
&& addrinphu(peer_client, &sr->that.client))
{
    if (best == NULL)
    {
        best = c;
        break;
    }

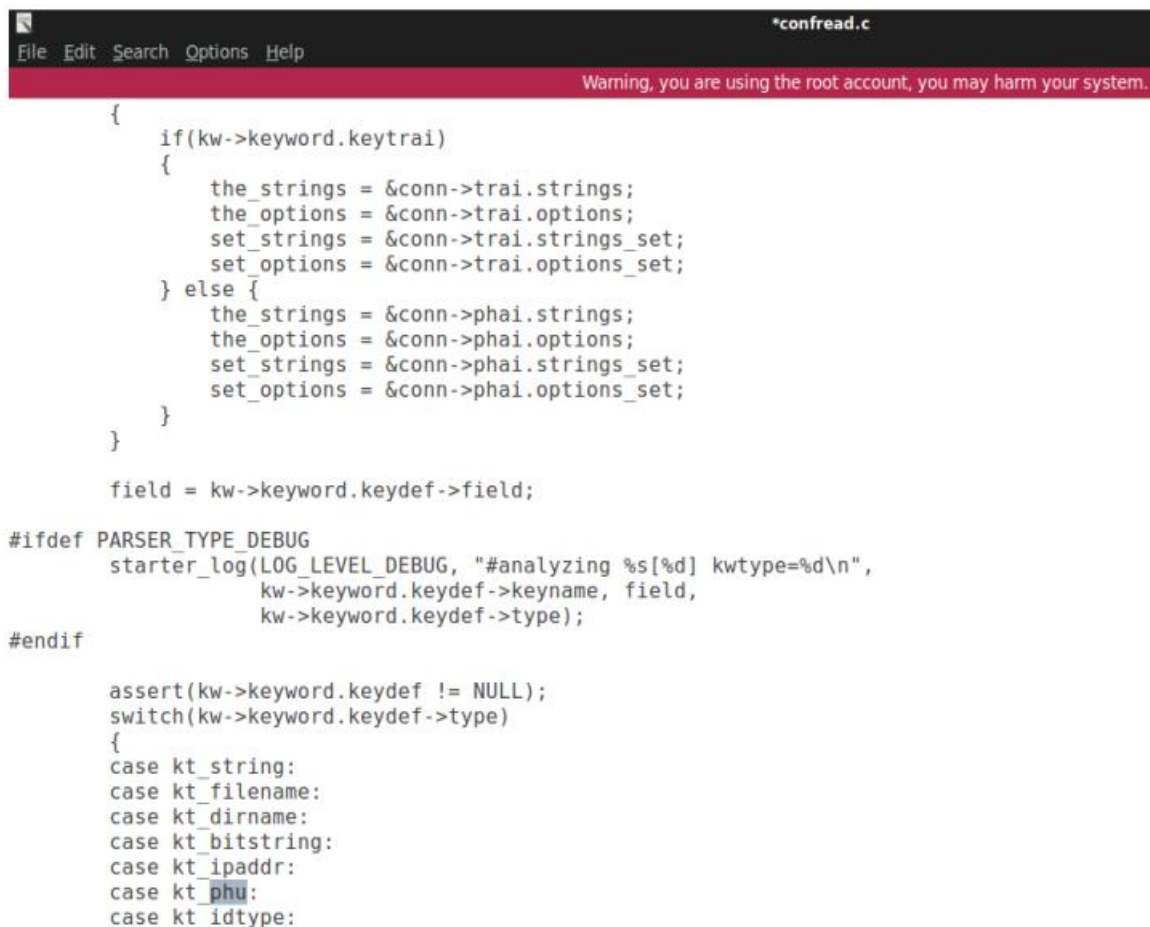
    DBG(DBG_OPPO,
        DBG_log("comparing best %s to %s"
            , best->name, c->name));

    for (bestsr = &best->spd; best!=c && bestsr; bestsr=bestsr->next)
    {
        if (!phuinphu(&bestsr->this.client, &sr->this.client)
            || (samephu(&bestsr->this.client, &sr->this.client)
                && !phuinphu(&bestsr->that.client
                    , &sr->that.client)))
        {
            best = c;
        }
    }
}
}
```

[Terminal - root@VPNS...] [*whack.c] [programs - File Mana...] [*connections.c]

Hình 3.4: Sửa đổi nội dung file connections.c trong mã nguồn

- File confread.c trong thư mục lib/libipsecconf đã được thay thế cả 3 ký tự nêu trên như trong Hình 3.5 sau



```
{
    if(kw->keyword.keytra)
    {
        the_strings = &conn->tra)strings;
        the_options = &conn->tra)options;
        set_strings = &conn->tra)strings_set;
        set_options = &conn->tra)options_set;
    } else {
        the_strings = &conn->pha)strings;
        the_options = &conn->pha)options;
        set_strings = &conn->pha)strings_set;
        set_options = &conn->pha)options_set;
    }
}

field = kw->keyword.keydef->field;

#ifdef PARSE)TYPE_DEBUG
    starter_log(LOG_LEVEL_DEBUG, "#analyzing %s[%d] kwtype=%d\n",
                kw->keyword.keydef->keyname, field,
                kw->keyword.keydef->type);
#endif

assert(kw->keyword.keydef != NULL);
switch(kw->keyword.keydef->type)
{
case kt_string:
case kt_filename:
case kt_dirname:
case kt_bitstring:
case kt_ipaddr:
case kt_phu:
case kt_idtype:
```

Hình 3.5: Sửa đổi nội dung file confread.c trong mã nguồn

Thực hiện tương tự với những file có phần đuôi là .c và .h còn lại trên mã nguồn bộ phần mềm OpenSwan.

Sau khi đã sửa đổi và biên dịch bộ phần mềm OpenSwan từ mã nguồn mới thì việc truyền tham số vào file cấu hình ipsec.conf không còn giống như trước, lúc này sẽ có một số tùy chọn mà đã được viết hóa buộc người dùng phải nhập đúng theo yêu cầu của mã nguồn mới. Những tùy chọn được sửa đổi và thay thế khi nhập vào file cấu hình ipsec.conf như Bảng 3.1 sau:

Bảng 3.1: Một số tùy chọn được sửa đổi và thay thế trong file ipsec.conf

STT	Ký tự ban đầu	Ký tự thay thế
1	left	trai
2	leftsubnet	traiphu
3	leftrsasigkey	trairsasigkey
4	right	phai
5	rightsubne	phaiphu
6	rightrsasigkey	Phairsasigkey

3.3.2. Việt hóa kiểm tra trạng thái IPSec

Để dễ dàng hơn trong việc kiểm tra và vận hành IPSec VPN, đồ án đã thực hiện sửa đổi phần hiển thị thông tin trạng thái IPSec nhằm dễ dàng hơn cho người sử dụng. Tìm kiếm và thay thế những ký tự được hiển thị ra khi người dùng thực hiện kiểm tra trạng thái IPSec VPN bằng cách sửa đổi nội dung file verify.in trong thư mục programs/verify của mã nguồn bộ phần mềm OpenSwan. Ví dụ như đoạn code được sửa đổi như trong Hình 3.6 sau:

```

sub installstartcheck {
    print "Kiểm tra giao thức IPsec đã được cài đặt và vận hành một cách chính xác:\n";

    printfun "Kiểm tra phiên bản và đường dẫn IPsec";
    run "ipsec --version";
    errchk "@out";
    print grep /Linux/, @out;

    printfun "Kiểm tra IPsec được hỗ trợ trong nhân";
    if ( -e "/proc/net/ipsec_eroute" || -e "/proc/net/pfkey" ) { $test="1" }
    errchk "$test";

# This requires KLIPS NAT-T patch > 2.4.x|
    if ( -e "/proc/net/ipsec_eroute" ) {

        printfun " KLIPS: hỗ trợ NAT Traversal";
        if ( -e "/sys/module/ipsec/parameters/natt_available" ) {
            run "cat /sys/module/ipsec/parameters/natt_available";
            if("@out" == "1\n")
                { warnchk "", "OLD STYLE"; }
            else {
                if("@out" == "2\n")
                    { errchk "OK"; }
                else
                    { warnchk "", "UNKNOWN"; }
            }
        }
        } else { warnchk "", "UNKNOWN"; }

    printfun " KLIPS: hỗ trợ OCF crypto offload";
    if ( -e "/sys/module/ipsec/parameters/ocf_available" ) {
        run "cat /sys/module/ipsec/parameters/ocf_available";
        if("@out" == "1\n")
            { errchk "OK"; }
    }

```

Hình 3.6: Sửa đổi nội dung file verify.in

Làm tương tự với những phần hiển thị còn lại trong file verify.in ta được kết quả khi kiểm tra trạng thái như trong Hình 3.7

```
Kiem tra giao thuc IPsec da duoc cai dat va van hanh mot cach chinh xac:
Kiem tra phien ban va duong dan IPsec [OK]
Linux Openswan 2.6.32 (klips)
Kiem tra IPsec duoc ho tro trong nhan [OK]
KLIPS: ho tro NAT Traversal [OK]
KLIPS: ho tro OCF crypto offload [N/A]
Ho tro nhan SAref [N/A]
Kiem tra Pluto hoat dong [OK]
Pluto lang nghe giao thuc IKE voi giao thuc truyen udp cong 500 [OK]
Pluto lang nghe giao thuc NAT-T voi giao thuc truyen udp cong 4500 [OK]
Kiem tra IP forwarding cua cac giao dien mang [OK]
Kiem tra NAT and MASQUERADEing [N/A]
Kiem tra for 'ip' command [OK]
Kiem tra /bin/sh is not /bin/dash [WARNING]
Kiem tra for 'iptables' command [OK]
Kiem tra Opportunistic Encryption [DISABLED]
```

Hình 3.7: Trạng thái IPsec sau khi đã sửa đổi mã nguồn bộ phần mềm OpenSwan

3.4. Kết luận chương 3

Chương 3 đã đưa ra được cấu trúc các thư mục trong mã nguồn của bộ phần mềm OpenSwan. Phân tích hoạt động của các module trong quá trình trao đổi và thiết lập kênh an toàn trên Pluto, việc mã hóa và giải mã gói tin trong miền thực thi của Klips. Can thiệp vào mã nguồn bộ phần mềm OpenSwan sửa đổi nội dung một số file thực thi để đưa ra một bộ mã nguồn mới giúp cho người dùng dễ dàng hơn trong việc triển khai và vận hành IPsec VPN. Để thấy được sự tiện ích của mã nguồn mới so với mã nguồn gốc chương tiếp theo của đề án sẽ thực nghiệm mô hình VPN site to site trên mã nguồn gốc và mã nguồn đã tùy biến.

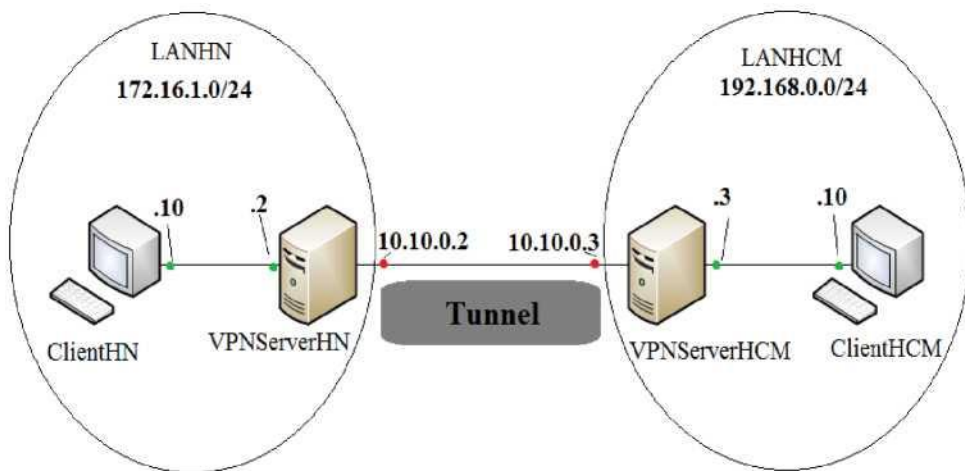
CHƯƠNG 4. THỰC NGHIỆM

4.1. Thực nghiệm 1: Triển khai hệ thống VPN từ mã nguồn OpenSwan

Khi chi nhánh mạng tại Hà Nội và Hồ Chí Minh của 1 công ty muốn thực hiện việc liên lạc và trao đổi thông tin với nhau mà vẫn đảm bảo về tính bảo mật các thông tin được truyền tải đến nhau. Mô hình VPN site to site dưới sự bảo mật của giao thức IPSec VPN được xây dựng ra để giải quyết vấn đề đó.

4.1.1. Mô hình thực nghiệm VPN site to site

Triển khai thực nghiệm VPN site to site sẽ thực hiện theo mô hình như trong Hình 4.1



Hình 4.1: Mô hình thực nghiệm VPN site to site

4.1.1.1. Các thành phần máy chủ, máy trạm

Vùng mạng nội bộ tại Hà Nội có dải địa chỉ: 172.16.1.0/24

- Máy chủ VPNServerHN: chạy hệ điều hành Linux có sử dụng bộ phần mềm OpenSwan. Đóng vai trò là gateway cho dải mạng nội bộ tại Hà Nội. Nó có 2 giao diện card mạng:
 - + Card public: 10.10.0.2 để giao tiếp với VPNServerHCM.
 - + Card private: 172.16.1.129 giao tiếp với mạng nội bộ Hà Nội.
- Máy ClientHN: Chạy hệ điều hành winserver 2003 có địa chỉ ip 172.16.1.10

Vùng mạng nội bộ tại Hồ Chí Minh có dải địa chỉ: 192.168.0.0/24

- Máy chủ VPNServerHCM: chạy hệ điều hành Linux có sử dụng bộ phần mềm OpenSwan. Đóng vai trò là gateway cho dải mạng nội bộ tại Hồ Chí Minh. Nó có 2 giao diện card mạng
 - + Card public: 10.10.0.3 để giao tiếp với VPNServerHN.

- + Card private: 192.168.0.129 giao tiếp với mạng nội Hồ Chí Minh.
- Máy ClientHCM: Chạy hệ điều hành win 7 có địa chỉ ip 192.168.0.10

4.1.1.2. Quá trình hoạt động

Khi người dùng từ mạng LAN Hà Nội và mạng LAN HCM thực hiện kết nối, luồng dữ liệu trao đổi sẽ đi qua hai VPNServer HN và HCM. Dữ liệu khi đến các VPN gateway sẽ được mã hóa và đóng gói lại, sau khi được đóng gói lại dữ liệu có dạng là các packet và được truyền trên mạng Internet để tới đích. VPN gateway đích khi nhận được các packet tiến hành giải mã để được giữ liệu gốc ban đầu. Rồi gửi đến người dùng trong mạng nội bộ của mình.

4.1.2. Triển khai thực nghiệm

4.1.2.1. Thiết lập máy chủ VPNServer

Máy chủ VPNServer được sử dụng trong thực nghiệm hay hệ điều hành CentOS 7. Được cài đặt bộ phần mềm OpenSwan 2.6.32 để tương thích với nhân của hệ điều hành. Trên đó có cài các gói hỗ trợ cho việc biên dịch và triển khai từ mã nguồn OpenSwan.

Tiến hành quá trình biên dịch và cài đặt mã nguồn:

Bước 1: Thiết lập máy chủ theo sơ đồ thực nghiệm:

- Thiết lập tên máy chủ
- Đặt địa chỉ IP
- Kiểm tra các kết nối

Bước 2: Tải mã nguồn bộ phần mềm OpenSwan

- Tải mã nguồn trực tiếp từ trang chủ của OpenSwan:

<https://www.openswan.org/>

- Hoặc sử dụng lệnh:

```
Wget https://download.openswan.org/openswan/old/openswan-2.6/openswan-2.6.32.tar.gz
```

Bước 3: Giải nén mã nguồn

Di chuyển vào thư mục chứa file OpenSwan vừa tải về thực hiện câu lệnh: tar -xvf openswan-2.6.32.tar.gz

Bước 4: Cài đặt các gói phần mềm hỗ trợ

Di chuyển vào thư mục openswan-2.6.32 thực hiện cài đặt một số gói phần hỗ trợ cho việc biên dịch mã nguồn được yêu cầu trong file README. Các hàm thư viện tính toán GNU và một số hỗ trợ khác:

- Gói dành cho Debian: libgmp3, libgmp3-dev, gawk/mawk, flex, bison, iproute, iptables.

- Gói dành cho RPM: gmp, gmp-dev

Bước 5: Bắt đầu biên dịch mã nguồn

Sử dụng lệnh: `make programs`

Bước 6: Cài đặt Klips

Để cài đặt hỗ trợ Klips cho bộ phần mềm OpenSwan sử dụng 2 câu lệnh sau:

1. `make KERNELSRC=/lib/modules/'uname -r'/build module`
2. `make KERNELSRC=/lib/modules/'uname -r'/build install mininstall`

Kiểm tra trạng thái gói OpenSwan sau khi đã biên dịch

Sử dụng câu lệnh: `ipsec verify`, trạng thái IPsec sau khi biên dịch như

trong Hình 4.2

```
vpn1@VPNServerHN:~$ sudo ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path [OK]
Linux Openswan U2,6.32/K(no kernel code presently loaded)
Checking for IPsec support in kernel [FAILED]
SAref kernel support [N/A]
Checking that pluto is running [FAILED]
  whack: Pluto is not running (no "/var/run/pluto/plutoctl") Two
or more interfaces found, checking IP forwarding [FAILED]
  whack: Pluto is not running (no "/var/run/pluto/plutoctl")
Checking for 'ip' command [OK]
Checking /bin/sh is not /bin/dash [WARNING]
Checking for 'iptables' command [OK]
Opportunistic Encryption Support [DISABLED]
```

Hình 4.2: Trạng thái bộ phần mềm OpenSwan sau khi biên dịch từ mã nguồn

Bước 7: Bật chức năng IP Forwarding sử dụng câu lệnh:

`Echo 1 > /proc/sys/net/ipv4/ip_forward`

Sau đó restart ipsec: `/etc/init.d/ipsec restart`

Trạng thái IPsec sau khi bật chức năng IP Forwarding như trong Hình 4.3

```
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path [OK]
Linux Openswan 2.6.32 (klips)
Checking for IPsec support in kernel [OK]
KLIPS: checking for NAT Traversal support [OK]
KLIPS: checking for OCF crypto offload support [N/A]
SAREF kernel support [N/A]
Checking that pluto is running [OK]
Pluto listening for IKE on udp 500 [OK]
Pluto listening for NAT-T on udp 4500 [OK]
Two or more interfaces found, checking IP forwarding [OK]
Checking NAT and MASQUERADEing [N/A]
Checking for 'ip' command [OK]
Checking /bin/sh is not /bin/dash [WARNING]
Checking for 'iptables' command [OK]
Opportunistic Encryption Support [DISABLED]
```

Hình 4.3: Trạng thái bộ phần mềm OpenSwan sau khi bật chức năng IP Forwarding

Bộ phần mềm OpenSwan đã được biên dịch thành công.

4.1.2.3 Cấu hình và cài đặt VPN Site to site từ mã nguồn đã biên dịch

- Trên VPNServerHN thực hiện những bước cấu hình sau:

Bước 1: Thực hiện trao đổi khóa công khai với VPNServerHCM

Export khóa công khai và import sang bên VPNServerHCM

Sử dụng lệnh: ipsec showhostkey --left, khóa công khai của bên

VPNServerHN như trong Hình 4.4

```
vpn1@VPNServerHN:~$ sudo ipsec showhostkey --left
# rsakey A00Btu+6h
leftrsasigkey=0sAQ0Btu+6hnIS/qM0ydiD47Yres0MU7eF11+kjWT9tB4SmDMT5eaLA8
g0IBQncBPstrrXCRHIfzVwbDITAj/5z7fGPgWJF6DoQuZo4LJbZf1Ani2z1SRyDBKkNh+l1TmAc0g/
VETn+MytV2xSQd05daNyNL97QXGysidHJ0Ggdet5jIqhQXaLYuqX5Kjy0ToKVqnpTSjccpj0jX0xvT
LD5AQglnCSAI5mw9v7e1sM6BnGvIqDHB98UkexKN5HmuS38WU4Ase5N8l9Iz0NPHqGXtJJzjWhX08M
Dzjq5oGQXqDYHnwyr9mUC1fwvdu7CzDiv6NckfAb0C+dKB+Moi0h04CqKKuvK5xw2uR/APtifNiBT1
9/
```

Hình 4.4: Khóa công khai của VPNServerHN

Bước 2: Cấu hình file ipsec.conf

Thực hiện lệnh: nano /etc/ipsec.conf

```
version 2 # Conforms to second version of ipsec.conf specification
```

```
config setup
```

```
nat_traversal=yes
```

```
#Bật hỗ trợ Nat-Traversal
```

```

        virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.1
6.0.0/12,%v6:fd00: :/8,%v6:fe80: :/10
        # Hồ những dải mạng bên trong
        protostack=klips
        #Quyết định giao thức stack được sử dụng
        Interfaces="ipsec0=eth0"
        # Giao diện card mạng được gán cho card ipsec0
conn %default
        authby=rsasig
        # Sử dụng hệ mật khóa RSA
conn HN-HCM
        left=10.10.0.2
        # Địa chỉ mạng public giao tiếp với VPNServerHCM
        leftsubnet=172.16.1.0/24
        # Dải mạng nội bộ HN
        right=10.10.0.3
        # Địa chỉ mạng public giao tiếp với VPNServerHN
        rightsubnet=192.168.0.0/24
        # Dải mạng nội bộ HCM
        type=tunnel
        # Kiểu giao thức truyền tin
        leftrsasigkey=0sAQOBtu+6hnIS/qMQydiD47Yres0MU7eF11+
kjWT9tB4SmDMT5eaLA8g0IBQncBPstrrXCRHIfzVWbDITAj/5z7fGPgWJF6
DoQuZo4LJbZflAni2zlSRYDBKkNh+lITmAcOg/VETn+MytV2xSQd05daNy
NL97QXGYsidHJ0Ggdet5jIqhQXaLYuqX5KjyoToKVqnpTSjccpj0jX0xvTID5
AQglncSAI5mw9v7elsM6BnGvIqDHB98ukexKN5HmuS38Wu4Ase5N819Iz
0NPHqGXtJJzjWhX08MDzjq5oGQXqDYHnwyr9mUCIfWvdu7CzDiv6Nckf
AbOC+dKB+MoiOh04CqKKuvK5xw2uR/APtifNiBT 19/
        # Khóa công khai của VPNServerHN
        rightrsasigkey=0sAQOD2PrJjZwPyMIW15SusBi5kcIa/aYad7K
jEFs9q4fN7rHRt9lUCIBCYVaXxI8wsIe6cxCyv3sggveNUR29cyUTvH86UWg

```

```
Q9vNdEZ5Twjg+QL88sGnnNOqKhxH4EBPyX/LFkjjPXm2k5TFFxWgwFev4
6NWS5q2x2+9T78PQciJtcx5Y/iowaVfanTlQCeqRTHHidBHd7bCmTjZUSCn
+vd1GnB7AkzLP2x7geMdiI/DiLLSx3neXQi6bEoUfVWN6Lat6Qg43lEGd3sO
hJoiNgU5mtAz2FipBNpOvTTcdjwytwDOU/Ukfp13cIp3xpInlZE3JDPfi7+MXI
h2r+MHtd18Y4vrpH64rj0y1p97o3st//QFH
```

```
# Khóa công khai của VPNServerHCM
```

```
auto=start
```

```
# Tải, định tuyến và bắt đầu thực hiện kết nối
```

Bước 3: Khởi động lại và kiểm tra trạng thái IPsec

Khởi động lại ipsec: /etc/init.d/ipsec restart

Kiểm tra trạng thái: ipsec verify, trạng thái IPsec sau khi đã thiết lập đường hầm bên VPNServerHN như trong Hình 4.5

```
vpn1@VPNServerHN:~$ sudo ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path [OK]
Linux Openswan 2.6.32 (klips)
Checking for IPsec support in kernel [OK]
KLIPS: checking for NAT Traversal support [OK]
KLIPS: checking for OCF crypto offload support [N/A]
SAREf kernel support [N/A]
Checking that pluto is running [OK]
Pluto listening for IKE on udp 500 [OK]
Pluto listening for NAT-T on udp 4500 [OK]
Two or more interfaces found, checking IP forwarding [OK]
Checking NAT and MASQUERADEing [N/A]
Checking for 'ip' command [OK]
Checking /bin/sh is not /bin/dash [WARNING]
Checking for 'iptables' command [OK]
Opportunistic Encryption Support [DISABLED]
```

Hình 4.5: Trạng thái IPsec trên VPNServerHN

– Trên VPNServerHCM thực hiện những bước cấu hình tương tự:

Bước 1: Thực hiện trao đổi khóa công khai với VPNServerHN Export khóa công khai và import sang bên VPNServerHN

Sử dụng câu lệnh: ipsec showhostkey --left, khóa công khai của bên VPNServerHCM như trong Hình 4.6

```
vpn2@VPNServerHCM:~$ sudo ipsec showhostkey --left
# rsakey A00D2PrJj
lefttrsasigkey=0sA00D2PrJjZwPyM1Wl5SusBi5kcIa/aYad7KjEFs9q4fN7rHRt9lUCI
BCYVaXx18wsIe6cxCyv3sggveNur29cyUTvH86UWg09vNdEZ5Twjg+QL88sGnnNOqKhxH4EBPyX/LF
kjjPXm2k5TFFxWgwFev46NWS5q2x2+9T78PQciJtcx5Y/iowaVfanTlQCeqRTHHidBHd7bCmTjZUSC
n+vd1GnB7AkzLP2x7geMdiI/DiLLSx3neXQi6bEoUfVWN6Lat6Qg43lEGd3s0hJoiNgU5mtAz2FipB
Np0vTTcdjwytwDOU/Ukfp13cIp3xpInlZE3JDPfi7+MXIh2r+MHtd18Y4vrpH64rj0y1p97o3st//Q
FH
```

Hình 4.6: Khóa công khai của VPNServerHCM

Bước 2: Cấu hình file ipsec.conf

Cấu hình tương tự như file ipsec.conf bên VPNServerHN

Bước 3: Khởi động lại và kiểm tra trạng thái của bộ phần mềm OpenSwan

Khởi động lại ipsec: /etc/init.d/ipsec restart

Kiểm tra trạng thái: ipsec verify, trạng thái IPSec sau khi đã thiết lập đường hầm bên VPNServerHCM như trong Hình 4.7

```
vpn2@VPNServerHCM:~$ sudo ipsec verify
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path [OK]
Linux Openswan 2.6.32 (klips)
Checking for IPsec support in kernel [OK]
  KLIPS: checking for NAT Traversal support [OK]
  KLIPS: checking for OCF crypto offload support [N/A]
  Saref kernel support [N/A]
Checking that pluto is running [OK]
  Pluto listening for IKE on udp 500 [OK]
  Pluto listening for NAT-T on udp 4500 [OK]
Two or more interfaces found, checking IP forwarding [OK]
Checking NAT and MASQUERADEing [N/A]
Checking for 'ip' command [OK]
Checking /bin/sh is not /bin/dash [WARNING]
Checking for 'iptables' command [OK]
Opportunistic Encryption Support [DISABLED]
```

Hình 4.7: Trạng thái IPSec trên VPNServerHCM

4.1.2.3 Kết nối và kiểm tra kết nối

- Kiểm tra trạng thái đường hầm IPSec

Sử dụng lệnh: ipsec auto --status

```
000 using kernel interface: klips
000 interface ipsec0/eth0 10.10.0.2
000 interface ipsec0/eth0 10.10.0.2
000 %myid = (none)
000 debug none
000
000 virtual_private (%priv):
000 - allowed 3 subnets: 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12
000 - disallowed 0 subnets:
000 WARNING: Disallowed subnets in virtual_private= is empty. If you have
```

000 private address space in internal use, it should be excluded!

000

000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=64, keysize=192, keysize=192

000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=128, keysize=128, keysize=256

000 algorithm ESP auth attr: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysize=128, keysize=128

000 algorithm ESP auth attr: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysize=160, keysize=160

000

000 algorithm IKE encrypt: id=3, name=OAKLEY_BLOWFISH_CBC, blocksize=8, keydeflen=128

000 algorithm IKE encrypt: id=5, name=OAKLEY_3DES_CBC, blocksize=8, keydeflen=192

000 algorithm IKE encrypt: id=7, name=OAKLEY_AES_CBC, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: id=65004, name=OAKLEY__SERPENT__CBC, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: id=65005, name=OAKLEY_TWOFISH_CBC, blocksize=16, keydeflen=128

000 algorithm IKE encrypt: id=65289, name=OAKLEY_TWOFISH_CBC_SSH, blocksize=16, keydeflen=128

000 algorithm IKE hash: id=1, name=OAKLEY_MD5, hashsize=16

000 algorithm IKE hash: id=2, name=OAKLEY_SHA1, hashsize=20

000 algorithm IKE hash: id=4, name=OAKLEY_SHA2_256, hashsize=32

000 algorithm IKE hash: id=6, name=OAKLEY_SHA2_512, hashsize=64

000 algorithm IKE dh group: id=2, name=OAKLEY_GROUP_MODP1024, bits=1024

000 algorithm IKE dh group: id=5, name=OAKLEY_GROUP_MODP1536, bits=1536

000 algorithm IKE dh group: id=14, name=OAKLEY_GROUP_MODP2048, bits=2048

000 algorithm IKE dh group: id=15, name=OAKLEY_GROUP_MODP3072, bits=3072

```

000 algorithm IKE dh group: id=16, name=OAKLEY_GROUP_MODP4096, bits=4096
000 algorithm IKE dh group: id=17, name=OAKLEY_GROUP_MODP6144, bits=6144
000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192
000 algorithm IKE dh group: id=22, name=OAKLEY_GROUP_DH22, bits=1024
000 algorithm IKE dh group: id=23, name=OAKLEY_GROUP_DH23, bits=2048
000 algorithm IKE dh group: id=24, name=OAKLEY_GROUP_DH24, bits=2048
000
000 stats db_ops: {curr_cnt, total_cnt, maxsz} :context={0,0,0} trans={0,0,0} at trs={0,0,0}
000
000 "HN-HCM": 172.16.1.0/24===10.10.0.2<10.10.0.2>[+S=C]...10.10.0.3<10.10.0.3>[+S=C]===192.168.0.0/24; unrouted; eroute owner: #0
000 "HN-HCM": myip=unset; hisip=unset;
000 "HN-HCM": ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "HN-HCM": policy: RSASIG+ENCRYPT+TUNNEL+PFS+IKEv2ALLOW+SAREFTRACK; prio: 24,24; interface: eth0;
000 "HN-HCM": newest ISAKMP SA: #0; newest IPsec SA: #0;
000
000

```

- Thực hiện kết nối giữa ClientHN tới ClientHCM
Ping kiểm tra kết quả kết nối như trong Hình 4.8

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 172.16.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.1.2

C:\Documents and Settings\Administrator>ping 192.168.0.10

Pinging 192.168.0.10 with 32 bytes of data:

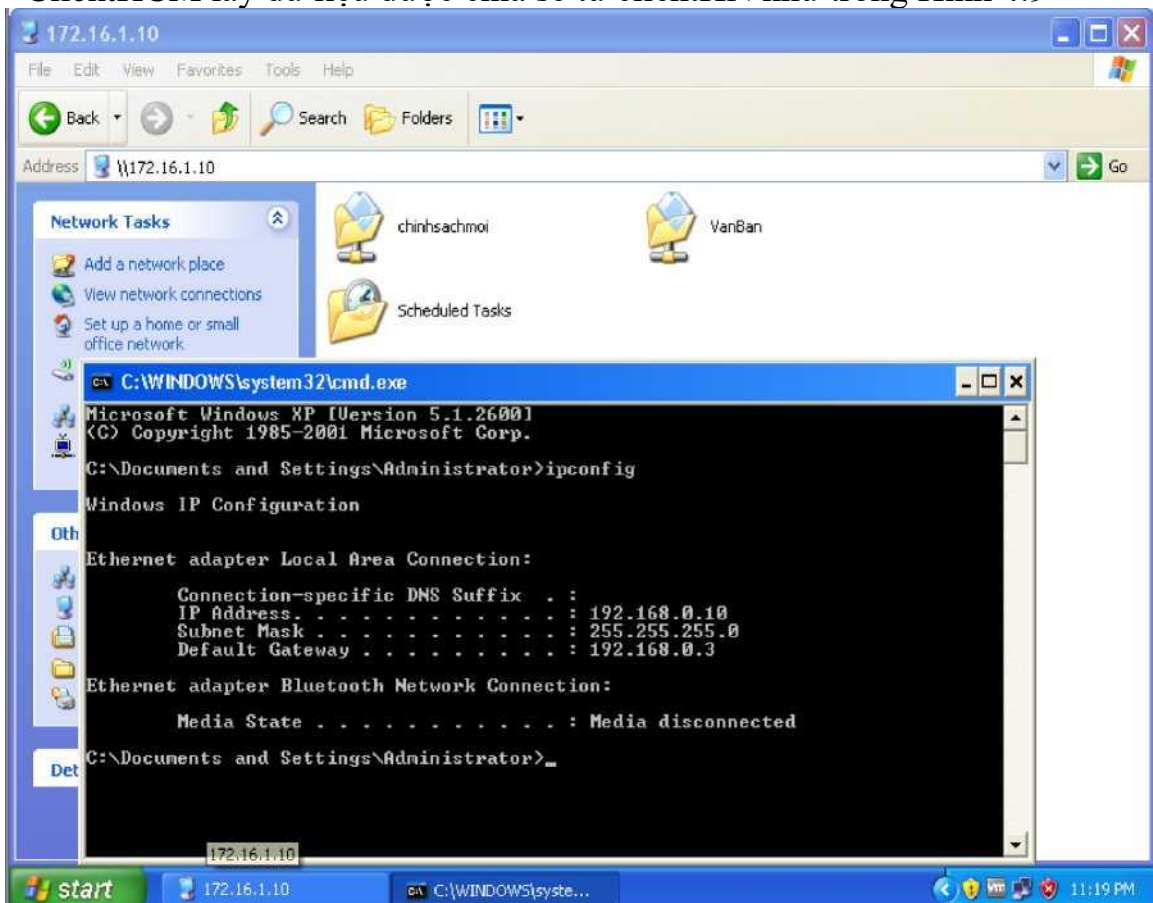
Reply from 192.168.0.10: bytes=32 time=1ms TTL=126
Reply from 192.168.0.10: bytes=32 time=1ms TTL=126
Reply from 192.168.0.10: bytes=32 time=1ms TTL=126
Reply from 192.168.0.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>_
```

Hình 4.8: Ping kiểm tra kết nối từ ClientHN tới ClientHCM

ClientHCM lấy dữ liệu được chia sẻ từ clientHN như trong Hình 4.9

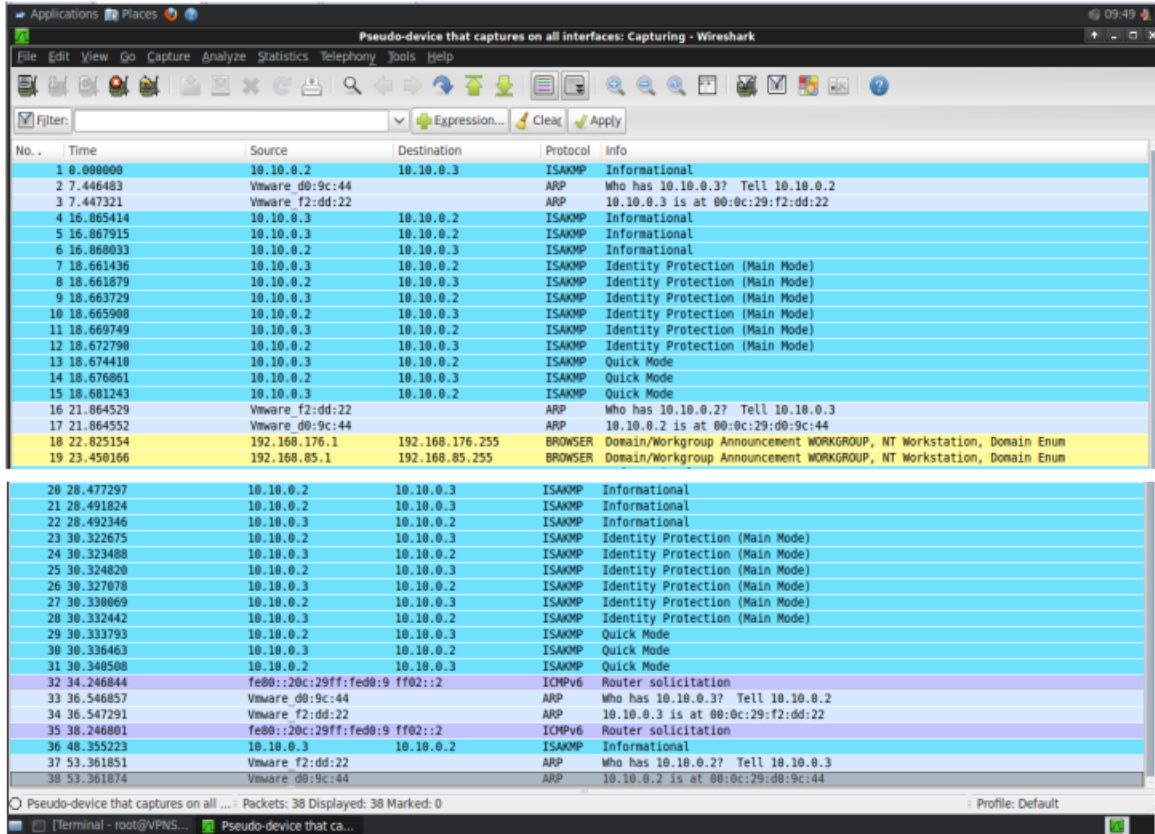


Hình 4.9: ClientHCM lấy dữ liệu được chia sẻ trên ClientHN

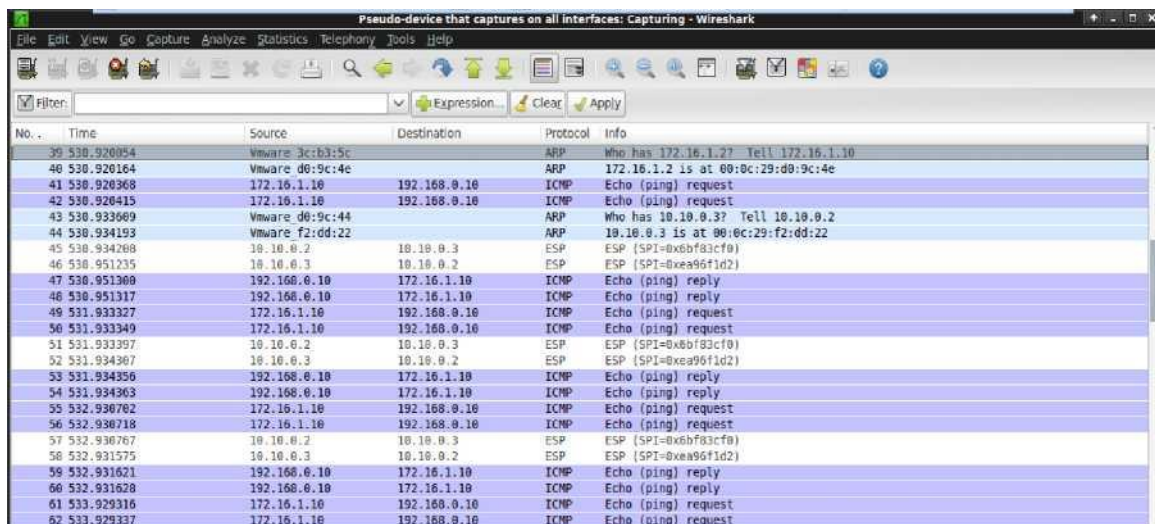
- Kiểm tra kết nối

Sử dụng phần mềm wireshark để bắt gói tin trên VPNServerHN

Quá trình trao đổi khóa và thiết lập kênh an toàn, kết quả như trong Hình 4.10 và Hình 4.11



Hình 4.10: Quá trình trao đổi khóa và thiết lập kênh an toàn trên VPNServerHN



Hình 4.11: Quá trình truyền tin trên kênh an toàn đã được thiết lập

4.1.3. Đánh giá kết quả thực nghiệm

Mô hình VPN site to site đã được triển khai và hoạt động nhằm giải quyết tốt vấn đề bài toán đặt ra. Kết quả thực nghiệm cho thấy một được hàm đã

được thiết lập giữa 2 vùng mạng, đường hầm đã được mã hóa và trong suốt với các máy client trong dải mạng nội bộ của 2 khu vực. Qua đó mà các nhân viên trong công ty có thể giao tiếp và trao đổi dữ liệu qua lại với nhau giữa 2 vùng mạng mà không cần phải quan tâm đến vấn đề bảo mật.

4.2. Thực nghiệm 2: Triển khai hệ thống VPN từ mã nguồn OpenSwan đã tùy biến

Thực nghiệm 2 của đồ án sẽ triển khai hệ thống VPN site to site từ mã nguồn OpenSwan đã tùy biến như trong phần 3.3 và dựa trên cơ sở thực nghiệm 1. Sử dụng mô hình trong hình 4.1 và các thành phần máy chủ, máy trạm như đã thiết lập trên thực nghiệm 1 cộng với bộ mã nguồn OpenSwan đã tùy biến trong phần 3.3 ta sẽ có 1 hệ thống VPN site to site dựa trên bộ mã nguồn OpenSwan đã tùy biến mà vẫn đảm bảo được những yêu cầu đề ra trong thực nghiệm 1, ngoài ra việc thiết lập và vận hành hệ thống VPN cũng trở nên đơn giản hơn với một số chức năng đã được viết hóa.

4.2.1. Triển khai thực nghiệm

4.2.1.1. Thiết lập máy chủ VPNServer

Tiến hành biên dịch và cài đặt mã nguồn bộ phần mềm OpenSwan đã tùy biến

Bước 1: Cài đặt các gói phần mềm hỗ trợ

Các hàm thư viện tính toán GNU và một số hỗ trợ khác:

- Gói dành cho Debian: libgmp3, libgmp3-dev, gawk/mawk, flex, bison, iproute, iptables
- Gói dành cho RPM: gmp, gmp-dev

Bước 2: Biên dịch mã nguồn đã tùy biến

Di chuyển vào thư mục mã nguồn đã tùy biến thực hiện lệnh biên dịch mã nguồn

Sử dụng lệnh: `make programs`

Bước 3: Cài đặt Klips cho mã nguồn đã tùy biến

Sử dụng 2 lệnh sau:

1: `make KERNELSRC=/lib/modules/'uname -r'/build module`

2: `make KERNELSRC=/lib/modules/'uname -r'/build install mininstall`

Bước 4: Bật chức năng IP Forwarding

Sử dụng lệnh: `echo 1 > /proc/sys/net/ipv4/ip_forward`

Sau đó restart ipsec: `/etc/init.d/ipsec restart`

Bước 5: Kiểm tra trạng thái IPsec

Sử dụng lệnh: `ipsec verify`

Trạng thái của IPsec sau khi đã biên dịch từ mã nguồn bộ phần mềm OpenSwan đã tùy biến như trong Hình 4.12 sau

```
Kiem tra giao thuc IPsec da duoc cai dat va van hanh mot cach chinh xac:
Kiem tra phien ban va duong dan IPsec [OK]
Linux Openswan 2.6.32 (klips)
Kiem tra IPsec duoc ho tro trong nhan [OK]
  KLIPS: ho tro NAT Traversal [OK]
  KLIPS: ho tro OCF crypto offload [N/A]
  Ho tro nhan SAREf [N/A]
Kiem tra Pluto hoat dong [OK]
  Pluto lang nghe giao thuc IKE voi giao thuc truyen udp cong 500 [OK]
  Pluto lang nghe giao thuc NAT-T voi giao thuc truyen udp cong 4500 [OK]
Kiem tra IP forwarding cua cac giao dien mang [OK]
Kiem tra NAT and MASQUERADEing [N/A]
Kiem tra for 'ip' command [OK]
Kiem tra /bin/sh is not /bin/dash [WARNING]
Kiem tra for 'iptables' command [OK]
Kiem tra Opportunistic Encryption [DISABLED]
```

Hình 4.12: Trạng thái IPsec sau khi biên dịch từ mã nguồn OpenSwan tùy biến

4.2.1.2 Cấu hình và cài đặt VPN site to site

- Trên VPNServerHN thực hiện những bước cấu hình sau:

Bước 1: Thực hiện trao đổi khóa công khai với VPNServerHCM

Export khóa công khai bên VPNServerEIN và import sang bên VPNServerHCM

Sử dụng lệnh: `ipsec showhostkey --tra`, khóa công khai của bên

VPNServerHN như trong Hình 4.13

```
root@VPNServerHN:~# ipsec showhostkey --tra
# rsakey AQRqhZtn
trairsasigkey=0sAQRqhZtn+M7xX8pGBUom0vcu4iZW9BxrcPKYLQd4h/skr7Nhh28j0S/
gBojKT2sx3exlmP3Nz98zh/TNHtmY9gyAWwoLrMNNNkiPMsX7bPA+RewYzRbtuUIIylcugM6DeJuGH3
BK0jNwe2cBylPlecWBJNTZgU3y9m08/VCgefFBRbuMlVfx4TqYmYekJphrPzkXxIN0LWVmGCoQRlMPf
S4ZasyzVKLSxoMXMEzRlxAhLEaiiR/TkY/g5cK8XXcRXdMXB2n5Gyi1DBUYws4o90RrPJw/oieadm3p0
9q+3pF04AeP8BqnVksVtTm9Lpd8dgcB0hXru9xth8crwsCWvA6KGTIXmWBHbLLI74cyUqLTX
```

Hình 4.13: Khóa công khai của VPNServerHN trên mã nguồn tùy biến

Bước 2: Cấu hình file ipsec.conf

Thực hiện lệnh: `nano /etc/ipsec.conf`

```
version 2 # Conforms to second version of ipsec.conf specification
config setup
```

```

nat_traversal=yes
#Bật hỗ trợ Nat-Traversal
virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.1
6.0.0/12,%v6:fd00: :/8,%v6:fe80: :/10
# Hỗ những dải mạng bên trong
protostack=klips
#Quyết định giao thức stack được sử dụng
Interfaces="ipsec0=eth0"
# Giao diện card mạng được gán cho card ipsec0
conn %default
    authby=rsasig
    # Sử dụng hệ mật khóa RSA
conn HN-HCM
    trai=10.10.0.2
    # Địa chỉ mạng public giao tiếp với VPNServerHCM
    traiphu=172.16.1.0/24
    # Dải mạng nội bộ HN
    phai=10.10.0.3
    # Địa chỉ mạng public giao tiếp với VPNServerHN
    phaiphu=192.168.0.0/24
    # Dải mạng nội bộ HCM
    type=tunnel
    # Kiểu giao thức truyền tin
    trairsasigkey=0sAQPRqhZtn+M7xX8pGBUomOvcu4iZW9Bxr
cPKYIQd4h/skr7Nhh28j0S/gBojKT2sx3exlmP3Nz98zh/TNHtmY9gyAWwwol
rMNNNkiPMsX7bPA+RewYzRbtuUIIylcugM6DeJuGH3BK0jNwe2cBy1PleW
BJNTZgU3y9mO8/VCgefFBRbuMlVxf4TqYmYekJphrPzkxxINOLWVmGCo
QRIMPfS4ZasyzVKLSXoMXMEzR1xAhlEaiiR/TkY/g5cK8XXcRXdMXB2n5
Gyi1DBUYWs4o9ORrPJw/oieadm3p09q+3pF04AeP8BqnVksvTtm9Lpd8dgcB
OhXru9xth8crwsCWvA6KGTIXmWBHblLI74cyUqlTX
    # Khóa công khai của VPNServerHN
    phairsasigkey=0sAQOD2PrJjZwPyMIWl5SusBi5kcIa/aYad7Kj

```


EFs9q4fN7rHRt9IUCIBCYVaXxl8wsIe6cxCyv3sggveNUr29cyUTvH86UWgQ
9vNdEZ5Twjg+QL88sGnnNOqKhxH4EBPyX/LFkjjPXm2k5TFFxWgwFev4
6NWs5q2x2+9T78PQciJtcx5Y/iowaVfanTIQCeqRTHHidBHd7bCmTjZUSCn
+vdlGnB7AkzLP2x7geMdiI/DiLLSx3neXQi6bEoUfVWN6Lat6Qg43IEGd3sO
hJoiNgU5mtAz2FipBNpOvTTcdjwytwDOU/Ukfp13cIp3xpInlZE3JDPfi7+MXI
h2r+MHtd 18Y4vrpH64rj 0y 1 p97o3st//QFH

Khóa công khai của VPNServerHCM

auto=start

Tải, định tuyến và bắt đầu thực hiện kết nối

Bước 3: Khởi động lại và kiểm tra trạng thái IPsec trên mã nguồn tùy biến

Khởi động lại ipsec: /etc/init.d/ipsec restart

Kiểm tra trạng thái: ipsec verify, trạng thái IPsec sau khi đã thiết lập đường hầm bên VPNServerHN như trong Hình 4.14

```
root@VPNServerHN:~# ipsec verify
Kiểm tra giao thức IPsec đã được cài đặt và vận hành một cách chính xác:
Kiểm tra phiên bản và đường dẫn IPsec [OK]
Linux Openswan 2.6.32 (klips)
Kiểm tra IPsec được hỗ trợ trong nhân [OK]
KLIPS: hỗ trợ NAT Traversal [OK]
KLIPS: hỗ trợ OCF crypto offload [N/A]
Hỗ trợ nhân SAREF [N/A]
Kiểm tra Pluto hoạt động [OK]
Pluto lắng nghe giao thức IKE với giao thức truyền udp cổng 500 [OK]
Pluto lắng nghe giao thức NAT-T với giao thức truyền udp cổng 4500 [OK]
Kiểm tra IP forwarding của các giao diện mạng [OK]
Kiểm tra NAT and MASQUERADEing [N/A]
Kiểm tra for 'ip' command [OK]
Kiểm tra /bin/sh is not /bin/dash [WARNING]
Kiểm tra for 'iptables' command [OK]
Kiểm tra Opportunistic Encryption [DISABLED]
```

Hình 4.14: Trạng thái IPsec VPNServerHN sau khi thiết lập trên mã nguồn tùy biến

- Trên VPNServerHCM thực hiện những bước cấu hình tương tự:

Bước 1: Thực hiện trao đổi khóa công khai với VPNServerHN

Export khóa công khai bên VPNServerHCM import sang bên VPNServerHN

Sử dụng lệnh: ipsec showhostkey --tra, khóa công khai của bên VPNServerHCM như trong Hình 4.15

```

root@VPNServerHCM:~# ipsec showhostkey --tra
# rsakey AQA2JRSg
trairsasigkey=0sAQA2JRSg3coaRGNv9LNvm10edrkl1UAYa4Rzk0LlrvNNeettqJxLld
TTp+zYLLKzZ8gtq43JR0CRtKqcPtRfTABs2/kIidVAZGCvt0Bjsex0TI6dY9eHmv6ce+K5atuTve/T
oZnwH3jYnPQbtJ4E8PoG80jLGEZQbh//eZZGv9EuJvkrGlcfp9poZY9bitT3baD3J3baq6HF18ehaS
uftJcIDXAUyKzAGrr975G+wYpXvVTfij0i7kKcQocB1Eloo4zHgUeYtzEKlzlcku6wRr6j0U3YmVw5
gm3Jwp9Y731J3y/wvk8/7AP0QtSxoFSZc+zKj+WdD025kA0xEIwU82IpgAPpMVGi9VqcR4Mqa5vVr0
cJ

```

Hình 4.1 5: Khóa công khai của VPNServerHCM trên mã nguồn tùy biến

Bước 2: Cấu hình file ipsec.conf

Thực hiện cấu hình tương tự như file ipsec.conf bên VPNServerHN

Bước 3: Khởi động lại và kiểm tra trạng thái IPsec trên mã nguồn tùy biến

Khởi động lại ipsec: /etc/init.d/ipsec restart

Kiểm tra trạng thái: ipsec verify, trạng thái IPsec sau khi đã thiết lập đường hầm bên VPNServerHCM như trong Hình 4 .16

```

root@VPNServerHCM:~# ipsec verify
Kiểm tra giao thức IPsec đã được cài đặt và vận hành một cách chính xác:
Kiểm tra phiên bản và đường dẫn IPsec [OK]
Linux Openswan 2.6.32 (klips)
Kiểm tra IPsec được hỗ trợ trong nhân [OK]
  KLIPS: Hỗ trợ NAT Traversal [OK]
  KLIPS: Hỗ trợ OCF crypto offload [N/A]
  Hỗ trợ SAREF kernel [N/A]
Kiểm tra Pluto hoạt động [OK]
  Pluto lắng nghe giao thức IKE với giao thức truyền udp cổng 500 [OK]
  Pluto lắng nghe giao thức NAT-T với giao thức truyền udp cổng 4500 [OK]
Kiểm tra IP forwarding của các giao diện mạng [OK]
Kiểm tra NAT and MASQUERADEing [N/A]
Kiểm tra for 'ip' command [OK]
Kiểm tra /bin/sh is not /bin/dash [WARNING]
Kiểm tra for 'iptables' command [OK]
Kiểm tra Opportunistic Encryption [DISABLED]

```

Hình 4.16: Trạng thái IPsec VPNServerHCM sau khi thiết lập trên mã nguồn tùy biến

4.2.1.3 Kết nối và kiểm tra kết nối

Việc thực hiện kết nối và kiểm tra kết nối cho ra những kết quả tương tự như trong phần 4.1.2.3

4.2.2. Đánh giá kết quả thực nghiệm

Qua việc triển khai hệ thống VPN từ mã nguồn OpenSwan đã tùy biến chúng ta có thể thấy bộ phần mềm OpenSwan đã tùy biến ở phần 3.3 hoạt động rất tốt. Với những kết quả thực nghiệm thu được tương tự như khi triển khai hệ thống VPN từ mã nguồn gốc của bộ phần mềm OpenSwan.

4.3. Kết luận chương 4

Chương 4 đã thực hiện triển khai hệ thống VPN site to site từ mã nguồn OpenSwan. Qua thực nghiệm 1, cho thấy việc biên dịch và triển khai IPsec VPN

từ mã nguồn bộ phần mềm OpenSwan không có nhiều khó khăn, hiệu quả mang lại từ OpenSwan với tính thực tế cao. Vì vậy, mà nó có thể được áp dụng vào môi trường thực tế với những yêu cầu nhất định để đạt được tính hiệu quả cao. OpenSwan là bộ phần mềm mã nguồn mở vậy nên bất kỳ ai cũng có thể trở thành nhà phát triển của nó, với thực nghiệm 2 của đề án sẽ giúp cho việc triển khai và vận hành IPSec VPN thông qua mã nguồn bộ phần mềm OpenSwan trở nên dễ dàng hơn.

KẾT LUẬN

Đồ án tốt nghiệp đề tài “**Nghiên cứu, thử nghiệm hệ thống VPN dựa trên OpenSwan**” cho thấy việc xây dựng hệ thống IPSec VPN dựa trên OpenSwan đáp ứng được các yêu cầu về tính bảo mật với chi phí triển khai thấp, phù hợp với nhiều mô hình công ty, tổ chức. Xây dựng hệ thống VPN dựa trên OpenSwan là một hướng giải quyết phù hợp với sự phát triển chung và yêu cầu đặt ra ngày càng cao của các công ty, tổ chức. Điều này góp phần vào việc thúc đẩy sự phát triển của ứng dụng công nghệ thông tin vào quản lý và an toàn thương mại điện tử trong thời kỳ hiện nay.

Đồ án đã hoàn thành được những mục tiêu đề ra như sau:

- Hệ thống lại kiến trúc tổng quan về VPN.
- Trình bày lý thuyết IPSec VPN.
- Nghiên cứu tổng quan về bộ phần mã nguồn mở OpenSwan.
- Phân tích, tùy biến mã nguồn bộ phần mềm OpenSwan.
- Thực nghiệm hệ thống VPN dựa trên OpenSwan:
 - + Hoàn thành thực nghiệm triển khai mô hình VPN Remote Access dựa trên gói cài đặt phần mềm OpenSwan.
 - + Hoàn thành thực nghiệm triển khai mô hình VPN Site to Site dựa trên việc biên dịch từ mã nguồn bộ phần mềm OpenSwan.
 - + Hoàn thành thực nghiệm triển khai mô hình VPN Site to Site dựa trên việc biên dịch từ mã nguồn bộ phần mềm OpenSwan đã tùy biến.

Bên cạnh những kết quả đạt được đồ án còn tồn tại những vấn đề sau:

- Chưa phân tích hết các module trong bộ mã nguồn OpenSwan.
- Các tùy chọn cấu hình IPSec VPN trong các thực nghiệm còn ở mức cơ bản.
- Việc tùy biến mã nguồn còn đơn giản. Chưa đi sâu vào nghiên cứu các hàm trong bộ mã nguồn.

Từ những vấn đề nêu trên em xin đưa ra hướng phát triển của đồ án:

- Thực hiện nghiên cứu sâu hơn về bộ phần mềm OpenSwan.
- Thiết lập các tùy chọn cấu hình IPSec VPN với nhiều kết hợp để đưa ra một thực nghiệm về hệ thống VPN với nhiều mức bảo mật.
- Việc tùy biến mã nguồn cần tối ưu hơn bằng cách can thiệp vào hoạt động của các hàm trong mã nguồn bộ phần mềm OpenSwan. Để đưa ra một bộ mã nguồn vừa dễ dàng cho người sử dụng với những chức năng việt hóa vừa tối ưu trong việc triển khai và vận hành IPSec VPN dựa trên mã nguồn bộ phần mềm OpenSwan.

TÀI LIỆU THAM KHẢO

Tài liệu tiếng việt

1. *Giáo trình An toàn mạng riêng ảo*, “Học viện Kỹ thuật Mật mã”.

Tài liệu tiếng anh

2. Dave Kosiur. *Building and Managing Virtual Private Networks*. 1998.
3. Jon C. Snader. *VPNs Illustrated: Tunnels, VPNs, and IPSec*. 2005
4. Paul Wouters, Ken Bantoft. *Building and Integrating Virtual Private Networks with OpenSwan*. 2006.
5. James S. Tiller. *A Technical Guide to IPSec Virtual Private Networks*. 2000
6. Naganand Doraswamy, Dan Harkins. *IPSec: The New Security Standard for the Internet, Intranets and Virtual Private networks, Second Edition*. 2003

Tài liệu trang web

7. Xelerance. *OpenSwan*
<URL: <https://www.openswan.org/>>