

TRƯỜNG ĐẠI HỌC HUẾ
TRƯỜNG ĐẠI HỌC KHOA HỌC
KHOA ĐIỆN, ĐIỆN TỬ & CÔNG NGHỆ VẬT LIỆU



ĐỒ ÁN CHUYÊN NGÀNH KỸ THUẬT VIỄN THÔNG 2

VPN SITE TO SITE

SVTH : HỒ VĂN NHẬT
MÃ SINH VIÊN : 19T1051013
NGÀNH : KỸ THUẬT VIỄN THÔNG
GVHD : HỒ ĐỨC TÂM LINH

Huế 6/2023

MỤC LỤC

| | |
|---|----|
| DANH MỤC HÌNH ẢNH..... | i |
| LỜI NÓI ĐẦU | 1 |
| CHƯƠNG I. TỔNG QUAN VỀ VPN..... | 2 |
| 1.1. ĐỊNH NGHĨA, CHỨC NĂNG VÀ ƯU ĐIỂM CỦA VPN..... | 2 |
| 1.1.1. Khái niệm cơ bản về VPN..... | 2 |
| 1.1.2. Chức năng của VPN..... | 3 |
| 1.1.3. Ưu điểm của VPN | 4 |
| 1.1.4. Các yêu cầu cơ bản đối với một giải pháp VPN..... | 6 |
| 1.2. ĐƯỜNG HÀM VÀ MÃ HÓA | 7 |
| CHƯƠNG II. CÁC KIỂU VPN..... | 8 |
| 2.1. CÁC VPN TRUY CẬP (Remote Access VPNs) | 8 |
| 2.2. CÁC VPN NỘI BỘ (INTRANET VPNS): | 10 |
| 2.3. CÁC VPN MỞ RỘNG (EXTRANET VPNS): | 12 |
| CHƯƠNG III. GIAO THỨC ĐƯỜNG HÀM IPSEC VPN | 15 |
| 3.1. GIỚI THIỆU CÁC GIAO THỨC ĐƯỜNG HÀM | 15 |
| 3.2. GIAO THỨC BẢO MẬT IP (IP SECURITY PROTOCOL) | 15 |
| 3.3. NHỮNG HẠN CHẾ CỦA IPSEC..... | 29 |
| CHƯƠNG IV. THIẾT LẬP VPN SITE TO SITE (DÙNG PHẦN MỀM PACKET TRACER)..... | 30 |
| 4.1. GIỚI THIỆU VỀ PHẦN MỀM CISCO PACKET TRACER..... | 30 |
| 4.2. THIẾT LẬP MÔ HÌNH VPN SITE TO SITE | 30 |
| 4.2.1. Mô hình VPN Site to Site giữa hai chi nhánh HUẾ và SÀI GÒN | 30 |
| 4.2.2. Cấu hình đặt địa chỉ IP | 31 |
| 4.2.3. Cấu hình VLAN & TRUNK | 31 |
| 4.2.4. Cấu hình định tuyến và DHCP trên 2 Router của 2 chi nhánh..... | 33 |
| 4.2.5. Cấu hình VPN Site – to – Site: | 34 |
| 4.2.6. Cấu hình DNS – Server cho Web – server và Mail – server..... | 36 |
| 4.3. KIỂM TRA KẾT QUẢ CẤU HÌNH | 36 |
| CHƯƠNG V. KẾT LUẬN..... | 43 |

DANH MỤC HÌNH ẢNH

| | |
|---|----|
| Hình 1.1. Mô hình VPN cơ bản..... | 2 |
| Hình 1. 2. Mô hình mạng VPN | 3 |
| Hình 1. 3. Ưu điểm của VPN so với mạng truyền thống | 5 |
| Hình 1. 4. Các Ưu điểm của VPN..... | 5 |
| Hình 1. 5. Đường hầm VPN | 7 |
| Hình 2. 1. Mô hình mạng VPN truy cập..... | 8 |
| Hình 2. 2. Cài đặt Remote Access VPN | 9 |
| Hình 2. 3. Mô hình mạng VPN nội bộ..... | 11 |
| Hình 2. 4. Mô hình mạng VPN mở rộng..... | 13 |
| Hình 2. 5. Thiết lập Extranet VPN..... | 14 |
| Hình 2. 6. Ba loại mạng riêng ảo | 14 |
| Hình 3. 1. Sơ đồ khung IPSec..... | 16 |
| Hình 3. 2. Chế độ Transport..... | 17 |
| Hình 3. 3. Chế độ Tunnel..... | 18 |
| Hình 3. 4. Thiết bị mạng thực hiện trong IPSec trong chế độ đường hầm | 19 |
| Hình 3. 5. ESP trong mode Tunnel và transport..... | 19 |
| Hình 3. 6. Các bước hoạt động của IPSec..... | 21 |
| Hình 3. 7. Sơ đồ kết nối hai Router chạy IPSec | 21 |
| Hình 3. 8. Xác định luồng traffic | 22 |
| Hình 3. 9. Bước một IKE | 23 |
| Hình 3. 10. Quá trình trao đổi đầu tiên | 23 |
| Hình 3. 11. Quá trình trao đổi thứ ba | 24 |
| Hình 3. 12. Bước 2 IKE | 25 |
| Hình 3. 13. Thỏa thuận tập transform | 26 |
| Hình 3. 14. Các thông số của SA..... | 27 |

| | |
|---|----|
| Hình 3. 15. Một phiên IPSec | 28 |
| Hình 3. 16. Kết thúc một phiên IPSec | 28 |
| Hình 4. 1. Sơ đồ mô phỏng VPN site to site..... | 30 |
| Hình 4. 2. Cấu hình DNS – Server..... | 36 |
| Hình 4. 3. Từ PC Phòng Kế Toán ping đến PC Phòng Kinh Doanh | 36 |
| Hình 4. 4. Từ PC Phòng Kế Toán ping đến PC Phòng Giám Đốc..... | 37 |
| Hình 4. 5. Từ PC Phòng Kế Toán truy cập Web server Huế..... | 37 |
| Hình 4. 6. Từ PC Phòng Kế Toán ping đến PC Phòng Kinh Doanh | 38 |
| Hình 4. 7. Từ PC Phòng Kế Toán ping đến PC Phòng Giám Đốc..... | 38 |
| Hình 4. 8. Từ PC Phòng Kế Toán truy cập Web server Sài Gòn..... | 38 |
| Hình 4. 9. Ping giữa hai chi nhánh phòng Kế Toán | 39 |
| Hình 4. 10. Ping giữa hai chi nhánh phòng Kinh Doanh | 39 |
| Hình 4. 11. Từ PC chi nhánh HUẾ truy cập Web SÀI GÒN | 40 |
| Hình 4. 12. Từ PC chi nhánh SÀI GÒN truy cập Web HUẾ | 40 |
| Hình 4. 13. Gửi Email từ Phòng kế toán đến Phòng kinh doanh cùng chi nhánh Huế... | 41 |
| Hình 4. 14. Gửi Email từ Phòng kế toán đến Phòng giám đốc cùng chi nhánh SÀI GÒN | 41 |
| Hình 4. 15. Gửi email giữa hai chi nhánh | 42 |

LỜI NÓI ĐẦU

Cùng với sự phát triển của công nghệ thông tin, công nghệ mạng máy tính và đặc biệt là mạng Internet ngày càng phát triển đa dạng và phong phú. Các dịch vụ trên mạng Internet đã xâm nhập vào hầu hết các lĩnh vực trong đời sống xã hội. 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 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.

Xuất phát từ những thực tế nêu trên, hiện nay trên thế giới đã xuất hiện rất nhiều công nghệ liên quan đến bảo mật hệ thống và mạng máy tính, việc nắm bắt những công nghệ này là hết sức cần thiết.

Chính vì vậy, thông qua việc nghiên cứu một cách tổng quan về bảo mật hệ thống và một công nghệ cụ thể liên quan đến bảo mật hệ thống, đó là công nghệ Mạng Riêng Ảo (VPN-Virtual Private Network) trong ***Đồ án chuyên ngành kỹ thuật viễn thông 2*** này của em có thể góp phần vào việc hiểu thêm và nắm bắt rõ về kỹ thuật VPN trong doanh nghiệp cũng như là trong nhà trường để phục vụ cho lĩnh vực học tập và nghiên cứu.

Trong quá trình xây dựng đồ án này, em đã nhận được rất nhiều sự giúp đỡ, góp ý, và ủng hộ của thầy cô giáo, bạn bè đồng nghiệp. Em xin chân thành cảm ơn sự hướng dẫn nhiệt tình của thầy **Hồ Đức Tâm Linh**, là thầy giáo trực tiếp hướng dẫn bài đồ án này của em.

Bảo mật hệ thống và kỹ thuật VPN là một vấn đề rộng và mới đối với Việt Nam, đồng thời do kinh nghiệm và kỹ thuật còn hạn chế, nội dung tài liệu chắc chắn sẽ còn nhiều sai sót, hy vọng các thầy cùng các bạn sinh viên sẽ đóng góp nhiều ý kiến bổ sung hoàn thiện để tài liệu được chính xác và hữu ích hơn.

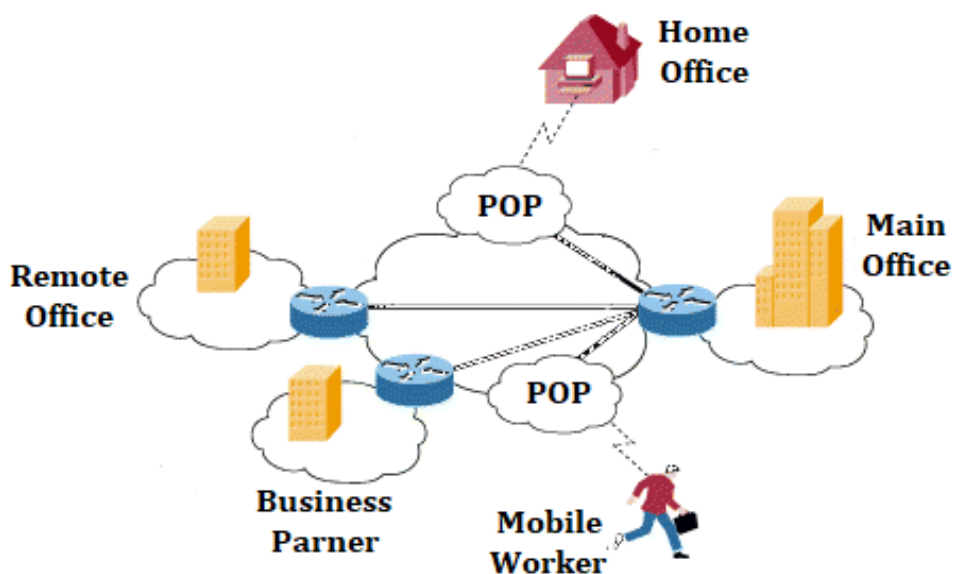
CHƯƠNG I.

TỔNG QUAN VỀ VPN

1.1. ĐỊNH NGHĨA, CHỨC NĂNG VÀ ƯU ĐIỂM CỦA VPN

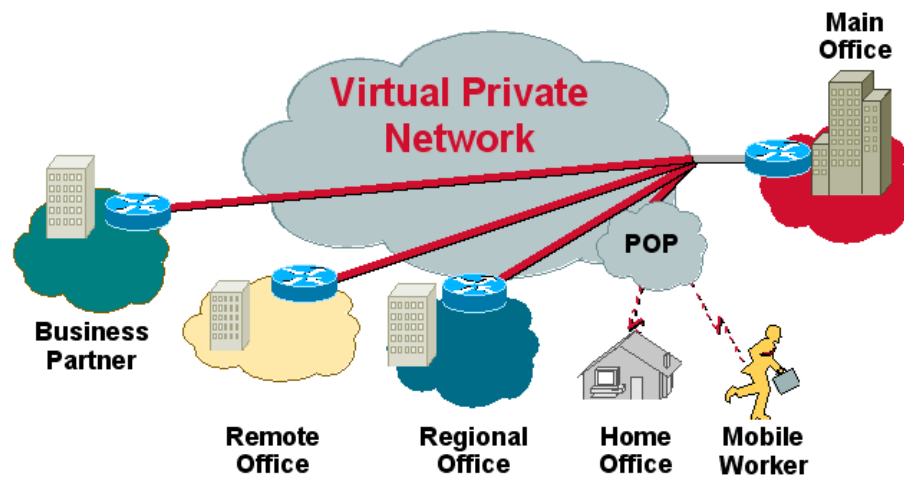
1.1.1. *Khái niệm cơ bản về VPN*

- ✓ Phương án truyền thông nhanh, an toàn và tin cậy đang trở thành mối quan tâm của nhiều doanh nghiệp, đặc biệt là các doanh nghiệp có các địa điểm phân tán về mặt địa lý. Nếu như trước đây giải pháp thông thường là thuê các đường truyền riêng (leased lines) để duy trì mạng WAN (Wide Area Network). Các đường truyền này giới hạn từ ISDN (128 Kbps) đến đường cáp quang OC3 (optical carrier-3, 155Mbps). Mỗi mạng WAN đều có các điểm thuận lợi trên một mạng công cộng như Internet trong độ tin cậy, hiệu năng và tính an toàn, bảo mật. Nhưng để bảo trì một mạng WAN, đặc biệt khi sử dụng các đường truyền riêng, có thể trở nên quá đắt khi doanh nghiệp muốn mở rộng các chi nhánh.
- ✓ Khi tính phổ biến của Internet gia tăng, các doanh nghiệp đầu tư vào nó như một phương tiện quảng bá và mở rộng các mạng mà họ sở hữu. Ban đầu, là các mạng nội bộ (Intranet) mà các site được bảo mật bằng mật khẩu được thiết kế cho việc sử dụng chỉ bởi các thành viên trong công ty.



Hình 1.1. Mô hình VPN cơ bản

- ✓ Về căn bản, mỗi VPN(virtual private network) là một mạng riêng rẽ sử dụng một mạng chung (thường là Internet) để kết nối cùng với các site (các mạng riêng lẻ) hay nhiều người sử dụng từ xa. Thay cho việc sử dụng bởi một kết nối thực, chuyên dụng như đường Leased Line, mỗi VPN sử dụng các kết nối ảo được dẫn qua đường Internet từ mạng riêng của công ty tới các site của các nhân viên từ xa.



Hình 1. 2. Mô hình mạng VPN

- ✓ Những thiết bị ở đầu mạng hỗ trợ cho mạng riêng ảo là switch, router và firewall. Những thiết bị này có thể được quản trị bởi công ty hoặc các nhà cung cấp dịch vụ như ISP..
- ✓ VPN được gọi là mạng ảo vì đây là một cách thiết lập một mạng riêng qua một mạng công cộng sử dụng các kết nối tạm thời. Những kết nối bảo mật được thiết lập giữa 2 host , giữa host và mạng hoặc giữa hai mạng với nhau.
- ✓ Một VPN có thể được xây dựng bằng cách sử dụng “Đường hầm” và “Mã hoá”. VPN có thể xuất hiện ở bất cứ lớp nào trong mô hình OSI. VPN là sự cải tiến cơ sở hạ tầng mạng WAN mà làm thay đổi hay làm tăng thêm tính chất của các mạng cục bộ.

1.1.2. Chức năng của VPN

VPN cung cấp ba chức năng chính:

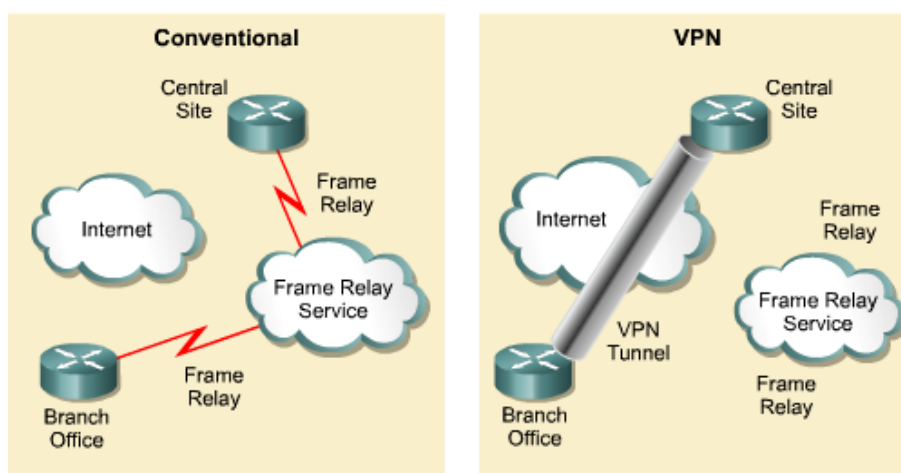
- ✓ **Sự tin cậy (Confidentiality):** Người gửi có thể mã hoá các gói dữ liệu trước khi truyền chúng ngang qua mạng. Bằng cách làm như vậy, không một ai có thể truy cập thông tin mà không được cho phép. Và nếu có lấy được thì cũng không đọc được.

- ✓ **Tính toàn vẹn dữ liệu (Data Integrity):** người nhận có thể kiểm tra rằng dữ liệu đã được truyền qua mạng Internet mà không có sự thay đổi nào.
- ✓ **Xác thực nguồn gốc (Origin Authentication):** Người nhận có thể xác thực nguồn gốc của gói dữ liệu, đảm bảo và công nhận nguồn thông tin.

1.1.3. Ưu điểm của VPN

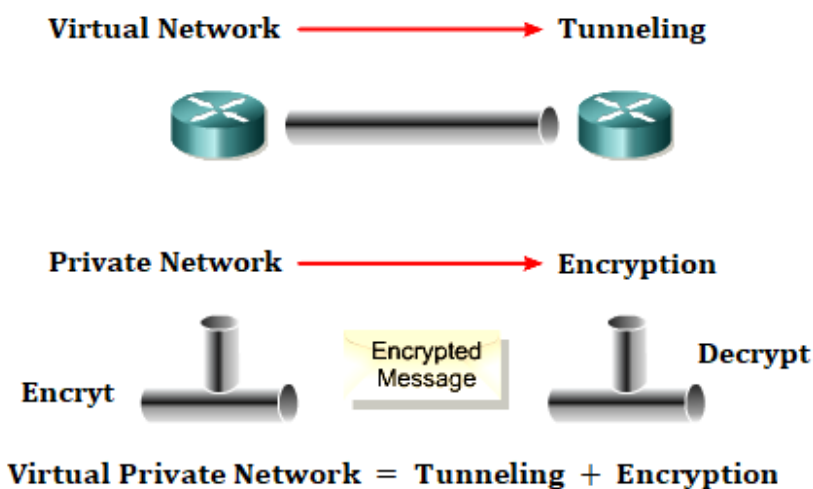
VPN có nhiều ưu điểm hơn so với các mạng leased-line truyền thống. Nó bao gồm:

- ✓ **VPN làm giảm chi phí hơn so với mạng cục bộ:** Tổng giá thành của việc sở hữu một mạng VPN sẽ được thu nhỏ, do chỉ phải trả ít hơn cho việc thuê băng thông đường truyền, các thiết bị mạng đường trục, và hoạt động của hệ thống. Giá thành cho việc kết nối LAN – to – LAN giảm từ 20 – 30% so với việc sử dụng đường Leased-line truyền thống. Còn đối với việc truy cập từ xa thì giảm tới từ 60 – 80%.
- ✓ **VPN tạo ra tính mềm dẻo cho khả năng quản lý Internet:** Các VPN đã kết thừa phát huy hơn nữa tính mềm dẻo và khả năng mở rộng kiến trúc mạng hơn là các mạng WAN truyền thống. Điều này giúp các doanh nghiệp có thể nhanh chóng và hiệu quả kinh tế cho việc mở rộng hay huỷ bỏ kết nối của các trụ sở ở xa, các người sử dụng di động..., và mở rộng các đối tác kinh doanh khi có nhu cầu.
- ✓ **VPN làm đơn giản hoá cho việc quản lý các công việc so với việc sở hữu và vận hành một mạng cục bộ:** Các doanh nghiệp có thể cho phép sử dụng một vài hay tất cả các dịch vụ của mạng WAN, giúp các doanh nghiệp có thể tập chung vào các đối tượng kinh doanh chính, thay vì quản lý một mạng WAN hay mạng quay số từ xa.
- ✓ **VPN cung cấp các kiểu mạng đường hầm và làm giả thiếu các công việc quản lý:** Một Backbone IP sẽ loại bỏ các PVC (Permanent Virtual Circuit) cố định tương ứng với các giao thức kết nối như là Frame Relay và ATM. Điều này tạo ra một kiểu mạng lưới hoàn chỉnh trong khi giảm được độ phức tạp và giá thành.



Hình 1. 3. Ưu điểm của VPN so với mạng truyền thống

- ✓ Một mạng VPN có được những ưu điểm của mạng cục bộ trên cơ sở hạ tầng của mạng IP công cộng. Các ưu điểm này bao gồm tính bảo mật và sử dụng đa giao thức.



Hình 1. 4. Các Ưu điểm của VPN

- ✓ Một mạng ảo được tạo ra nhờ các giao thức đường hầm trên một kết nối IP chuẩn. GRE (Generic Routing Protocol), L2TP (Layer 2 Tunneling Protocol) và IPSec là ba phương thức đường hầm.
- ✓ Một mạng cục bộ là một mạng mà đảm bảo độ tin cậy, tính toàn vẹn và xác thực, gọi tắt là CIA. Mã hoá dữ liệu và sử dụng giao thức IPSec giúp giữ liệu có thể chung chuyển trên Web với các tính chất CIA tương tự như là một mạng cục bộ.

1.1.4. Các yêu cầu cơ bản đối với một giải pháp VPN

Có 4 yêu cầu cần đạt được khi xây dựng mạng riêng ảo.

- **Tính tương thích (compatibility)**

Mỗi công ty, mỗi doanh nghiệp đều được xây dựng các hệ thống mạng nội bộ và diện rộng của mình dựa trên các thủ tục khác nhau và không tuân theo một chuẩn nhất định của nhà cung cấp dịch vụ. Rất nhiều các hệ thống mạng không sử dụng các chuẩn TCP/IP vì vậy không thể kết nối trực tiếp với Internet. Để có thể sử dụng được IP VPN tất cả các hệ thống mạng riêng đều phải được chuyển sang một hệ thống địa chỉ theo chuẩn sử dụng trong internet cũng như bổ sung các tính năng về tạo kênh kết nối ảo, cài đặt cổng kết nối internet có chức năng trong việc chuyển đổi các thủ tục khác nhau sang chuẩn IP. 77% số lượng khách hàng được hỏi yêu cầu khi chọn một nhà cung cấp dịch vụ IP VPN phải tương thích với các thiết bị hiện có của họ.

- **Tính bảo mật (security)**

Tính bảo mật cho khách hàng là một yếu tố quan trọng nhất đối với một giải pháp VPN. Người sử dụng cần được đảm bảo các dữ liệu thông qua mạng VPN đạt được mức độ an toàn giống như trong một hệ thống mạng dùng riêng do họ tự xây dựng và quản lý.

Việc cung cấp tính năng bảo đảm an toàn cần đảm bảo hai mục tiêu sau:

- Cung cấp tính năng an toàn thích hợp bao gồm: cung cấp mật khẩu cho người sử dụng trong mạng và mã hoá dữ liệu khi truyền.
- Đơn giản trong việc duy trì quản lý, sử dụng. Đòi hỏi thuận tiện và đơn giản cho người sử dụng cũng như nhà quản trị mạng trong việc cài đặt cũng như quản trị hệ thống.

- **Tính khả dụng (Availability):**

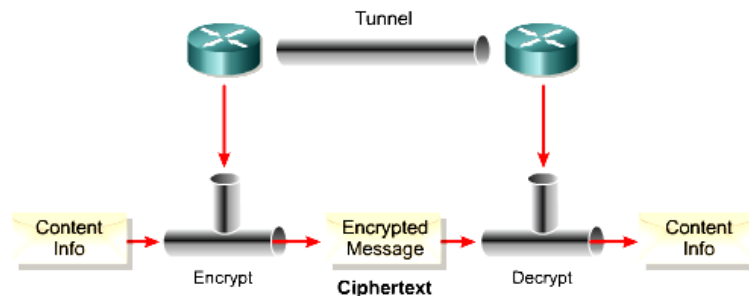
Một giải pháp VPN cần thiết phải cung cấp được tính bảo đảm về chất lượng, hiệu suất sử dụng dịch vụ cũng như dung lượng truyền.

- **Tiêu chuẩn về chất lượng dịch vụ (QoS):**

Tiêu chuẩn đánh giá của một mạng lưới có khả năng đảm bảo chất lượng dịch vụ cung cấp đầu cuối đến đầu cuối. QoS liên quan đến khả năng đảm bảo độ trễ dịch vụ trong một phạm vi nhất định hoặc liên quan đến cả hai vấn đề trên

1.2. ĐƯỜNG HÀM VÀ MÃ HÓA

Chức năng chính của VPN đó là cung cấp sự bảo mật bằng cách mã hoá qua một đường hầm.



Hình 1. 5. Đường hầm VPN

Đường hầm (Tunnel) cung cấp các kết nối logic, đi từ điểm qua mạng IP không hướng kết nối. Điều này giúp cho việc sử dụng các ưu điểm các tính năng bảo mật. Các giải pháp đường hầm cho VPN là sử dụng sự mã hoá để bảo vệ dữ liệu không bị xem trộm bởi bất cứ những ai không được phép và để thực hiện đóng gói đa giao thức nếu cần thiết. Mã hoá được sử dụng để tạo kết nối đường hầm để dữ liệu chỉ có thể được đọc bởi người nhận và người gửi.

Mã hoá(Encryption) chắc chắn rằng bản tin không bị đọc bởi bất kỳ ai nhưng có thể đọc được bởi người nhận. Khi mà càng có nhiều thông tin lưu thông trên mạng thì sự cần thiết đối với việc mã hoá thông tin càng trở nên quan trọng. Mã hoá sẽ biến đổi nội dung thông tin thành trong một văn bản mật mã mà là vô nghĩa trong dạng mật mã của nó. Chức năng giải mã để khôi phục văn bản mật mã thành nội dung thông tin có thể dùng được cho người nhận.

CHƯƠNG II.

CÁC KIỂU VPN

VPNs nhằm hướng vào 3 yêu cầu cơ bản sau đây :

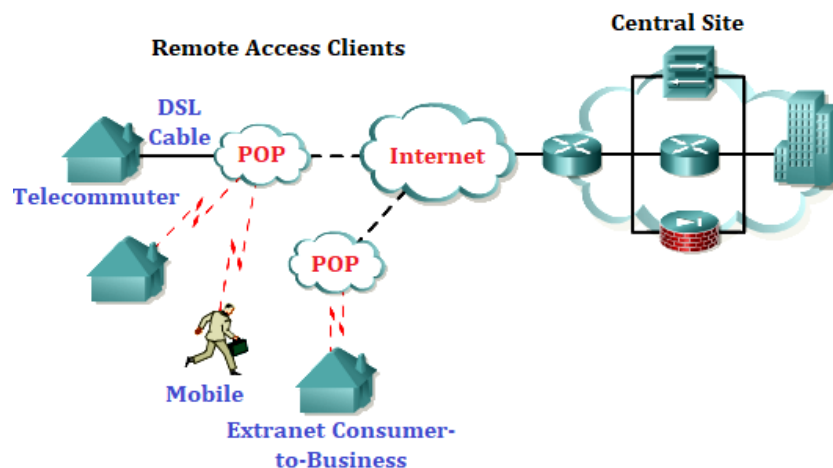
- Có thể truy cập bất cứ lúc nào bằng điều khiển từ xa, bằng điện thoại cầm tay, và việc liên lạc giữa các nhân viên của một tổ chức tới các tài nguyên mạng.
- Nối kết thông tin liên lạc giữa các chi nhánh văn phòng từ xa.
- Được điều khiển truy nhập tài nguyên mạng khi cần thiết của khách hàng, nhà cung cấp và những đối tượng quan trọng của công ty nhằm hợp tác kinh doanh.

Dựa trên những nhu cầu cơ bản trên, ngày nay VPNs đã phát triển và phân chia ra làm 3 phân loại chính sau :

- Remote Access VPNs.
- Intranet VPNs.
- Extranet VPNs.

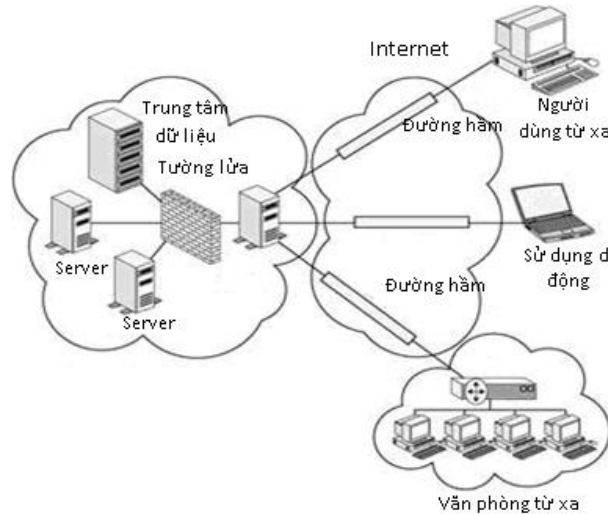
2.1. CÁC VPN TRUY CẬP (Remote Access VPNs)

- Giống như gợi ý của tên gọi, Remote Access VPNs cho phép 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 tổ chức. 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 hợp tác.
- Các truy cập VPN thường yêu cầu một vài kiểu phần mềm client chạy trên máy tính của người sử dụng. Kiểu VPN này thường được gọi là VPN truy cập từ xa.



Hình 2. 1. Mô hình mạng VPN truy cập

- Một số thành phần chính:
 - Remote Access Server (RAS) : được đặt tại trung tâm có nhiệm vụ xác nhận và chứng nhận các yêu cầu gửi tới.
 - Quay số kết nối đến trung tâm, điều này sẽ làm giảm chi phí cho một số yêu cầu ở khá xa so với trung tâm.
 - Hỗ trợ cho những người có nhiệm vụ cấu hình, bảo trì và quản lý RAS và hỗ trợ truy cập từ xa bởi người dùng.
- Bằng việc triển khai Remote Access VPNs, những người dùng từ xa hoặc các chi nhánh văn phòng chỉ cần cài đặt một kết nối cục bộ đến nhà cung cấp dịch vụ ISP hoặc ISP's POP và kết nối đến tài nguyên thông qua Internet.



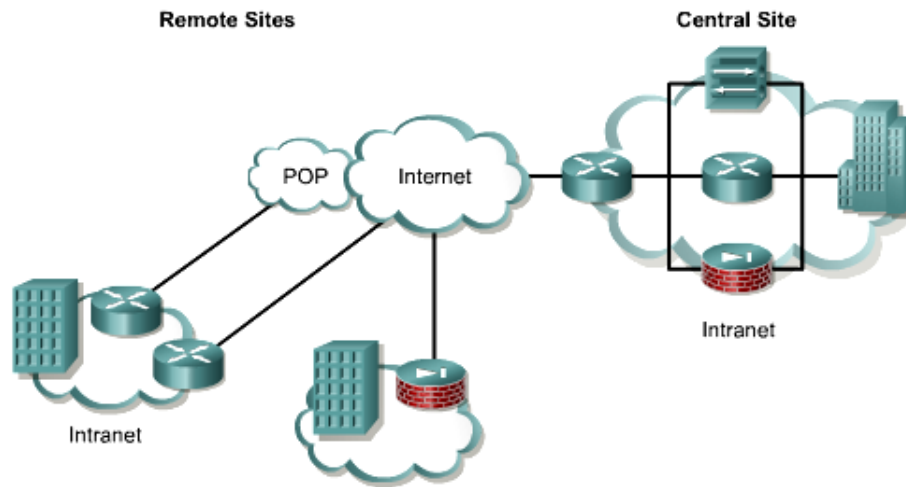
Hình 2. 2. Cài đặt Remote Access VPN

- Thuận lợi chính của Remote Access VPNs :
 - Sự cần thiết của RAS và việc kết hợp với modem được loại trừ.
 - Sự cần thiết hỗ trợ cho người dùng cá nhân được loại trừ bởi vì kết nối từ xa đã được tạo điều kiện thuận lợi bởi ISP.
 - Việc quay số từ những khoảng cách xa được loại trừ , thay vào đó, những kết nối với khoảng cách xa sẽ được thay thế bởi các kết nối cục bộ.
 - Giảm giá thành chi phí cho các kết nối với khoảng cách xa.
 - Do đây là một kết nối mạng tính cục bộ, do vậy tốc độ nối kết sẽ cao hơn so với kết nối trực tiếp đến những khoảng cách xa.

- VPNs cung cấp khả năng truy cập đến trung tâm tốt hơn bởi vì nó hỗ trợ dịch vụ truy cập ở mức độ tối thiểu nhất cho dù có sự tăng nhanh chóng các kết nối đồng thời đến mạng.
- Ngoài những thuận lợi trên, VPNs cũng tồn tại một số bất lợi khác như :
 - Remote Access VPNs cũng không bảo đảm được chất lượng phục vụ.
 - Khả năng mất dữ liệu là rất cao, thêm nữa là các phân đoạn của gói dữ liệu có thể đi ra ngoài và bị thất thoát.
 - Do độ phức tạp của thuật toán mã hoá, protocol overhead tăng đáng kể, điều này gây khó khăn cho quá trình xác nhận. Thêm vào đó, việc nén dữ liệu IP và PPP-based diễn ra vô cùng chậm chạp và tồi tệ.
 - 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.

2.2. CÁC VPN NỘI BỘ (INTRANET VPNS):

- Intranet VPNs được sử dụng để kết nối đến các chi nhánh văn phòng của tổ chức đến Corporate Intranet (backbone router) sử dụng campus router. Theo mô hình này sẽ rất tốn chi phí do phải sử dụng 2 router để thiết lập được mạng, thêm vào đó, việc triển khai, bảo trì và quản lý mạng Intranet Backbone sẽ rất tốn kém còn tùy thuộc vào lượng lưu thông trên mạng đi trên nó và phạm vi địa lý của toàn bộ mạng Intranet.
- Để giải quyết vấn đề trên, sự tốn kém của WAN backbone được thay thế bởi các kết nối Internet với chi phí thấp, điều này có thể giảm một lượng chi phí đáng kể của việc triển khai mạng Intranet.
- Intranet VPNs là một VPN nội bộ được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một công ty. Điều này cho phép tất cả các địa điểm có thể truy cập các nguồn dữ liệu được phép trong toàn bộ mạng của công ty. Các VPN nội bộ liên kết trụ sở chính, các văn phòng, và các văn phòng chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối mà luôn luôn được mã hoá. Kiểu VPN này thường được cấu hình như là một VPN Site-to-Site.

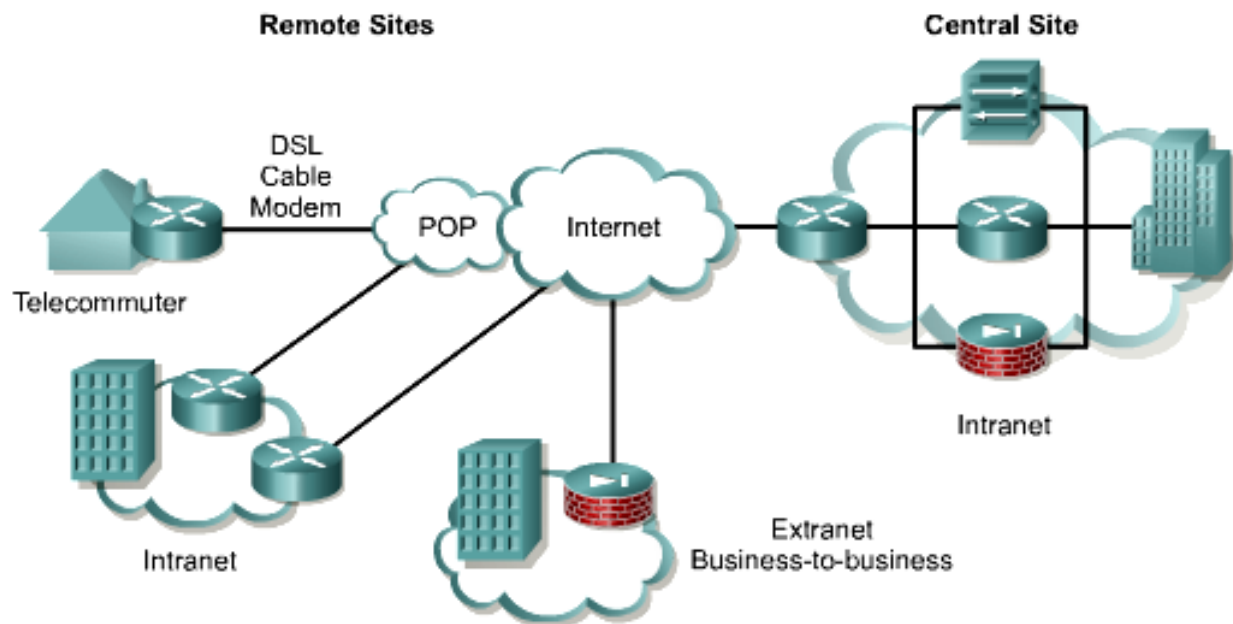


Hình 2. 3. Mô hình mạng VPN nội bộ.

- Những thuận lợi chính của Intranet setup dựa trên VPN:
 - Hiệu quả chi phí hơn do giảm số lượng router được sử dụng theo mô hình WAN backbone
 - Giảm thiểu đáng kể số lượng hỗ trợ yêu cầu người dùng cá nhân qua toàn cầu, các trạm ở một số remote site khác nhau.
 - Bởi vì Internet hoạt động như một kết nối trung gian, nó dễ dàng cung cấp những kết nối mới ngang hàng.
 - Kết nối nhanh hơn và tốt hơn do về bản chất kết nối đến nhà cung cấp dịch vụ, loại bỏ vấn đề về khoảng cách xa và thêm nữa giúp tổ chức giảm thiểu chi phí cho việc thực hiện Intranet.
- Những bất lợi chính kết hợp với cách giải quyết :
 - Bởi vì dữ liệu vẫn còn tunnel trong suốt quá trình chia sẻ trên mạng công cộng-Internet-và những nguy cơ tấn công, như tấn công bằng từ chối dịch vụ (denial-of-service), vẫn còn là một mối đe dọa an toàn thông tin.
 - Khả năng mất dữ liệu trong lúc di chuyển thông tin cũng vẫn rất cao.
 - Trong một số trường hợp, nhất là khi dữ liệu là loại high-end, như các tập tin multimedia, việc trao đổi dữ liệu sẽ rất chậm chạp do được truyền thông qua Internet.
 - Do là kết nối dựa trên Internet, nên tính hiệu quả không liên tục, thường xuyên, và QoS cũng không được đảm bảo.

2.3. CÁC VPN MỞ RỘNG (EXTRANET VPNS):

- Không giống như Intranet và Remote Access-based, Extranet không hoàn toàn cách li từ bên ngoài (outer-world), Extranet cho phép truy cập những tài nguyên mạng cần thiết của các đối tác kinh doanh, chẳng hạn như khách hàng, nhà cung cấp, đối tác những người giữ vai trò quan trọng trong tổ chức.
- Mạng Extranet rất tốn kém do có nhiều đoạn mạng riêng biệt trên Intranet kết hợp lại với nhau để tạo ra một Extranet. Điều này làm cho khó triển khai và quản lý do có nhiều mạng, đồng thời cũng khó khăn cho cá nhân làm công việc bảo trì và quản trị. Thêm nữa là mạng Extranet sẽ khó mở rộng do điều này sẽ làm rối tung toàn bộ mạng Intranet và có thể ảnh hưởng đến các kết nối bên ngoài mạng. Sẽ có những vấn đề bạn gặp phải bất thành linh khi kết nối một Intranet vào một mạng Extranet. Triển khai và thiết kế một mạng Extranet có thể là một cơn ác mộng của các nhà thiết kế và quản trị mạng.
- Các VPN mở rộng cung cấp một đường hầm bảo mật giữa các khách hàng, các nhà cung cấp, và các đối tác qua một cơ sở hạ tầng công cộng sử dụng các kết nối mà luôn luôn được bảo mật. Kiểu VPN này thường được cấu hình như là một VPN Site-to-Site. Sự khác nhau giữa một VPN nội bộ và một VPN mở rộng đó là sự truy cập mạng mà được công nhận ở một trong hai đầu cuối của VPN. Hình 2.4 dưới đây minh họa một VPN mở rộng.



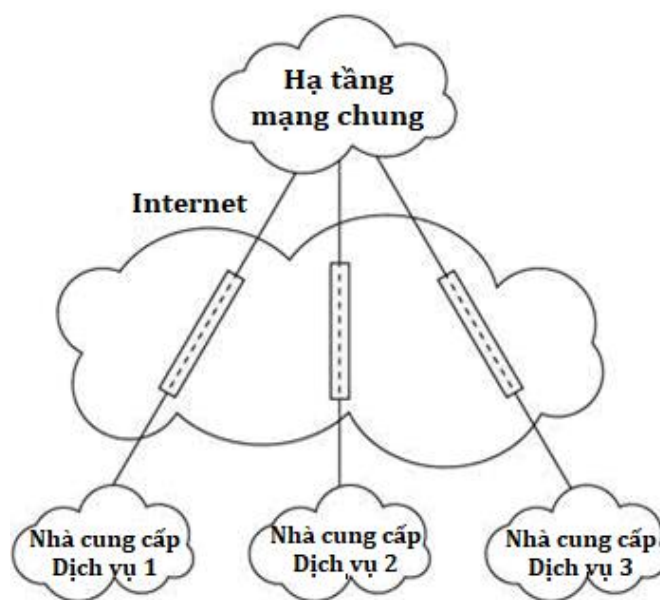
Hình 2. 4. Mô hình mạng VPN mở rộng.

➤ Một số thuận lợi của Extranet :

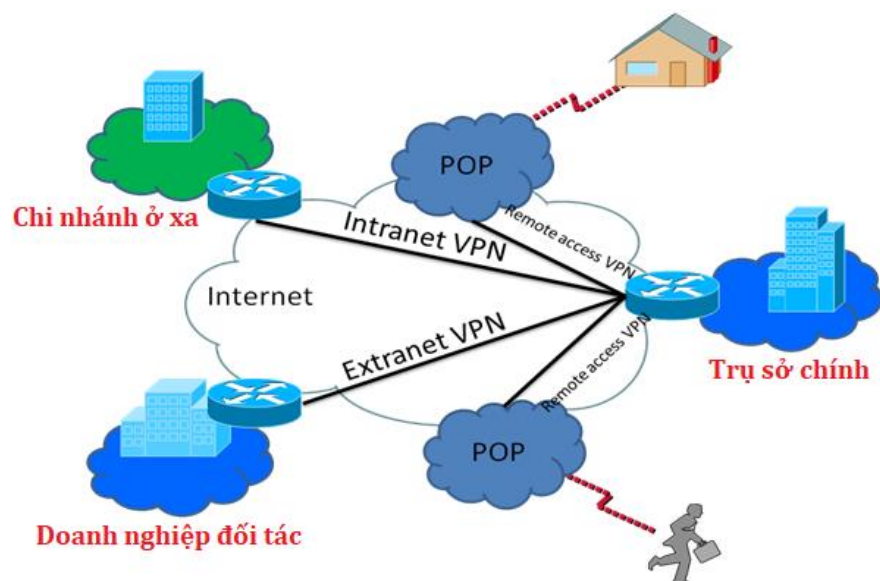
- Do hoạt động trên môi trường Internet, chúng ta có thể lựa chọn nhà phân phối khi lựa chọn và đưa ra phương pháp giải quyết tùy theo nhu cầu của tổ chức.
- Bởi vì một phần Internet-connectivity được bảo trì bởi nhà cung cấp (ISP) nên cũng giảm chi phí bảo trì khi thuê nhân viên bảo trì.
- Dễ dàng triển khai, quản lý và chỉnh sửa thông tin.

➤ Một số bất lợi của Extranet :

- Sự đe dọa về tính an toàn, như bị tấn công bằng từ chối dịch vụ vẫn còn tồn tại.
- Tăng thêm nguy hiểm sự xâm nhập đối với tổ chức trên Extranet.
- Do dựa trên Internet nên khi dữ liệu là các loại high-end data thì việc trao đổi diễn ra chậm chạp.
- Do dựa trên Internet, QoS cũng không được bảo đảm thường xuyên.



Hình 2. 5. Thiết lập Extranet VPN



Hình 2. 6. Ba loại mạng riêng ảo

CHƯƠNG III.

GIAO THỨC ĐƯỜNG HẦM IPSEC VPN

Giao thức đường hầm là một nền tảng trong VPN. Giao thức đường hầm đóng vai trò quan trọng trong việc thực hiện đóng gói và vận chuyển gói tin để truyền trên đường mạng công cộng.

Có ba giao thức đường hầm cơ bản và được sử dụng nhiều trong thực tế và đang được sử dụng hiện nay là giao thức tầng hầm chuyển tiếp lớp 2 L2F, giao thức đường hầm điểm tới điểm (PPTP), giao thức tầng hầm lớp 2 Layer. Trong chương này sẽ đi sâu hơn và cụ thể hơn các giao thức đường hầm nói trên. Nó liên quan đến việc thực hiện IP-VPN trên mạng công cộng.

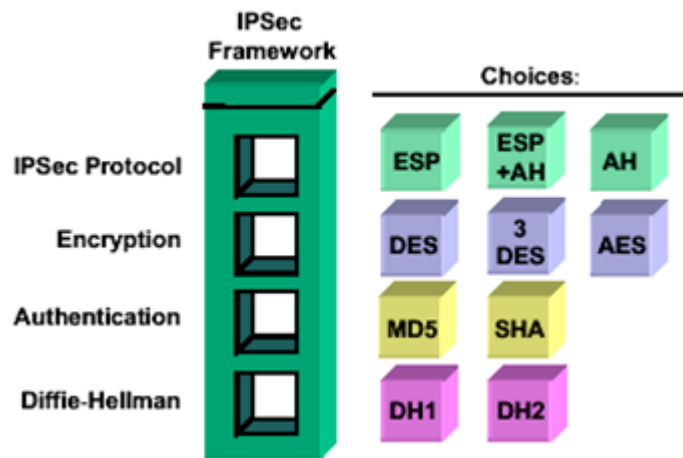
3.1. GIỚI THIỆU CÁC GIAO THỨC ĐƯỜNG HẦM

☑ Có rất nhiều giao thức đường hầm khác nhau trong công nghệ VPN, và việc sử dụng các giao thức nào liên quan đến các phương pháp xác thực và mật mã đi kèm. Một số giao thức đường hầm phổ biến hiện nay là:

- Giao thức tầng hầm chuyển tiếp lớp 2 (L2F).
- Giao thức đường hầm điểm tới điểm (PPTP).
- Giao thức tầng hầm lớp 2 (L2TP).
- GRE
- IPSEC

3.2. GIAO THỨC BẢO MẬT IP (IP SECURITY PROTOCOL)

IPSec không phải là một giao thức. Nó là một khung của các tập giao thức chuẩn mở được thiết kế để cung cấp sự xác thực dữ liệu, tính toàn vẹn dữ liệu, và sự tin cậy dữ liệu.



Hình 3. 1. Sơ đồ khung IPsec

IPsec chạy ở lớp 3 và sử dụng IKE để thiết lập SA giữa các đối tượng ngang hàng. Dưới đây là các đối tượng cần được thiết lập như là một phần của sự thiết lập SA.

- Thuật toán mã hoá.
- Thuật toán băm (Hash).
- Phương thức xác thực.
- Nhóm Diffie-Hellman.

Chức năng của IPsec là để thiết lập sự bảo mật tương ứng giữa hai đối tượng ngang hàng. Sự bảo mật này xác định khoá, các giao thức, và các thuật toán được sử dụng giữa các đối tượng ngang hàng. Các SA IPsec có thể chỉ được thiết lập như là vô hướng.

Sau khi gói tin được chuyển tới tầng mạng thì gói tin IP không gắn liền với bảo mật. Bởi vậy, không cam đoan rằng IP datagram nhận được là:

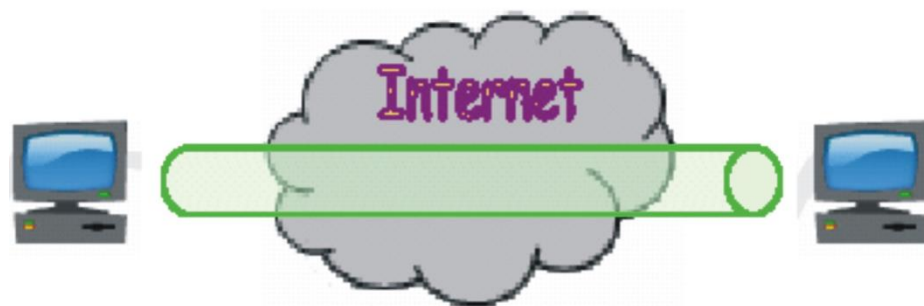
- Từ người gửi yêu cầu.
- Dữ liệu gốc từ người gửi.
- Không bị kiểm tra bởi bên thứ 3 trong khi gói tin đang được gửi từ nguồn tới đích.

IPsec là một phương pháp để bảo vệ IP datagram. IPsec bảo vệ IP datagram bằng cách định nghĩa một phương pháp định rõ lưu lượng để bảo vệ, cách lưu lượng đó được bảo vệ và lưu lượng đó được gửi tới ai. IPsec có thể bảo vệ gói tin giữa các host, giữa công an ninh mạng, hoặc giữa các host và công an ninh. IPsec cũng thực hiện đóng gói dữ liệu và xử lý các thông tin để thiết lập, duy trì, và hủy bỏ đường hầm khi không dùng đến

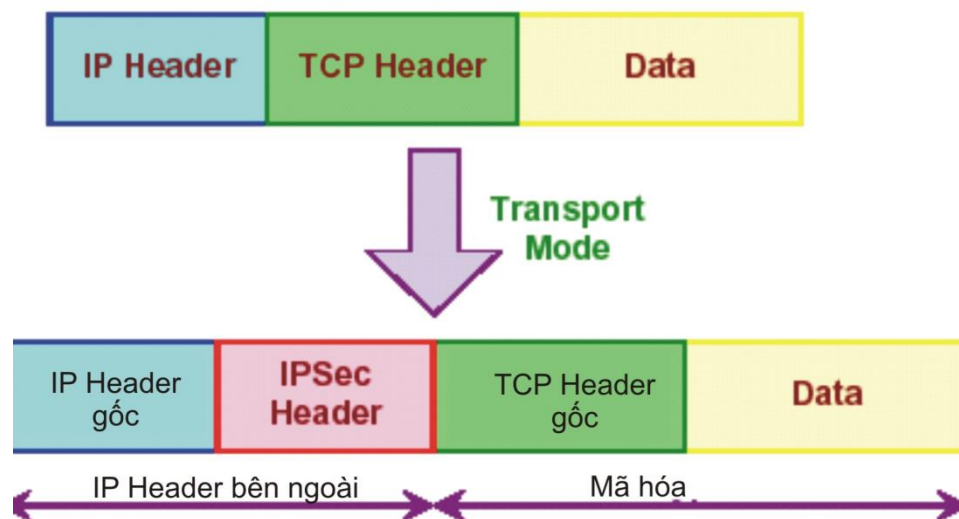
nữa. Các gói tin truyền trong đường hầm có khuôn dạng giống như các gói tin bình thường khác và không làm thay đổi các thiết bị, kiến trúc cũng như các ứng dụng hiện có trên mạng trung gian, qua đó cho phép giảm đáng kể chi phí để triển khai và quản lý.

Nó là tập hợp các giao thức được phát triển bởi IETF để hỗ trợ sự thay đổi bảo mật của gói tin ở tầng IP qua mạng vật lý. IPSec được phát triển rộng rãi để thực hiện VPN. IPSec hỗ trợ hai chế độ mã hóa: transport và tunnel

Chế độ transport chỉ mã hóa phần payload của mỗi gói tin, nhưng bỏ đi phần header không sờ đến. Ở bên nhận, thiết bị IPSec_compliant sẽ giải mã từng gói tin.



Sử dụng chế độ Transport (Tunnel) Giữa hai Host

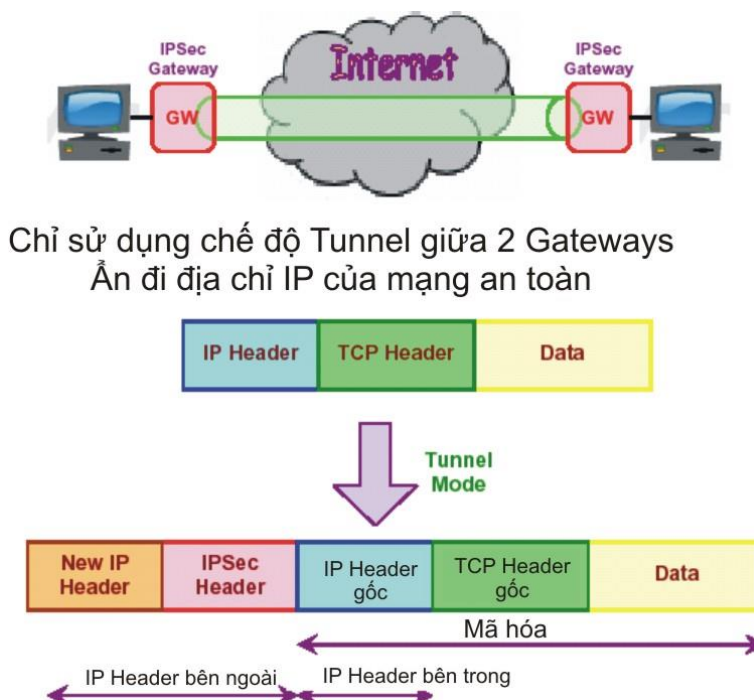


Hình 3. 2. Chế độ Transport

Mode transport bảo vệ phần tải tin của gói dữ liệu, các giao thức ở lớp cao hơn, nhưng vận chuyển địa chỉ IP nguồn ở dạng “clear”. Địa chỉ IP nguồn được sử dụng để định tuyến các gói dữ liệu qua mạng Internet. Mode transport ESP được sử dụng giữa hai máy, khi địa chỉ đích cuối cùng là địa chỉ máy của chính bản thân nó. Mode transport cung cấp tính bảo mật chỉ cho các giao thức lớp cao hơn.

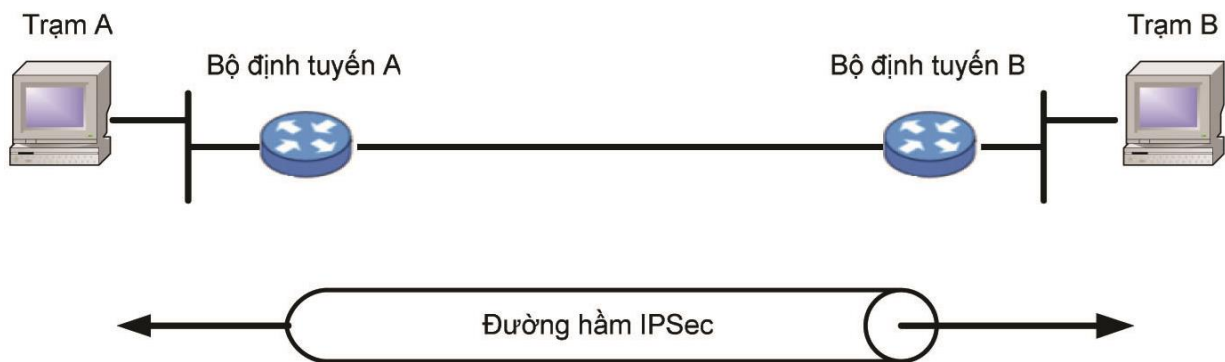
Nhược điểm của chế độ này là nó cho phép các thiết bị trong mạng nhìn thấy địa chỉ nguồn và đích của gói tin và có thể thực hiện một số xử lý (như phân tích lưu lượng) dựa trên các thông tin của tiêu đề IP. Tuy nhiên, nếu dữ liệu được mã hóa bởi ESP thì sẽ không biết được thông tin cụ thể bên trong gói tin IP là gì. Theo IETF thì chế độ truyền tải chỉ có thể được sử dụng khi hai hệ thống đầu cuối IP-VPN có thực hiện IPSec.

Chế độ tunnel mã hóa cả phần header và payload để cung cấp sự thay đổi bảo mật nhiều hơn của gói tin. Ở bên nhận, thiết bị IPSec_compliant sẽ giải mã từng gói tin. Một trong nhiều giao thức phổ biến được sử dụng để xây dựng VPN là chế độ đường hầm IPSec.

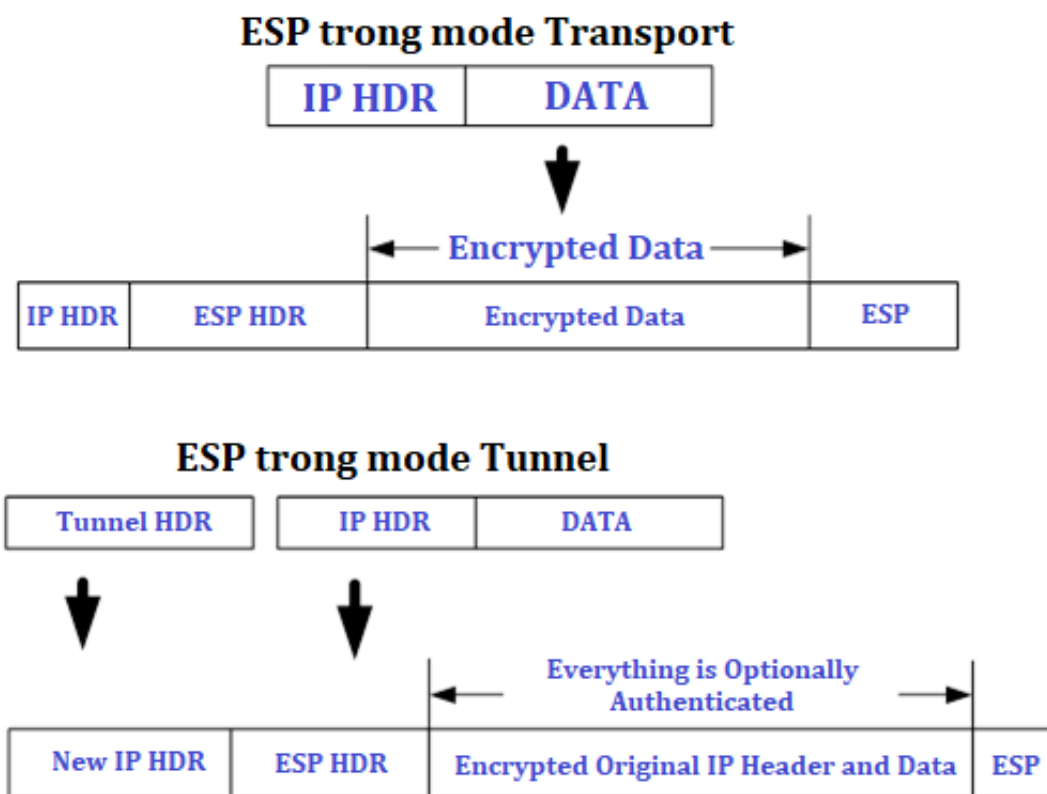


Hình 3. 3. Chế độ Tunnel

Chế độ này cho phép các thiết bị mạng như bộ định tuyến thực hiện xử lý IPSec thay cho các trạm cuối (host). Khi sử dụng chế độ đường hầm, các đầu cuối của IPSec-VPN không cần phải thay đổi ứng dụng hay hệ điều hành.



Hình 3. 4. Thiết bị mạng thực hiện trong IPsec trong chế độ đường hầm



Hình 3. 5. ESP trong mode Tunnel và transport

IPsec được phát triển cho lí do bảo mật bao gồm tính toàn vẹn không kết nối, xác thực dữ liệu gốc, anti_replay, và mã hóa. IETF định nghĩa theo chức năng của IPsec.

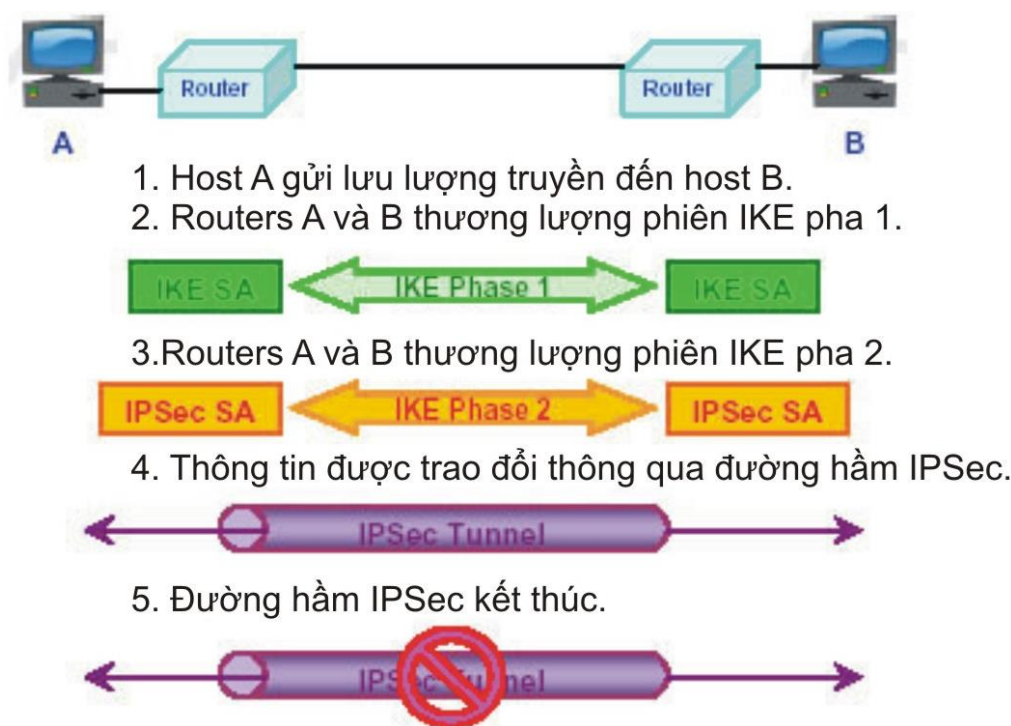
- *Tính xác thực*: Mọi người đều biết là dữ liệu nhận được giống với dữ liệu được gửi và người gửi yêu cầu là người gửi hiện tại.
- *Tính toàn vẹn*: Đảm bảo rằng dữ liệu được truyền từ nguồn tới đích mà không bị thay đổi hay có bất kỳ sự xáo trộn nào.

- *Tính bảo mật*: Người gửi có thể mã hóa các gói dữ liệu trước khi truyền qua mạng công cộng và dữ liệu sẽ được giải mã ở phía thu. Bằng cách làm như vậy, không một ai có thể truy nhập thông tin mà không được phép. Thậm chí nếu lấy được cũng không đọc được.
- *Mã hóa*: Một cơ cấu cơ bản được sử dụng để cung cấp tính bảo mật.
- *Phân tích lưu lượng*: Phân tích luồng lưu lượng mạng cho mục đích khâu trừ thông tin hữu ích cho kẻ thù. Ví dụ như thông tin thường xuyên được truyền, định danh của các bên đối thoại, kích cỡ gói tin, định danh luồng sử dụng, vv..
- *SPI*: Viết tắt của chỉ số tham số an toàn (security parameter index), nó là chỉ số không có kết cấu rõ ràng, được sử dụng trong liên kết với địa chỉ đích để định danh liên kết an toàn tham gia.

Phương pháp bảo vệ IP datagram bằng cách sử dụng một trong các giao thức IPSec, Encapsulate Security Payload (ESP) hoặc Authentication Header (AH). AH cung cấp chứng cứ gốc của gói tin nhận, toàn vẹn dữ liệu, và bảo vệ anti_replay. ESP cung cấp cái mà AH cung cấp cộng với tính bảo mật dữ liệu tùy ý. Nền tảng bảo mật được cung cấp bởi AH hoặc ESP phụ thuộc vào thuật toán mã hóa áp dụng trên chúng.

Dịch vụ bảo mật mà IPSec cung cấp yêu cầu khóa chia sẻ để thực hiện tính xác thực và bảo mật. Giao thức khóa chia sẻ là Internet Key Exchange (IKE), là một phương pháp chuẩn của xác thực IPSec, dịch vụ thương lượng bảo mật, và phát sinh khóa chia sẻ.

Quá trình hoạt động của IPSec: IPSec đòi hỏi nhiều thành phần công nghệ và phương pháp mã hóa. Hoạt động của IPSec có thể được chia thành 5 bước chính:



Hình 3. 6. Các bước hoạt động của IPsec



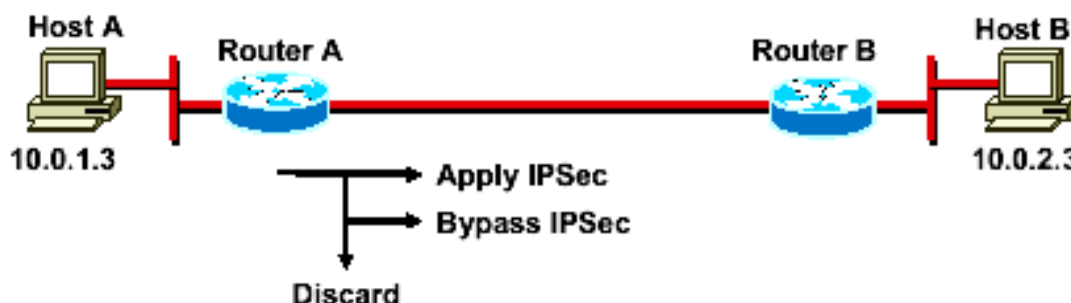
Hình 3. 7. Sơ đồ kết nối hai Router chạy IPsec

Mục đích chính của IPsec là để bảo vệ luồng dữ liệu mong muốn với các dịch vụ bảo mật cần thiết. Quá trình hoạt động của IPsec được chia thành năm bước:

- ✓ Xác định luồng traffic cần quan tâm: Luồng traffic được xem là cần quan tâm khi đó các thiết bị VPN công nhận rằng luồng traffic bạn muốn gửi cần bảo vệ.
- ✓ Bước 1 IKE: Giữa các đối tượng ngang hàng (peer), một tập các dịch vụ bảo mật được thoả thuận và công nhận. Tập dịch vụ bảo mật này bảo vệ tất cả các quá trình trao đổi thông tin tiếp theo giữa các peer.
- ✓ Bước 2 IKE: IKE thoả thuận các tham số SA IPsec và thiết lập “matching” các SA IPsec trong các peer. Các tham số bảo mật này được sử dụng để bảo vệ dữ liệu và các bản tin được trao đổi giữa các điểm đầu cuối. Kết quả cuối cùng của hai bước IKE là một kênh thông tin bảo mật được tạo ra giữa các peer.

- ✓ Truyền dữ liệu: Dữ liệu được truyền giữa các peer IPSec trên cơ sở các thông số bảo mật và các khoá được lưu trữ trong SA database.
- ✓ Kết thúc đường hầm “Tunnel”: Kết thúc các SA IPSec qua việc xoá hay timing out.

Bước 1: Xác định luồng traffic cần quan tâm

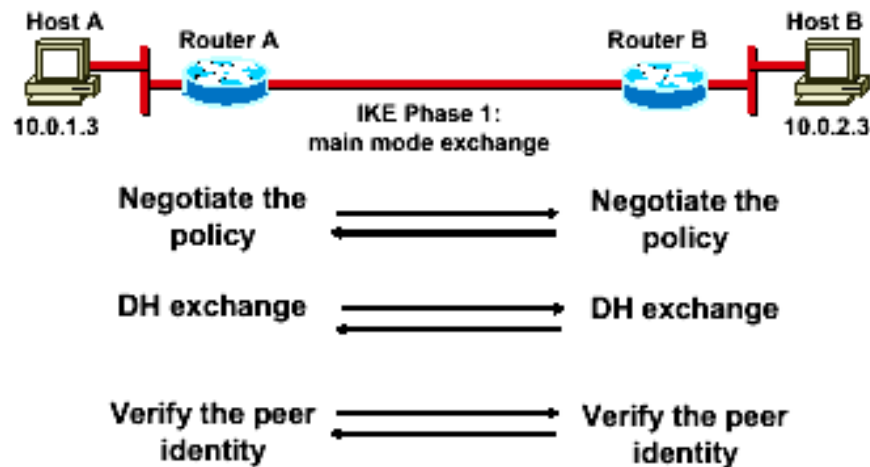


Hình 3. 8. Xác định luồng traffic

Việc xác định luồng dữ liệu nào cần được bảo vệ được thực hiện như là một phần trong việc tính toán một chính sách bảo mật cho việc sử dụng của một VPN. Chính sách được sử dụng để xác định luồng traffic nào cần bảo vệ và luồng traffic nào có thể gửi ở dạng “clear text”. Đối với mọi gói dữ liệu đầu vào và đầu ra, sẽ có ba lựa chọn: Dùng IPSec, cho qua IPSec, hoặc huỷ gói dữ liệu. Đối với mọi gói dữ liệu được bảo vệ bởi IPSec, người quản trị hệ thống cần chỉ rõ các dịch vụ bảo mật được sử dụng cho gói dữ liệu. Các cơ sở dữ liệu chính sách bảo mật chỉ rõ các giao thức IPSec, các mode, và các thuật toán được sử dụng cho luồng traffic.

Các dịch vụ này sau đó được sử dụng cho luồng traffic dành cho mỗi Peer IPSec cụ thể. Với VPN Client, bạn sử dụng các cửa sổ thực đơn để chọn các kết nối mà bạn muốn bảo mật bởi IPSec. Khi các luồng dữ liệu mong muốn truyền tới IPSec Client, client khởi tạo sang bước tiếp theo trong quá trình: Thoả thuận một sự trao đổi bước 1 IKE.

Bước 2: Bước 1 IKE

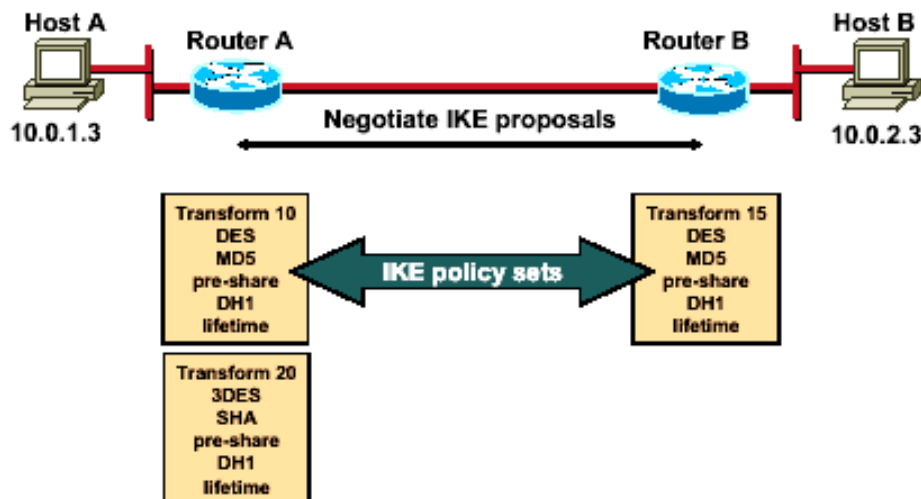


Hình 3. 9. Bước một IKE

Mục đích cơ bản của bước 1 IKE là để thỏa thuận các tập chính sách IKE, xác thực các đối tượng ngang hàng, và thiết lập một kênh bảo mật giữa các đối tượng ngang hàng. Bước 1 IKE xuất hiện trong hai mode: Main mode và Aggressive mode.

Main mode có ba quá trình trao đổi hai chiều giữa nơi khởi tạo và nơi nhận:

Quá trình trao đổi đầu tiên:



Hình 3. 10. Quá trình trao đổi đầu tiên

Trong suốt quá trình trao đổi đầu tiên các thuật toán và các hash được sử dụng để bảo mật sự trao đổi thông tin IKE đã được thỏa thuận và đã được đồng ý giữa các đối tượng ngang hàng. Trong khi cố gắng tạo ra một kết nối bảo mật giữa máy A và máy B qua Internet, các kế hoạch bảo mật IKE được trao đổi giữa Router A và B. Các kế hoạch bảo vệ định nghĩa giao thức IPsec hiện tại đã được thỏa thuận (ví dụ ESP).

Dưới mỗi kế hoạch, người khởi tạo cần phác hoạ những thuật toán nào được sử dụng trong chính sách (ví dụ DES với MD5). Ở đây không phải là thoả thuận mỗi thuật toán một cách riêng biệt, mà là các thuật toán được nhóm trong các tập, một tập chính sách IKE. Một tập chính sách mô tả thuật toán mã hoá nào, thuật toán xác thực nào, mode, và chiều dài khoá. Những kế hoạch IKE và những tập chính sách này được trao đổi trong suốt quá trình trao đổi đầu tiên trong chế độ main mode. Nếu một tập chính sách match được tìm thấy giữa hai đối tượng ngang hàng, main mode tiếp tục. Nếu không một tập chính sách match nào được tìm thấy, tunnel là torn down.

Trong ví dụ ở trong hình trên, RouterA gửi các tập chính sách IKE 10 và 20 tới RouterB. RouterB so sánh tập chính sách của nó, tập chính sách 15, với những tập chính sách nhận được từ RouterA. Trong trường hợp này, có một cái match: Đó là tập chính sách 10 của Router A match với tập chính sách 15 của Router B.

Quá trình trao đổi thứ hai

Sử dụng một sự trao đổi DH để tạo ra các khoá mật mã chia sẻ và qua quá trình này các số ngẫu nhiên gửi tới các đối tác khác, signed, và lấy lại xác thực định nghĩa của chúng. Khoá mật mã chia sẻ được sử dụng để tạo ra tất cả các khoá xác thực và mã hoá khác. Khi bước này hoàn thành, các đối tượng ngang hàng có cùng một mật mã chia sẻ nhưng các đối tượng ngang hàng không được xác thực. Quá trình này diễn ra ở bước thứ 3 của bước 1 IKE, quá trình xác thực đặc tính của đối tượng ngang hàng.

Quá trình thứ ba – xác thực đặc tính đối tượng ngang hàng:



Hình 3. 11. Quá trình trao đổi thứ ba

Các phương thức xác thực đối tượng ngang hàng:

- Pre-shared keys
- RSA signatures
- RSA encrypted nonces

Bước thứ ba và cũng là bước trao đổi cuối cùng được sử dụng để xác thực các đối tượng ngang hàng ở xa. Kết quả chính của main mode là một tuyến đường trao đổi thông tin bảo mật cho các quá trình trao đổi tiếp theo giữa các đối tượng ngang hàng được tạo ra. Có ba phương thức xác thực nguồn gốc dữ liệu:

- Các khoá pre-shared: Một giá trị khoá mật mã được nhập vào bằng tay của mỗi đối tượng ngang hàng được sử dụng để xác thực đối tượng ngang hàng.
- Các chữ ký RSA: Sử dụng việc trao đổi các chứng nhận số để xác thực các đối tượng ngang hàng.
- RSA encryption nonces: Nonces (một số ngẫu nhiên được tạo ra bởi mỗi đối tượng ngang hàng) được mã hoá và sau đó được trao đổi giữa các đối tượng ngang hàng.

Hai nonce được sử dụng trong suốt quá trình xác thực đối tượng ngang hàng.

Trong aggressive mode, các trao đổi là ít hơn với ít gói dữ liệu hơn. Mọi thứ đều được trao đổi trong quá trình trao đổi đầu tiên: Sự thoả thuận tập chính sách IKE, sự tạo ra khoá chung DH, một nonce. Trong aggressive mode nhanh hơn main mode.

Bước 3 – Bước 2 IKE



Hình 3. 12. Bước 2 IKE

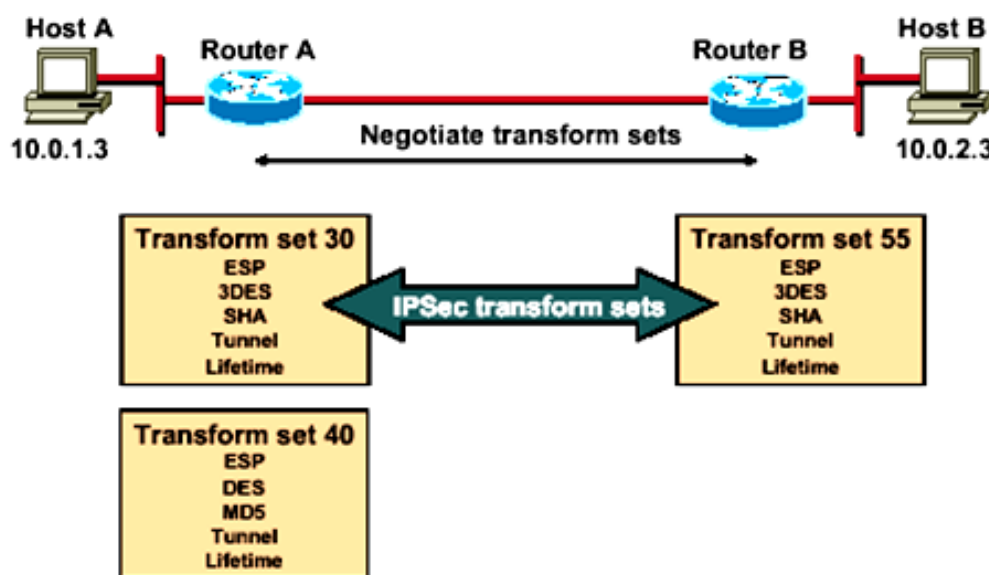
Mục đích của bước 2 IKE là để thoả thuận các thông số bảo mật IPsec được sử dụng để bảo mật đường hầm IPsec. Bước 2 IKE thực hiện các chức năng dưới đây:

- Thoả thuận các thông số bảo mật, các tập transform IPsec.
- Thiết lập các SA IPsec.
- Thoả thuận lại theo chu kỳ các SA IPsec để chắc chắn bảo mật.
- Có thể thực hiện thêm một sự trao đổi DH.

Trong bước 2 IKE chỉ có một mode, gọi là Quick mode. Quick mode xuất hiện sau khi IKE đã được thiết lập đường hầm bảo mật trong bước 1 IKE. Nó thoả thuận một transform IPSec chia sẻ, và thiết lập các SA IPSec. Quick mode trao đổi các nonce mà được sử dụng để tạo ra khoá mật mã chia sẻ mới và ngăn cản các tấn công “replay” từ việc tạo ra các SA không có thật.

Quick mode cũng được sử dụng để thoả thuận lại một SA IPSec mới khi thời gian sống của SA IPSec đã hết. Quick mode được sử dụng để nạp lại “keying material” được sử dụng để tạo ra khoá mật mã chia sẻ trên cơ sở “keying material” lấy từ trao đổi DH trong bước 1.

Các tập Transform IPSec

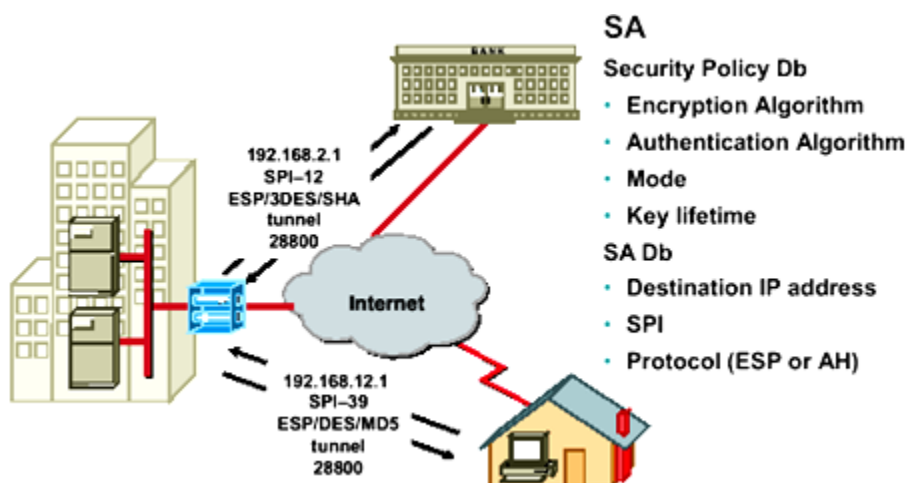


Hình 3. 13. Thỏa thuận tập transform

Kết quả cuối cùng của bước 2 IKE là thiết lập một phiên IPSec bảo mật giữa các điểm đầu cuối. Trước khi điều này có thể xảy ra, mỗi cặp của các điểm đầu cuối thoả thuận mức bảo mật yêu cầu (ví dụ, các thuật toán xác thực và mã hoá cho một phiên). Không những là thoả thuận những giao thức riêng biệt, các giao thức được nhóm vào trong các tập, một tập transform IPSec. Các tập transform IPSec được trao đổi giữa các peer trong suốt quá trình “quick mode”. Nếu một “match” được tìm thấy giữa các tập, phiên thiết lập IPSec sẽ tiếp tục. Nếu ngược lại thì phiên sẽ bị huỷ bỏ.

Trong ví dụ trong hình trên, RouterA gửi các tập transform IPSec 30 và 40 đến RouterB. RouterB so sánh tập transform của nó với những cái đã nhận được từ RouterA. Trong ví dụ này, có một cái “match”. Tập transform 30 của RouterA match với tập transform 55 của RouterB. Các thuật toán mã hoá và xác thực có dạng một SA.

SA (Security Association)



Hình 3. 14. Các thông số của SA

Khi mà các dịch vụ bảo mật được đồng ý giữa các peer, mỗi thiết bị ngang hàng VPN đưa thông tin vào trong một SPD (Security Policy Database). Thông tin này bao gồm thuật toán xác thực, mã hoá, địa chỉ IP đích, mode truyền dẫn, thời gian sống của khoá .v.v. Những thông tin này được coi như là một SA. Một SA là một kết nối logic một chiều mà cung cấp sự bảo mật cho tất cả traffic đi qua kết nối. Bởi vì hầu hết traffic là hai chiều, do vậy phải cần hai SA: một cho đầu vào và một cho đầu ra.

Thiết bị VPN gán cho SA một số thứ tự, gọi là SPI (Security Parameter Index). Khi gửi các thông số riêng biệt của SA của qua đường hầm, Gateway, hoặc Host chèn SPI vào trong tiêu đề ESP. Khi mà đối tượng ngang hàng IPSec nhận được gói dữ liệu, nó nhìn vào địa chỉ IP đích, giao thức IPSec, và SPI trong SAD (Security Association Database) của nó, và sau đó xử lý gói dữ liệu theo các thuật toán được chỉ ra trong SPD.

IPSec SA là một sự tổ hợp của SAD và SPD. SAD được sử dụng để định nghĩa địa chỉ IP đích SA, giao thức IPSec, và số SPI. SPD định nghĩa các dịch vụ bảo mật được sử dụng cho SA, các thuật toán mã hoá và xác thực, mode, và thời gian sống của khoá. Ví dụ, trong kết nối từ tổng công ty đến nhà băng, chính sách bảo mật cung cấp một vài đường hầm bảo mật sử dụng 3DES, SHA, mode tunnel, và thời gian sống của khoá là 28800. Giá trị SAD là 192.168.2.1, ESD, và SPI là 12.

Bước 4 – Phiên IPSec



Hình 3. 15. Một phiên IPSec

Sau khi bước 2 IKE hoàn thành và quick mode được thiết lập, traffic sẽ được trao đổi giữa máy A và máy B qua một đường hầm bảo mật. Traffic mong muốn được mã hoá và giải mã theo các dịch vụ bảo mật được chỉ ra trong SA IPSec.

Bước 5 – Kết thúc đường hầm



Hình 3. 16. Kết thúc một phiên IPSec

Các SA IPSec kết thúc thông qua việc xoá hay bằng timing out. Một SA có thể time out khi lượng thời gian đã được chỉ ra là hết hoặc khi số byte được chỉ ra đã qua hết đường hầm. Khi các SA kết thúc, các khoá cũng bị huỷ. Khi các SA IPSec tiếp theo cần cho một luồng, IKE thực hiện một bước 2 mới, và nếu cần thiết, một sự thoả thuận mới trong bước 1 IKE. Một sự thoả thuận thành công sẽ tạo ra các SA và các khoá mới. Các SA mới thường được thiết lập trước khi các SA đang tồn tại hết giá trị.

Năm bước được tổng kết của IPSec

| Bước | Hoạt động | Miêu tả |
|------|--|--|
| 1 | Lưu lượng truyền bắt đầu quá trình IPSec | Lưu lượng được cho rằng đang truyền khi chính sách bảo mật IPSec đã cấu hình trong các bên IPSec bắt đầu quá trình IKE. |
| 2 | IKE pha một | IKE xác thực các bên IPSec và thương lượng các IKE SA trong suốt pha này, thiết lập kênh an toàn cho việc thương lượng các IPSec SA trong pha hai. |
| 3 | IKE pha hai | IKE thương lượng tham số IPSec SA và cài đặt IPSec SA trong các bên. |
| 4 | Truyền dữ liệu | Dữ liệu được truyền giữa các bên IPSec dựa trên tham số IPSec và những khóa được lưu trong CSDL của SA. |
| 5 | Kết thúc đường hầm IPSec | IPSec SA kết thúc qua việc xóa hoặc hết thời gian thực hiện. |

3.3. NHỮNG HẠN CHẾ CỦA IPSEC

Mặc dù IPSec đã sẵn sàng đưa ra các đặc tính cần thiết để đảm bảo thiết lập kết nối VPN an toàn thông qua mạng Internet, nó vẫn còn ở trong giai đoạn phát triển để hướng tới hoàn thiện. Sau đây là một số vấn đề đặt ra mà IPSec cần phải giải quyết để hỗ trợ tốt hơn cho việc thực hiện VPN:

- ✓ Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kỹ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- ✓ IKE vẫn là công nghệ chưa thực sự khẳng định được khả năng của mình. Phương thức chuyển khóa thủ công lại không thích hợp cho mạng có số lượng lớn các đối tượng di động.
- ✓ IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- ✓ Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- ✓ Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

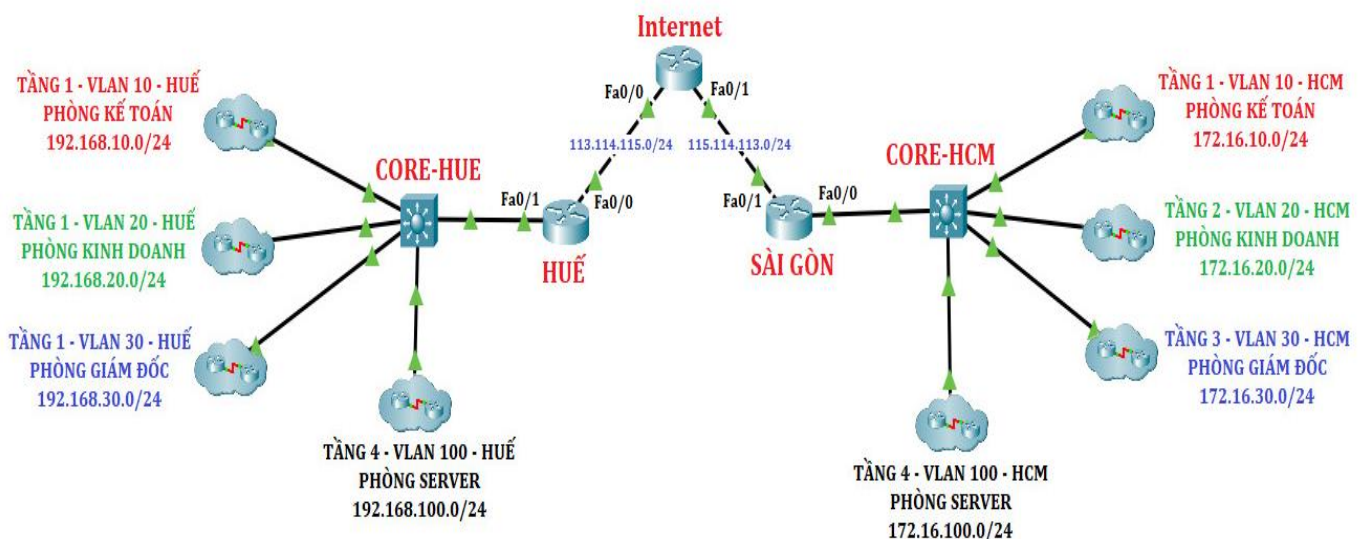
CHƯƠNG IV. THIẾT LẬP VPN SITE TO SITE (DÙNG PHẦN MỀM PACKET TRACER)

4.1. GIỚI THIỆU VỀ PHẦN MỀM CISCO PACKET TRACER

- ✓ Hiện nay có rất nhiều phần mềm tạo Lab ảo được sử dụng để giúp đỡ các bạn trong quá trình học và tìm hiểu các thiết bị mạng của Cisco.
- ✓ Cisco Packet Tracer là phần mềm rất tiện dụng cho các bạn bước đầu đi vào khám phá, xây dựng và cấu hình các thiết bị của Cisco, nó có giao diện rất trực quan với hình ảnh giống như Router thật, bạn có thể nhìn thấy các port, các module. Bạn có thể thay đổi các module của chúng bằng cách drag-drop những module cần thiết để thay thế, bạn có thể chọn loại cable nào cho những kết nối của bạn. Bạn cũng có thể nhìn thấy các gói tin đi trên các thiết bị của bạn như thế nào.

4.2. THIẾT LẬP MÔ HÌNH VPN SITE TO SITE

4.2.1. Mô hình VPN Site to Site giữa hai chi nhánh HUẾ và SÀI GÒN



Hình 4. 1. Sơ đồ mô phỏng VPN site to site

4.2.2. Cấu hình đặt địa chỉ IP

Bảng địa chỉ:

| Device | Interface | IP Address | Subnet Mask | Default – gateway |
|-----------------------|------------------|-----------------|---------------|-------------------|
| HUE | Fa0/0 | 113.114.115.1 | 255.255.255.0 | N/A |
| | Fa0/1.10 | 192.168.10.1 | 255.255.255.0 | N/A |
| | Fa0/1.20 | 192.168.20.1 | 255.255.255.0 | N/A |
| | Fa0/1.30 | 192.168.30.1 | 255.255.255.0 | N/A |
| | Fa0/1.100 | 192.168.100.1 | 255.255.255.0 | N/A |
| SAIGON | Fa0/1 | 115.114.113.1 | 255.255.255.0 | N/A |
| | Fa0/0.10 | 172.16.10.1 | 255.255.255.0 | N/A |
| | Fa0/0.20 | 172.16.20.1 | 255.255.255.0 | N/A |
| | Fa0/0.30 | 172.16.30.1 | 255.255.255.0 | N/A |
| | Fa0/0.100 | 172.16.100.1 | 255.255.255.0 | N/A |
| INTERNET | Fa0/0 | 113.114.115.2 | 255.255.255.0 | N/A |
| | Fa0/1 | 115.114.113.2 | 255.255.255.0 | N/A |
| DNS-SERVER | NIC | 192.168.100.254 | 255.255.255.0 | 192.168.100.1 |
| WEB-SERVER-HUE | NIC | 192.168.100.2 | 255.255.255.0 | 192.168.100.1 |
| WEB-SERVER-HCM | NIC | 172.16.100.2 | 255.255.255.0 | 172.16.100.1 |
| MAIL-SERVER | NIC | 192.168.100.3 | 255.255.255.0 | 192.168.100.1 |

4.2.3. Cấu hình VLAN & TRUNK

| Switch | VLAN | Tên VLAN | Port |
|-----------------|------------|------------------|------|
| CORE-HUE | 10 | PHONG-KE-TOAN | |
| | 20 | PHONG-KINH-DOANH | |
| | 30 | PHONG-GIAM-DOC | |
| | 100 | PHONG-SERVER | |
| CORE-HCM | 10 | PHONG-KE-TOAN | |
| | 20 | PHONG-KINH-DOANH | |
| | 30 | PHONG-GIAM-DOC | |
| | 100 | PHONG-SERVER | |

| CORE – HUE | CORE – HCM |
|--|--|
| <pre> CORE-HUE(config)#vtp mode server CORE-HUE(config)#vtp domain hue.com CORE-HUE(config)#vtp password hue.com CORE-HUE(config)#vlan 10 CORE-HUE(config-vlan)#name PHONG-KE-TOAN CORE-HUE(config-vlan)#vlan 20 CORE-HUE(config-vlan)#name PHONG-KINH-DOANH CORE-HUE(config-vlan)#vlan 30 CORE-HUE(config-vlan)#name PHONG-GIAM-DOC CORE-HUE(config-vlan)#vlan 100 CORE-HUE(config-vlan)#name PHONG-SERVER CORE-HUE(config-vlan)#exit CORE-HUE(config)#int g0/1 CORE-HUE(config-if)#switchport trunk encapsulation dot1q CORE-HUE(config-if)#switchport mode trunk </pre> | <pre> CORE-HCM(config)#vtp mode server CORE-HCM(config)#vtp domain hcm.com CORE-HCM(config)#vtp password hcm.com CORE-HCM(config)#vlan 10 CORE-HCM(config-vlan)#name PHONG-KE-TOAN CORE-HCM(config-vlan)#vlan 20 CORE-HCM(config-vlan)#name PHONG-KINH-DOANH CORE-HCM(config-vlan)#vlan 30 CORE-HCM(config-vlan)#name PHONG-GIAM-DOC CORE-HCM(config-vlan)#vlan 100 CORE-HCM(config-vlan)#name PHONG-SERVER CORE-HCM(config-vlan)#exit CORE-HCM(config)#int g0/1 CORE-HCM(config-if)#switchport trunk encapsulation dot1q CORE-HCM(config-if)#switchport mode trunk </pre> |

✓ SW – KETOAN – HUE:

```

SW-KETOAN-HUE(config)#vtp mode client
SW-KETOAN-HUE(config)#vtp domain hue.com
SW-KETOAN-HUE(config)#vtp password hue.com
SW-KETOAN-HUE(config)#int g0/1
SW-KETOAN-HUE(config-if)#switchport mode trunk
SW-KETOAN-HUE(config-if)#exit
SW-KETOAN-HUE(config)#int range fa0/1-24
SW-KETOAN-HUE(config-if-range)#switchport mode access
SW-KETOAN-HUE(config-if-range)#switchport access vlan 10
SW-KETOAN-HUE(config-if-range)#spanning-tree portfast

```

Làm tương tự với các Switch còn lại thuộc chi nhánh HUE

✓ SW – KETOAN – HCM:

```

SW-KETOAN-HCM(config)#vtp mode client
SW-KETOAN-HCM(config)#vtp domain hcm.com
SW-KETOAN-HCM(config)#vtp password hcm.com
SW-KETOAN-HCM(config)#int g0/1
SW-KETOAN-HCM(config-if)#switchport mode trunk
SW-KETOAN-HCM(config-if)#exit
SW-KETOAN-HCM(config)#int range fa0/1-24
SW-KETOAN-HCM(config-if-range)#switchport mode access
SW-KETOAN-HCM(config-if-range)#switchport access vlan 10
SW-KETOAN-HCM(config-if-range)#spanning-tree portfast

```

Làm tương tự với các Switch còn lại thuộc chi nhánh SAI GON

4.2.4. Cấu hình định tuyến và DHCP trên 2 Router của 2 chi nhánh

| | |
|------------|--|
| HUE | <pre>HUE(config)#ip route 0.0.0.0 0.0.0.0 113.114.115.2 HUE(config)#ip dhcp pool 10 HUE(dhcp-config)#network 192.168.10.0 255.255.255.0 HUE(dhcp-config)#default-router 192.168.10.1 HUE(dhcp-config)#dns-server 192.168.100.254 HUE(config)#ip dhcp pool 20 HUE(dhcp-config)#network 192.168.20.0 255.255.255.0 HUE(dhcp-config)#default-router 192.168.20.1 HUE(dhcp-config)#dns-server 192.168.100.254 HUE(config)#ip dhcp pool 30 HUE(dhcp-config)#network 192.168.30.0 255.255.255.0 HUE(dhcp-config)#default-router 192.168.30.1 HUE(dhcp-config)#dns-server 192.168.100.254 HUE(config)#ip dhcp pool 100 HUE(dhcp-config)#network 192.168.100.0 255.255.255.0 HUE(dhcp-config)#default-router 192.168.100.1 HUE(dhcp-config)#dns-server 192.168.100.254</pre> |
| HCM | <pre>HCM(config)#ip route 0.0.0.0 0.0.0.0 115.114.113.2 HCM(config)#ip dhcp pool 10 HCM(dhcp-config)#network 172.16.10.0 255.255.255.0 HCM(dhcp-config)#default-router 172.16.10.1 HCM(dhcp-config)#dns-server 192.168.100.254 HCM(config)#ip dhcp pool 20 HCM(dhcp-config)#network 172.16.20.0 255.255.255.0 HCM(dhcp-config)#default-router 172.16.20.1 HCM(dhcp-config)#dns-server 192.168.100.254 HCM(config)#ip dhcp pool 30 HCM(dhcp-config)#network 172.16.30.0 255.255.255.0 HCM(dhcp-config)#default-router 172.16.30.1 HCM(dhcp-config)#dns-server 192.168.100.254 HCM(config)#ip dhcp pool 100 HCM(dhcp-config)#network 172.16.100.0 255.255.255.0 HCM(dhcp-config)#default-router 172.16.100.1 HCM(dhcp-config)#dns-server 192.168.100.254</pre> |

4.2.5. Cấu hình VPN Site – to – Site:

Bước 1: Cấu hình ISAKMP

```
HUE(config)#crypto isakmp policy 10
HUE(config-isakmp)#hash md5
HUE(config-isakmp)#authentication pre-share
HUE(config-isakmp)#group 2
HUE(config-isakmp)#exit
HUE(config)#crypto isakmp key cisco123 address 115.114.113.1
```

```
HCM(config)#crypto isakmp policy 10
HCM(config-isakmp)#hash md5
HCM(config-isakmp)#authentication pre-share
HCM(config-isakmp)#group 2
HCM(config-isakmp)#exit
HCM(config)#crypto isakmp key cisco123 address 113.114.115.1
```

Bước 2: Cấu hình access-list cho phép VPN Traffic

```
HUE(config)#ip access-list extended 100
HUE(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 172.16.10.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 172.16.20.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 172.16.30.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 172.16.100.0 0.0.0.255

HUE(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 172.16.10.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 172.16.20.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 172.16.30.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 172.16.100.0 0.0.0.255

HUE(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.255 172.16.30.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.255 172.16.20.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.255 172.16.10.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.30.0 0.0.0.255 172.16.100.0 0.0.0.255

HUE(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 172.16.10.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 172.16.20.0 0.0.0.255
HUE(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 172.16.30.0 0.0.0.255
```

```
HCM(config)#ip access-list extended 100
HCM(config-ext-nacl)#permit ip 172.16.10.0 0.0.0.255 192.168.10.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.10.0 0.0.0.255 192.168.20.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.10.0 0.0.0.255 192.168.30.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.10.0 0.0.0.255 192.168.100.0 0.0.0.255

HCM(config-ext-nacl)#permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.20.0 0.0.0.255 192.168.20.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.20.0 0.0.0.255 192.168.30.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.20.0 0.0.0.255 192.168.100.0 0.0.0.255

HCM(config-ext-nacl)#permit ip 172.16.30.0 0.0.0.255 192.168.30.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.30.0 0.0.0.255 192.168.20.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.30.0 0.0.0.255 192.168.100.0 0.0.0.255

HCM(config-ext-nacl)#permit ip 172.16.100.0 0.0.0.255 192.168.10.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.100.0 0.0.0.255 192.168.20.0 0.0.0.255
HCM(config-ext-nacl)#permit ip 172.16.100.0 0.0.0.255 192.168.30.0 0.0.0.255
```

Bước 3: Tạo IPSec Transform

```
HUE(config)#crypto ipsec transform-set MYSET esp-des esp-md5-hmac
HCM(config)#crypto ipsec transform-set MYSET esp-des esp-md5-hmac
```

Bước 4: Tạo Crypto Map

```
HUE(config)#crypto map MYMAP 10 ipsec-isakmp
HUE(config-crypto-map)#set peer 115.114.113.1
HUE(config-crypto-map)#set transform-set MYSET
HUE(config-crypto-map)#match address 100

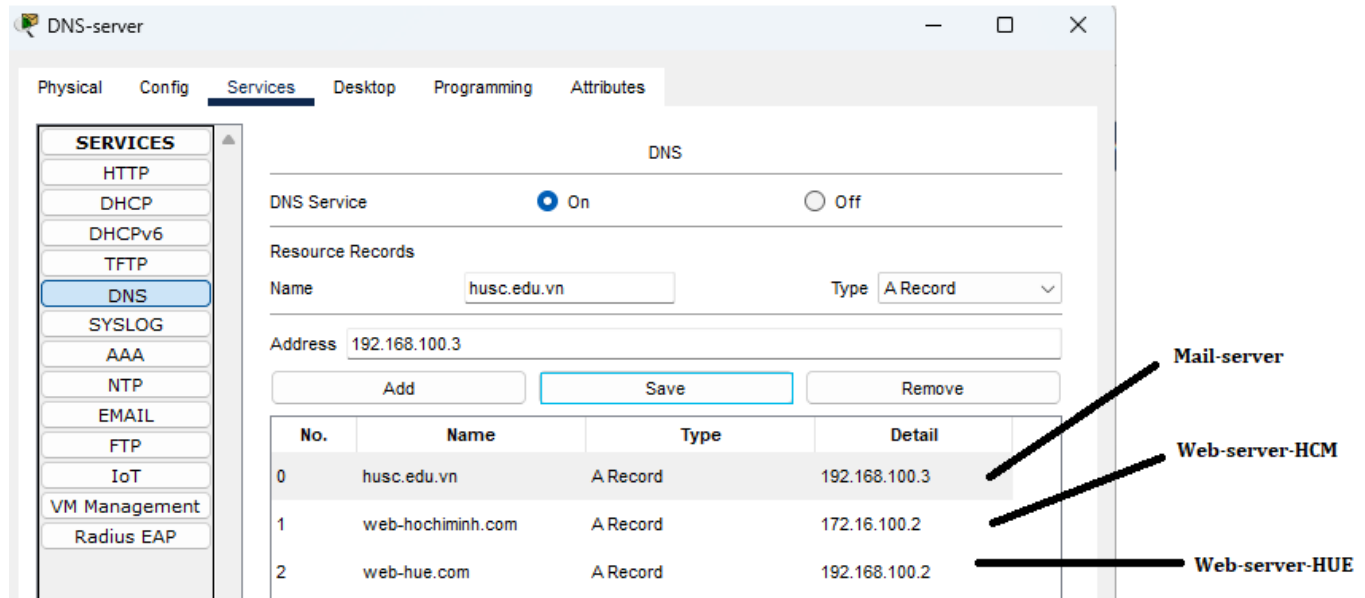
HCM(config)#crypto map MYMAP 10 ipsec-isakmp
HCM(config-crypto-map)#set peer 113.114.115.1
HCM(config-crypto-map)#set transform-set MYSET
HCM(config-crypto-map)#match address 100
```

Bước 5: Gán Crypto Map vào cổng nối ra internet

```
HUE(config)#interface fa0/0
HUE(config-if)#crypto map MYMAP

HCM(config)#interface fa0/1
HCM(config-if)#crypto map MYMAP
```

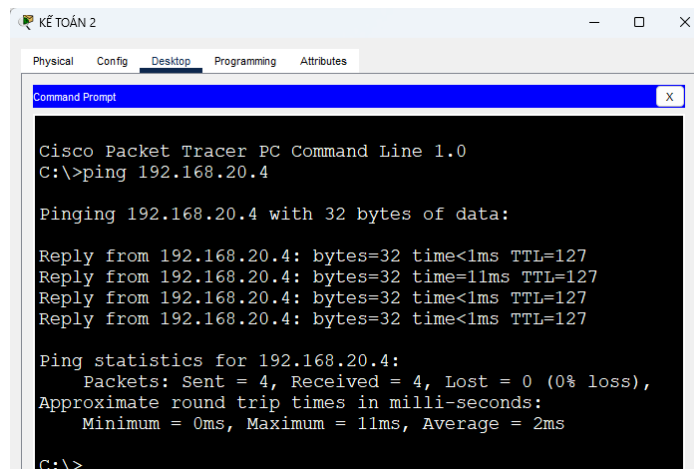
4.2.6. Cấu hình DNS – Server cho Web – server và Mail – server



Hình 4. 2. Cấu hình DNS – Server

4.3. KIỂM TRA KẾT QUẢ CẤU HÌNH

- Kiểm tra hệ thống nội bộ trong chi nhánh HUẾ:
 - Từ PC Phòng Kế Toán ping đến PC Phòng Kinh Doanh:



Hình 4. 3. Từ PC Phòng Kế Toán ping đến PC Phòng Kinh Doanh

- Từ PC Phòng Kế Toán ping đến PC Phòng Giám Đốc:

```

C:\>ping 192.168.30.2

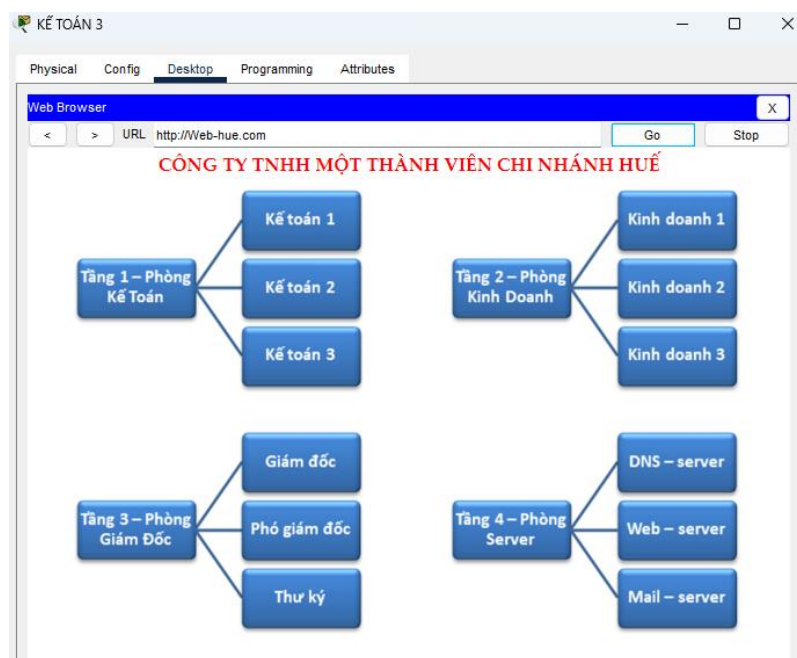
Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time<1ms TTL=127
Reply from 192.168.30.2: bytes=32 time=1ms TTL=127
Reply from 192.168.30.2: bytes=32 time=10ms TTL=127
Reply from 192.168.30.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
  
```

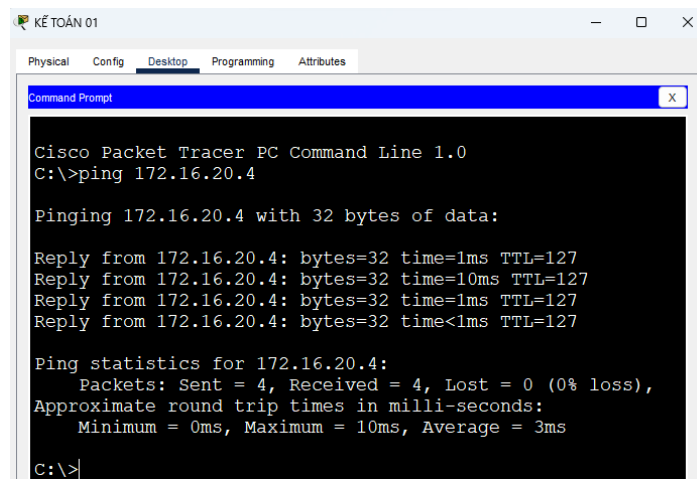
Hình 4. 4. Từ PC Phòng Kế Toán ping đến PC Phòng Giám Đốc

- Từ PC Phòng Kế Toán truy cập Web server Huế:



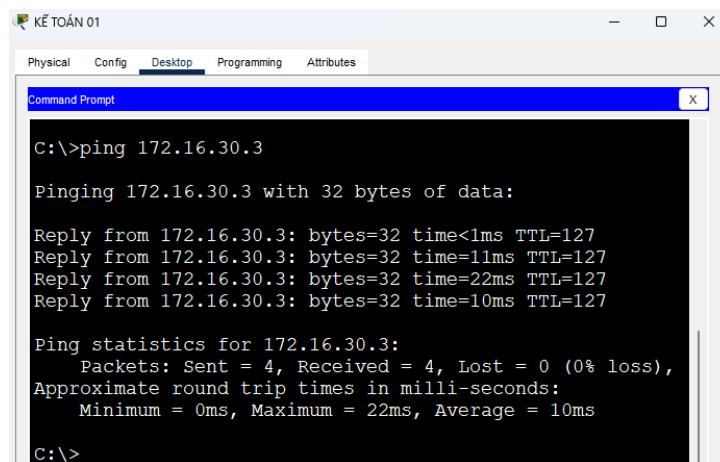
Hình 4. 5. Từ PC Phòng Kế Toán truy cập Web server Huế

- Kiểm tra hệ thống nội bộ trong chi nhánh SÀI GÒN:
 - Từ PC Phòng Kế Toán ping đến PC Phòng Kinh Doanh:



Hình 4. 6. Từ PC Phòng Kế Toán ping đến PC Phòng Kinh Doanh

- Từ PC Phòng Kế Toán ping đến PC Phòng Giám Đốc:



Hình 4. 7. Từ PC Phòng Kế Toán ping đến PC Phòng Giám Đốc

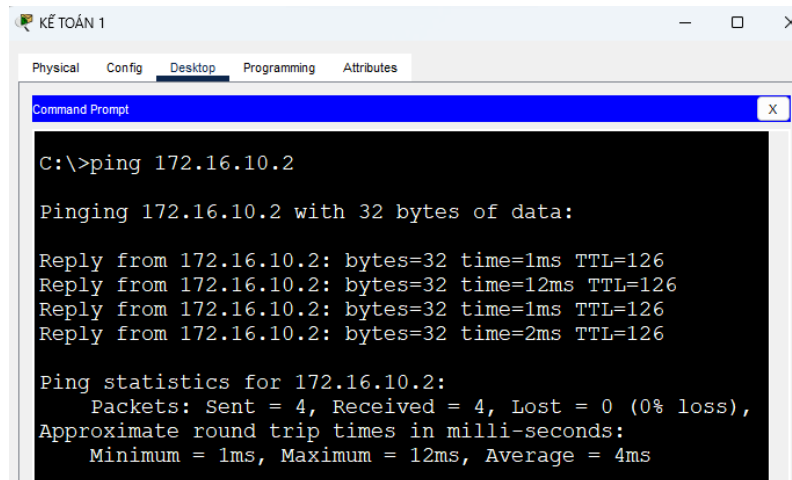
- Từ PC Phòng Kế Toán truy cập Web server Sài Gòn:



Hình 4. 8. Từ PC Phòng Kế Toán truy cập Web server Sài Gòn

➤ Kiểm tra kết nối VPN:

- Từ PC Phòng Kế Toán chi nhánh HUẾ ping đến PC Phòng Kế Toán chi nhánh SÀI GÒN:



```
KẾ TOÁN 1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.16.10.2

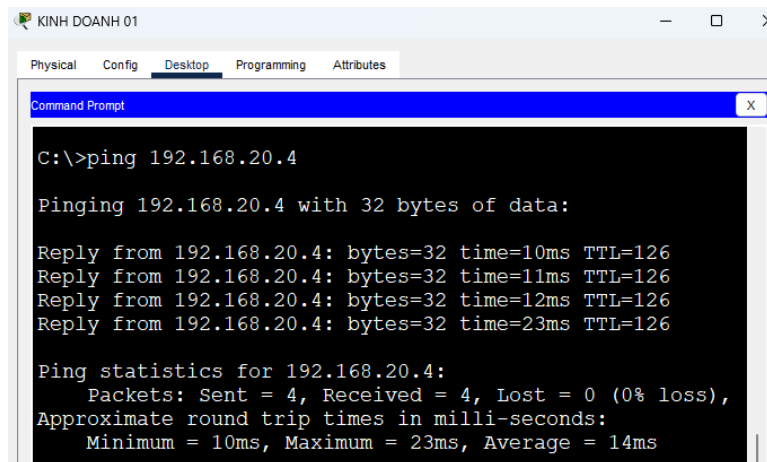
Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time=1ms TTL=126
Reply from 172.16.10.2: bytes=32 time=12ms TTL=126
Reply from 172.16.10.2: bytes=32 time=1ms TTL=126
Reply from 172.16.10.2: bytes=32 time=2ms TTL=126

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 4ms
```

Hình 4. 9. Ping giữa hai chi nhánh phòng Kế Toán

- Từ PC Phòng Kinh Doanh chi nhánh SÀI GÒN ping đến PC Phòng Kinh Doanh chi nhánh HUẾ:



```
KINH DOANH 01
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.20.4

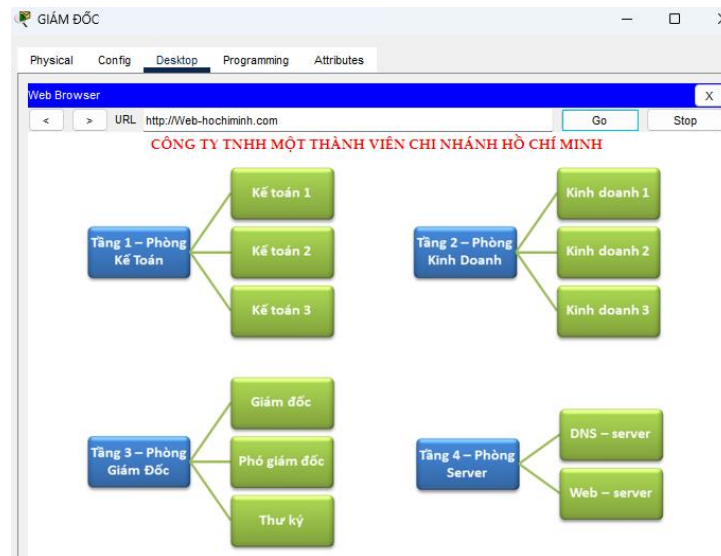
Pinging 192.168.20.4 with 32 bytes of data:

Reply from 192.168.20.4: bytes=32 time=10ms TTL=126
Reply from 192.168.20.4: bytes=32 time=11ms TTL=126
Reply from 192.168.20.4: bytes=32 time=12ms TTL=126
Reply from 192.168.20.4: bytes=32 time=23ms TTL=126

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 23ms, Average = 14ms
```

Hình 4. 10. Ping giữa hai chi nhánh phòng Kinh Doanh

- Từ PC chi nhánh HUẾ truy cập Web SÀI GÒN



Hình 4. 11. Từ PC chi nhánh HUẾ truy cập Web SÀI GÒN

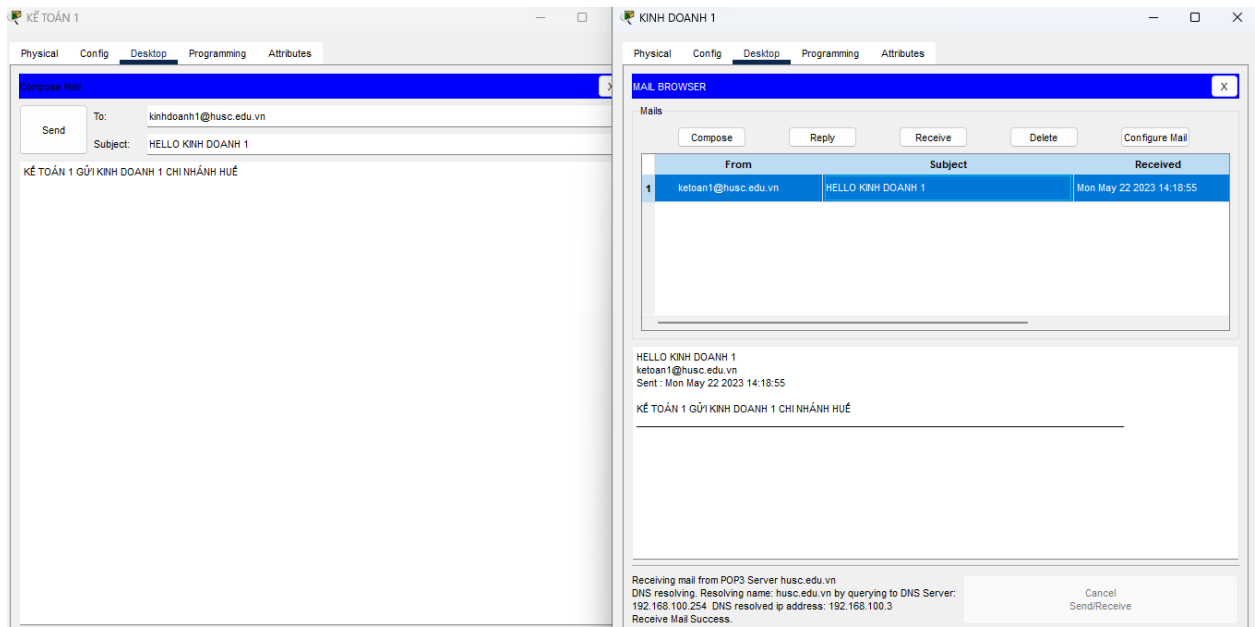
- Từ PC chi nhánh SÀI GÒN truy cập Web HUẾ



Hình 4. 12. Từ PC chi nhánh SÀI GÒN truy cập Web HUẾ

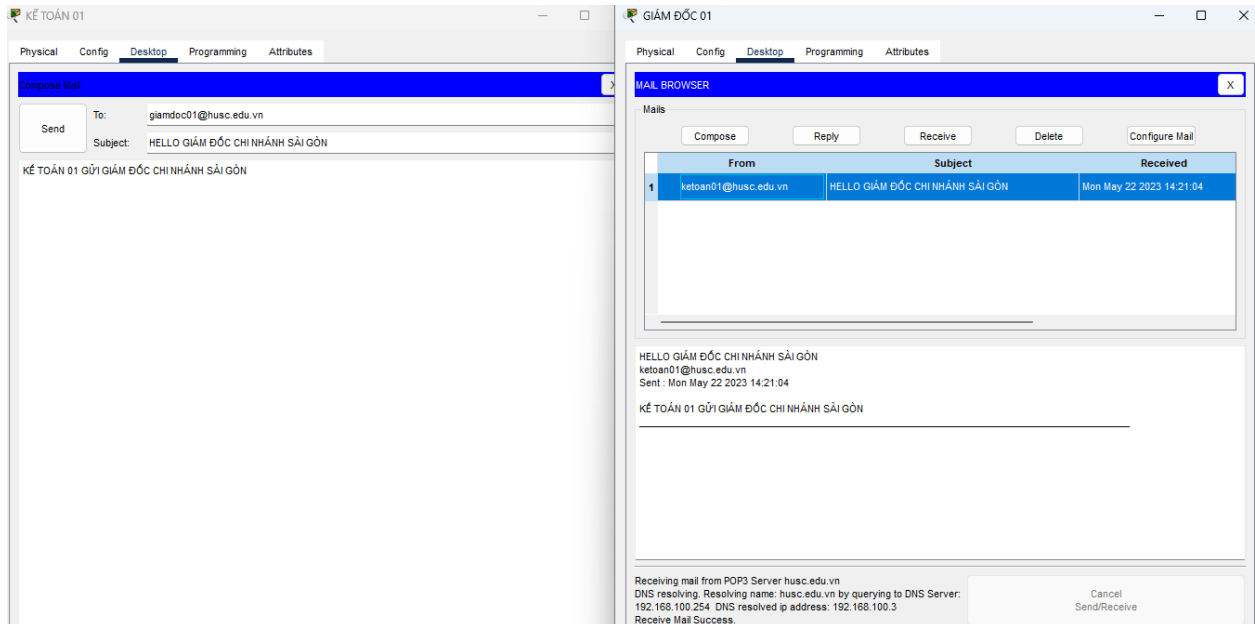
➤ Gửi email:

- Trong cùng chi nhánh HUẾ:



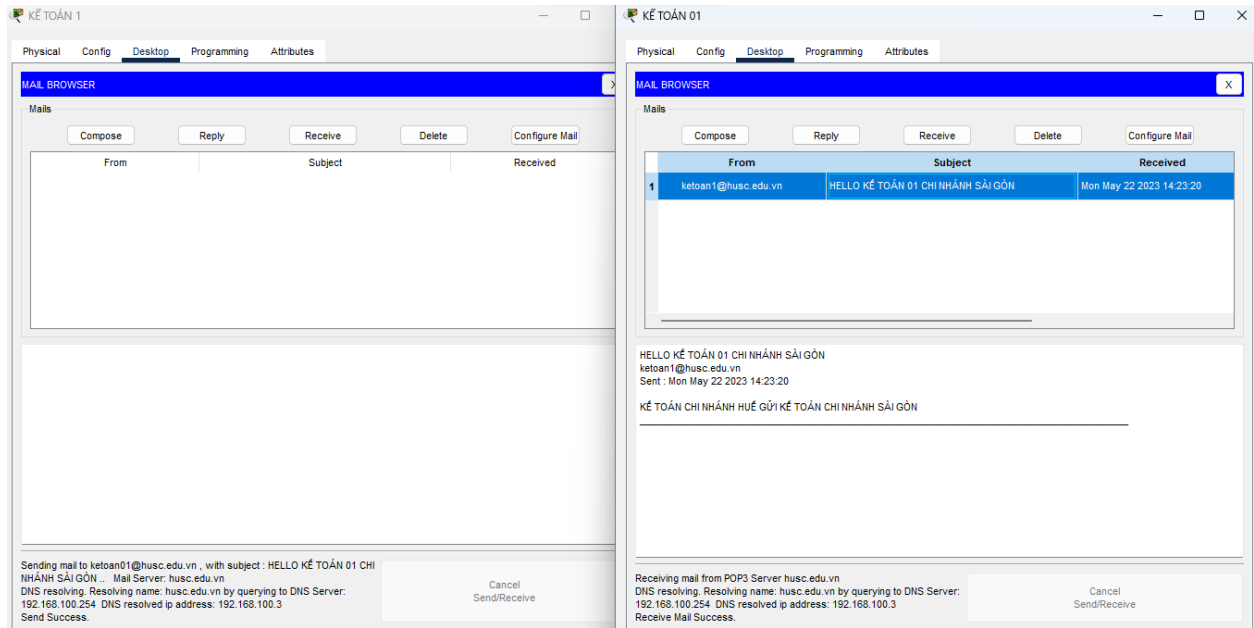
Hình 4. 13. Gửi Email từ Phòng kế toán đến Phòng kinh doanh cùng chi nhánh Huế

- Trong cùng chi nhánh SÀI GÒN:



Hình 4. 14. Gửi Email từ Phòng kế toán đến Phòng giám đốc cùng chi nhánh SÀI GÒN

- Khác chi nhánh:



Hình 4. 15. Gửi email giữa hai chi nhánh

CHƯƠNG V.

KẾT LUẬN

Công nghệ mạng riêng ảo VPN (Virtual Private Network) là một công nghệ tương đối mới, việc nghiên cứu và triển khai các loại mạng VPN đòi hỏi nhiều thời gian và công sức.

Trong bài đồ án này, em đã trình bày những khái niệm cơ bản nhất về VPN, vấn đề bảo mật hệ thống, nghiên cứu một cách kỹ lưỡng cơ sở lý thuyết.

Trong phần thực nghiệm của đồ án, em đã xây dựng và cấu hình thành công mạng VPN Site to Site.

Trong một khoảng thời gian ngắn, em không thể tránh khỏi những sai sót, em xin chân thành cảm ơn thầy cô đặc biệt là thầy Hồ Đức Tâm Linh, bạn bè, đồng nghiệp đã giúp đỡ, góp ý em hoàn thành đồ án này.

TÀI LIỆU THAM KHẢO

- [1]. Quản trị mạng và ứng dụng của Active Directory, tác giả K/S Ngọc Tuấn
NXB Thống kê năm 2004.
- [2]. Mạng truyền thông công nghiệp, tác giả Hoàng Minh Sơn, NXB Khoa học kỹ
thuật năm 2004.
- [3]. 100 thủ thuật bảo mật mạng, tác giả K/S Nguyễn Ngọc Tuấn, Hồng Phúc
NXB Giao thông vận tải, năm 2005.
- [4]. TS Nguyễn Tiến Ban và Thạc sĩ Hoàng Trọng Minh, “Mạng riêng ảo VPN”,
2007.
- [5]. PGS-TS. Nguyễn Văn Tam - Giáo trình An toàn mạng ĐH Thăng Long.
- [6]. D_link Australia & NZ, “Virtual Private Network self study”.
- [7]. Stephen Thomas, “SSL and TLS Essential”.
- [8]. David Bruce, Yakov Rekhter - (2000) Morgan Kaufmann Publisher - MPLS
Technology and Application MPLS_Cisco.pdf.