Whitepaper

Increase MPLS and SD-WAN Speeds and Reduce Operating Costs

Connecting Office Networks with MPLS and SD-WAN

MPLS and SD-WAN are popular methods for connecting offices together so that users can access internal network resources from any office **location securely**. Of the choices available to accomplish this task, MPLS and SD-WAN are the most **widely deployed methods**.

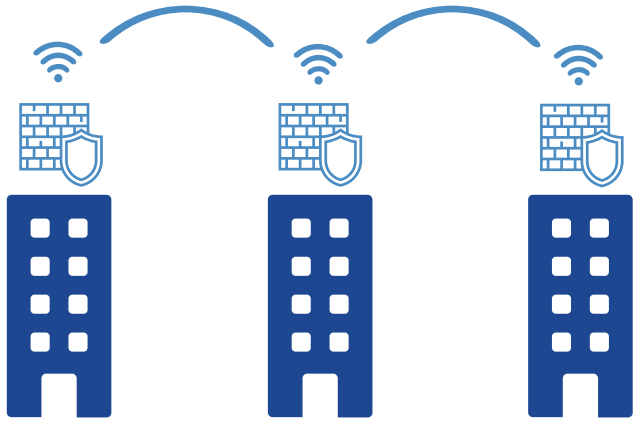
MPLS

Multiprotocol Label Switching, or MPLS, has been the traditional means of connecting offices using private network connections. Typically, if offices nee**d** to be connected, an organization **can** contact their Internet Service Provider and request private network links between the offices so that sensitive data **can** flow between them with ease. The ISP **can** accomplish this by offering private MPLS links which serve the purpose of connecting offices in a secure manner.

MPLS links, provided by an ISP, connect offices securely

SD-WAN

SD-WAN can be used to accomplish the same task of connecting offices securely. Instead of purchasing private MPLS links from the ISP, administrators can use SD-WAN to create private links by leveraging on-prem firewalls at each branch location to create site-to-site encrypted connections over commodity internet bandwidth. SD-WAN relies on having on-prem appliances at each office location so that the private connections between the offices can be established. Because SD-WAN uses inexpensive commodity bandwidth, the cost per megabit is much lower than MPLS. It does, however, require appliances that can handle creating large enough encrypted connections between offices which adds cost.



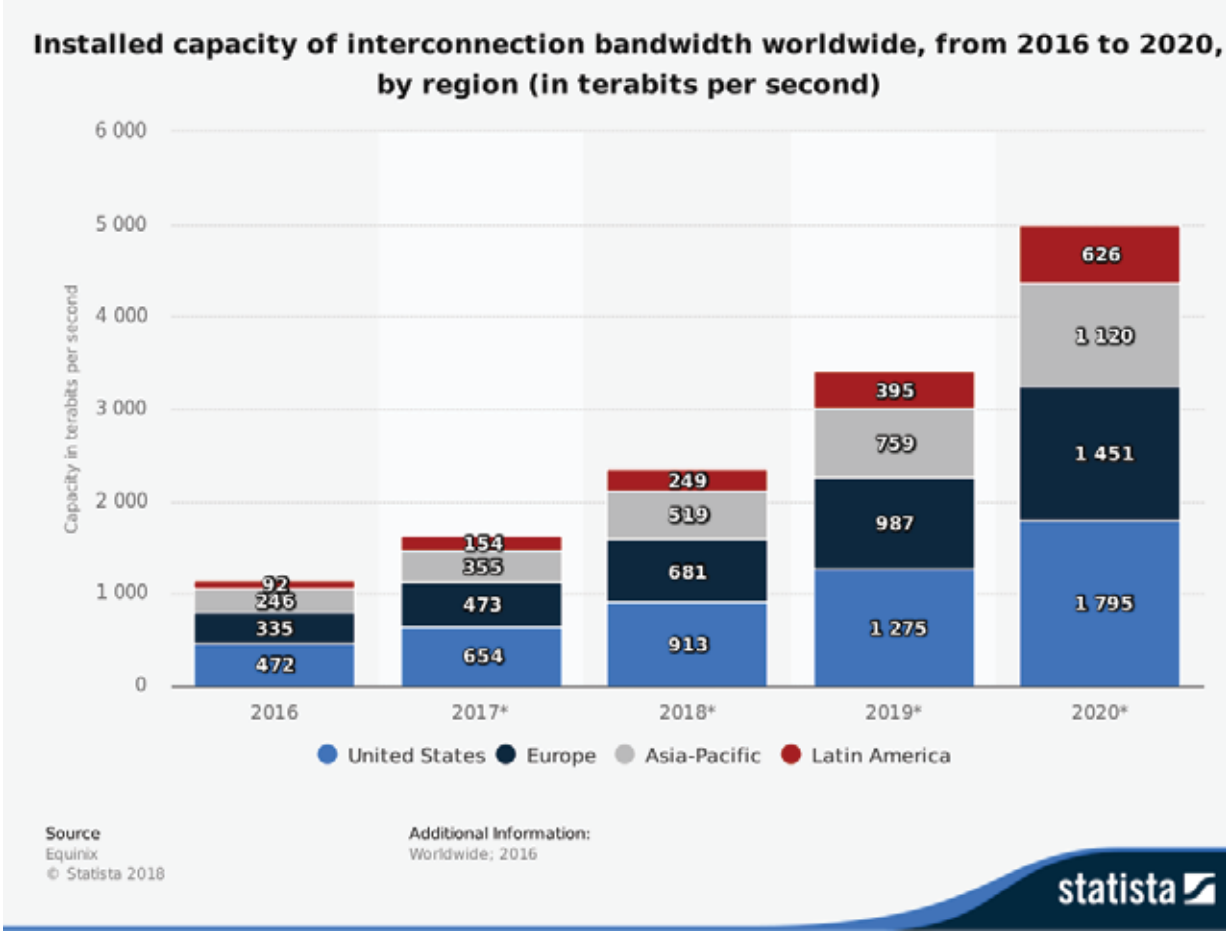
SD-WAN uses appliances at each office to create secure connections over commodity bandwidth

The Shift from MPLS to SD-WAN is Driven by Cost and Efficiency

A big driver for moving from MPLS to SD-WAN is cost. The cost per megabit of private MPLS bandwidth is typically in the range of $300-$600 per megabit, per month. The cost of commodity bandwidth, which is used by SD-WAN, is a small fraction of that and typically falls under $5 per megabit, per month, or less. The total cost of implementing SD-WAN includes the cost of the appliances at each branch office location, which is required to establish the encrypted connections between the offices themselves. Including the equipment costs into the equation, implementing SD-WAN is typically still lower than the costs of running dedicated MPLS links, provided by the ISP, to connect offices together.

Why is Bandwidth Between Offices Increasing?

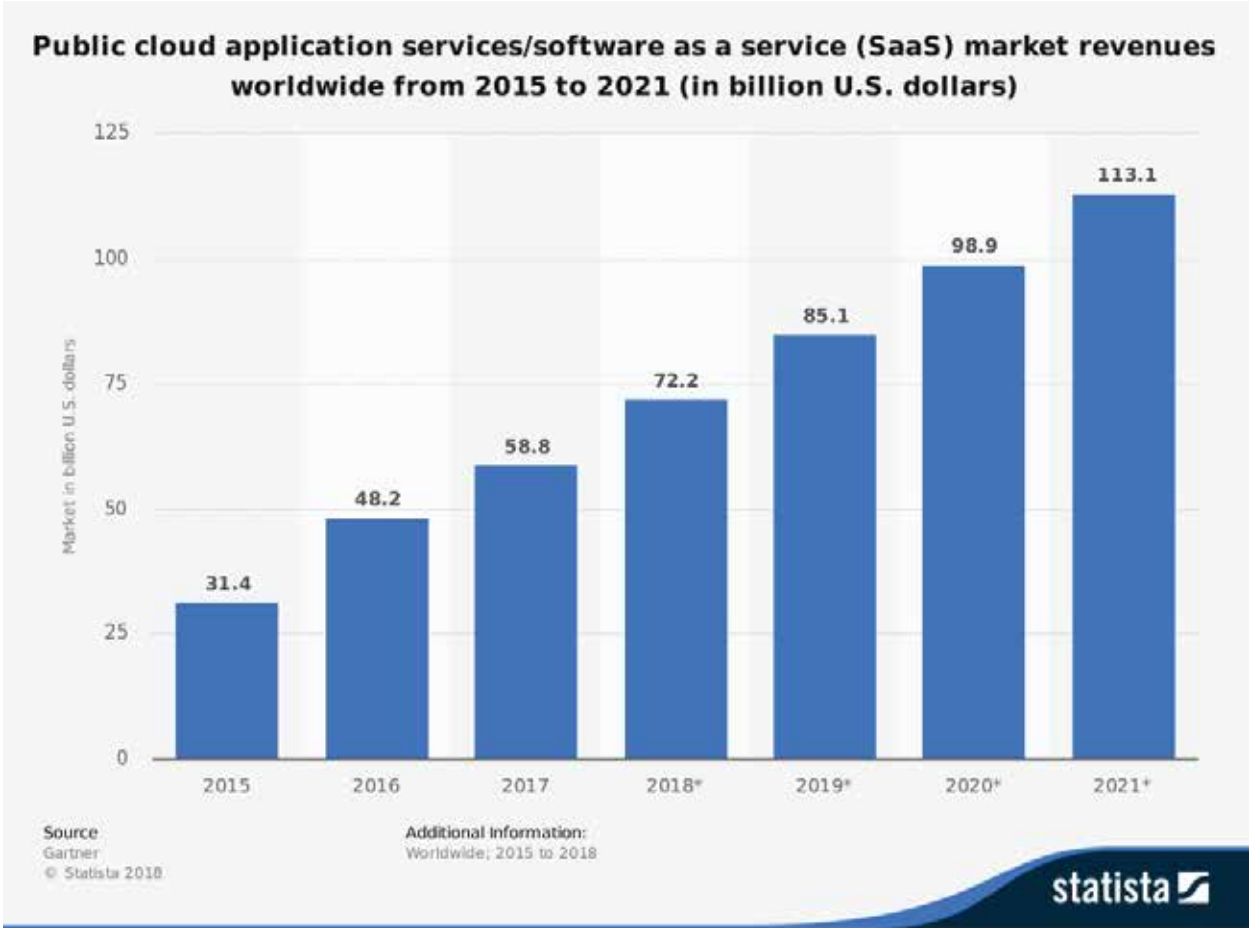
An important question to consider when migrating from a MPLS strategy to a SD-WAN strategy for connecting offices is why bandwidth between offices is increasing to begin with. With virtually every application moving to the cloud, the amount of internet-bound bandwidth is increasing at staggering rates. According to Equinix, the total installed capacity of interconnection bandwidth is projected to grow from 1,144 terabits per second in 2016 to over 4,991 terabits per second in 2020. This traffic increase is primarily between the offices and the internet, not between the offices themselves.



As applications move to the cloud, it would follow that bandwidth between offices should be decreasing as well due to users accessing those applications in the cloud versus other offices on internal networks. If bandwidth between offices is decreasing due to fewer on-prem hosted applications, the need for more bandwidth between offices should also be decreasing. The load on MPLS and SD-WAN links will decrease as more applications become SaaS delivered in the cloud, as more and more bandwidth exchanges between users and the internet occur directly, versus between users and other internal office locations.

The reality is that likely site-to-site internal traffic is **likely** increasing because user-to-internet traffic is being routed over internal networks. The reasons for this vary, but typical reasons include the need to secure traffic between users and the internet. Other reasons might include needing to restrict login to cloud admin portals to users within the corporate network which is accomplished by restricting admin portals to corporate owned IP address space. Sending internet bound traffic from users to centrally hosted on-prem **internet security** appliances is not only non-ideal, it is unsustainable as bandwidth increases will continue **occur** for the years to come.

A quick look at the growth of cloud adoption and SaaS paints a grim future for an appliance- based security approach. Gartner estimates the growth of SaaS to be almost 400% from 2015 to 2021.



Lower Cost and Increase Employee Productivity by Using Local Branch Office Break-outs for Internet Traffic

Ideally, the recommendation is to send traffic between users and traffic destined to the internet directly from the branch offices. Only traffic that is destined to internal applications should be sent over private MPLS or SD-WAN links. Without shifting to this strategy, both MPLS and SD-WAN strategies will struggle to keep pace with user bandwidth demands.

5 outcomes of using MPLS without direct branch office internet break-outs

1. The need to purchase more MPLS private bandwidth will increase as users access more cloud applications in a SaaS based future. This will result in extraordinary costs.

2. User productivity will decrease substantially as traffic between users and cloud applications will slow due to saturated private internal links resulting in massive productivity losses.

3. The need to kick off a SD-WAN project will likely arise, which can lead to high labor costs, appliance purchases in order to implement the SD-WAN project as well as possible network interruptions during implementation.

4. Cloud application use will saturate newly purchased MPLS bandwidth quickly, resulting in a poor user experience and sunk costs.

5. More security appliances will have to be purchased at the core data center to secure the increasing volume of site-to-site bandwidth. At the rate of bandwidth increase, this will likely lead to more complex network topologies that include network load balancers, redundancy and higher skill-set labor which is limited in availability.

5 outcomes of using SD-WAN without direct branch office internet break-outs

1. As site-to-site bandwidth increases due to increased SaaS use, the branch office appliances will hit their peak throughput for site-to-site VPN. This will result in the need to replace the appliances with larger appliances at each branch office **to maintain site-tos-site connectivity** resulting in incredibly high costs.

2. Splitting internet bound traffic at the branch office firewall without any security will result in more infections and breaches as the traffic goes between users and the internet without security.

3. Enabling deep file inspection functionality, including SSL inspection, at the low-end model branch office appliance will cause appliance throughput to the internet to decrease substantially resulting in slow connections between users and the internet. This will result in lost productivity and high costs.

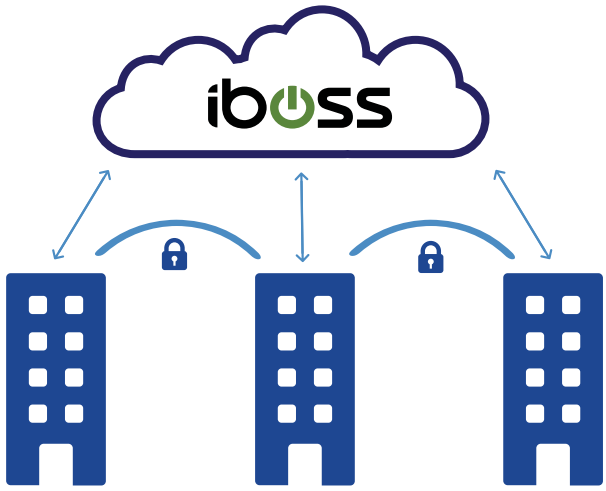
4. Increased labor will have to be acquired to deploy and manage the appliances at each office, including replacements, upgrades and **maintenance**.

5. As with MPLS, the issues of hosting centralized security appliances still exist **with SD-WAN**. More security appliances will have to be purchased at the core data center to secure the increasing volume of site-to-site bandwidth. At the rate of bandwidth increase, this will likely lead to more complex network topologies that include network load balancers, redundancy and higher skill-set labor which is limited in availability.

Regardless of whether MPLS or SD-WAN is used for the purposes of connecting offices, the continued rise of SaaS applications will drive bandwidth up and to the point that any strategy that involves sending internet traffic through private links will reach a saturation point. This will result in slow connections for users, lost end-user productivity, higher labor costs, higher site-to-site bandwidth costs, and higher infrastructure costs to name a few of the many challenges.

Make MPLS and SD-WAN More Efficient by Implementing Cloud-Based Internet Security

To alleviate these challenges, internet and cloud bound traffic should go between users and the internet directly from the branch offices via local internet breakouts. Using a strategy of local branch office internet breakouts for cloud-bound traffic, users will experience faster speeds to cloud applications and higher productivity. Additionally, using branch office cloud breakouts will remove the load from the site-to-site private connections. This includes eliminating a vast amount of bandwidth traversing current MPLS or SD-WAN connections. This also creates a sustainable path into the future. As bandwidth continues to increase due to internet and cloud application use, this load is not added to the private links. Instead, the increased load is sent directly to the cloud over commodity bandwidth. Remember, even a SD-WAN strategy requires on-prem appliances to create private and encrypted links between offices and increasing load on these links will bring the branch office appliances to their maximum throughput capacity quickly.



Send internet-bound traffic directly to cloud security from branch-office break-outs

To implement internet breakouts directly from branch offices to the cloud, security must be applied to the traffic between users and the internet. Although turning these features on at on-prem SD-WAN appliances may seem like a reasonable choice, deep file and traffic protection, including SSL inspection, puts a heavy load on the branch office appliance. This reduces the maximum throughput that can be used for the purpose of connecting offices to each other, as the CPU cycles at branch office appliances are consumed attempting to secure internet traffic, rather than connecting offices. In addition, turning these security features on typically reduces internet bound capacity substantially, resulting in slow cloud connections.

Fortunately, applying internet security for local branch office breakouts is easily accomplished using a cloud-based internet security approach. Since data from users heading to the internet is heading toward the cloud anyway, applying internet security in the cloud not only eliminates the burden on local branch office on-prem appliances, it also applies security at infinite scale using elastic cloud capacity. Users experience fast internet connections to cloud applications and the internet as compliance, web filtering, malware prevention and data loss prevention are applied within the cloud security platform.

Cloud-Based Internet Security Creates a Sustainable Path to the Future

A sustainable strategy for the cloud-first future is to compliment your MPLS or SD-WAN with cloud-based internet security. Some of the benefits include:

1. As cloud bandwidth increases, this load is removed from your site-to-site connections, including MPLS and SD-WAN links.

2. Users experience fast connections to critical business applications, making users more productive.

3. The need to deploy more MPLS bandwidth or increase SD-WAN investments is reduced or eliminated as the increased bandwidth is typically destined to the internet, not on-prem equipment as SaaS use continues to increase.

4. Reduced and eliminated security appliance purchases at the core data center as increased cloud use does not require more appliances. The increased number of appliances needed to account for increased bandwidth exponentially increases cost and complexity as load balancers and more advanced network skill-sets are required. Security in the cloud eliminates the need for any security appliances at branch offices or at the core data center.

5. Creates a sustainable path to continue to use MPLS and SD-WAN while site-to-site bandwidth is still required, restricted only to internal traffic.

Choose the Right Cloud Security For the Cloud-First Future

Not all cloud architectures are created equal. Leveraging newer cloud security platforms built on containerized cloud architectures allow for a more seamless migration from appliances to the cloud, without sacrificing features or processes. This results in reduced time and resources when shifting to a cloud-based platform. The cloud security platform must have all capabilities available within the security appliance deployment. This includes compliance, web filtering, malware prevention, malware infection detection and data loss prevention. These capabilities are found within the iboss cloud platform which delivers these capabilities in the cloud. Cloud internet security compliments MPLS and SD-WAN strategies naturally and sets a solid foundation for the cloud-first future.

About iboss

iboss is a cloud security company that provides organizations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture, backed by 110 patents and over 100 points of presence globally, iboss protects more than 4000 organizations worldwide.

To learn more, visit www.iboss.com