viptela White paper

Inserting Network Services using Cisco SD-WAN

Use case scenario

The Cisco SD-WAN solution is a cloud-delivered overlay WAN architecture that enables digital and cloud transformation at enterprises. It significantly reduces WAN costs and time to deploy new services, and, builds a robust security architecture crucial for hybrid networks.

Executive summary

Deploying Layer 4 to 7 network services like firewalls, load balancers, and Intrusion Prevention Systems (IPS) in today's enterprise networks is a complicated process that can take weeks or months. The delays are primarily associated with the complexity of configuring the service infrastructure, determining the impact on upstream and downstream devices, and implementing change control. At the same time, the requirements for on-demand security services have increased due to the cloud and mobility.

The Cisco SD-WAN solution provides the flexibility for Network Functions Virtualization (NFV) services to be advertised and implemented on-demand.

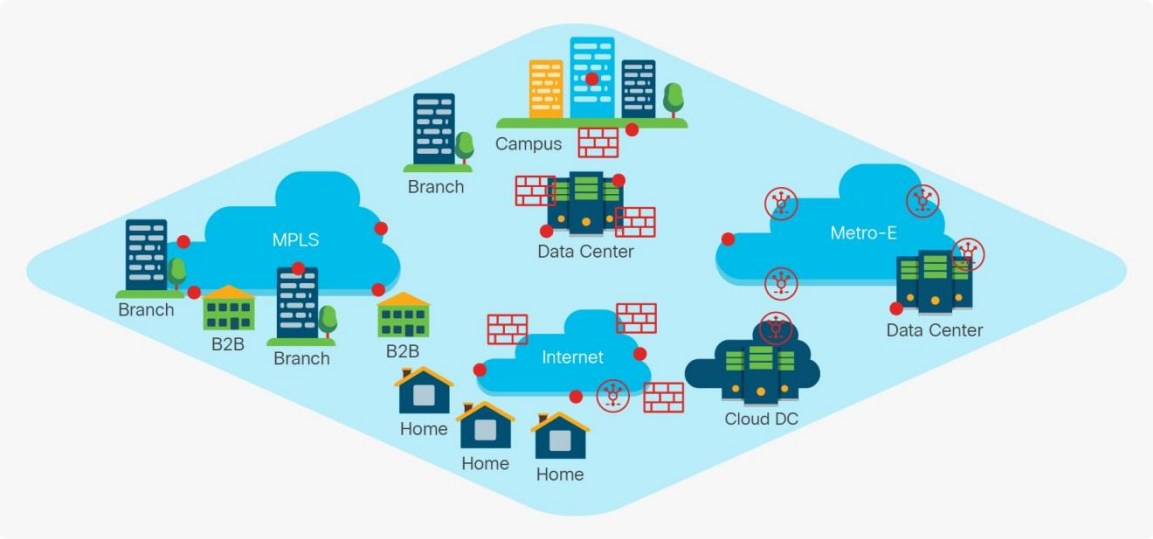
The network services problems

The security perimeter at the enterprise is rapidly disappearing with adoption of cloud-based applications, mobility, and the requirement for ubiquitous access regardless of location. The traditional model of backhauling traffic to select DMZs for purposes of performing network services (such as firewall and IDP/IDS) within four-walls is inefficient and cost prohibitive for large enterprises. Delivering better user experience demands flexibility in deploying applications and network services anywhere. But two fundamental problems interfere with achieving this goal.

Problem 1: The network is unaware of network services

The traditional network is designed for optimizing connectivity between the source and the destination. Network services are inserted along the path in an unstructured manner. As a result, complex policies need to be added on different routing devices in order to force traffic through the services cluster. Figure 1 illustrates the traditional WAN with network services like firewalls and load-balancers distributed at multiple points in the network.

Figure 1. Complex distribution of network services



Problem 2: Right-sizing capacity of network services is difficult

Network architects and designers must always make tradeoffs between the time required to deploy new applications and the capacity required to optimize the performance of these applications. An example is that of public cloud or SaaS applications and BYOD access that have introduced large scale shifts in the use of network services capacity. This results in network services that are under-built in some locations and over-built in the great majority of locations.

While Network Functions Virtualization (NFV) or cloud-based security can address the capacity problem by dynamically adding capacity on demand, there is an enormous burden on the network to optimize routing to direct traffic to the NFV or cloud resources. Today's rigid network architectures cannot implement this requirement.

Traditional approaches to addressing network services

There are two schools of thought on deploying scalable network services.

- Centrally program the rules to insert network services for a flow.
- Treat network service as a function and use standard import and export capabilities to influence behavior at every node.

While these approaches attempt to address the two problems mentioned above, they introduce new challenges.

Table 1. Today's options for network services insertion

Traditional Approach	Technology	Associated Problems
Centrally program information to insert a network service for a flow.	OpenFlow, XMPP	• Flow-by-flow manipulation from a centralized point is not scalable. • Chaining of network services becomes operationally complex.
Treat network services as a function, and use import and export techniques.	MP-BGP extensions, route-target -based import and export	• Complex per-node and per-service policies hinder their deployments • Very easy to get into loops and sub-optimal paths • Change control is extremely difficult — requiring complex upfront planning

The Cisco SD-WAN approach

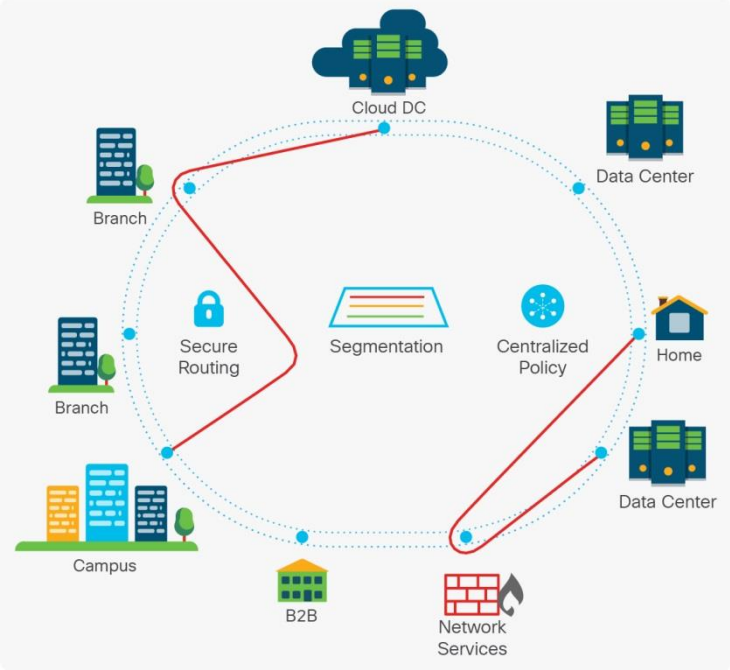
The architecture of the Cisco SD-WAN solution allows network services to be advertised easily across the network and allows packet flow to be influenced to redirect network traffic to the desired network services. This functionality is made possible by a routing protocol that implements sophisticated algorithms to advertise services throughout the virtual network, and by simple policy definition that reroutes traffic through the service locations.

You can achieve service insertion using Cisco SD-WAN in two simple steps:

Step 1. Advertise the availability of a network service from the Cisco vEdge routers

Step 2. Create policies centrally on the vSmart controller to insert a network service or create a service chain based on various attributes (such as prefixes, application, and user).

Figure 2. Network service insertion with Viptela



Additional benefits

Aside from awareness of network services and the ability to right-size capacity, there are added benefits to this approach. You can:

- Load-balance traffic to network service clusters based on location of the source and/or destination.
- Consolidate network-service clusters based on requirements and apply them selectively to traffic. For instance, send all traffic from remote workers through a Tier 2 scrubbing site, and send all traffic destined to financial applications through a regional Tier 1 IDP/firewall cluster.
- Create multiple categories of service chains without affecting every device. One example is to direct destination port 443 traffic through a web proxy and then a firewall. Another example is to direct traffic from any source trying to reach applications in the prefix 10.192.2.0/24 first through an IDP/IDS and then through a load balancer.

- Move traffic from one network service cluster to another during a maintenance window, all with a single centralized policy

Since advertisement of network service is inherent in the solution, dynamic changes (addition or deletion) to physical or virtual network services are immediately advertised to the entire network. Additionally, there is complete predictability in the path leading up to the service chain that makes deployment and troubleshooting extremely easy.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-739466-00 10/17