Transform Your Business with a Holistic Approach to Hybrid WANs

FROST & SULLIVAN

An Executive Brief Sponsored by AT&T

Roopashree Honnachari
Industry Director – Business Communication Services
& Cloud Computing Services

August 2016

INTRODUCTION

The enterprise wide area networking (WAN) space is going through a major transformation. While the traditional WAN applications—voice, video and data—continue to drive WAN bandwidth demand, the growing penetration of cloud computing, big data applications, and mobility applications are dictating new requirements on the enterprise WAN. Hybrid cloud deployments encompassing on-premises private cloud, hosted private, and public cloud are forcing enterprises to re-evaluate a hybrid WAN strategy.

A hybrid WAN strategy encompasses a combination of private and public network services. Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) are the most commonly deployed WAN solutions, as they are private networks that never touch the Internet, and that offer a high level of reliability and performance. Dedicated Internet Access and Internet-based IPsec VPNs complement MPLS VPNs as a cost-effective option for connecting distributed enterprise locations. A hybrid WAN allows enterprises to configure routing policies to keep mission-critical applications (for example, ERP hosted in a private data center) on MPLS; while low priority applications (for example, access to public cloud applications) run on Internet-based VPNs. As enterprises embrace hybrid WAN, network security and mobility are two other critical factors that need to be tightly integrated into their WAN strategy.

In this paper, we evaluate the benefits of the new and enhanced MPLS VPNs that incorporate Software-Defined Networking (SDN) and Network Function Virtualization (NFV) technologies; the value IPsec VPNs add to a hybrid WAN; the need for integrating mobility and security in enterprise hybrid WAN strategy; and how a managed solution approach can fast-track your journey to a hybrid WAN.

THE ENHANCED MPLS VPN

SDN and NFV technologies are revolutionalizing the WAN space. SDN technology does for network services what virtual machines (VM) do for servers—it enables physical network resources to be pooled together and consumed on-demand. NFV is a related network architecture that proposes virtualization technology to networks. The aim of NFV is to replace the multitude of proprietary network elements—hardware-based switches and routers usually contained within a network service provider (NSP) network—with industry standard, centrally managed commodity-based servers.

Reduced Hardware Costs: The traditional MPLS VPN network consists of managed, dedicated customer premise equipment (CPE) for various WAN functions—for example, router, WAN optimization device, security CPE, etc. NFV enables WAN functions to be deployed in software, as a virtual network function (VNF) that facilitates the shift from dedicated hardware to virtual CPE, which can be provisioned in minutes. In the enhanced VPN network, a virtualized universal CPE (uCPE) replaces multiple proprietary hardware, which significantly reduces network costs. The uCPE is a plug-and-play device that can be provisioned in minutes, is simple to manage for IT teams, and results in reduced Total Cost of Ownership (TCO) for the enterprise.

Faster Installation Times: Installation intervals or delivery times promised with traditional MPLS VPN services can range from 30 to 90 days—or more, in some scenarios. The lengthy cycle time is attributed to a number of factors, including evaluating customer site readiness, ensuring that all the required network elements are in place;

and, if not, sending a truck out to install the necessary hardware at customer site; and configuring the circuit. By combining NFV with SDN, a virtual CPE can be instantiated, and network resources can be provisioned in near real time; as opposed to months, as is the case in traditional network architectures.

The enhanced MPLS VPN offers several benefits, as detailed above. However, the growing penetration of cloud, mobility and Internet-of-Things (IoT) applications is driving enterprises to evaluate a hybrid WAN strategy to distribute traffic among private VPNs and Internet-based circuits. Internet-based services such as Dedicated Internet Access (DIA), IPsec VPN and business class broadband circuits are inexpensive and ubiquitously available, making them a great choice for offloading less mission-critical applications onto them.

THE GROWING ROLE OF IPSEC VPNS AND DIA IN HYBRID WAN

IP VPNs are CPE-based VPNs that are provisioned using tunneling protocols for emulating a private network on public infrastructure (public Internet and private IP). The various tunneling protocols include IPSec, Secure Socket Layer (SSL), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP). IP VPNs provisioned over the ubiquitous Internet makes them a great choice for unmatched global network access to connect distributed locations and remote users. Enterprises could either create site-to-site CPE-based IP VPNs to connect distributed locations, and/or implement a remote access client on the end-user device to enable remote/mobile user connectivity to corporate applications.

Remote access IP VPNs can be used to connect remote and mobile workers using multiple access methods, including Wi-Fi, mobile broadband cards, DSL and Ethernet, making use of the global public Internet network coverage. In this model, the VPN client resides on the end-user device—PC, laptops, smartphones—enabling enterprises to extend access to corporate applications to remote and mobile users, business partners, suppliers, and vendors that are geographically distributed.

Similarly high-speed DIA circuits delivered over multiple access links—copper, cable, fiber and wireless—can be used to connect branch sites with inexpensive, but carrier-grade Internet links. DIA links offer symmetrical, dedicated bandwidth with Internet, eliminating the issues that come with best-effort, oversubscribed Internet. Leading network service providers also offer managed DIA services that include faster delivery intervals, service level agreements (SLA), and self-service portal access for network monitoring and bandwidth scalability.

IMPACT OF MOBILITY ON NETWORK TRANSFORMATION

Enterprise mobility solutions help provide "anytime, anywhere" access to enterprise applications for remote and mobile employees, and are an important piece in the hybrid WAN solution. Using mobile remote access solutions, employees can use the company-provided or employee-owned mobile device to route desk phone calls, access all the IP PBX and Unified Communications (UC) features, and securely connect to enterprise VPNs. In addition to extending remote access to employees, enterprises can also use remote access solutions to securely connect with strategic business suppliers, distributors, and vendors managing inventories.

While enterprise mobility has its benefits, it also represents a challenge for IT departments to manage and monitor multiple types of devices (and applications) running over various carrier networks (and varying rate plans), and enforce policies to provision secure access to corporate applications over the device. The cost and

complexity of implementing mobility solutions, ROI concerns, and lack of internal IT expertise are some of the top-ranked challenges that enterprises face while evaluating mobility solutions. The complexity only increases with the bring-your-own-device (BYOD) option, which facilitates employees' use of their personal devices to access enterprise applications.

In this increasingly complex and rapidly changing technical environment, leveraging the skill of a managed service provider that can deploy and manage Mobile Remote Access Service (MRAS)—to extend corporate VPN connectivity to any mobile device, including laptops, smartphones, tablets, etc., using a global VPN client—can enable businesses to implement mobile applications that are optimized, convenient, and secure.

NETWORK SECURITY IS A CRITICAL PIECE

As enterprises look to hybrid WAN—consisting of MPLS VPNs, Internet-based VPNs, and mobile remote access—network security becomes a critical piece. While private VPNs ensure that the data never touches the public Internet, the fact that not all users are connected to MPLS VPNs using a dedicated secure network link, and remote users can access corporate applications over public Internet, brings with it a tremendous amount of network security risks.

The inclusion of mobility—a varied set of devices including connected laptops, smartphones, tablets, etc., trying to access enterprise applications over different access networks (3G/4G, public Wi-Fi, residential Internet access)—only increases the complexity of the network, and underlines the need for inclusion of a security solution in the network transformations.

Distributed locations, mobility, and the Internet's role in business have forced the perimeter to be virtually everywhere: in servers, laptops, tablets, and smartphones; at on-premises traffic aggregation points; in front of application servers; and at Internet gateway locations. Applying security policies at all of these locations is prudent and cost-effective. However, enterprises cannot do this alone. They need a security services partner that offers hardware platforms and software that span all of these locations, and that are supported by universal and centralized management.

In order to ensure that security is fully coordinated, enterprises should select a service provider with a deeply rooted security mindset. Provider attributes to look for include a global threat-sensing network supported by a 24x7 staff of security professionals. In addition, the provider's network services should be designed and tested following demanding standards to ensure the highest levels of attack defenses possible. Coupled with a substantial portfolio of managed security services for use in endpoints, on-premises, in the traffic-unifying MPLS IP VPN network and in data centers, enterprises gain assurances that end-to-end, comprehensive and tightly coordinated security is in place and operational—a necessity in a connected world.

WHY CHOOSING A MANAGED HYBRID WAN COULD BE THE RIGHT CHOICE FOR YOUR ORGANIZATION

As described in the earlier sections of this paper, a hybrid WAN strategy consists of multiple pieces of network solutions that need to be tightly integrated for a successful hybrid WAN deployment. Key benefits of working with a global network service provider such as AT&T, which can offer and manage the hybrid WAN are:

- Tap into AT&T's global MPLS/IP VPN network that includes NFV-based solutions. AT&T Network Functions on Demand, a key component of the AT&T Network on Demand platform, is available today in conjunction with AT&T VPN service globally across 76 countries. The solution supports a virtual router from Juniper and a virtual firewall from Fortinet, both running on an industry-standard AT&T Universal CPE, or uCPE.
- Tap into AT&T's global IPsec and DIA footprint. AT&T offers a broad footprint of IPsec VPNs and managed DIA services across US and global locations. The services are backed by AT&T network security capabilities, thus facilitating enterprises to deploy hybrid WAN solutions in a secure and cost-effective manner. In locations where AT&T's network is not available, the company will procure, deploy and manage the access network from providers, thus eliminating the need for enterprise to deal with multiple access providers.
- Tap into AT&T's integrated best-in-breed security solutions. AT&T, along with its global MPLS VPN and IPsec VPN network, offers an elaborate suite of security solutions: end-point security, Intrusion Detection/Prevention Solution (IDS/IPS), Unified Threat Management (UTM), managed CPE-based and hosted firewalls, and mobile security solutions.
- Tap into AT&T's mobility solutions. AT&T's Network-based IP VPN Remote Access (ANIRA) service and Global Network Client establish a seamless connection between the customer's existing wired VPN and all desired wireless communications networks. After a simple download, one click on their device provides mobile workers with access to the AT&T network—including 4G, 3G, IP/MPLS, broadband, and Wi-Fi connections.

Lastly, WAN management is a complex process, and requires expertise on the enterprise end for network managers to run and operate a global WAN. The process can be daunting when it involves multiple wired and wireless technologies. Most organizations are reducing their network/IT staff, to control costs, while putting pressure on existing staff to achieve operations efficiency. Working with a managed hybrid WAN provider that can deploy and manage the solution end-to-end can result in reduced TCO and improved WAN operational efficiency.

Roopa Honnachari

Industry Director – Business Communication Services & Cloud Computing Services
Frost & Sullivan
rshree@frost.com

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041