White Paper

Flexible Network-Based, Enterprise-Class Software-Defined Solutions for Hybrid Public/Private Network Connectivity

Sponsored by: AT&T

Courtney Munroe
June 2018

EXECUTIVE SUMMARY

Today's enterprise WAN networking environment is characterized by global coverage; an end-to-end software-defined, application-aware environment; and increasing use of on-demand applications. This environment is flexible enough to support an almost limitless combination of on-premise equipment, centralized configuration and management via SDN tooling, and underlying carrier-agnostic networking. Enterprise adoption of hybrid software-defined platforms that leverage diverse protocols such as MPLS-enabled VPNs for larger sites and IPSec network-based VPNs and SD-WAN for smaller locations is on the rise. Enterprises of all sizes expect flexible, secure, and robust hybrid WAN connectivity for business applications from anywhere at anytime.

IN THIS WHITE PAPER

This IDC white paper discusses the following:

- The impact of software-defined networking/network functions virtualization, including SD-WAN, facilitates application-based management and network-agnostic, dynamic policy-based routing.
- Augmenting MPLS VPN with IPSec VPN both for "same site" connectivity and as a hybrid VPN offers a unique opportunity for enterprises to connect all of their existing high-speed data, voice, and video enterprise applications over this hybrid private/public network platform with the inherent qualities of MPLS — predictable performance, security, quality of service (QoS), and low latency — along with the cost-effectiveness and ubiquity of both wired and cellular broadband internet.
- IDC believes that enterprises are most likely to select an SD-WAN/VPN communication service provider that offers a platform for managed customer premises equipment (CPE) services and managed or comanaged applications such as security and dynamic policy-based routing along with a managed MPLS VPN service that can integrate with an internet-based IPSec VPN service. This provides access to business applications regardless of location, access technology, or cost constraints.
- AT&T's MPLS-enabled VPN and IP VPN platforms combine to provide secure private IP and public internet VPN access to create ultra-flexible hybrid networks, including remote access users, that allow enterprises to connect their applications between offices, home workers, remote users, or locations, including access to public and private cloud services. This IDC white paper also examines how enterprises can leverage SDN/NFV with VPN network

applications and offers recommendations for hybrid network SDN/NFV VPN platforms. It also discusses the benefits of AT&T's FlexWare platform and MPLS and IPSec VPN platforms for secure internet VPN, remote access, and hybrid VPN network solutions.

ENTERPRISE TRENDS AND NETWORK VPN MARKET OVERVIEW

Market Overview

SD-WAN and hybrid VPNs have emerged as important components of a managed network service because enterprises increasingly depend on distributed intelligent networking and VPNs to support access to VoIP, enterprise data, storage, and security applications between all of their business sites and remote workers.

According to IDC, the North American managed SD-WAN market was $145 million in 2017 and will grow to $1.8 billion in 2022. The U.S. IP VPN market was $8.5 billion for network-based services and $1.7 billion for IPSec VPN services. This represents revenue associated with communication SPs, not vendor direct sales of CPE.

According to IDC, the North American managed SD-WAN market was $145 million in 2017 and will grow to $1.8 billion in 2022. The U.S. IP VPN market was $8.5 billion for network-based services and $1.7 billion for IPSec VPN services.

MPLS network-based VPNs provide enterprises with the best choice for predictable, managed, and secure private WAN IP network connectivity from any on-net enterprise location to any other on-net location for a whole range of business applications, including large data transfers, security, VoIP, telepresence, storage, and image and video transfers.

MPLS VPN customers can continue to maintain their own IP addressing plans and also take advantage of a communications service provider's class of service (CoS) per application to enable the appropriate quality of service. Enterprise application-specific traffic requirements such as performance, latency, and QoS map to the contracted service provider's SLA for a managed MPLS VPN service.

SD-WAN with both dynamic routing and static routing is becoming more and more critical for enterprises that need secure, distributed branch networking. As business organizations decentralize their workforces to be closer to customers or to encourage more flexible home-work environments, they are creating different VPN site types and find themselves looking for a solution that combines the best of all worlds. Datacenters need large private WAN connectivity, large locations may want MPLS with internet and dynamic policy-based routing from SD-WAN, and medium-sized locations may be dual internet with static policy-based WAN, while temporary sites or semimobile sites may be connected only via LTE.

The mobile remote worker is likely to have access to any combination of broadband, wireless 3G/4G, and/or WiFi networks and needs to securely connect to the VPN with a variety of wireless devices such as laptops, smartphones, or tablets. The integration of devices, applications, and services for onsite workers and remote workers within the same VPN network is critical, and user experience and network performance are equally important in both environments.

For remote mobile workers, a hybrid solution that includes SD-WAN and remote access network VPN services employing IPSec enables ubiquitous IP access, which is probably the single most important characteristic of a VPN (secure access over the internet or any IP connection for maximum reach for

single users or small sites). Other important attributes are centralized application management and faster and more efficient deployment of applications.

SD-WAN leveraging IPSec can be used to create secure VPNs over the internet. When used over the internet, IPSec provides point-to-point connections. IPSec secures data through encryption and authentication and allows the enterprise to maintain its own IP addressing plan through tunnels between sites. IPSec is ideal for connecting isolated company sites and mobile remote workers as well as enabling temporary connections to a VPN (events, pop-up stores, and exhibitions). It also serves as a temporary backup for an MPLS VPN network recovery.

Today, many enterprises employ more than one type of VPN service: a managed MPLS VPN for some locations, a separate IPSec VPN for remote access, and possibly even an SSL-based VPN solution for some employees. Integrating application performance requirements across an enterprise is extremely complex. Consider, for example, point-to-point IPSec tunnels — when a new tunnel is added, customer premises equipment will often need to be reconfigured in accordance with the changed logical network topology. In addition, packet characteristics may be hidden inside an IP tunnel, preventing the recognition of high-priority flows and making CoS usage difficult and limited to the edge of the network.

Enterprises continue to use one or both, and sometimes, new applications such as telepresence or business continuity can be extended to a larger number of sites and users by employing a hybrid network IP VPN solution.

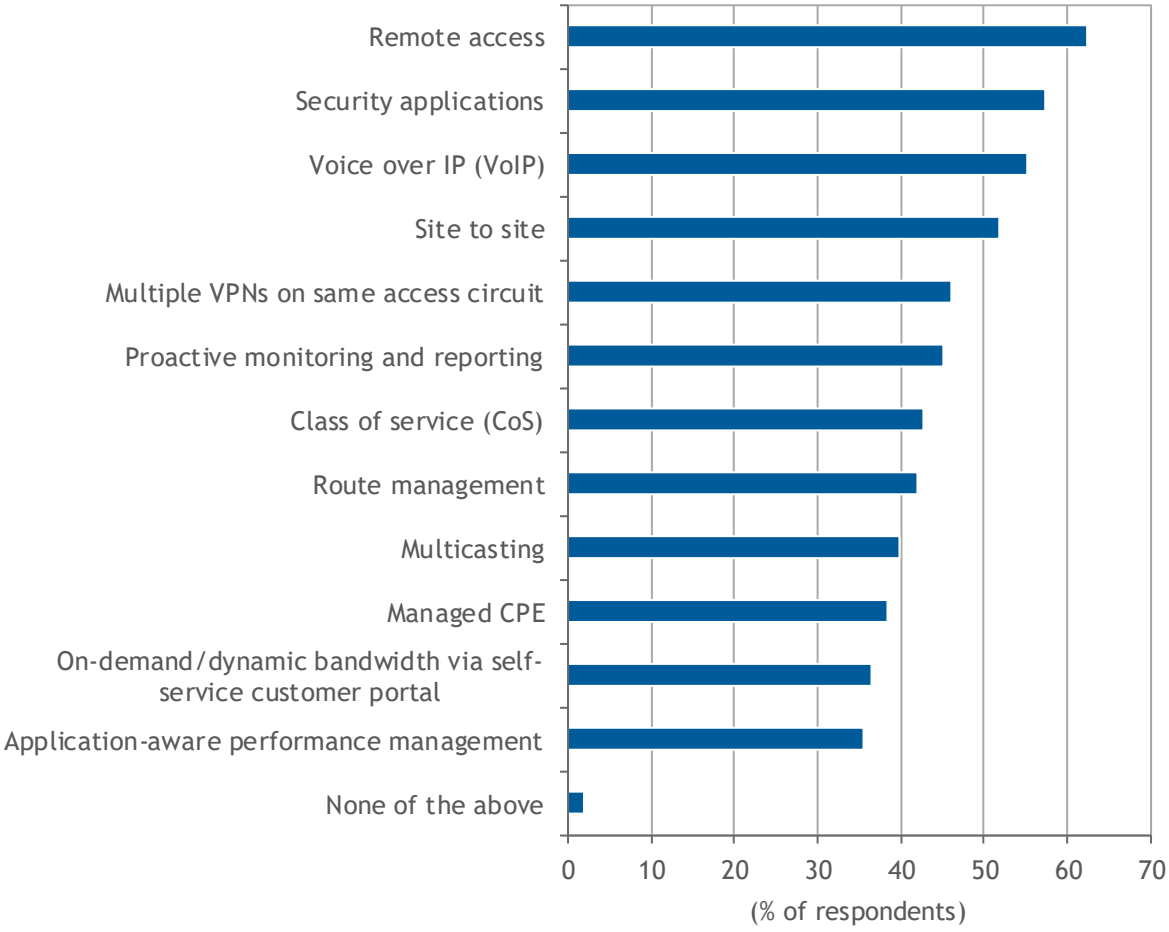
ENTERPRISE APPLICATIONS FOR NETWORK SDN, SD-WAN, MPLS VPN, REMOTE ACCESS IPSEC VPN, AND HYBRID VPN

Today, enterprises have a wide array of choices regarding distributed intelligent edge network software-defined offerings, including dynamic or static SD-WAN, managed or unmanaged MPLS or IPSec VPN, hybrid VPN, or remote access options. In addition, applications for security, WAN acceleration, VoIP, and so forth can now be presented as virtualized functions with centralized SDN configuration and management. In fact, according to an IDC survey, more than 50% of respondents use MPLS IP VPN to support VoIP over their own networks (see Figure 1).

FIGURE 1

Enterprise IP VPN Usage Trends

Q. Currently, what features/use cases have you implemented on your network-based MPLS IP VPN and which do you plan to implement within one year?



n = 401

Base = respondents who use network-based MPLS IP VPN

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is not weighted.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's *U.S. Enterprise Communications Survey,* March 2017

This section reviews some enterprise use cases and applications for each of the following types of VPN deployments:

- SD-WAN service
- Managed and unmanaged MPLS VPN service
- Managed and unmanaged IPSec IP VPN service
- Hybrid managed MPLS and IPSec network VPN service

SD-WAN complements VPNs with zero-touch deployments and centralized management of applications — and in a hybrid multinetwork environment. SD-WAN facilitates both capex and opex savings with faster, more efficient implementation of branch site connectivity. It also offers increased flexibility because remote locations can be managed in a network-agnostic manner, and applications can be optimized for QoS based on specific business requirements. Users also gain additional flexibility from centralized path control and route management, along with additional security options.

In the case of an unmanaged VPN service, the enterprise is responsible for providing the CPE device; configuring the CoS, multiple VPNs, and security attributes; and managing the impact on the VPN network when a new business application is introduced or a change to an application is instantiated. The enterprise has to self-monitor network performance.

In a managed MPLS VPN, enterprises can securely access network reports and monitor the performance, latency, and bandwidth usage of their private data, voice, and video traffic via a unique customer portal that is part of the service offering and sometimes included as part of an SLA. The ability to leverage communication SP expertise to adhere to data governance, industry compliance, regulatory, and privacy requirements is another important factor in considering a managed MPLS VPN versus an unmanaged MPLS VPN because of the cost and complexity involved with developing and administering VPN policies in-house.

IPSec-based network IP VPNs are increasingly a popular choice for enterprises trying to connect small offices/home offices (SOHOs), retail locations (restaurants, stores, and kiosks), and remote workers to their corporate VPN. Customers use a VPN appliance/firewall to provide an encrypted IPSec connection to access the internet via a broadband or wireless network or even another service provider's fixed network for these smaller sites. For remote workers, thin VPN client software can be installed on smartphones, tablets, and laptops that enables simple plug-and-play VPN connectivity choices with built-in security policies to allow VPN access via any available internet connection. The third use case involves combining both managed MPLS and IPSec network-based IP VPNs into a hybrid solution to handle an enterprise's on-net and off-net locations and workers.

Today, many enterprises have a mix of sites — including mobile workers, SOHOs, branches, and large datacenter and campus environments — that all need to connect to the same corporate network with secure, predictable network performance. A communication service provider that supports a hybrid network-based VPN, as shown in Figure 2, enables enterprises to maintain consistent service policies, application performance, and secure connectivity to corporate applications for workers from any location. However, hybrid network-based VPNs can also carry greater management challenges, making it crucial to develop a comprehensive network strategy and select the right service provider.

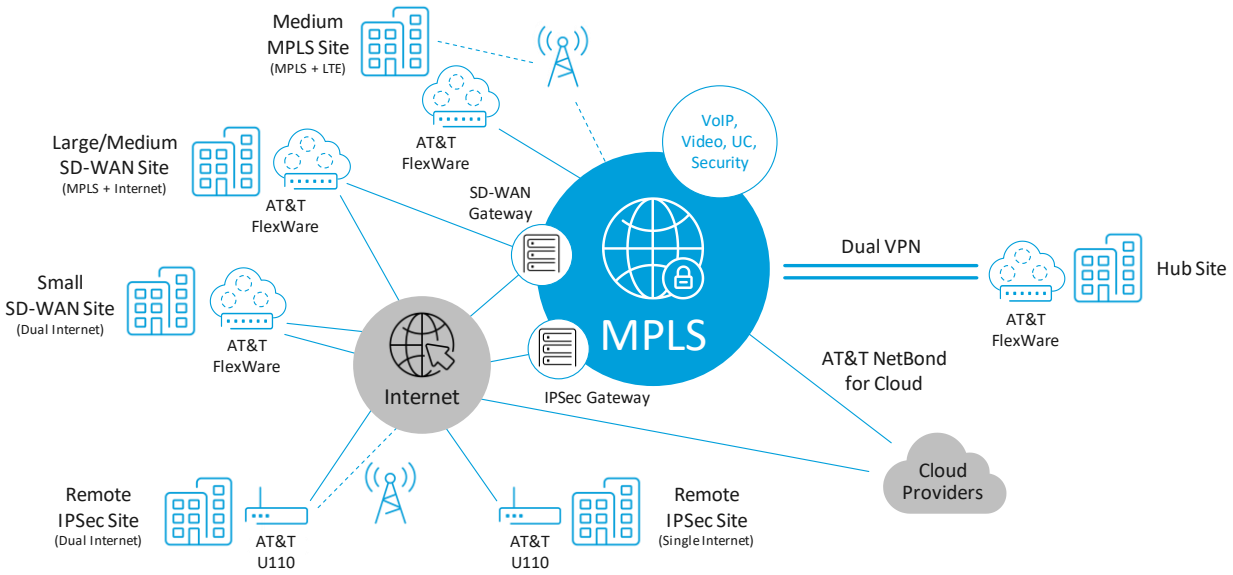
One of the more popular applications for employing a hybrid IP VPN solution is an enterprise telepresence service that extends telepresence sessions from corporate office locations that are part of the MPLS VPN network to remote access IP VPN sites or even individual workers accessing the

VPN. This can be a cost-effective form of secure internal company communication, and it is gaining popularity as corporations reduce travel budgets and increase real-time collaboration.

One of the more interesting applications for this type of hybrid IP VPN solution is employing an IPSec-based VPN that provides temporary access to corporate MPLS network-based VPN resources. Disaster recovery and failover are two applications that can utilize 3G/4G cellular networks to provide alternative VPN connectivity for MPLS-based network sites that experience an outage. This application becomes very important if a location's network VPN service is temporarily disrupted because of a cut fiber or copper cable or for wider-scale disaster recovery if a major natural disaster occurs and employees cannot travel to their business establishments.

FIGURE 2

One Integrated Hybrid Network



Source: AT&T, 2018

VPN PLATFORM REQUIREMENTS TO SUPPORT HYBRID NETWORK VPN APPLICATIONS

Today's communication service provider has to be able to offer a VPN platform solution that has the flexibility to support the use of hybrid network-based MPLS and IPSec VPN networks for diverse enterprise environments. These hybrid platforms increasingly have to provide 99.99% or 99.999% network availability and SLAs that enterprises are accustomed to with a managed MPLS VPN network.

AT&T SD-WAN network-based static solutions are designed to provide highly secure access to critical business applications regardless of location, access type, or device across a unified global platform — the AT&T Global Network. Dynamic routing to AT&T MPLS VPN services via high-speed backbone infrastructure is based on MPLS network technology, offering enterprises consistent application

performance on a global basis. The AT&T MPLS VPN solution supports service differentiation by employing CoS for latency-sensitive applications.

IDC recommends that enterprises consider a hybrid VPN solution based on the following six attributes that AT&T supports in an MPLS VPN platform and the AT&T SD-WAN network-based static IPSec platform:

- **Breadth of access and extended global reach.** AT&T's VPN solution enables consistent application capabilities for small office locations as if they were at headquarters with backup options for business continuity.
- **Flexibility.** AT&T's network flexibility provides remote access to an enterprise's intranet via the MPLS VPN, including simultaneous access to the internet via IPSec when connecting to public internet sites, WiFi hotspots, or cloud services.
- **Resiliency.** AT&T SD-WAN network-based static is easy to configure, and the on-premise AT&T VPN gateway can be combined with wireless technology as a redundant connection, restoring VPN service very quickly. The AT&T network gateways are mirrored, geographically separated, and load balanced to ensure network uptime.
- **Security.** AT&T's SD-WAN over-the-top static uses IPSec to create paths that carry encrypted enterprise data over public networks, creating a highly secure pathway. This enables integration of applications with enterprise core infrastructure from multiple types of connections, such as broadband, wireless, WiFi, or dial-up.
- **Proactive management and reporting.** AT&T provides VPN network management services, application performance reporting, and network monitoring of both MPLS- and IPSec-based VPN enterprise sites via a customer web portal.
- **Service agility.** AT&T SD-WAN network-based static is for telecommuters, mobile workers, and remote staff in an office setting. The AT&T VPN Gateway along with AT&T SD-WAN network-based static provides a complete solution for these settings. Mobility options include 3G/4G wireless or WiFi access to AT&T SD-WAN network-based static, providing fast connections and extending the reach of the enterprise VPN.

OUTLOOK FOR HYBRID SD-WAN, MPLS, AND IPSEC NETWORK VPNS

Enterprise edge networking including both LAN and WAN environments can reap tremendous benefits and flexibility with the implementation of a hybrid network and cloud-based solution that includes the options discussed in this study. SD-WAN networks combined with mesh VPNs based on MPLS or IPSec depending on the attributes of the sites can be centrally managed and optimized over any underlying network.

Enterprises expect their own IP VPN network expansion requirements will include a mix of always-connected on-net sites, remote small offices, remote workers, mobile workers, and external partner sites. A hybrid VPN platform solution that incorporates and leverages software-defined routing and management as well as MPLS and IPSec VPN solutions will be more appealing and more cost-effective for enterprises that have off-net users who infrequently access the VPN. The hybrid VPN will become important as IDC predicts that enterprise IT applications and hosting of applications will shift over time to cloud or mobile environments.

Best-in-class network IP VPN platforms can address the growing need to securely connect these business applications from any combination of wireless networks, the internet, public cloud providers, and private IP/MPLS networks.

Communication SPs such as AT&T also refine edge solutions with software-defined functionality that improves flexibility in a cost-efficient manner while providing network-agnostic options and application-centric management capabilities.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com