At a Glance

The Viptela Secure Extensible Network (SEN) solution is an industry-leading platform that deliver secure end-to-end network virtualization. Enterprises can use the SEN solution to build large-scale networks with full integration of routing, security, centralized policy, and orchestration. The end result is a network that is operationally easy to manage and that eliminates disconnects between business and IT.

Technical Challenges in Today's Networks

Enterprises today face significant business challenges as their legacy networking infrastructure becomes increasingly complex. Providing connectivity across the enterprise involves:

- Managing multiple disparate transport networks (MPLS, Metro Ethernet, SSL over Internet, and IPsec)
- Embedding policy and control at every hop in the network
- Addressing security vulnerabilities created by inadequate network-wide segmentation and weak encryption policies
- Long provisioning times related to rolling out new applications that require network-specific behavior
- Simple change requests that take months to complete due to distributed complexity
- Performance issues related to public cloud, VDI, and bandwidth-hungry applications

A refreshing new approach is needed for building large-scale networks that provide the benefits of virtualization end-to-end, without increasing costs, compromising security, or creating delays in the rollout of new services.

The Viptela Approach

The Viptela SEN solution addresses these technical challenges with five key architectural elements:

1. Enable transport independence

2. Automatically secure any routed end-points

3. Provide end-to-end network segmentation

4. Enforce policies with a centralized controller

5. Enable advertisement of network services

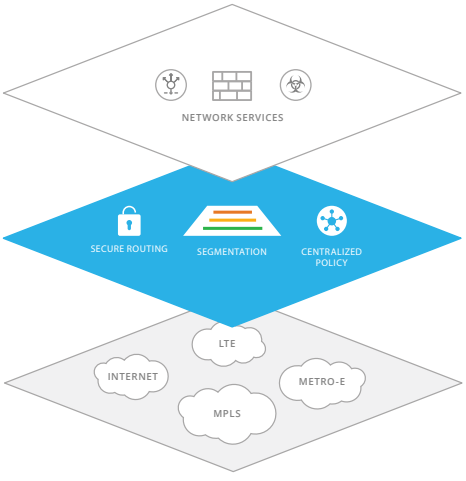

Figure 1: The Viptela Secure Extensible Network

Benefits

- Securely extend the enterprise's footprint anywhere
- Freedom to choose any transport network, independent of the carrier's service
- Optimized performance for public clouds and the Internet
- Centralized enforcement of access control and network policies
- Network-wide segmentation for lines of business, compliance, and business partners
- Centralization of network-based services

Components

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

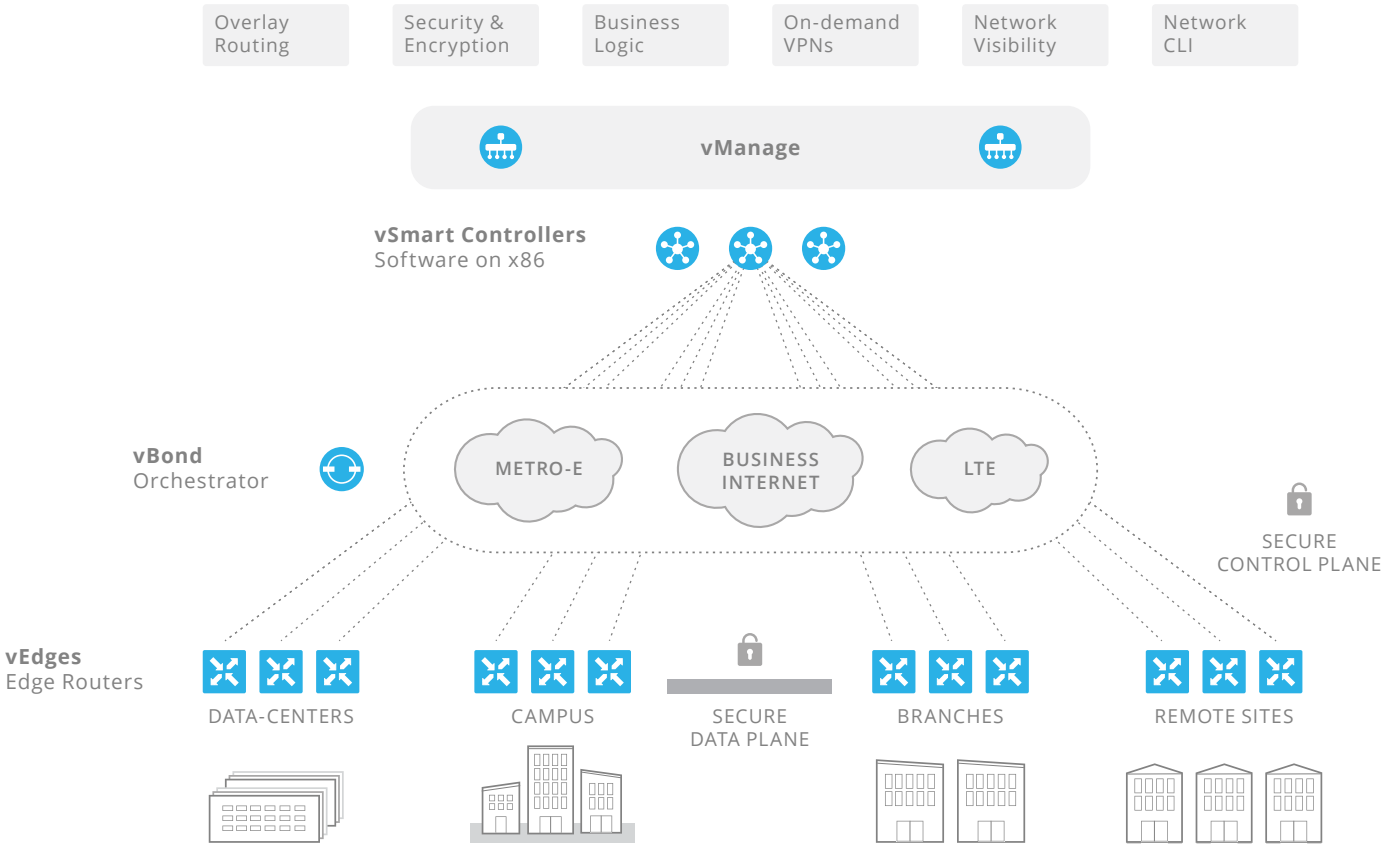

Figure 2: Components of the Viptela SEN solution

vSmart Controller

The vSmart controller is the brains of the overlay network. It establishes 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 in the SEN. There are two types of vEdge routers:

	VEDGE1000	VEDGE2000
Size	Half-width, 1RU	Full-width, 1RU
Encryption Capacity	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 8x GE 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 & Monitoring System

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

Use Cases

Transport-Agnostic VPNs

The Viptela SEN solution provides a cost-effective secure IP fabric over any underlying transport.

End-to-end Network Segmentation

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

Regional Internet Exit

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

B2B Partner Network

Enterprises with a dynamic partner ecosystem can rapidly on board business partners over any transport network.

Encryption at Scale

The Viptela SEN solution provides powerful encryption capabilities, using automated key management and device authentication to secure any network infrastructure.

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.

Features

FEATURES	BENEFITS
Centralized policy and distributed enforcement	The Viptela 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 of 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 ensures 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 operation of the Viptela network is “secure” and “encrypted.” Keys can be rotated as frequently as required without impacting performance. The SEN can scale to multiple tens of thousands of network end-points 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 the data plane, effectively providing 99.999% availability.
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.

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