viptela White paper

Business Partner Networks Using Cisco 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

The growing ecosystem of business partners within enterprises makes it difficult to manage the associated network, security, and audit requirements. Providing secure connectivity from the enterprise is cumbersome, repetitive, and error-prone, and it introduces unnecessary delays. The inability to enforce robust network-wide security policies on partner connections has led to vulnerabilities creeping across the corporate systems and other business partners.

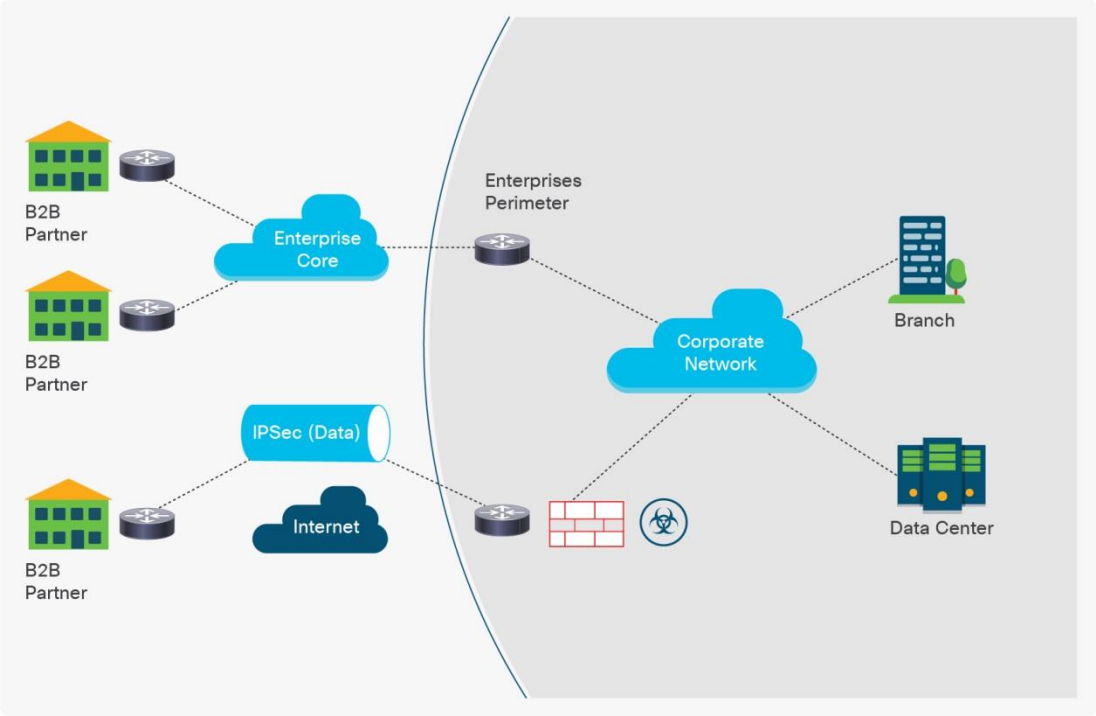
The Cisco SD-WAN solution addresses these challenges by creating an overlay infrastructure to onboard partners and at the same time to securely isolate them by means of network segmentation and centralized policies. Collectively this ensures the protection of critical assets and prevents vulnerabilities of the weakest link to leak elsewhere.

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. Its capabilities include:

- Providing connectivity from the partner premises to the enterprise using MPLS or IP Security (IPsec) VPNs.
- Configuring, installing, and maintaining a physical routing device (known as customer premises 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 be 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 deploying MPLS or IPSec VPNs and the CPE device at the partner site.
- Processes for maintaining secure, end-to-end isolation between the partner network and the corporate network are inadequate.

Among other challenges:

- You must apply policies 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 headends 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 and 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 reconvergence
Scaling	• Redundant CPE devices • Redundant paths (dual head ends) • Fast network reconvergence

Meeting these requirements with traditional technology is not feasible because it entails defining complex configurations at multiple points in the network and applying them to the routing, security, and policy elements in the network. A new approach is needed to seamlessly address these requirements.

The Cisco SD-WAN approach

The Cisco SD-WAN solution provides an architecture that elegantly integrates routing, security, centralized policy, and orchestration to address all the requirements of a partner network. With the Cisco SD-WAN solution, enterprises can:

Extend secure connectivity instantly

Cisco SD-WAN delivers a VPN solution that is agnostic to the underlying transport (MPLS, broadband, LTE or Metro-E). This capability makes it possible for the enterprises' footprint to securely extend to any partner location over any transport.

Isolate the partner network

You can maintain the partner network 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.

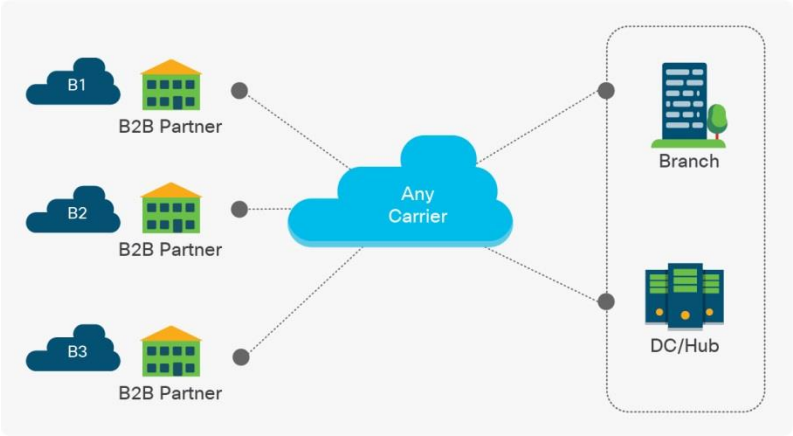
Provide automatic authentication and encryption

All traffic on the Cisco SD-WAN network is always encrypted (AES-256) with frequent rekeying. The CPE devices use 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 business partner network with Cisco SD-WAN



The result is a dynamic and extensible VPN solution that addresses the major requirements for quickly providing business partners with full end-to-end security.

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 C11-739464-00 10/17