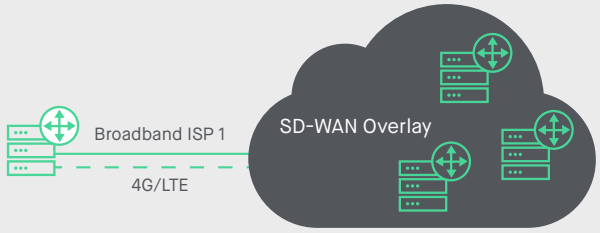
CenturyLink
Managed Cisco SD-WAN

DATA SHEET

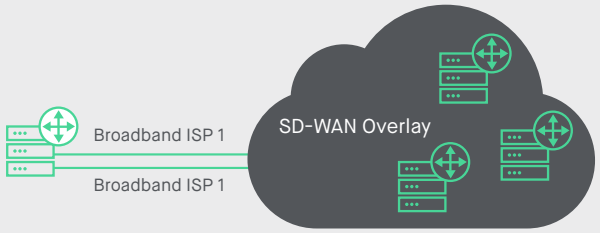
CenturyLink Managed Cisco SD-WAN solution provides advanced routing, segmentation, and security capabilities for interconnecting complex enterprise networks. Its cloud-based network management, orchestration, and overlay technologies make it easy to deploy and manage next-generation WAN architectures. The Cisco SD-WAN solution is powered by the Viptela platform, delivering secure end-to-end network virtualization. Enterprises can use this solution to build large-scale networks with full integration of routing, security, centralized policy, and orchestration.

Common Deployment Options



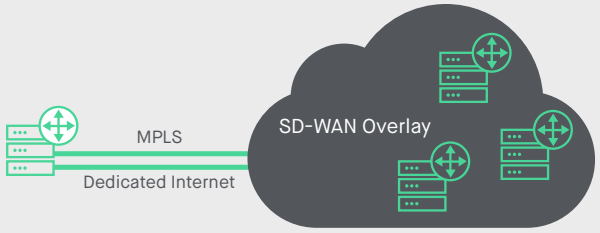
Broadband + LTE

Ideal for low priority branches or remote locations



Dual Broadband

Perfect for branch locations and/or data centers for networks without MPLS



MPLS + Internet

For sites with high-priority and mission-critical applications, typically data centers and/or headquarters

CenturyLink®

Use Cases

Transport-Agnostic VPNs

This provides a cost-effective and secure IP fabric over any underlying transport.

B2B Partner Network

These are enterprises with a dynamic partner ecosystem that can rapidly onboard partners over any transport.

Network Service Insertion

Network services, like firewalls, IPS and load balancers, can be consolidated at centralized locations, and traffic can be routed through these services with simple policy changes.

End-to-End Network Segmentation

Sensitive traffic among different lines of business and different business partners can be secured by end-to-end segmentation.

Encryption at Scale

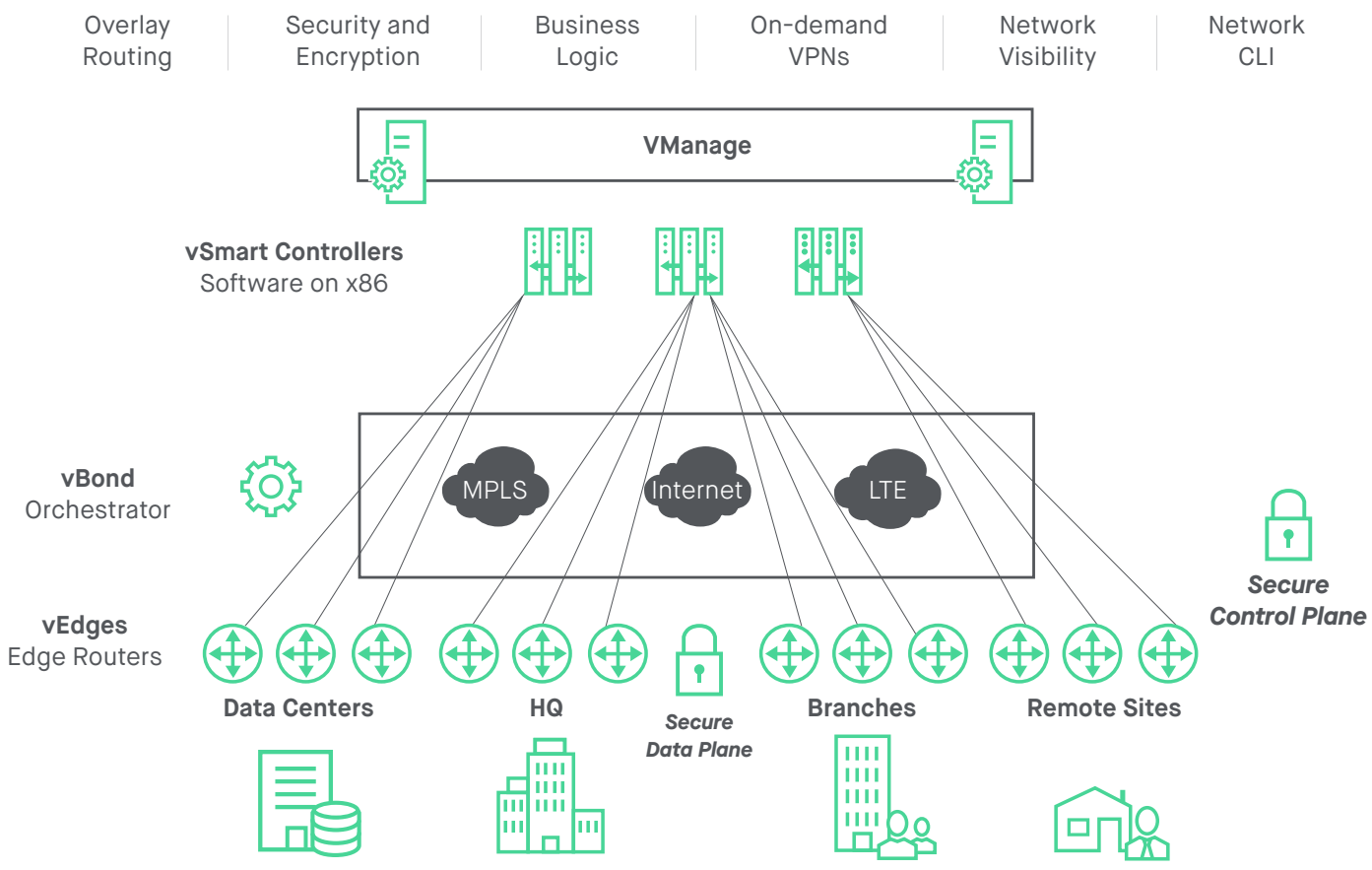
This provides powerful encryption capabilities using automated key management and device authentication to secure nearly any network infrastructure.

Regional Internet Exit

Enterprises can deliver optimal user experience for cloud, VDI and internet applications by enabling regional internet exit points.

Components

The four major components of the solution are the vSmart Controller, vEdge Router, vBond Orchestrator and the vManage Configuring and Monitoring System.



CenturyLink®

vSmart Controller

The vSmart controller is the brains of the overlay network. It established a secure DTLS connection to each vEdge router in the network and runs an Overlay Management Protocol (OMP) to share routes, security and policy information. The centralized policy engine in the vSmart controller provides rich inbound and outbound policy constructs to manipulate routing information, access control, segmentation, extranets and service chaining.

The vSmart controller is a virtual appliance that runs on a VMware vSphere ESXi Hypervisor that has a minimum of two vCPUs and 4 GB of memory. It uses pre-installed security credentials that allow it to automatically authenticate each new vEdge device before it joins the network.

vEdge Routers

The vEdge routers are full-featured IP routers that perform standard functions, such as OSPF, BGP, QoS, ACLs, and routing policies, in addition to the overlay control and data plane. Each vEdge router automatically establishes secure DTLS sessions with the vSmart controller and establishes standard IPsec sessions with other vEdge routers. There are three types of vEdge routers:

	vEdge 100	vEdge 1000	vEdge 2000
Size	Tabletop or 1RU	Half-width, 1RU	Full-widths, 1RU
Encryption Capacity	100 Mbps	1 Gbps	10 Gbps
Fixed Ports		8xGE SFP (10/100/1000)	4xGE SFP FIXED (10/100/1000)
Pluggable Interface Modules		N/A	Two modules (choice of 8xGE SFP or 2x10GE SFP+)

vBond Orchestrator

The vBond Orchestrator is a modular piece of software that runs on a vEdge router. It automatically facilitates the control plane bring up process, performs initial authentication, and orchestrates the connectivity between the vSmart controllers and the vEdge routers. The vBond Orchestrator plays an important role in enabling the Viptela devices that sit behind NAT to communicate with the broader network.

vManage Network Configuration and Monitoring System

The vManage is a centralized system that enables configuration management and monitoring of the solution. It is a virtual appliance that runs on VMware vSphere ESXi Hypervisor with a minimum of two vCPUs and 8 GB of memory.

Features	Benefits
Centralized policy and distributed enforcement	The Overlay Management Protocol (OMP) centrally influences all routes and policy information for each segment of the Viptela network. This feature eliminates any bottleneck in building the largest topologies and enables quick turnaround in changes to the network.
Automated secure bring up	The vEdge routers have a factory-installed Trusted Platform Module (TPM) chip with a signed certificate. This built-in security helps ensure automated, foolproof authentication of any new vEdge routers joining the network and is a major advantage when deploying tens of thousands of end points.
Encrypted control and data traffic	The default mode of the operation of the Viptela network is “secure” and “encrypted.” Keys can be rotated as frequently as required without impacting performance. It can scale to multiple tens of thousands of network endpoints and 100k+ routes while still providing multipoint security.
Scale-out architecture with redundancy	Multiple Viptela devices can be added to supplement capacity and provide redundancy. The architecture can withstand multiple failures in the overlay network for both the control and data plane.
End-to-end network segmentation	End-to-end network segmentation can be enabled rapidly without additional control plane protocols. This segmentation provides robust protection of the network from outside attackers and provides secure separation internally within the multiple application segments.