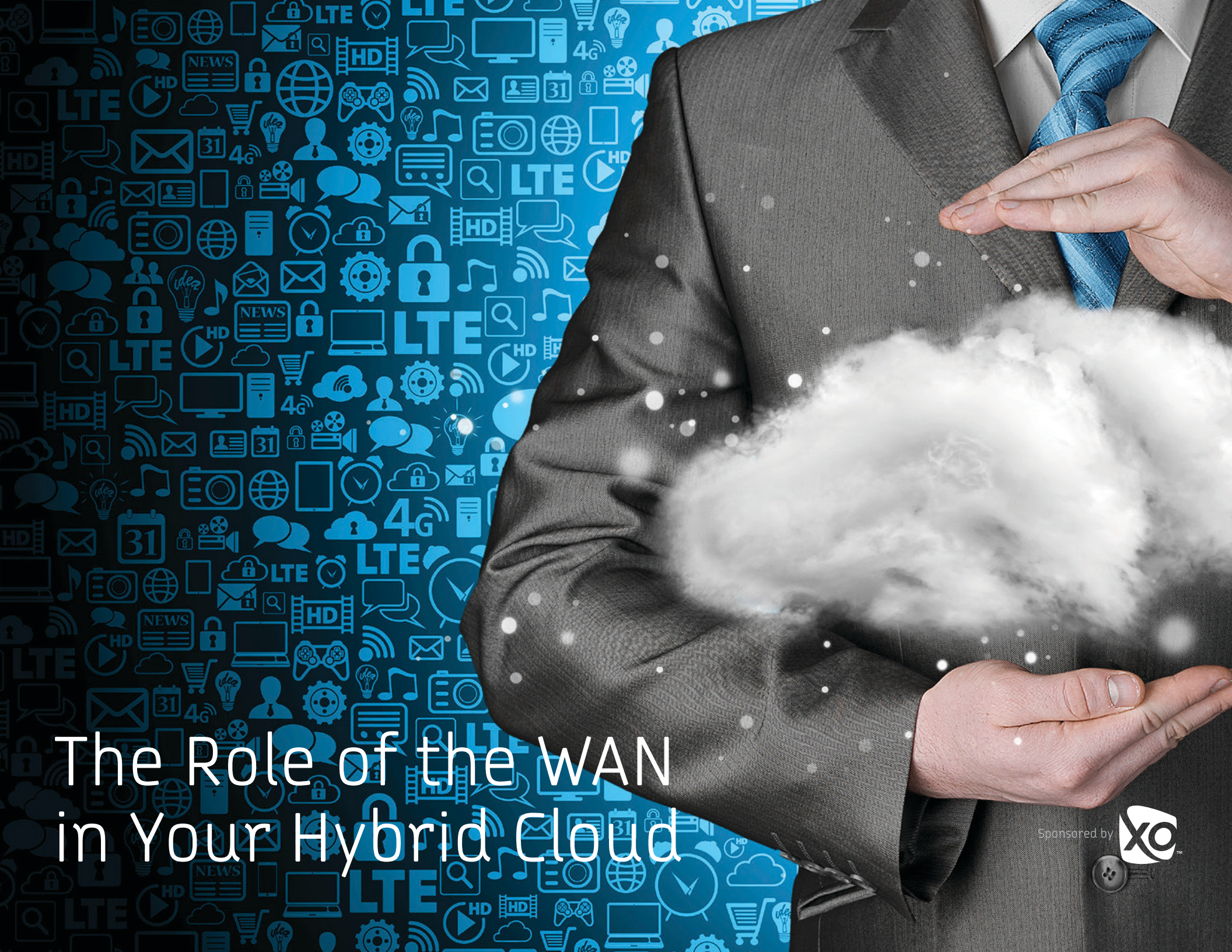


The Role of the WAN in Your Hybrid Cloud

Sponsored by XO

The Role of the WAN in **Your Hybrid Cloud**

So you want flexible access to resources inside and outside of your own data center? Make sure your WAN is up to the job.

The **Expanding Data** Center

The data center is expanding to allow you to take advantage of resources from all over. For starters, you likely have your own private data center, where you run applications behind your own corporate firewall. And you can virtualize your data center to create a so-called “private cloud.” With your private cloud, you gain the ability to turn up applications and services quickly on a pay-for-use basis.

But many enterprises would like to reach beyond just what they can build and virtualize themselves. There are also public cloud services that you can integrate with your own data to create a hybrid public/private cloud. Getting access to resources wherever they might reside is a best-of-all-worlds scenario that puts all data and communications at employees’ fingertips and empowers them. The hybrid cloud opens the floodgates to fast IT – the ability to turn up services dynamically as business needs dictate – which in turn drives business agility and innovation.

Benefits of the Hybrid Cloud

The hybrid cloud gives you fast access to cutting-edge services as they continue to emerge from public cloud providers. For example, most enterprises can benefit from new advances in the areas of storage, software, infrastructure, and development much faster than they could if they tried to keep pace with technology on their own. You just consume these resources in the form of a service rather than building and updating them yourself. The cloud provider continually refreshes the technology behind the scenes, so it doesn't become obsolete.

In fact, some lines of business (LOB) are already circumventing their internal IT departments to get these services. A 2013 Frost & Sullivan Stratecast study, for example, concluded that more than three-fourths (78%) of LOB managers were using as many as five software-as-a-service (SaaS) apps that had not been approved by their companies.[1] These folks aren't trying to be sneaky; they're simply trying to get their jobs done and stay competitive.

But bypassing IT can create hidden costs and security risks. Subscriptions might be duplicated and Internet links to services might go unsecured. So it's best if the model becomes legitimized, managed, and streamlined through IT. You give the LOBs what they need while also maintaining an eye on cost by reducing the number of separate cloud accounts. And you gain control over security and app performance.

> ...more than three-fourths (78%) of LOB managers were using as many as five software-as-a-service (SaaS) apps that had not been approved by their companies.

1 http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf

New Challenges: **WAN Security and Performance**

At the center of the hybrid cloud effort is your WAN. The WAN is the thoroughfare that moves data, services, and sessions back and forth between users and resources. So your WAN needs to be highly available and secure.

It also needs to perform comparably to a LAN. This is tricky, given that WANs can introduce distance-related latency. Packet loss and retransmissions could also be present, further impacting performance in chicken-and-egg transmission loops. Taking a performance hit in order to use cloud services isn't acceptable: users don't care where the resources reside as long as they are readily available and do the job. If they don't get the same experience as they would when locally connected, they won't use the service.

In fact, network security and performance concerns with the public cloud are the primary sticking points impeding progress with the hybrid cloud model. Traditional IT personnel are understandably uncomfortable releasing the company's data – its crown jewels – from the private data center and into someone else's environment. And guaranteeing solid application experiences to users over distance takes some finessing.

That's why, if you're serious about running a hybrid cloud, you really need business-grade WAN services that keep corporate data private and allow visibility into applications and data to overcome performance issues. You also need application management tools to stay on top of things.

Prepping Your WAN

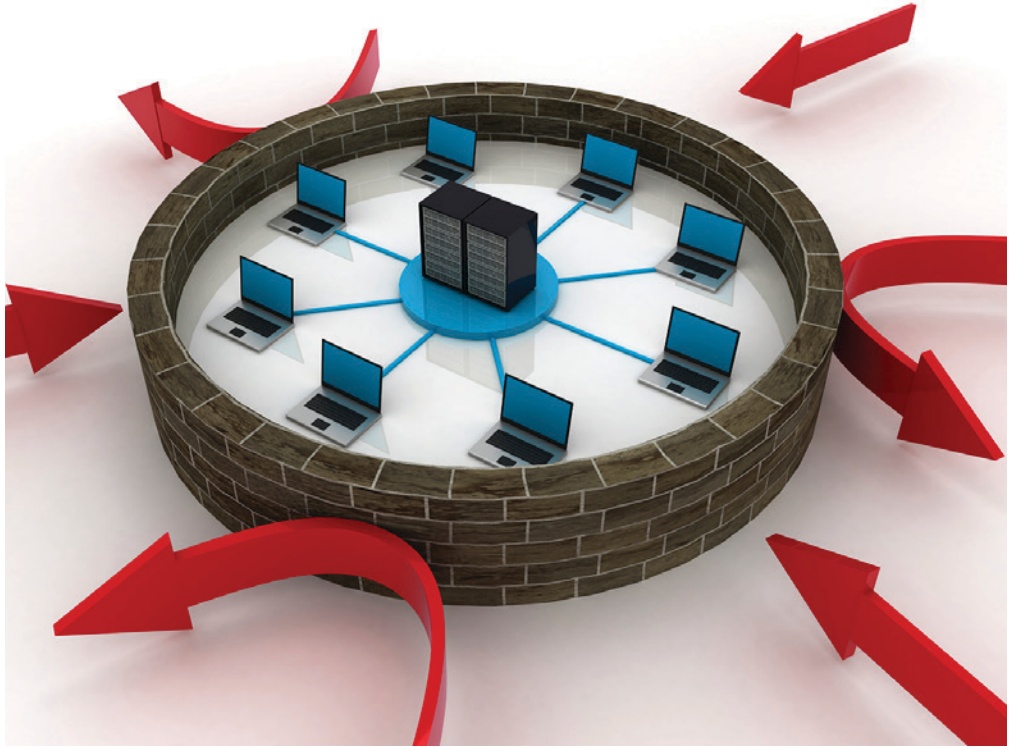
The public Internet is a best-effort and inherently insecure transport network. By contrast, Multiprotocol Label Switching Virtual Private Network (MPLS VPN) is an advanced network technology with built-in security and quality-of-service (QoS) features. A single operator controls network engineering and optimization, end to end. As such, an MPLS VPN-based WAN is the much stronger candidate for creating an integrated network foundation for your hybrid cloud.

Security. MPLS VPNs partition one company's traffic from another's to keep data private. There are other types of security you might need, too, including firewalls, intrusion prevention, and possibly encryption. There are good arguments in favor of using hosted network security services for these functions. Hosted services are both more scalable and secure than building the security capabilities yourself.

New security risks are discovered every day, and network vendors and service providers continually update their services with day-one patches and fixes. To do that internally across a large number of distributed sites could force your IT staff to spend nearly all its time on security patching alone. This isn't scalable, which also makes the approach riskier. One missed patch could be all it would take for a major breach.

- *Firewalls and intrusion prevention.* Using network-hosted security generally involves a network-based firewall, configured with your rules and policies as to what traffic will be allowed on and off your portion of the business-grade VPN service you use. Firewall products and services usually integrate unified threat management (UTM) services, which scan for known malware. They filter or quarantine any suspicious packets from your production network to ensure that your organization is protected from denial-of-service (DoS) attacks.

Since most organizations also conduct business on the public Internet, it's important to also secure your traffic as it moves from the VPN onto the unprotected Internet. So as you consider your network-hosted security service, check for secure gateway services between VPN and Internet (see figure). Such services

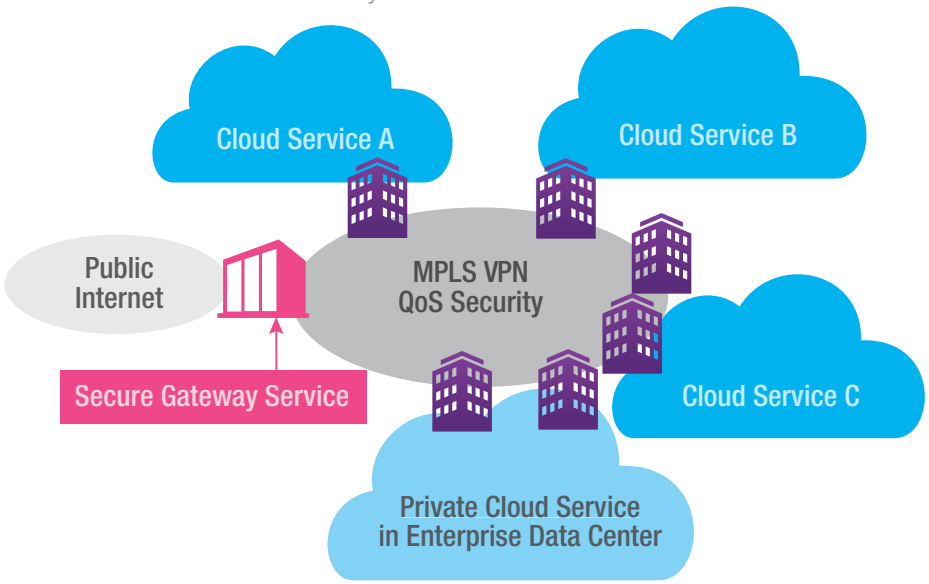


prevent you from picking up a network infection when using the unprotected public Internet by scanning and filtering traffic as it enters and leaves your VPN.

- *Data encryption*. Should you encrypt your data as it traverses the WAN to and from the cloud? There are a couple of schools of thought here. If using the public Internet, encryption is a documented best practice. But what about when using already partitioned MPLS VPN services? For some enterprises, encryption over an MPLS VPN is security overkill; for others, it's a "belt and suspenders" approach to doubling up their security. Financial institutions, certain government agencies, and others simply feel more comfortable if their data is not only partitioned but encrypted, too.

  If you do encrypt, keep a couple things in mind. Encryption increases your overhead, so check with your MPLS VPN provider about its impact on your performance service-level agreements (SLAs). Also, you might consider encryption directly from one of your premises sites rather than in the network if your last-mile connection isn't a VPN connection. A consumer-grade broadband Internet connection, such as xDSL or cable modem link, for example, will transport data "in the clear" to your first VPN point of presence (PoP). Using MPLS VPN technology to connect each corporate and cloud site is recommended, as described below.

MPLS VPN as WAN in a Hybrid Cloud Model



All corporate, data center, branch, and cloud sites are direct nodes on the MLPS VPN. The VPN provides secure gateway services as companies venture out onto the public Internet to conduct business.

Performance management. Public Internet services, again, are best-effort services; they do not come with any SLAs for network uptime or maximum latency, packet loss, and jitter. It's best, then, when creating a WAN foundation for your hybrid cloud to turn to a business-class service with QoS features baked in. In addition to security partitioning, for example, MPLS VPNs contain SLAs for basic network metrics (latency, packet loss, jitter) and built-in packet prioritization for QoS.

To make sure your WAN supporting your hybrid cloud is high performing, you'll want to do the following:

- Connect your cloud locations and corporate data center nodes directly to your MPLS network.
- Deploy WAN optimization tools for traffic shaping, load balancing, and application acceleration. These can be obtained by traditional procurement methods or "as a service" in the network
- Anticipate bandwidth requirements and investigate bandwidth-on-demand service options that will allow your capacity to grow and shrink in sync with your needs.

Summary

The hybrid cloud is the expanded data center of future. But its success, in large part, rests on the robustness of the WAN that provides access to all the various resources in any number of far-flung sites. Using a business-grade WAN service that gives you control over network security and performance of all sites – including the cloud sites – is essential. And it's usually more cost-effective and secure to use tools to control these variables that reside in the network, rather than attempting to continually upgrade and patch them at many distributed sites. Trying to keep up on your own requires IT resources that you might simply not have.

Any application experience is only as strong as its weakest link: if the security and network performance of a cloud experience don't match that of a local experience, your hybrid cloud project will fall short. Users will remain unempowered or will work around you to get the capabilities they require at additional cost and potential risk to your enterprise. So when creating your hybrid cloud, be sure to keep your eye on the WAN.

We also recommend that you visit XO's Network Enabled Cloud page to learn about the elements that comprise an intelligent network.

This ebook is sponsored by XO Communications.

About XO Communications:

XO Communications is a leading nationwide provider of advanced IP communications, intelligent networking, and cloud computing services for business, large enterprise and wholesale customers. These customers include more than half of the Fortune 500, in addition to leading cable, mobile wireless and domestic and international telecommunications companies.

XO offers a superior customer experience through its innovative solutions, its employees' focus on customers and the proven performance of its advanced network. To learn more about XO Communications, visit www.xo.com or blog.xo.com.

For XO updates, follow us on:
Twitter | Facebook | Linkedin | SlideShare | YouTube