NETWORKWORLD
The Leader In Network Knowledge
www.networkworld.com January 22, 2015

Viptela brings Software-Defined WANs to the enterprise

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

In April 2014, Zeus Kerravala wrote in Network World that the software-defined WAN (SD-WAN) is now a business imperative. He cites several reasons why the time is right for companies to reconsider their WAN architecture.

First of all, cloud and mobile computing, as well as applications such as video and voice over the network, are creating vastly different traffic patterns than the old style of client/server computing. Next, business agility is the enterprise mantra today, but traditional WAN architectures are too inflexible to enable the much-needed application agility. And last but not least, the complexity of the WAN makes it increasingly difficult to make even small changes in a reasonable timeframe.

I'm going to toss one more factor into the argument: cost. The cost to contract with a service provider to set up a WAN link for a branch location can be quite expensive. For example, a company can pay roughly $200 a month for 1 Mbps of link capacity. CIOs that have many branch locations claim telecom costs and transmission costs can consume a significant part of their networking budget.

The fundamental problem is that large companies often have three or more different networks. They have an MPLS network to address the connectivity needs between branches, business partners and headquarters. They have the Internet to connect to cloud applications, cloud data centers, home users and other types of facilities. And they have their Metro Ethernet network, which provides point-to-point solutions between different parts of the enterprise. The complexity of this routing architecture is the bane of the CIO, the line-of-business owner, and the network architect.

A group of accomplished architects from Cisco, Juniper Networks and Alcatel-Lucent got together about three years ago to form Viptela, Inc. to address these issues through Software Defined Networking (SDN) at the WAN level. The Viptela Secure Extensible Network (SEN) solution for architecture transformation involves five steps:

1. Enable transport independence
2. Enable security at routing scale
3. Enable network-wide segmentation
4. Centrally enforce policy and business logic
5. Insert layer 4-7 services on demand

In the first step, Viptela disaggregates the service from the physical network. No matter what forms of connectivity an organization has, Viptela builds an overlay on top of those different types of connectivity. This enables complete transport independence that is not tied to any particular form of service.

The second step is to provide security in the form of encryption and device authentication. Most approaches tackle security on a point-to-point basis, which doesn't scale well in many cases, say, for a bank with thousands of branches and tens of thousands of ATMs.

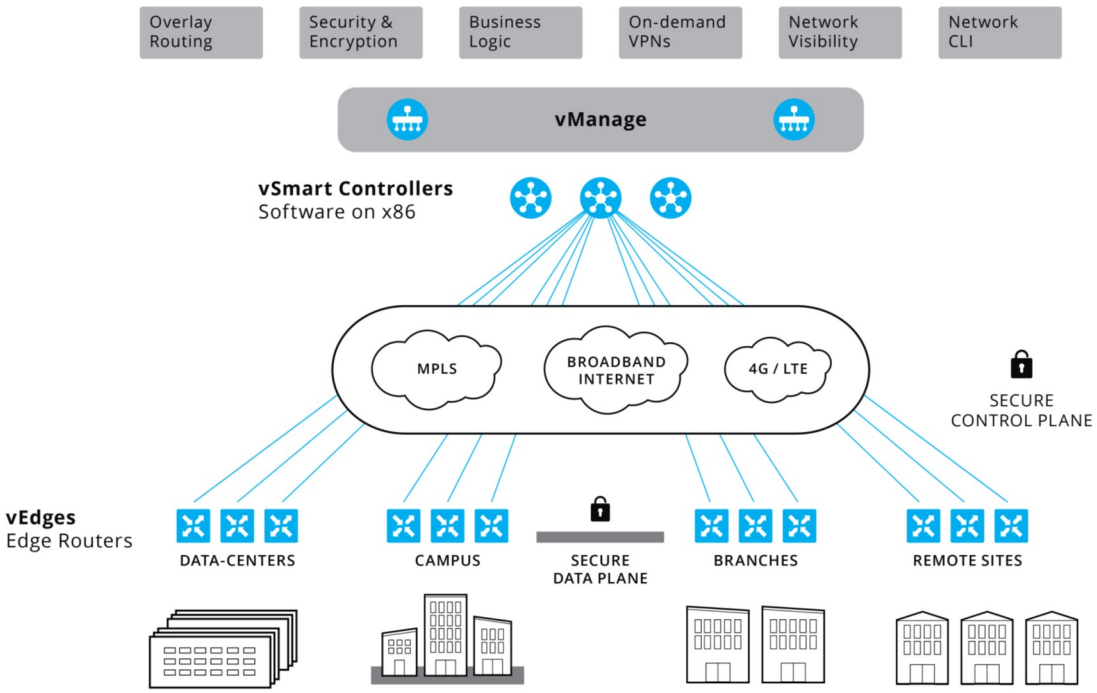
Instead, the Viptela founders took their expertise in routing protocols and developed a solution to provide encryption and security from an any-to-any perspective. It doesn't matter if it's a 10 node network or a 10,000 or 100,000 node network—they say there is no scale issue with security and there is no dependency on the size of the network with regard to encryption. The Viptela router is able to connect all entities and automatically route traffic among those as if they were on one seamless VPN connection.

The third step is network segmentation. Since Viptela technology enables the overlay, the company is able to segment the network on an end-to-end basis. Many organizations are clamoring for the ability to isolate networks from each other; for example, to separate lines of business or to create a business partner network. The Viptela solution allows an enterprise to build multiple logical topologies any way they want, and each of these different segments of network can have different encryption schemes.

Step four involves centralized policy and centralized control of all the devices across the network. Each of the locations enforce the policies of a specific location, but all of the locations are influenced by the

centralized controller. If necessary, an organization can have multiple controllers in order to meet resiliency requirements, and all controllers operate in a fully redundant, active-active mode.

And in step five, Viptela enables layer 4-7 network services to be advertised. Today there is a lot of talk of network functions virtualization (NFV) and aggregating network functions at a few locations. The big challenge is having to make changes to direct traffic to and from the services. Viptela enables organizations to spin up any third-party service on the network and connect it to the Viptela overlay. Then anyone wanting to use



those services sets a centralized policy to direct traffic to that particular location. The same principle extends to cloud services. For example, Viptela partners with Zscaler to deliver a cloud-based infrastructure to power and protect cloud, SaaS and Internet applications.

Viptela builds a secure IT fabric that connects each site of the enterprise, where every site is logically one hop away from any of the others. It is a full mesh of IPsec tunnels with centralized policy and segmentation across this network. But it could also be a combination of hub-and-spoke, partial-mesh and full-mesh if desired.

The Viptela Secure Extensible Network (SEN) solution is comprised of three major components, as shown in the illustration above.

Each different facility of an enterprise – a data center, a campus, a branch or other remote site – has a device called a vEdge router. It is a full featured IP router that performs standard functions and automatically establishes secure DTLS (Datagram Transport Layer Security) sessions with the vSmart controller. It also establishes standard IPsec sessions with other vEdge routers in the SEN.

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.

And finally, the vManage Network Configuration and Monitoring System is a centralized system that enables configuration management and monitoring of the Viptela SEN solution.

According to Viptela, the solution can be implemented in a matter of hours. The vendor says its target market is the large enterprise that has many locations, including banks, retail merchants and healthcare facilities.

The Viptela SEN solution aims to solve a number of problems that exist with today's WAN architectures. With this solution, organizations can adapt their business quickly when issues or opportunities arise. Network changes can be handled centrally across the entire enterprise, so they take hours instead of days or weeks.

New services and applications can be rolled out quickly—even high bandwidth ones like a virtual teller application. Security is improved because of increased network segmentation and the encryption from one point to any other in the network. And, networking costs can be significantly reduced. As Kerravala put it, an SD-WAN is a simpler WAN that's easier to manage, more agile, and better aligned with today's computing needs.