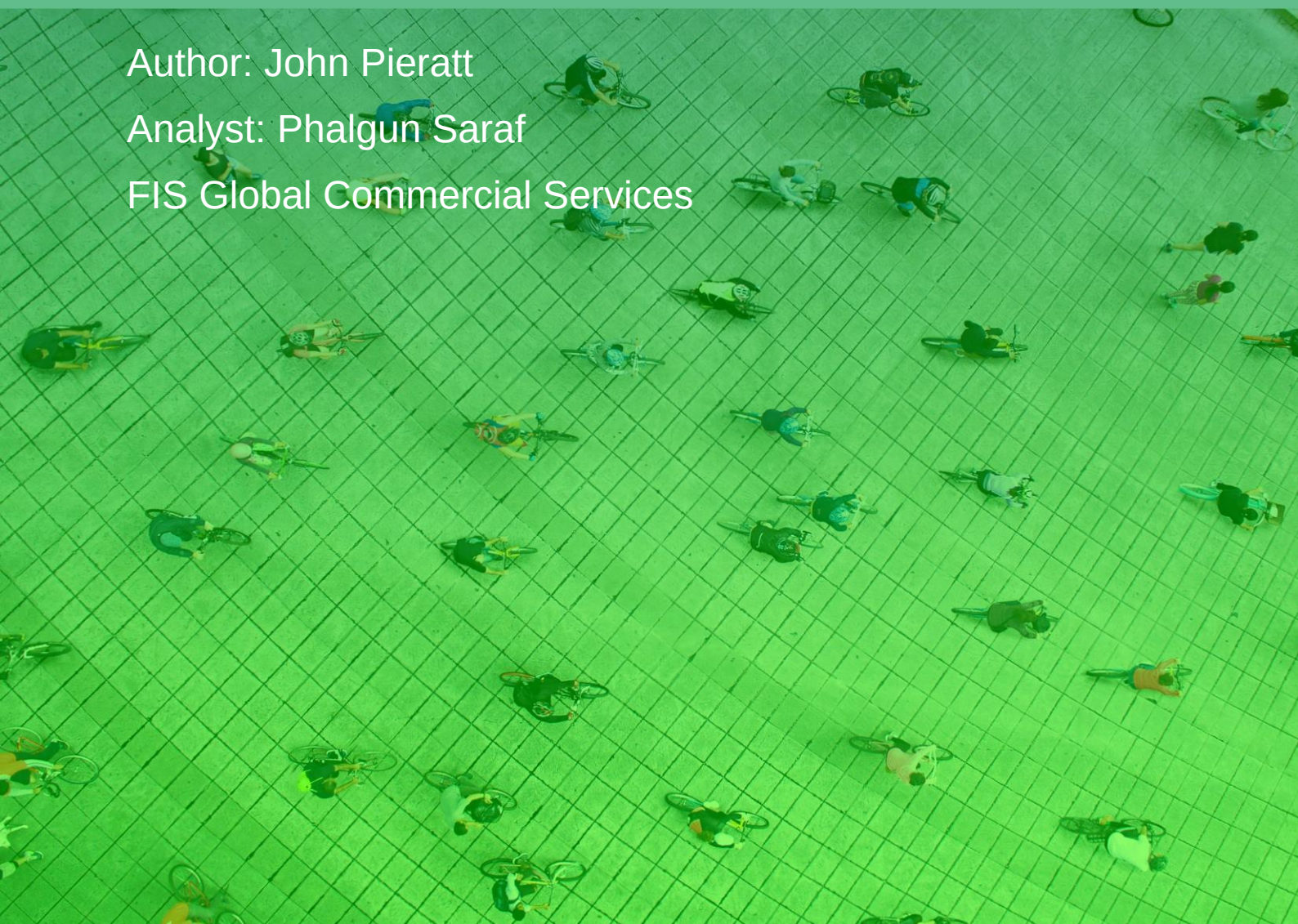
WHITE PAPER

Journey to Managed SD-WAN Services

Author: John Pieratt
Analyst: Phalgun Saraf
FIS Global Commercial Services



Executive Summary

Organizations all over the world are facing budgetary pressures to develop business strategies that reduce time to market, increase savings and strengthen regulatory compliance. They want to accelerate the pace of change, but traditional IT environments can't match that pace in modern enterprises, as they often fail to satisfy current needs and market demands. Inability to address time, budget and compliance-related challenges significantly weakens an organization's industry position and slows growth. With new service models like IaaS, PaaS and SaaS, businesses strive to gain increased agility, flexibility and scalability.

Business connection requirements have outgrown the ability of MPLS WAN to connect remote offices, data centers and the cloud. SD-WAN technology helps in creating hybrid networks that join multiple access technologies such as IP services, dynamic traffic routing and real-time connection provision, based on available bandwidth or selected criteria, as well as reducing aggregate bandwidth costs.

Software defined networking (SDN) is now a focus area in enterprise networking. This approach of decoupling and encapsulating the software (control plane) from the hardware (forwarding plane) is opening opportunities for network programmability and creating flexibility in network construction that diverges from the legacy vendor-locking ecosystem.

SD-WAN's focus is to redefine efforts towards provisioning, management and optimization of WAN, connecting enterprise networks in a software-centric way and bringing cost-effectiveness and simplicity in managing these connections. Furthermore, for distributed enterprises, maintaining a secure, reliable and high performing wide area network (WAN) for every remote site can be an IT department's biggest and most costly challenge. SDN prevents any kind of breach or security lapse as there are separate isolated segments for each application or database, which helps in creating a robust security mechanism.

SD-WAN setup should be transport agnostic in order to ensure the organization isn't tied to any specific vendor and can adopt new transports as they become available. With SD-WAN, enterprises add multiple transports into the mix. SD-WAN technologies enable us to manage them as a single fabric instead of separate and distinct networks. SD-WANs that use hybrid networking can increase mobility at the remote locations and easily and securely deliver new apps, including high-definition video, collaboration apps and omni-channel applications.

According to Gartner, SD-WAN is specific to enterprise WANs and applies to branches of all sizes, geographies and vertical markets. SD-WAN provides the greatest benefit for organizations that are:

- Moving toward a hybrid WAN topology to support public cloud services.
- Seeking to reduce traditional business-class carrier services budgets.
- Wanting to reduce management complexity of their WAN.
- Looking to reduce the cost of existing WAN remote branch equipment, often during a refresh cycle.
- Working with a large number (more than 25) of remote branches.
- Aggressively deploying video to branch office locations.
- Maintaining limited or no IT personnel on-site in remote branches.

Challenges with traditional networks

Digital transformation is essential to business agility, and despite countless new apps and technologies, some distributed enterprises with outdated or underpowered WANs find transformation beyond reach. Organizations expect their current WANs to do more without additional CapEx investment.

Legacy routing protocols: Any change to topology or segmentation requires retuning (at best) or redesign (at worst) of your routing protocols. Many of these routing protocols interact with service provider routing protocols, which further adds complexity and reduces business responsiveness.

Security: Traditional networking technologies aren't well suited to dynamically implement new security postures based on changing topologies or threats. They are also challenged when it comes to providing differentiated security services based on application type and context. Securing multiple distributed locations is a challenge for IT departments due to the intricacy of remotely managing multiple network devices, temperamental VPNs, vulnerable internet connections and applications with conflicting security and performance requirements.

Vendor lock ins: Legacy networks are generally built with one vendor's proprietary switches and routers. Every three to five years these need a refresh, considering each location requires many different network devices to perform basic business operations. In addition to the price of the infrastructure, the cost includes implementation, upgrades, maintenance plans, network integration and support fees.

Problematic monitoring: Legacy WANs have multiple hardware and software portions that are difficult to monitor continuously. There is no encapsulation of underlying hardware, which makes it difficult to administer. Furthermore, legacy WANs are also unable to easily gain visibility into cloud and SaaS apps.

Benefits of SD-WAN

Replacing hardware with software: SD-WAN enables organizations to focus on business benefits from application centricity rather than worrying about physical hardware and network connectivity. It allows administrators to tie applications, users, policies and security together across the network without getting into the nitty gritty of traffic and bandwidth management, thus reducing costs.

Centralized monitoring: The SD-WAN provides centralized control and monitoring of all organization-owned components or moving parts. One of the primary benefits is the ability to monitor all service level agreement (SLA) transport paths. Centralized control provides a holistic view of enterprise SD-WAN performance and allows network administrators to monitor all the transport paths.

Network segmentation and security: Centralized control also supports strong security by creating a dynamic security perimeter that implements enterprise-level security at branch locations. Because the security perimeter is implemented with software, network administrators can verify compliance with security requirements at any time.

Business agility: Rapid implementation of WAN services to remote offices without the need for technical on-site support. The bandwidth can easily be adjusted (expanded or decreased) depending on business needs.

Bandwidth cost reduction: Network is readily available, quick to deploy and comes at a much lower cost than equivalent MPLS networks. SD-WAN provides the reliability and security benefits of WAN services at lower prices.

Optimized for the cloud: SD-WAN eliminates the constraints of MPLS networks and integrates security, performance and connectivity between cloud and workplace, significantly improving the experience for users in remote locations when they use SaaS or cloud-based applications.

Work with FIS Global Commercial Services

Our SD-WAN Solution

A proven cloud services partner, FIS is the largest fintech company in the world providing a full range of enterprise-class IT services – with a track record of successful SD-WAN deployments. Our SD-WAN solution

provides the increased bandwidth, centralized management of branch offices, in depth analytics and highly secured access that financial institutions and the banking industry require.

Dynamic path selection: Dynamic multi-path optimization is comprised of automatic link monitoring, auto detection of provider, and auto configuration of link characteristics, routing and quality of service (QoS) settings.

Smart QoS: Granular classification of 2,500+ applications enables smart control. The defaults set the QoS policies for core business objectives with IT, required only to establish traffic priority. Being aware of the application profile enables automation of bandwidth allocations and QoS configurations.

Application performance monitoring: FIS continuously monitors performance of critical voice, video or data applications with the ability to alert IT staff. This analysis provides administrators a comprehensive before-and-after view into application behavior on individual links and the SD-WAN enhancements.

Zero-touch deployment: SD-WAN Edge appliances automatically connect, authenticate and obtain configuration instructions once they are connected to the network in this deployment. Our SD-WAN solution gives the customer a highly available deployment model that integrates the existing network with support for OSPF routing protocol and benefits from dynamic learning and automation.

Security: Stateful and context aware, integrated next-generation firewall delivers granular control of micro applications and support for protocol-hopping applications such as Skype. The secure firewall is user and device OS aware with the ability to segregate voice, video, data and compliance traffic. Corporate policies for BYOD devices are easily controlled. Each application is also assigned its own virtual application network to protect against breach propagation, known as micro segmentation.

Lower cost of ownership and managed services: We significantly streamline enterprise-wide SD-WAN implementation and eliminate the need for IT departments to maintain their own SD-WAN data centers. This results in very fast time to execution for initial installations and future upgrades, and can be done at web scale and at the lowest possible cost. This service also provides round-the-clock monitoring, alert notification, hardware and software troubleshooting, diagnostics and issue resolution.