End-to-End Network Segmentation
Use Case Scenario

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

Segmentation and secure isolation of traffic in an enterprise are important for mitigation against attacks, protecting sensitive content, and enabling services with different characteristics. While VLANs can be used for segmentation within a site, no practical options are available over the wide area network (WAN). Viptela addresses this major security threat with a simple architecture that enables end-to-end, encrypted, network segmentation that can be managed with centrally controlled policies.

Drivers for End-to-End Network Segmentation

Network segmentation has existed for over a decade, and has been implemented in multiple forms. At the most rudimentary level, segmentation provides traffic isolation. The most common forms of network segmentation are VLANs (for Layer 2 solutions) and VRFs (for Layer 3 solutions). However, VLANs provide only site-specific segmentation and VRFs are too complex for wider deployments.

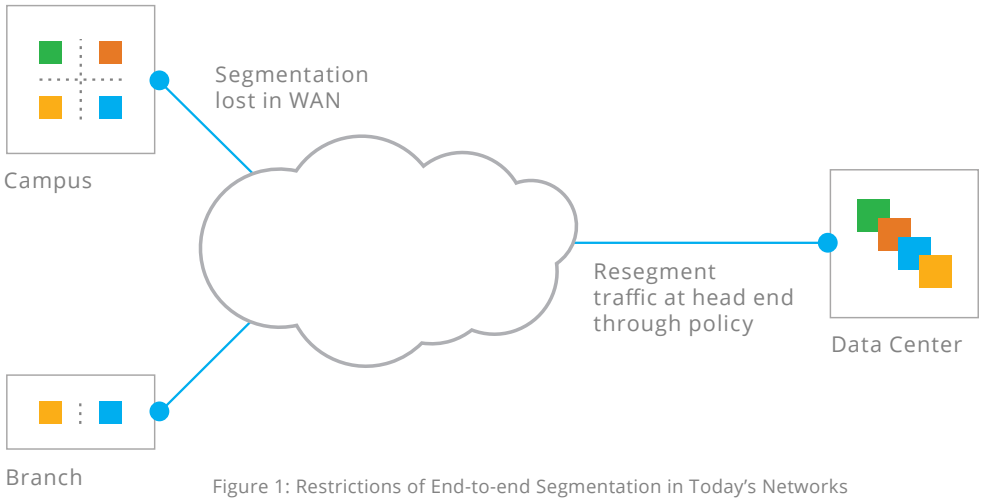

Figure 1: Restrictions of End-to-end Segmentation in Today's Networks

But ubiquity of access, a disappearing security perimeter, and a surge of cloud services necessitate end-to-end segmentation to improve isolation and elevate security within the network infrastructure. Some compelling scenarios are:

- Segmentation of lines of businesses, regardless of location
- Separation of guest Wi-Fi access for clients and partners
- Compliance and audit such as PCI-DSS and HIPAA
- Isolating on-demand development and test labs that span multiple locations
- Different privileges for BYOD based on user, device and location based policies throughout the network
- Multi-tenant and B2B partners
- Digital signage and DVR services

This list keeps growing as the enterprise embraces new applications and services to remain competitive and to reduce time to market.

Problems with Traditional Approaches

One inherent limitation of segmentation is its scope. Today's segmentation solutions are complex and limited to single devices or pairs of directly connected devices. To extend the segmentation functionality throughout the network, the relevant identifying information must be carried to all relevant points in the network.

There are two approaches to providing this network-wide segmentation and the table below calls out the problems associated with each.

APPROACH	EXAMPLES	ASSOCIATED PROBLEMS
Define a grouping policy on a single device and enforce the policy at every point in the network	VRF Lite and Hop-by-hop VRFs	• Not scalable • Too many points in the network to enforce policy • Head end becomes un-manageably complex • Change control is extremely difficult
Define the policy at the Edge and carry the segmentation information in the data traffic	MPLS Layer 3 VPNs	• Complexity associated with signaling the segmentation information (e.g. MP-BGP and MPLS RSVP in the case of Layer-3 VPNs) • Lack of flexibility in enforcing policies based on locations or sites

Table 1: Traditional Approaches for Network Segmentation

Network Segmentation with Viptela

The Viptela Secure Extensible Network (SEN) integrates routing, security, centralized policy and orchestration to provide a secure network with innate capabilities for end-to-end segmentation.

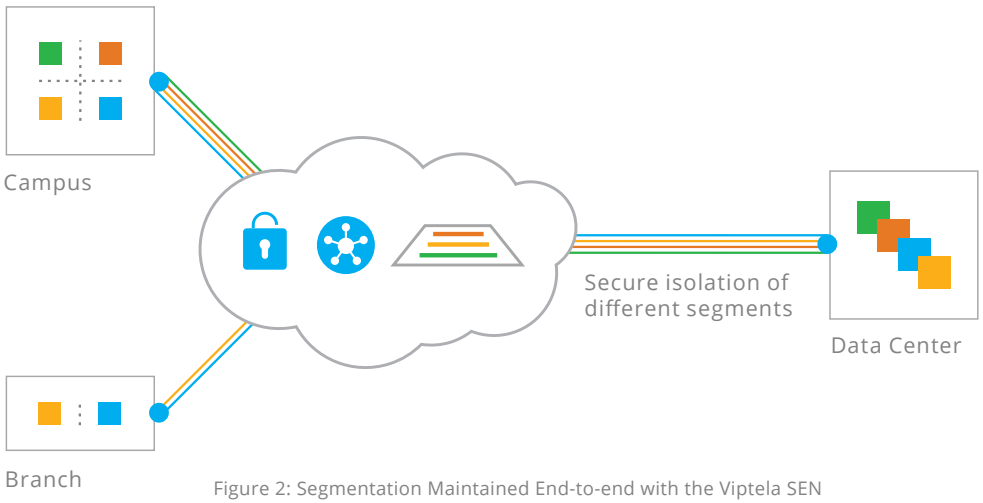

Figure 2: Segmentation Maintained End-to-end with the Viptela SEN

In the Viptela SEN, segmentation is implemented at the edges of the network and is maintained throughout the entire network, securely isolating data traffic within different segments. Segmentation information is communicated to all relevant points in the network without external mechanisms or additional protocols, an advantage that simplifies network design. With the Viptela SEN solution, enterprises can:

- Segment by physical interface, VLANs, application profiles, and so on
- Create end-to-end network segmentation over an existing network, but without modifying any devices in the path
- Enforce segmentation-based policies (for example, guest WiFi traffic should take the least cost circuit, while preserving high-SLA circuit for revenue generating traffic)
- Control which segments gain access based on location, thereby preventing attacks on remote sites
- Enforce network policies based on segments (for example, traffic from unknown BYOD devices is routed through a DMZ scrubbing site before allowing access to the network)
- Control encryption keys and rekey timer per segment (e.g. PCI-DSS compliant traffic should use a different key from the finance department)

The end result is an enterprise network that is agile and easy to control, and that provides secure segmentation of traffic from different lines of business and different partners.

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