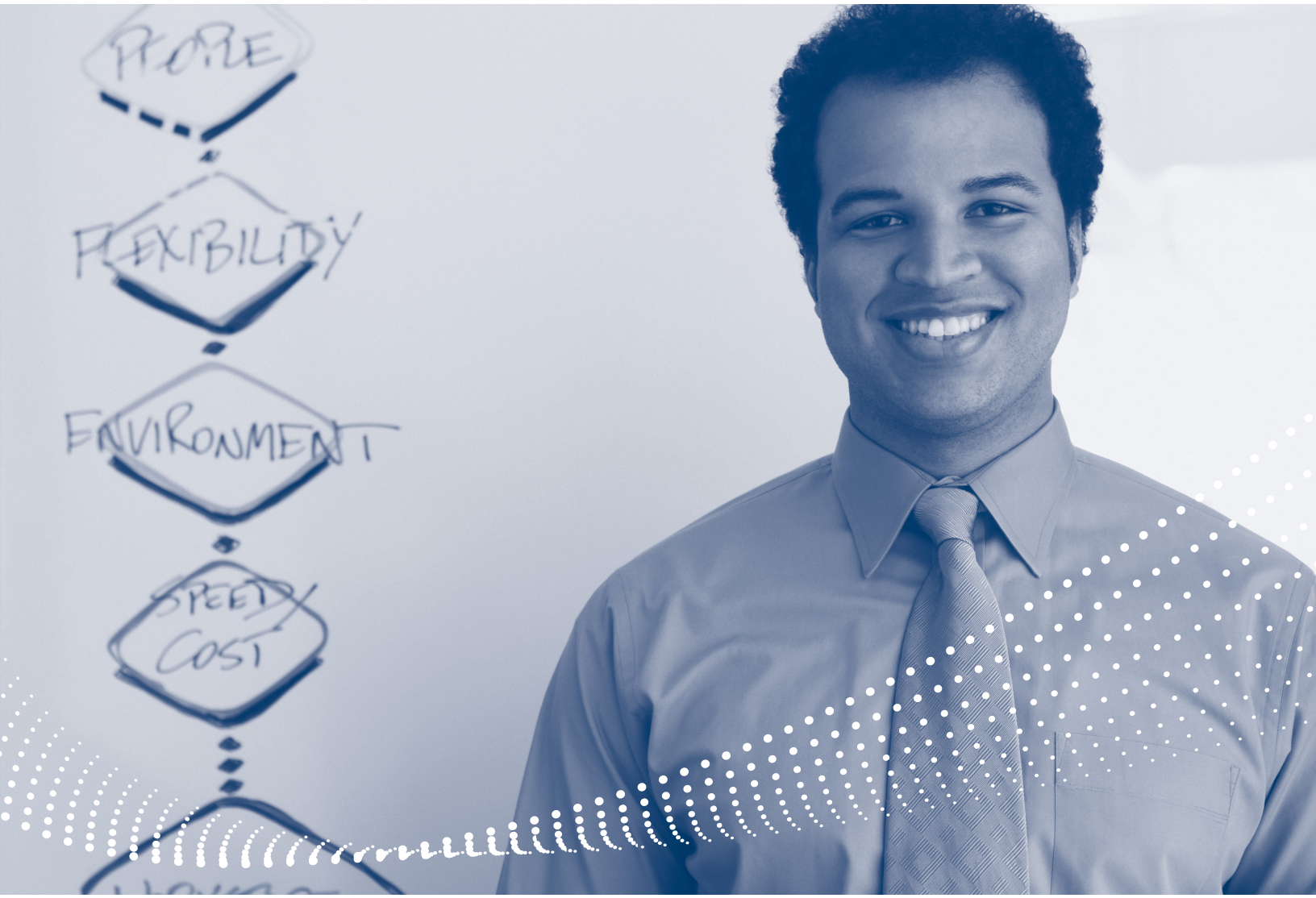
HughesON™

8 Fit Points to Help You Find the Right-Sized SD-WAN

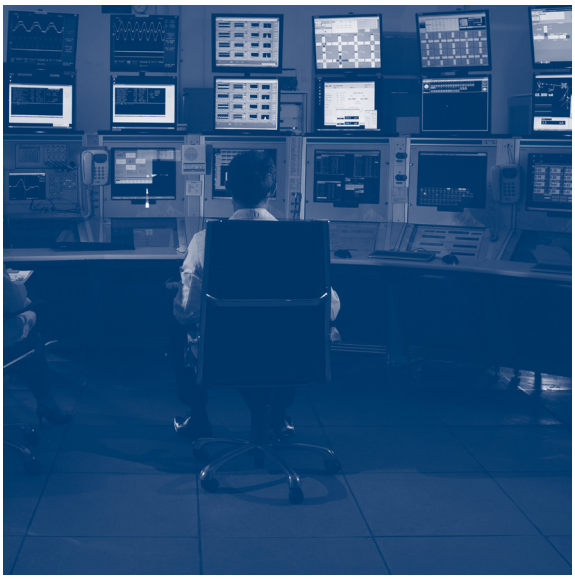


INTRODUCTION

What would it mean for you to have a Software-Defined Wide Area Network (SD-WAN) tailored to fit your business? Would it mean you could launch your digital transformation initiatives and no longer be limited by your legacy MPLS circuits? Or, that you could be confident your network is secure in spite of having thousands of employees working from home? Or, that you could deploy touchless Payment Card Industry (PCI) compliant payment options easily across all your locations?

For these and many other reasons, SD-WAN is not a simple off-the-shelf purchase. It requires a custom fit to truly meet your business needs and enhance operations and security; much like a custom-made suit will fit better than one that's been pulled off the rack. Here, we define "8 Fit Points" to help you assess your current situation and determine how to get an SD-WAN solution tailored to your business.

Fit Point #1: Security



Theoretically, everyone understands the need for network security. But let's look at some hard data to better quantify the issues of risk and need, and to underscore its importance. According to predictions by Cybersecurity Ventures, cybercrime damages will cost $6 trillion annually across the globe by 2021. That's double the figure from 2015, which came in at roughly $3 trillion.

Why such a dramatic increase? Because there has been exponential growth in the types and numbers of devices that connect to networks over the past 5 years, as mobile use has been unleashed. There has also been a huge shift to applications and network resources residing in the Cloud. And all of these predictions were made in 2019, long beforethe pandemic, so they don't even account for the added risksand complications associated with a remote work environment. Consequently, there are now many critical access points outside the control of the traditional enterprise network, all of which need to be enveloped by the network's security.

The State of Firewalls

The first step is to compare the level of security your enterprise demands with the types of protection available through various firewalls (and particularly those you have deployed on your network). One simple comparison is to look at a stateful (traditional) firewall versus a stateless one, versus a next generation firewall. The goal of any firewall is to guard against network intruders. Stateful and stateless refer to how packets of data are processed.

A stateful firewall tracks the operating characteristics of your network's connections. It constantly analyzes data traffic and packets to determine which can be approved to pass through the network's connections. Those that do not pass scrutiny, known as the handshake, are blocked. Such limited protection provides a small measure of security, but can inadvertently allow threats to pass through. For this reason, a stateful firewall can be adequate to protect and isolate communications between devices within a closed private network. However, once devices on the network gain Internet access, or the public utilizes Guest Wi-Fi services, filtering becomes more complex because the potential attack surface and its security requirements expand. Stateless firewalls, on the other hand, use packet filtering rules, which include contextual information about the network connection itself to determine which data is approved to pass through.

A next-generation firewall (NGFW) does it all (and more). NGFWs combine port and protocol inspection, as well as application-level inspection and filtering to approve or block access. They also apply intrusion detection and prevention (IDS/IPS) technologies, and incorporate near real-time intelligence from outside the firewall to update security measures like white/black lists, application signatures, and virus/malware definitions. The NGFW's ability to filter packets based on applications provides greater control and visibility into which ones are trying to access and transit your network. This helps to prevent unwanted or dangerous applications, like malware, from penetrating the network.

It is interesting to note that most current SD-WAN solutions come with a stateful firewall, rather than with a proven integrated NGFW. Yet as noted earlier, the shift to Cloud-based applications and Software as a Service (SaaS/XaaS) means very few enterprises run a 100% closed private network. Of course, this is particularly true since the pandemic hit. In certain sectors, like retail, where Guest Wi-Fi services and mobile associates are critical to the brand experience, there is an even greater need for web and content filtering.

NGFWs offer this type of protection, so you can enable employees and customers to access the Internet safely and provide a range of amenity-based services, such as Web browsing, email and social media without exposing the network or its users to cyber threats.

Building the Right Security Architecture

The next step to considering or preparing for an SD-WAN transformation, is to assess your security architecture. For example, if you have legacy applications that require filtering within a branch or store location, the deployment of an NGFW at the edge is essential. That's because to fully protect devices that are used for PCI-compliant transactions which may also communicate with non-compliant devices, there must be strong edge security at the branch location to meet PCI standards.

An additional factor is the location of security enforcement. This is critical because policy enforcement can be resource intensive; deploying IPS/IDS at the edge, for example, may compromise computing power and throughput. But if most of the risky traffic you're trying to protect is funneled through an aggregation point, such as a data center or Cloud POP, it makes more sense to place enforcement closer to the access point where resources will be more readily available.

Still another option when it comes to architecture is the Secure Web Gateway (SWG). The SWG is a distributed Cloud-based series of checkpoints where all traffic flows to keep unauthorized users and threats from entering your network. Because this architecture analyzes user access rather than device access, it adopts a "Zero Trust" model. This approach verifies every access request before permission is granted, no matter where that request comes from. It may be in the form of edge-based policy management or an SWG approach that manages policies at the Internet Cloud POP.

Either is ideal for SD-WAN deployments because edge-based policy management mitigates the riskiest traffic traveling directly from specific store or branch locations to the Internet. Beyond addressing how and where your network analyzes data, be sure to also think about other critical issues that may affect your business, such as how you process transactions securely and protect customer payment information, as well as safeguard your own employees' data.

Assess Your In-House Capabilities

Now, you need to consider the staff resources, expertise, and capabilities you have in-house to handle your network's security, especially in a complex SD-WAN environment. That includes looking at how much time you are willing to devote to staying current on technologies and threats. (Unless you have a highly trained security operations team, it is unlikely that you have the resources readily available in-house to internalize and react to all threat feeds and alerts that may arise.) You may instead want to explore having a Managed Service Provider (MSP) who can provide the specialized resources and tools required for a secure SD-WAN. The right partner can perform network scans; facilitate the PCI audit process; provide management, detection and response services; and ensure your network has all the critical components—from the right firewalls to the appropriate security architecture—to meet your business' needs and operational requirements.

Fit Points #2 and #3: Bandwidth and Cost

Let's first define bandwidth as the maximum rate of data transfer across a given path. Essentially, it's how big the pipes are in your network. Now, consider the growing demands placed on that bandwidth. These may stem from media-rich applications, interactive real-time inventory systems, or an increase in the total number of applications you depend upon, or having your network monitor traffic and prioritize critical applications. All of these examples contribute to the reasons you run out of bandwidth and your network is sluggish, or you feel compelled to acquire more bandwidth. But you're not alone. They also account for why there is a 20% annual increase in the need for bandwidth.

Compounding these issues is the proliferation of the "Internet of Things" (IoT) and mobile devices. For example, in your various branches or store locations, you may see a rise in IoT devices such as high definition multi-purpose cameras for frictionless checkout, loss prevention data, and planogram management. You may also be deploying mobile devices like associate tablets and kiosks. Even in-store robots that increase customer engagement levels require substantial bandwidth to interact in a manner that enhances the in-store experience.

Bandwidth without Breaking the Bank

Clearly, this rising demand for bandwidth is not going to abate any time soon. Of course, it seems as if broadband circuits are ubiquitous; and they deliver much greater capacity, to the point of last-mile Gigabit per second service—far more than what is available with legacy MPLS circuits. If your enterprise has stores or branch offices in exurban areas, you likely know that despite the continued growth in broadband availability, speed, coverage, and quality, all still vary considerably based on geography and infrastructure capability. Yet SD-WAN enables service and connectivity assurance to support a distributed environment. That's why, when reviewing MPLS vs. SD-WAN, the case for SD-WAN becomes even more compelling, because you can optimize much lower cost per bit broadband circuits and reduce costs over time.

An often overlooked aspect of considering or comparing SD-WAN solutions is addressing both the underlay and overlay costs. This concept is tightly tied to our 8 Fit Points. When you tailor an SD-WAN solution for your unique business needs and operational practices, you don't end up paying for unnecessary features or capabilities.

Right-sizing the last mile of connectivity and reducing the costs associated with over-provisioning will also affect your total costs immediately. So it's crucial to understand any variable costs related to a solution and how they impact your total cost of ownership (TCO). Since your TCO impacts every site on your network, every month, for the full term of your agreement, it needs to be included in your long-term planning assumptions.

There are also other service-related elements that can add to your network spend. These include whether you want a 24/7 help desk, or white-glove design and installation, ongoing maintenance and operations, on-site repair, and the support to manage multiple Internet Service Providers (ISPs) and vendors. While all are important pieces of network operations and management, their ongoing expenditures can increase network underlay costs four-to-seven times.

By quantifying your enterprise bandwidth needs, costs, and budget constraints, you'll gain a full picture of your requirements.

Fit Points #4, #5, #6: Cloud Access, Real-Time Apps, and Agility

People talk about "the Cloud" as if it's a single massive entity. But the Cloud is really a metaphor for the Internet and for not having a dedicated on-site server. Cloud providers offer storage service for data, programs and applications, which users access over the Internet in what becomes cloud computing. These transactions may actually interact with multiple, highly distributed cloud points of presence (POPs), even though from the user's perspective it may appear as if there's a single cloud service fabric. Network access must therefore be responsive to cloud locations that are dynamic, virtual, and elastic. When analyzing the type of cloud access your enterprise needs, it's important to understand this "behind the scenes" nature of the Cloud.

Is Your Strategy in the Clouds?

Today, according to Gartner, most organizations do not have a formal cloud strategy, although by 2022, 70% of organizations intend to have one. A cloud strategy essentially outlines the role of the Cloud in your organization and is critical if you are making SD-WAN related decisions.

Here's why. Organizations with a cloud-first or smart-cloud approach require an SD-WAN solution with large scale cloud infrastructure "on-ramps" to address access to POPs. These on-ramps assure direct access to critical cloud services, regardless of their location within the cloud service fabric. This results in faster, more efficient network response times, and a far better user experience.

Facilitating broad and efficient access to multiple cloud POPs also requires a robust network of SD-WAN gateways to ensure that each point is optimized for performance. With POPs, there are cloud exchanges where traffic funnels converge into massive, centralized aggregation points. While this enables cloud service providers to best serve combined applications and service requests, it can result in network latency and delays experienced by your users.

One strategy to remedy this issue is to co-locate the SD-WAN gateways within these cloud exchanges. By placing the cloud service and SD-WAN routing access at the same site, you can optimize performance of cloud service delivery to reduce latency in applications and transactions.

Collectively, these types of decisions can greatly impact your approach to SD-WAN and deliver true network transformation.

What are Your Priorities?

Another crucial point regarding your network's functionality and performance is the role of applications and their priority in real-time, when multiple transactions occur simultaneously. Simple put: some apps in a network take priority over others. You don't want your Voice over IP (VoIP) service to cut out during a customer call because another customer is streaming videos at your coffee bar.

In the past, voice and video often drove the need for increased bandwidth. Today, the list of key drivers has expanded to include other applications and scenarios, such as collaboration tools like Microsoft Teams, Zoom, and Slack; a nation of remote employees who must work across multiple platforms; and the exponential growth of mobile and smart devices. Recognizing how many real-time applications you have and knowing their importance in your ecosystem, will help you find an SD-WAN solution to prioritize your critical operations and apps. Doing so will optimize network performance.

SD-WAN stands out in this area because it delivers intelligent path control that allows a network to route traffic around congestion, overcoming last mile challenges with broadband service. Quality of Service (QoS) and prioritization schemes mean critical real-time apps can take precedence over less time sensitive apps, such as email or software downloads. Leading SD-WAN solutions will also provide automatic and dynamic app classification and a multi-level priority queue. Forward Error Correction, or FEC, can sense network inefficiencies and replicate critical app data to further improve the likelihood of successful delivery, again enhancing the user experience.

Because buying more bandwidth is not always feasible or affordable, it's important to recognize that the greater the number of apps and users on your network, the greater your need will be for the types of optimization tools and technologies SD-WAN delivers.

How Agile are You?

If you're one of the over 25% of organizations who have had to cancel digital initiatives because your network could not handle or adapt to the desired new technology, then you know all too well why agility is critical—it points to how quickly you can make changes to your network. For example, can you run different configurations at different sites? How easily can you pilot new technologies and then roll-out a winning solution? Can you be nimble in the face of market changes, so your business can stay competitive and responsive? Answers to these types of questions define agile.

An SD-WAN solution supports increased agility because it separates the physical underlay connectivity from the overlay management and data planes. This enables you to alter the underlay circuits, and, say upgrade from 4G to 5G without impacting the SD-WAN overlay. You can also create multiple store or branch profiles so each can operate with different configurations and technology deployments while still being managed and optimized by a single interface. All of this means you can truly tailor your network to your needs, down to the location level, and be positioned to quickly test or deploy new technologies and support faster speed-to-market for your products and services.

Fit Points #7 and #8: Service Levels and Partnerships

One of the most critical early decisions to make as you assess your current and future networking needs is whether to pursue an MSP or do-it-yourself (DIY) approach. Such a decision requires having a clear understanding of your needs. Do you have remote workers who need secure access to the network's resources? Are you relying more and more on Cloud applications? Do you have plans to rollout new technologies, devices, or service capabilities?

Armed with such insights, you can then consider the level of skills and expertise you have in-house. Also think about the time and energy it will require to either develop or recruit the skills and resources you may need. Even if you have the in-house capabilities, you may decide to use an MSP for certain expertise and services. The right MSP partner can provide access to a broad buffet of service options—from fully managed offerings to "bring your own broadband" to shared service models that will enable you to deploy portions of a DIY approach and use a hybrid model elsewhere as desired.

To determine which approach will best fit your business, pinpoint how much service coverage you need by asking the following questions:

- What level of technical expertise do you have in-house?
- Do you need extended hours or 24/7 coverage?
- Can you deploy a large-scale network change without interrupting your core business or do you want a partner to help ensure a smooth transition?
- Do you want or need zero-touch provisioning?
- How much time over the next 5 years do you want your team to devote to network maintenance and updating?
- How quickly will your team be able to adjust network behaviors to reflect changing business practices or technology deployments?
- Do you anticipate the need to run test pilots in one location, followed by a roll out of a proven proof of concept elsewhere?
- Do you have a help desk and ticketing system that needs support?
- With a clearer understanding of available resources (and gaps) you can then consider your service level requirements.

Ensuring Service Levels

Typically, with an MSP there is a service level agreement (SLA) in place to address and guide certain aspects of network service, like its quality and availability, and to specify who is responsible for managing performance. Even if you apply a DIY approach, it is essential to consider how you will ensure network service levels. For example:

- Are you ready to assume the burden of staying current with the latest technology updates and advances?
- How much time are you willing to expend managing the day-to-day operations, especially if they require extended hours, 24x7 coverage, or on-site support?
- Is your team equipped to handle network optimization tasks?
- Do you need access to network analytics?
- Will you be dependent on manual processes? Or, are you willing and able to invest in integration with all your vendors and Internet service providers (ISPs) to achieve efficiencies?
- Will you be transitioning away from MPLS and toward broadband? And, are you willing to take on the management of multiple ISPs and service plans across the network?

As Gartner noted in its DIY vs MNS report (2017), based on an organization's IT capabilities, an MSP is the recommended way to deliver network infrastructure if you are not operating at an advanced capabilities level. Even if you can deliver at this heightened level of service management, you may still choose to use an MSP over gaining added control (plus added cost and management effort) from the DIY approach because you prefer having a lean IT team, are focused on cost savings, or are building agility and scalability into your operations. While a fully managed solution may carry higher costs, the benefits associated with relinquishing maintenance tasks and optimization efforts alone will pay quick dividends.

Ultimately, you should consider whether your IT staff might be best served by focusing on improving operational or business processes rather than on managing your network. And whether you want a reliable partner who is able to not only look ahead to trends and market changes, but also handle the day-to-day patching and release updates associated with network maintenance. Again, while fully managed solutions may be pricier, there is no doubt the MSP offers greater capabilities at a similar cost while also providing a simplified and more direct way toward meeting or exceeding SLAs.

Preserving Your Partnerships

You've invested great time and expense in your network. And you may have components in your technology stack (along with technology partners) that you like and want to continue to use and work with. Maybe you rely heavily on Cisco for all your routers and switches. Or, you consider Fortinet security to be a must-have component of your overall security architecture. It's reasonable to want any new solution to work with parts of your existing infrastructure and for it to include your preferred technology partners.

The right MSP partner should be willing and able to integrate your favorites into your SD-WAN solution. There should be no need to sacrifice what's already working for you. The MSP should also be able to deliver best-of-breed options to close specific capabilities gaps. In this way they provide a blended solution that is truly tailored for your business. Some MSPs, such as Hughes, have forged their own partnerships with industry leaders like Cisco, Fortinet, and VMware that can deliver added benefits.

To identify which stack components and partners to preserve, ask yourself these questions:

- What parts of your infrastructure currently perform well?
- What would you like to keep?
- Do any parts of your infrastructure hold certifications or meet compliance regulations that you'd like to hang on to?

By using these 8 Fit Points as your guide, you can assess your current situation and consider your network needs thoroughly and holistically. You'll be able to look far beyond the numbers to better understand each discrete decision. And, you'll end up with a tailored SD-WAN solution designed to fit just right!

For additional information, please call 1-888-440-7126 or visit business.hughes.com.

HUGHES®
An EchoStar Company

business.hughes.com

11717 Exploration Lane
Germantown, MD 20876 USA