Improving Cloud & Internet Performance

Use Case Scenario

viptela

Viptela is now part of Cisco. 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

Enterprises today face two major networking problems with regards to public cloud and Internet applications. Because of the centralized Internet exit architectures of enterprise networks, the application performance has been degrading when compared to home networks. Second, branch sites are running out of capacity to handle Internet traffic. With Internet traffic rising at double-digit rates and accounting for the majority of enterprise traffic, the MPLS link capacity is being fast exhausted. The Viptela Secure Extensible Network (SEN) solution solves these shortcomings by securely providing optimized Internet exit points, and, enabling high bandwidth at branch locations, thus removing the obstacles to enhanced performance.

The Network Architecture Problem

Enterprises are rapidly adopting the public cloud infrastructure, so while the majority of traffic used to flow to the data center, it now flows to the Internet. However, this change is presenting major challenges as a result of the rigid restrictions of legacy network architectures.

Problem 1: Poor User Experience (UX) for Cloud and Internet Applications

Legacy network designs consolidated application and service controls at centralized DMZs and data centers. The result is that enterprise traffic destined for the Internet or public clouds must be backhauled through a centralized DMZ facility, as shown below. This causes the traffic to "trombone" or "hairpin," resulting in an inefficient route that increases the distance between the user and the application.

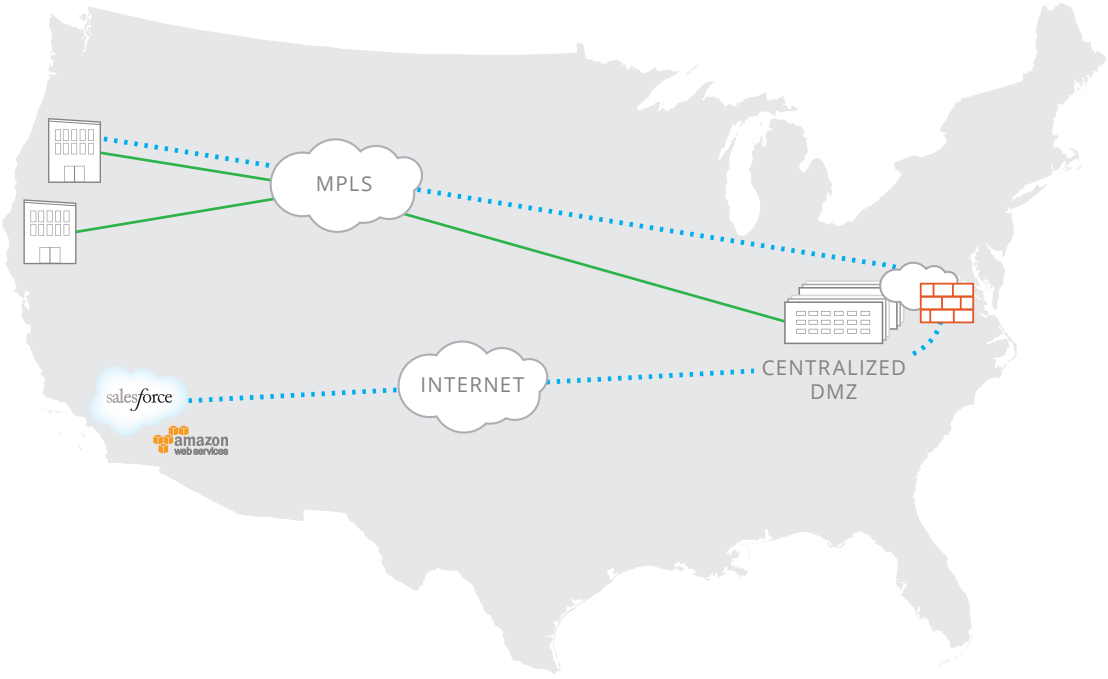

Figure 1: Traffic trombone effect due to centralized DMZ

Problem 2: Low Bandwidth at Branches

The bandwidth requirements at branch sites are rapidly rising, driven by an increased adoption of SaaS applications, Internet video, and hosted VDI applications. Each site may soon require in excess of 10–20 Mbps due to these applications. But most branch sites are straddled with a capacity of 1.5 Mbps, and the cost to scale capacity using legacy TDM and MPLS technologies is unreasonably high.

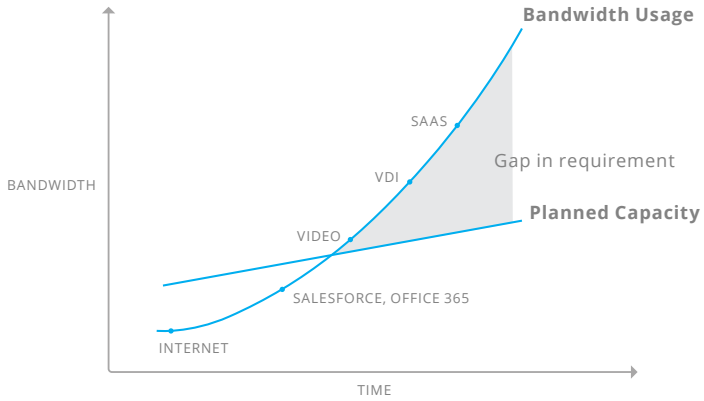

Figure 2: Gap in bandwidth requirements at branches

Traditional Approaches to Addressing Performance Problems

Two common approaches are available to address the cloud and Internet performance problem:

- Decentralize, and deploy multiple Internet exits.
- Enable high-bandwidth connectivity directly from the branch sites.

However, the combination of security, complexity, and cost arising from the rigidity of traditional MPLS technology makes these solutions impracticable on a large scale.

TRADITIONAL APPROACH	TECHNOLOGY	ASSOCIATED PROBLEMS
Regional Internet exits with an MPLS architecture	Multiple regional nodes are equipped with DMZs and connected via MPLS VPNs	• Requires expensive links at the regional exits • Per-branch bandwidth remains low; MPLS upgrades for capacity are cost prohibitive • Traffic management and change control are difficult
High-bandwidth Internet exits from the branches themselves	Each branch needs an Internet connection, a mini-DMZ infrastructure, and security policies defined on each branch router	• There is complexity in replicating security policies (FW/IPS/content filtering) at every branch • Scaling mini-DMZs can be cost-prohibitive • Change control on thousands of nodes is impractical

The Viptela Approach

The Viptela Secure Extensible Network (SEN) solution provides an architecture that elegantly integrates routing, security, centralized policy, and orchestration to address the bandwidth and performance issues related to cloud and Internet applications, enabling enterprises to extend their secure footprint anywhere.

Step 1
Enable High-Bandwidth Branch Links

The Viptela transport-agnostic VPN solution can be enabled at any branch over high-bandwidth business Internet circuits. This solution is incorporated into the Viptela secure overlay network and fully integrates into existing MPLS VPNs or other solutions.

Step 2
Enable Regional Internet Exits

A small number of regional Internet exit points—strategically distributed across the geographic footprint of the enterprise—is enabled. Each regional exit becomes part of the Viptela secure overlay network and is equipped with mini-DMZ capabilities that meet the enterprise's security policies.

Step 3
Define Centralized Policies for Controlling Traffic

Policies are defined to control data traffic so that Internet traffic at branch sites can be directed to the nearest regional exit over high-bandwidth links. These policies are applied on a centralized controller and provide flexibility both for defining primary and backup Internet exits and for directing the use of centralized DMZs when needed.

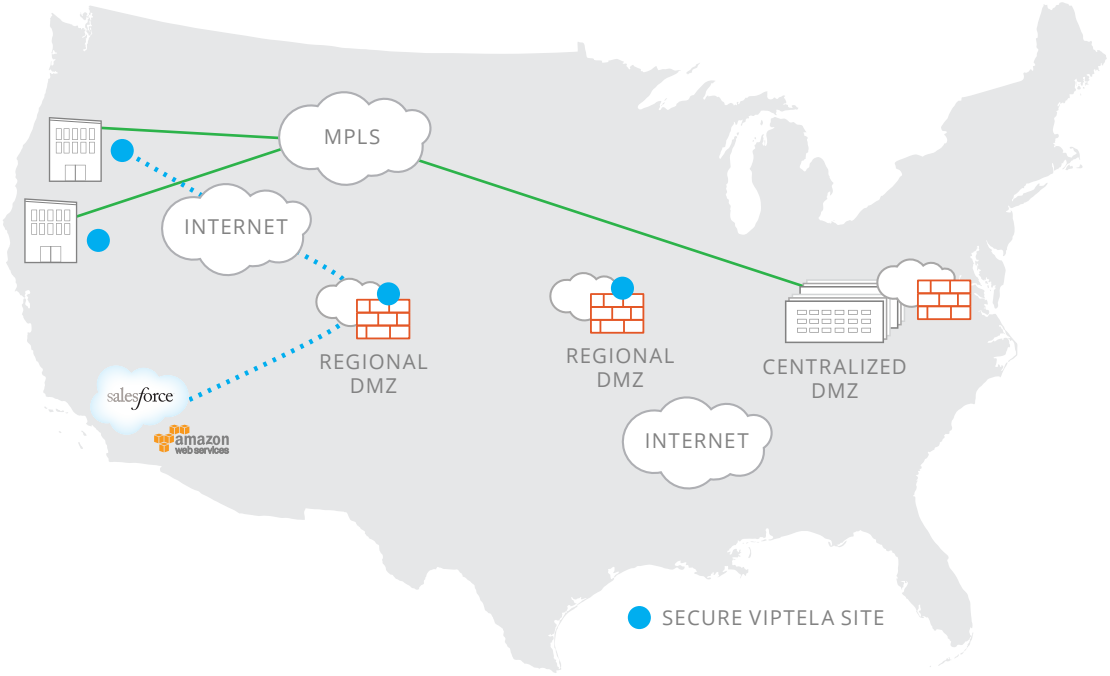

Figure 3: Viptela-enabled Optimized Internet Solution

The end result is an enterprise network that is fully optimized for cloud and Internet applications and that is fully capable of handling the rapid growth in Internet traffic in the enterprise.

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