

## WHITE PAPER

---

### Assessing the Benefits of Outsourced Private IP VPNs

---

Sponsored by: iPass

---

Ron Kaplan  
April 2006

#### IDC OPINION

Broadband VPNs deliver a flexible and cost-effective approach to networking, and they are particularly well suited to companies with many small offices or retail locations. Broadband VPNs that use the public Internet offer the ability to easily utilize multiple service providers and broadband access technologies instead of needing to interconnect various private networks. However, there are pitfalls. The large number of broadband providers and the differences between their services present challenges for a company hoping to knit together a broadband VPN using DSL, cable modem, and broadband satellite connections from a variety of providers. IDC believes that partnering with a managed service provider, which would aggregate and manage the disparate broadband connections, is the most effective way for a large company to build a broadband VPN.

#### IN THIS WHITE PAPER

This IDC White Paper examines broadband VPNs, assessing the advantages and disadvantages of public and private VPNs, and provides recommendations on how to overcome the drawbacks through partnering with a managed service provider.

#### SITUATION OVERVIEW

Confronted with the need to connect sites securely and cost-effectively, while delivering reliable and dependable access to applications, network managers have several options. Dial-up networks are slow and tend to get congested because of large files and latency-sensitive applications. Legacy solutions, such as private line and frame relay, offer dependable quality, but tend to be relatively expensive to install and operate.

IP VPNs, both public and private, offer another alternative. The private IP VPNs typically run over a carrier's private MPLS network, and tend to be overkill in terms of features and pricing for companies with many small branch offices or retail locations. A well-managed broadband public VPN offers a cost-effective solution with an appropriate level of features that is both secure and reliable.

These broadband VPNs use DSL or cable modems to connect sites to the public Internet, which is much more cost effective than the private lines that are typically used in frame relay and private IP VPN solutions. An encryption technology such as IPSec or SSL keeps the data secure.

IDC sees several advantages for using a public network instead of a private network for broadband VPNs. Public networks enable a maximum number of possible connections; customers can implement DSL, cable modem, broadband satellite from multiple providers, and the sites will all interconnect over the public Internet. This is highly desirable when using broadband VPNs because DSL and/or cable modem access may not be available at each site, and the customer will likely need to use multiple providers to knit together complete coverage. Connecting broadband sites from multiple providers over the public Internet is far easier than having to interconnect multiple private networks running MPLS.

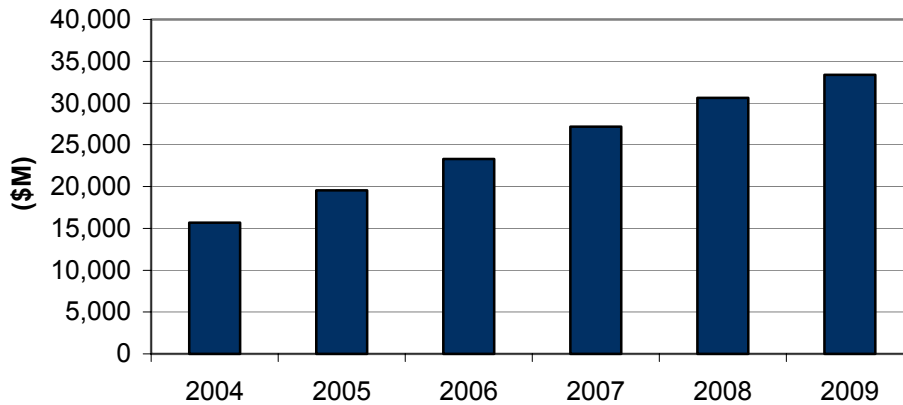
In contrast to frame relay and private lines, which are typically not encrypted, broadband VPNs are encrypted across both the access lines and through the Internet. This makes broadband ideal for retail transactions, where customer data needs to be kept secure, but where a more expensive and feature-laden private IP VPN is overkill.

Although broadband was first intended as an Internet access service for residential customers, the technologies have matured and improved, and now are available from some providers in business versions with SLAs and 24 x 7 customer support. Broadband VPNs also offer a flexible approach to building networks. Because the underlying transport is the Internet and not a private network, customers can knit together access from a variety of carriers, using a combination of DSL and cable modem, as well as perhaps other access methods. The flexibility of this network architecture means that it is easy to connect teleworkers and traveling employees remotely.

Although still not ubiquitous, broadband is now widely available from a range of providers, including telecom carriers, Internet service providers (ISPs), cable TV providers, and independent broadband companies, and its use is growing (see Figure 1). In many cities, there are multiple providers, and customers benefit from the competition. However, when constructing a broadband VPN, dealing with multiple providers in each city can cause headaches. Specifications, service levels, equipment, port speeds, and features can differ greatly from provider to provider, and also within different markets of the same provider. Each provider may specify a different broadband router or bridge, which ratchets up support and training costs in the customer's IT department. Providers will also offer differing SLAs with varying guarantees on service and network uptime, mean time to repair, and latency. This causes risks when a company is trying to deliver reliable access to corporate applications to all branch sites.

**FIGURE 1**

U.S. Broadband Services Revenue, 2004–2009 (\$M)



Source: IDC U.S. Broadband Services 2005–2009 Forecast (IDC #34134, October 2005)

In terms of service availability, there's no way for a network manager to get a comprehensive view of what's available or what's possible until the service order is in progress. Some sites that appear to be eligible for service will not be. This leads to false starts and causes companies to change strategies for broadband VPN deployment in midstream. Once the service is up and running with multiple service providers, the network manager must deal with multiple invoices with differing contract terms, creating additional work for legal, vendor management, and accounts departments.

In the case of a large-scale do-it-yourself (DIY) deployment, the obstacles are particularly significant. Each site needs a broadband connection installed, and this would mean dealing with multiple vendors, just for Internet access. The next step is to install and configure a VPN device, usually a router, at each site, train local staff in its operation, and then maintain and support it. Typically, the various broadband service providers would not support VPN issues, leaving the network manager to troubleshoot on his own. In addition, there would be no end-to-end SLAs up to enterprise standards from the various broadband providers.

The headaches inherent in a large-scale DIY broadband VPN are such that network managers tend to agree that the challenges are not worth the cost savings. However, there is a solution: outsourcing the management of the broadband VPN to a managed service provider.

The managed service provider coordinates multiple broadband providers — telcom carriers, cable operators and other ISPs — to deliver a coherent broadband VPN to the customer. The managed service provider (MSP) chooses the best connectivity option for each given site — DSL, cable modem, or even T1 or satellite — and then handles installation, billing, and customer service, and manages quality and security. Through its experience with the different broadband service providers, the MSP determines which options deliver the best quality and bandwidth for the price. The MSP delivers end-to-end SLAs across multiple service providers and equipment

types, and guarantees the operation of the corporate VPN. Instead of dealing with 20 different broadband providers and six different equipment vendors, the customer deals only with the MSP, which has more leverage than the customer with the broadband operators because it manages the VPNs of multiple customers. The MSP can deliver the service for a single cost-effective, nationwide price because of its bulk buying power.

## FUTURE OUTLOOK

While in theory a managed service provider can deliver end-to-end quality and security in a broadband VPN, not all providers are the same. IDC suggests several points for a company to consider when shopping for a managed service provider to handle their broadband VPN:

- ☒ Does the MSP deliver end-to-end, 24 x 7 management? Does it provide end-to-end SLAs for support of network performance as well as customer support metrics, such as site-to-site delay, throughput and availability, on-time installation, proactive notification, billing accuracy?
- ☒ Does the MSP offer a range of connectivity options and deal with a wide range of providers? Broadband availability differs from city to city, and neighborhood to neighborhood. To be effective and to deliver the greatest value to its customers, an MSP must not be wedded to specific vendors or technologies.
- ☒ Does the MSP supply a detailed network design and pre-qualification? The MSP should be able to map out in advance its strategy for building the broadband VPN, based on its existing relationships with broadband service providers.
- ☒ Does the MSP offer detailed end-to-end reporting? Is this reporting just network operations center (NOC) to customer site, or is it truly customer site to customer site? Is the reporting real-time and historic? Reporting is key in catching small problems before they become big ones and in improving VPN efficiency.
- ☒ Does the MSP offer professional services to help with complex issue? Certain applications, such as Voice over IP, or certain deployment issues may require in-depth consulting services to ensure that the network is configured and operating optimally.
- ☒ Does the MSP centrally and securely manage end points, including configuration, inventory, or operating system upgrades?
- ☒ Does the MSP offer access to multiple tier 1 ISPs? Having redundant access to multiple ISPs is particularly important for datacenter locations to ensure business continuity. Does the MSP provide dial-up or wireless backup for branch sites?

## **CONCLUSION**

IDC believes that for companies with a large number of branch sites interested in a broadband VPN, managed IP VPN services deliver an overall level of quality and service that is difficult to match at the same cost internally. Using public networks gives the network the flexibility to connect sites with broadband access from any provider, using any broadband technology. While broadband Internet access for a single location is relatively easy and straightforward to install, the task grows increasingly complex when needing to serve multiple locations in different cities. This situation involves multiple providers, different broadband technologies, and diverse equipment types. The complexity further increases when layering a VPN on top of the broadband access.

A managed service provider that meets the criteria laid out in this paper should be capable of delivering an end-to-end broadband VPN meeting a company's networking requirements, while capitalizing on the cost benefits of broadband.

## **DEFINITIONS**

- ☒ DSL: Digital subscriber line
- ☒ IP: Internet protocol
- ☒ ISP: Internet service provider
- ☒ MPLS: Multiprotocol label switching
- ☒ MSP: Managed service provider
- ☒ NOC: Network operations center
- ☒ SSL: Secure Sockets Layer
- ☒ VPN: Virtual private network

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.