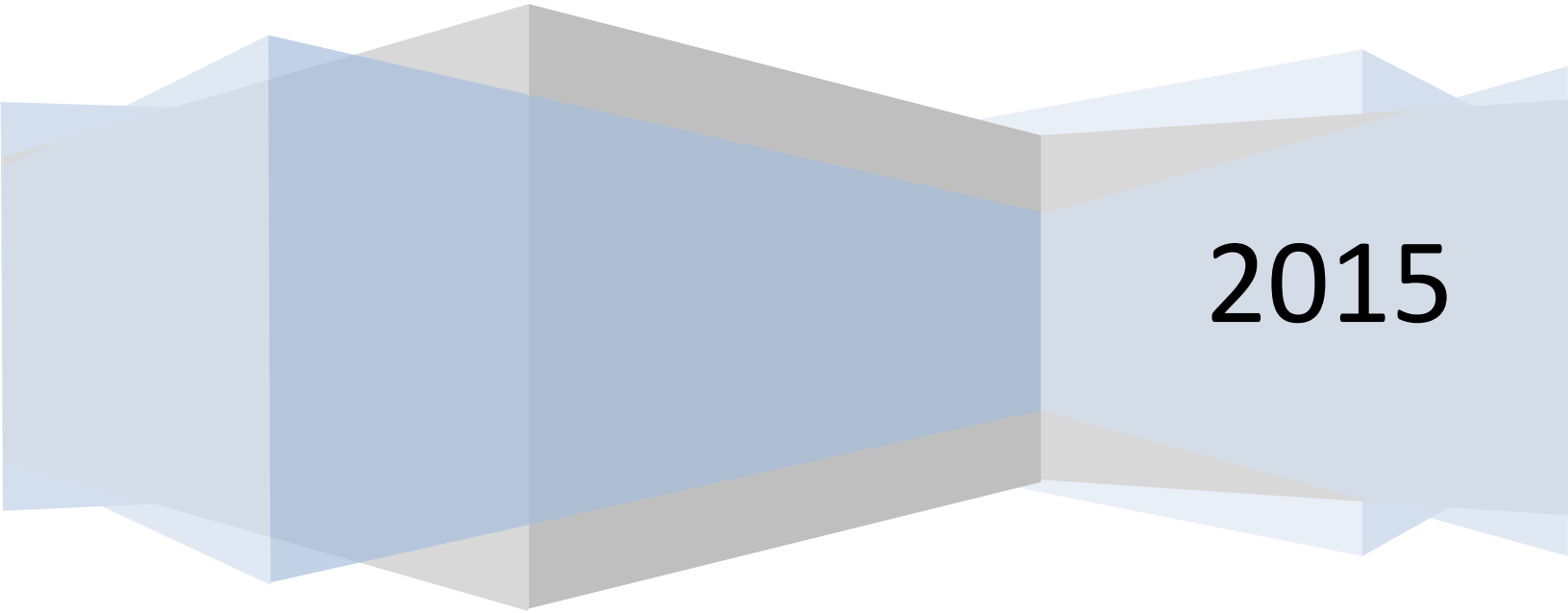
Network World and Robin Layland present

The 2015 WAN Challenge

Your Guide to Understanding and Choosing a Hybrid WAN and SD-WAN Solution



2015

The Future of the Branch Office is a Hybrid WAN

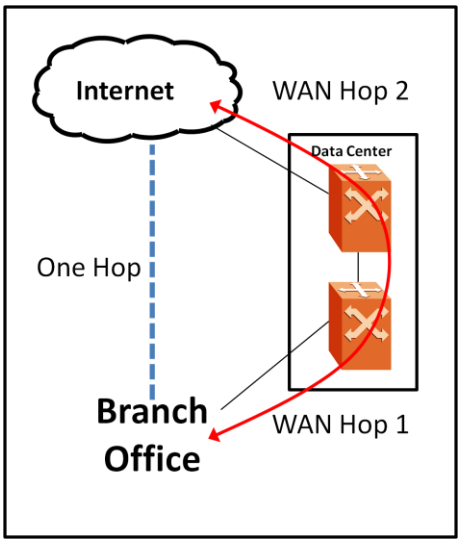
Robin Layland
Principal Analyst
Layland Consulting

Your Guide to Selecting a the Right Hybrid WAN and SD-WAN Solution

Traditional WAN architecture had a spoke and hub design. Enterprises architected a connection to the nearest data center using MPLS or some other leased-line style connection. Using symmetrical optimization technology at both the branch and data center squeezed out more bandwidth and reduced response time. All Internet-bound traffic passed through the data center's security, creating a strong perimeter defense for the enterprise. The data center also has web screening to ensured employees didn't go someplace inappropriate or create a security risk. This WAN design for branch offices worked for decades, but it doesn't any more.

The days of needing to send all traffic from your branch offices to the data center by the MPLS is over. While a significant number of business applications still reside on servers in the enterprise's data center, an increasing number are in the cloud. They are either SaaS (Software-as-a-Service) applications such as Salesforce, or the enterprise is using a cloud service like AWS to host applications.

The branch office is also generating additional business traffic destined for other Internet sites. This includes everything from booking travel reservations, watching videos for training, or just catching up with what competitors are doing.



The other big driver of change is personal Internet usage. Everyone knows you should use the Internet at work for business, not personal reasons, but side-surfing happens. Just blocking usage is not an option because, depending on the job, you can't always tell what usage is personal and what is business. It is impossible to tell if an employee is watching a video to learn something job-related or just catching up on the latest kitten video. The web and apps are just as useful for business as for your personal life. Trying to figure out which is which and setting up blocking isn't worth the time and effort it takes and may upset your employees.

The result is that balance between Internet and data center service traffic is shifting. In 2000 most of the traffic would have been destined for data center servers. Now it is starting to shift strongly in favor of the Internet. Bringing all that traffic back to the data center introduces several costs.

First, it adds unnecessary hops. In the diagram, the Internet bound traffic leaves the branch office and takes a WAN hop to the data center. Within the data center, it has to take one or more hops to get from the router supporting the branch office to the Internet router, plus the trips through all the security and other equipment providing services. Next it takes another WAN hop to reach the Internet. This increases latency. If the traffic goes directly to the Internet, there is only one WAN hop (the dotted line).

Next is the cost issue. You are paying WN freight twice instead of once as with a direct Internet connection. Costs also mount because that extra hop uses expensive MPLS bandwidth rather than a lower cost Internet broadband connection. When Internet traffic was a small part of the overall traffic, extra cost and delays were easily absorbed, but that equation changes as the Internet percentage grows.

Hybrid WAN

The solution is to move to a hybrid WAN architecture. The basic concept of a hybrid WAN is simple. A hybrid WAN solution has at least two connections from the branch office. One is the traditional MPLS (or other technology) that connects directly back to the data center. All the normal business traffic destined for the data center, plus any other traffic you want specifically routed through the data center, takes this path. The other connection is made through direct broadband to the Internet allowing traffic to flow directly to the broader Internet or as a VPN connection to the data center

A hybrid WAN solves the problems with older WAN architecture. Using the direct path to the Internet eliminates the extra hops and latency associated with Internet traffic going through the data center. It reduces cost since Internet broadband is lower in cost than an MPLS link. This can reduce, sometimes significantly, the WAN cost to the branch office. Additionally, using a VPN back to the data center over the Internet gives you an alternative path back to the data center, increasing availability and throughput.

Another key feature of a hybrid WAN is path selection. A hybrid WAN can decide which link is the best path for the traffic based on real-time monitoring of latency, utilization and error rates over the link.

Complete Solution

A hybrid WAN is a step up from the old WAN architecture, but to gain full benefit from it, you need to make sure it can do more than just supporting two links. WAN optimization techniques are still important and should be part of your solution, but you need to ask how they support not just the MPLS link, but the Internet connection as well. The issue is that older WAN optimization solutions were symmetrical. That means they had hardware or software at both ends of the link, something easy to do when you owned both ends. This allowed the solution to provide significant bandwidth reduction along with other benefits, which still applies to the MPLS link to the data center. With the Internet link, you only have the optimization solution on one end - the branch office. Vendors need to explain their asymmetrical optimization technique -- what they can do to help when the optimization solution is only on one end.

Just because you can't put equipment at your SaaS vendor’s facility, there are ways to get the benefits of symmetric optimization. Some SaaS vendors may support a software version of your optimization solution. Your cloud vendor may be able to support a software version of your optimization solution that allows you to get full symmetrical benefits. Additionally, many WAN optimization/hybrid vendors have other creative ways to help. Again the important thing is to ask them.

Another key feature is path selection. A hybrid WAN can decide which link is the best path for the traffic based on real-time monitoring of latency, utilization and error rates over the link. It is important to understand how the vendor performs path selection. It is generally based on the application. You need a vendor that can report and understand the characteristics of the applications using the link. This information is also useful for control and security purposes. Have the vendor explain in depth their path selection ability.

Turning your hybrid WAN into a software-defined WAN (SD-WAN) is a step up from just a hybrid WAN. Basically an SD-WAN means the path selection and configuration are controlled by policies. This approach has several benefits. It allows you to move to a “no-touch branch office” so you can bring up and reconfigure the branch office more easily and quickly. It also allows you to have a rich set of policies driving path selection.

Security

"Direct to the Internet" does present some security issues. With traditional WAN architecture, all the traffic headed to the Internet goes through your security infrastructure in the data center. The direct connection means you need to consider how to you are going to provide security at the branch. There are three basic approaches to providing security:

- Replicate all or part of your security infrastructure at the branch as needed
- Route all or part of the Internet traffic to a cloud security vendor and have them provided the security
- Establish hubs closer to the branches in the cloud where you run the necessary security.

Security should not stop you from implementing a hybrid WAN. Any one of these solutions has proved its ability to solve the security issue. Additionally, hybrid WAN vendors may provide solutions such as web filtering that can help by replicating the web security at your data center. It is important to have them explain how they can help solve the security issues and how they can work with other security vendors to provide a more complete solution. A hybrid WAN is already a step in the right direction because it understands the applications going over the link and provides you greater visibility.

Questions to Ask

When comparing solutions, here are a few questions to consider. It is by no means a complete list.

- How easy is it to set up their solution and make changes? Does it fit within your current controls and management structure?
- Does it understand the applications that are running over your network? What type of reporting does the vendor provide?
- How is path selection done? What variables are considered? Is it static or dynamic?
- How easy is it to set up policies? Do they provide "out of the box" policy for common applications? Does it fit within existing policy framework?
- What type of security features do they provide? Can they easily block websites and do they have the ability know which are bad ones?
- Do they provide a complete SD-WAN solution or have a path to one?

The Challenge

It is clear that moving to a new WAN architecture is the right direction. Hybrid WANs and SD-WANs provide significant advantage over the old single-link design. The question is “Which hybrid WAN solution is right for my network?” Not all hybrid WAN solutions are created equal. Many can't handle the challenges and complexity created by the move to this new WAN architecture. You need to understand the differences between vendors, and then find the one that best fits into your WAN strategy.

I have ask **Blue Coat** to explain how they meet the challenge of today's WAN**.** Rather than having them list everything they do (which is a long list), I asked them to explain their view on the changing WAN landscape and their primary competitive differentiators, concentrating on where they excel compared to the entire industry. Your next step is to read and listen to what they have to say, so you can understand how they can help you implement the right WAN solution for your enterprise.

This document is just one part of the 2015 WAN Challenge. There are also two webcasts at the Challenge site. In each of these webcasts, I bring together two experts to explore hybrid WAN issues in depth. You can find the webcast, along with additional material on application and network performance management, at the Challenge site at Network World -- or click on this link to go there directly.

BLUE COAT®

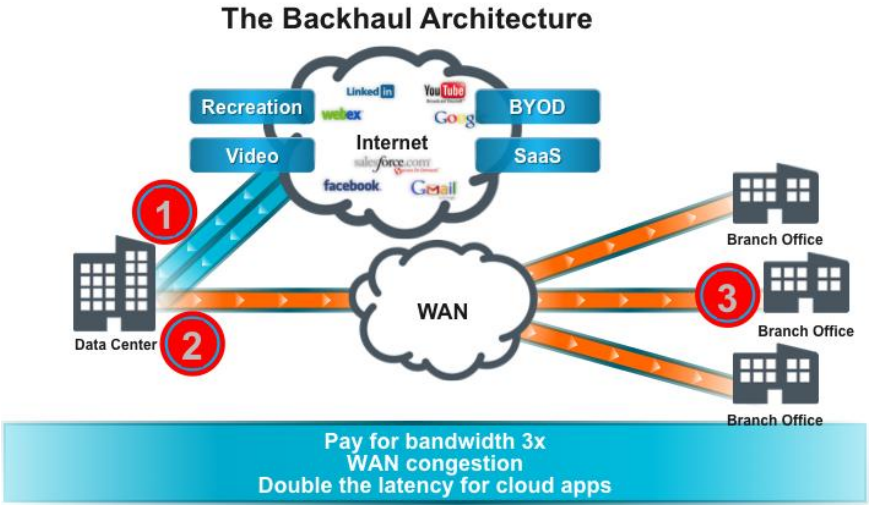
Optimizing and Securing the Hybrid WAN

Mark Urban
Senior Director
Product Marketing

The New WAN Combines MPLS and Internet Connectivity

The legacy WAN has served companies well with predictable, reliable performance., As applications have moved out of the data center into the cloud, the expense and lack of flexibility of MPLS-only WANs are becoming issues. This has led many companies to experiment with “hybrid WANs” that combine traditional MPLS links with direct Internet access links for branch/remote locations. This approach offers significant benefits, including:

- Increased availability for both internal and cloud-delivered applications by adding redundant network paths
- Improved end-user performance by eliminating hops in the traffic path and decreasing congestion on the MPLS WAN link
- Lower costs by eliminating the “triple payments” for internet traffic backhauled over the MPLS WAN and the ability to shift to less expensive internet access links



The Internet, however, is a public network, and maintaining security at remote locations becomes a key concern. You need the same authentication, access policy, malware protection, and logging that is present in the data center.

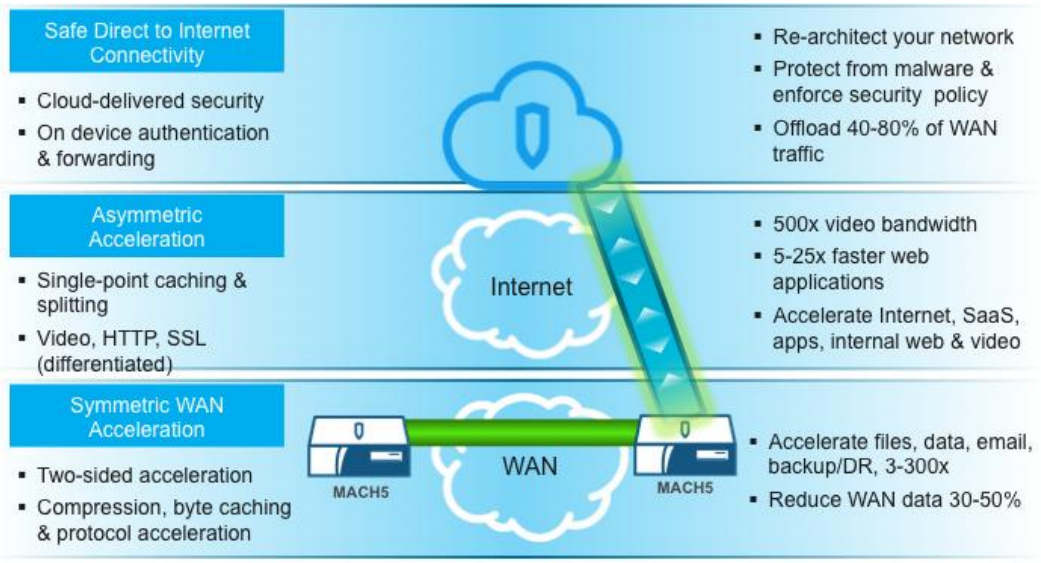
Blue Coat’s Cloud Security Service delivers the same protection as on-premises ProxySG appliances – with a true hybrid model that unifies policy and consolidates log reporting. Moreover, leveraging Blue Coat’s MACH5 appliance allows you to provide asymmetric WAN Optimization technologies – content caching, video stream splitting, and QOS – to the direct Internet traffic, while also providing traditional symmetric branch-to-data center optimization for the MPLS WAN link. This increases performance even more, while reducing bandwidth significantly, creating a superior user experience.

The Old Backhaul and the New Hybrid WAN

The traditional enterprise architecture "backhauls: internet access traffic, forcing internet traffic to travel from the branch office over an MPLS link to the centralized Internet access point, then out to the internet. If you are accessing content from the internet - whether it's a SalesForce.com dashboard or a YouTube

video - you pay three times for the bandwidth once at the data center internet ingress point, once at the data center MPLS egress point, and once at the branch office MPLS ingress point.

In addition, the congestion on the MPLS link causes performance problems, as does the fact that the path takes an extra "hop" through the data center. This architecture is especially problematic with today's network traffic loads.



Today, 50-80 percent of the network traffic to an enterprise branch and remote office comes from the internet. From Buzzfeed, Yahoo, FoxNews and LifeHacker…to YouTube, Netflix, iTunes and HBO…to app stores and OS updates for iOS and Android devices, the internet is the playground for infinite content choices. Of course, it also is the origin for cloud applications like Office365, Service Now, SalesForce, Successfactors, and more. When you move all that traffic over a backhaul architecture, you create severe bandwidth constraints and performance issues.

A hybrid WAN combines a traditional MPLS WAN link with a direct internet access link at a branch office/remote location. That allows internet traffic to be offloaded from the MPLS WAN, freeing up space for internal business applications to run (and potentially reducing bandwidth requirements, saving money).

Benefits of Direct Internet Access

The first benefit of direct Internet access (DIA) is availability: by adding a second link, you create redundancy that can be leveraged if one or the other link goes down. While it is never expected that either will go down, an alternate path can assure even higher availability numbers, allowing for continued operations in those events.

The second benefit is performance. Offloading internet traffic from the MPLS WAN frees up space for internal applications to run, which translates to improved performance for your corporate-hosted applications. Your cloud-hosted applications also avoid that congested link and skip the "hop" to the data center – a double performance boost. Asymmetric QoS and caching technologies at branch locations can boost performance even more.

Finally, by taking cloud application and recreational Internet traffic directly to the internet, you pay just once for that traffic – at the branch ingress/egress point. This avoids "triple link tax" of the backhaul architecture, where you pay at the data center Internet ingress, data center WAN egress, and the branch office WAN Ingress. That's before factoring in the price difference between MPLS links and Internet access links. In the U.S., domestic MPLS can be at a minimum 10-20 percent more expensive than Internet access bandwidth—but for international links, MPLS can be 10-20 times the price of internet access links.

Optimization of Internet Links

There are two huge challenges with DIA at branches: optimization and security. Traditional WAN optimization operates between the branch office and the datacenter ("symmetric" operation), requiring an appliance or virtual appliance on each side. Blue Coat solves this problem with symmetric technology: protocol acceleration, byte caching, and compression. The problem is that the same technology does not apply to internet traffic where you don't have something on the far side of the network; you can't put an appliance on SalesForce.com or on YouTube. When you're dealing with internet traffic, you have to shift into a mode where you use asymmetric technologies, optimizing with a single point.

Blue Coat has three critical asymmetric technologies that solve the problem: content and video caching, live video stream splitting, and QoS-based on patented TCP rate control. None requires a point of presence on the far end of the \internet, or even in the cloud.

- Content and video caching can store entire objects to serve to multiple people, saving massive amounts of bandwidth and improving performance. Objects include documents (.doc, PDF, etc.), CRM/business intelligence queries and dashboards, entire OS updates (Apple, Android, MSFT), entire apps, or video files (on-demand training and communications as well as YouTube and CNN). When a new version of iOS comes out, it can save thousands of gigabytes by caching the OS—or that next viral Star Wars trailer.
- Live video stream splitting takes a single Flash or HTML video streams and splits it to whatever user needs to watch it. It's like multicast with no setup and it's able to work on internet-based content as well.
- TCP Rate Control based QoS is able to manage TCP window sizing in order to meter the sending rates of remote servers (vs. the more limited queue-based model).

Although DIA breaks the traditional WAN optimization model, asymmetric technologies can significantly boost performance and availability, while reducing bandwidth the congestion.

Security

Security is the greatest barrier to the hybrid WAN. The main reason for backhauling architecture is to put all that traffic through the layers of security resident at the data center. Today, however, Security-as-a-Service (SECaaS) offerings such as Blue Coat's Cloud Security Service have emerged, empowering enterprises to safely connect branch offices to the internet with the same authentication, access policies, malware protection, and logging that they configure on their main data center internet link.

More than 15,000 of the world's largest enterprises entrust Blue Coat with their web security, including 80 percent of the Fortune 500. Blue Coat built a global cloud-based web security service that complements its on-premises appliances. Blue Coat's Cloud Security Service delivers that same protection as on-premises ProxySG appliances, with a true hybrid model that unifies policy and consolidates log reporting.

Conclusion

MPLS-only WANs made sense when applications lived primarily in the data center. Today, however, there is a pressing need for a more flexible, more cost-efficient option that accommodates cloud-based applications as well as data center applications. By bringing enterprise-grade security to the new hybrid WAN, Blue Coat has empowered enterprises to exploit the advantages of both MPLS and internet connectivity across the WAN—without fear of increasing the risk of a security breach.

For more information about Blue Coat's solutions, please visit: bluecoat.com