TITANIUM

BY FULCRUM IT PARTNERS

The retail IT leader's guide to migrating from MPLS to SD-WAN

Table of contents

Executive Summary

The enterprise network in the retail space has undergone a transformation in recent years. Covid-19 has forced many bricks and mortar stores to develop eCommerce offers, and demand for in-store digital services and an omnichannel customer experience is putting additional pressures on the network. No longer is it predominantly on-premise, it's now also in the cloud.

Back at HQ many departments are still operating remotely or using hybrid models, benefitting from cloud platforms but putting even more pressure on legacy networks. All these factors, and more, are driving the adoption of next generation technologies like SD-WAN.

While traditional networks using technology such as MPLS are not completely redundant, retailers that want effective, scalable and affordable ways to deliver the services customers and staff want, do need to ensure their networks are optimised for an omnichannel experience.

Problems with latency and poor performance are barriers to productivity, competitiveness and profitability, which is why IT leaders in the retail space need solutions that work for physical and digital channels.

In this guide we explore these challenges and how you can design and deploy a secure network that reduces complexity and costs while improving performance and security.improving performance and security.

Understand the jargon!

Throughout this guide we use various acronyms. Here is a quick glossary of networking terminology.

LAN

A LAN, Local Area Network, comprises all the components - cables, access points, switches, routers etc. - needed for devices to exchange data securely in one physical location. In a business environment, such as an office, a LAN ensures employees and guest users can access your corporate network when working at that location.

WAN

When an organisation has multiple LAN environments, such as in different offices, a WAN connects these smaller networks across longer distances. WAN, Wide Area Network, refers to a group of networks distributed across a large geographic area - different cities or countries - which are connected to each other so they can exchange data. Typically these networks are run in a private environment, your organisation's, to allow secure operations across multiple sites including business premises and remote hubs.

MPLS

If you're reading this guide it's probably because you're already using MPLS technology and are exploring updating or replacing it. MPLS stands for Multiprotocol Label Switching. It routes data packets (for example when you send an email, use VoIP or video conferencing) from one internet router to its destination using labels. These labels contain information about the data packet's priority level and forwarding decisions - a predetermined path that routes traffic using the shortest path over private wide area networks.

SD-WAN

Software-Defined Wide Area Networks (SD-WAN) are next generation WANs that enable end-to-end enterprise connectivity to corporate applications, cloud services and workloads regardless of location. As the name suggests, SD-WAN makes the network control and management processes available as software so they can be configured and deployed easily. It is a highly flexible and scalable solution that connects remote networks across large geographic distances.

It should be noted that SD-WAN doesn't necessarily replace MPLS. SD-WAN networks can manage multiple types of connections, including MPLS, and route traffic over the best path in real time. It connects your sites (offices and remote workers) to your cloud environments using multiple connectivity services such as Azure Virtual WAN, AWS Transit Gateway, MPLS, internet and even 4G/5G.

Secure SD-WAN

Secure SD-WAN integrates a retailer's network infrastructure and security architecture, enabling networks to transform at scale without compromising security. This approach, pioneered by cybersecurity companies like Fortinet, combines next-generation firewalls with SD-WAN networking capabilities to provide consistent security enforcement across flexible perimeters. It also eliminates MPLS-required traffic backhaul to deliver an improved user experience without compromising security.

SASE

Secure Access Service Edge (SASE), pronounced 'sassy', is an enterprise networking and security concept first defined by Gartner. SASE packages up different network security functions, such as SD-WAN, SWG, CASB, ZTNA and FWaaS, into a unified, cloud-native service.

SSE

A component of a SASE solution, SSE stands for Security Service Edge and can also be deployed independently. SSE is the convergence of SWG, CASB, and ZTNA network security functions into a single cloud service.

SWG

Secure Web Gateway (SWG) protects end users from threats such as phishing and malware from the internet.

CASB

Cloud Access Security Broker (CASB) are security policy enforcement points that can be on-premises or cloud-based, which interjet when a cloud-based resource is accessed that is governed by a specific policy or policies. These include, but are not limited to, authentication, single sign-on, authorization, credential mapping, device profiling and encryption policies.

ZTNA

Zero Trust Network Access (ZTNA) is a solution that hides an application or set of applications from discovery, public visibility, reducing the surface area for attack. To access the application, end users are verified based on identity, context and policy adherence criteria.

FWaaS

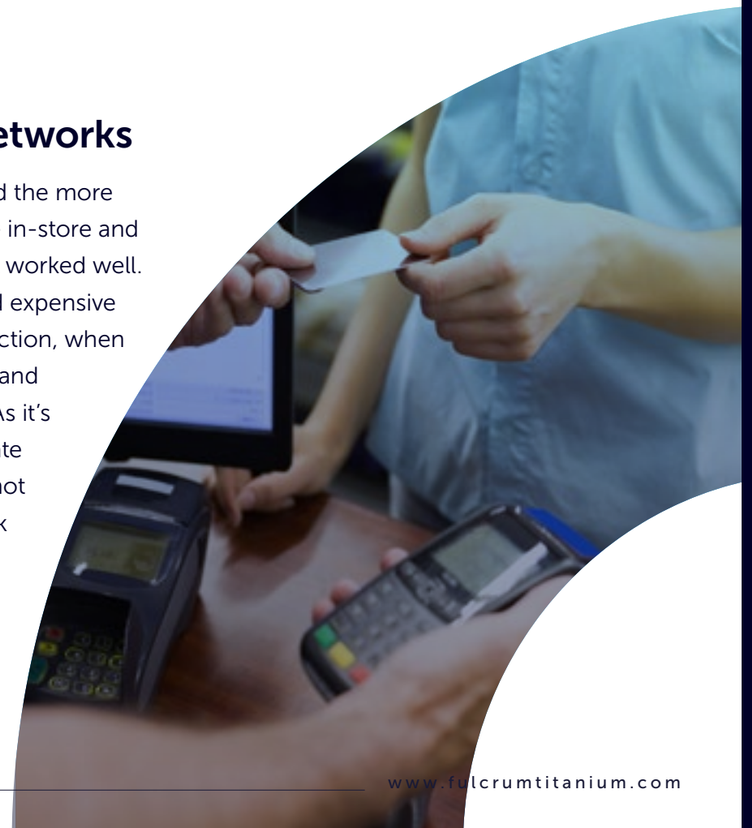
Firewall as a Service (FWaaS) combines next-generation firewall security with a unified threat management (UTM) platform to protect from advanced threats. FWaaS is a cloud-based service that provides hyperscale, next-generation firewall (NGFW) capabilities including web filtering, advanced threat protection (ATP), an intrusion prevention system (IPS) and more.

Why migrate to SD-WAN?

A traditional enterprise WAN utilising MPLS involves installing physical MPLS circuits at multiple sites so that data packets can be transported between them. For example, between a branch and a corporate data centre based at HQ. This approach is secure and effective, ensuring data is moved quickly along predetermined paths and is protected within a virtual private network (VPN).

The benefits of MPLS networks

Before the advent of cloud services, and the more recent blurring of the lines between the in-store and digital customer experience, this model worked well. While legacy MPLS can be complex and expensive compared to a standard internet connection, when used as originally designed it's efficient and provides a good end-user experience. As it's a virtual private network it is also separate from the public internet and therefore not vulnerable to some types of cyberattack such as denial of service attacks.



MPLS and the cloud

But once you start integrating cloud-based services such as mobile POS systems, electronic price tags, NFC and VR technology and in-store apps, or run back-office apps in the cloud, MPLS becomes more of a barrier to productivity than an asset. That's because with MPLS all traffic from the cloud needs to go through a central hub, corporate HQ, before being sent on to a branch or end-user. It's a hub-and-spoke connection model. This creates a pinch point which is exasperated by the bandwidth required by many cloud services, such as video and mobile apps.

Backhauling traffic from a remote site (shops or a remote workers' home offices) via the data centre at HQ, wastes bandwidth, increases latency and slows down network and application performance.

For many retailers it is more effective to send traffic directly to the cloud and remove the MPLS pinch point altogether. If your business has migrated fully to the cloud a legacy MPLS network is likely to be expensive to maintain and does not provide you with the flexibility and scalability digital services require.

New technologies for today's network architectures

This is where SD-WAN steps in. SD-WAN supports multiple connection types, such as broadband, 4G/5G LTE and also MPLS. It uses rules and policies to select the best path to send traffic, instead of the predetermined paths MPLS uses. For example, SD-WAN technology identifies data packets by application, user, source and destination and then selects a WAN link based on network conditions, traffic characteristics and your quality of service (QoS) requirements. It applies policies across all WAN devices so data is sent by the most efficient and secure route depending on its attributes. This is known as dynamic path selection.

This centralised approach also increases network security as it can apply internal security policies across the entire network. This has clear benefits when utilising cloud applications that require secure remote access such as Amazon Web Services (AWS) or if you provide customers with services like free in-store WiFi. Security for cloud apps can be integrated into your connectivity fabric, with mission-critical data and traffic protected and segmented from other parts of the enterprise network.

Hybrid approach

Retailers that have on-premise data centres and legacy apps may still have a MPLS network requirement. If you need to transport data from a shop to corporate HQ, or between branches, an existing MPLS network is a secure and effective way to do this.

In this scenario a hybrid approach is an option and, as explored earlier, SD-WAN solutions route network traffic in the most efficient way possible to meet your QoS requirements, which could be via a MPLS connection.

SD-WAN summary of benefits

Whether you continue to use your MPLS network for some traffic or not, SD-WAN can support your legacy workloads as well as new digital services. Here are the key advantages of migrating to SD-WAN:

1: Supports omnichannel strategies

Gives customers and employees a consistent and equal experience, boosting their productivity and helping the business become more competitive and profitable.

2: Improves performance

SD-WAN is configured to prioritise business-critical traffic and real-time services and route them by the optimal path. This reduces latency issues, and packet loss, and improves productivity - and your ability to collect payments.

3: Reduces site visits

SD-WAN simplifies and optimises your network with a single, centralised solution in the Cloud, reducing visits to physical branches. If you take advantage of a Managed SD-WAN, the service provider will be responsible for most site visits relating to the service.

4: Reduces costs

A Managed SD-WAN service can reduce costs by aggregating licensing across multiple sites and reducing your total cost of ownership. It also moves traffic away from expensive MPLS networks, leveraging low-cost local internet access where appropriate, as well as direct cloud access.

5: Improves the in-store customer experience

Customers want digital technology in-store such as interactive fitting rooms, free WiFi and charging hubs, mobile POS systems, electronic price tags, NFC and VR technology and in-store apps and kiosks. To deliver this level of in-store customer experience your network must do a lot of heavy lifting. SD-WAN improves network uptime, performance and redundancy.

6: Supports expansion plans

SD-WAN can reduce the time it takes to install and configure the network infrastructure at new sites, and the time it takes to deploy new online services. SD-WAN scales and flexes with your business' needs. It can also overlay and integrate any legacy networks that you "inherit" because of M&A activities.

7: Protects the brand

Customers are often quick to complain about poor service and it's never been so easy to give a retailer a bad review. Any inconvenience such as an issue with a POS or the free WiFi not working, could result in a negative comment on social media or on a review site. SD-WAN can prevent service disruptions by utilising automatic failover, and as it constantly monitors the network it knows the optimal path to send business-critical traffic at any given time.

8: Helps you get the benefits of the cloud

Enabling direct cloud access from a branch or remote site, eliminates backhauling traffic so cloud applications perform at their best. This also improves network performance across other areas of the network - as traffic to the cloud is no longer routed to HQ first.

9: Boosts security

SD-WAN allows you to apply corporate security policies across the entire network, on-premise and in the cloud. A Managed SD-WAN service can also limit PCI scope and reduce your compliance costs. By outsourcing to a MSP, PCI-DSS compliance for that part of your infrastructure is their responsibility.

10: Reduces complexity

Customers want digital technology in-store such as interactive fitting rooms, free WiFi and charging hubs, mobile POS systems, electronic price tags, NFC and VR technology and in-store apps and kiosks
To deliver this level of in-store customer experience your network must do a lot of heavy lifting.
SD-WAN improves network uptime, performance and redundancy.

Use cases for SD-WAN

Multi-site organisations

Retailers with multiple sites often have a complex IT infrastructure that creates many headaches for the IT team. This is especially true when sites have been added through mergers and acquisitions, which all need to be securely connected but may be using diverse networks and technology.

Inconsistent technologies deployed across individual sites create vulnerabilities and a lack of visibility of cybersecurity threats, potentially increasing the attack surface if networks are not connected securely. It also means the user experience (whether for customers or staff) is inconsistent between different locations, which can be detrimental to the brand and profitability.

As SD-WAN can overlay existing connection types, it can be deployed quickly to secure all networks and integrate them with corporate security solutions. For example, all traffic can be routed through a next-gen firewall to provide a high performing security perimeter encompassing all new and existing sites.

By accessing a Managed SD-WAN service you can substantially reduced management overheads and captured the following key benefits:

- High-quality, fast, dependable and consistent connectivity at all its sites
- More time to focus on strategic IT activities as your Managed Service Provider (MSP) manages the service and technical support
- Lower costs via bill consolidation and generating maximum economies of scale for the business
- Flexibility and scalability that's aligned with the business' growth strategy: a solution that can be quickly deployed across new sites
- Increased visibility and management across its whole estate from a single 'pane of glass'

IVC Evidensia case study

For a real life example of how SD-WAN supports growing businesses, read our case study with veterinary group IVC Evidensia. Click here.

Deliver an in-store digital experience

Unlike legacy in-store technology, the solutions customers and staff want to use today are almost entirely in the cloud. For example, a mobile POS system (mPOS) uses mobile app technology to take payments from anywhere in the store on a smartphone, tablet or wireless device. Customers don't need to go to the checkout, staff can process their payment anywhere where there's connectivity.

Similarly, RFID solutions for stock management are cloud-hosted. These solutions are used for stock inventory but are also a useful customer service tool, enabling shop floor staff to check the availability of goods, and if an item is out-of-stock locally arrange a home delivery or click and collect service from another store or warehouse.

While the network infrastructure needs to be fit for purpose to utilise these technologies, i.e. no connectivity black spots, SD-WAN will continuously optimise the network to ensure staff and customers can access these services.

Free your IT team from time-draining site visits

A Managed SD-WAN service not only provides the visibility need across the entire network to optimise performance remotely, but also gives you access to a team of networking experts. If managing the network is taking your team away from other critical activities, especially factoring in the time it takes to travel to and from retail sites, this is a perfect solution.

Specialist Managed Service Providers also reduce internal overheads and help address recruitment challenges in a field where there is a significant skills shortage.

Remote and hybrid workforce

Many office-based staff in retail companies continue to work remotely, or only visit the office for a day or two each week. When remote workers are reliant on their home broadband connection or VPNs they often have an unequal experience compared to their colleagues working in an office due to poor network performance and bandwidth contentions. They may also pose a security risk if accessing business-critical applications via an unsecure connection.

SD-WAN uses your business' policies to determine the best pathway based on the characteristics of both the data packet and its source and destination. This includes security policies so the more critical the data packet, and more vulnerable it is, the more secure the pathway selected

In a home working environment SD-WAN enables some traffic to go to the corporate HQ; some to go directly to cloud services (Microsoft 365, AWS etc.) under the company's rules and parameters; and other traffic is routed externally - such as traffic to social media sites. This ensures critical data and applications are protected while freeing up the company's bandwidth and infrastructure from less critical and sensitive traffic.

Should you roll out SD-WAN for remote workers?

Not every employee working from home needs SD-WAN. If end-users just need to access cloud applications like Microsoft 365, their access is governed by your security policies and identity and access controls, and SD-WAN is probably not needed.

However, if they need to access larger applications in the cloud or on-premise, or if the increase in productivity offsets the cost of the SD-WAN, this option is worth exploring.

How to overcome migration challenges

Before you embark on a migration from MPLS to SD-WAN it is helpful to understand what factors might stand in your way to a successful transition, and how to overcome them.

In our experience of helping retail businesses migrate to SD-WAN, these are the most common challenges you can face:

1: Lack of internal capacity and experience

According to Gartner a true SD-WAN solution supports zero-touch provisioning (ZTP) which in theory means deployment is straightforward. When provisioning branches or home users, ZTP allows your IT team to remotely provision a router anywhere in the WAN.

However, you still need the expertise and time to design the network solution, select and install the SD-WAN products and set up SD-WAN network management and monitoring.

As with any IT project, best practice is to conduct an internal skills and resource assessment and address any shortfalls with training, hiring or engaging external support.

2: Selecting the wrong product

The WAN is mission-critical and therefore the selection of a SD-WAN product cannot be taken lightly. Before you select a product you must have a clear picture of what it needs to do, and how it will integrate into your existing IT environment.

Key points to consider include:

- Integration with legacy routing protocols such as BGP and OSPF
- The ability to talk to legacy non-SD-WAN sites and work across MPLS networks, as well as the SD-WAN fabric
- The ability to scale the solution as new non-SD-WAN sites are added during the transition, and later if new sites are acquired
- Interoperability with security solutions
- A consumption model that works for your business.

3: No clear business case

When selecting a SD-WAN product it must also be aligned with your business case for transitioning to the technology. As explored earlier in this guide there are many reasons retailers migrate from MPLS to SD-WAN, and advantages when you do.

Be clear why you're embarking on this transition and what your expectations are before you choose a product. Some products work better with a legacy infrastructure than others, but perhaps do not deliver the SD-WAN innovation you may want. Other products may be more focused on SD-WAN and offer poorer integration with legacy protocols. If reducing costs is a driver for the migration then consumption models will help determine the right product.

With a clear business case for migrating to SD-WAN you can better evaluate different vendors and solutions.

4: Lack of planning

As explored in the next section of this guide, planning is a vital step to a successful migration. To minimise disruption you will need to:

- Understand how the SD-WAN solution connects to your data centre, cloud and security stack,
- Create a standardised template for your branch architecture,
- Factor in any network upgrades that might be required, such as new circuits, routers or IPs, and when this work will be complete,
- Identify how your applications will utilise the SD-WAN, andPlan how legacy sites will interoperate until they become SD-WAN sites.

It is also vital that your project team knows exactly what their responsibilities are and who will do what. At this stage you may also want to revisit your internal capacity and expertise. Bringing in external support to help deploy the solution or provide a Managed SD-WAN service, may be the best option for your team, instead of the DIY approach.

5 steps to a successful MPLS to SD-WAN migration

Whether you are planning to replace your MPLS network completely with SD-WAN or operate a hybrid network, we recommend following these steps to ensure a successful migration.

Network audit and review

Start with your current network and conduct an audit and review across all sites. This should include:

- **Devices**: what devices are connecting to your network including BYOD
- **Cybersecurity vulnerabilities:** a network survey will help you identify any vulnerabilities such as outdated security patches
- **Bandwidth demand:** review the current usage and distribution of your bandwidth
- **Network infrastructure:** audit any problems with your network. infrastructure
- **Data security:** review data and file security and current controls and policies
- **Network upgrades:** identify any poor performing hardware.
- **Future demand:** if the migration is designed to create a network infrastructure that will support new digital services, you will need to estimate how much additional bandwidth will be required.

Network design

SD-WAN network design should take into account the existing network infrastructure and what can be kept, what needs to be upgraded and what connections should be replaced. SD-WAN can overlay your existing network, but existing routers and gateways must be able to integrate with the SD-WAN solution.

A key aspect of SD-WAN design is how it integrates with the cloud and how it manages policy enforcement, encryption, external traffic routing and application performance.

At this stage you will decide on the right SD-WAN product and services for your needs.

Migration roadmap

The next step is to develop a roadmap which will chart the steps that need to be taken technically and practically to transition from your current network to SD-WAN. This will include controls and process maps, key tasks, KPIs and deliverables, milestones and deadlines.

Depending on the size of your network, migrating from MPLS to SD-WAN is generally not something that can be done overnight. For many retailers your legacy network will be connected to the SD-WAN for some time as you move each site to SD-WAN.

A controlled step-by-step approach is essential to manage disruption and ensure the migration doesn't impact your company's ability to trade more than necessary. A site-by-site approach is also advantageous as it is not uncommon to uncover hidden issues during the migration project. These issues can then be resolved before migrating the next site to SD-WAN.

SD-WAN migration

Now the magic happens! The technology is installed and configured, tested and deployed. With detailed planning this should progress according to your migration roadmap and result in a successful transition to SD-WAN.

Optimise, monitor and manage

After your new technology and services go live, you now enter a period of optimising performance before transitioning to BAU.

At this stage there will be further opportunities for optimisation and improvements to fit the evolving needs of your business. SD-WAN's dynamic pathway selection is designed to accelerate data traffic, but it can only do this if it's given the right information. Ongoing optimisation will help you make the technology work harder for your business, and get a better return on your investment.

Our approach

Fulcrum Titanium provides a Managed SD-WAN solution that ensures our retail customers not only get the benefits of secure SD-WAN, we also monitor and manage the technology for you - optimising the performance of your critical applications.

We practice what we preach, following the migration steps outlined in this guide and then supplying a high-performance, secure and affordable service. Our SD-WAN managed service features:

- Managed installation with engineers on site
- Zero touch provisioning
- Routing of applications based on configured policy
- Complete visibility of network conditions and security landscape
- Intuitive user interfaces
- Dynamic propagation of changes
- Centrally defined security policy
- 24/7 service desk with 4h break-fix on parts

Powered by Fortinet

Fulcrum Titanium has partnered with Fortinet, one of the most trusted names in network security and a Leader in the Gartner®2021 Magic Quadrant™ for WAN Edge Infrastructure.

Fortinet Secure SD-WAN delivers the following key business outcomes:

Improved User Experience: An application-driven approach provides broad application steering with accurate identification, advanced WAN remediation, and accelerated cloud on-ramp for optimised network and application performance.

Accelerated Convergence: The industry's only organically developed, purpose-built, and ASIC-powered SD-WAN enables thin edge (SD-WAN, routing) and WAN Edge (SD-WAN, routing, NGFW) to secure all applications, users, and data anywhere

Efficient Operations: Simplify operations with centralised orchestration and enhanced analytics for SD- WAN, security, and SD-Branch at scale

Natively Integrated Security: A built-in next-generation firewall (NGFW) combines SD-WAN and security capabilities in a unified solution to preserve the security and availability of the network

To find out more, book a discovery call with our network security team.

CLICK TO BOOK A DISCOVERY CALL

Next Steps

Do you have any questions? If you want to learn more about migrating to SD-WAN or would like to explore further whether it's right for your business, speak to us.

Book a free 30 minute, no obligation discovery call with one of our network consultants to discuss your objectives, ask any questions and take the next step.

CLICK TO BOOK A DISCOVERY CALL

About Fulcrum Titanium

Fulcrum Titanium specialises in integrating state-of-the-art technologies to offer businesses comprehensive, straightforward solutions, which are proactively supported and enable organisations to operate with ease.

Founded in 1998, Fulcrum Titanium is well-practised in supporting organisations of all sizes, and from all sectors, at every stage of their digital journey. By providing the very best technology advice, products and services, we help our customers to achieve digital transformations which increase their employees' engagement, enhance their customers' experiences, generate greater productivity and take their businesses to a whole new level.

Contact us

Need to learn more about how our solutions can help drive your business forward? Contact our team today!

Email Fulcrum Titanium
enquiries@fulcrumtitanium.com

Call Fulcrum Titanium
+44(0)118 960 2500

Find out more
www.fulcrumtitanium.com

TITANIUM

BY FULCRUM IT PARTNERS

©Copyright 2023 Fulcrum Titanium. The information contained herein is subject to change without notice. Sales of products and services by Fulcrum Titanium are subject to Fulcrum Titanium's terms and conditions, which are available on request. Fulcrum Titanium shall not be liable for technical or editorial errors or omissions contained herein.