viptela White paper

Improving SaaS Performance Using 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

Enterprises today face major user experience problems for SaaS applications on account of networking problems. The centralized Internet exit architecture is inefficient and results in poor SaaS performance. And branch sites are running out of capacity to handle Internet traffic which is a concern because more than 50% of branch traffic is destined to the cloud. More importantly there are many dynamic changes in Internet gateways and the SaaS hosting servers that lead to unpredictability in performance.

The Cisco SD-WAN solution solves these problems by creating multiple Internet exit points, adding high bandwidth at branch locations, and dynamically steering around problems in real-time, resulting is an optimal SaaS user experience at all branches.

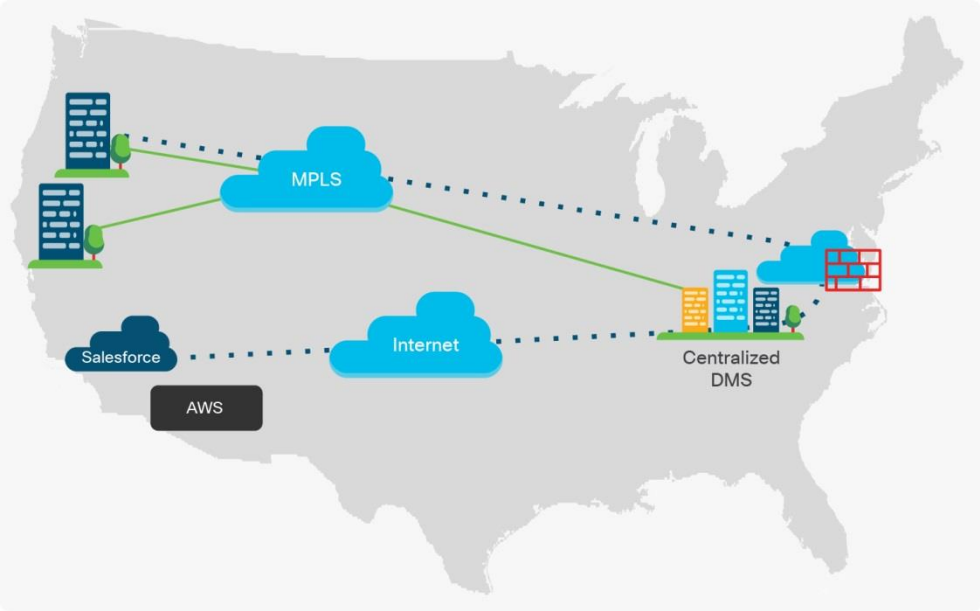
The network architecture problem

Enterprises are rapidly adopting SaaS, 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. As a result, 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**, creating an inefficient route that increases the distance between the user and the application.

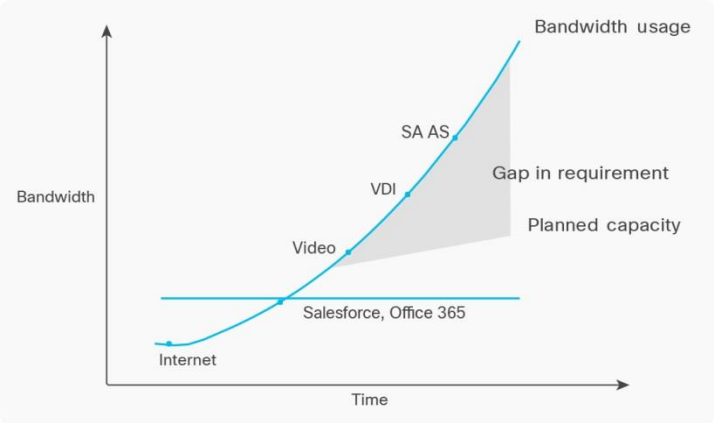
Figure 1. Traffic trombone effect due to centralized DMZ



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 to 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



Problem 3: Variability of the Internet gateways and SaaS hosting locations.

The various Internet gateways go through dynamic changes in latency and other metrics throughout the day. By the same measure, the SaaS hosting locations go through different levels of loads during different parts of the day. Thus in order to get the best user experience for a SaaS application, we must choose the right Internet exit and the right hosting location at that given moment. Traditional network architectures cannot do this.

Traditional approaches to addressing performance problems

Two common approaches are available to address SaaS performance problems:

- Decentralize, and deploy multiple Internet exits.
- Provide 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 through 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 (firewall, IPS, IDS, and content filtering) at every branch • Scaling mini-DMZs can be cost-prohibitive • Change control on thousands of nodes is impractical

The Cisco SD-WAN approach

The Cisco SD-WAN solution provides an architecture that elegantly integrates routing, security, centralized policy, and orchestration. It addresses the bandwidth and performance issues related to cloud and Internet applications, so enterprises can extend their secure footprint anywhere.

Step 1

Provide high-bandwidth branch links

You can deploy the Cisco SD-WAN solution at any branch over high-bandwidth Internet circuits. This solution is incorporated into the Cisco secure overlay network and fully integrates into existing MPLS VPNs or other solutions.

Step 2

Enable branch and regional Internet exits

This step involves enabling a small number of branch and regional Internet exit points strategically distributed across the enterprise. Each regional exit becomes part of the Cisco SD-WAN overlay network integrates into mini-DMZ posture.

Step 3

Define centralized policies for controlling traffic

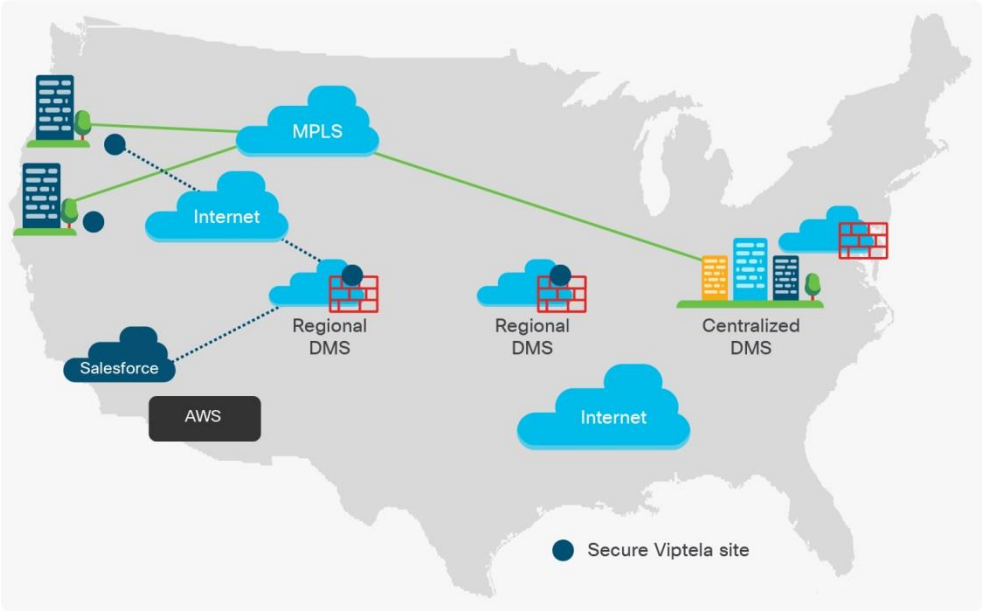
Define policies controlling SaaS application traffic to the nearest Internet exit over high-bandwidth links. These policies, applied on a centralized controller, provide flexibility both for defining primary and backup Internet exits.

Step 4

Enable real-time optimization on supported SaaS applications

A group of supported SaaS applications (like Office365, Salesforce etc.) can be enabled for real-time optimization. Cisco SD-WAN agents are able to determine the best link, best Internet exit, and the best SaaS hosting location at that given moment, and direct traffic accordingly.

Figure 3. Optimized Internet solution with Cisco SD-WAN



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

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 C11-739645-00 10/17