Network Service Insertion Using Viptela

Use Case Scenario

viptela

Viptela is now part of Cisco.

The Viptela SEN empowers the CIO to significantly reduce costs, dramatically improve time to enable new services, and raise the security threshold across the network.

Executive Summary

Enabling Layer 4–7 network services like firewalls, load balancers and IPS in today's enterprise networks is a complicated process that can take weeks or months. The delays are primarily associated with time taken for 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 services have increased due to Cloud and mobility. The Viptela Secure Extensible Network (SEN) solution provides the flexibility for network function virtualization 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 and performing network services (e.g. 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 service cluster. Figure 1 illustrates the traditional WAN with network services like firewalls and load-balancers distributed at multiple points in the network.

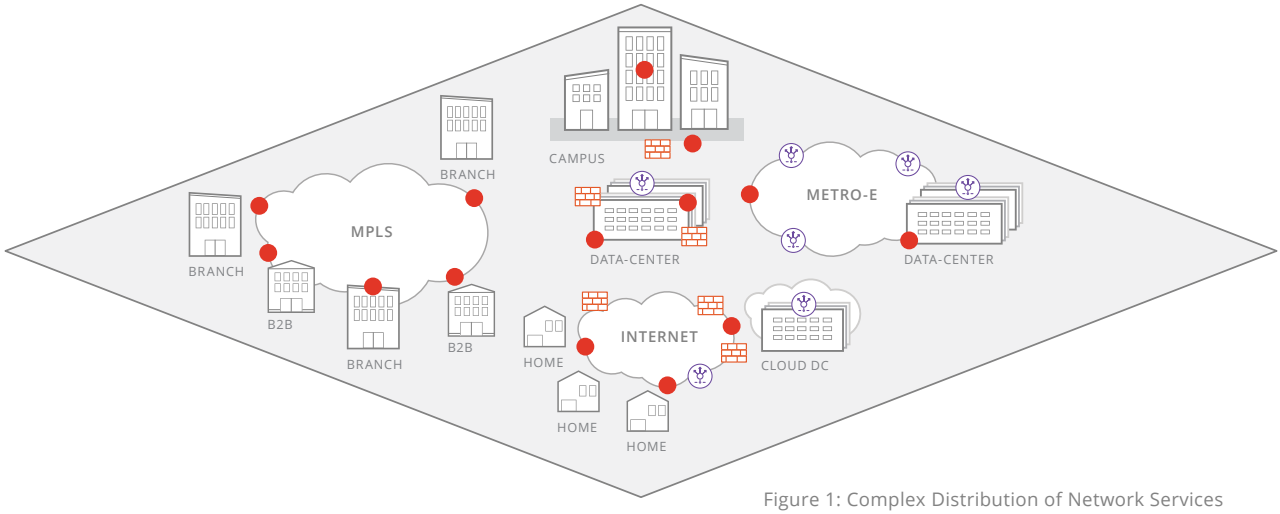

Figure 1: Complex Distribution of Network Services

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

Network architects and designers must always make tradeoffs between the time required to enable new applications and the capacity required to optimize the performance of these applications. An example is that of public cloud / SaaS applications and BYOD that have introduced large scale shifts in capacity utilization of network services. This results in network services that are under built in some locations, and over built in the great majority of locations. When the CIO looks at the aggregate, the utilization numbers fall very short.

While network function virtualization (NFV) can address the capacity problem by dynamically adding capacity on demand, there is an enormous burden on the network to optimizing routing to direct traffic to the NFV resources. Today's rigid network architectures cannot implement this requirement.

Traditional Approaches to Addressing Network Services

While no publicly known customer deployments exist for scalable network service insertion, there are two common schools of thought when it comes to network service insertion.

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

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

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 / export techniques	MP-BGP extensions, Route-Target based import / export	• Complex per-node and per-service policies to influence hinder deployment • Very easy to get into loops and sub-optimal paths. • Change control is extremely difficult — requiring complex upfront planning

Table 1: Today's Options for Network Services Insertion

The Viptela Approach

The architecture of the Viptela Secure Extensible Network (SEN) 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.

Service insertion using Viptela SEN can be achieved in two simple steps:

Step 1: Advertise the availability of a network service from the Viptela 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, eg, prefixes, application, user etc.

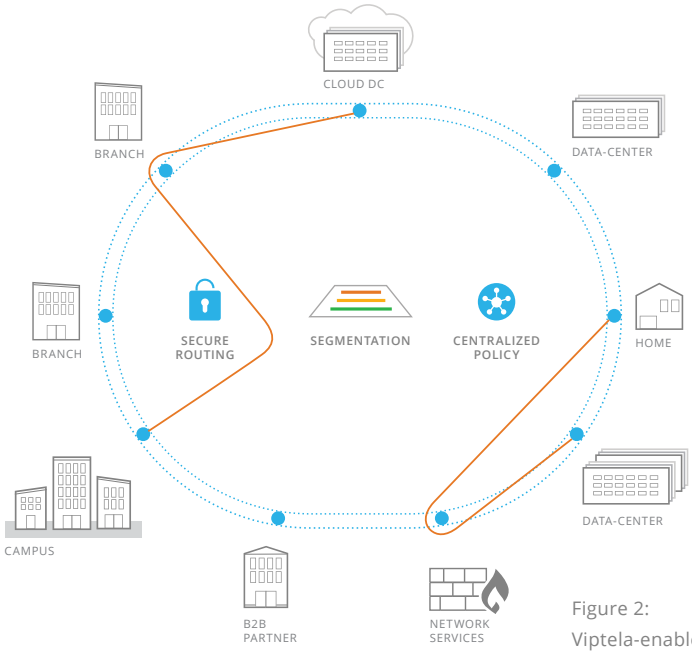

Figure 2:
Viptela-enabled Network Service Insertion

Additional Benefits

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

- 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. E.g. 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/FW cluster
- Create multiple categories of service chains without impacting 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.

The Viptela Secure Extensible Network

For more information on the Viptela solution and how it can help your network, please contact sales@viptela.com

viptela

Viptela Inc., San Jose, California, USA
Tel: 800 525 5033, www.viptela.com