Lumen[SM] SD-WAN with Cisco Viptela

Lumen SD-WAN with Cisco Viptela provides advanced routing, segmentation, and security capabilities for interconnecting and complex enterprise networks. Its cloud-based network management, orchestration, and overlay technologies make it easy to deploy and manage next-generation WAN architectures. This SD-WAN solution delivers 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

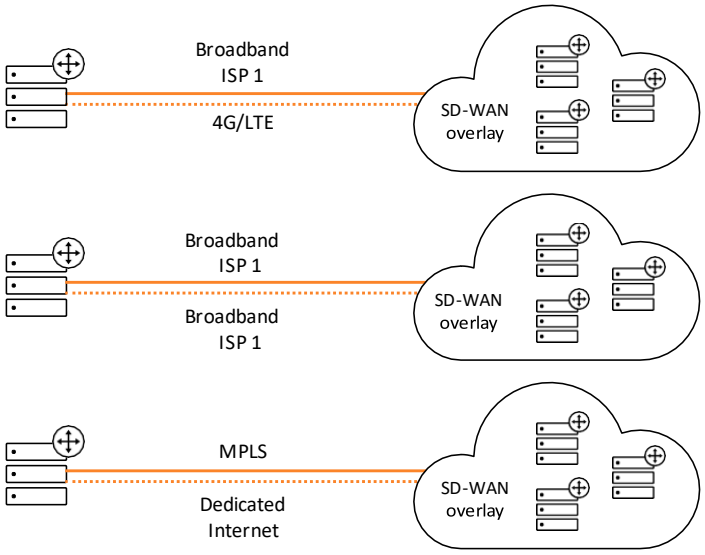
Ideal for low-priority branches or remote locations

Dual Broadband

Designed for networks without MPLS, at branch locations or data centers

MPLS + Internet

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



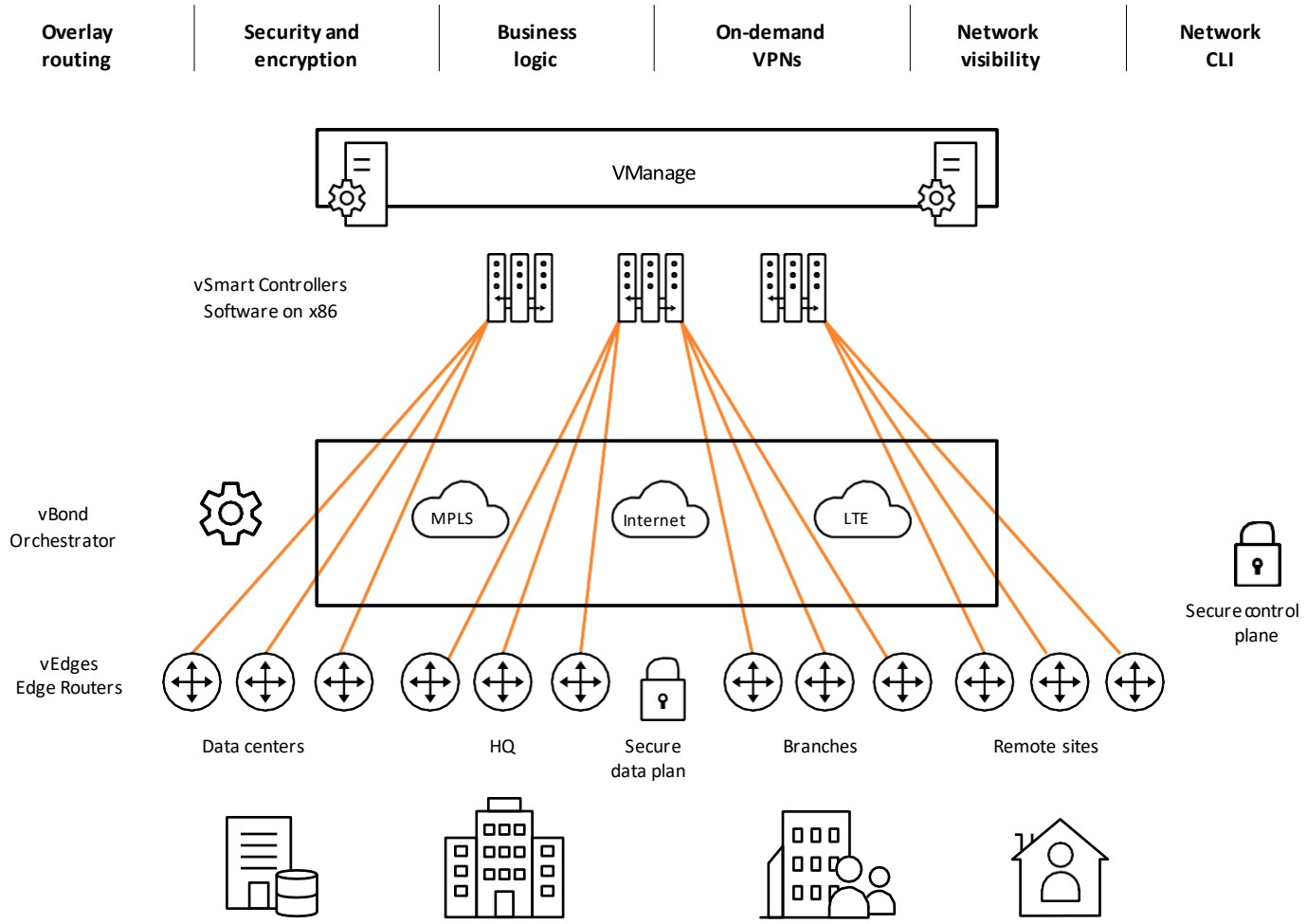
Use Cases

- **Transport-agnostic VPNs:** Cost-effective and secure IP fabric over virtually any underlying transport
- **B2B partner network:** Enterprises with a dynamic partner ecosystem that can rapidly onboard partners over virtually any transport
- **Network service insertion:** Network services such as 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 partners can be secured
- **Encryption at scale:** Powerful encryption capabilities using automated key management and device authentication to secure nearly any network infrastructure
- **Regional internet exit:** Enterprises can deliver optimal end user experience for cloud, VDI and internet applications by enabling regional internet exit points

LUMEN®
TECHNOLOGIES

Components

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



vSmart Controller

The vSmart controller is the brains of the overlay network. It establishes a secure Datagram Transport Layer Security (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, with a minimum of two vCPUs and 4GB of memory. It uses preinstalled security credentials to automatically authenticate each new vEdge device before it joins the network.

vEdge Routers

vEdge routersare full-featured IP routers that perform standard functions such as OSPF, BGP, QoS, ACLs, and routing policies with integrated enterprise firewall functionality, in addition to overlay control and data planes. Each vEdge router automatically establishes secure DTLS sessions with the vSmart controller and 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

This centralized system 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 8GB of memory.

vManage Network Configuration and Monitoring System

This centralized system 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 8GB of memory.

Features	vEdge 100
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 bottlenecks—even in building the largest topologies—and enables quick turnaround in network changes.
Automated secure bringup	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.
Integrated enterprise firewall	vEdge devices come with integrated enterprise firewall functionality, including user-based security policies and segmentation, IPsec, VPN, NAT and ACLs standard. This eliminates the need for multiple pieces of networking and security hardware at SD-WAN sites. It also enhances security and simplifies infrastructure management.
Encrypted control and data traffic	The default mode of the Viptela network operation is “secure and encrypted.” Keys can be rotated as frequently as needed 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. Segmentation provides robust protection of the network from outside attackers as well as internal attackers.

LUMEN® TECHNOLOGIES