Business Partner Networks Using Viptela

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

The growing ecosystem of business partners within enterprises makes it difficult to manage the associated network, security, and audit requirements. Enabling secure connectivity from the enterprise is cumbersome, repetitive, and error-prone, and it introduces unnecessary delay. The ability to enforce network-wide security policies on partner connections is poor at best, and this weakness can allow the leaking of sensitive information or unauthorized access. The Viptela Secure Extensible Network (SEN) solution addresses these challenges by creating an overlay infrastructure to on-board partners expeditiously, and provides isolation and policy controls that automatically protect sensitive content.

Challenges in the Partner Network

Enterprises have different types of business partners that need varied access to the corporate network. The partners include maintenance companies, outsourcing vendors, suppliers, and even consumers of network services provided by the enterprise. The traditional architecture of a partner network is shown in Figure 1. It entails:

- Providing connectivity from the partner premises to the enterprise using MPLS or IPsec VPNs.
- Configuring, installing, and maintaining a physical routing device (known as customer premise equipment or CPE) at the partners' premises
- Defining policies (ACLs) at every major hub and intermediate point in the enterprise network to restrict service prefix advertisements and protect sensitive traffic

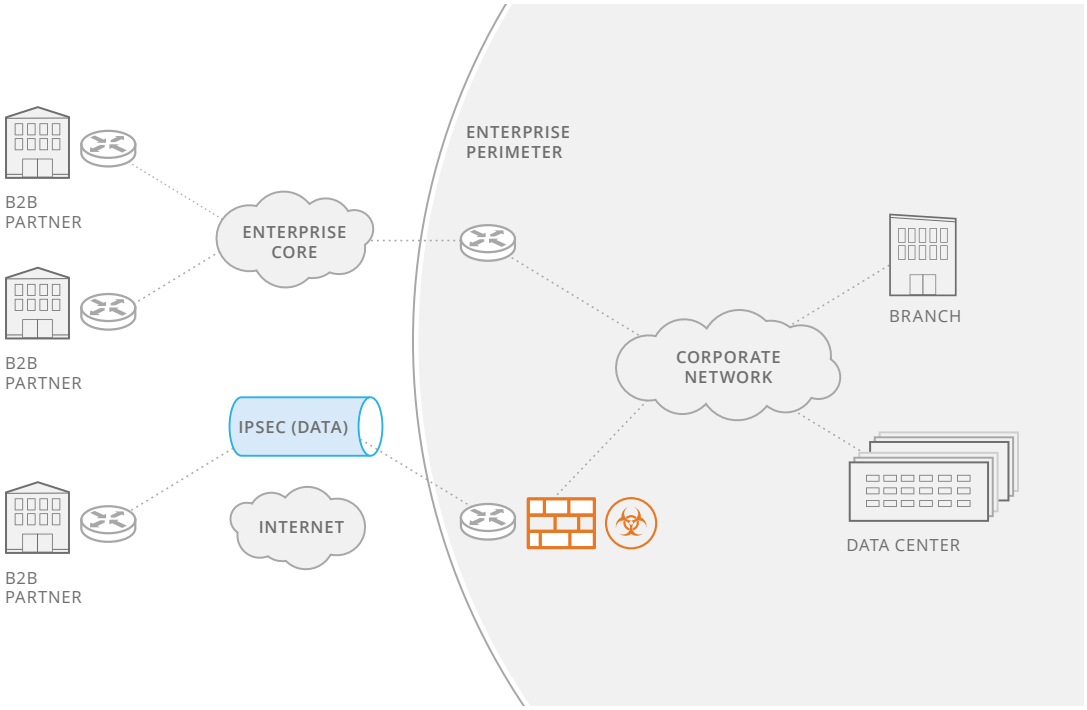

Figure 1: A Traditional Business Partner Network

However multiple challenges emerge from legacy architectures:

- Keys and certificates on CPE devices are unaccounted for and may not updated for years. This situation arises because enterprises do not control both sides of the CPE and change control requires manual effort.
- External dependencies and delays exist in enabling MPLS or IPSec VPNs, and deploying the CPE device at the partner site.
- Processes for maintaining secure, end-to-end isolation between the parter network and the corporate network are inadequate.
- Policies must be applied at each hub site, so policy complexity increases as an enterprise has more partners.
- Restricting business partners to their specific service locations can be extremely challenging. The traditional approach of backhauling all partner traffic to a pair of head ends is both cost prohibitive and bad for user experience.

Ideal Requirements for a Partner Network

To maintain a dynamic ecosystem of partners, an enterprise would ideally require the following from a typical partner network.

CATEGORY	REQUIREMENTS
Circuits & Access	• Flexibility to use one or more transport circuits (MPLS, broadband, LTE or Metro-E) depending on SLA • Ability to access business partner services regardless of location
Routing	• Ability to enforce pure hub-and-spoke communication and to explicitly disallow spoke-to-spoke communication
Policy	• Access control that restricts which enterprise service prefixes are advertised to the partner
Security	• Encryption of all partner traffic with periodic rekeying (hourly, daily, or on demand) • Authentication of all permissible network devices • Secure end-to-end segmentation that extends deep inside the enterprise network to protect sensitive enterprise content
Redundancy	• Redundant CPE devices • Redundant paths (dual head ends) • Fast network re-convergence
Scaling	• Redundant CPE devices • Redundant paths (dual head ends) • Fast network re-convergence

Meeting these requirements with traditional technology is not feasible, because complex configurations must be defined at multiple points in the network and applied to the routing, security, and policy elements in the network. A new approach is needed to seamlessly address these requirements.

The Viptela Approach

The Viptela Secure Extensible Network (SEN) solution provides an architecture that elegantly integrates routing, security, centralized policy, and orchestration to address all the requirements of a partner network. With the Viptela SEN solution, enterprises can:

Extend Secure Connectivity Instantly

Viptela delivers a VPN solution that is agnostic to the underlying transport (MPLS, Broadband, LTE or Metro-E). This capability enables the enterprises footprint to securely extend to any partner location over any transport.

Enable Isolation

The partner network can be maintained on one or more VPN segments that are securely isolated throughout the enterprise network. This separation prevents exposure of sensitive enterprise traffic to the partner network.

Provide Automatic Authentication and Encryption

All traffic on the Viptela network is always encrypted (AES-256) with frequent rekeying. The CPE devices utilize an automated authentication and bring-up procedure, which is tamper proof.

Enforce Policy and Control Centrally

Enterprises can exercise full control of all entities of the partner network, and enforce policies to control prefix advertisements, restrict access and insert security services using a centralized controller.

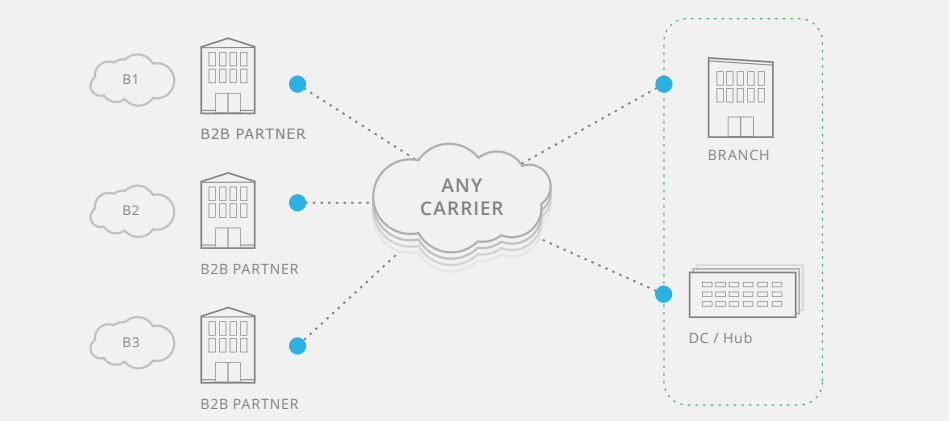

Figure 2: A Viptela-enabled Business Partner Network

The result is a dynamic and extensible VPN solution that addresses the major requirements for enabling business parters rapidly with full end-to-end security.

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