

**BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**



BÁO CÁO THỰC TẬP TỐT NGHIỆP ĐẠI HỌC

***Đề tài: “XÂY DỰNG HỆ THỐNG MẠNG BẢO
MẬT ĐA LỚP CHO HỘI SỞ NGÂN HÀNG VỚI
CISCO ASA VÀ VPN”***

Người hướng dẫn : ThS. ĐÀM MINH LINH
Sinh viên thực hiện: NGUYỄN BÁ TRUNG – N21DCAT060
LÊ KHÁNH BÌNH ĐỨC – N21DCAT013
ĐINH VĂN HẬU – N21DCAT017

Lớp : D21CQAT01-N
Khóa : 2021-2026
Ngành : AN TOÀN THÔNG TIN
Hệ : ĐẠI HỌC CHÍNH QUY

TP. HCM, tháng 08/2025



BÁO CÁO THỰC TẬP TỐT NGHIỆP ĐẠI HỌC

***Đề tài: “XÂY DỰNG HỆ THỐNG MẠNG BẢO
MẬT ĐA LỚP CHO HỘI SỞ NGÂN HÀNG VỚI
CISCO ASA VÀ VPN”***

Người hướng dẫn : ThS. ĐÀM MINH LỊNH
Sinh viên thực hiện: NGUYỄN BÁ TRUNG – N21DCAT060
LÊ KHÁNH BÌNH ĐỨC – N21DCAT013
ĐINH VĂN HẬU – N21DCAT017

Lớp : D21CQAT01-N
Khóa : 2021-2026
Ngành : AN TOÀN THÔNG TIN
Hệ : ĐẠI HỌC CHÍNH QUY

BẢNG PHÂN CÔNG

Thành Viên	Nhiệm vụ
Nguyễn Bá Trung	<ul style="list-style-type: none">– Tìm hiểu giao thức định tuyến ISIS, RIP, OSPF và BGP, cách thiết lập và quản lý định tuyến động– Tìm hiểu định tuyến tĩnh ip route– Cấu hình định tuyến kết hợp động (OSPF)/tĩnh cho các Router và các Router chi nhánh
Lê Khánh Bình Đức	<ul style="list-style-type: none">– Tìm hiểu kiến trúc, chức năng và cấu hình cơ bản của Cisco ASA Firewall, bao gồm NAT, ACL, VPN, zone-based Firewall– Tìm hiểu nguyên lý hoạt động và cấu hình AnyConnect VPN– Cấu hình 3 Zone ASA Firewal– Cấu hình cho người dùng tại Site chính và BR truy cập các Site qua ASA– Cấu hình AnyConnect cho quản trị truy cập các dịch vụ trong vùng DMZ
Đinh Văn Hậu	<ul style="list-style-type: none">– Tìm hiểu EVE-NG và VMWARE Worktation Pro– Tìm hiểu nguyên lý hoạt động và cấu hình IPSec VPN– Cấu hình IPSec làm đường kết nối VPN chính và dự phòng

LỜI CẢM ƠN

Để hoàn thành bài báo cáo thực tập tốt nghiệp này, đầu tiên nhóm chúng em xin gửi lời biết ơn sâu sắc đến quý thầy cô Học viện Công Nghệ Bưu Chính Viễn Thông cơ sở TP. Hồ Chí Minh. Các thầy cô đã tận tình giảng dạy, truyền đạt kiến thức và kinh nghiệm quý báu trong suốt quá trình học tập. Sự hướng dẫn tận tâm ấy đã giúp chúng em vững vàng hơn trong quá trình học.

Chúng em xin gửi lời cảm ơn sâu sắc đến quý thầy cô khoa Công nghệ Thông tin 2, đặc biệt là thầy hướng dẫn. Thầy đã tận tình hướng dẫn nhóm từ những bước đầu tiên đến khi hoàn thiện bài báo cáo thực tập tốt nghiệp. Sự hỗ trợ của thầy là yếu tố quan trọng giúp chúng em hoàn thành tốt nhiệm vụ này.

Do kiến thức còn hạn chế và thiếu kinh nghiệm thực tế, bài báo cáo của chúng em khó tránh khỏi những thiếu sót. Chúng em mong nhận được ý kiến đóng góp quý báu từ quý thầy cô để đề tài được hoàn thiện hơn. Những ý kiến này sẽ là hành trang quý giá cho chúng em trong tương lai.

Nhóm chúng em xin kính chúc quý thầy cô luôn dồi dào sức khỏe và đạt nhiều thành công trong công việc. Chúc Ban Giám đốc Học viện tiếp tục dẫn dắt nhà trường phát triển vững mạnh. Chúng em hy vọng sẽ tiếp tục nhận được sự giúp đỡ từ thầy cô trong tương lai.

TP. HCM, tháng 08 năm 2025

Nhóm thực hiện

Nhóm 4

MỤC LỤC

MỞ ĐẦU	1
1. Lý do lựa chọn đề tài	1
2. Mục đích của đề tài.....	1
3. Phạm vi nghiên cứu	1
4. Phương pháp nghiên cứu	1
5. Kết cấu của đề tài.....	1
CHƯƠNG 1. CƠ SỞ LÝ THUYẾT.....	3
1.1. Tìm hiểu về môi trường triển khai	3
1.1.1. Các khái niệm.....	3
1.2. Mô hình 3 lớp Cisco	3
1.2.1 Lớp Access (Access Layer)	4
1.2.2 Lớp Distribution (Distribution Layer)	5
1.2.3 Lớp Core (Core Layer).....	5
1.3. Tìm hiểu về giao thức định tuyến	6
1.3.1 Định tuyến tĩnh.....	6
1.3.2 Định tuyến động (OSPF).....	7
1.4. Tìm hiểu về IPSEC VPN	8
1.4.1. IPSEC	8
1.4.2. Thành phần của IPSEC	8
1.5. Firewall Cisco ASA	9
1.6. Anyconnect VPN	9
CHƯƠNG 2. ĐỀ XUẤT MÔ HÌNH BẢO MẬT CHO HỆ THỐNG MẠNG LỖI	
NGÂN HÀNG	12
2.1. Đề xuất mô hình	12
2.1.1. Mô hình tổng quát.....	12
2.1.2. Mô hình bao gồm	12
2.1.3. Giải thích yêu cầu mô hình	13
2.2. Nền tảng xác thực.....	13
2.2.1. Nền tảng xác thực tracer	13
2.2.2. Các giao thức xác thực.....	13
CHƯƠNG 3. TRIỂN KHAI THỰC NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ	14

3.1. Triển khai thực nghiệm	14
3.1.1. Thiết lập mô hình	14
3.1.2. Bảng thành phần.....	14
3.2. Cài đặt và cấu hình	15
3.2.1. Cài đặt các máy ảo	15
3.3. Đánh giá kết quả	19
3.3.1. Kết quả cấu hình	19
3.3.2. Kết quả thực nghiệm	32
CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	48
TÀI LIỆU THAM KHẢO	49
PHỤ LỤC.....	50

DANH MỤC CÁC KÝ HIỆU – CHỮ VIẾT TẮT

Chữ viết tắt	Từ	Ý nghĩa
EVE-NG	Emulated Virtual Environment – Next Generation	
IOS	Internetwork Operating System	
IPSEC	Internet Protocol Security	Giao thức bảo mật mạng
IP	Internet Protocol	Giao thức mạng
BR	Branch	Chi nhánh
ISP	Internet Service Provider	Hệ điều hành
GW	Gateway	Địa chỉ gateway
DHCP	Dynamic Host Configuration Protocol	Giao thức cấu hình máy chủ
OSPF	Open Shortest Path First	Giao thức định tuyến động
VPN	Virtual Private Network	Mạng riêng ảo
CIDR	Classless Inter Domain Routing	Định tuyến liên kết miền không phân lớp
VLSM	Variable Length Subnet Mask	Phân chia không gian mạng
ESP	Encapsulating Security Payload	
AH	Authentication Header	
IKE	Internet Key Exchange	

BẢNG 1: Bảng danh mục ký hiệu - chữ viết tắt

DANH MỤC CÁC BẢNG VẼ

BẢNG 1: Bảng danh mục ký hiệu - chữ viết tắt.....	iv
BẢNG 2: Bảng Các tính năng của giải pháp di động an toàn Cisco AnyConnect...	11
BẢNG 3: Bảng IP và subnet cho các thành phần trong mạng.....	15

DANH MỤC CÁC HÌNH VẼ

HÌNH 2.1 Mô hình tổng quát	12
HÌNH 3.1 Mô hình triển khai	14
HÌNH 3.2 Cấu hình Router BR	19
HÌNH 3.3 Cấu hình Router ISP	20
HÌNH 3.4 Cấu hình Router GW1	20
HÌNH 3.5 Cấu hình GW2	21
HÌNH 3.6 Cấu hình Router CORE1	21
HÌNH 3.7 Cấu hình Router CORE2	22
HÌNH 3.8 DHCP Server trên Router BR	22
HÌNH 3.9 DHCP Server trên Router CORE1	22
HÌNH 3.10 Cấu hình DHCP Server trên Router CORE2	22
HÌNH 3.11 Cấu hình IPSEC Profile trên Router BR	23
HÌNH 3.12 Cấu hình Tunnel10 và Tunnel20	24
HÌNH 3.13 Cấu hình IPSEC trên Router GW1	24
HÌNH 3.14 Cấu hình Tunnel10	25
HÌNH 3.15 Cấu hình IPSEC Profile cho Router GW2	25
HÌNH 3.16 Cấu hình Tunnel20	26
HÌNH 3.17 Cấu hình định tuyến BR	26
HÌNH 3.18 Cấu hình định tuyến GW1	26
HÌNH 3.19 Cấu hình định tuyến GW2	27
Hình 3.20 Cấu hình định tuyến tới DMZ	27
HÌNH 3.21 Định tuyến Tunnel10 và Tunnel20	27
HÌNH 3.22 Cấu hình OSPF trên BR	27
HÌNH 3.23 Cấu hình OSPF trên GW1	28
HÌNH 3.24 Cấu hình OSPF trên GW2	28
HÌNH 3.25 Cấu hình OSPF trên Router CORE1	28
HÌNH 3.26 Cấu hình OSPF trên Router CORE2	28
HÌNH 3.27 Cấu hình 3 Zone ASA	29
HÌNH 3.28 Cấu hình định tuyến trên ASA	29
HÌNH 3.29 Cấu hình ACL Inside	29
HÌNH 3.30 Pool địa chỉ cho VPN Client	30
HÌNH 3.31 Tạo user	30

HÌNH 3.32 Tạo group-policy	30
HÌNH 3.33 Tạo ACL cho Split Tunnel.....	30
HÌNH 3.34 Tạo Tunnel-group.....	31
HÌNH 3.35 Bật webvpn và kích hoạt AnyConnect.....	31
HÌNH 3.36 Tạo Object network.....	31
HÌNH 3.37 NAT cho VPN client.....	31
HÌNH 3.38 Gán ACL	32
HÌNH 3.39 Mở HTTP Server.....	32
HÌNH 3.40 Cấp địa chỉ IP cho VPC1-BR.....	32
HÌNH 3.41 Cấp địa chỉ IP cho VPC2-BR.....	33
HÌNH 3.42 Cấp địa chỉ IP cho VPC1-C1	33
HÌNH 3.43 Cấp địa chỉ IP cho VPC2-C1	34
HÌNH 3.44 Cấp địa chỉ IP cho VPC1-C2	34
HÌNH 3.45 Cấp địa chỉ IP cho VPC2-C2	34
HÌNH 3.46 Kiểm tra kết nối BR tới CORE1	35
HÌNH 3.47 Kiểm tra kết nối BR	35
HÌNH 3.48 Ping thành công vào LAN 172.17.0.2.....	35
HÌNH 3.49 Kiểm tra đường đi	36
HÌNH 3.50 Kiểm tra khi tắt GW1 và GW2	36
HÌNH 3.51 Ping thất bại.....	36
HÌNH 3.52 Capture e0/0 trên BR.....	37
HÌNH 3.53 Kiểm tra dự phòng	37
HÌNH 3.54 Truy cập vào IP của Zone Outside.....	38
HÌNH 3.55 Đăng nhập	39
HÌNH 3.56 Tải về.....	39
HÌNH 3.57 Truy cập IP của ASA	40
HÌNH 3.58 Cảnh báo kết nối.....	40
HÌNH 3.59 Kết nối.....	41
HÌNH 3.60 Kiểm tra kết nối.....	41
HÌNH 3.61 Kiểm tra lịch sử.....	42
HÌNH 3.62 Xem thông tin kết nối.....	43
HÌNH 3.63 Route được kết nối	44

HÌNH 3.64 Kiểm tra kết nối DMZ	44
HÌNH 3.65 Chứng thực AnyConnectVPN	45
HÌNH 3.66 Các gói TCP	45
HÌNH 3.67 Capture eth1	46
HÌNH 3.68 Ping từ VPC1-C1	46
HÌNH 3.69 Ping từ VPC1-C2	47

MỞ ĐẦU

1. Lý do lựa chọn đề tài

Lựa chọn đề tài “*Xây dựng hệ thống mạng bảo mật đa lớp cho hội sở ngân hàng với Cisco ASA và VPN*” xuất phát từ nhiều lý do quan trọng sau đây:

Bảo vệ tài sản và dữ liệu quan trọng: Hội sở ngân hàng hiện nay dựa nhiều vào các hệ thống mạng và dữ liệu để thực hiện các hoạt động hàng ngày. Mất mát hoặc vi phạm dữ liệu có thể gây hậu quả nghiêm trọng cho hội sở bao gồm các thiệt hại về tài chính và danh tiếng. Sử dụng thiết bị chuyên dụng trong hệ thống an toàn bảo mật mạng giúp đảm bảo rằng các tài sản và dữ liệu quan trọng được bảo vệ tốt nhất khỏi các mối đe dọa mạng.

Hiệu suất và tích hợp tối ưu: Các thiết bị chuyên dụng thường được tối ưu hóa để đáp ứng các yêu cầu riêng biệt của bảo mật mạng. Chúng có thể cung cấp hiệu suất cao và tích hợp tốt với các hệ thống mạng hiện có của hội sở. Điều này giúp tối ưu hóa hiệu quả và giảm thiểu thời gian và công sức đầu tư vào việc triển khai và quản lý hệ thống bảo mật.

Đáp ứng các yêu cầu đặc thù: Mỗi hội sở có các yêu cầu bảo mật riêng biệt phù hợp với môi trường và quy mô của họ. Thiết bị chuyên dụng cho phép tùy chỉnh và cấu hình linh hoạt để đáp ứng các yêu cầu đặc thù của hội sở một cách chính xác.

Quản lý dễ dàng: Các thiết bị chuyên dụng thường đi kèm với các công cụ quản lý tập trung, giúp quản lý hệ thống an toàn mạng một cách dễ dàng và hiệu quả. Điều này giúp giảm thiểu lỗi con người và tăng cường khả năng phát hiện và phản ứng nhanh chóng đối với các mối đe dọa.

Hỗ trợ kỹ thuật chuyên sâu: Khi sử dụng các thiết bị chuyên dụng, hội sở thường có sẵn hỗ trợ kỹ thuật chuyên sâu từ nhà cung cấp hoặc nhà sản xuất. Điều này đảm bảo rằng họ sẽ nhận được giải pháp và giúp đỡ nhanh chóng trong trường hợp xảy ra sự cố hoặc vấn đề bảo mật.

2. Mục đích của đề tài

Đề tài “Xây dựng hệ thống mạng bảo mật đa lớp cho hội sở ngân hàng với Cisco ASA và VPN” nhằm đề xuất mô hình và triển khai hệ thống mạng an toàn, bảo vệ dữ liệu tài chính và giao dịch ngân hàng trước các mối đe dọa mạng. Hệ thống sử dụng Cisco ASA, IPSec VPN, và AnyConnect VPN để đảm bảo tính bí mật, toàn vẹn, và sẵn sàng.

Đề tài cung cấp cơ hội thực hành trên EVE-NG, nghiên cứu các giao thức định tuyến (OSPF, BGP, ISIS, RIP) và cấu hình bảo mật đa lớp (NAT, ACL, zone-based firewall), giúp xây dựng mô hình mạng thực tiễn, tăng cường kỹ năng và đáp ứng nhu cầu bảo mật của ngân hàng.

3. Phạm vi nghiên cứu

Sử dụng ảo hóa VMWare và thiết bị Cisco (Router, Switch, Firewall ASA) trong việc xây dựng một mô hình hệ thống an toàn bảo mật mạng cho hội sở.

4. Phương pháp nghiên cứu

Các phương pháp được thực hiện trong quá trình nghiên cứu gồm: phương pháp phân tích, phương pháp so sánh, phương pháp tổng hợp. Đề tài cũng vận dụng những lý thuyết cơ bản, những lý luận khoa học trong lĩnh vực công nghệ thông tin.

5. Kết cấu của đề tài

Bố cục đề tài gồm 4 phần:

NHÓM 4, D21CQAT01-N

Chương 1: Cơ sở lý thuyết.

Chương 2: Đề xuất mô hình bảo mật cho hệ thống mạng lõi.

Chương 3: Triển khai thực nghiệm và đánh giá kết quả.

Chương 4: Kết luận và hướng phát triển.

CHƯƠNG 1. CƠ SỞ LÝ THUYẾT

1.1. Tìm hiểu về môi trường triển khai

1.1.1. Các khái niệm

EVE-NG (Emulated Virtual Environment – Next Generation) là một trong các công cụ giả lập mạnh nhất hiện nay, thừa hưởng các tính năng của UnetLab, EVE-NG cũng có thể giả lập rất nhiều loại thiết bị mạng đang được sử dụng rộng rãi, với nhiều nền tảng hệ thống điều hành khác nhau: router/switch của Cisco (sử dụng Cisco IOL hoặc IOS trên nền Dynamip Server), thiết bị mạng của Juniper, nhiều loại firewall thông dụng.

Cisco IOL (Cisco IOS on Linux) là một giả lập hệ điều hành mạng Cisco IOS (Internetwork Operating System) chạy trên nền tảng Linux. Nó cho phép thử nghiệm và tạo các môi trường mạng ảo để mô phỏng, kiểm tra và thực hành các thiết lập mạng Cisco mà không cần phải sử dụng các thiết bị vật lý thực tế.

VMware Workstation là một phần mềm cho phép người dùng chạy máy ảo trên máy tính vật lý, người dùng có thể tạo và hủy máy ảo dễ dàng trên máy chủ chỉ cần bằng công cụ này. Tại VMware Workstation, người dùng sẽ chạy được máy ảo ở máy tính để bàn bằng hệ điều hành Windows hoặc Linux đều ổn.

Lý do lựa chọn môi trường

Thị trường dẫn đầu: VMWare là một trong những nhà cung cấp hàng đầu về công nghệ ảo hóa, được tin dùng và sử dụng rộng rãi trên toàn cầu. Hỗ trợ từ một nhà cung cấp được thừa nhận như VMWare giúp đảm bảo tính tin cậy và hiệu quả của hệ thống ảo hóa.

Tích hợp mạnh mẽ: VMWare cung cấp các công cụ quản lý mạnh mẽ và tích hợp sâu vào hạ tầng mạng hiện có. Nó cũng hỗ trợ tích hợp với nhiều công nghệ và sản phẩm khác, cho phép môi trường mạng linh hoạt và dễ quản lý.

Tích hợp nhiều hệ điều hành mạng: EVE-NG là một giải pháp ảo hóa mạng mạnh mẽ cho phép mô phỏng và triển khai các thiết bị mạng, như Router, Switch, Firewall, và thậm chí máy chủ máy tính trong môi trường ảo. EVE-NG hỗ trợ mô phỏng các hệ điều hành mạng phổ biến như Cisco IOS, Juniper JunOS, Palo Alto PAN-OS, và nhiều hệ điều hành khác, cho phép xây dựng môi trường thử nghiệm và kiểm tra mạng phức tạp.

Hỗ trợ giao tiếp mạnh mẽ: EVE-NG là một dự án mã nguồn mở với cộng đồng sôi nổi của các nhà phát triển và người dùng. Cộng đồng này cung cấp các hướng dẫn, tài liệu và tư vấn hữu ích để hỗ trợ người dùng triển khai và sử dụng EVE-NG một cách hiệu quả.

1.2. Mô hình 3 lớp Cisco

Mô hình 3 lớp phân cấp của Cisco là một khung thiết kế mạng tiêu chuẩn được phát triển bởi Cisco Systems để xây dựng các mạng doanh nghiệp một cách có cấu trúc, hiệu quả và dễ mở rộng. Mô hình này được giới thiệu từ những năm 1990 và đã trở thành nền tảng cho nhiều thiết kế mạng hiện đại, đặc biệt trong môi trường doanh nghiệp lớn nơi cần xử lý lưu lượng dữ liệu cao, đảm bảo tính sẵn sàng và bảo mật. Thay vì sử dụng thiết kế mạng phẳng, nơi tất cả các thiết bị kết nối trực tiếp mà không có phân cấp, mô

hình 3 lớp chia mạng thành ba lớp chính: Access Layer (Lớp Truy cập), Distribution Layer (Lớp Phân phối) và Core Layer (Lớp Lõi). Điều này giúp cô lập lỗi, tối ưu hóa hiệu suất và dễ dàng quản lý. [1]

Mục đích chính của mô hình là giải quyết các vấn đề trong mạng lớn, như tắc nghẽn lưu lượng, độ trễ cao và khó khăn trong việc mở rộng. Bằng cách phân chia chức năng rõ ràng, mô hình cho phép lưu lượng dữ liệu chảy theo hướng từ dưới lên (access → distribution → core), với mỗi lớp tập trung vào vai trò cụ thể. Trong mạng nhỏ, các lớp có thể được gộp lại, ví dụ kết hợp Distribution và Core để tiết kiệm chi phí, nhưng ở mạng lớn, việc tách biệt giúp tăng tính linh hoạt. Mô hình này được áp dụng rộng rãi trong các tài liệu thiết kế của Cisco, như Enterprise Campus 3.0 Architecture, và là một phần quan trọng trong chương trình chứng chỉ CCNA.

Theo các tài liệu từ Cisco, mô hình hierarchical không chỉ giới hạn ở ba lớp mà có thể mở rộng thành hai lớp cho mạng nhỏ hơn hoặc thêm các lớp phụ để xử lý địa lý phức tạp. Tuy nhiên, ba lớp cơ bản vẫn là tiêu chuẩn vàng, mang lại lợi ích như tính khả mở, độ tin cậy và dễ bảo trì. Chúng ta sẽ khám phá chi tiết từng lớp, bao gồm chức năng, công nghệ, lợi ích và các cân nhắc thiết kế, dựa trên các nguồn uy tín từ Cisco và các trang giáo dục. [2]

1.2.1 Lớp Access (Access Layer)

Lớp Access là lớp thấp nhất trong mô hình, đóng vai trò như "cổng vào" của mạng, nơi các thiết bị cuối như máy tính, điện thoại IP, máy in, camera và access point không dây kết nối trực tiếp. Chức năng chính của lớp này là cung cấp kết nối cho người dùng và thiết bị, thực hiện kiểm soát truy cập ban đầu, phân loại lưu lượng và áp dụng các chính sách bảo mật cơ bản. Không giống như mạng phẳng nơi tất cả lưu lượng có thể lan tỏa khắp nơi, lớp Access giữ lưu lượng cục bộ trong các miền và phạm vi riêng biệt, giảm tắc nghẽn và tăng hiệu suất. Chức năng chi tiết: Lớp này xử lý việc kết nối thiết bị, cung cấp Power over Ethernet (PoE) cho các thiết bị như điện thoại VoIP hoặc access point, và thực hiện các dịch vụ khám phá thiết bị. Nó cũng chịu trách nhiệm tạo các VLAN (Virtual Local Area Networks) để phân đoạn mạng, giúp cô lập lưu lượng và tăng bảo mật. Ví dụ, trong một văn phòng, các thiết bị của bộ phận tài chính có thể được đặt trong VLAN riêng để tránh truy cập từ bộ phận khác. [2]

Công nghệ và thiết bị: Sử dụng chủ yếu các switch lớp 2 như Cisco Catalyst 2960 hoặc 9300 series. Các giao thức chính bao gồm 802.1X cho xác thực, CDP (Cisco Discovery Protocol) và LLDP (Link Layer Discovery Protocol) để khám phá thiết bị, cũng như các tính năng bảo mật như port security, DHCP snooping, Dynamic ARP Inspection (DAI) và IP Source Guard. QoS (Quality of Service) được áp dụng ở đây để phân loại và đánh dấu gói tin, ví dụ sử dụng NBAR (Network-Based Application Recognition) để nhận diện ứng dụng và ưu tiên lưu lượng voice/video. Trong mạng hiện đại, lớp này hỗ trợ PoE+ hoặc UPoE cho các thiết bị IoT.

Lợi ích: Lớp Access tăng cường bảo mật bằng cách hoạt động như "rào chắn" đầu tiên chống lại các mối đe dọa như tấn công DoS, ARP spoofing hoặc truy cập trái phép.

Nó hỗ trợ tính di động cho người dùng, cho phép thiết bị kết nối động mà không cần cấu hình thủ công. So với mạng phẳng, lớp này giảm thiểu va chạm, dẫn đến hiệu suất cao hơn và dễ dàng mở rộng bằng cách thêm switch mà không ảnh hưởng toàn bộ mạng.

1.2.2 Lớp Distribution (Distribution Layer)

Lớp Distribution là lớp trung gian, tổng hợp lưu lượng từ nhiều lớp Access và kết nối chúng với Core Layer. Nó đóng vai trò như "người gác cổng" cho các chính sách mạng, xử lý định tuyến giữa các VLAN (inter-VLAN routing), lọc gói tin và áp dụng các quy tắc bảo mật nâng cao. Lớp này giúp giữ lưu lượng cục bộ không lan ra toàn mạng, giảm tải cho Core và tăng hiệu quả tổng thể.

Chức năng chi tiết: Tổng hợp lưu lượng từ các switch Access, thực hiện routing Layer 3, hỗ trợ kết nối WAN và áp dụng ACL (Access Control Lists) để kiểm soát truy cập. Nó cũng xử lý dịch địa chỉ NAT, policy enforcement và QoS queuing để ưu tiên lưu lượng quan trọng trong lúc tắc nghẽn. Trong mô hình Routed Access, lớp này có thể đẩy routing xuống Access để tăng tốc độ hội tụ.

Công nghệ và thiết bị: Sử dụng switch đa lớp hoặc router như Cisco Catalyst 9300 hoặc 4500 series. Các giao thức bao gồm EIGRP, OSPF cho routing, HSRP/VRRP cho dự phòng, và Spanning Tree Protocol (STP) biến thể như Rapid PVST+ để tránh lặp. Hỗ trợ VRF (Virtual Routing and Forwarding) cho virtualization và MPLS cho việc thiết kế lưu lượng. Bảo mật bao gồm CoPP (Control Plane Policing) để bảo vệ CPU khỏi tấn công.

Lợi ích: Tăng tính khả mở bằng cách tổng hợp nhiều Access block, hỗ trợ cân bằng tải và nhanh chóng hội tụ sau lỗi. Nó cung cấp biên giới chính sách, giúp mạng dễ quản lý và bảo mật hơn so với mạng phẳng, nơi không có phân cách rõ ràng dẫn đến rủi ro cao. Trong môi trường doanh nghiệp, lớp này đảm bảo lưu lượng nhạy cảm như dữ liệu tài chính được lọc trước khi đến Core. [3]

1.2.3 Lớp Core (Core Layer)

Lớp Core là "xương sống" của mạng, chịu trách nhiệm vận chuyển lưu lượng lớn với tốc độ cao và độ trễ thấp giữa các khối mạng. Nó tập trung vào chuyển mạch nhanh, không xử lý các chính sách phức tạp để tránh làm chậm mạng, và đảm bảo tính sẵn sàng cao nhất.

Chức năng chi tiết: Kết nối các khối phân phối, hỗ trợ kết nối với trung tâm dữ liệu hoặc mạng WAN, và vận chuyển lưu lượng toàn cầu. Nó xử lý hàng gigabit dữ liệu, ưu tiên QoS dựa trên marking từ lớp dưới, và cung cấp tính năng hạn chế lỗi ở một khu vực không ảnh hưởng toàn bộ.

Công nghệ và thiết bị: Sử dụng switch cao cấp như Cisco Catalyst 9600 hoặc Nexus serie. Các giao thức bao gồm OSPF/EIGRP cho routing nhanh, MPLS cho VPN lớp 3, và EtherChannel cho các liên kết dư thừa. Hỗ trợ cáp quang để đạt băng thông cao với độ trễ thấp.

Lợi ích: Đảm bảo hiệu suất cao cho ứng dụng thời gian thực như video conferencing hoặc VoIP. So với mạng phẳng, lớp Core giảm độ phức tạp bằng cách chỉ tập trung vào forwarding, giúp mạng mở rộng dễ dàng mà không cần thay đổi toàn bộ cấu trúc. [3]

1.3. Tìm hiểu về giao thức định tuyến

1.3.1 Định tuyến tĩnh

Định tuyến tĩnh là phương pháp cấu hình thủ công các tuyến đường trên router để hướng dẫn gói tin di chuyển từ mạng nguồn đến mạng đích. Không giống như định tuyến động sử dụng các giao thức như RIP, OSPF hay EIGRP để tự động học và cập nhật tuyến đường, định tuyến tĩnh yêu cầu quản trị viên nhập trực tiếp thông tin vào bảng định tuyến. Trong môi trường Cisco IOS, lệnh chính để cấu hình định tuyến tĩnh là "ip route". Lệnh này cho phép định nghĩa mạng đích, subnet mask và next-hop (địa chỉ hoặc interface tiếp theo để chuyển tiếp gói tin). Định tuyến tĩnh phù hợp cho mạng nhỏ, ổn định, hoặc khi cần kiểm soát chặt chẽ lưu lượng, nhưng nó không tự động thích ứng với thay đổi mạng.

Lệnh "ip route" được sử dụng ở chế độ global configuration và là công cụ cốt lõi để thêm tuyến tĩnh. Khi một gói tin đến router, router sẽ tra cứu bảng định tuyến để tìm tuyến đường khớp. Nếu khớp với tuyến tĩnh, gói tin sẽ được chuyển tiếp theo next-hop đã định nghĩa. Nếu không có tuyến nào, router có thể sử dụng tuyến mặc định để gửi đến gateway cuối cùng, thường là kết nối internet hoặc mạng ngoài. [4]

1.3.1.1 Cách hoạt động của IP Route

Bước 1: Xác định thông tin tuyến đường: Xác định mạng đích và subnet mask. Đồng thời, cần xác định next-hop hoặc exit interface.

Bước 2: Cấu hình tuyến đường tĩnh: Sử dụng lệnh ip route trong chế độ cấu hình toàn cục trên router Cisco.

Bước 3: Kiểm tra và xác minh: Sau khi cấu hình, router lưu tuyến đường vào bảng định tuyến với ký hiệu "S" (static).

Bước 4: Quản lý và bảo trì: Nếu mạng thay đổi (ví dụ: next-hop không còn tồn tại), quản trị viên phải xóa tuyến đường bằng lệnh no ip route và thêm tuyến mới. Tuyến dự phòng có thể được cấu hình với administrative distance cao hơn để thay thế khi tuyến chính thất bại.

1.3.1.2 Ưu và nhược điểm của IP Route

Ưu điểm:

- + Đơn giản và dễ cấu hình: Lệnh ip route dễ sử dụng, không yêu cầu kiến thức sâu về giao thức định tuyến.
- + Tiết kiệm tài nguyên: Không sử dụng CPU hoặc băng thông để trao đổi thông tin định tuyến như OSPF hoặc EIGRP.
- + Bảo mật cao: Không có rủi ro từ các giao thức động bị tấn công (như routing table poisoning).

- + Kiểm soát chính xác: Quản trị viên có thể chỉ định đường đi cố định, phù hợp cho mạng stub hoặc kết nối WAN.
- + Hiệu suất ổn định: Không có thời gian hội tụ, đảm bảo lưu lượng đi đúng tuyến đã định.

Nhược điểm:

- + Không linh hoạt: Không tự động cập nhật khi mạng thay đổi (ví dụ: liên kết đứt), yêu cầu can thiệp thủ công.
- + Khó quản lý ở mạng lớn: Cấu hình nhiều tuyến tính trên nhiều router dễ gây lỗi và tốn thời gian.
- + Không hỗ trợ load balancing tự động: Cần cấu hình thủ công tuyến dự phòng hoặc cân bằng tải.
- + Yêu cầu hiểu biết về cấu trúc mạng: Quản trị viên phải biết rõ địa chỉ mạng và next-hop để cấu hình đúng.

1.3.2 Định tuyến động (OSPF)

OSPF (Open Shortest Path First) là một giao thức định tuyến nội dựa trên thuật toán link state routing được sử dụng trong một hệ thống mạng hay một khu vực xác định. Mỗi bộ định tuyến của OSPF sẽ chứa thông tin của tất cả các tên miền để có thể dựa vào đó và xác định được quãng đường đi ngắn nhất và tốt nhất giữa bộ định tuyến nguồn và đích. Do đó, mục tiêu chính của giao thức này là tìm hiểu về các tuyến đường.

Giao thức OSPF đạt được mục tiêu của nó bằng cách tìm hiểu mọi bộ định tuyến và các mạng con có trong toàn bộ hệ thống mạng. Các bộ định tuyến này đều chứa những thông tin về mạng tương tự nhau và được bộ định tuyến tìm hiểu bằng cách gửi Link State Advertisement (LSA). Mọi thông tin về bộ định tuyến, mạng con và những thông tin khác đều được chứa trong LSA. Khi LSA đầy, OSPF sẽ thực hiện việc lưu trữ thông tin trong LSDB (cơ sở dữ liệu có trạng thái liên kết) một cách đồng nhất. [4]

1.3.2.1 Cách hoạt động của OSPF

Bước 1: Chọn Router ID: Để giao thức OSPF có thể hoạt động được thì người dùng phải tạo ra một định danh gọi là Router ID (Router tự tạo định danh, Người dùng tự cấu hình định danh).

Bước 2: Thiết lập mối quan hệ láng giềng: Hai router được xem là láng giềng nếu chúng đáp ứng được các điều kiện sau: Cùng Area – ID, Cùng Subnet, Cùng thông số (hello/dead), Cùng xác thực trên hai cổng.

Bước 3: Trao đổi LSDB: Với vai trò như tấm bản đồ, LSDB chính là căn cứ để Router tính toán định tuyến. Mỗi Router sẽ tiến hành giao tiếp và trao đổi với nhau theo từng đơn vị thông tin LSA.

Bước 4: Tính toán trong giao thức OSPF bằng định tuyến.

1.3.2.2 Ưu và nhược điểm của OSPF**Ưu điểm:**

- + Router có thể dễ dàng lựa chọn đường đi bằng cách sử dụng những thông tin mới nhất
- + Giao thức định tuyến OSPF có khả năng hỗ trợ CIDR và VLSM.
- + Mỗi Router sẽ đồng bộ về toàn bộ cấu trúc hệ thống mạng và một bộ hồ sơ đầy đủ nên chúng rất khó bị lặp vòng.

Nhược điểm:

- + OSPF tốn nhiều bộ nhớ và yêu cầu năng lực xử lý cao hơn nên chi phí đầu tư sẽ không phù hợp với các tổ chức nhỏ có thiết bị cũ hay chi phí hạn hẹp.
- + Hệ thống mạng phải chia thành nhiều vùng nhỏ để giảm độ phức tạp và độ lớn của cơ sở dữ liệu.
- + OSPF đòi hỏi người quản trị phải nắm rõ giao thức.

1.4. Tìm hiểu về IPSEC VPN**1.4.1. IPSEC**

IPSec (Internet Protocol Security) là một giao thức mạng được sử dụng rộng rãi để cung cấp một môi trường an toàn và bảo mật cho việc truyền thông tin qua mạng công cộng, như internet. IPSec được sử dụng phổ biến để thiết lập các kết nối VPN (Virtual Private Network) giữa hai hoặc nhiều vị trí mạng để bảo mật dữ liệu và truyền thông giữa chúng.

Mục tiêu chính của IPSec là bảo vệ dữ liệu thông qua hai tính năng cơ bản:

- Chứng thực (Authentication): IPSec xác minh tính xác thực của các thiết bị trong kết nối VPN để đảm bảo rằng chỉ các thiết bị được ủy quyền mới có thể tham gia vào kết nối. Điều này ngăn chặn các cuộc tấn công giả mạo.
- Mã hóa (Encryption): IPSec sử dụng mã hóa để mã hóa dữ liệu gửi qua mạng. Dữ liệu được mã hóa sẽ không thể đọc được khi bị gián đoạn trong quá trình truyền tải, bảo vệ dữ liệu khỏi việc bị đánh cắp hoặc lộ ra bên ngoài.

1.4.2. Thành phần của IPSEC

Các thành phần cơ bản của IPSec bao gồm:

- ESP (Encapsulating Security Payload): Thêm khả năng mã hóa và xác thực vào gói tin.
- AH (Authentication Header): Cung cấp khả năng xác thực và chứng thực cho gói tin nhưng không mã hóa dữ liệu.
- IKE (Internet Key Exchange): Để thiết lập các kết nối IPSec an toàn, cần có một cơ chế trao đổi khóa bí mật giữa các thiết bị. IKE đảm nhận vai trò này và được sử dụng để thiết lập các thông số bảo mật trước khi thiết lập kết nối IPSec.

IPSec VPN được sử dụng rộng rãi trong hội sở để bảo vệ dữ liệu và truyền thông giữa các vị trí mạng khác nhau, cho phép nhân viên từ xa truy cập vào tài nguyên công ty một cách an toàn và bảo mật. Ngoài ra, IPSec cũng có thể được triển khai trên các thiết bị cá nhân như máy tính hoặc điện thoại thông minh để bảo mật thông tin cá nhân khi kết nối với mạng công cộng. [5]

1.5. Firewall Cisco ASA

Cisco ASA (Adaptive Security Appliance) là một loạt các thiết bị tường lửa và VPN (Virtual Private Network) do hãng Cisco Systems sản xuất. ASA được sử dụng phổ biến trong các môi trường hội sở và tổ chức để cung cấp bảo mật mạng và bảo vệ dữ liệu khỏi các mối đe dọa từ bên ngoài.

Tầm quan trọng:

- ASA là một tường lửa mạnh mẽ, giúp kiểm soát và theo dõi lưu lượng mạng đi vào và ra khỏi mạng hội sở. Nó giám sát các gói tin và quyết định xem chúng có được phép truyền qua hay không, dựa trên các chính sách bảo mật được thiết lập trước.
- ASA hỗ trợ triển khai các kết nối VPN, cho phép người dùng từ xa kết nối vào mạng hội sở một cách an toàn và mã hóa. Điều này giúp nhân viên từ xa truy cập vào tài nguyên công ty và dữ liệu mà không cần phải truyền qua internet công cộng.
- Một số phiên bản ASA cung cấp tích hợp IPS (Intrusion Prevention System) và IDS (Intrusion Detection System). IPS giúp phát hiện và ngăn chặn các cuộc tấn công mạng tiềm ẩn, trong khi IDS cung cấp cảnh báo và giám sát các hoạt động đáng ngờ trên mạng.
- ASA hỗ trợ tích hợp nhiều dịch vụ bảo mật như antivirus, anti-spam, URL filtering và content filtering để giúp ngăn chặn các mối đe dọa từ các nội dung độc hại trên internet.
- Quản lý dễ dàng thông qua giao diện dòng lệnh (CLI) hoặc giao diện đồ họa (ASDM - Adaptive Security Device Manager). ASDM cung cấp giao diện đồ họa thân thiện hơn cho việc cấu hình và quản lý ASA.
- Chế độ hoạt động: ASA có thể hoạt động ở các chế độ khác nhau, bao gồm chế độ tường lửa, chế độ VPN, chế độ chuyển mạch và chế độ giám sát. ASA có thể triển khai như một tường lửa đơn lẻ hoặc là thành phần của một hệ thống bảo mật mạng. [6]

1.6. Anyconnect VPN

Cisco AnyConnect VPN là một giải pháp VPN (Virtual Private Network) của Cisco Systems, được sử dụng để cung cấp môi trường truyền thông an toàn và bảo mật cho việc truy cập mạng từ xa. AnyConnect VPN cho phép người dùng kết nối với mạng hội sở hoặc tổ chức từ bất kỳ địa điểm nào thông qua internet, đồng thời đảm bảo bảo mật dữ liệu và thông tin truyền qua kênh kết nối.

Cisco AnyConnect VPN hỗ trợ nhiều nền tảng, bao gồm Windows, macOS, Linux, iOS và Android. Điều này cho phép người dùng kết nối vào mạng từ các thiết bị di động và máy tính cá nhân.

AnyConnect Secure Mobility Client là tùy chọn máy khách Cisco được ưa chuộng. Nó được cập nhật liên tục và bao gồm hỗ trợ cho cả tùy chọn VPN IPsec và SSL. Các cấu hình AnyConnect được cấu hình ở phía máy chủ VPN và được triển khai cho máy khách, và máy khách AnyConnect cũng hỗ trợ IKEv2.0 và các tiêu chuẩn mã hóa cao cấp mới hơn của NSA Suite B. Việc lựa chọn loại mã hóa nào được hỗ trợ được cấu

hình cùng với cấu hình tại máy chủ VPN để mỗi máy khách có tùy chọn sử dụng nhiều giao thức VPN tùy thuộc vào kết nối máy khách cụ thể.

Ngoài việc hỗ trợ cả giao thức VPN SSL và IPsec, máy khách AnyConnect Secure Mobility còn hỗ trợ một số mô-đun khác nhau giúp mở rộng khả năng của nó. Các mô-đun này bao gồm AnyConnect VPN, AnyConnect VPN Start Before Login, AnyConnect Diagnostic and Reporting Tool, AnyConnect Network Access Manager, AnyConnect Posture, AnyConnect Telemetry và AnyConnect Web Security. [7]

An toàn và mã hóa: AnyConnect VPN sử dụng nhiều lớp bảo mật và giao thức mã hóa mạnh mẽ để đảm bảo tính bảo mật của dữ liệu khi được truyền qua mạng công cộng. Các giao thức bảo mật thông thường bao gồm IPsec, SSL (Secure Sockets Layer) và DTLS (Datagram Transport Layer Security)

Tính năng	Mô tả
Tuân thủ điểm cuối hợp nhất (Unified Endpoint Compliance)	Cisco AnyConnect ISE Agent cung cấp khả năng kiểm tra tư thế (posture) và khắc phục sự cố của điểm cuối một cách hợp nhất cho Cisco ISE trên môi trường có dây, không dây và VPN. Đây là nguồn chính để kiểm tra posture của điểm cuối, bao gồm phiên bản hệ điều hành, bản cập nhật mới nhất của phần mềm diệt virus và các tài nguyên khác nhằm tăng cường bảo mật và tuân thủ. Ngoài ra, posture endpoint cũng có thể được cung cấp thông qua Cisco Hostscan với ASA.
Truy cập mạng an toàn cao (Highly Secure Network Access)	Cisco AnyConnect Network Access Manager cung cấp các tính năng kết nối tiên tiến, cho phép quản trị viên kiểm soát mạng hoặc tài nguyên mà thiết bị đầu cuối được phép truy cập. Nó cung cấp IEEE 802.1X được cấu hình như một phần của xác thực, phân quyền và ghi log (AAA), đồng thời hỗ trợ các công nghệ mã hóa độc đáo như MACsec IEEE 802.1AE.
Bảo mật web (Web Security)	Cisco AnyConnect tích hợp mô-đun bảo mật web, hoạt động thông qua Cisco Web Security Appliance (WSA) tại chỗ hoặc dịch vụ Cisco Cloud Web Security (CWS) trên nền tảng đám mây. Việc kết hợp bảo mật web với truy cập VPN cho phép quản trị viên cung cấp khả năng di động an toàn toàn diện cho tất cả người dùng, đặc biệt hữu ích trong triển khai BYOD. Doanh nghiệp có thể lựa chọn phương án triển khai để bảo vệ mạng trước phần mềm độc hại từ web và kiểm soát, bảo mật việc sử dụng web.

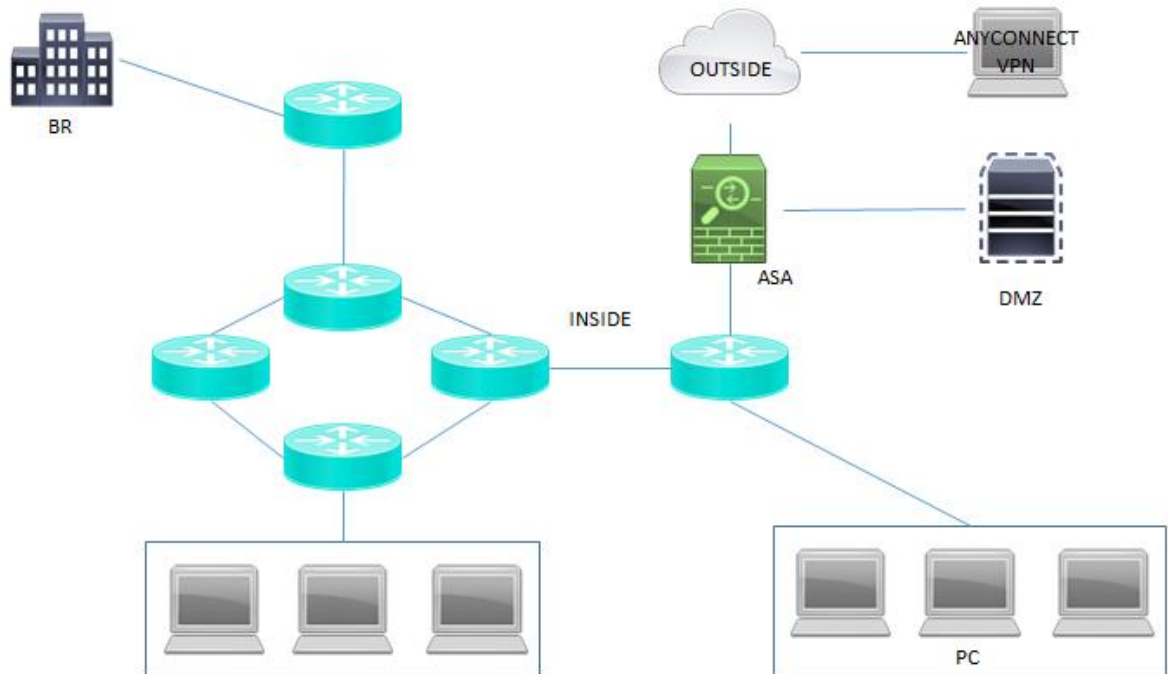
Truy cập không cần cài đặt client (Clientless Access)	Cisco ASA cung cấp kết nối SSL qua nhiều trình duyệt trên nhiều nền tảng khác nhau. ASA cho phép quản trị viên cung cấp VPN không cần cài client cho các thiết bị không được quản lý và truy cập vào các ứng dụng web hoặc TCP/IP. Điều này được thực hiện qua công nghệ rewriter, plugin hoặc smart tunnel dựa trên SSL nhúng trong trình duyệt, đồng thời áp dụng kiểm soát truy cập chi tiết và bảo mật đầu-cuối.
Truy cập hạ tầng máy tính để bàn ảo (VDI) (Virtual Desktop Infrastructure Access)	Cisco ASA có thể kết thúc phiên VDI với mức độ bảo mật cao, cung cấp truy cập minh bạch đến các ứng dụng và desktop ảo. Hỗ trợ cả truy cập qua client và không cần client cho thiết bị di động, laptop, và máy tính để bàn. Việc truy cập tài nguyên ảo có tính bảo mật cao, không phụ thuộc nhà cung cấp và hưởng lợi từ chính sách truy cập thống nhất cho cả tài nguyên ảo và truyền thống.
Hỗ trợ thiết bị di động (Mobile Device Support)	Với xu hướng BYOD, quản trị viên cần hỗ trợ năng suất của người dùng bằng cách cho phép sử dụng thiết bị cá nhân để truy cập từ xa vào mạng công ty. Cisco AnyConnect có thể triển khai trên hầu hết các thiết bị phổ biến hiện nay. Truy cập từ xa bảo mật cao có thể được áp dụng cho toàn bộ thiết bị hoặc theo ứng dụng doanh nghiệp chọn lọc với VPN theo ứng dụng. Chức năng VPN theo ứng dụng giúp ngăn các ứng dụng không được phép truy cập tài nguyên bảo mật, giảm rủi ro phần mềm độc hại và chi phí băng thông cho truy cập từ xa.

BẢNG 2: Bảng Các tính năng của giải pháp di động an toàn Cisco AnyConnect

CHƯƠNG 2. ĐỀ XUẤT MÔ HÌNH BẢO MẬT CHO HỆ THỐNG MẠNG LỖI NGÂN HÀNG

2.1. Đề xuất mô hình

2.1.1. Mô hình tổng quát



HÌNH 2.1 Mô hình tổng quát

2.1.2. Mô hình bao gồm

- Vùng chi nhánh (BR):
 - Đại diện cho một văn phòng chi nhánh cần kết nối bảo mật về trụ sở chính (qua GW1 hoặc GW2).
 - Cung cấp DHCP cho máy trạm ở chi nhánh.
 - Tất cả lưu lượng đi về trung tâm được mã hóa bằng IPsec.
- Vùng chính (CORE - Mạng nội bộ trung tâm)
 - Đóng vai trò xương sống mạng nội bộ của trụ sở chính.
 - Chạy OSPF để định tuyến giữa các vùng LAN, DMZ, và VPN.
 - CORE1 nối với GW1 và GW2 để nhận route từ chi nhánh.
 - CORE2 nối với ASA inside và LAN nội bộ.
- Vùng DMZ (Demilitarized Zone):
 - Lưu trữ các dịch vụ công khai hoặc bán công khai (web server, mail server, ứng dụng).
 - Cho phép truy cập từ VPN client (AnyConnect) hoặc từ mạng nội bộ, nhưng được tách biệt khỏi inside để tăng bảo mật.

- Outside:
 - Nơi VPN AnyConnect client kết nối vào.
 - Nhận lưu lượng từ bên ngoài vào ASA.
 - Đây là vùng “không tin cậy” – bảo mật thấp nhất.
 - Chỉ cho phép các dịch vụ, port được ACL/NAT cho phép

2.1.3. Giải thích yêu cầu mô hình

- Cấu hình ban đầu: cấu hình địa chỉ IP theo bảng thành phần
- VPN:
 - ✓ Cấu hình IPSEC VPN từ BR về GW1 làm đường kết nối VPN chính.
 - ✓ Cấu hình IPSEC VPN từ BR về GW2 làm đường kết nối VPN dự phòng.
 - ✓ Cấu hình Anyconnect VPN từ Laptop về Firewall ASA.
- Firewall ASA
 - ✓ Cấu hình 3 Zone trên ASA Firewall lần lượt (Inside, Outside, DMZ).
 - ✓ Đảm bảo tất cả người dùng trên các site có thể truy cập ASA.
 - ✓ Cho phép người dùng Anyconnect có thể truy cập dịch vụ trong DMZ.

2.2. Nền tảng xác thực

2.2.1. Nền tảng xác thực tracer

Traceroute là một công cụ trong mạng được sử dụng để theo dõi quá trình một gói dữ liệu đi từ máy tính nguồn đến máy tính đích thông qua các nút mạng trung gian. Traceroute giúp biết được đường đi mà gói dữ liệu sẽ đi qua trên mạng, cũng như thời gian mà gói dữ liệu mất để đi qua từng nút mạng.

Khi chạy một lệnh traceroute, nó sẽ gửi ra một loạt các gói dữ liệu có giá trị TTL (Time to Live) khác nhau. TTL là số lượng các nút mạng mà gói dữ liệu được phép đi qua trước khi bị loại bỏ. Khi gói dữ liệu đi qua mỗi nút mạng, giá trị TTL sẽ giảm đi 1 và nút mạng đó sẽ gửi lại một thông báo báo lỗi (ICMP Time Exceeded) cho máy tính nguồn. Dựa trên các thông báo này, traceroute xây dựng một báo cáo hiển thị các nút mạng mà gói dữ liệu đã đi qua và thời gian mà gói mất để đi qua từng nút.

Kết quả của lệnh traceroute thường bao gồm danh sách các nút mạng (hoặc địa chỉ IP) mà gói dữ liệu đã đi qua và thời gian mà gói mất để đi qua từng nút. Điều này giúp hiểu rõ hơn về đường đi của dữ liệu trên mạng và xác định được điểm nào có thể gây trễ hay vấn đề trong kết nối mạng.

2.2.2. Các giao thức xác thực

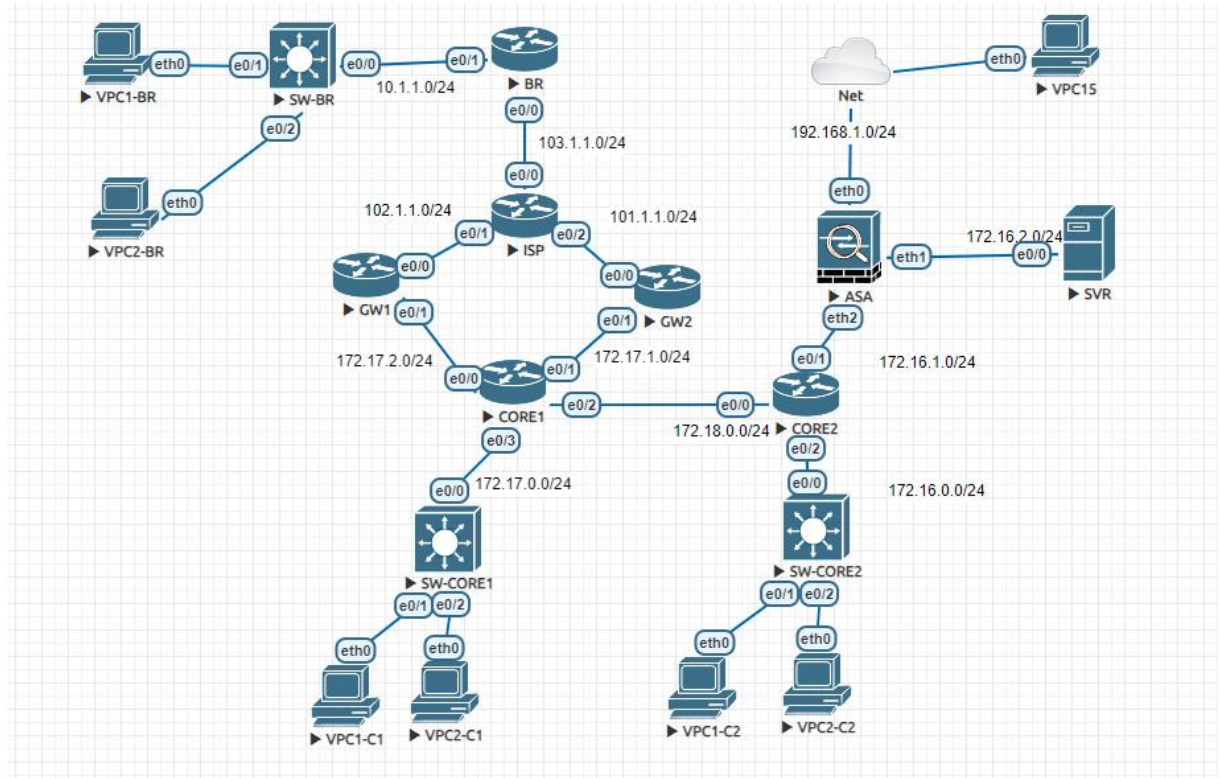
Các giao thức sử dụng trong báo cáo

- Giao thức DHCP
- Giao thức OSPF
- Giao thức IPSEC
- Giao thức Anyconnect VPN

CHƯƠNG 3. TRIỂN KHAI THỰC NGHIỆM VÀ ĐÁNH GIÁ KẾT QUẢ

3.1. Triển khai thực nghiệm

3.1.1. Thiết lập mô hình



HÌNH 3.1 Mô hình triển khai

3.1.2. Bảng thành phần

STT	Server name	IP	Subnet
1	VPC	DHCP	/24
2	Router BR	E0/0: 103.1.1.254 E0/1: 10.1.1.254	/24
3	Router ISP	E0/0: 103.1.1.1 E0/1: 102.1.1.1 E0/2: 101.1.1.1	/24
4	Router GW1	E0/0: 102.1.1.254 E0/1: 172.17.2.254	/24
5	Router GW2	E0/0: 101.1.1.254 E0/1: 172.17.1.254	/24
6	Router CORE1	E0/0: 172.17.2.1 E0/1: 172.17.1.1 E0/2: 172.18.0.1 E0/3: 172.17.0.1	/24

7	Router CORE2	E0/0: 172.18.0.254 E0/1: 172.16.1.254 E0/2: 172.16.0.254	/24
8	SVR	E0/0: 172.16.2.200	/24
9	ASA	Eth0: 192.168.1.10 Eth1: 172.16.2.1 Eth2: 172.16.1.1	/24
10	Tunnel0	10.0.0.2	/30
11	Tunnel20	10.0.1.2	/30

BẢNG 3: Bảng IP và subnet cho các thành phần trong mạng

3.2. Cài đặt và cấu hình

3.2.1. Cài đặt các máy ảo

- Cấu hình chung: cài đặt IP theo bảng thành phần ở phần 3.1.2.
- Cấu hình nâng cao:
 - Router: Cấu hình DHCP, OSPF, IPSEC VPN.
 - ASA: Cấu hình Zone, Anyconnect VPN.
 - Server: Routing

• 3.2.2. Cấu hình

3.2.2.1. Cấu hình IP

```
Router(config)# interface [ethernet 0/x]
Router(config-if)# ip address [ip address][subness mask]
Router(config-if)# no shutdown
```

3.2.2.2. Cấu hình DHCP

- Cấu hình DHCP Server


```
Router(config)# ip dhcp pool [pool name]
Router(config-dhcp)# network [network address] [subnet mask]
Router(config-dhcp)# default-router [host address]
Router(config-dhcp)# dns-server [dns server address]
```

- Cấu hình DHCP Client

```
Router(config-if)# ip address dhcp
```

3.2.2.3. Cấu hình routing

```
Router(config)# ip route network [mask] {address | interface} [distance]
[permanent]
```

3.2.2.4. Cấu hình OSPF

```
Router(config)# router ospf process-id
```

```
Router(config-router)# network address wildcard-mask area area-id
```

3.2.2.5. Cấu hình IPSEC VPN

▪ **Thiết lập VPN Tunnel**

```
Router(config)# interface Tunnel10
```

```
Router(config-if)# ip address 10.0.0.1 255.255.255.252
```

```
Router(config-if)# tunnel source 102.1.1.254
```

```
Router(config-if)# tunnel mode ipsec ipv4
```

```
Router(config-if)# tunnel destination 103.1.1.254
```

```
Router(config-if)# tunnel protection ipsec profile MYPROFILE
```

▪ **Cấu hình IPSEC Profile**

```
Router(config)# crypto isakmp policy 10
```

```
Router(config-isakmp)# authentication pre-share
```

```
Router(config-isakmp)# group 2
```

```
Router(config)# crypto isakmp key TEST address 101.1.1.254
```

```
Router(config)# crypto ipsec transform-set MYSET esp-des esp-sha-hmac
```

```
Router(config-crypto-trans)# mode tunnel
```

```
Router(config)# crypto ipsec profile MYPROFILE
```

```
Router(ipsec-profile)# set transform-set MYSET
```

3.2.2.6. Cấu hình ASA

▪ **Cấu hình Zone Outside**

```
ciscoasa(config)# interface Ethernet0
```

```
ciscoasa(config-if)# nameif outside
```

```
ciscoasa(config-if)# security-level 0
```

```
ciscoasa(config-if)# ip address 192.168.1.10 255.255.255.0
```

▪ **Cấu hình Zone DMZ**

```
ciscoasa(config)# interface Ethernet1
```

```
ciscoasa(config-if)# nameif dmz
```

```
ciscoasa(config-if)# security-level 50
```

```
ciscoasa(config-if)# ip address 172.16.2.1 255.255.255.0
```

▪ **Cấu hình Zone Inside**

```
ciscoasa(config)# interface Ethernet2
```

```
ciscoasa(config-if)# nameif inside
```

```
ciscoasa(config-if)# security-level 100
```

```
ciscoasa(config-if)# ip address 172.16.1.1 255.255.255.0
```

- **Cấu hình chính sách cho phép icmp**

```
ciscoasa(config)# policy-map global_policy
```

```
ciscoasa(config-pmap)# class inspection_default
```

```
ciscoasa(config-pmap-c)# inspect icmp
```

- **Định nghĩa object network để NAT hoạt động**

```
ciscoasa(config)# object network [network object name]
```

```
ciscoasa(config-network-object)# subnet [network address] [subnet mask]
```

- **Static routes trên ASA**

```
ciscoasa(config)# route [zone asa name] [address] [subnet mask] [gateway]
```

- **Tạo HTTP Server**

```
ciscoasa(config)# http server enable
```

```
ciscoasa(config)# http [network address] [subnet mask] outside
```

3.2.2.7. Cấu hình AnyConnect VPN

- **Tạo pool địa chỉ cấp cho VPN client**

```
ciscoasa(config)# ip local pool VPNPOOL [address begin]-[address end] mask [subnet mask]
```

- **Cấu hình webvpn**

- **Enable webvpn trên cổng outside của ASA**

```
ciscoasa(config)# webvpn
```

```
ciscoasa(config-webvpn)# enable outside
```

- **Khai báo disk**

```
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-4..5.04029-webdeploy-k9.pkg 1
```

- **Cho phép anyconnect và essentials**

```
ciscoasa(config-webvpn)# anyconnect enable
```

- **Cấu hình nhiều group khi người dùng đăng nhập vào như sau**

```
ciscoasa(config-webvpn)# tunnel-group-list enable
```

```
ciscoasa(config-webvpn)# anyconnect-essentials
```

- **Tạo ACL cho Split Tunnel**

```
ciscoasa(config)# access-list SPLIT-TUNNEL-LIST standard permit [network address] [subnet mask]
```

- **Tạo tên Group Policy muốn áp cho client**

```
ciscoasa(config)# group-policy ANYCONNECT_POLICY internal
```

- **Gán các thuộc tính cho group vừa tạo**

```
ciscoasa(config)# group-policy ANYCONNECT_POLICY attributes
```

- **Chọn giao thức mà VPN được hỗ trợ cho group**

```
ciscoasa(config-group-policy)# vpn-tunnel-protocol ssl-client ssl-clientless
```

- **Cấu hình tính năng split-tunnel**

```
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
```

- **Access list cho phép client VPN được phép truy cập những nơi nào**

```
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT-TUNNEL-LIST
```

- **DNS Server cho group**

```
ciscoasa(config-group-policy)# dns-server value 8.8.8.8
```

- **Add pool dhcp cấp cho VPN client**

```
ciscoasa(config-group-policy)# address-pools value VPNPOOL
```

- **Định nghĩa Connect Profile**

```
ciscoasa(config-group-webvpn)# tunnel-group ANYCONNECT type remote-access
```

- **Cấu hình thuộc tính cho Connect profile ANYCONNECT_POLICY bao gồm các chính sách trong Group Policy**

```
ciscoasa(config)# tunnel-group ANYCONNECT general-attributes
```

```
ciscoasa(config-tunnel-general)# default-group-policy
```

```
ANYCONNECT_POLICY
```

```
ciscoasa(config-tunnel-general)# address-pool VPNPOOL
```

```
ciscoasa(config-tunnel-general)# authentication-server-group LOCAL
```

- **Kết hợp Group-Alias và Group-list lại với nhau**

```
ciscoasa(config)# tunnel-group ANYCONNECT webvpn-attributes
```

```
ciscoasa(config-tunnel-webvpn)# group-alias RemoteVPN enable
```

- **Tạo user để client connect vào**

```
ciscoasa(config)# username vpnuser password 123456 privilege 15
```

```
ciscoasa(config)# username vpnuser attributes
```

```
ciscoasa(config-username)# service-type remote-access
```

- **NAT cho VPN client truy cập DMZ**

```
ciscoasa(config)# nat (outside,outside) source dynamic VPNPOOL interface
```

- **NAT cho inside truy cập DMZ**

```
ciscoasa(config)# nat (inside,dmz) source static any any destination  
static DMZPOOL DMZPOOL no-proxy-arp
```

- **ACL (Access Control List)**

```
ciscoasa(config)# access-list [ACL name] extended permit ip [source  
address] [subnet mask] [destination address] [subnet mask]
```

```
ciscoasa(config)# access-group [ACL name] in interface [zone asa  
name]
```

3.3. Đánh giá kết quả

3.3.1. Kết quả cấu hình

3.3.1.1. Kết quả cấu hình địa chỉ IP

- Cấu hình địa chỉ IP cho các cổng trên Router BR. Cổng Ethernet 0/1 kết nối với ISP. Cổng Ethernet0/2 nối với mạng LAN của chi nhánh.

```
interface Ethernet0/0  
no shutdown  
ip address 103.1.1.254 255.255.255.0  
duplex auto  
!  
interface Ethernet0/1  
no shutdown  
ip address 10.1.1.254 255.255.255.0  
duplex auto  
!
```

HÌNH 3.2 Cấu hình Router BR

- Cấu hình địa chỉ IP của Router ISP. Cổng Ethernet0/1 nối trực tiếp tới router BR. Các cổng Ethernet0/1 và 0/2 kết nối tương ứng với router GW1 và GW2.

```
interface Ethernet0/0
no shutdown
ip address 103.1.1.1 255.255.255.0
duplex auto
!
interface Ethernet0/1
no shutdown
ip address 102.1.1.1 255.255.255.0
duplex auto
!
interface Ethernet0/2
no shutdown
ip address 101.1.1.1 255.255.255.0
shutdown
duplex auto
```

HÌNH 3.3 Cấu hình Router ISP

- Cấu hình địa chỉ IP Router GW1. Cổng Ethernet0/0 kết nối trở lại tới ISP. Ethernet0/1 kết nối với router CORE1 hình thành liên kết tới hội sở trung tâm.

```
interface Ethernet0/0
no shutdown
ip address 102.1.1.254 255.255.255.0
duplex auto
!
interface Ethernet0/1
no shutdown
ip address 172.17.2.254 255.255.255.0
duplex auto
!
```

HÌNH 3.4 Cấu hình Router GW1

- Cấu hình địa chỉ IP Router GW2. Cổng Ethernet0/0 cũng kết nối trở lại ISP. Còn Ethernet0/1 cũng kết nối tới router CORE1 đóng vai trò là đường truyền dự phòng.

```
interface Ethernet0/0
no shutdown
ip address 101.1.1.254 255.255.255.0
duplex auto
!
interface Ethernet0/1
no shutdown
ip address 172.17.1.254 255.255.255.0
duplex auto
```

HÌNH 3.5 Cấu hình GW2

- Cấu hình địa chỉ IP Router CORE1. Đóng vai trò là lõi của hội sở, Ethernet0/0 và Ethernet0/1 kết nối với GW1 và GW2. Ethernet0/2 kết nối với CORE2 là lõi thứ hai của hội sở. Ethernet0/3 kết nối mạng LAN của chính nó.

```
!
interface Ethernet0/0
no shutdown
ip address 172.17.2.1 255.255.255.0
duplex auto
!
interface Ethernet0/1
no shutdown
ip address 172.17.1.1 255.255.255.0
duplex auto
!
interface Ethernet0/2
no shutdown
ip address 172.18.0.1 255.255.255.0
duplex auto
!
interface Ethernet0/3
no shutdown
ip address 172.17.0.1 255.255.255.0
duplex auto
!
```

HÌNH 3.6 Cấu hình Router CORE1

- Cấu hình địa chỉ IP Router CORE2. Cũng giống như CORE1 là lõi của hội sở ngân hàng, có Ethernet0/0 kết nối với CORE1. Ethernet0/1 kết nối với firewall ASA và Ethernet0/2 kết nối mạng LAN của chính nó.

```
interface Ethernet0/0
no shutdown
ip address 172.18.0.254 255.255.255.0
duplex auto
!
interface Ethernet0/1
no shutdown
ip address 172.16.1.254 255.255.255.0
duplex auto
!
interface Ethernet0/2
no shutdown
ip address 172.16.0.254 255.255.255.0
duplex auto
```

HÌNH 3.7 Cấu hình Router CORE2

3.3.1.2. Kết quả cấu hình DHCP

- Cấu hình DHCP Server trên Router BR

```
ip dhcp pool LAN-BR
network 10.1.1.0 255.255.255.0
default-router 10.1.1.254
dns-server 8.8.8.8
```

HÌNH 3.8 DHCP Server trên Router BR

- Cấu hình DHCP Server trên Router CORE1

```
ip dhcp pool LAN-C1
network 172.17.0.0 255.255.255.0
default-router 172.17.0.1
dns-server 8.8.8.8
```

HÌNH 3.9 DHCP Server trên Router CORE1

- Cấu hình DHCP Server trên Router CORE2

```
ip dhcp pool LAN-C2
network 172.16.0.0 255.255.255.0
default-router 172.16.0.254
dns-server 8.8.8.8
```

HÌNH 3.10 Cấu hình DHCP Server trên Router CORE2

3.3.1.3. Kết quả cấu hình IPSEC

- Cấu hình IPSEC Profile trên Router BR. Bao gồm isakmp là hai bên xác thực nhau và tạo kênh bảo mật ban đầu. Và ipsec hai bên dùng kênh bảo mật đã thiết lập để trao đổi dữ liệu. Cuối cùng tạo profile với transform-set.

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
crypto isakmp key VPNKEY address 102.1.1.254
crypto isakmp key VPNKEY2 address 101.1.1.254
!
!
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
  mode tunnel
!
crypto ipsec profile MYPROFILE
  set transform-set MYSET
!
crypto ipsec profile MYPROFILE2
  set transform-set MYSET
!
```

HÌNH 3.11 Cấu hình IPSEC Profile trên Router BR

- Tạo hai Tunnel10 làm đường chính gắn với GW1 và Tunnel20 làm đường dự phòng gắn với GW2. Các thông số bao gồm IP, địa chỉ nguồn, địa chỉ đích, mode ipv4. Và thêm chính sách IPSEC vừa tạo phía trên.

```
interface Tunnel10
  no shutdown
  ip address 10.0.0.2 255.255.255.252
  ip ospf cost 10
  tunnel source 103.1.1.254
  tunnel mode ipsec ipv4
  tunnel destination 102.1.1.254
  tunnel protection ipsec profile MYPROFILE
!
interface Tunnel20
  no shutdown
  ip address 10.0.1.2 255.255.255.252
  ip ospf cost 100
  tunnel source 103.1.1.254
  tunnel mode ipsec ipv4
  tunnel destination 101.1.1.254
  tunnel protection ipsec profile MYPROFILE2
!
```

HÌNH 3.12 Cấu hình Tunnel10 và Tunnel20

- Cấu hình IPSEC Profile trên Router GW1. Cũng tương tự như trên BR, GW1 cũng tạo profile cho ipsec nhưng cần lưu ý đến địa chỉ. Và khóa và tên profile phải trùng với tên profile gắn vào Tunnel10 trên BR.

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
crypto isakmp key VPNKEY address 103.1.1.254
!
!
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
  mode tunnel
!
crypto ipsec profile MYPROFILE
  set transform-set MYSET
!
```

HÌNH 3.13 Cấu hình IPSEC trên Router GW1

- Tạo Tunnel10 tương tự với Tunnel10 trên BR. Và quan trọng là địa chỉ đích và địa chỉ nguồn phải trái ngược với trên BR. Cuối cùng gắn profile đã tạo vào Tunnel10.

```
interface Tunnel10
no shutdown
ip address 10.0.0.1 255.255.255.252
ip ospf cost 10
tunnel source 102.1.1.254
tunnel mode ipsec ipv4
tunnel destination 103.1.1.254
tunnel protection ipsec profile MYPROFILE
!
```

HÌNH 3.14 Cấu hình Tunnel10

- Cấu hình IPSEC Profile tương tự trên Router GW2. Cũng tương tự như trên GW1, GW2 cũng tạo profile cho ipsec nhưng cũng cần lưu ý đến địa chỉ. Và khóa và tên profile cũng phải trùng với tên profile gắn vào Tunnel20 trên BR

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key VPNKEY2 address 103.1.1.254
!
!
crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
mode tunnel
!
crypto ipsec profile MYPROFILE2
set transform-set MYSET
!
```

HÌNH 3.15 Cấu hình IPSEC Profile cho Router GW2

- Cấu hình Tunnel20 tương tự với Tunnel20 trên BR. Nhưng với địa chỉ nguồn và địa chỉ đích cũng trái ngược với Tunnel20 trên BR. Và cũng gắn profile đã tạo vào Tunnel20.

```
interface Tunnel20
no shutdown
ip address 10.0.1.1 255.255.255.252
ip ospf cost 100
tunnel source 101.1.1.254
tunnel mode ipsec ipv4
tunnel destination 103.1.1.254
tunnel protection ipsec profile MYPROFILE2
!
```

HÌNH 3.16 Cấu hình Tunnel20

3.3.1.4. Kết quả cấu hình định tuyến routing

- Cấu hình định tuyến static route để BR reach IP public của GW1 và GW2. BR muốn tạo VPN tới GW1 và GW2, nên phải biết đường đi đến IP public của chúng. Mục đích của định tuyến tĩnh này là khi BR gửi gói tin IKE/IPsec để thiết lập VPN, gói tin phải đi qua ISP và đến đúng GW1 hoặc GW2. Nếu không có route này, BR sẽ không biết gửi mấy gói handshake VPN đi đâu.

```
no ip http server
no ip http secure-server
ip route 101.1.1.254 255.255.255.255 103.1.1.1
ip route 102.1.1.254 255.255.255.255 103.1.1.1
!
```

HÌNH 3.17 Cấu hình định tuyến BR

- Cấu hình định tuyến static route để GW1 trả lời BR. Nếu không có route này, khi BR gửi gói tin VPN đến, GW1 sẽ nhận được, nhưng khi gửi trả lời, GW1 không biết đường quay về mạng → VPN sẽ không hoàn tất.

```
no ip http server
no ip http secure-server
ip route 103.1.1.0 255.255.255.0 102.1.1.1
!
```

HÌNH 3.18 Cấu hình định tuyến GW1

- Cấu hình định tuyến static route để GW2 reach BR public. Cũng tương tự khi static route để GW2 trả lời BR. Nếu không có route này GW2 không biết đường quay về.

```
no ip http server
no ip http secure-server
ip route 103.1.1.0 255.255.255.0 101.1.1.1
!
```

HÌNH 3.19 Cấu hình định tuyến GW2

- Cấu hình định tuyến trên GW1, GW2, CORE1, CORE2. Mục đích là để các mạng của router này biết đường đi đến vùng dmz. Là một phần quan trọng để các máy trong inside có thể truy cập dmz.

```
ip route 172.16.2.0 255.255.255.0 172.16.1.1
!
```

Hình 3.20 Cấu hình định tuyến tới DMZ

- Cấu hình định tuyến Tunnel10 và Tunnel20 đi qua ISP và đích đến là GW1 và GW2. Mục đích của định tuyến này là khi gói tin có đích đến là 10.0.0.0 nó sẽ qua GW1. Tương tự khi có gói tin có đích đến là 10.0.1.0 nó sẽ qua GW2.

```
no ip http server
no ip http secure-server
ip route 10.0.0.0 255.255.255.252 102.1.1.254
ip route 10.0.1.0 255.255.255.252 101.1.1.254
!
```

HÌNH 3.21 Định tuyến Tunnel10 và Tunnel20

3.3.1.5. Kết quả cấu hình OSPF

- Cấu hình OSPF trên BR bao gồm ospf hai Tunnel là 10 và 20 cộng thêm mạng LAN chi nhánh.

```
router ospf 1
network 10.0.0.0 0.0.0.3 area 0
network 10.0.1.0 0.0.0.3 area 0
network 10.1.1.0 0.0.0.255 area 0
!
```

HÌNH 3.22 Cấu hình OSPF trên BR

- Cấu hình OSPF trên GW1 (Một đường Tunnel10 và một đường kết nối với CORE1)

```
router ospf 1
 network 10.0.0.0 0.0.0.3 area 0
 network 172.17.2.0 0.0.0.255 area 0
!
```

HÌNH 3.23 Cấu hình OSPF trên GW1

- Cấu hình tương tự với GW2 (Một đường Tunnel20 và một đường kết nối với CORE1)

```
router ospf 1
 network 10.0.1.0 0.0.0.3 area 0
 network 172.17.1.0 0.0.0.255 area 0
!
```

HÌNH 3.24 Cấu hình OSPF trên GW2

- Cấu hình OSPF trên Router CORE 1

```
router ospf 1
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.1.0 0.0.0.3 area 0
 network 172.17.0.0 0.0.255.255 area 0
 network 172.18.0.0 0.0.255.255 area 0
!
```

HÌNH 3.25 Cấu hình OSPF trên Router CORE1

- Cấu hình OSPF trên Router CORE 2

```
router ospf 1
 network 172.16.0.0 0.0.255.255 area 0
!
```

HÌNH 3.26 Cấu hình OSPF trên Router CORE2

3.3.1.6. Kết quả cấu hình Anyconnect

- Cấu hình 3 Zone trên ASA
 - Zone Outside dùng để kết nối tới Internet bên ngoài
 - Zone DMZ là vùng chứa các Server
 - Zone Inside chứa các máy nội bộ bao gồm các CORE


```

interface Ethernet0
  nameif outside
  security-level 0
  ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1
  nameif dmz
  security-level 50
  ip address 172.16.2.1 255.255.255.0
!
interface Ethernet2
  nameif inside
  security-level 100
  ip address 172.16.1.1 255.255.255.0
!

```

HÌNH 3.27 Cấu hình 3 Zone ASA

- Cấu hình định tuyến trên ASA. Định tuyến ra outside tất cả các dây mạng với next-hop là dây mạng outside. Định tuyến inside tới tất cả các mạng LAN và mạng trung gian với next-hop là dây mạng inside của ASA.

```

route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
route inside 10.1.1.0 255.255.255.0 172.16.1.254 1
route inside 172.16.0.0 255.255.255.0 172.16.1.254 1
route inside 172.17.0.0 255.255.0.0 172.16.1.254 1
route inside 172.18.0.0 255.255.255.0 172.16.1.254 1

```

HÌNH 3.28 Cấu hình định tuyến trên ASA

- ACL (Access Control List) cho phép các máy trong Inside truy cập DMZ. Giới hạn truy nhập với các mạng trong inside và Tunnel. Giúp hạn chế truy nhập và quản lý truy nhập.

```

access-list INSIDE extended permit ip 172.17.0.0 255.255.0.0 172.16.2.0 255.255.255.0
access-list INSIDE extended permit ip 172.18.0.0 255.255.255.0 172.16.2.0 255.255.255.0
access-list INSIDE extended permit ip 172.16.1.0 255.255.255.0 172.16.2.0 255.255.255.0
access-list INSIDE extended permit ip 172.16.0.0 255.255.255.0 172.16.2.0 255.255.255.0
access-list INSIDE extended permit ip 10.1.1.0 255.255.255.0 172.16.2.0 255.255.255.0
access-list INSIDE extended permit ip 10.0.0.0 255.255.255.252 172.16.2.0 255.255.255.0
access-list INSIDE extended permit ip 10.0.1.0 255.255.255.252 172.16.2.0 255.255.255.0

```

HÌNH 3.29 Cấu hình ACL Inside

- Cấu hình Anyconnect VPN

- Tạo pool địa chỉ cấp cho VPN client. Khi client sử dụng AnyConnect để kết nối thì sẽ được cấp dãy ip từ 192.168.100.10 đến 192.168.100.50. Và đặt tên là VPNPOOL.

```
ip local pool VPNPOOL 192.168.100.10-192.168.100.50 mask 255.255.255.0
```

HÌNH 3.30 Pool địa chỉ cho VPN Client

- Tạo user để xác thực VPN. User này sẽ do quản trị viên tạo với username là vpnuser, password sẽ được mã hóa và với quyền 15. Cài đặt dịch vụ là truy cập từ xa.

```
username vpnuser password F9udxVdK8y0dCLcd encrypted privilege 15
username vpnuser attributes
service-type remote-access
```

HÌNH 3.31 Tạo user

- Tạo một group-policy tên ANYCONNECT_POLICY là bộ quy tắc áp dụng cho người dùng VPN. Các quy tắc bao gồm: cho phép kết nối VPN qua Cisco AnyConnect Client và qua web browser, chỉ định chế độ Split Tunnel — chỉ những mạng được chỉ định mới đi qua VPN, còn lại đi Internet trực tiếp. Khi kết nối thì cấp DNS server là 8.8.8.8 và pool client như trên.

```
group-policy ANYCONNECT_POLICY internal
group-policy ANYCONNECT_POLICY attributes
  dns-server value 8.8.8.8
  vpn-tunnel-protocol ssl-client ssl-clientless
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT-TUNNEL-LIST
  address-pools value VPNPOOL
```

HÌNH 3.32 Tạo group-policy

- Tạo ACL cho Split Tunnel. Chỉ route mạng DMZ qua VPN, còn Internet client truy cập trực tiếp (split tunnel). Giúp giảm tải VPN, tăng tốc truy cập, chỉ bắt buộc encrypt các mạng nội bộ.

```
access-list SPLIT-TUNNEL-LIST standard permit 172.16.2.0 255.255.255.0
```

HÌNH 3.33 Tạo ACL cho Split Tunnel

- Tạo tunnel-group loại truy cập từ xa cho AnyConnect VPN. Gắn chính sách vừa tạo vào tunnel-group. Tạo group truy cập là RemoteVPN.

```
tunnel-group ANYCONNECT type remote-access
tunnel-group ANYCONNECT general-attributes
  address-pool VPNPOOL
  default-group-policy ANYCONNECT_POLICY
tunnel-group ANYCONNECT webvpn-attributes
  group-alias RemoteVPN enable
!
```

HÌNH 3.34 Tạo Tunnel-group

- Bật webvpn và kích hoạt AnyConnect. Webvpn sẽ cho phép truy cập ASA từ outside. Cho phép tải xuống AnyConnect 4.5. Và Cho phép anyconnect từ web browser cùng với tunnel-group-list.

```
webvpn
  enable outside
  anyconnect-essentials
  anyconnect image disk0:/anyconnect-win-4.5.04029-webdeploy-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
```

HÌNH 3.35 Bật webvpn và kích hoạt AnyConnect

- Tạo Object network. Bao gồm hai object network là VPNPOOL và DMZPOOL. Định nghĩa dãy mạng anyconnect client cấp phát và dãy mạng trong dmz.

```
object network VPNPOOL
  subnet 192.168.100.0 255.255.255.0
object network DMZPOOL
  subnet 172.16.2.0 255.255.255.0
```

HÌNH 3.36 Tạo Object network

- NAT cho VPN client. Tạo NAT cho người dùng kết nối bằng anyconnect từ zone outside sang outside. Giúp VPN client có thể truy cập ra Internet thông qua ASA outside.

```
nat (outside,outside) source dynamic VPNPOOL interface
```

HÌNH 3.37 NAT cho VPN client

- Gán ACL cho VPN truy cập DMZ và DMZ trả lời. Cho phép DMZ trả lời các dãy mạng đáng tin do người quản trị cài đặt. Giúp việc gói ping từ inside hay outside có thể được phản hồi.

```
access-list OUTSIDE extended permit ip 192.168.100.0 255.255.255.0 172.16.2.0 255.255.255.0
access-list DMZ extended permit ip 172.16.2.0 255.255.255.0 192.168.100.0 255.255.255.0
access-list DMZ extended permit ip 172.16.2.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list DMZ extended permit ip 172.16.2.0 255.255.255.0 172.17.0.0 255.255.0.0
access-list DMZ extended permit ip 172.16.2.0 255.255.255.0 172.18.0.0 255.255.255.0
```

HÌNH 3.38 Gán ACL

- Mở HTTP Server. Cho phép dãy 192.168.1.0 được truy cập từ bên ngoài từ outside.

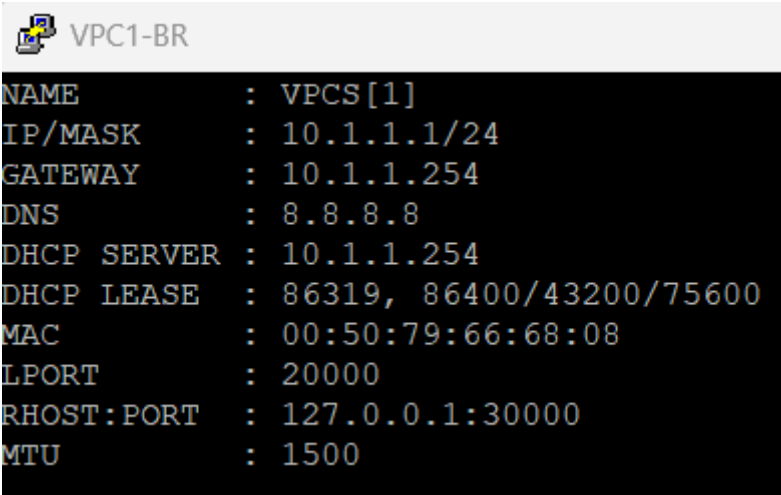
```
http server enable
http 192.168.1.0 255.255.255.0 outside
```

HÌNH 3.39 Mở HTTP Server

3.3.2. Kết quả thực nghiệm

3.3.2.1. Thực nghiệm cấp phát địa chỉ IP tự động

- Thực nghiệm cấp phát địa chỉ IP tự động cho các máy trong BR (VPC1-BR và VPC2-BR).
 - VPC1-BR

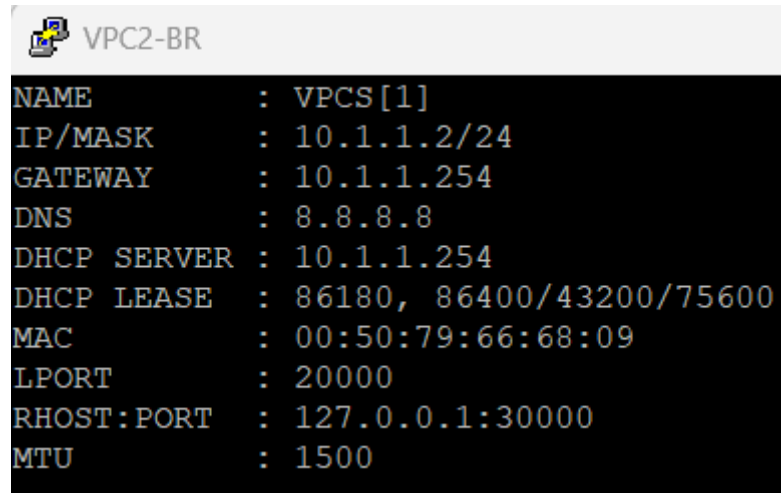


VPC1-BR

```
NAME      : VPCS[1]
IP/MASK    : 10.1.1.1/24
GATEWAY    : 10.1.1.254
DNS        : 8.8.8.8
DHCP SERVER : 10.1.1.254
DHCP LEASE  : 86319, 86400/43200/75600
MAC        : 00:50:79:66:68:08
LPORT      : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU        : 1500
```

HÌNH 3.40 Cấp địa chỉ IP cho VPC1-BR

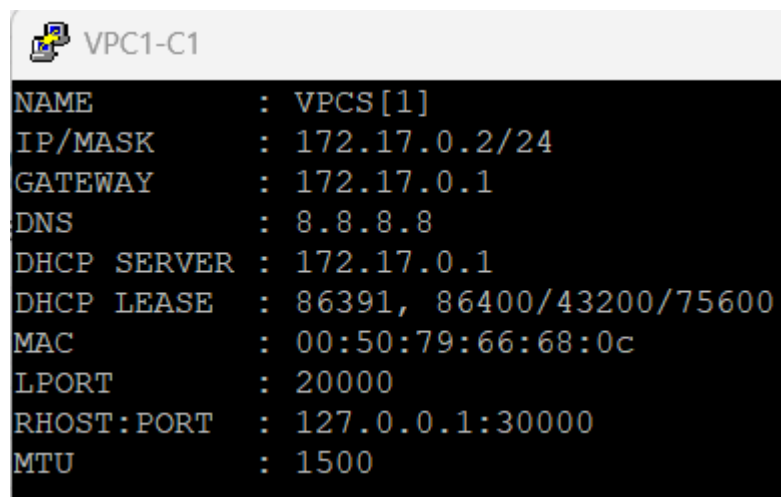
- VPC2-BR

A screenshot of a terminal window titled 'VPC2-BR'. It displays the configuration for a VPC interface. The text is as follows:

```
NAME      : VPCS[1]
IP/MASK    : 10.1.1.2/24
GATEWAY    : 10.1.1.254
DNS        : 8.8.8.8
DHCP SERVER : 10.1.1.254
DHCP LEASE  : 86180, 86400/43200/75600
MAC        : 00:50:79:66:68:09
LPORT      : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU        : 1500
```

HÌNH 3.41 Cấp địa chỉ IP cho VPC2-BR

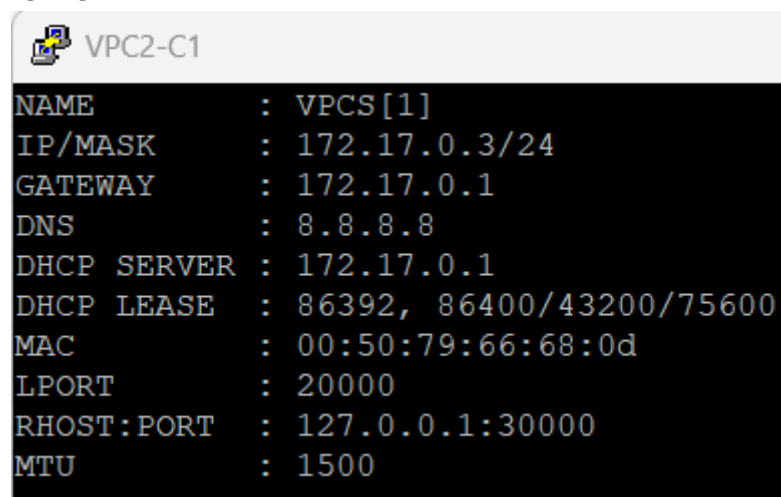
- Thực nghiệm cấp phát địa chỉ IP tự động cho các máy trong CORE1 (VPC1-C1 và VPC2-C1).
 - VPC1-C1

A screenshot of a terminal window titled 'VPC1-C1'. It displays the configuration for a VPC interface. The text is as follows:

```
NAME      : VPCS[1]
IP/MASK    : 172.17.0.2/24
GATEWAY    : 172.17.0.1
DNS        : 8.8.8.8
DHCP SERVER : 172.17.0.1
DHCP LEASE  : 86391, 86400/43200/75600
MAC        : 00:50:79:66:68:0c
LPORT      : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU        : 1500
```

HÌNH 3.42 Cấp địa chỉ IP cho VPC1-C1

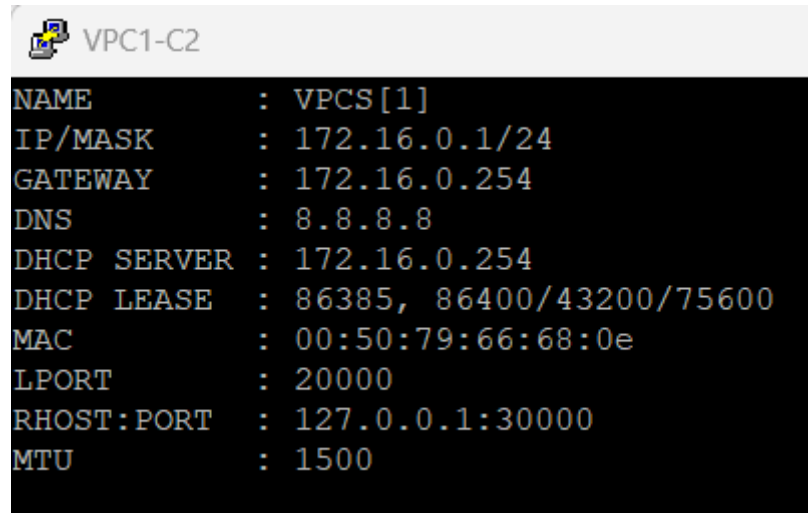
- VPC2-C1

A screenshot of a terminal window titled 'VPC2-C1'. It displays the configuration for a VPC interface. The text is as follows:

```
NAME      : VPCS[1]
IP/MASK    : 172.17.0.3/24
GATEWAY    : 172.17.0.1
DNS        : 8.8.8.8
DHCP SERVER : 172.17.0.1
DHCP LEASE  : 86392, 86400/43200/75600
MAC        : 00:50:79:66:68:0d
LPORT      : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU        : 1500
```

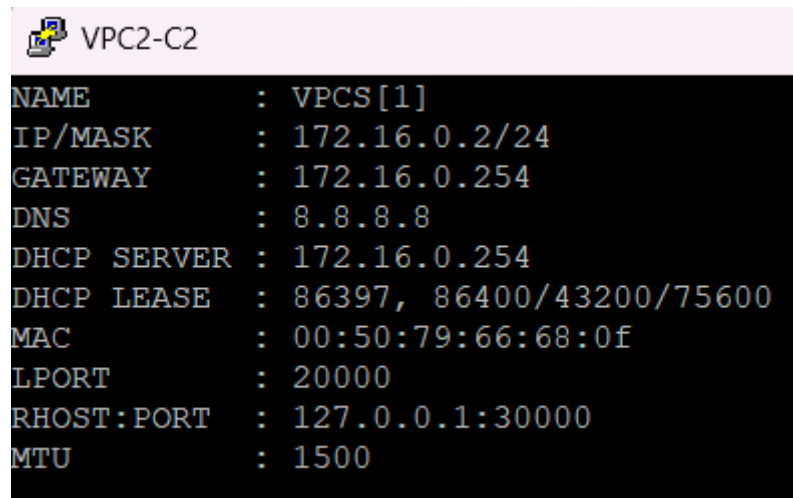
HÌNH 3.43 Cấp địa chỉ IP cho VPC2-C1

- Thực nghiệm cấp phát địa chỉ IP tự động cho các máy trong CORE2 (VPC1-C2 và VPC2-C2).
 - VPC1-C2



HÌNH 3.44 Cấp địa chỉ IP cho VPC1-C2

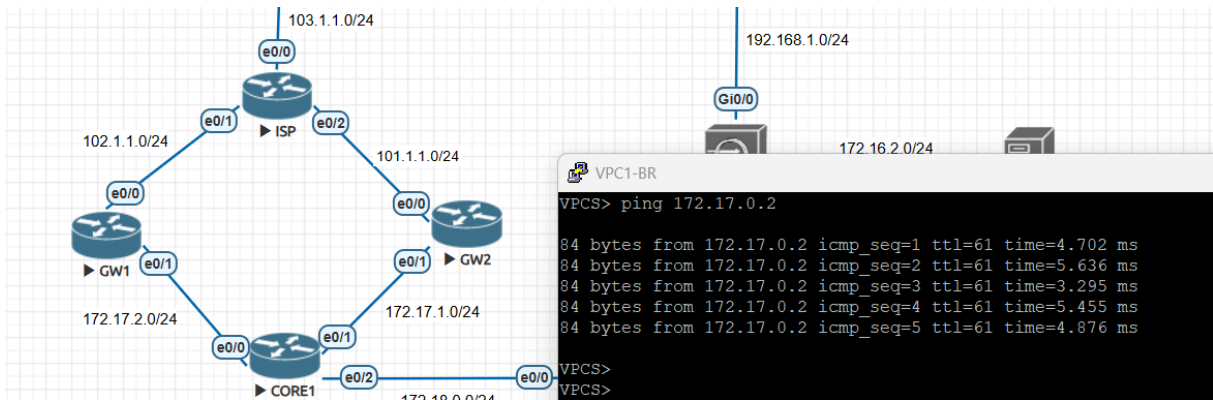
- VPC2-C2



HÌNH 3.45 Cấp địa chỉ IP cho VPC2-C2

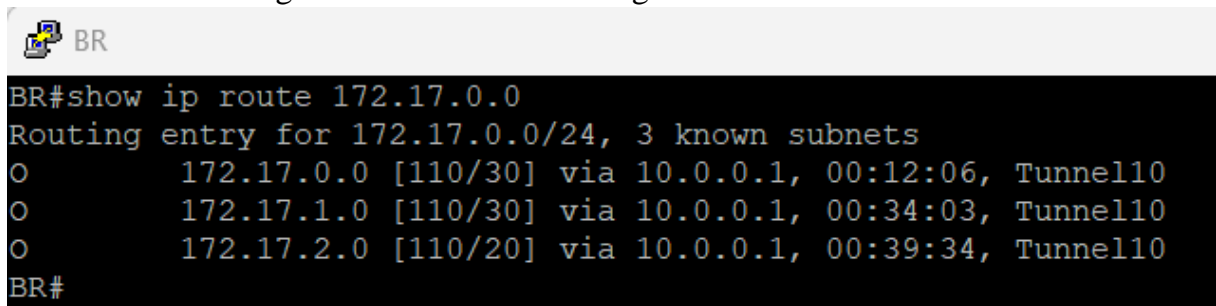
3.3.2.2. Thực nghiệm dự phòng

- Kiểm tra thử kết nối từ BR tới CORE1 bằng cách ping từ VPC1-BR tới VPC1-C1. Nếu gói tin thành công có nghĩa là Tunnel được thông qua. Thiết lập IPsec thành công.



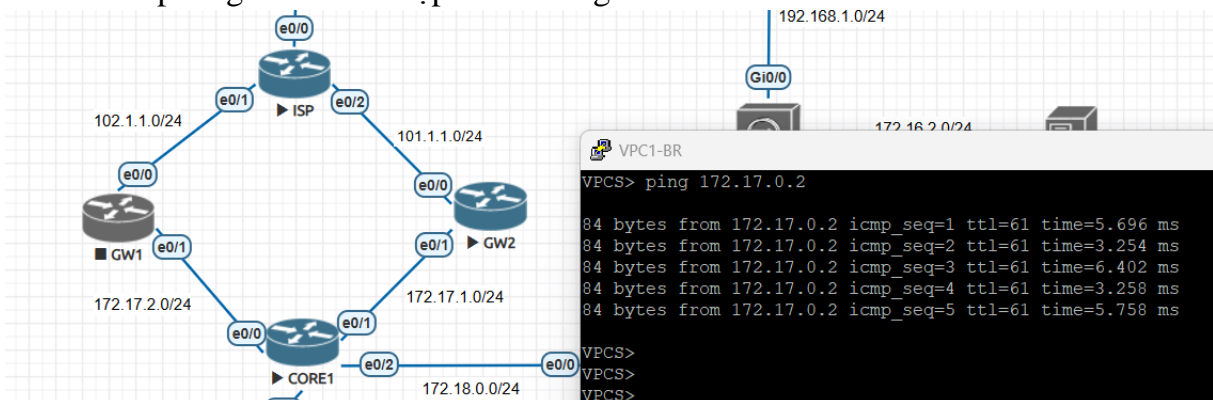
HÌNH 3.46 Kiểm tra kết nối BR tới CORE1

- Kiểm tra đường đi khi Router BR ping đến dãy LAN 172.17.0.0/24 của CORE1. Ta thấy đường đi qua Tunnel10 đã được thiết lập IPsec. Thiết lập thành công BR1 về GW1 làm đường kết nối VPN chính.



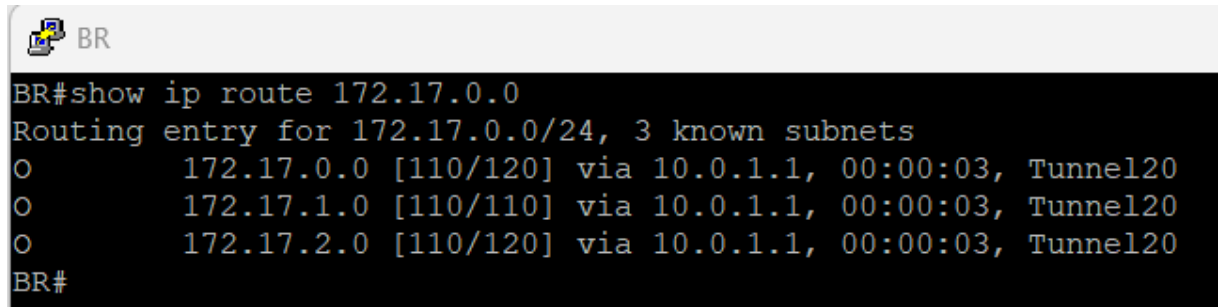
HÌNH 3.47 Kiểm tra kết nối BR

- Thử nghiệm khi GW1 tắt, ta ping từ VPC1-BR đến VPC1-C1. Vẫn ping được thành công cho thấy khi GW1 tắt đường đi vẫn không bị gián đoạn. Đường dự phòng GW2 thiết lập thành công.



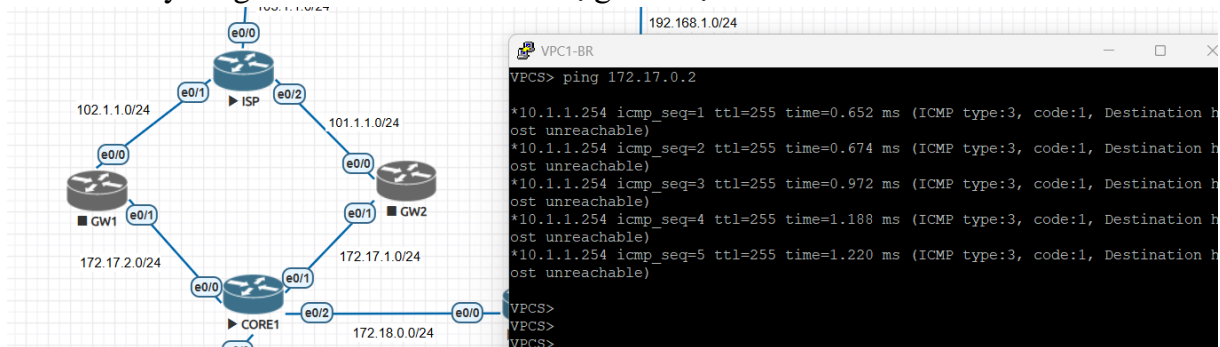
HÌNH 3.48 Ping thành công vào LAN 172.17.0.2

- Kiểm tra lại đường đi. Ta thấy đã đổi thành Tunnel20. Sau khi GW1 tắt thì sẽ tự động sử dụng Tunnel20. Thiết lập thành công BR1 về GW2 làm đường kết nối VPN dự phòng.

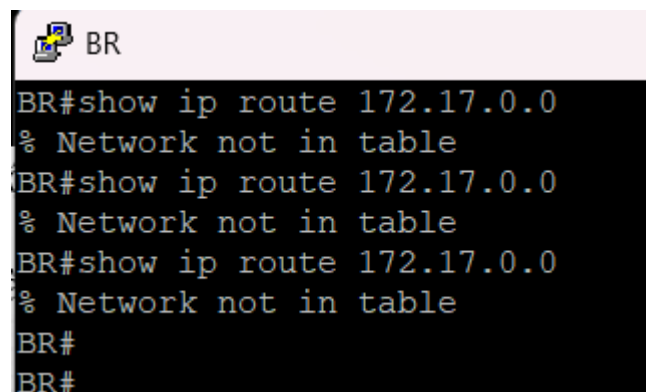


HÌNH 3.49 Kiểm tra đường đi

- Kiểm tra khi cả hai GW1 và GW2 cùng tắt. Khi ping thì hiển thị “Destination host unreachable” có nghĩa là không tìm thấy đường đi đến 172.17.0.2. Cho thấy rằng khi tắt cả hai GW thì bị gián đoạn kết nối.



HÌNH 3.50 Kiểm tra khi tắt GW1 và GW2



HÌNH 3.51 Ping thất bại

- Sử dụng wireshark để capture e0/0 trên BR, ta được các gói từ nguồn 103.1.1.254 (BR) đến 102.1.1.254 (GW1) và ngược lại với
 - ESP (Protocol): Đây là gói Encapsulating Security Payload, xác nhận gói IPSEC thực
 - SPI (Security Parameter Index): Xác định phiên IPSec đang hoạt động

7	8.114646	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
8	9.917323	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)
9	12.936794	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
10	12.939575	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)
11	13.942787	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
12	13.944929	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)
13	14.915125	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
14	14.948213	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
15	14.950407	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)
16	15.953425	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
17	15.954818	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)
18	16.834597	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)
19	16.955905	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
20	16.957676	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)
21	16.987974	aa:bb:cc:00:20:00	aa:bb:cc:00:20:00	LOOP	60 Reply
22	17.306215	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
23	17.768625	aa:bb:cc:00:10:00	aa:bb:cc:00:10:00	LOOP	60 Reply
24	19.295602	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)
25	24.178677	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
26	26.084464	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)
27	26.992596	aa:bb:cc:00:20:00	aa:bb:cc:00:20:00	LOOP	60 Reply
28	27.106191	103.1.1.254	102.1.1.254	ESP	166 ESP (SPI=0x50ec276f)
29	27.775180	aa:bb:cc:00:10:00	aa:bb:cc:00:10:00	LOOP	60 Reply
30	28.931214	102.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0x827b538d)

HÌNH 3.52 Capture e0/0 trên BR


- Tương tự khi tắt GW1 thì GW2 sẽ thay thế và đóng vai trò là đường dự phòng.

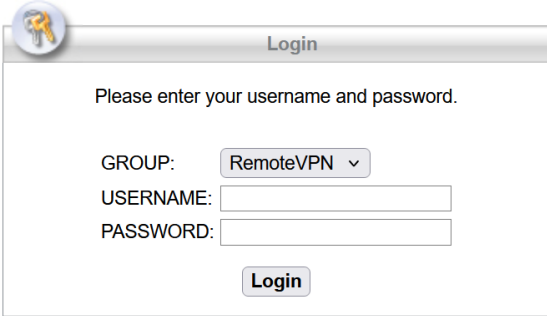
8	11.013776	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
9	11.960811	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
10	11.964019	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)
11	12.966380	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
12	12.969609	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)
13	13.322424	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)
14	13.973161	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
15	13.975126	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)
16	14.736393	103.1.1.254	102.1.1.254	ESP	150 ESP (SPI=0x50ec276f)
17	14.977151	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
18	14.978526	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)
19	15.982732	103.1.1.254	101.1.1.254	ESP	166 ESP (SPI=0xb5bdeaf7)
20	15.987945	101.1.1.254	103.1.1.254	ESP	166 ESP (SPI=0xfa0c75d7)

HÌNH 3.53 Kiểm tra dự phòng

3.3.2.3. Thực nghiệm Anyconnect VPN

- Truy cập vào IP của ZONE Outside trên ASA. Tuy nhiên ASA 9.15 là phiên bản cũ chỉ hỗ trợ TLSv1. Nên sử dụng FireFox với cài đặt cho phép TLSv1.

 **SSL VPN Service**



Login

Please enter your username and password.

GROUP: RemoteVPN ▾

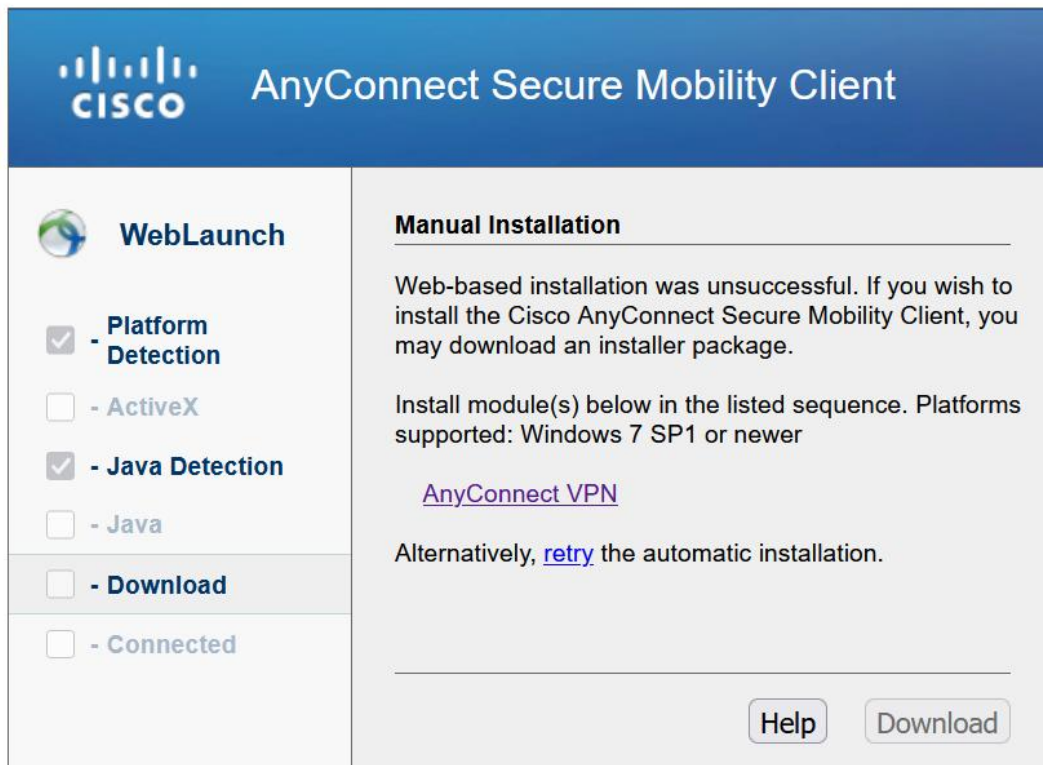
USERNAME:

PASSWORD:

Login

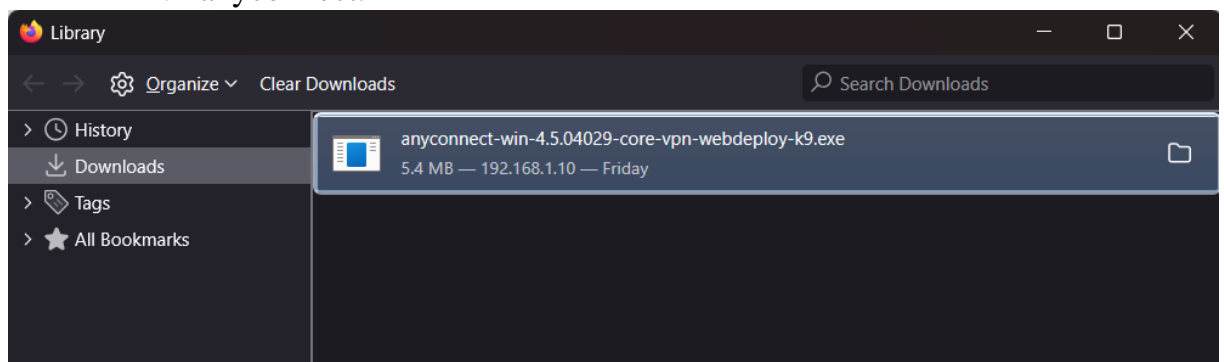
HÌNH 3.54 Truy cập vào IP của Zone Outside

- Đăng nhập tài khoản và mật khẩu đã tạo. Trang web sẽ cho phép tải xuống Cisco Secure Client để sử dụng AnyConnect VPN. Đây là phần mềm cho phép kết nối AnyConnect do Cisco tạo ra.



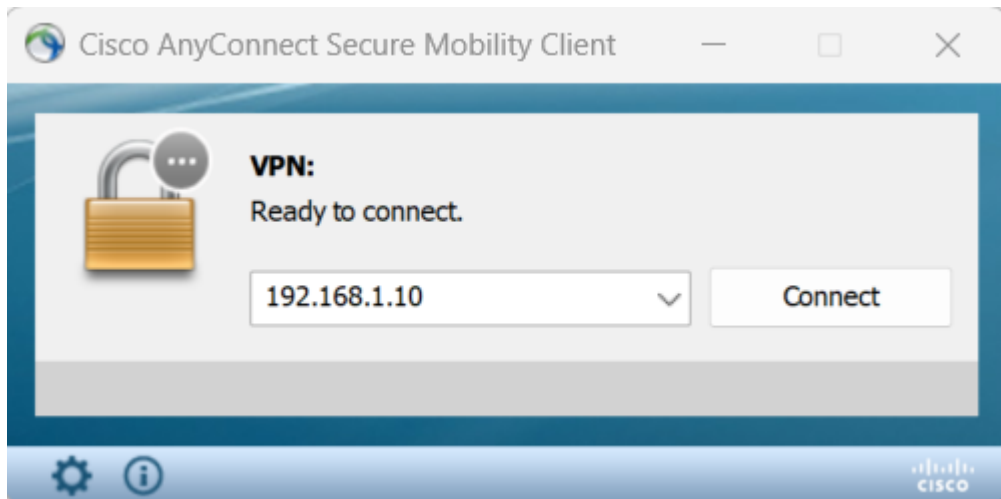
HÌNH 3.55 Đăng nhập

- Tải về anyconnect.



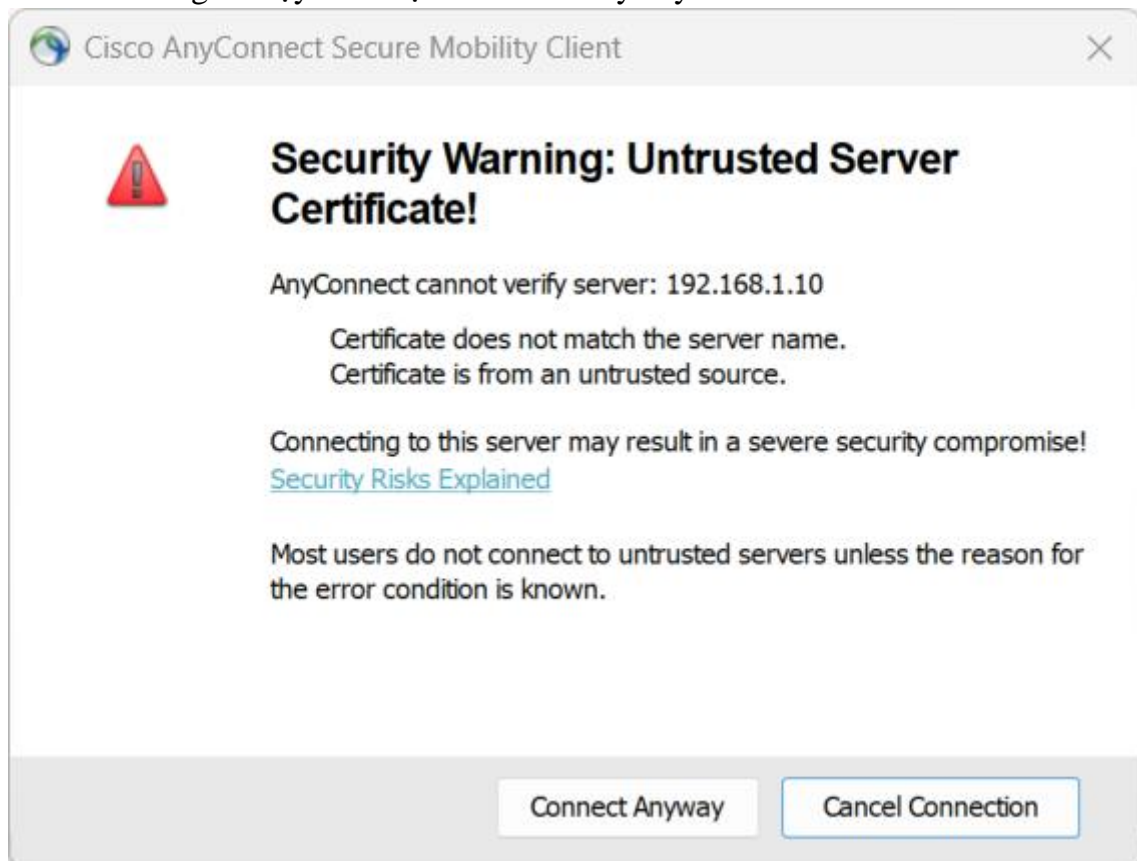
HÌNH 3.56 Tải về

- Cài đặt trên máy tính. Sau khi cài đặt truy cập IP của outside ASA.



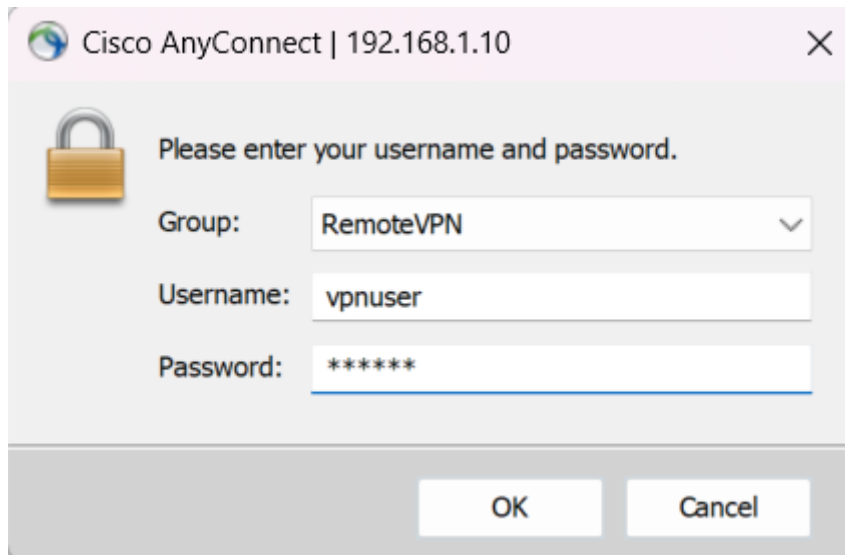
HÌNH 3.57 Truy cập IP của ASA

- Cảnh báo khi kết nối vào Server không tin cậy. Đây là cảnh báo khi kết nối đến Server mà chưa có chứng chỉ trùng với tên server và chứng chỉ từ nguồn không tin cậy. Ta chọn Connect Anyway.



HÌNH 3.58 Cảnh báo kết nối

- Chọn Group RemoteVPN và điền Username, Password được cung cấp từ nhà quản trị để kết nối.



HÌNH 3.59 Kết nối

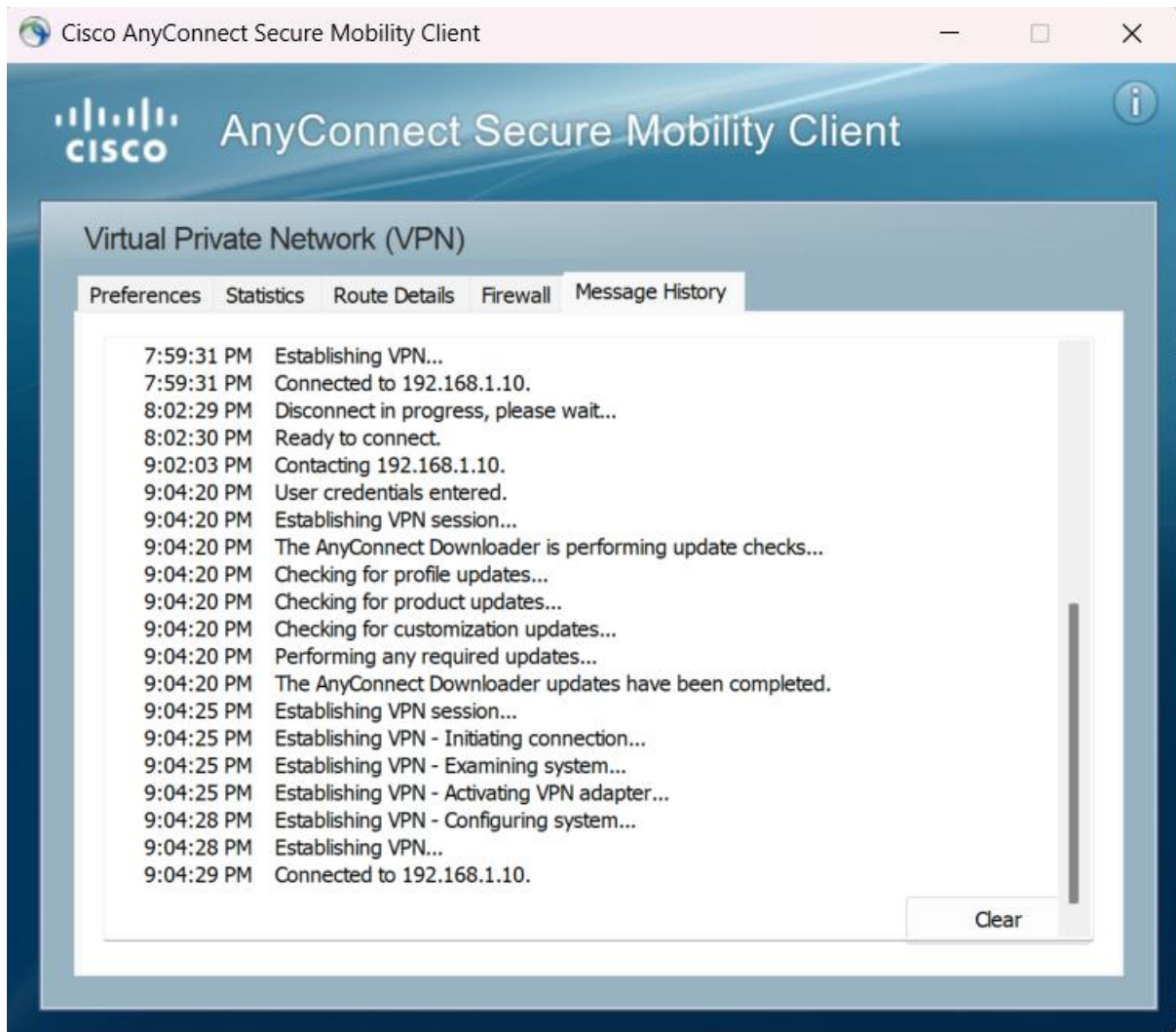
- Kiểm tra máy đã kết nối thành công chưa bằng lệnh `ipconfig /all` trên cmd. Nếu hiện IP trong VPN Pool là 192.168.100.10 (IP mà AnyConnect cung cấp) cho thấy đã kết nối thành công. Các thông số cũng được cung cấp khi tạo chính sách trên ASA như DNS Server là 8.8.8.8.

```
Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : 
Description . . . . . : Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows x64
Physical Address. . . . . : 00-05-9A-3C-7A-00
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::21e9:d1bd:d705:87ed%15(Preferred)
Link-local IPv6 Address . . . . : fe80::a5c5:5832:2c14:6079%15(Preferred)
IPv4 Address. . . . . : 192.168.100.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 117441946
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-C7-CC-65-E8-6A-64-AC-AB-F4
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
```

HÌNH 3.60 Kiểm tra kết nối

- Hoặc có thể xem lịch sử kết nối trong Cisco Secure Client. Bao gồm hình thành VPN, kết nối đến 192.168.1.10, hình thành session, ... đều được hiển thị chi tiết. Giúp hiểu về cách thành lập kết nối AnyConnect.



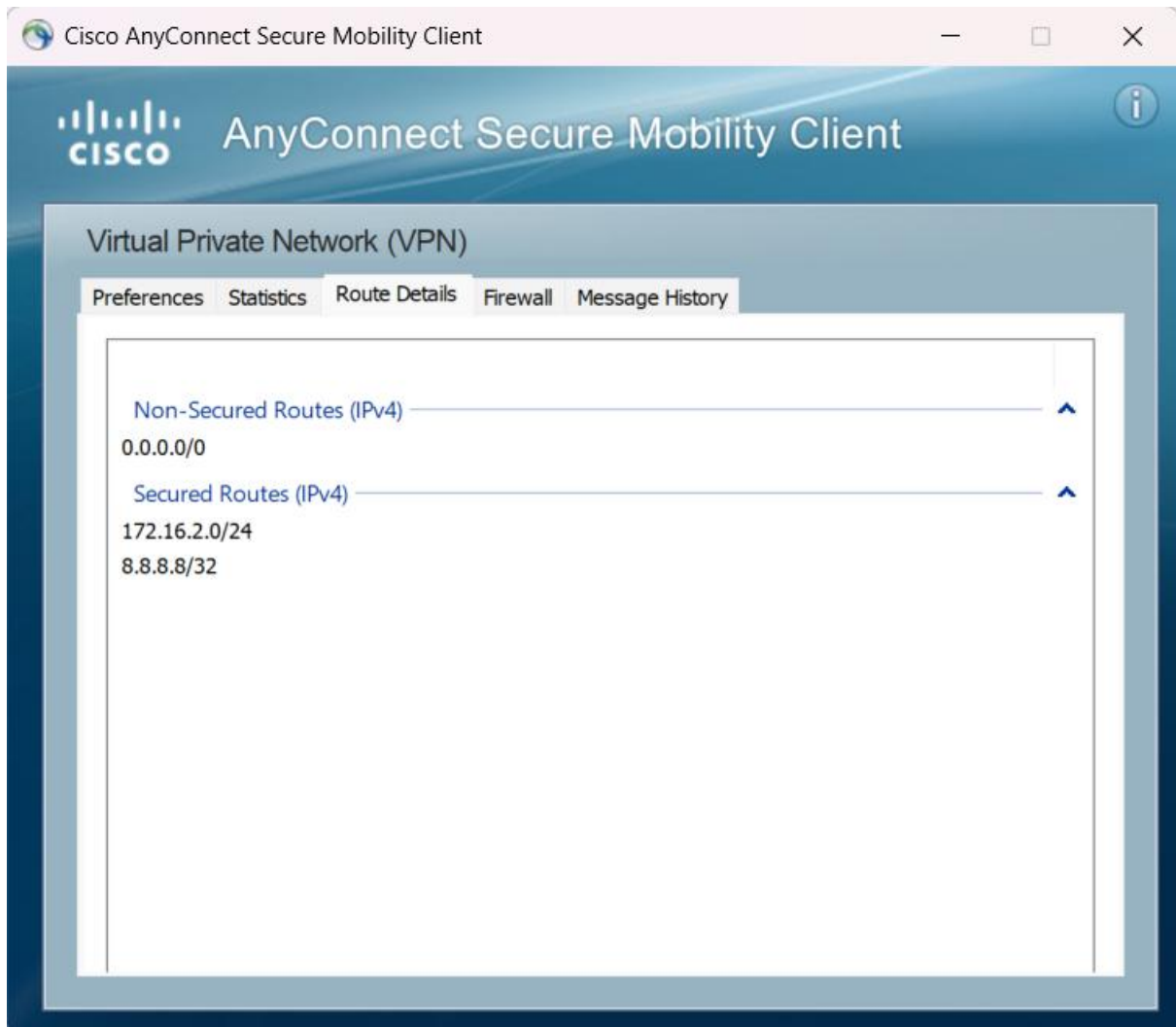
HÌNH 3.61 Kiểm tra lịch sử

- Xem thông tin kết nối qua tab Statistics. Các thông số có thể xem như trạng thái, thời gian đã kết nối, IP của client,... Cũng như byte đã gửi, byte đã nhận,...



HÌNH 3.62 Xem thông tin kết nối

- Xem các route bảo mật bao gồm vùng DMZ, DNS server . Các dây mạng còn lại là không an toàn. Điều này giúp giảm tải lượng VPN khi vào DMZ, giúp truy cập nhanh hơn và độ trễ thấp.



HÌNH 3.63 Route được kết nối

- Kiểm tra kết nối đến DMZ bằng cách ping từ Anyconnect Client đến SVR. Kết quả ping thành công cho thấy rằng có thể truy cập DMZ từ xa. Và để hiểu rõ hơn thì sẽ sử dụng Wireshark để xem gói tin.

```
C:\Users\Legion>ping 172.16.2.100

Pinging 172.16.2.100 with 32 bytes of data:
Reply from 172.16.2.100: bytes=32 time=8ms TTL=64
Reply from 172.16.2.100: bytes=32 time=2ms TTL=64
Reply from 172.16.2.100: bytes=32 time=1ms TTL=64
Reply from 172.16.2.100: bytes=32 time=1ms TTL=64

Ping statistics for 172.16.2.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

HÌNH 3.64 Kiểm tra kết nối DMZ

- Sử dụng Wireshark để chứng thực AnyConnectVPN
 - Bắt được các gói DNS của AnyConnect Client

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.10	8.8.8.8	DNS	74	Standard query 0xe4e9 A www.google.com
2	6.388205	192.168.100.10	8.8.8.8	DNS	80	Standard query 0x3de4 A beacons.gcp.gvt2.com
3	6.417674	192.168.100.10	8.8.8.8	DNS	80	Standard query 0x3de4 A beacons.gcp.gvt2.com
4	7.419949	192.168.100.10	8.8.8.8	DNS	80	Standard query 0x3de4 A beacons.gcp.gvt2.com
5	9.186563	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x1cb9 A www.facebook.com
6	9.215179	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x1cb9 A www.facebook.com
7	9.430077	192.168.100.10	8.8.8.8	DNS	80	Standard query 0x3de4 A beacons.gcp.gvt2.com
8	10.215386	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x1cb9 A www.facebook.com
9	12.221160	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x1cb9 A www.facebook.com
10	12.964480	192.168.100.10	8.8.8.8	DNS	74	Standard query 0x13eb A www.google.com
11	13.003017	192.168.100.10	8.8.8.8	DNS	74	Standard query 0x13eb A www.google.com
12	13.435007	192.168.100.10	8.8.8.8	DNS	80	Standard query 0x3de4 A beacons.gcp.gvt2.com
13	13.978435	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x8051 A www.msftncsi.com
14	14.003548	192.168.100.10	8.8.8.8	DNS	74	Standard query 0x13eb A www.google.com
15	14.018595	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x8051 A www.msftncsi.com
16	15.018899	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x8051 A www.msftncsi.com
17	15.159483	192.168.100.10	8.8.8.8	DNS	86	Standard query 0x0d24 A web-chat-e2ee.facebook.com
18	15.188722	192.168.100.10	8.8.8.8	DNS	86	Standard query 0x0d24 A web-chat-e2ee.facebook.com
19	15.219632	Cisco_3c:7a:00	Cimsys_33:44:55	ARP	42	Who has 192.168.100.1? Tell 192.168.100.10
20	15.219755	Cimsys_33:44:55	Cisco_3c:7a:00	ARP	42	192.168.100.1 is at 00:11:22:33:44:55
21	16.012024	192.168.100.10	8.8.8.8	DNS	74	Standard query 0x13eb A www.google.com
22	16.195026	192.168.100.10	8.8.8.8	DNS	86	Standard query 0x0d24 A web-chat-e2ee.facebook.com
23	16.226008	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x1cb9 A www.facebook.com
24	16.932652	192.168.100.10	8.8.8.8	DNS	79	Standard query 0x34dd A clients2.google.com
25	16.962288	192.168.100.10	8.8.8.8	DNS	79	Standard query 0x34dd A clients2.google.com
26	17.023504	192.168.100.10	8.8.8.8	DNS	76	Standard query 0x8051 A www.msftncsi.com
27	17.975418	192.168.100.10	8.8.8.8	DNS	79	Standard query 0x34dd A clients2.google.com
28	18.022696	192.168.100.10	8.8.8.8	DNS	80	Standard query 0x0b13 A beacons.gcp.gvt2.com
29	18.052240	192.168.100.10	8.8.8.8	DNS	80	Standard query 0x0b13 A beacons.gcp.gvt2.com
30	18.206076	192.168.100.10	8.8.8.8	DNS	86	Standard query 0x0d24 A web-chat-e2ee.facebook.com

HÌNH 3.65 Chứng thực AnyConnectVPN

- Các gói TCP và TLSv1 giao tiếp giữa máy Client (192.168.1.24) và ASA (192.168.1.10). Khi ping được gửi qua VPN (AnyConnect), nó sẽ được mã hóa trong TLSv1 khi nhìn từ bên ngoài.

No.	Time	Source	Destination	Protocol	Length	Info
153	13.701787	192.168.1.24	192.168.1.10	TCP	54	58092 → 443 [ACK] Seq=974 Ack=102 Win=65101 Len=0
154	13.701790	192.168.1.24	192.168.1.10	TCP	54	[TCP Dup ACK 153#1] 58092 → 443 [ACK] Seq=974 Ack=102 Win=65101 Len=0
155	14.072917	192.168.1.24	192.168.1.10	TLSv1	155	Application Data
156	14.072920	192.168.1.24	192.168.1.10	TCP	155	[TCP Retransmission] 58092 → 443 [PSH, ACK] Seq=974 Ack=102 Win=65101 Len=101
157	14.074042	192.168.1.10	192.168.1.24	TCP	54	443 → 58092 [ACK] Seq=102 Ack=1075 Win=32768 Len=0
158	14.074043	192.168.1.10	192.168.1.24	TCP	54	[TCP Dup ACK 157#1] 443 → 58092 [ACK] Seq=102 Ack=1075 Win=32768 Len=0
159	14.672083	192.168.1.24	192.168.1.10	TLSv1	155	Application Data
160	14.672087	192.168.1.24	192.168.1.10	TCP	155	[TCP Retransmission] 58092 → 443 [PSH, ACK] Seq=1075 Ack=102 Win=65101 Len=101
161	14.676152	192.168.1.10	192.168.1.24	TCP	54	443 → 58092 [ACK] Seq=102 Ack=1176 Win=32768 Len=0
162	14.676155	192.168.1.10	192.168.1.24	TCP	54	[TCP Dup ACK 161#1] 443 → 58092 [ACK] Seq=102 Ack=1176 Win=32768 Len=0
163	14.676911	192.168.1.10	192.168.1.24	TLSv1	155	Application Data
164	14.676912	192.168.1.10	192.168.1.24	TCP	155	[TCP Retransmission] 443 → 58092 [PSH, ACK] Seq=102 Ack=1176 Win=32768 Len=101
165	14.717742	192.168.1.24	192.168.1.10	TCP	54	58092 → 443 [ACK] Seq=1176 Ack=203 Win=65000 Len=0
166	14.717746	192.168.1.24	192.168.1.10	TCP	54	[TCP Dup ACK 165#1] 58092 → 443 [ACK] Seq=1176 Ack=203 Win=65000 Len=0
167	15.334599	192.168.1.24	192.168.1.10	TLSv1	171	Application Data
168	15.334512	192.168.1.24	192.168.1.10	TCP	171	[TCP Retransmission] 58092 → 443 [PSH, ACK] Seq=1176 Ack=203 Win=65000 Len=117
169	15.335369	192.168.1.10	192.168.1.24	TCP	54	443 → 58092 [ACK] Seq=203 Ack=1293 Win=32768 Len=0
170	15.335371	192.168.1.10	192.168.1.24	TCP	54	[TCP Dup ACK 169#1] 443 → 58092 [ACK] Seq=203 Ack=1293 Win=32768 Len=0
171	15.686947	192.168.1.24	192.168.1.10	TLSv1	155	Application Data
172	15.686950	192.168.1.24	192.168.1.10	TCP	155	[TCP Retransmission] 58092 → 443 [PSH, ACK] Seq=1293 Ack=203 Win=65000 Len=101
173	15.687789	192.168.1.10	192.168.1.24	TCP	54	443 → 58092 [ACK] Seq=203 Ack=1394 Win=32768 Len=0
174	15.687791	192.168.1.10	192.168.1.24	TCP	54	[TCP Dup ACK 173#1] 443 → 58092 [ACK] Seq=203 Ack=1394 Win=32768 Len=0
175	15.688178	192.168.1.10	192.168.1.24	TLSv1	155	Application Data
176	15.688180	192.168.1.10	192.168.1.24	TCP	155	[TCP Retransmission] 443 → 58092 [PSH, ACK] Seq=203 Ack=1394 Win=32768 Len=101
177	15.732725	192.168.1.24	192.168.1.10	TCP	54	58092 → 443 [ACK] Seq=1394 Ack=304 Win=64899 Len=0
178	15.732729	192.168.1.24	192.168.1.10	TCP	54	[TCP Dup ACK 177#1] 58092 → 443 [ACK] Seq=1394 Ack=304 Win=64899 Len=0
179	15.895416	192.168.1.24	192.168.1.10	TLSv1	155	Application Data
180	15.895419	192.168.1.24	192.168.1.10	TCP	155	[TCP Retransmission] 58092 → 443 [PSH, ACK] Seq=1394 Ack=304 Win=64899 Len=101
181	15.896254	192.168.1.10	192.168.1.24	TCP	54	443 → 58092 [ACK] Seq=304 Ack=1495 Win=32768 Len=0
182	15.896257	192.168.1.10	192.168.1.24	TCP	54	[TCP Dup ACK 181#1] 443 → 58092 [ACK] Seq=304 Ack=1495 Win=32768 Len=0

HÌNH 3.66 Các gói TCP

- Khi sử dụng Wireshark bắt quan Ethernet1 của ASA (Vùng DMZ). Ta thấy gói ping ICMP rõ ràng hơn khi đi từ VPN Client đến SVR.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.10	172.16.2.100	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 4)
2	0.000189	Private_66:68:10	Broadcast	ARP	64	Who has 172.16.2.1? Tell 172.16.2.100
3	0.000541	50:00:00:11:00:01	Private_66:68:10	ARP	42	172.16.2.1 is at 50:00:00:11:00:01
4	0.001602	172.16.2.100	192.168.100.10	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=64 (request in 1)
5	1.010219	192.168.100.10	172.16.2.100	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 6)
6	1.010473	172.16.2.100	192.168.100.10	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=64 (request in 5)
7	2.024682	192.168.100.10	172.16.2.100	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 8)
8	2.024836	172.16.2.100	192.168.100.10	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=64 (request in 7)
9	3.040255	192.168.100.10	172.16.2.100	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 10)
10	3.040330	172.16.2.100	192.168.100.10	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=64 (request in 9)

HÌNH 3.67 Capture eth1

3.3.2.4. Thực nghiệm kết nối INSIDE vào DMZ

- Ping từ VPC1-C1 vào SVR

```

VPCS> ping 172.16.2.200

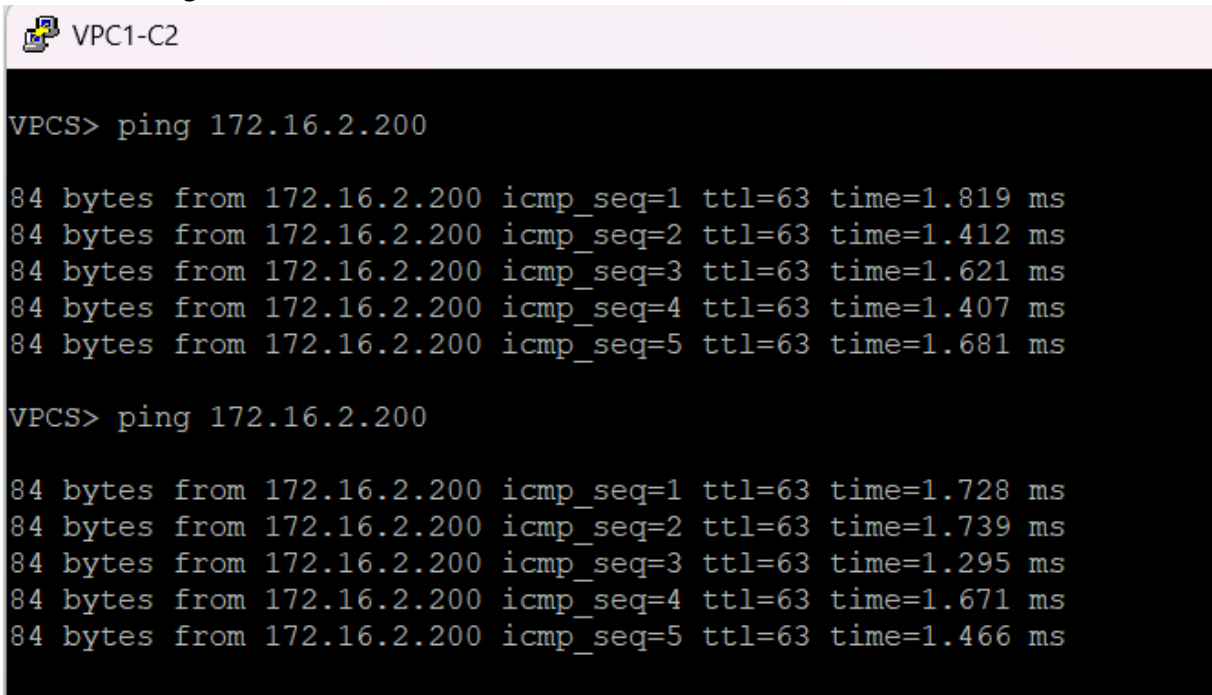
84 bytes from 172.16.2.200 icmp_seq=1 ttl=62 time=3.467 ms
84 bytes from 172.16.2.200 icmp_seq=2 ttl=62 time=1.721 ms
84 bytes from 172.16.2.200 icmp_seq=3 ttl=62 time=1.819 ms
84 bytes from 172.16.2.200 icmp_seq=4 ttl=62 time=1.926 ms
84 bytes from 172.16.2.200 icmp_seq=5 ttl=62 time=1.869 ms

VPCS> ping 172.16.2.200

84 bytes from 172.16.2.200 icmp_seq=1 ttl=62 time=2.061 ms
84 bytes from 172.16.2.200 icmp_seq=2 ttl=62 time=1.873 ms
84 bytes from 172.16.2.200 icmp_seq=3 ttl=62 time=1.978 ms
84 bytes from 172.16.2.200 icmp_seq=4 ttl=62 time=1.459 ms
84 bytes from 172.16.2.200 icmp_seq=5 ttl=62 time=1.357 ms
  
```

HÌNH 3.68 Ping từ VPC1-C1

- Ping từ VPC1-C2 vào SVR



```
VPC1-C2
VPCS> ping 172.16.2.200
84 bytes from 172.16.2.200 icmp_seq=1 ttl=63 time=1.819 ms
84 bytes from 172.16.2.200 icmp_seq=2 ttl=63 time=1.412 ms
84 bytes from 172.16.2.200 icmp_seq=3 ttl=63 time=1.621 ms
84 bytes from 172.16.2.200 icmp_seq=4 ttl=63 time=1.407 ms
84 bytes from 172.16.2.200 icmp_seq=5 ttl=63 time=1.681 ms

VPCS> ping 172.16.2.200
84 bytes from 172.16.2.200 icmp_seq=1 ttl=63 time=1.728 ms
84 bytes from 172.16.2.200 icmp_seq=2 ttl=63 time=1.739 ms
84 bytes from 172.16.2.200 icmp_seq=3 ttl=63 time=1.295 ms
84 bytes from 172.16.2.200 icmp_seq=4 ttl=63 time=1.671 ms
84 bytes from 172.16.2.200 icmp_seq=5 ttl=63 time=1.466 ms
```

HÌNH 3.69 Ping từ VPC1-C2

CHƯƠNG 4: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**Kết quả đạt được:**

- Đề xuất được mô hình hệ thống an toàn bảo mật mạng cho hội sở bằng các thiết bị chuyên dụng đáp ứng hầu hết các kịch bản thực tế của doanh nghiệp vừa và nhỏ.
- Đạt được những yêu cầu đã đề ra cho hệ thống an toàn bảo mật mạng cho hội sở:
 - Mô hình hệ thống đáp ứng được một phần an toàn bảo mật mạng cho hội sở.
 - Cấu hình kết hợp giữa định tuyến động và tĩnh giúp kết nối linh hoạt giữa các chi nhánh, phân vùng.
 - Cấu hình VPN đảm bảo an toàn đường truyền cho giao tiếp giữa chi nhánh và trung tâm. Thiết lập đường đi dự phòng khi đường chính gặp vấn đề đảm bảo tính sẵn dùng và độ trễ thời gian.
 - Cấu hình Anyconnect VPN cho người quản trị có thể kết nối về Firewall ASA. Nhận IP từ ASA đáp ứng nhu cầu kết nối từ xa đảm bảo kết nối nhanh chóng và không gặp cản trở địa lý nhưng vẫn đảm bảo an toàn vì được theo dõi hoạt động bằng Firewall.
 - Phân vùng mạng rõ ràng Outside, Inside, DMZ và mô phỏng chi nhánh – trung tâm giúp dễ dàng bảo mật từng phần. Đảm bảo khi một phân vùng gặp vấn đề vẫn không ảnh hưởng các phân vùng khác.
 - Ứng dụng được danh sách kiểm soát truy nhập (ACL) và mạng NAT góp phần nâng cao an toàn và giảm truy cập. Điều này giúp hội sở không bị nghẽn mạng khi nhiều người dùng cùng lúc.
 - ASA làm điểm quản lý tập trung vai trò điều khiển truy cập và bảo vệ dịch vụ.

Hạn chế:

- Bảo mật AnyConnect chưa tối ưu: người dùng khi kết nối có quyền cao. ACL quá rộng: Cho phép toàn bộ inside và một phần outside kết nối DMZ. Chưa có bảo vệ chống DDoS vào dịch vụ VPN.
- IPSec và AnyConnect sử dụng các thuật toán RSA, SHA, AES, ... tương đối cũ gặp nhiều vấn đề về bảo mật. Chưa có giám sát hoạt động VPN và phát hiện bất thường.

Hướng phát triển đề tài:

- Hạn chế quyền của người dùng kết nối AnyConnect ở mức quản trị. Cùng với sử dụng các giao thức xác thực như MFA hoặc chứng chỉ. Chỉ cho phép công và dịch vụ cần thiết vào DMZ không permit toàn IP. Giới hạn số kết nối VPN đồng thời. Kết hợp thiết bị hoặc dịch vụ chống DDoS trước ASA.
- Sử dụng các thuật toán hiện đại như SHA-256/512, Diffie-Hellman Group 19-21, IKE version2 và TLSv4 mạnh mẽ và chống lại các cuộc tấn công ngày càng tinh vi. Kết hợp IDS/IPS giám sát lưu lượng mạng đi qua các vùng trọng điểm và đặc biệt là vùng DMZ.

TÀI LIỆU THAM KHẢO

- [1] M. Al-shawi, “CCDE Study Guide: Enterprise Campus Architecture Design,” Nov 23, 2015.
- [2] cisco, “Enterprise Campus 3.0 Architecture: Overview and Framework,” 2008.
- [3] Cisco, “Small Enterprise Design Profile (SEDP) Overview”.
- [4] Satoshi Nakatsukasa, Yusaku Izumi, Keisuke Ikushima, Osanori Koyama, Yutaka Katsuyama, “Static & OSPF routing integration scheme for lightpath reconfigurations in IP-over-CWDM networks,” 2008.
- [5] W. Yuanxun, Z. Shuang, K. Deqi, L. Xuan, Z. Tao và C. Lan, “Performance Test and Analysis of Ground-Air Communication Network based on IPsec VPN”.
- [6] Nitin Naik, Changjing Shang, Qiang Shen, Paul Jenkins, “D-FRI-CiscoFirewall: Dynamic Fuzzy Rule Interpolation for Cisco ASA Firewall,” *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2019.
- [7] S. Wilkins, “Why You Should Use Cisco AnyConnect Instead of the Cisco VPN Client,” 2014.
- [8] Gerbert Roitburd; Matthias Ortmann; Matthias Hollick; Jiska Classen, “Very Pwnable Network: Cisco AnyConnect Security Analysis,” 2021.
- [9] Harahus, Maroš, Čavojský, Matúš, Bugár, Gabriel, Pleva, Matúš, “Interactive Network Learning: An Assessment of EVE-NG Platform in Educational Settings,” 2024.
- [10] Elaine Barker, Quynh Dang, Sheila Frankel, Karen Scarfone, Paul Wouters, “Guide to IPsec VPNs,” 2020.
- [11] C. C. f. C. Security, “Cyber Activity Impacting CISCO ASA VPNs,” 2024.

PHỤ LỤC