For Enterprise IT:

Extend Your VPN to Bring Better Security, Performance and Reliability to the Cloud

Table of Contents

Enterprise IT leaders are increasingly embracing cloud models to drive down costs, boost agility and enable digital transformation for their businesses. IDC says "cloud first" will become the new mantra for enterprise IT, predicting that enterprise spending on cloud-related technologies and services will exceed $500 billion by 2020, more than three times what it is today.[1]

1 "IDC Predicts the Emergence of 'the DX Economy' in a Critical Period of Widespread Digital Transformation and Massive Scale-up of 3rd Platform Information Technologies in Every Industry," IDC, Nov. 4, 2015

TechTarget Custom Media

A TECHTARGET WHITE PAPER

In addition, a recent State of the Cloud survey found that 95% of enterprises are using cloud at some level—public, private or hybrid—and 82% of enterprises have a strategy to use multiple clouds.[2] On average, companies deploying cloud models are using three public clouds and three private clouds, either for running existing applications or experimenting with new business services.

With organizations putting more of their business-critical applications and data into the cloud, IT teams are facing a whole new set of very important connectivity challenges. In the cloud era, IT must ensure that security, performance, governance and compliance are not compromised as data and applications flow between multiple clouds and multiple data centers.

However, as many IT teams are finding out the hard way, simply using the Internet as the connective tissue between multiple clouds and multiple data centers is a risky proposition. Without investing in the proper technologies, the public Internet exposes organizations to significant risks that can adversely affect security, application performance and compliance.

At the same time, however, building on-premises solutions to address these challenges can be a highly expensive and complex endeavor. IT has to make a significant upfront capital investment in technology—routers, switches, WAN ports, security appliances and other solutions. What's more, IT needs to invest to ensure redundancy, and typically has to overprovision resources to address peak load requirements.

Furthermore, operating expenses are also costly because the solution needs to be managed, maintained and upgraded. And even with all of that, an on-premises solution will typically lack the agility, simplicity, flexibility and elastic scalability that organizations need and expect from their cloud-based environments.

Fortunately, there is a better way.

Enterprise IT teams can now extend the use of their MPLS virtual private network (VPN) to provide fast and highly secure connectivity for delivering business applications and data between multiple clouds and multiple data centers. By expanding the capabilities of the VPN, IT can deliver the network security, performance and control of a private cloud, with the economics, agility and elasticity of public clouds. What's more, using VPN enables IT to take advantage of a usage-based pricing model that results in lower costs and better budgeting predictability.

In this white paper we examine the benefits of using a VPN model to support and enable highly secure cloud connectivity for the enterprise. We also compare the VPN model to other potential solutions and provide guidelines in what features and functions to look for in a service.

2 "2016 State of the Cloud Report," RightScale, February 2016

The Risks of Using Public Internet

The shift to cloud models is creating opportunities for businesses, but it is also creating challenges for enterprise IT departments. As more applications get delivered through cloud models, IT must ensure maximum performance and availability. As users become more mobile and more devices are connected to the business through the Internet of Things, IT must contend with many more security vulnerabilities. As organizations seek greater agility through self-service provisioning and shared resources, IT must deploy solutions that support faster and simpler deployments—along with elastic scalability to meet on-demand requirements.

The challenges are exacerbated by the reality that most organizations are using multiple clouds and multiple data centers. If the business is relying on the Internet to connect these clouds and data centers, it is adding significant—and unnecessary—risks into the equation. These risks include:

- **Performance:** Public Internet traffic is subject to "hair pinning," which occurs when traffic is routed through additional locations to adhere to traffic security policies. This can lead to inefficient traffic flows and higher latency.
- **Availability:** Public Internet relies on "best effort" data transmission. Because of a variety of potential congestion factors, the delivery of critical data and applications can be delayed (or worse).
- **Security:** Public Internet is inherently less protected than a VPN, which means traffic is more vulnerable to DDoS (distributed denial-of-service) attacks, with less IT control over security policies and protections. This increases risk significantly.

IT can attempt to address these challenges by building their own private redundant networks, but the IT team had better be prepared for a major expense and a massive allocation of resources. As mentioned earlier, there is a host of equipment that must be purchased to set up the network. To add redundancy, IT must design and provision two separate connections. To support peak demands, IT must overprovision resources.

It could take months (or longer) for the IT team to design the network, specify the equipment, place purchase orders and get the equipment up and running, fully tested and fully deployed. Then there are the costs of ongoing maintenance, upgrades, user support, management and replacement. In addition, IT teams must account for the capital equipment costs and operational costs of supporting multiple branches and locations, as well as an increasingly mobile workforce.

Going through this type of on-premises deployment is time-consuming and risky. There will be a lot more to manage but, unfortunately, the network still may not have many of the features the business is looking for from its cloud deployments, particularly in delivering pooled resources, self-service delivery models and automated chargebacks. One more concern: At the rate technology is advancing, with the growth of new models such as software-defined networking, by the time the network is fully operational portions of it may already be obsolete.

The Benefits of VPN-Based Connectivity for the Cloud

The far better alternative is to extend the capabilities of a VPN that is already in place. With this model, IT can quickly and without hassle deliver the highly secure and high-performance connectivity their organizations require for multiple clouds and multiple data centers. Using an MPLS VPN service as the connective glue for cloud-based applications allows organizations to overcome the challenges inherent in public Internet connectivity, i.e., performance, security and availability. Another major advantage is that the IT team doesn't have to slog through the process of building and managing another private, redundant network. With the right VPN service, IT teams can take advantage of the following benefits:

- **Enterprise-grade network security:** Each company's traffic is isolated from other cloud or Internet traffic, thereby decreasing the risk of DDoS attacks and similar Internet-facing threats.
- **Higher performance and availability:** Customers can route traffic directly to cloud services, which means less latency, packet loss and jitter. Also, redundancy is built-in and pre-configured.
- **Simpler and faster deployments:** All elements are pre-integrated, deployed and managed as a cloud service. The only thing IT has to worry about is selecting a bandwidth level.
- **Greater control for governance and compliance:** Customers can use a self-service portal to gain visibility into and control over network and computing resources.
- **Elastic scalability and on-demand capabilities:** Cloud and network resources can scale automatically and dynamically in tandem, which means customers can easily address changing performance requirements. In addition, when bandwidth spikes unexpectedly, customers can burst on demand.

- **Lower costs and more predictable cost management:** With a usage-based pricing model, IT teams have a predictable monthly pricing structure with the flexibility to make adjustments when needed.

What to Look for in a Solution

IT departments are facing many difficult challenges in modernizing their infrastructures to support the shift to cloud computing, as well as related initiatives around mobility, social networking, big data analytics and the Internet of Things. By using an MPLS VPN for connectivity of cloud-based applications, IT can strengthen, secure and simplify one of their highest priorities. The key is to choose the right solution, with the right set of features, from the right service provider.

One of the groundbreaking solutions in the market is AT&T NetBond®, which is available to both new and existing customers of AT&T MPLS VPN. Because AT&T NetBond is an extension of AT&T's existing VPN service, AT&T customers don't need any additional equipment or access lines to get up and running quickly. The cloud services and network are already pre-integrated and the cloud resources become another node on the existing VPN. This dramatically simplifies deployments and ongoing management.

AT&T NetBond also addresses another critical factor in today's environment: support for a broad ecosystem of cloud providers. Organizations want to have the flexibility of utilizing multiple public clouds in addition to their own private/hybrid clouds, so a VPN-based solution for highly secure cloud connectivity must work with all of the leading third-party cloud providers. AT&T has an extensive NetBond ecosystem with industry-leading providers such as Amazon Web Services™, Box, Blue Jeans Network, Cisco, CSC Agility Platform™, Digital Realty, Equinix, HPE Helion, IBM®, Microsoft, Salesforce.com, SoftLayer®, Sungard® Availability Services™, Tech Mahindra, Virtustream® and VMware®.

In addition to simplified deployments and a broad ecosystem of cloud providers, AT&T NetBond addresses all of the other major features and functions that IT departments should be looking for in a cloud connectivity solution, including:

- **Advanced Technology:** AT&T NetBond is built on a robust and scalable technology platform designed to meet the availability and performance requirements of enterprise applications and workloads. With AT&T NetBond, customers route traffic directly to cloud services and can use CoS traffic marking to ensure quality of service for business-critical applications. Customers have experienced as much as 50% lower latency with AT&T NetBond, when compared to cloud connectivity over a traditional Internet connection.
- **Multi-Layered Security:** With intelligent centralized routing control, AT&T NetBond isolates each company's traffic from other cloud and Internet traffic, providing enterprise-grade network security for applications and workloads. Security risks such as DDoS are minimized, with applications delivered across multiple clouds and data centers through a highly secure network connection via the AT&T MPLS private network.

- **Cloud Economics:** With AT&T NetBond, service fees are based on a minimum bandwidth commitment, so there is a predicable monthly pricing model for IT budgeting. Organizations can also scale network resources as demands fluctuate (or burst) for greater business agility.
- **Simplified Management and Provisioning:** Customers can use a self-service portal for visibility and control over network and computing resources. With on-demand provisioning, organizations can reduce deployment time from days to minutes, while also avoiding the expenses involved in overprovisioning resources.

One of the other advantages of using AT&T NetBond is that it is part of a broader portfolio of cloud solutions from a global leader with a trusted reputation for building best-of-breed networks and supporting enterprise-class IT environments. For example, AT&T NetBond customers can also use services such as AT&T Colocation Services as well as AT&T Cloud Storage.

With AT&T Colocation services, customers can connect to the cloud from their private colocation infrastructure for an integrated hybrid solution using AT&T MPLS VPN. AT&T NetBond with AT&T Cloud Storage provides customers with a highly secure connection from their AT&T VPN to a private cloud where users can easily access, share, back up and restore files from virtually any location at any time.

Taking the Next Step

Cloud computing is becoming critical to enterprises in driving next-generation business agility and competitiveness. Organizations are embracing multiple clouds as part of an effort to support new economic models, mobility, big data analytics, the Internet of Things and other critical next-generation business initiatives.

With more business-critical applications and data running in cloud environments, IT decision-makers have to ensure that the connections between multiple clouds and data centers are secure, reliable, simple to provision, easily scalable and cost efficient. Simply relying on the public Internet is becoming too risky, and building on-premises solutions is too expensive.

By extending the proven technology of an MPLS VPN into cloud environments, IT teams can secure cloud connectivity and improve the performance and availability of cloud applications. In choosing a VPN-based connection, it is important to work with a provider that delivers leading technology, simplified deployments, cloud economics and the highest levels of cloud security.

As it has done so often in the past, AT&T is once again providing leadership in delivering innovative connectivity solutions to help enterprises secure and advance their use of cloud models.

For more information on how AT&T NetBond can help your organization deliver highly secure and reliable cloud connectivity, please contact AT&T at http://www.att.com/netbond.