ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

BẢN BÁO CÁO SD-WAN VÀ SD-ACCESS

TP. HỒ CHÍ MINH - NĂM 2021

Lời mở đầu

Hệ thống mạng hiện thời đã phát triển rất nhiều so với chục năm về trước, sự phát triển này đã mang lại những lợi ích to lớn trong nhiều lĩnh vực nhất là trong truyền tải thông tin. Nhưng bên cạnh đó sự phát triển còn mang lại nhiều vấn đề phức tạp trong quá trình quản lý và duy trì các hệ thống mạng ngày càng đồ sộ và dày đặc thì ta cần một giải pháp nhằm quản lý hệ thống dễ dàng và đem lại hiệu suất tốt. Dẫn đến các doanh nghiệp chuyên nghiên cứu về các giải pháp hạ tầng mạng, phần mềm quản lý mạng xuất hiện. Một trong những doanh nghiệp đi đầu về lĩnh vực này đó chính là Cisco với các giải pháp SD-Wan, SD-Access sẽ được nhắc tới rõ hơn trong bản báo cáo này.

Mục lục

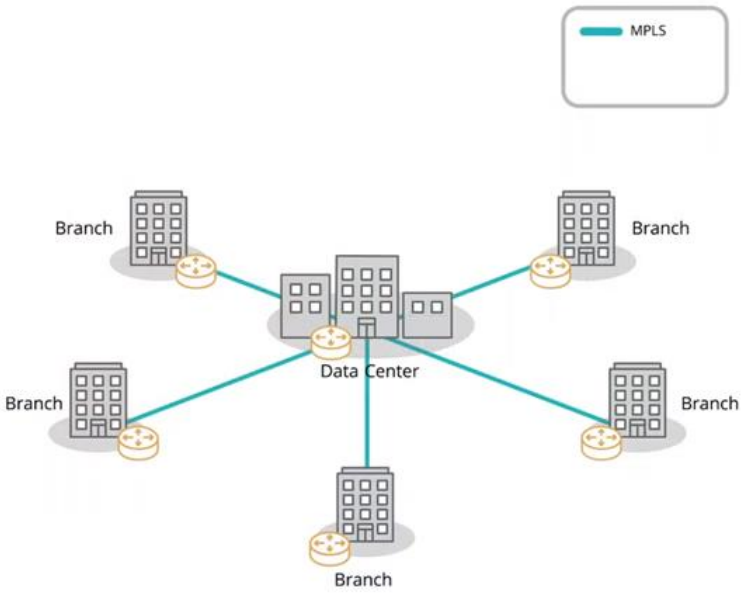
Nội dung

Chương 1: SD-Wan 1
1.1 Mạng WAN truyền thống 1
1.2 SD-Wan là gì 4
1.3 Các tính năng nổi bật của SD-Wan 6
1.4 SD-Wan hoạt động như thế nào? 6
1.5 SD-WAN sử dụng bất kỳ công nghệ truyền dẫn nào, bao gồm MPLS, băng thông rộng và LTE 7
1.6 Vì sao sử dụng SD-Wan? 8
1.7 Các loại giải pháp SD-Wan 9
1.8 Cisco SD-WAN 10
1.8.1 Tổng quan về giải pháp Cisco SD-WAN 10
1.8.2 Các tính năng nổi bật trong giải pháp Cisco SD-WAN 11
1.8.3 Tối ưu hoá hiệu suất ứng dụng 13
1.8.4 Truy cập Internet trực tiếp an toàn 14
1.8.5 Kết nối đa đám mây – Multicloud Connectivity 15
1.9 Cisco component 16
1.9.1 Management Plane 17
1.9.2 Control Plane 17
1.9.3 ORCHESTRATION PLANE 22
1.9.4 DATA PLANE 26
Chương 2: SD-Access 29
2.1 Tổng quan về SD-Access 29
2.1.1 Khái niệm SD-Access 29
2.1.2 Cấu trúc của SD-Access 30
2.1.3 Quản lý SD-Access với Cisco DNA center 32
2.1.4 Lợi ích của SD-Access 33
2.2 SD-Access Fabric 35
2.2.1 Tổng quan 35
2.2.2 Thành phần của Fabric 38
2.2.3 Cách thức hoạt động của Fabric 39
2.3 Cisco DNA Center 42
2.3.1 Tổng quan 42
2.3.2 Nguyên lý của kiến trúc 42
2.3.3 Khả năng tự động hóa 43

Chương 1: SD-Wan

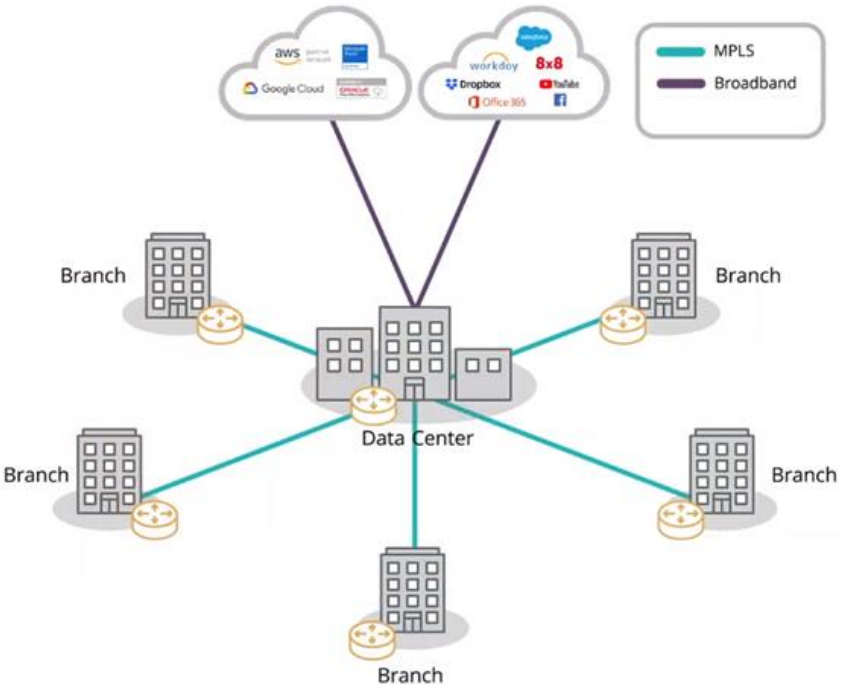
1.1 Mạng WAN truyền thống

- Trong năm 2021, các doanh nghiệp đang trải qua quá trình chuyển đổi số mạnh mẽ hơn bao giờ hết. Với sự phát triển của công nghệ 4.0, nhu cầu về làm việc từ xa, nhu cầu về thiết bị di động, thiết bị IoT, ứng dụng SaaS và dịch vụ điện toán đám mây tăng trưởng một cách chóng mặt, rất nhiều ứng dụng được đưa lên nền tảng đám mây và nhiều dịch vụ được sử dụng thông qua mạng Internet. cùng với đó là các nhu cầu về bao mật ngày càng tăng, các ứng dụng đòi hỏi phải có một kết nối ưu tiên và tối ưu hóa, có tính sẵn sàng cao. Trong khi các yếu tố về chí phí, thời gian và nhân lực triển khai, vận hành hệ thống phải giảm xuống.



- Tuy nhiên Mô hình mạng WAN truyền thống là một mô hình kết nối tập chung được thiết kế để kết nối các nhân viên làm việc từ xa đến các ứng dụng được host trên data center, tất cả các tài nguyên, ứng dụng mà nhân viên có quyền truy cập, sử dụng đều nằm trong data center của tổ chức, doanh nghiệp. Và hiện tại MPLS là công nghệ WAN được đa số các tổ chức, doanh nghiệp lựa chọn cho mục đích kết nối các văn phòng về data center vì nó đảm bảo tính bảo mật của hệ thống, thiết bị bảo mật, có thể là firewall, được đặt ở data center và filter (lọc) các

traffic từ các văn phòng đi đến data center và hạn chế tối đa việc nhân viên truy cập Internet.



Mô hình diện rộng truyền thống

- Nhưng môt vài sự thay đổi cơ bản đã xuất hiện trong những năm qua. Đầu tiền, những ứng dụng trước đó được đặt tại data center đã bắt đầu được các tổ chức, doanh nghiệp dịch chuyển lên nền tảng cloud như Azure, AWS, Google cloud. Thứ hai, các doanh nghiệp cũng đang khai thác các dịch vụ SaaS như Office 365, Gmail, Dropbox vào trong môi trường làm việc và cả hai loại hình dịch vụ này đều được truy cập thông qua kết nối internet. Ta sẽ thấy càng ngày càng nhiều tổ chức, doanh nghiệp đang đầu tư vào xu hướng đó. Lúc này traffic đến các ứng dụng đặt tại các dịch vụ cloud sẽ đi đến data center thông qua các đường truyền MPLS và đi ra bên ngoài bằng các đường truyền Internet tại data center và ngược lại. Điều này dẫn đến mô hình kết nối tập trung về data center sẽ khiến cho các đường truyền MPLS vốn có băng thông thấp sẽ trở thành điểm tắt nghẽn.

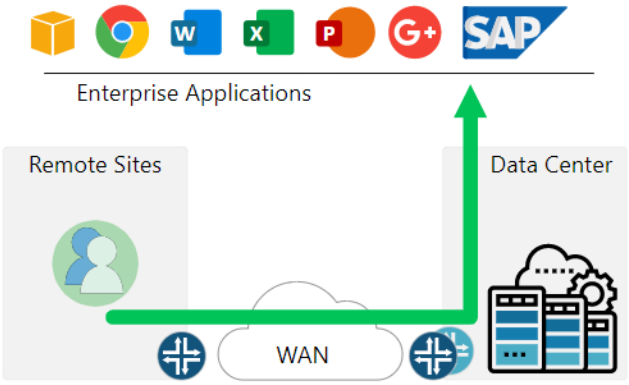


Figure 1. Traditional WAN architecture - Centralized Connectivity

- Mạng WAN truyền thống gặp rất nhiều vấn đề kết nối tới các dịch vụ điện toán đám mây như không đủ băng thông hoặc chi phí băng thông cao, downtime cao, hiệu suất SaaS kém, hoạt động phức tạp, quy trình làm việc phức tạp để kết nối các dịch vụ đám mây, thời gian triển khai dài, khả năng hiển thị ứng dụng bị hạn chế.

- Trước viễn cảnh đó mạng WAN truyền thống bộc lộ nhiều nhược điểm như:

  + Chi phí: việc nâng cấp đường truyền MPLS sẽ rất tốn kém vì băng thông MPLS không hề rẻ tí nào.

  + Hiệu suất ứng dụng thấp: traffic đi từ văn phòng đến Data center rồi di chuyển lên cloud sẽ làm tăng độ trễ dẫn đến hiệu suất của các ứng dụng SaaS trở nên kém đi.

  + Độ khả dụng: tất cả mọi traffic đổ về data center của công ty sẽ làm giảm tính khả dụng của các đường truyền từ đó gia tăng downtime.

  + Khó mở dộng: Trong kiến trúc mang diện rộng WAN cơ chế điều khiển và chuyển tiếp dữ liệu được tích hợp trên cùng một thiết bị vật lý và các thiết bị này ĐỘC LẬP với nhau. Vì vậy, nếu số lượng thiết bị ngày môt tăng sẽ gây nên sự phức tạp trong mạng lưới và gây khó khăn cho người quản trị viên trong quá trình vận hành và điều khiển hệ thống. Việc có bất kỳ thay đổi nào trong các thiết bị của mạng đều mất rất nhiều thời gian, chi phí cao. các mạng

mạch ảo MPLS thường rất phức tập và khó triển khai từ đó làm cho doanh nghiệp gặp khó khăn khi mở thêm các chi nhánh.

+ Tính bảo mật: một giải pháp cho rằng tại sao chúng tao không lắp đặt các đường truyền internet tại các văn phòng để truy cập các ứng dụng ở trên dịch vụ cloud vì giá thành rẻ và chất lượng tốt hơn. Nhưng giải pháp này gặp phải các vấn đề về bảo mật.

1.2 SD-Wan là gì

-Là một phương pháp để triển khai mạng diện rộng áp dụng các nguyên lý của Sofware-Defined Networking để giúp mạng WAN truyền thống đạt độ linh hoạt cao hơn.SD-WAN được thiết kế để đơn giản hóa việc quản lý lưu lượng mạng và phần tử trong hệ thống mạng bằng cách tách phần cứng mạng khỏi cơ chế điều khiển của nó, các thành phần điều khiển này được đưa về quản lý tập chung bằng phần mềm. Đồng thời cải thiện hiệu suất của các ứng dụng trong hệ thống mạng giúp đem lại trải nghiệm tốt nhất cho người dùng tại các vị trí phân táng như chi nhánh, văn phòng. Hơn nữa, Cisco SD-WAN còn đáp ứng được các nhu cầu về bảo mật cho doanh nghiệp lớn.

- Ứng dụng quan trọng của SD WAN là cho phép các công ty xây dựng mạng WAN có hiệu năng tương đương hoặc cao hơn bằng việc sử dụng các truy cập Internet thương mại giá rẻ thay thế một phần hoặc toàn bộ các công nghệ kết nối WAN truyền thống sử dụng kết nối riêng mắc tiền như MPLS

- Sự bùng nổ mức độ truy cập Internet đã định nghĩa lại kết cấu mạng WAN. Bây giờ là lúc các dịch vụ băng thông rộng được sử dụng nhiều trong kiến trúc mạng SD-WAN của doanh nghiệp. Ngoài các mối quan tâm về hiệu quả, về độ tin cậy, về bảo mật, chúng ta thường nghe nhắc đến các yếu tố như:

+ Làm thế nào bạn bảo mật một kết nối Internet để tạo ra một kết nối SD-WAN bảo mật?

+ Làm thế nào bạn chỉ ra các giới hạn về độ trễ và các giới hạn về hiệu năng của các kết nối bang thông rộng?

+ Làm thế nào bạn đảm bảo được các nhóm lưu lượng video không chèn lấn các ứng dụng kinh doanh quan trọng khác?

+ Nếu một doanh nghiệp có hàng trăm hoặc hàng ngàn các chi nhánh, làm thế nào bạn có thể đơn giản hóa việc cấu hình, quản lý và mở rộng?

- Đáp án cho các câu hỏi trên là chuyển đổi sang một nền tảng SD-WAN mới trong đó hợp nhất SD-WAN, routing, tối ưu hóa mạng WAN, tường lửa, phân tách mạng và các chức năng điều khiển bên trong một nền tảng platform duy nhất. SD-WAN cho phép tận dụng các kết nối băng thông rộng để truyền các lưu lượng của các ứng dụng thay vì chỉ dùng các đường truyền này như một giải pháp dự phòng. Bằng cách tận dụng hết các đường MPLS hoặc thậm chí thay thế MPLS bằng các giải pháp băng thông rộng, các doanh nghiệp có thể gia tăng băng thông WAN trong khi vẫn giảm thiểu các chi phí mạng WAN.

- Nếu so sánh với mạng WAN truyền thống, chức năng điều khiển hạ tầng mạng WAN được phân phối đều trên tất cả thiết bị mạng. Các router chỉ cần định tuyến lưu lượng mạng dựa trên địa chỉ TCP/IP và Access Control List. Cơ chế điều khiển và chuyển tiếp dữ liệu cùng nằm trên một thiết bị vật lý là router và mỗi thiết bị này hoạt động độc lập với nhau. Chính vì vậy, khi xây dựng một mạng diện rộng người quản trị sẽ phải tự tay thiết lập cấu hình cho từng thiết bị bên trong mạng, đối với các mạng WAN nhỏ thì vấn đề này không quá quan trọng, tuy nhiên trong bối cảnh hiện nay một mạng diện rộng WAN của doanh nghiệp lớn có thể tồn tại hàng trăm router tại nhiều chi nhánh khác nhau dẫn đến việc thiết lập cấu hình cho từng router trở thành một công việc khó khăn, và gia tăng sự phức tạp trong mạng lưới gây khó khăn cho người quản trị mạng trong quá trình vận hành và điều khiển hệ thống. Hơn nữa trong quá trình làm việc chỉ cần một sai sót nhỏ của con người thì cả hệ thống sẽ không thể hoạt động được, việc dò tìm lỗi và xử lý là một công việc không hề dễ dàng gì.

- Các chính sách mạng không đồng nhất dẫn đến mỗi lần thực hiện một chính sách thì người quản trị mạng phải cấu hình lại hàng ngàn thiết bị. Ví dụ trong một doanh nghiệp lớn, mỗi khi một máy chủ được phát sinh thì người quản trị phải mất hàng giờ, thậm chí là vài ngày để thực hiện cấu hình cần thiết. Tính

phức tạp của mạng WAN truyền thống làm cho công việc này trở nên khó khăn đối với các nhà quản trị để có thể áp dụng một chính sách người dùng, QoS hay các quy tắt bảo mật.

1.3 Các tính năng nổi bật của SD-Wan

- Tính sẵn sàng (High availability): SD-WAN cung cấp khả năng linh hoạt làm giảm tối đa thời gian ngừng mạng. Công nghệ phải có tính năng phát hiện thời gian thực của sự cố mất kết nối và tự động chuyển sang kết nối khác để hoạt động.
- Chất lượng dịch vụ (QoS): SD-WAN hỗ trợ chất lượng dịch vụ bằng cách ưu tiên mức độ ứng dụng, ưu tiên băng thông cho các ứng dụng quan trọng nhất. SD WAN sẽ lựa tuyến kết nối động, gửi ứng dụng trên tuyến nhanh hơn hoặc thậm chí tách ứng dụng chạy trên cả hai tuyến để cải thiện hiệu suất.
- Bảo mật (Security): So với MPLS, SD-WAN tận dụng các công cụ bảo mật (IPSEC) để xác thực, giám sát và mã hóa kênh kết nối.
- Quản trị và khắc phục sự cố: SD-WAN cung cấp giao diện đồ họa (GUI) được ưu tiên hơn giao diện dòng lệnh (CLI) giúp người quản trị lựa chọn tuyến tự động, cấu hình và quản lý tại trung tâm cho các thiết bị đầu cuối.
- Cân bằng tải (load balancing): khả năng bao quát toàn cục về trạng thái mạng, SD-WAN thực hiện kỹ thuật chia tải lưu lượng truy cập mạng bằng cách yêu cầu chuyển tuyến mới theo tình trạng mạng hiện tại nhằm đem đến trải nghiệm người dùng tốt nhất.

1.4 SD-Wan hoạt động như thế nào?

-Về cơ bản, SD-Wan giúp bộ phận IT kiểm soát toàn bộ mạng Wan, mạng biên, thậm chí cloud như là 1 mạng thống nhất, mà không có sự mất mát về mặt tính năng nào.

- Giải pháp SD-WAN dùng phần mềm và các chức năng điều khiển để điều hướng lưu lượng mạng trên mô hình mạng WAN. SD-WAN quản lý lưu lượng dưa trên các yếu tố là độ ưu tiên lưu lượng mạng của ứng dụng, chất lượng dịch vụ QoS và các yêu cầu bảo mật. Mô hình mạng WAN truyền thống, chức năng

điều khiển hạ tầng mạng WAN được phân phối đều trên các thiết bị mạng (router,…). Các router chỉ định tuyến lưu lượng mạng dưa trên địa chỉ TCP/IP và các Access Control List (Danh sách các thiết bị được quyền truy cập tài nguyên).

- Khi SD-WAN gửi các lưu lượng mạng đi đến cloud như SaaS hay IaaS thông qua kết nối Internet, các người dùng cuối sẽ nhận được chất lượng truy cập tốt nhất. Tuy nhiên, không phải tất cả các lưu lượng đi đến cloud hay các lưu lượng web đều đc đối xử như nhau. Nhiều ứng dụng cloud và ccác nhà cung cấp dịch vụ cloud áp dụng các cơ chế bảo mật mạnh mẽ. Việc truy cập trực tiếp các ứng dụng này từ các chi nhánh thông qua Internet sẽ cần các cơ chế bảo mật để bảo vệ doanh nghiệp khỏi các mối đe dọa.

- Sự thông minh và khả năng nhận dạng các ứng dụng khi chúng sử dụng mạng cho phép SD-WAN định tuyến đường đi (path) cho các lưu lượng mạng dưa trên ứng dụng chứ không còn chỉ đơn giản dựa trên TCP/IP.

1.5 SD-WAN sử dụng bất kỳ công nghệ truyền dẫn nào, bao gồm MPLS, băng thông rộng và LTE

- Giải pháp SDWAN hỗ trợ nhiều phương tiện truyền dẫn (kết nối)khác nhau. Người dùng có thể dễ dàng thêm bất kỳ loại kết nối vào mạng WAN, từ MPLS (chuyển mạch nhãn đa giao thức) truyền thống, đường truyền kết nối internet dành riêng (Dedicated), kết nối băng thông rộng (Broadband), hay thậm chí kết nối không dây như 3G/4G/LTE và kết nối vệ tinh. Mạng SD-WAN sẽ áo hóa và xem các dịch vụ này như những tài nguyên mạng.

- Ngày nay, với xu thế công nghệ, nhiều người dùng có xu hướng từ bỏ công nghệ truyền thống như MPLS, chuyển sang công nghệ mới như VPN (mạng riêng ảo), Internet. Tuy vậy, với một số lĩnh vực đặc thù như ngành tài chính, luật và chăm sóc sức khỏe y tế, việc bảo mật thông tin cá nhân là quan trọng, và được quy định bởi các chế tài, việc duy trì một mạng dành riêng là yêu cầu bắt buộc, đồng thời đảm bảo việc kết nối dễ dàng, thuận tiện ở mức quốc gia và toàn cầu, mà vẫn phải tuân theo chính sách bảo mật chung của doanh nghiệp. Bên

cạnh đó, cần tính toán tới khả năng thay đổi theo xu hướng và nhu cầu thị trường, việc mở rộng điểm kết nối, cũng như yêu cầu thay đổi băng thông, lúc đó, giải pháp SD-WAN là lựa chọn tối ưu.

1.6 Vì sao sử dụng SD-Wan?

- Với SD-WAN chúng ta không còn phụ thuộc vào đường truyền MPLS để kết nối giữa các site, có nhiều lựa chọn hơn, đó có thể là đường truyền Internet Broadband, LTE…, với SD-WAN đường truyền WAN lúc này chỉ là nền tảng để tạo các overlay link để kết nối giữa các site. Nếu bạn nhìn lại những ứng dụng mà chúng ta sử dụng suốt những năm qua như voice, video conference… những ứng dụng này sẽ bị ảnh hưởng đáng kể bởi các vấn đề mất gói tin (packet loss), độ trễ, độ nhiễu của đường truyền. Lấy ví dụ về voice ip, chỉ cần 2% mất gói tin đã đủ làm người bên kia không thể hiểu được những gì bạn nói. SD-WAN giúp bạn thấy được đường truyền WAN của bạn đáp ứng như thế nào từ góc độ chất lượng dịch vụ, và bắt đầu routing dựa trên đó. Sẽ không có BGP, OSPF mà giờ đây chất lượng dịch vụ sẽ quyết định đường nào là tối ưu nhất, qua đó các ứng dụng quan trọng trong kinh doanh của các tổ chức, ứng dụng có cơ hội được trải nghiệm một cách tốt nhất.

-SD-WAN được thúc đẩy bởi 3 yếu tố là hiệu quả, trải nghiệm và bảo mật.

- Khi nói đến yếu tố hiệu quả, hệ thống mạng đang thay đổi, các doanh nghiệp hiện tại đang sử dụng nhiều đường truyền WAN như MPLS, VPN tunnel, Internet… cho việc trao đổi dữ liệu. Điều này dẫn đến nhu cầu làm sao có thể quản lý các đường truyền WAN này một cách hiệu quả nhất.
- Với yếu tố trải nghiệm, hiện nay với sự bùng nổ của các dịch vụ cloud, tất cả các doanh nghiệp, nhà cung cấp dịch vụ đều quan tâm đến chất lượng của các đường truyền WAN mà họ đang sử dụng ảnh hưởng thế nào đến các dịch vụ mà họ cung cấp trên đó. Vì vậy hệ thống mạng hiện nay cần phải có khả năng xác định được những yếu tố nào ảnh hưởng đến việc trao đổi dữ liệu, trải nghiệm ứng dụng khi ứng dụng đó chạy trên các đường truyền WAN khác nhau. Ví dụ phòng IT cung cấp giải phải pháp video conference cho toán bộ công ty bao gồm hội sở và các chi nhánh, cũng như với đối tác, thì cần phải

biết được chất lượng của dịch vụ này khác nhau như thế nào khi chạy trên đường truyền MPLS hoặc đường truyền Internet từ đó nắm bắt được những yếu tố nào ảnh hưởng đến chất lượng của dịch vụ.

- Và yếu tố cuối cùng được quan tâm nhiều nhất hiện nay là bảo mật, tất cả tổ chức cần phải có sự kiểm soát chặt chẽ về bảo mật, và cần có khả năng giảm thiểu các mối đe dọa hiện có, đang diễn ra, hoặc đang phát triển đối với hệ thống mạng liên quan đến việc sử dụng các đường truyền WAN.

- Hiện tại, các doanh nghiệp đều đang sử dụng cùng lúc nhiều loại đường truyền WAN khác nhau cho việc trao đổi dữ liệu không chỉ giới hạn ở một hoặc hai. Trong đó có thể có MPLS, Metro Ethernet, Internet Broadband, LTE, private line. Vì vậy khi nhắc đến yếu tố hiệu quả và trải nghiệm, nghĩa là với việc sử dụng nhiều đường truyền WAN, các tổ chức, doanh nghiệp sẽ không muốn một vài đường truyền chỉ được sử dụng trong trường hợp dự phòng khi có sự cố xảy ra với các đường truyền còn lại, đây là một sự lãng phí lớn. Cần phải có giải pháp kết hợp các đường truyền hiện có để tối ưu việc trao đổi dữ liệu một các đơn giản nhất. Song song với việc đó vũng cần phải đảm bảo yếu tố bảo mật khi sử dụng nó. Mọi thứ phải được mã hóa, mọi thứ phải được bảo vệ, Những điều này đã thúc đẩy cho sự phát triển của SD-WAN.

1.7 Các loại giải pháp SD-Wan

- Hiện nay, trên thị trường có rất nhiều thương hiệu nổi tiếng đang triển khai giải pháp công nghệ SD-WAN như các giải pháp công nghệ SD-WAN của Cisco công nghệ SD-WAN của Fortinet, Peplink, Zyxel, Sophos,…

- Cisco cung cấp 2 giải pháp SD-WAN là Meraki và Viptela. Cả 2 sản phẩm đều áp dụng giải pháp SD-WAN và có vài tính năng trùng nhau. Tuy nhiên, mỗi sản phẩm đều hướng đến một thị trường khác nhau.

+ Meraki: là mô hình SD-WAN cho các doanh nghiệp nhỏ, và ít phức tạp hơn Viptela.

+ Viptela: là môt hình mạng SD-WAN nhiều tính năng hơn, thích hợp cho các cơ sở hạ tầng mạng của các doanh nghiệp lớn.

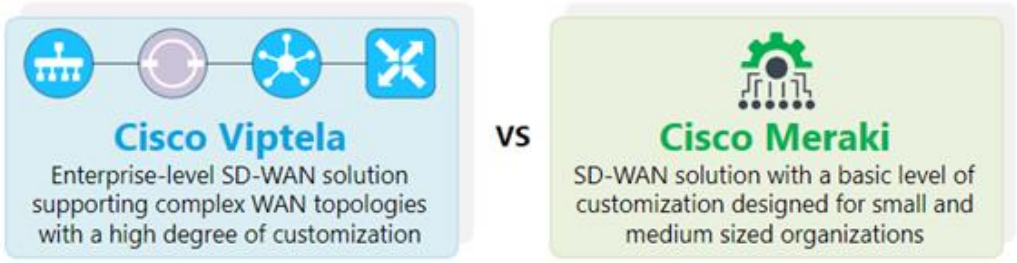
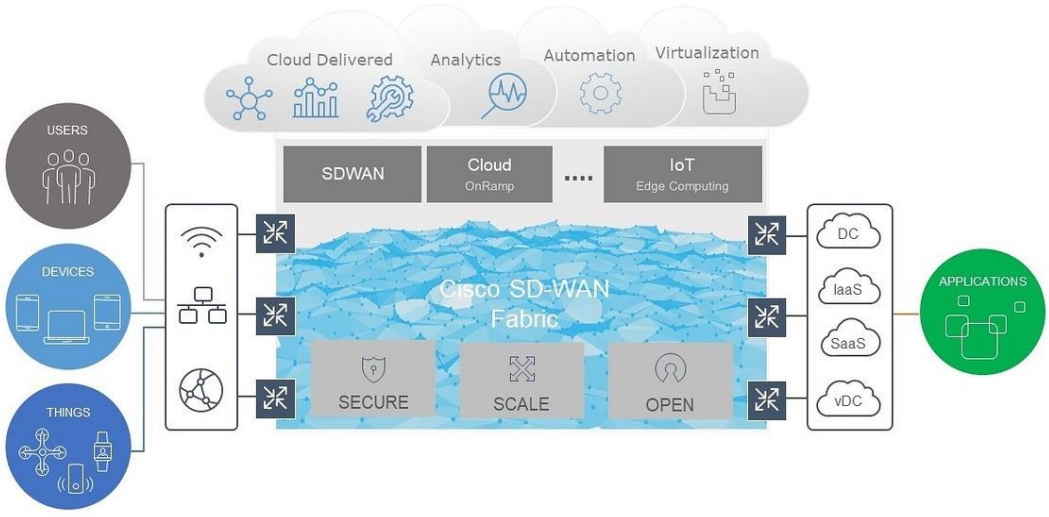


Figure 7. Cisco's SD-WAN solutions

1.8 Cisco SD-WAN

1.8.1 Tổng quan về giải pháp Cisco SD-WAN

- Giải pháp Cisco SD-WAN là dựa trên kiến trúc SD-WAN mà hãng Cisco cung cấp tới các doanh nghiệp cho phép chuyển đổi kỹ thuật số, đám mây doanh nghiệp. Nó tích hợp đầy đủ các giao thức định tuyến, bảo mật, chính sách và điều phối vào các mạng quy mô lớn. Cisco SD-WAN có hỗ trợ multi-tenancy (nhiều khách hàng cùng sử dụng chung cơ sở dữ liệu nhưng lại hoàn toàn độc lập với nhau) hoặc được phân phối trên nền tảng đám mây với tính tự động hoá cao, an toàn, có thể mở rộng và nhận biết ứng dụng với các phân tích phong phú như phân tích ứng dụng, các kết nối, lưu lượng mạng,…



- Công nghệ Cisco SD-WAN giải quyết các vấn đề và thách thức của việc triển khai mạng. Một số lợi ích bao gồm:

+ Quản lý tập trung và quản lý chính sách, cũng như đơn giản hoá hoạt động, giúp giảm thời gian xây dựng và triển khai.

+ Tận dụng hiệu quả các công nghệ WAN để cắt giảm chi phí và tăng tính đa dạng trong kết nối. Điều này có nghĩa là các kiểu truyền tải có thể là bất kỳ kiểu truyền tải nào, chẳng hạn như Internet, MPLS, 3G/4G/LTE, vệ tinh hoặc các đường truyền thuê bao riêng.

+ Triển khai linh hoạt. Do sự tách biệt giữa control plane và data plane, thiết bị có thể được triển khai tại cơ sở hoặc trên đám mây hoặc kết hợp cả hai.

+ Bảo mật mạnh mẽ và toàn diện bao gồm khả năng mã hoá dữ liệu mạnh mẽ, phân đoạn mạng đầu cuối, nhận dạng chứng chỉ của thiết bị với các chính sách, kết hợp cùng với tường lửa và dịch vụ khác.

+ Kết nối liền mạch giữa các chi nhánh, đám mây và mạng WAN.

+ Khả năng hiển thị và nhận biết ứng dụng với Service-Level Agreement (SLA) theo thời gian thực.

+ Tự động hoá tối ưu các ứng dụng đám mây (SaaS, IaaS), dẫn đến hiệu suất ứng dụng được cải thiện cho người dùng.

+ Khả năng phân tích chi tiết cho phép khắc phục sự cố nhanh chóng và đưa ra các đề xuất để lập kế hoạch phân phối tài nguyên hiệu quả.

1.8.2 Các tính năng nổi bật trong giải pháp Cisco SD-WAN

-Hiện nay, giải pháp Cisco SD-WAN được sử dụng chính cho bốn trường hợp sau:

+ Dùng cho việc tự động và kết nối an toàn giữa các văn phòng, trung tâm dữ liệu và các đám mây công cộng/riêng tư thông qua các kiểu truyền tải độc lập.

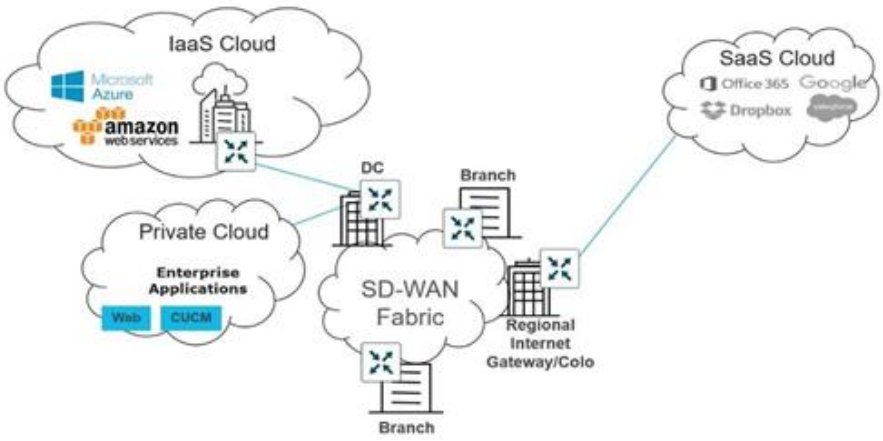
+ Dùng cho việc tối ưu hoá hiệu suất ứng dụng nhằm cải thiện trải nghiệm sử dụng ứng dụng cho người dùng tại các văn phòng.

+ Dùng cho việc truy cập Internet trực tiếp một cách an toàn.

+ Dùng cho việc kết nối các văn phòng với các ứng dụng đám mây qua một đường đi tối ưu và thông qua các điểm Colocation/Exchange để có thể áp dụng các dịch vụ bảo mật.

-Mạng WAN tự động và kết nối an toàn – Secure Automated WAN

- Cisco SD-WAN là một mô hình mạng tự động và bảo mật tập trung vào việc cung cấp các kết nối an toàn giữa các chi nhánh, trung tâm dữ liệu, các địa điểm, các đám mây công cộng và riêng tư qua một mạng truyền tải độc lập. Việc tự động này cũng bao gồm việc triển khai các dịch vụ, chính sách cho các thiết bị một cách đơn giản bằng cách sử dụng các mẫu chính sách phổ biến có sẵn và có thể mở rộng trong việc quản lý tự động, điều khiển từ xa.



Mạng WAN tự động kết nối an toàn tới các dịch vụ đám mây

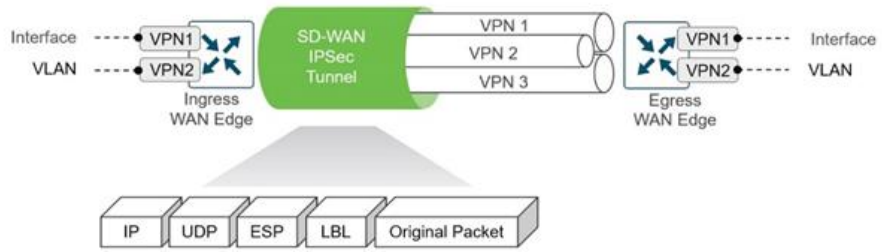
-Trong Cisco SD-WAN có các đặc tính phù hợp cho việc tự động kết nối an toàn cho mạng WAN:

+ Cấu hình tự động hoàn toàn - Zero-touch provisioning ZTP: Là tính năng cung cấp điều khiển từ xa cho bộ định tuyến ở bất kỳ đâu trong mạng WAN. Bộ định tuyến WAN Edge sẽ tự động phát hiện các controllers và tự động tải các cấu hình, chính sách đã được thiết lập trước đó trước khi thiết lập các đường hầm IPsec để kết nối tới các thành phần còn lại trong mạng. Tính năng tự động này giúp giảm chi phí nhân sự IT

+ Mở rộng băng thông: cho phép tận dụng các kết nối băng thông rộng điều hướng các lưu lượng của các ứng dụng thay vì chỉ dùng các đường truyền này

như một giải pháp dự phòng. Bằng cách tận dụng hết các đường MPLS hoặc thậm chí thay thế MPLS bằng các giải pháp băng thông rộng, các doanh nghiệp có thể gia tăng băng thông WAN trong khi vẫn giảm thiểu các chi phí mạng WAN.

+ Phân đoạn VPN: Việc tách biệt lưu lượng truy cập vào bộ định là một giải pháp nhằm tăng tính bảo mật cho hệ thống mạng. Lưu lượng truy cập vào bộ định tuyến sẽ được gán một VPN, giúp không chỉ tách biệt lưu lượng người dùng mà còn tách biệt thông tin bảng định tuyến. Điều này đảm bảo rằng lưu lượng người dùng trong một VPN không thể truyền hay nhận dữ liệu từ VPN khác trừ khi được cấu hình để làm như vậy. Khi lưu lượng được truyền qua WAN, một nhãn sẽ được chèn sau ESP header để xác định VPN mà lưu lượng của người dùng thuộc về.



Phân đoạn end-to-end

+ Quản lý tập trung: vManage thường đảm nhận việc quản lý lỗi, cấu hình, theo dõi hiệu suất hệ thống và bảo mật. vManage còn đem lại sự đơn giản trong việc triển khai các dịch vụ, chính sách, định tuyến bằng những mẫu chính sách có sẵn, dẫn đến việc giảm thời gian triển khai.

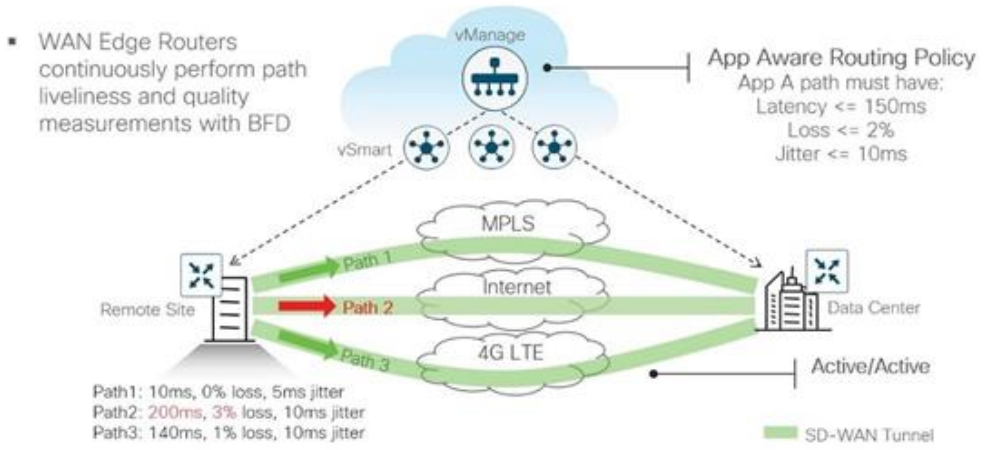
1.8.3 Tối ưu hoá hiệu suất ứng dụng

- Hiện nay, có rất nhiều vấn đề trong mạng có thể ảnh hưởng đến hiệu suất ứng dụng của người dùng, chẳng hạn như mất gói tin(packet-loss), đường truyền bị tắc nghẽn, độ trễ cao và việc lựa chọn đường đi trong mạng WAN không được tối ưu. Việc tối ưu hóa tải nghiệm ứng dụng cho người dùng luôn là mục tiếp hàng đầu để thúc đẩy nâng suất làm việc. Giải pháp Cisco SD-WAN có thể giảm thiểu sự mất mát gói tin, chập chờn và độ trễ cũng như khắc phục các lỗi chuyển tiếp gói tin của mạng WAN bằng cách lựa chọn những con đường đi tối ưu nhất.

- Công nghệ Cisco SD-WAN sẽ giúp giải quyết vấn đề tối ưu hoá hiệu suất ứng dụng nhờ vào các đặc tính sau:

+ Định tuyến nhận biết ứng dụng – Application-Aware Routing: cho phép tạo các chính sách SLA (service level argeement) tùy chỉnh cho lưu lượng mạng và đo lường hiệu suất ứng dụng theo thời gian thực bằng BFD. Lưu lượng mạng của ứng dụng được định tuyến đến các kết nối hỗ trợ SLA được thiết lập dành cho ứng dụng đó. Khi bị giảm hiệu suất lưu lượng truy cập của ứng dụng có thể được chuyển hướng đến các đường dẫn khác tối ưu hơn.

+ Chất lượng dịch vụ (QoS): QoS bao gồm phân loại, sheduling, queueing, shaping và kiểm soát lưu lượng truy cập trên các cổng interface của bộ định tuyến WAN. Tính năng QoS được thiết kế để giảm thiểu độ trễ, chập chờn và mất gói của các luồng ứng dụng quan trọng.



Định tuyến nhận diện ứng dụng

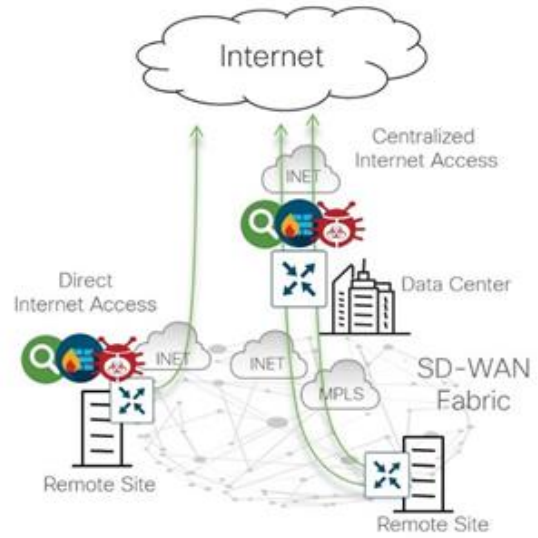
+ Trong hình trên path 2 không đáp ứng được yêu cầu của ứng dụng A nào đó nên kết nối đó sẽ không được dùng để định tuyến lưu lượng mạng của ứng dụng.

1.8.4 Truy cập Internet trực tiếp an toàn

- Trong mạng WAN truyền thống, lưu lượng mạng đi đến Internet từ các chi nhánh sẽ được điều chỉnh lại ở trung tâm dữ liệu, nơi lưu lượng truy cập sẽ được kiểm tra bảo mật trước khi lưu lượng mạng đi từ chi nhánh ra ngoài Internet và ngược lại. Theo thời gian, nhu cầu về lưu lượng truy cập Internet ngày càng tăng

và ngày càng có nhiều công ty sử dụng ứng dụng của họ trên thông qua nền tảng đám mây. Vì vậy, cách mà lưu lượng truy cập phải đi qua một trung tâm dữ liệu như vậy sẽ tăng độ trễ và ảnh hưởng đến hiệu suất ứng dụng.

- Truy cập Internet trực tiếp (Direct Internet Access - DIA) có thể giúp giải quyết những vấn đề về độ trễ và tăng hiệu suất ứng dụng bằng cách cho phép chi nhánh truy cập vào Internet trực tiếp thông qua một VPN.



Truy cập Internet trực tiếp so với truy cập Internet tập trung

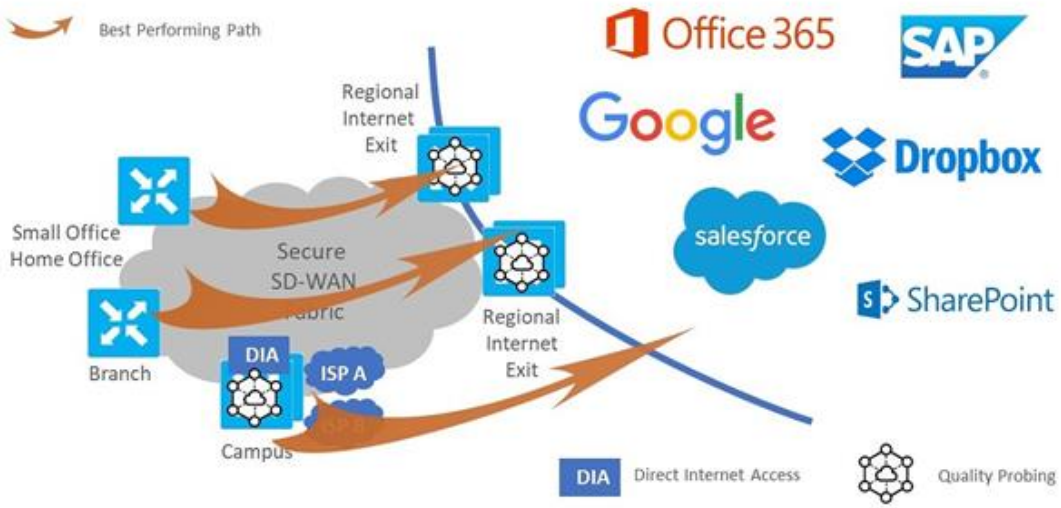
- Cisco SD-WAN có thể giúp giải quyết vấn bảo mật khi truy cập internet của công ty bằng cách tận dụng các tính năng bảo mật của SD-WAN được nhúng trên các thiết bị IOS XE SD-WAN hoặc Các tính năng bảo mật SD-WAN của IOS XE bao gồm các Firewall để nhận biết các ứng dụng doanh nghiệp, hệ thống sẽ phát hiện xâm nhập (IDS)/hệ thống ngăn chặn xâm nhập (IPS), bảo mật lớp DNS/Web, Lọc URL, SSL Proxy và bảo vệ trước các phần mềm độc hại (AMP).

1.8.5 Kết nối đa đám mây – Multicloud Connectivity

- Với sự phát triển về tốc độ kết nối ngày càng nhanh như hiện nay thì có rất nhiều ứng dụng đã và đang có trên rất nhiều đám mây và có thể truy cập qua nhiều phương tiện, thiết bị. Kết nối đa đám giúp tối ưu và đảm bảo độ bảo mật trong kết nối giữa các khu vực từ xa với các ứng dụng IaaS hay SaaS.

- Trong Cisco SD-WAN có tính năng Cloud onRamp cho các ứng dụng đám mây IaaS, SaaS và các điểm Colocation/Exchang nhằm tự động đưa ra và điều hướng

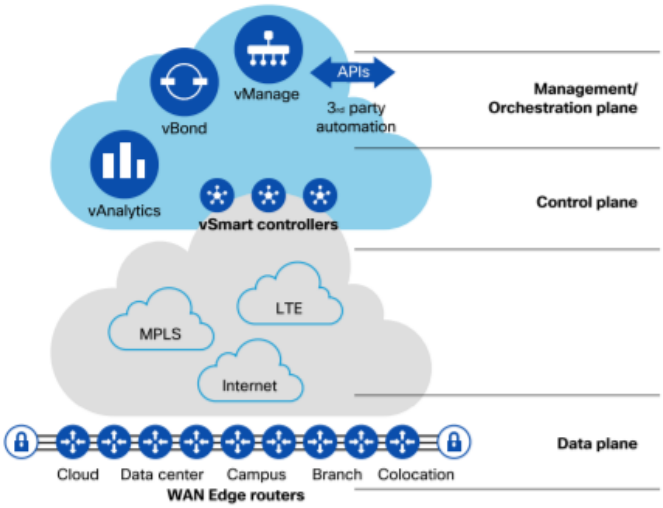
những lưu lượng từ các văn phòng đi tới các nhà cung cấp dịch vụ đám mây một cách tối ưu nhất.



1.9 Cisco component

- Cisco Viptela SD-WAN được cấu tạo từ 4 plane(lớp): Orchestreation plane, Management plane, control plane và data plane. Mỗi plane có một chức năng riêng và được tách biệt hoàn toàn với các plane khác. Ví dụ, nếu ta thay thế một thiết bị ở data plane thì việc đó không ảnh hưởng đến các plane khác và ngược lại.

- Nếu so sánh với mạng WAN truyền thống, mỗi thiết bị đều đảm nhiệm vai trò của từng plane. Forwarding packet (data plane), chạy giao thức OSPF, BGP, PIM (control plane), được quản lý thông qua CLI (management plane).



1.9.1 Management Plane

- vManager

- vManager đóng vai trò như một hệ thống quản lý tập chung. Cisco vManage cung cấp bảng điều khiển dưới dạng giao diện người dùng để các quản trị viên có thể tương tác, thiết lập và quản lý các thiết bị vEdge nằm bên trong cấu trúc mạng. Về bản chất, Cisco vManage là phần mềm chạy trên server đặt tại các vị trí trung tâm như data center.

-vManager có vai trò thu thập các dữ liệu, phân tích và cảnh báo khi có một sự kiện nào đó xảy ra trong mạng.

- vManager dùng để lưu trữ các certificate credentials(thông tin xác thực chứng chỉ), configuration (cấu hình) cho các thành phần thiết bị mạng vEdge. Khi các thiết bị vEdge tham gia vào mạng lưới, chúng sẽ gửi các request yêu cầu vManage gửi các thông tin cấu hình và chứng chỉ (certificate) cho chúng, vManage nhận dược request ngay lập tức sẽ đẩy các certificate va configuration cho các thiết bị vEdge.

1.9.2 Control Plane

- Control connection

- Control connection là loại kết nối nằm ở control plane dùng để xác thực, và trao đổi thông tin giữa các thiết bị trong hệ thống mạng. Control connection có 2 loại

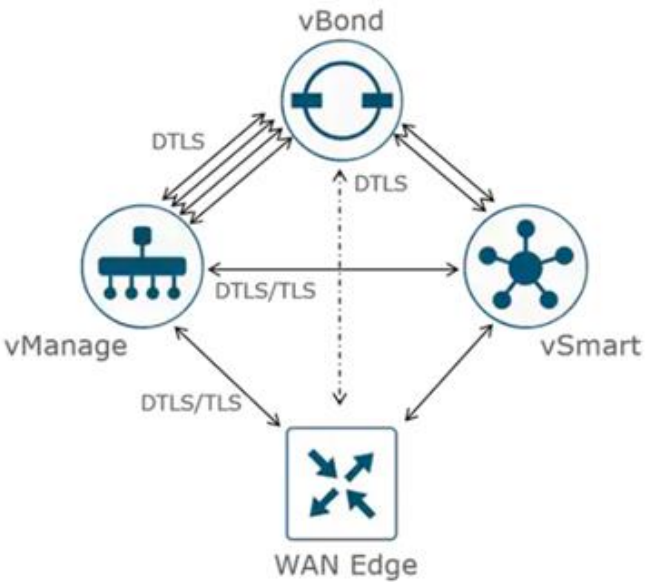
là DTLS tunnel hoặc TLS tunnel ứng với 2 giao thức tầng transport là UDP và TCP.

- Theo như thiết lập mặc định tất cả thiết bị đều sử dụng kết nối DTLS để giao tiếp với nhau.

- Quá trình thiết lập control connection:

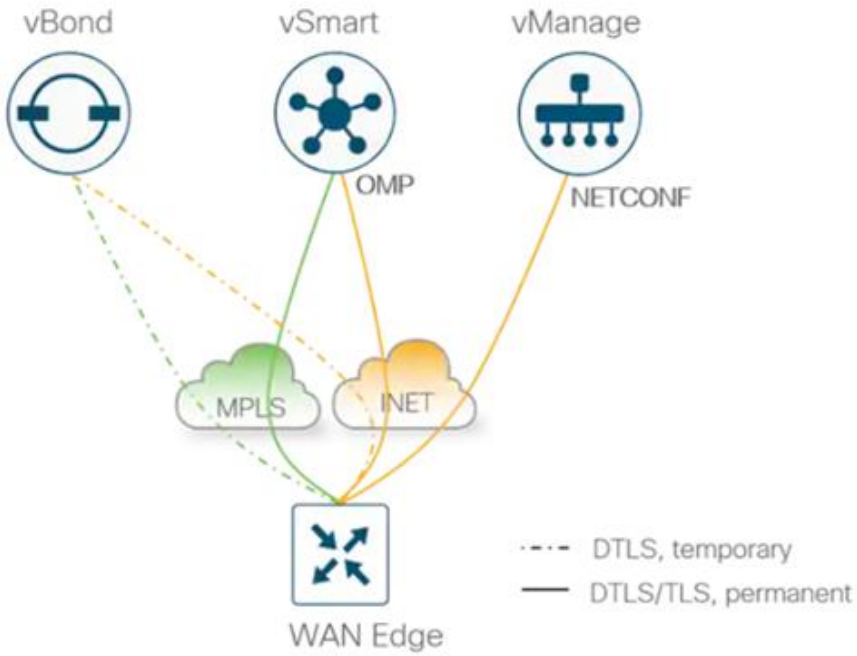
+ Router: Thiết bị WAN Edge sẽ cố gắng thiết lập control connection trên tất cả mọi phương tiện truyền dẫn ứng với interface của nó. Đầu tiên là thiết lập control connection với vBond orchestrator, tuy nhiên chỉ một control connection kết nối đến vBond ứng với một loại phương tiện truyền dẫn (một control connection ứng với MPLS, một với Internet) và kết nối này chỉ là tạm thời.

+ Controller: Tiếp theo WAN Edge router sẽ thiết lập một control connection vĩnh viễn trên một phương tiện truyền dẫn ứng với mỗi vSmart controller và MỘT vManage trong mạng lưới, khi quá trình kết nối này thành công WAN Edge router sẽ từ bỏ control connection với vBond.



- Không phải WAN Edge router đều kết nối với tất cả vSmart controller bên trong mạng lưới, điều này phụ thuộc vào sự thiết lập của người quản trị mạng. Thông thường chỉ cần WAN Edge thiết lập một.

- Control connection giữa các controller: vManage và vSmart controller sẽ liên lạc và xác thực với vBond controller, rồi thiết lập control connection (DTLS) với chính vBond controller, và sau đó vManage và vSmart sẽ thiết lập MỘT control connection với nhau. Mỗi core (lên đến 8) tương ứng trong vManage và vSmart sẽ duy trì một control connection với một vBond. Ví dụ vSmart có 2 vCPUs thì sẽ có 2 controll conection được tạo với vBond.



- Khi control connection được tạo giữa vManage và WAN Edge router, NETCONF được dùng để giúp vManage cung cấp các thông tin cho vEdge router, vEdge còn thiết lập quan hệ peer-to-peer thông qua giao thức OMP với vSmart

- vSmart Controller

- vSmart Controller được xem như bộ não của kết cấu mạng Cisco SD-WAN có vai trò giám sát control plane của mạng lưới Cisco SD-WAN, thiết lập, thay đổi và duy trì các kết nối tạo nên cấu trúc mạng Cisco SD-WAN.

- vSmart controller thường sẽ được cài đặt trước các thông tin cho phép vSmart xác thực tất cả các vEdge router muốn kết nối vào kết cấu của mạng. Việc xác

thực giúp đảm bảo chỉ nhựng thiết bị phù hợp mới được phép hoạt động trên mạng lưới. Sau mỗi lần xác thực thành công, các vSmart controller sẽ thiết lập một DTLS đến từng vEdge router. Sau đó các vEdge router và vSmart controller sẽ thiết lập quan hệ peer-to-peer trong giao thức OMP (Overlay Management Protocol OMP). OMP là một giao thức tựa như BGP, có thể quảng bá các routes, các giá trị next-hop, key và các thông tin chính sách cần thiết để duy trì mạng SDWAN. Từ đó vSmart Controller có thể xây dựng nên bảng định tuyến OMP. vSmart controller sẽ xử lý các OMP route được học từ các router SDWAN (hoặc từ các vSmart controller) để xác định được cấu trúc mạng và tính được đường đi tốt nhất đến mạng đích. Sau đó nó sẽ quảng bá các thông tin học được từ các routes này đến các vEdge router (hoặc vSmart controller) khác trong mạng.

- vSmart controller cũng triển khai các chính sách được tạo ra trên vManage, chẳng hạn như các chuỗi dịch vụ, các kỹ thuật lưu lượng, các phân mảnh trên sơ đồ VPN topology. Ví dụ khi có một chính sách tạo ra trên vManage cho một ứng dụng (chẳng hạn như Youtube) trong đó yêu cầu không được mất gói nhiều hơn 1% và độ trễ ít hơn 150ms, chính sách đó sẽ được tải xuống vSmart Controller. vSmart controller sẽ chuyển các chính sách này sang một định dạng mà các router SDWAN có thể hiểu. Sau đó các router sẽ tự động triển khai các chính sách mà không cần can thiệp bằng giao diện dòng lệnh CLI.

- AUTHORIZED LIST MODEL – Mẫu danh sách xác thực

- Tất cả thiết bị WAN Edge và controller phải xác thực với nhau thông qua authorized list model, tất cả thiết phải được xác thực trước khi khởi tạo control connection và tham gia vào cấu trúc mạng.

- Có 2 loại authorized list được phân phởi bởi vManage, một dành cho controllers và một dành cho WAN Edge:

  + Authorized controller list: danh sách này được tạo ra khi người quản trị tự tay kết nối các controller đến interface của vManage. Danh sách này sẽ được phân phối từ vManage đến các controllers và từ vBond đến vSmart controller

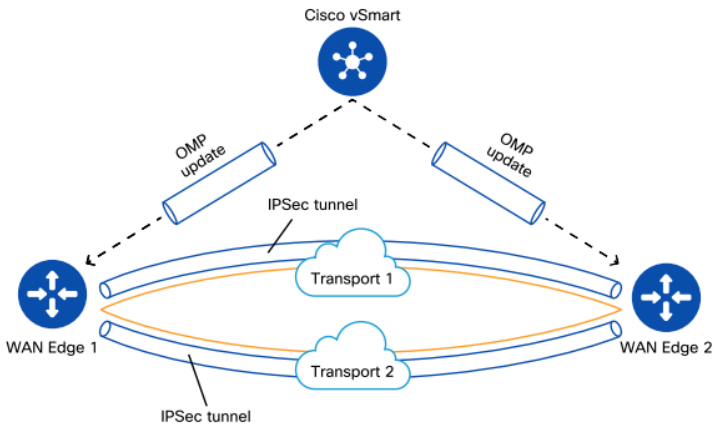
+ Authorized serial number list: là danh sách chứa mã số xác thực cho các thiết bị WAN Edge, danh sách này có thể được truy suất thủ công hoặc tự động từ vManage bởi người dùng có tài khoản xác thực Cisco CCO. Sau khi danh sách này được tải lên vManage thì vManage sẽ phân phối cho các controller khác

+ Với WAN Edge authorized serial number list, người quản trị có thể lựa chọn mức độ tin tưởng đối với mỗi WAN Edge router:

- Valid: router đã được xác thực và vận hành trên hệ thống mạng.
- Invalid: Router chưa được xác thực vì vậy không có control connection nào được khởi tạo với nó.
- Staging: Router được xác thực và khởi tạo control connection nhưng giao thức OMP sẽ không được sử dụng. Trạng thái này giúp ta kiểm tra router trước khi cho nó tham gia vào hệ thống mang.

+ OMP (Overplay Management Protocol) – OMP là giao thực định tuyến của Cisco có tính năng gần giống giao thức BGP.OMP được sử dụng bên trong các DTLS tunnel giữa các vSmart controller với nhau và giữa vSmart controller với vEdge router, giúp vận chuyển các thông tin control plane dùng thiết lập nên mạng overlay như route, next hop, key và thông tin chính sách. vSmart Controller hoạt động gần giống như BGP route reflector, nó nhận các route từ vEdge router, xử lý và thực thi chính sách lên đó, sau đó quảng bá các route cho router khác. OMP quảng bá 3 loại route từ vEdge router đến vSmart controller:

- OMP routes: Bản chất OMP là các route mà WAN Edge router học được từ giao thức định tuyến OSPF, EIGRP,… đi kèm với các thông tin khác như TLOC
- TLOC route: dùng để quảng bá các TLOC khác, bao gồm tập hợp các thông tin như TLOC public, private IP, Site ID, preperrence, encrytion key,...
- Service routes:



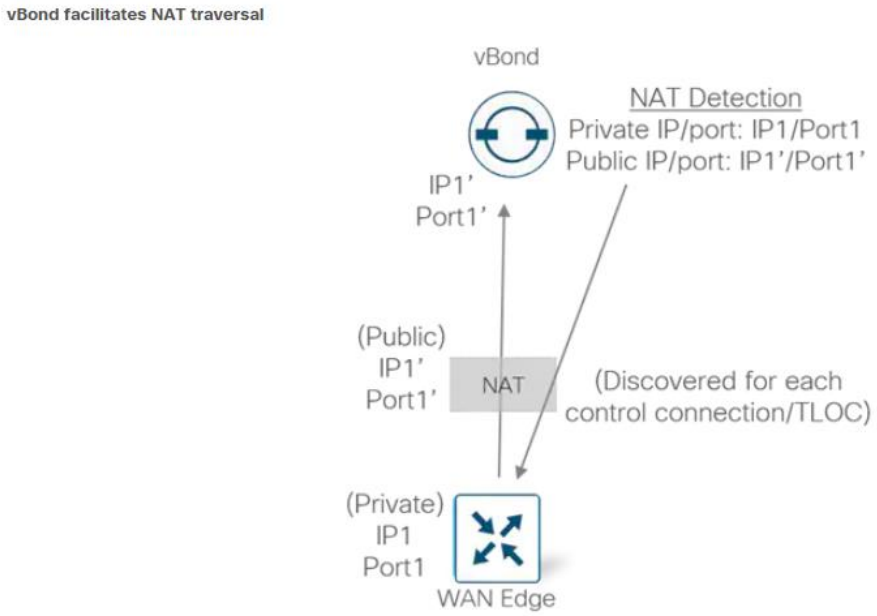
1.9.3 ORCHESTRATION PLANE

- vBond Orchestrator

- vBond Orchestrator có chức năng kết nối vSmart Controllers với vEdge router. Và xác thực các thiết bị đang muốn tham gia vào kết cấu mạng. Vì thế nó phải có một IP public riêng để các thiết bị có thể kết nối đến, xác thực và tham gia vào mạng.

- Control plane connection: mỗi vBond có một kết nối DTLS tunnel với từng vSmart controller trong cùng một vùng mạng. Ngoài ra vBond Orchestrator tạo kết nối DTLS tunnel với các vEdge router để xác thực chúng trước khi cho phép các router tham gia vào mạng.

- NAT traversal: Các vEdge router và vSmart controller dù có đứng sau một NAT thì vBond vẫn có thể kết nối chúng với nhau, giúp cho các vEdge router và controller biết được IP và port mapped/translated của chính chúng để chúng có thể quảng bá các thông tin đó khi khởi tạo control connection với nhau.



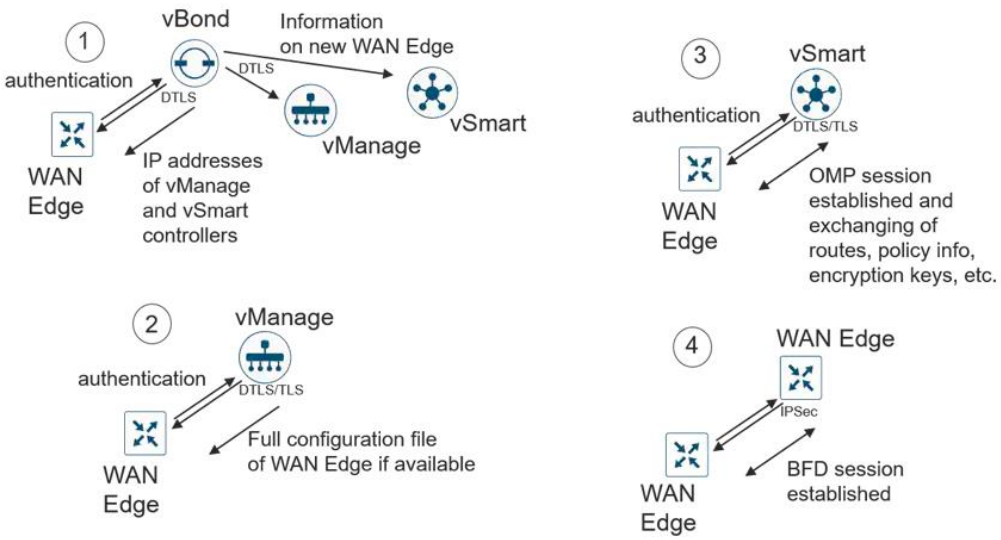
- Load balancing (cân bằng tải) – vBond Orchestrator thực hiện tính năng load balancing khi vùng mạng có nhiều vSmart controller.

- vBond Orchestrator tạo DTLS tunnel với vSmart Controller và Edge router để thực hiện việc xác thực nhằm đảm bảo chỉ có các thiết bị hợp lệ mới được phép tham gia vào cấu trúc mạng Cisco SD-WAN. Kết nối DTLS giữa vSmart Controller và vBond là kết nối lâu dài để vBond controller có thể thông báo cho vSmart controller khi vEdge router tham gia mạng. Kết nối DTLS giữa vEdge router và vBond là kết nối tạm thời vBond sẽ chia sẻ các thông tin mà vEdge dùng để kết nối đến vSmart, DTLS tunnel giữa vBond và vEdge chấm dứt khi vEdge kết nối đến vSmart.

- Đưa các thiết bị WAN Edge vào mạng

- Để tham gia vào mạng lưới, vEdge router cần phải thiết lập kết nối với vManage để nhận configuration (cấu hình), và kết nối với vSmart thì thiết bị mới tham gia vào mạng lưới. Tuy nhiên, để thấy được vManage và vSmart thì các router phải kết nối với vBond.

Figure 19. Bringing a WAN Edge into the overlay



1. Thông qua tiến trình thiết lập tự động (automated provisioning ZTP hay PnP), WAN Edge router tạo một DTLS tunnel với vBond để thực hiện quá trình xác thực (authentication). Sau khi quá trình xác thực hoàn tất, vBond gửi địa chỉ IP của vSmart controller và vManage cho WAN Edge router. vBond đồng thời phải thông báo cho vManage và vSmart biết về sự xuất hiện của WAN Edge router trong mạng lưới.

2. WAN Edge router thiết lập kết nối DTLS hoặc TLS với vManage và ngắt kết nối DTLS với vBond. WAN Edge router đồng thời xác thực với vManage, sau khi quá trình xác thực hoàn tất, vManage sẽ gửi configuration file (cấu hình) về các WAN Edge router.

3. WAN Edge router thiết lập kết nối DTLS/TLS với vSmart troller thông qua mỗi liên kết truyền dẫn tới vSmart controller đó. Sau khi quá trình xác thực hoàn tất. Giao thức OMP được thực hiện giúp router học được route, including prefixs, TLOCS, service routes, encryption keys, và policy (chính sách).

4. WAN Edge router cố gắng thiết lập các phiên BFD với các TLOC từ xa bằng Ipsec trên mỗi liên kết truyền dẫn. (cái này từ từ chỉnh lại).

TLOC - Transport Location: là điểm kết nối WAN Edge router và mạng WAN.

- Onboarding the WAN Edge router – WAN Edge router tham gia vào mạng

- Thông thường có hai cách giúp WAN Edge router tham gia vào mạng. Phương pháp đầu tiên là phương pháp thủ công (manual method), ta sẽ cấu hình router thông qua cửa sổ console. Phương pháp thứ hai là phương pháp thiết lập tự động, thông qua cơ chế Zero-Touch Provision (ZTP) hoặc Plug-and-play, với phương pháp này ta chỉ cần kết nối router vào mạng và bật nguồn, công việc thiết lập sẽ được tự động hóa.

- **Manual**:

  + Cấu hình IP và Gateway cho interface kết nối vào mạng của router, hoặc thiết lập DHCP cho router để nó nhận IP.

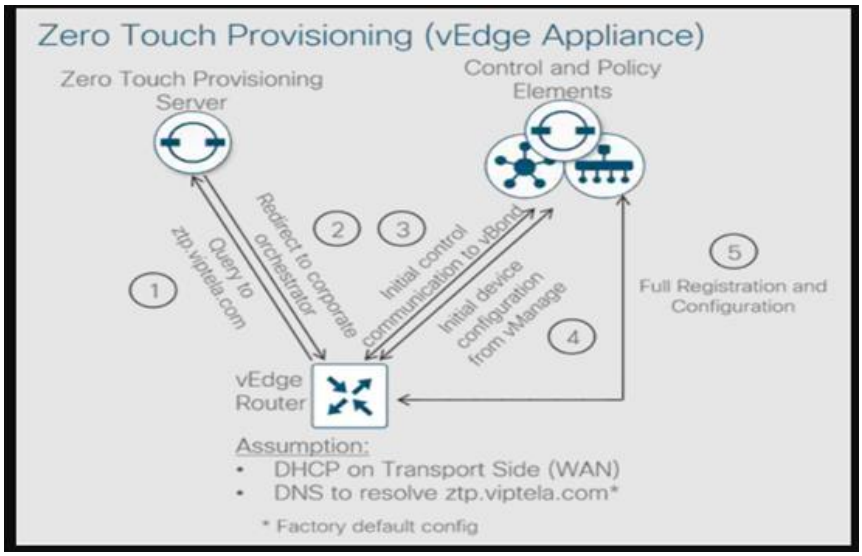
  + Thiết lập IP hoặc hostname của vBond cho router, nếu dùng hostname thì phải đảm bảo router có thể phân giải được

  + Thiết lập organizaiton name, ip hệ thống, ID của site,… blah blah mấy thứ linh tinh

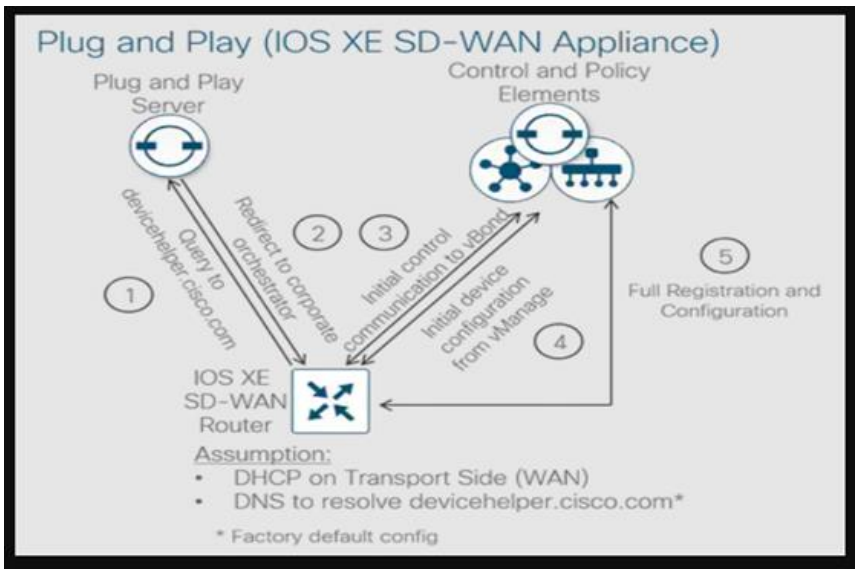
- **Automated Device Provisioning (ZTP or PnP)**

  + ZTP là cơ chế cấu hình tự động cho các thiết bị vEdge, PnP là cơ chế cấu hình tự động cho các thiết bị SD-WAN chạy HĐH IOS XE. Cả 2 cơ chế này khá giống nhau.

  + Khi các WAN Edge router kết nối mạng lần đầu tiên. Các vEdge router sẽ tự động kết nối với ZTP server ztp.viptela.com để lấy thông tin về vBond Orchestrator. Tương tự, đối với cơ chế PnP router sẽ truy cập đến PnP server devicehelper.cisco.com để lấy thông tin vBond Orchestrator mà nó sẽ kết nối đến. Sau khi đã có thông tin về vBond Orchetrator trong mạng lưới, các WAN Edge router sẽ kết nối đến vManage và vSmart controller để lấy cấu hình và giam gia vào mạng lưới.



Zero Touch Provisioning for vEdge devices



Plug and play for IOS XE SD-WAN devices

Tóm gọn như vậy: khi gắn router vào mạng ấy, vBond có nhiệm vụ nối cho mấy cái router đó biết về vManage và vSmart => router phải biết được IP của vBond - nó phải kết nối với vBond. Mà để kết nối được với vBond thì có 2 cách:

+ Thủ công: là ta cấu hình IP hoặc hostname của vBond cho router.

+ tự động: thông qua cơ chế ZTP, hoặc PnP router tự biết IP hoặc hostname của vBond.

1.9.4 DATA PLANE

- vEdge Router:

- Là thiết bị phần cứng hoặc phần mềm trên máy ảo, có nhiệm vụ vận chuyển dữ liệu đi khắp mạng lưới. Các thành phần chính của vEdge router gồm:

+ Kết nối DTLS – mỗi vEdge router sẽ thiết lập và duy trì một control plane connection với một vSmart Controller mà nó đang giao tiếp. Kết nối này chỉ được dựng lên sau khi quá trình xác thực được hoàn tất, kết nối DTLS giúp vận chuyển các payload đã được mã hóa từ vEdge router đến vSmart controller. Các payload sẽ chứa các thông tin giúp vSmart Controller có thể định hình nên network topology để từ đó tính toán ra route tốt nhất từ nguồn đến đích.

- Transport Locators - TLOC

-TOLC (transport locator): có thể xem đây chính là điểm kết nối giữa một thiết bị WAN Edge với một phương tiện truyền dẫn của mạng WAN. Một TLOC gồm ba thành phần chính là System-IP, Transport Color, Encapsulation Type.

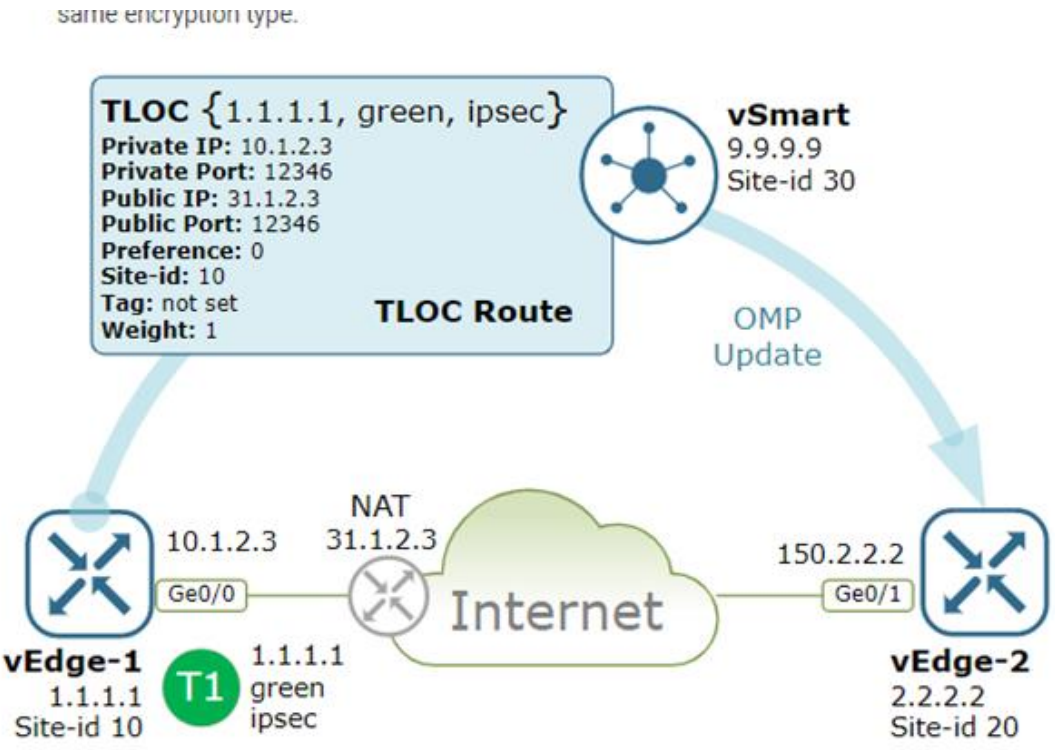


Figure 1. Cisco SD-WAN Forming an IPsec tunnel - Step 1

+ System-IP: là một số dùng để định danh thiết bị WAN trong mạng. Nó giống như Router-ID được dùng trong giao thức định tuyến BGP.

+ Transport Color: là tập hợp các màu dùng để biểu diễn các loại phương tiện truyền dẫn bên trong mạng WAN như MPLS, Internet, LTE, 5G,…

+ Encapsulation Type: giá trị này dùng để xác định một TLOC đang dùng loại tunnel (IPSec hoặc GRE) nào, để từ đó giúp hai TLOC kết nối với nhau.

- Khi một thiết bị vEdge kết nối vào internet tại interface G0/0, nó sẽ nhận đc IP/Mask/Default Gateway từ DHCP và nhận đc transport color và encapsulation type từ controller (hoặc là ta tự thiết lập). Sau đó nó sẽ cố gắng tạo kết nối đến các vBond/vManage/vSmart. Khi quá trình này hoàn tất nó sẽ nhận đc system-IP, transport color, encapsulation type. TLOC route sẽ đc vSmart quảng bá cho các thiết bị khác và ngược lại (vSmart quảng bá TLOC route của WAN Edge router khác cho vEdge ban đầu).

- Cuối cùng các vEdge sẽ có thể tạo tunnel Ipsec với nhau để tạo một phiên BDF.

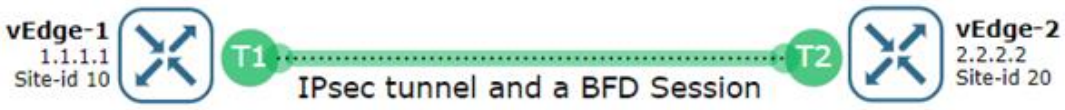


Figure 4. Cisco SD-WAN Forming an IPsec tunnel - Step 4

Chương 2: SD-Access

SD Access là một giải pháp được cung cấp bởi Cisco có thể đáp ứng được các nhu cầu quản lý về hệ thống mạng nhằm nâng cao năng suất, giảm chi phí và tránh gây lãng phí tài nguyên trong hệ thống mạng và tự động triển khai.

SD Access cung cấp một kiến trúc end-to-end một cách tự động cho người dùng, thiết bị,... trong một hệ thống mạng dựa trên các chính sách của doanh nghiệp, điều này đảm bảo các doanh nghiệp có những truy cập an toàn vào hệ thống của họ và nhiều lợi ích khác.

2.1 Tổng quan về SD-Access

2.1.1 Khái niệm SD-Access

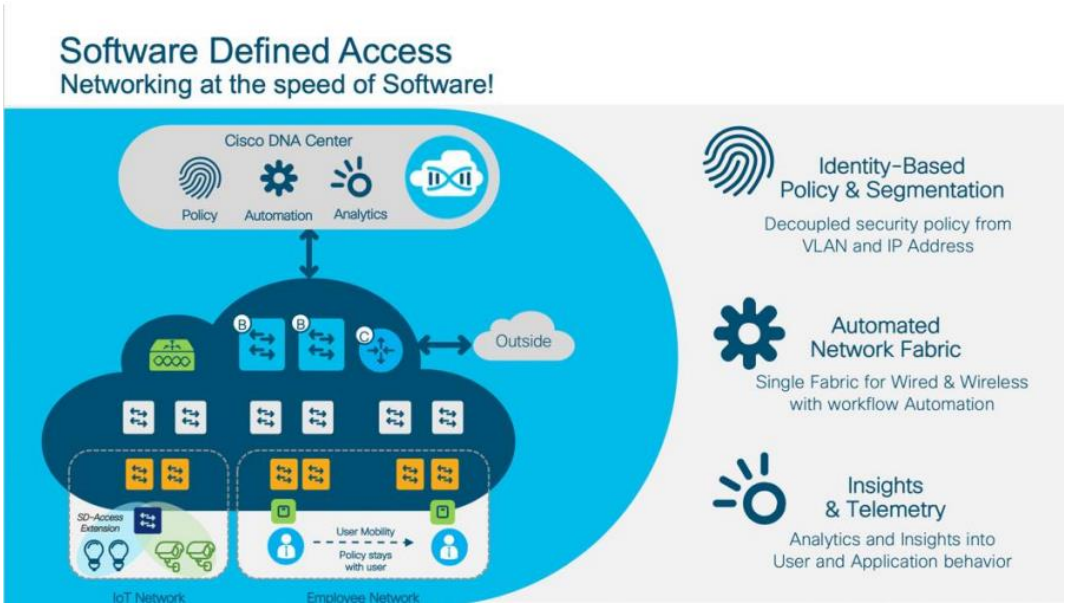
-SD Access là một giải pháp do Cisco cung cấp dựa trên chính sách và sự phân nhóm từ mạng biên cho tới các ứng dụng. SD Access được cung cấp thông qua Cisco Digital Network Architecture Center (Cisco DNA Center) là nơi cung cấp các cài đặt về chính sách, quản lý các phần tử trong mạng.

-Trong doanh nghiệp, hệ thống mạng có thể mở rộng ra thành nhiều vị trí, nhiều domain, sites,… chẳng hạn như mạng chính và mạng nhánh. Trong mỗi hệ thống mạng mới lại xuất hiện nhiều thiết bị tạo thành hệ thống mạng thì các dịch vụ của SD Access cung cấp cho chúng ta cách quản lý dễ dàng và hiệu quả cho hệ thống.

-SD Access được chia ra làm hai phần chính:

+ Mạng Fabric (mạng trục): là nơi các thiết bị kết nối với nhau.

+ Cisco DNA Center: như một bảng điều khiển cung cấp các giải pháp.



Tổng quan về SD Access

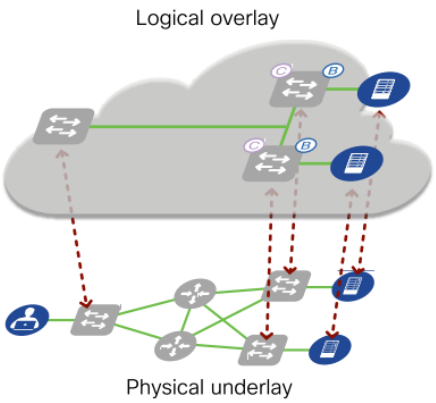
2.1.2 Cấu trúc của SD-Access

a. Network Fabric của SD-Access

-Ta có thể chia một hệ thống mạng doanh nghiệp thành hai lớp khác nhau, mỗi lớp cho một mục đích nhất định.

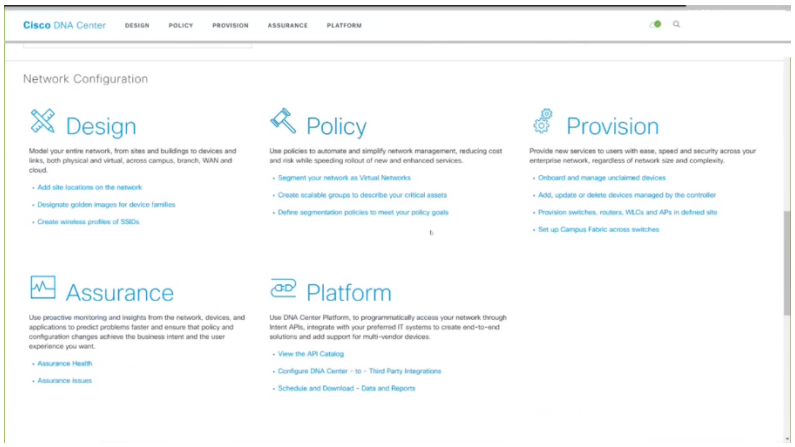
-Một lớp bao gồm các thiết bị phần cứng như router, switch được kết nối với nhau tạo thành một hệ thống (ta gọi là underlay) và một lớp ảo do chúng ta định nghĩa nơi người dùng kết nối vào mạng và là nơi các chính sách của doanh nghiệp được áp dụng (ta gọi là overlay).

DIAGRAM Underlay and overlay networks



Cấu trúc của mạng fabric (mạng trục)

b. Cisco DNA Center



Giao diện Cisco DNA center

-Đây là một bộ điều khiển mạng và bảng điều khiển cho bạn toàn quyền quản lý hệ thống mạng của mình, tối ưu các khoản đầu tư của công ty vào thiết bị, phần mềm của Cisco, giảm chi phí vào các hoạt động IT. Giải pháp này làm được những việc đó bằng cách cung cấp 1 bảng điều khiển duy nhất điều phối và quản lý các tác vụ quản lý quan trọng. Bằng cách này, bộ phận IT có thể nhanh chóng phản hồi, xử lý các thay đổi bất thường của hệ thống nhanh hơn và hiệu quả hơn.

c. SD-Access policy

Một lợi ích thường thấy của SD Access là khả năng cung cấp dịch vụ dựa trên chính sách của mạng trục, chẳng hạn như:

+ Bảo mật phân nhóm.

+ Chất lượng dịch vụ.

+ Dịch vụ cho các ứng dụng.

d. Phân nhóm trong SD-Access

-Là một phương thức để chia các người dùng có cùng đặc điểm hay mục đích sử dụng thành các nhóm khác nhau vì mục đích bảo mật, tận dụng tối đa IP.

-Trong SD Access Fabric VXLAN phân nhóm người dùng bằng cách dùng VNI (virtual network identifier) và trường SGT (scable group tag) trong VXLAN header.

-Có hai kiểu phân nhóm chính trong SD Access

+ Phân nhóm lớn: phân một mô hình mạng lớn thành các mô hình mạng ảo nhỏ hơn (virtual network – VN) bằng cách nhận diện mạng và phân nhóm bảng forwarding. Phân nhóm lớn sẽ tạo ra định tuyến và forwarding ảo trong mạng ảo.

+ Phân nhóm nhỏ: phân một nhóm người dùng hoặc một nhóm thiết bị trong một VN. Phân nhóm nhỏ sử dụng scalable group access control lists (SGACLs), hay còn được biết đến là một ACL dựa trên chính sách.

-Virtual Network (VN) là một thành phần của mạng trục, cung cấp các dịch vụ của Layer 2 và Layer 3, đồng thời định nghĩa Layer 3 routing domain. VXLAN VNI được dùng cho cả phân nhóm của cả hai Layer.

-Scable group là một ID gán cho một nhóm các người dùng trong mạng trục.

2.1.3 Quản lý SD-Access với Cisco DNA center

-Như đã nói ở trên, Cisco DNA center cung cấp một bảng điều khiển để xây dựng, vận hành cũng như quản lý mạng trục, ngoài ra DNA center cũng cung cấp các phân tích chi tiết để theo dõi hệ thống.

-Có hai chức năng chính của Cisco DNA Center:

- Tự động hóa dựa trên bối cảnh:

+ DNA Center tự động cung cấp định nghĩa và sự quản lý theo chính sách group-based, cùng với việc tự động cấu hình tất cả những gì liên qua tới chính sách.

+ Cisco DNA Center được kết hợp Cisco ISE (Identity Services Engine) để cung cấp khả năng thực thi chính sách, cơ chế bảo mật, ngữ cảnh về người dùng, thiết bị.

+ Với Cisco DNA Center, các team IT có thể quản lý hoàn toàn các cơ sở hạ tầng một cách dễ dàng hơn mà không phải lo về các chi tiết triển khai. Điều này cũng khiến cho khả năng sai sót do con người gây ra được hạn chế và chuẩn hóa mô hình mạng một cách dễ dàng.

- Cisco DNA Assurance:

+ Cisco DNA Assurance của Cisco DNA Center được phát triển để trở thành giải pháp toàn diện cho khách hàng với các tính năng như đảm bảo và phân tích mạng.

+ Cisco DNA Center thu thập các thông tin và đánh giá tương quan các thành phần đang được triển khai như thế nào.

2.1.4 Lợi ích của SD-Access

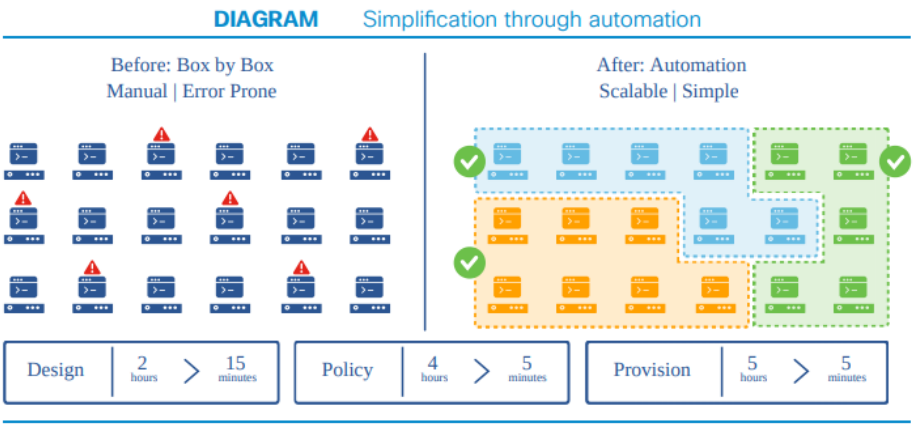
a. Tự động triển khai trên quy mô lớn

-SD Access có thể tự động triển khai một hệ thống lớn mà không cần người quản trị mạng phải biết những kiến thức phức tạp ở mạng underlay.

-SD Access có thể cung cấp một kết nối linh hoạt và tự động giữa các domain trong doanh nghiệp như một phương thức để giảm sự rủi ro và bất ổn.

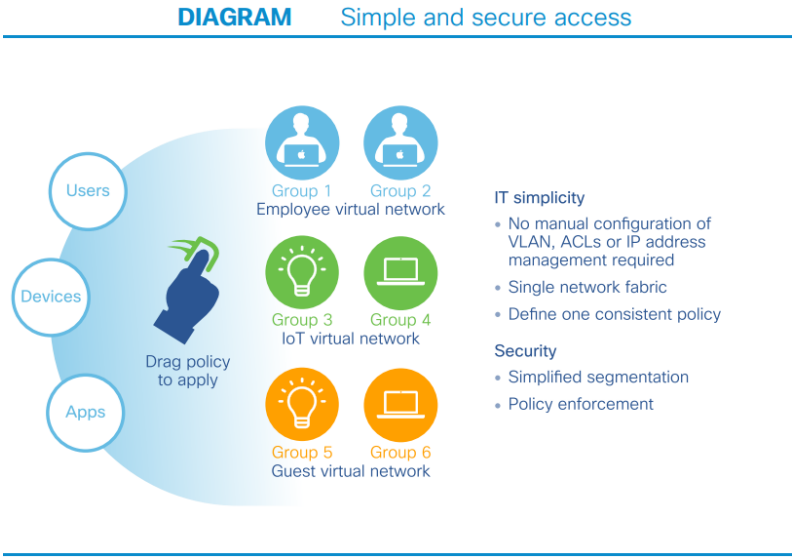
-SD Access có thể hoạt động trên quy mô lớn với rất nhiều site khác nhau.

-Do đó SD Access dễ dàng đáp ứng mọi yêu cầu kết nối mới một cách hoàn toàn tự động.



Thời gian setup và tính chính xác được cải thiện đáng kể từ sau khi sử dụng SD-Access

b. Cung cấp kết nối bảo mật cho người dùng



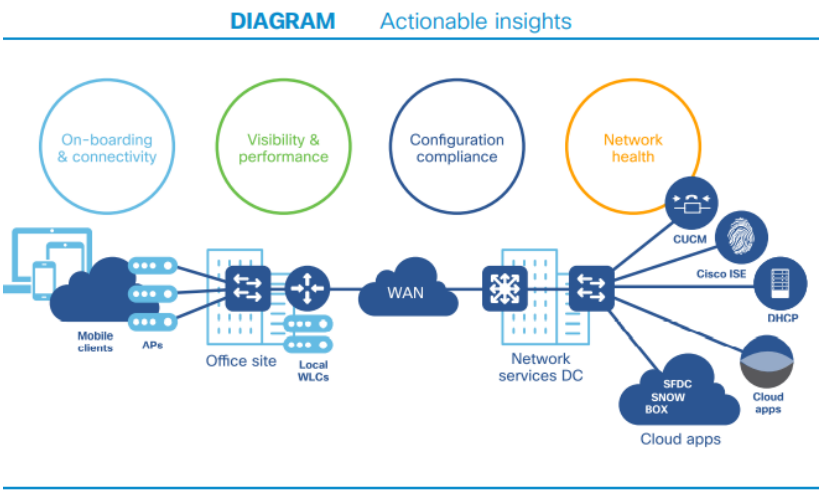
Các thao tác áp dụng chính sách cũng như cập nhật dễ dàng

-SD Access cung cấp các phương pháp để định nghĩa kiểm soát truy cập và chính sách phân nhóm trong mạng. Điều này giúp đơn giản hóa việc áp dụng chính sách, nâng cấp cho từng nhóm.

c. Các phân tích chi tiết

-Việc xử lý vấn đề diễn ra kém hiệu quả và tốn thời gian có rất nhiều nguyên nhân, tools kém hiệu quả hay các chức năng bị hạn chế, độ phức tạp của hệ thống mạng hay việc thiếu các chính sách nhất quán.

-Cisco DNA Assurance cung cấp cái nhìn chi tiết vào các mạng bằng cách thu thập và so sánh các phép đo chi tiết từ nhiều nguồn khác nhau như nhật ký hệ thống, SNMP, NetFlow, AAA, DHCP và DNS. Điều này cung cấp cho người quản trị những thông tin chi tiết để có thể tối ưu hóa cơ sở hạ tầng mạng và hỗ trợ các quyết định kinh doanh tốt hơn.



2.2 SD-Access Fabric

2.2.1 Tổng quan

SD-Access underlay:

- Bao gồm các thiết bị mạng như router, switches,…và giao thức định tuyến lớp 3 truyền thống tạo nên một nền tảng đơn giản linh hoạt và có thể mở rộng để giao tiếp với các thiết bị mạng.

- Underlay không sử dụng cho lưu lượng của khách (khách sẽ kết nối với overlay).

- Các thành phần trong mạng của underlay phải thiết lập kết nối Ipv4 với nhau. Nghĩa là một mạng có kết nối Ipv4 có thể tận dụng làm underlay.

- Mặc dù mọi mô hình và giao thức định tuyến có thể sử dụng ở underlay, việc triển khai mô hình các thiết bị của Layer 3 vẫn nên được thiết kế tốt để đảm bảo hiệu năng, tính mở rộng và tính khả dụng cao.

-Ngoài ra, việc chạy cấu trúc mạng trục logic trên underlay cung cấp chức năng tích hợp cho đa đường và hội tụ được tối ưu hóa, đồng thời đơn giản hóa việc triển khai, khắc phục sự cố và quản lý sự phát triển của mạng lưới.

- Trung tâm Cisco DNA cung cấp dịch vụ tự động hóa mạng LAN theo quy định để tự động phát hiện, cung cấp và triển khai các thiết bị mạng theo thiết kế tốt nhất đã được xác thực của Cisco. Khi phát hiện thiết bị, underlay cho

phép plug-and-play để tự động áp dụng các cài đặt IP và giao thức định tuyến cần thiết.

- Cisco DNA Center tự động hóa mạng LAN bằng cách sử dụng giao thức định tuyến intermediate system (IS-IS) hoặc open shortest path first (OSPF). Lý do để sử dụng hai phương thức này:

+ Cả hai đều sử dụng cơ sở là phương thức định tuyến shortest-path first (Dijkstra).

+ IS-IS phổ biến trong các mạng của ISP.

+ OSPF phổ biến trong mạng doanh nghiệp và mạng WAN.

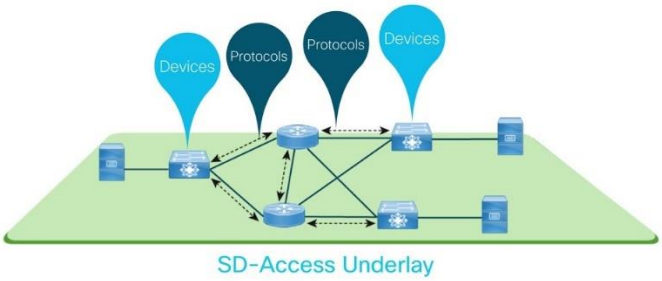
+ Giao thức Link state không quảng bá toàn bộ routing table, thay vào đó phương thức này quảng bá topology mạng (các kết nối trực tiếp, router hàng xóm,…), nên toàn bộ router trong mạng sẽ có toàn bộ thông tin về topology mạng.

+ Giao thức định tuyến link state cung cấp hệ thống phân cấp nhiều cấp độ (hoặc area), nên việc cập nhật được ẩn đi ngoài area đã được xác định.

+ Giao thức định tuyến link state hỗ trợ định tuyến classless, gửi cập nhật bằng địa chỉ multicast.

+ Giao thức định tuyến link state sử dụng thuật toán Dijkstra để xác định đường đi ngắn nhất đến mỗi node trong topology mạng.

+ Giao thức định tuyến link state hội tụ (converge) nhanh hơn phương thức distance vector.



SD-Access Overlay:

-Overlay là một lớp mô hình ảo được tạo ra trên lớp vật lý.

-Overlay có 3 block chính:

+Fabric data plane: được tạo ra từ quá trình đóng gói sử dụng VXLAN, kèm theo group policy option (GPO).

+Fabric control plane: phương thức LISP đóng vai trò mapping & resolving trong mạng (liên kết với VXLAN tunnel endpoints).

+Fabric policy plane: biến mục đích sử dụng hoặc kinh doanh thành chính sách sử dụng group-based policies.

-Ngoài ra overlay cũng có thêm các công nghệ sau:

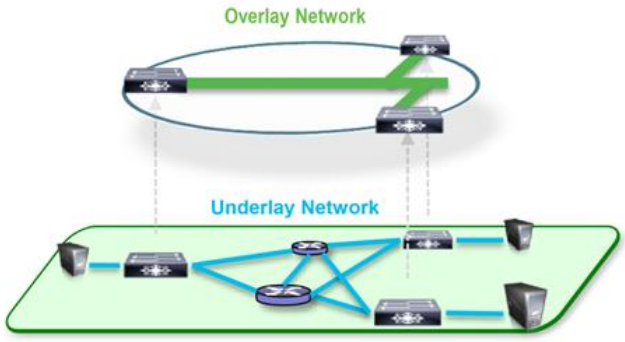
+VXLAN-GPO: cung cấp một vài tiện ích để vận hành SD Access như:

- Hỗ trợ cả Layer 2 & Layer 3.
- Có thể vận hành mọi IP base network & group-base policy với phương thức phân mảnh tích hợp.

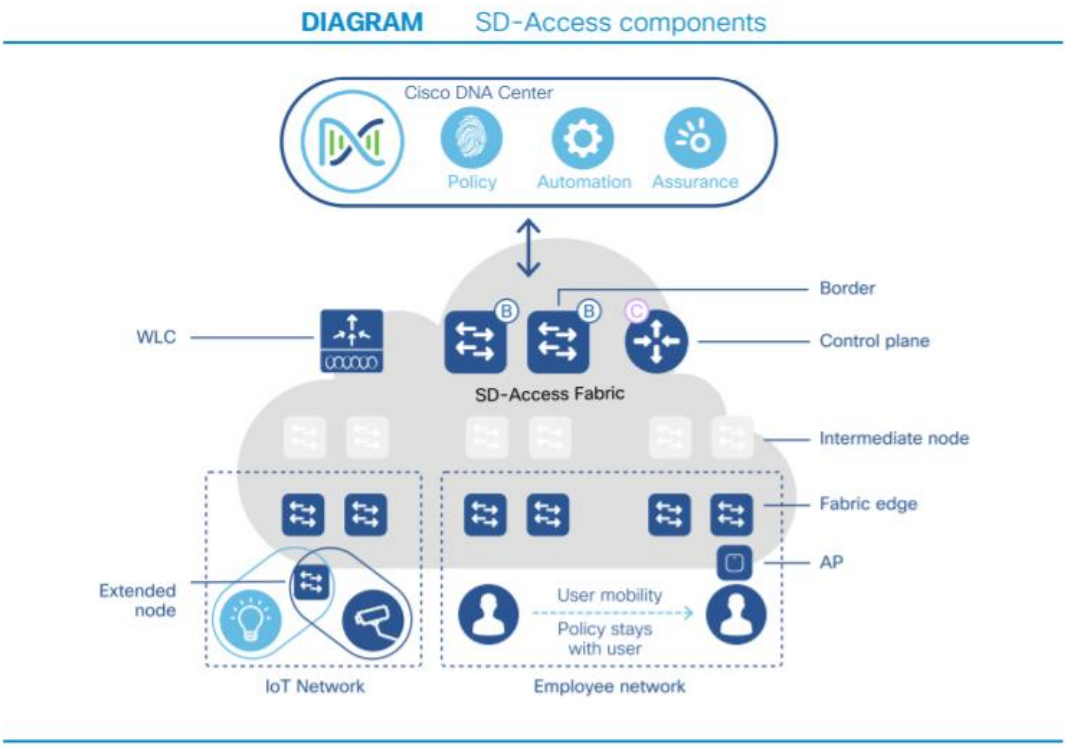
+Phương thức LISP: đơn giản hóa việc routing bằng cách loại bỏ bớt router để xử lý các IP đích và các đường định tuyến:

- Có những router đóng vai trò map server/map resolver, tức fabric control plane.

- Router chỉ cần quản lý mạng của chính nó và map server sẽ đóng vai trò định tuyến tới các end point.



2.2.2 Thành phần của Fabric



-Fabric control plane: đóng vai trò như một trung tâm database, theo dấu mọi người dùng, thiết bị khi họ tham gia vào hệ thống mạng. Fabric control plane cho phép các thiết bị mạng (router, switch, WLCs, …) truy cập vào database này để truy vết địa chỉ người dùng nếu họ có tham gia vào fabric. Bằng cách này, fabric control plane đóng vai trò như single source of truth, nơi lưu trữ các địa chỉ, vị trí các endpoint có gắn với fabric.

-Fabric border node: dùng để liên kết với tầng 2, 3 của mạng truyền thống hoặc để liên kết với các fabric site khác. Fabric border node chịu trách nhiệm trong

việc phiên dịch hoàn cảnh (translate of context) (người dùng/ thiết bị trong quá trình tìm đường đi hoặc định danh) từ một fabric site sang một fabric site khác hoặc sang một mạng truyền thống. Fabric border cũng là thiết bị đảm nhiệm việc giao tiếp với fabric control plane từ một fabric site khác nhằm trao đổi về khả năng tiếp cận và các chính sách.

-Fabric edge node: thiết bị này sẽ lo việc kết nối các endpoint tới fabric, cũng như là công đoạn đóng gói, mở gói, điều phối lưu lượng truy cập từ các endpoint tới và vào fabric. Fabric edge node hoạt động trong vùng của fabric, là nơi đầu tiên của fabric kết nối tới người dùng và thực hiện các chính sách.

-Fabric intermediate node: là thiết bị đơn giản nhất trong toàn bộ kiến trúc SD-Access fabric. Nó đóng vai trò như một thiết bị layer 3 mạng truyền thống, kết nối tới fabric control plane, border node, edge node và cung cấp phần underlay của layer 3 cho traffic trên fabric overlay.

-Fabric-enabled access point (AP): bộ phận này của kiến trúc gắn với fabric edge node nhằm kết nối người dùng không dây tới network fabric.

-Fabric wireless LAN controller (WLC): WLC hỗ trợ fabric-enabled APs được gắn với fabric edge switch. Không chỉ xử lý các tác vụ thông thường gắn với WLC mà nó còn xử lý các sự giao tiếp với fabric control plane dành cho người dùng không dây khi đăng ký hoặc chuyển vùng.

-EndPoint: đơn giản là các thiết bị đầu cuối, thiết bị mà người dùng sử dụng để tham gia vào các mạng, đó có thể là người dùng kết nối dây trực tiếp vào network fabric hoặc người dùng không dây liên kết với fabric AP. Các endpoint được liên kết với fabric edge node.

-Cisco Idenity Service Engine (ISE): đây là một sản phẩm vận chuyển tập trung vào thu thập thông tin, danh tính và tuân thủ chính sách bảo mật. ISE có khả năng định danh, thu thập thông tin các thiết bị mạng, endpoint qua nhiều dạng khác nhau.

-Cisco DNA-center: đây là trung tâm quản lý, điều khiển cho giải pháp SD-Access và là nơi tự động hóa các tác vụ cần để khởi động và quản lý SD-Access.

2.2.3 Cách thức hoạt động của Fabric

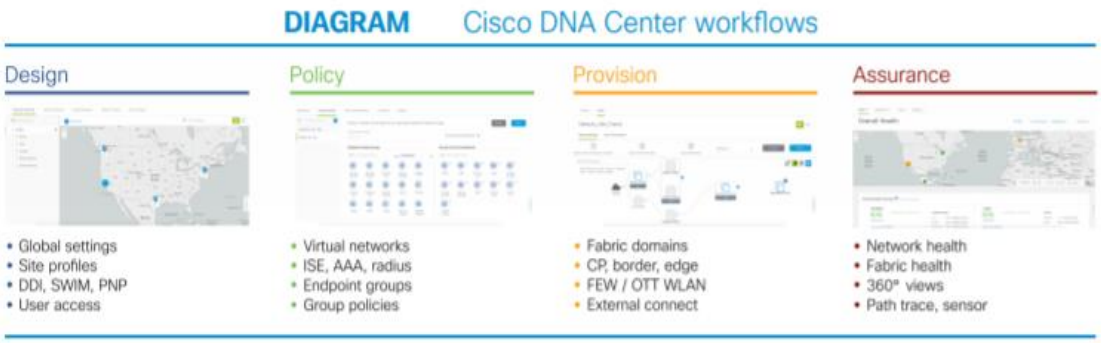
Control plane:

+ Hỗ trợ phân mảnh nhóm người dùng.

+ Mang được địa chỉ MAC.

+ Đánh dấu các task.

2.3 Cisco DNA Center



2.3.1 Tổng quan

Đây là một nền tảng hoạt động tập trung dành cho sự tự động hóa end-to-end và đảm bảo cho các môi trường WAN, LAN, WLAN của doanh nghiệp. Nền tảng này cho phép người quản lý có thể thao tác toàn bộ hoạt động quản lý mạng trong 1 bảng điều khiển.

2.3.2 Nguyên lý của kiến trúc

-Cisco DNA center được thiết kế để mở rộng quy mô sao cho phù hợp với quy mô từ vừa đến lớn của các mạng doanh nghiệp. Nó bao gồm một bộ điều khiển, khả năng tự động hóa và một ngăn xếp chức năng phân tích dữ liệu nhằm việc giám sát.

-Một số thành tựu nổi bật được Cisco DNA center làm được:

+ Tính khả dụng cao, cả cho các thiết bị phần cứng và các gói phần mềm.

+ Cơ chế lưu và khôi phục - phòng các trường hợp gây tổn hại mạng lưới.

+ Cơ chế kiểm soát truy cập dựa trên vai trò - nhằm phân biệt các truy cập người dùng dựa trên vai trò, phạm vi.

+ Interface có thể lập trình được nhằm tạo thêm các đối tác có hệ sinh thái tương thích hoặc các lập trình viên tương tác với Cisco DNA center.

2.3.3 Khả năng tự động hóa

-Mục đích chính của DNA center chính là chuyển hóa các ý định về công việc của các quản trị viên mạng thành các cấu hình thiết bị. Cisco DNA controller bao gồm cở sở dữ liệu thông tin mạng, các chính sách và công cụ tự động hóa, và nó bao gồm luôn cả người lập trình viên.

-Bộ điều khiển (controller) đó có thể khám phá toàn bộ kiến trúc mạng và quét định kỳ hệ thống mạng nhằm tạo ra nguồn sự thật (single source of truth) chứa thông tin các thiết bị tham gia trong mạng, phần mềm hệ thống đang sử dụng, cấu hình mạng,…Tất cả các thông tin này được lưu trữ bên trong controller network information database.

Hết