

Whitepaper

Broadband IP-VPN: The “Econo-Net” Branch/Remote Office Connectivity and Security Solution for Use as a Primary Network or Back-Up to a Carrier Grade, Core Enterprise Network

September 2008



S2S Communications
A Fiberlink Company
8 Tower Bridge, Suite 825
161 Washington Street
Conshohocken, PA 19428
P: 610-260-4710
F: 610-260-4711

Table of Contents

<i>Introduction</i>	3
<i>Broadband IP-VPN Technology Overview</i>	4
<i>Branch Office “Econo-Net”</i>	6
<i>Primary Network Architecture</i>	9
<i>Finding a new Role in the Core Network</i>	12
<i>Life-Cycle Management: “Build vs. Buy”</i>	13

About S2S Communications

S2S Communications LLC (www.s2scommunications.com) recently completed its spin-off from sister company Fiberlink Communications Corporation (www.fiberlink.com), the well-established end-point secure mobility provider. S2S is a managed services provider delivering network design, engineering, implementation and management to its Fortune 1000 customer base, relying on a suite of managed broadband VPN products and services. S2S is focused on developing remote business office/workplace connectivity and security solutions utilizing broadband-based transport and IP-VPN secure networking products and services, while at the same time creating the next generation technology through its internal R&D effort. Our current offerings include:

- A suite of secure managed network access products/services
- Utilization of high-speed, low-cost broadband Internet access (XDSL, Cable, WWAN) with a national and global footprint
- Turnkey solution approach (bundled hardware and fully-managed solution)
- 24x7 proactive management via global NOC
- Remote/Branch office network solution:
 - Connect remote offices to corporate data center(s) via Internet-based secure IP-VPN architecture
 - Extend corporate LAN and applications to systems/users at a remote/branch office or retail store
- Broadband connectivity solutions (e.g. teleworker, remote workplace, etc.)
- MPLS over DSL
- Wireless wide area network (WWAN) connectivity for branch office redundant, temporary and permanent applications
- Unified threat management (UTM) capabilities

Introduction

Business Drivers

Larger enterprises typically have remote and branch offices that represent more than half of an organization's total work force. In larger retail organizations, this percentage can be even higher. According to the industry analyst group Nemertes Research, in 2005 approximately 91% of employees worked in locations other than headquarters – up from 85% in 2003.

Smaller branch offices may contain as few as 5 and up to 50 workers. For these workers at smaller offices or retail stores, having access to important business applications is as important as employees at a large corporate HQ. In fact, in cases where employees are engaged in direct front-line functions (e.g. sales and services), there is even a more pressing need to be networked to critical business processes. The legacy approaches (non-IP) to provide access to the applications are inadequate in terms of performance and cost of ownership. A variety of factors drive the inadequacies, including increasing traffic volume, increased Internet usage, new application types, an evolving threat landscape and mounting regulatory pressures.

As companies migrate from legacy carrier connectivity solutions they are seeking a new branch office solution – one that provides affordability, higher speed transport, scalability, flexibility and robust protection from security threats. The state of the art networks of today incorporate carrier-grade MPLS in the core WAN, coupled with secure cost-effective IP-VPN networks to serve the smaller/remote office environment.

A Note about the Retail Sector

The retail vertical sector is highly competitive. To the extent that corporations find themselves constantly being challenged to gain an edge on their competitors, while striving to maintain customer loyalty and attract a broader base. This marketplace is all about providing customers with goods and services in a way that keeps them coming back for more. For companies with bricks and mortar stores, the steady growth of online shopping has created a true buyer's market. Retailers are working to re-engineer a new customer experience that requires real-time collection of sales data, buying patterns, the status of current campaigns, inventory stock levels, etc. These metrics are instrumental in continuously fine-tuning the supply chain, including purchasing, distribution, staffing and physical layout at individual stores. From an IT perspective, these business requirements drive the need for effective and timely communication between the branches and regional headquarter facilities, and perhaps directly to distribution centers or even other stores. Retail-driven companies are even lighting up their storefronts with WIFI access for corporate/regional managers and customers. There is clearly a new paradigm taking place within the retail sector.

The environment mandates a new solution for networking the many distributed sites in the retail industry – one that enables relatively high bandwidth and secure/reliable communications at a low price point. The IP-VPN network solution has become the preferred wide area network solution because it is capable of consolidating all of the required security and networking capabilities into a single platform.

Broadband IP-VPN Solution Overview

The Genesis

The Internet has created a ubiquitous wide area network available to anyone with a computer and an access connection. The mid to late 1990's saw the development of a technology that utilized protocol encapsulation, "tunneling", techniques, coupled with new data encryption technologies to enable secure data communications between two computing end points. This technology, known as IPSec Virtual Private Network (VPN), quickly became the de-facto standard for mobile PC user/remote access into the corporate network.

Initially, Internet access was provisioned through ISP dial accounts running at analog dial speed. But another dynamic was taking place based on new technologies known as broadband. Telcos invested in broadband infrastructure based on a new set of broadband standards (e.g., xDSL, Cable). Broadband transport was clearly a major catalyst for the utilization of IP-VPN technology in the corporate WAN. A recent FCC report states that broadband is available via DSL to 79 percent of local telephone company subscribers, and via cable Internet to 93 percent of cable television subscribers. Although it is important to note that these statistics are focused on the B2C market, the general trend for the past 5 years is that both DSL and Cable Internet continue to increase in availability to business users at remote/branch office locations. Cable Internet still has a relatively low penetration rate for business usage because the cable infrastructure was constructed to serve the residential community. Lack of cable connections at many commercial property locations, and high costs associated with creating cable connectivity, limits the current usage of Cable in business applications.

Key Characteristics

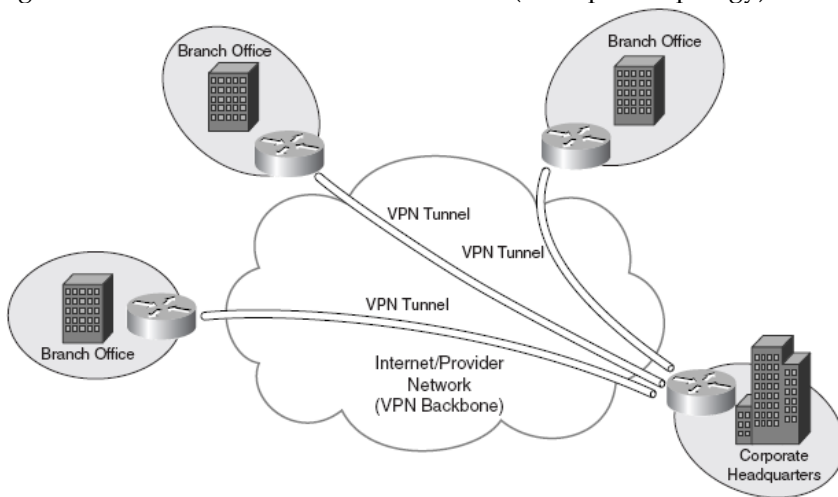
- IPSec protocol is a suite of IETF open standards and supports a combination of the following network security functions:
 - 100% IP-based protocol and not dependent on specific/private transport offerings
 - Data confidentiality—Encrypts packets before transmission
 - Data integrity—Authenticates packets to help ensure that the data has not been altered during transmission
 - Data origin authentication—Authenticates the source of received packets, in conjunction with data integrity service
- Support for highest level of encryption standards including Triple DES (3DES), and the 256-bit Advanced Encryption Standard (AES), the highest level available today
- The IPSec protocol provides protection for IP packets by allowing network designers to specify the traffic that needs protection, define how that traffic is to be protected, and control who can receive the traffic
- IPSec VPNs afford flexible design topology supporting traditional hub-and-spoke, mesh and hybrid topologies
- Industry leading appliances used for VPN networks have robust firewall and unified threat functionality and can also afford QoS, policy/route based VPN, and open layer-3 protocol support including RIP and OSPF
- Enterprises that need support for other Layer 3 protocols, such as AppleTalk or IPX, can use protected generic routing encapsulation (GRE) tunnels over IPSec

Key Strengths

- Provides highest degree of wide area network value because it can utilize relatively low-cost, high speed broadband Internet access as the transport.

- Strong security—Inherently strong security features enable user authentication, data confidentiality, and integrity. Users are authenticated with digital certificates or preshared keys. Packets that do not conform to the security policy are dropped.
- Support for teleworkers and mobile workers—Headend IPsec VPN devices scale, to serve up to thousands of geographically dispersed offices.
- Ease of deployment—No service provider intervention is required to set up the VPN, although many enterprises choose to take advantage of the service provider’s managed-service experience for regional or national multi-site deployments to reduce costs, accelerate service introduction, and mitigate risk.
- Reduced congestion at hub site—When configured for “split tunneling,” the branch office VPN appliance can forward Internet-destined traffic directly instead of through an IPsec tunnel, and establish a tunnel only for related traffic being forwarded to the hub. This reduces congestion at the hub site. Furthermore, packets directed through the split tunnel can be locked down based on firewall rule sets and other access control mechanisms.

High Level VPN Branch Office Architecture (hub-spoke topology)



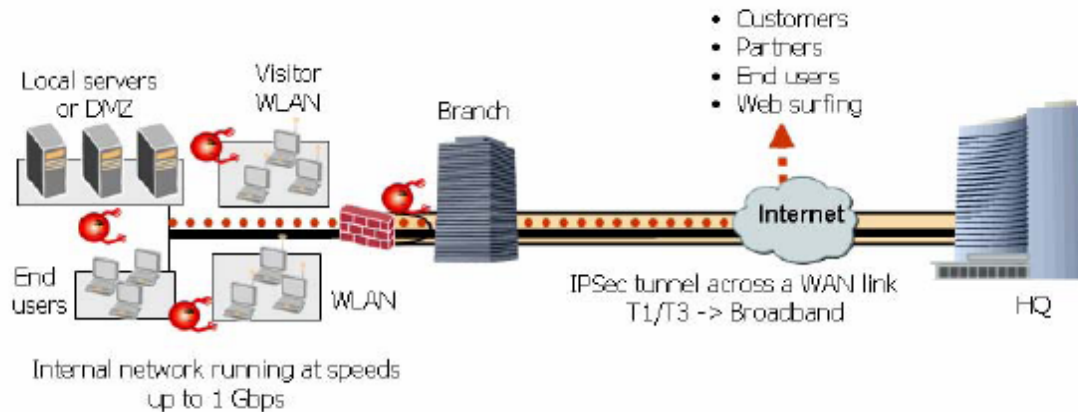
VPN Application Goals, Objectives and Trends

Current VPN solutions combine powerful networking functionality with best in class layered security applications, including in-line network based Intrusion Detection/Prevention System (IPS), Anti-Virus (AV) and Web content filtering. The new classes of devices with these capabilities are known as Unified Threat Management (UTM) appliances. When VPN networks are properly designed, engineered and managed, a branch office solution is capable of delivering the following:

- Fast and secure site-to-site VPN connections. This is primarily to establish access to centrally located applications and resources, but should also include support for employee remote access and direct connections to local partners.
- Direct, secure Internet access. This is important to avoid the growing disadvantages associated with backhauling Internet traffic through a regional headquarters location. Given the layered security features now available in UTM appliances, the decision to split out Internet traffic can be rationalized by IT Security staff.
- Improved security for internal networks and systems. This applies directly to the branch office, but will also indirectly benefit all other sites connected to it.
- Improved ease of use and economics. This can be accomplished by having an appliance, appropriately sized for the location, that can consolidate as many security and networking

capabilities as practical without making any compromises, especially in terms of quality of the security functions, performance, and reliability.

Business Level View of Branch Office VPN



Branch Office “Econo-Net”

Broadband IP-VPN, MPLS or legacy Frame Relay? The IT Network staff will have analyzed the pros and cons of each technology and solution at one time or another. The short answer to the question is: It Depends! There are a number of variables to consider when selecting the most appropriate solution:

1. **What are the company's WAN objectives?**
 - Do we simply need to connect remote offices to a central location for server resource access?
 - Are there any critical applications such as voice that must run across the WAN?
2. **Is cost a primary decision factor?**
3. **How much bandwidth do we really need?**

Broadband IP-VPN

If the primary objectives include networking remote/branch offices with one or more corporate data centers to extend access to computing resources such as File Servers, Email Servers, vertical business applications and the like, and you can tolerate a lesser degree of availability than carrier-grade private networks, then broadband IP-VPN is the solution you should consider. **VPN is by far the most cost effective way to establish a private wide area network.**

Frame Relay

Frame Relay is legacy, carrier-grade technology that was engineered on an over subscription model. Carriers will sell a Committed Information Rate (CIR) using a permanent virtual circuit (PVC) on their Frame Relay Network. This rate is the bandwidth you are guaranteed by the carrier. CIR speeds are based on the DS-X hierarchy standard (i.e. 56K, 128K, 256K, etc.). You may burst above your purchased CIR, but in times of heavy network congestion any packets sent above the CIR will be eligible for discard by the carrier. Carriers have progressively lowered Frame Relay costs to retain existing customers, but in more recent years have been aggressively working to migrate their existing customers to MPLS. As

corporations evaluated the alternatives, many have chosen to implement broadband IP-VPN and realize total cost of ownership (TCO) savings of 50% or more.

MPLS

If there are Quality of Service (QoS) sensitive applications running across the WAN (e.g. high quality VoIP), then you should consider MPLS. MPLS is a private networking technology similar in concept to Frame Relay in that it is delivered in the "cloud". The primary difference with MPLS is that one can purchase QoS of service for applications across the WAN. During the provisioning process, the carrier will interview you in order to determine which applications are important to your business and will subsequently build a QoS template to service those applications on the WAN. These applications will be given priority over all other traffic in times of peak load. MPLS will, generally, always be more costly than IP-VPN; however, MPLS is a private network solution and the only current technology that supports QoS.

MPLS and IP-VPN Compare and Contrast (adapted from Cisco Systems) -

	MPLS-Based VPN	IPSec-Based VPN
Topology	Site-to-site VPN: Hub-and-spoke or full-mesh	Site-to-site VPN: Mainly hub-and-spoke
Security		
<i>Session authentication</i>	Establishes VPN membership during provisioning, based on logical port and unique route descriptor Defines access to a VPN service group during service configuration; denies unauthorized access	Authenticates through digital certificate or preshared key Drops packets that do not conform to the security policy
<i>Confidentiality</i>	Separates traffic, which achieves same results delivered in trusted Frame Relay or ATM network environments	Uses a flexible suite of encryption and tunneling mechanisms at the IP network layer
QoS and SLAs	Enables SLAs with a scalable, robust QoS mechanism and traffic-engineering capability	Does not address QoS and SLAs directly, although Cisco® IPSec VPN deployments can preserve packet classification for QoS within an IPSec tunnel
Scalability	Highly scalable because no site-to-site peering is required Capable of supporting tens of thousands of VPNs over the same network	Acceptable scalability in most typical hub-and-spoke deployments Scalability becomes challenging for a very large, fully meshed IPSec VPN deployment; may require supplemental planning and coordination to address key distribution, key management, and peering configuration
Management		
<i>Site-to-site support</i>	Yes	Yes
<i>Remote access support</i>	Yes, if used in conjunction with IPSec	Yes
<i>Provisioning</i>	Requires one-time provisioning of customer edge and provider edge devices to enable the site to become a member of a MPLS VPN group	Reduces operational expense through centralized network-level provisioning for CPE-based service offering Uses centralized provisioning for network-based service offering
<i>Service deployment</i>	Needs MPLS-enabled network elements at the core and edge of the service provider network	Can be deployed across any existing IP networks or the Internet
VPN client	Is not required because MPLS VPN is a network-based VPN service; users do not need VPN clients to interact with the network	Is required for client-initiated IPSec VPN deployments Cisco VPN client software is supported by Microsoft Windows, Solaris, Linux, and Macintosh operating systems
Place in network	Core network	Local loop, edge, and off-net
Transparency	Resides at the network layer Transparent to applications	Resides at the network layer Transparent to applications

Frame Relay to IP-VPN-

Corporations currently using Frame Relay at remote/branch offices undoubtedly have users and business applications that can tolerate to minor service interruptions. These Frame Relay users should seriously

evaluate a broadband IP-VPN solution. If properly engineered, implemented and managed, a VPN network solution should afford overall site availability in the range of 99.5%-99.9%. Fully redundant solutions can be expected to deliver greater than 99.9% availability. The most immediate and tangible benefit of the IP-VPN approach is real cost savings, which are significant when compared to Frame Relay. For example, a network with 25 branch offices using hub-spoke topology and Frame Relay 128K CIR PVCs would incur costs in the range of \$5K-\$7K/month. Using a typical mix of broadband circuits with VPN, the monthly circuit costs would be approximately half, plus there is the added benefit of increased bandwidth associated with the DSL or Cable Internet access. A high availability broadband solution using dual broadband access links or wireless 3G back-up could still be implemented for less cost than the Frame solution. Additionally, significantly more bandwidth would be afforded for both load dynamic traffic routing and/or fail-over configurations.

Forrester Research, Inc. stated in a recent analyst survey.....

We continue to see stable adoption levels of site-to-site IPsec VPNs and we don't see enterprises abandoning the technology anytime soon. Why? Many enterprises are currently re-architecting the branch office network. As part of this trend, many companies are abandoning the costly legacy, dedicated circuit hub-and-spoke model for site-to-site branch office connectivity in favor of either (1) MPLS for high-bandwidth converged voice, video, and data network or (2) IP-VPN for low-cost, encrypted connectivity across the Internet. Again, we recommend this latter choice if you:

- Have a simple mix of apps and access to low-cost broadband. Site-to-site IPsec is ideal for firms that need a couple of megabytes of bandwidth for non-latency sensitive apps like email, office productivity tools, and file sharing services.
- Want to allow direct Internet access at the branch. Typically, most companies backhaul Internet traffic to a central site where security gear like firewalls, intrusion prevention systems, and gateway antivirus can prevent malicious activity from spreading to the corporate WAN. However, with the popularity of security-oriented branch routers like Cisco's ISR or Juniper's SSG products, firms can shift to a decentralized model, allowing split-tunneling, a process whereby Internet-bound traffic is scanned and protected before safely routing it directly to the Internet at the branch and corporate-only traffic is sent directly across the IPsec intranet.

Economy and Security

The economies of IP-VPN stem from the use of the public Internet as the transport vehicle. Because the wide area network is a public venue, there is increased exposure to potential security vulnerabilities. This is why IPsec was originally developed. Advanced encryption techniques protect information packets transported across the Internet. By encrypting the TCP packets, a secure tunnel is created that provides exceptional levels of protection from potential leakage or loss of confidential information.

There is one simple overriding rule or best practice when it comes to information security. Robust security can be only achieved through a layered solution. This means protection against threats coming from both network and application vectors. The UTM appliances used in IP-VPN networks have the capability to protect against threats coming from both vectors. Network threats are protected through firewall rules and Intrusion Prevention service. Application threats, typically in the form of email attachments or file downloads, are detected and removed by the AV scanning service in the appliance.

Lastly, the corporation's workstations at the remote or branch office should be protected by the appropriate security software, coupled with periodic content updates as mandated and implemented by the IT organization.

VPN "Econo-Net" Summary-

Branch offices and their personnel are a vital business asset. As such, it is essential to efficiently and effectively provide them with access to necessary computing resources regardless of whether those resources are operated within central-site locations or at other points accessible via the Internet. At the same time, an evolving threat landscape and mounting regulatory pressure require organizations to enhance internal security at branch offices. Of course, all of this needs to be done within budget. In summary, IP-VPN branch office solution is capable of delivering the following:

- Fast and secure site-to-site VPN connections. Because the Internet is the wide area network, it mandates the need for high level data encryption and proper/best practice firewall configuration.
- Direct, secure Internet access for split tunneling applications. This is important to avoid the growing disadvantages associated with backhauling Internet traffic through a regional headquarters location.
- Improved security for internal networks and systems. This applies directly to the branch office, but will also indirectly benefit all other sites connected to it.
- Improved ease of use and economics. This can be accomplished by having an appliance that is appropriately sized for the location use cases and that can consolidate as many security and networking capabilities as practical without making compromises. Fortunately, with today's Unified Threat Management appliances from Cisco, Juniper, Fortinet, SonicWall and others, the security layers are packaged into a single hardware footprint and service subscription.

Primary Network Architecture

Technical Architecture and Application Overview

Unlike private lines that are an expensive, non-redundant, and present a single point of failure and switched circuits that rely on a single carrier's network and availability, Layer 3 site to site VPN Tunnels using IPSec Encryption utilize the entire Internet cloud as their transport domain. As such, they garner the full redundancy, availability, reliability, and resiliency of an existing, public, worldwide backbone network. In this manner, a Central Corporate Data Center may house email servers, accounting and transaction servers, application servers, file servers and network domain services that require access from hundreds of branch offices all across the country. In the past, this could be a very expensive solution as each office would need a private line or switched circuit for each of the remote sites that provided a meager amount of bandwidth, priced based on compounding factors such as distance. And if the company needed redundant connections, the already high cost was doubled.

On the other hand, broadband Internet is widely deployed and inexpensive to purchase and maintain. Also, the bandwidth of broadband and flexibility of the VPN technology allow for a wide array of networking possibilities. Redundant connections, split tunneling, secure firewalling, and policy management are all at the customers' disposal. In a proven solution for an electronic gaming company, VPN/firewall appliances are placed at the retail branches. A broadband Internet access connection is provisioned at the remote locations and a large dedicated carrier grade circuit is provisioned at the corporate data center. Also, at the data center, redundant VPN concentrators are deployed to terminate the incoming VPN tunnels. The branch site VPN/Firewalls and the core site VPN Concentrators are

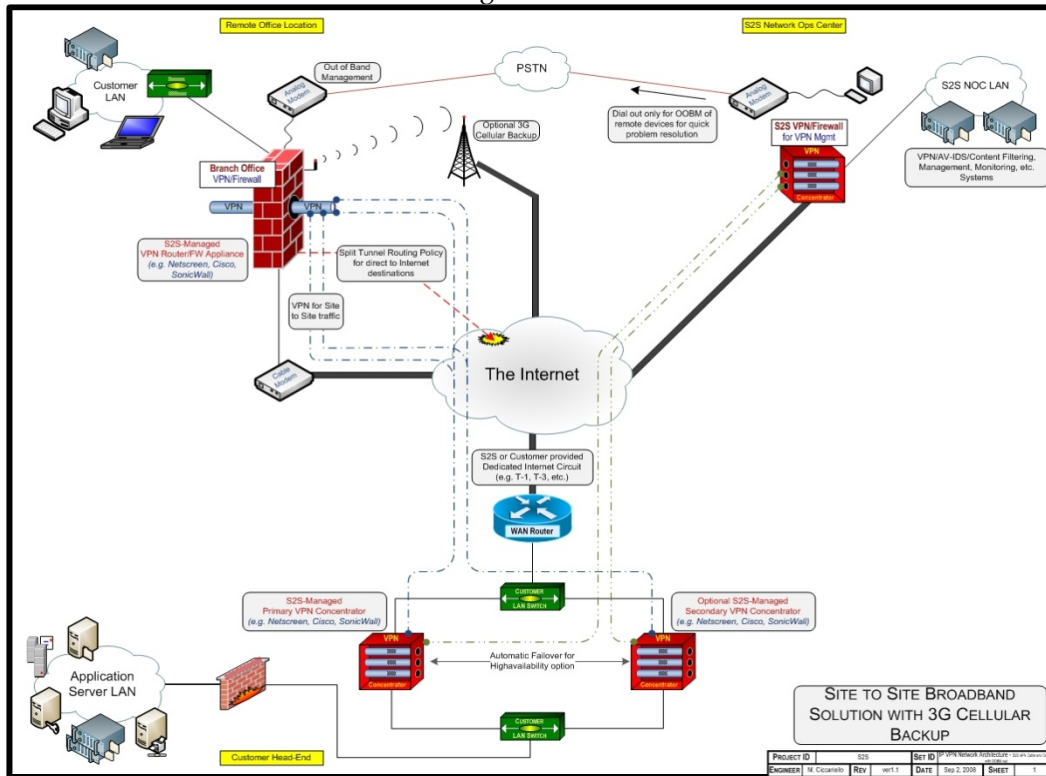
programmed with security keys and policies to ensure the identity of the end sites while they attempt to establish a tunnel. The branch office VPN/Firewall is configured to create two tunnels, one to each VPN concentrator, just in case one of becomes inaccessible. Once the branch office comes online, the VPN tunnels are negotiated, authenticated, and authorized. Through this secure tunnel, the central offices' servers are now available to enforce network domain policies and to provide common services such as email, files, and applications. This particular gaming company uses the tunnel to allow customers to download games from the corporate server farm to play on kiosk machines. Some retail companies may have credit card transactions go directly to the credit card verification website via https so a split tunnel solution is implemented.

In split tunneling, the VPN/Firewall has a security policy, governing which traffic can use the tunnel, which traffic can go directly to the Internet, and which traffic must stay within the site. Many retail companies now offer Internet to customers in their store either through kiosk machines or through wireless networking. Split tunneling, combined with proper firewall policies and utilization of "security zones", will allow customers to connect directly to the Internet without the possibility of gaining access to the VPN tunnel and the corporate intranet. Restaurants too can use the split tunnel to allow their networked IP jukebox to download songs from a subscribed provider while keeping all inventory tracking, register transactions and accounting data separated.

QoS is another feature that can be implemented at the remote sites to guarantee available bandwidth (VPN network only) for high priority company traffic. Though kiosk machines for Internet browsing may be an added bonus that a company may want to give their customers, it is not such a priority that they would sacrifice business critical traffic bandwidth. QoS can make sure that the proper bandwidth is always available for priority data traffic. Also, if the bandwidth on a backup connection is limited, QoS policies can be designed to further scrutinize traffic and allow only the most critical data through.

Though broadband service is relatively reliable, backup for a possible network failure by an ISP needs to be anticipated. Depending on what is available in a branch office area, backup technologies can include dial-up, ISDN, wireless or even a secondary broadband provider. Backup connections work seamless to the end user. When the primary Internet connection fails, so does the VPN tunnel. A backup Internet connection will then initiate connection to the Internet cloud and establish a new VPN tunnel (or tunnels) to the central datacenter VPN concentrators. The use of analog dial back-up is popular in the retail sector because the mission-critical application of credit processing can still be reasonably supported at analog dial speeds.

Technical Architecture and Solution Diagram



Another important aspect of the modern VPN landscape is operational/trouble management, which starts with a best practice approach to network monitoring and key metric threshold alerting. Network monitoring ensures that all sites are operational, functioning as designed, and problems are being addressed proactively by a 24x 7 staff so that issues are resolved to meet critical business SLAs. Monitoring and management can be accomplished through an IPSec VPN tunnel from a Network Operations Center to the corporate headquarters VPN Concentrators. From there, policies are created to allow insight into the health of the network through logging, traps, and statistical collection and reporting. When outages do occur, visibility into the network is even more critical. With VPN's down and remote sites cut off from headquarters, "Out of Band Management" is an integral part of the VPN solution. With hundreds of branch sites across the country, it is not feasible to have a dedicated network engineer on staff to troubleshoot the access router. Out of Band Management allows the ability to dial into the console port of the VPN/Firewall Router to troubleshoot the problem and to achieve resolution as quickly as possible. An Out of Band Access Solution can be achieved using an existing or new dedicated phone line and a V.92 analog fax modem. Out of Band Management affords higher services levels through reduced time to restore (TTR) and improved availability.

Utilizing 3G Wide Area Wireless

Mobile wireless data technology has matured considerably with the introduction of 3G. Major wireless carriers such as Verizon, AT&T Wireless and Sprint have nationwide coverage and through various 2.5/3G technologies (and emerging 4G/WiMax) that afford bandwidth from 100Kbps to over 10Mbps data rates. In many cases, this "always on" wireless bandwidth rivals landline broadband such as DSL. Fixed-point, wireless devices and cards are available to integrate with a VPN appliance making the utilization of wireless for backup or primary connectivity seamless and nearly transparent to end users.

Wireless will eventually replace the dial back-up redundant connection often used in broadband VPN solutions today, particularly in the retail sector. In addition to this logical progression, integrated wireless technology makes it more feasible and economic for business applications such as loss prevention surveillance/recording, temporary VPN network connectivity at construction locations, hospitality and promotional events, seasonal retail and services-sector applications. It is also useful in establishing rapid provisioned VPN connectivity in retail applications and temporary or promotional events, while land-line broadband facilities are being provisioned.

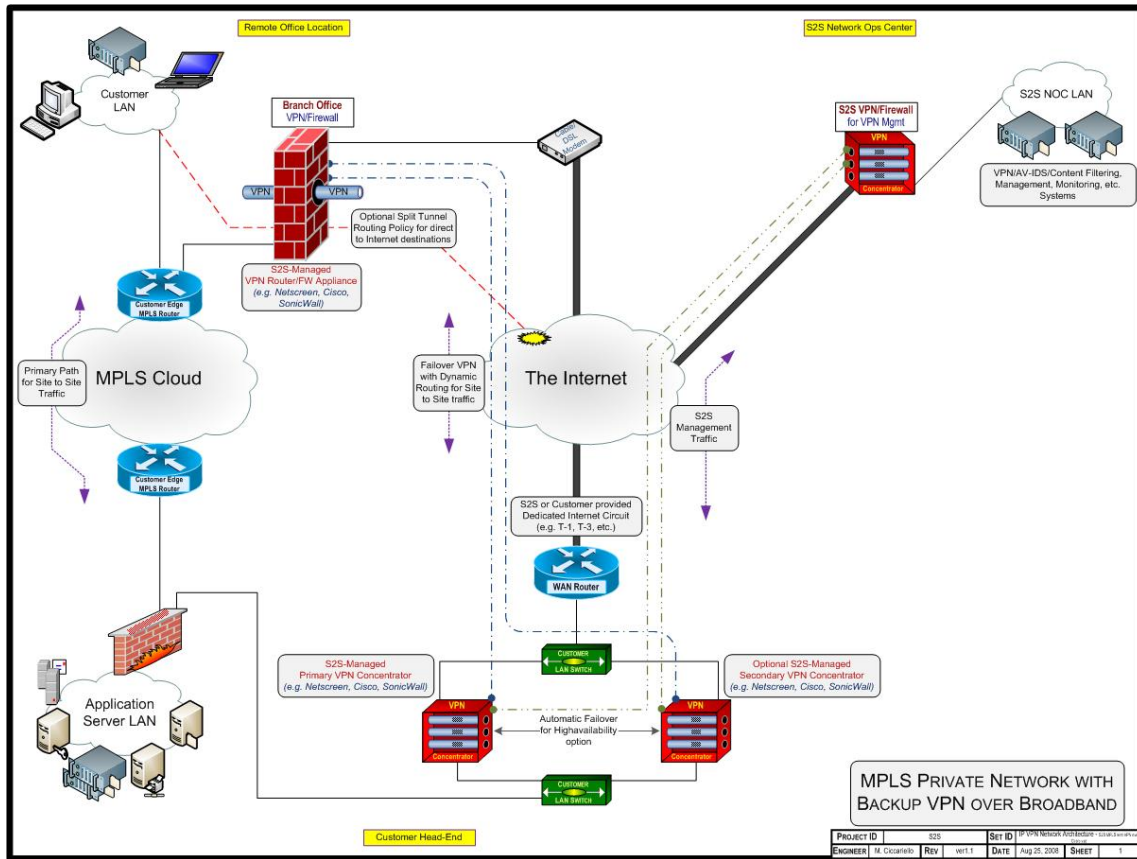
Finding a new Role in the Core Network

For organizations with larger and regional corporate offices and centers, there are performance, reliability and compliance guidelines that may drive the need for carrier-grade private wide area networks. Many corporations have already migrated from legacy private network solutions such as Frame Relay to the latest MPLS backbone services. While MPLS is a secure and efficient technology, two needs still arise. When using MPLS networks, one must still address redundancy. While the internal MPLS cloud is highly reliable, customer and provider devices can still fail. A backup solution is needed which has sufficient bandwidth and security to temporarily replace a high speed MPLS connection. An IPSec Tunnel over broadband addresses both these requirements. Think of it as “mission-critical networking”.

Another issue relates to the need for Internet traffic backhauling at the remote office. A private MPLS network does not provide direct Internet connectivity for the remote site. All Internet traffic must travel over the MPLS network to the corporate data center and traverse the corporation’s Internet access connections. Depending on the company’s web traffic demands, sending all Internet data over the MPLS, and out a shared Internet access pipe, may not be the most efficient option. If using an IP-VPN broadband backup solution, the remote sites will already have an Internet connection. The VPN/Firewall/Router device can be configured to create network policies allowing secure straight through Internet access for remote-site web traffic. This would allow bandwidth intensive web activity, such as streaming data applications and web collaboration tools, to be diverted from the MPLS backbone, while also providing a redundant solution for critical remote sites. Security policies can be enforced in the remote VPN appliance through the use of one or more mechanisms, including firewall rules, access control lists (ACLs) and web content filtering applications.

There are additional benefits and use cases that arise when having a secondary, high-speed broadband IP-VPN connection in place. Network engineers can configure their core WAN routers to route all or specific source/destination packets to either one of the two WAN interfaces. One technique is to route packets based on WAN interface metrics, such as latency, for example. Thus, if one interface incurs more latency than the other, traffic could be routed across the network with the lowest degree of latency. In this scenario, the traffic could be broken down to a particular application. Depending on the type of broadband circuit and specific provider package, the available bandwidth may even be greater than the core MPLS network at a given time. Routing techniques can be developed to optimize the use of the bandwidth through metric-based preferred route techniques.

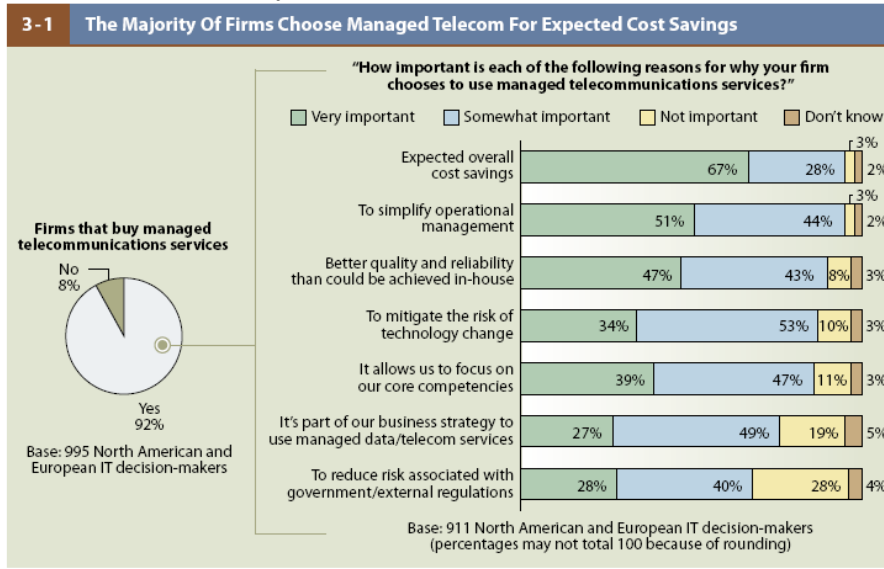
Redundant Architecture in the Core MPLS Network



Life Cycle Management: “Build vs. Buy”

Corporations consider a number of variables when making the decision whether to build and maintain their VPN network or to select a strategic partner that can turnkey both implementation and management of a solution and services. Although important criteria such as availability of resources, skills, and competing core initiatives are front and center in the decision making process, generally, many decisions are motivated by expected cost savings. A recent Forrester Research survey indicated that (95%) of the firms surveyed said expected cost savings are “important” in their decision to use managed telecom services, with 67% considering it to be “very important”. Other considerations that were very important to respondents included simplifying operational management (51%) and the need for better quality and reliability than could be achieved in-house (47%).

Forrester Research Survey Results



Broadband Provisioning-

IP-VPN implementations using broadband connectivity present another set of challenges outside of the network design and engineering aspects. Unless a corporation has ever had significant experience and expertise with circuit provisioning, consider finding a provider with considerable past experience. Bluntly put, provisioning broadband circuits to many locations with numerous providers can be a downright unpleasant process. There are many issues and exceptions that can and will occur, such as outside/inside wiring, installation coordination, installation failures and drop-outs due to line or physical entrance facility issues, and so forth. Provisioning efforts are best left to providers capable of managing the process end-to-end. Successful provisioning efforts are accomplished through project management excellence, focusing on vigilant tracking and exception handling of orders, frequent communication and elimination of surprises, to the extent possible.

Companies should also consider the challenge of managing the multiple broadband providers required to afford the level of overall coverage needed among the branch offices. As attractive as broadband is from a cost perspective, the complexity of managing dozens of broadband provider relationships diminishes the value of any cost savings and may lead to a higher total cost of ownership, after all the management costs are factored in. A service provider that can act as a manager and aggregator on behalf of the customer and oversee the installation and implementation from end-to-end allows the enterprise to realize the cost benefits of a broadband-based VPN solution without encountering the escalating operational overhead expenses as well as impact to Finance and A/P resources.

Do it Yourself (DIY) Taxonomy and TCO Exposed

An internally managed, CPE-based IP VPN is one of the earliest deployment models. IT Network managers deploy a dedicated VPN device at each location and manage the service themselves. The VPN device could be an integrated appliance, firewall or a router with VPN capabilities. Enterprises choose the hardware, install the system and manage every function. For a time, this was the only option for network managers. Today, enterprises choose this model when they have available resources, skills, expertise, operational core competencies and demand complete control of the environment. For most organizations, however, the challenges and costs of this approach quickly outweigh the benefits. The

most significant challenge for network managers is the overall complexity in managing the entire IP VPN life-cycle effort. It's expensive to deploy and configure all the devices, and the network manager is responsible for a long task list of operational requirements, including:

- Design/Engineering
- Sourcing (multiple vendors)
- Ordering equipment and services
- Internet access circuit provisioning
- Configuration management
- Implementation/installation
- Network and device monitoring and management
- Technical support
- ISP Broadband circuit trouble management
- Reporting
- Billing/metering
- Dispute resolution
- Cabling

On-going operational costs make up the largest area of spending when calculating the TCO of an IP VPN. According to Yankee Group research, IT organizations can expect to spend more than 9 hours per managed device per month on operational tasks, including support requirements of network, systems and security administrators and help desk staff. In addition, network managers need to worry about their equipment vendor possibly discontinuing support or investment for their equipment, spending additional money on network and security management software, as well as maintaining the necessary skills of their staff. In addition to the management headache associated with the equipment and service, the IT organization must manage its ISPs. In all likelihood, the various branch offices combined may use dozens of different broadband suppliers. Prices and service levels can vary considerably. It also means billing issues and the inability to negotiate lower rates and volume discounts. For many organizations, the operational burden of the equipment and access services make an internally managed solution the least attractive option for secure, reliable branch access.

CPE-Based DIY IP VPN Operational Requirements

Source: Yankee Group

Operational Requirement	Hours per Month per Device
Network/Systems Administrator Support Requirements	6.40
Security Administration Support Requirements	2.00
Help Desk/Billing Support Requirements	0.64

Managed IP-VPN as a Service

Organizations seeking to optimize all relevant factors should choose a CPE-based managed broadband IP VPN service. A broadband-based service can bring many of the benefits of a do-it-yourself (DIY), CPE-based VPN deployment without the management burden and capital expense. A service provider

deploys a dedicated VPN appliance at each branch office and manages everything from installation to ongoing monitoring and support. This enables the enterprise to turn sites on quickly and easily. In addition, the service provider can order and provision the broadband access. This offers a tremendous benefit to the organization; it receives one bill for the services. By using a broadband-based managed VPN service, the cost is much lower and the organization can focus on business issues rather than focusing on many of the management headaches that come with managing multiple carrier networks and the day-to-day management of equipment. The IT department can focus on more valuable contributions and strategic initiatives. Other major benefits include:

- **Centralized policy control and management:** Network managers receive the benefit of a distributed, flexible solution while at the same time being able to centrally manage security and access policies for their entire organization.
- **Operational cost savings:** Network management is much simpler, and there are vastly reduced support costs.
- **Capital cost savings:** In many cases, the service provider owns and manages the equipment. There are no asset-related expenses.
- **Scalability:** Network managers can quickly provision new sites. Since it is a managed offering, it can scale quickly, leveraging ubiquitous broadband access and the expertise of the service provider.
- **Better value:** Services costs less and deliver high-speed, secure connectivity to every branch location.

Distributed organizations with many branch offices can capture the benefits of both the internally managed CPE-based approach and the network-based approach with this solution. It also addresses the major challenges of each. In particular, it centralizes the purchase and support of the VPN equipment and the aggregation of broadband services. It delivers reliable, secure branch location access at a much lower cost (see table below).

CPE-Based DIY IP VPN vs. Broadband-Based Managed IP VPN

Source: Yankee Group

<i>Operational Support Category</i>	<i>DIY CPE-Based Approach</i>	<i>Broadband-Based Managed IP VPN</i>
<i>Network/Systems Administrator Monthly Support Requirements per Device (in Hours)</i>	6.0	0.0
<i>System Administration Monthly Support Requirements per Device (in Hours)</i>	2.0	0.0
<i>Help Desk/Billing Monthly Support Requirements per Device (in Hours)</i>	0.5	0.0
<i>Total Support Hours per Month</i>	9	0
<i>Number of Sites</i>	100	100
<i>Total Required Support Hours</i>	850	0
<i>Average Hourly Salary per Support Person</i>	\$40	\$40
<i>Managed Device Monthly Service Fee</i>	-	\$50
<i>Monthly Support Costs</i>	34,000	\$5,000

The importance of secure access to corporate information from branch locations cannot be overemphasized. Today's networked organizations rely on their branches to reach customers, enhance

service levels and generate revenue. Network managers are responsible for delivering new, productivity-enhancing applications to every user in the organization's value chain. How well enterprises accomplish these goals can be the difference between success and failure, being a market leader, or falling behind competitively. A broadband-based managed IP VPN service can meet many of the network challenges that distributed organizations face and reduce costs at the same time. It can help companies transform how they communicate and share information, while simultaneously reducing IT operational costs. It's a network service that truly delivers value for each dollar spent.

What to Look for in a Provider

Proven experience and operational support excellence are essential hallmarks of a managed service provider. Look for a provider who pays attention to the details and asks a lot of questions and is not ready to hand you a proposal after the first call or meeting. Providers demonstrate their experience and subject matter expertise through knowledge they are able to convey during conversations and meetings with the corporate IT network team. They will drill down to the detail in virtually every facet of their service and the overall project, while exuding an overall sense of credibility and genuine concern for your business problem. Experienced providers know the right questions to ask, focus on solving business problems, have broad-based knowledge about business systems and applications, and work collaboratively with a customer during up-front engagements and through requirements discovery.

You'll want to gain comfort that the provider is a strategic partner and extension of the IT organization. They should be very "high touch" in all life-cycle aspects and continually strive to bring the highest level of customer experience possible. There are a number of providers outside of the carrier community who are extremely experienced and savvy with IP-VPN services. A number of these providers were early pioneers in developing, delivering and managing VPN services. The carriers had to play a catch-up game as they were losing considerable business from customers who migrated from Frame Relay to broadband IP-VPN. The following are attributes to look for in a managed solution provider:

- High degree of broadband aggregation (DSL, Cable, Wireless), not tied to a one-network footprint
- Mass circuit provisioning expertise
- Experience with customers in diverse vertical sectors (retail, entertainment, automotive, insurance, etc.)
- Turn key-solution: providing the life-cycle components as a service and ability to bundle major components (e.g., hardware) into a recurring charge model
- Consolidated billing: aggregation of all underlying suppliers into a single monthly invoice to the customer
- Proactive Monitoring and Management: 24x7 help desk staffed with seasoned domain experts in broadband-based solutions
- On-line portal for dashboard network performance, trouble ticketing and move/add/change/disconnect (MACD)
- Flexible SLA - circuit provisioning, MTTR, chronic condition, network performance, etc
- Multiple service entitlements packages
- Support for industry leading VPN appliances
- Single point of contact for all network issues (connectivity, configurations, MACD).
- Very high-touch approach to project/customer relationship management
- Proven experience, recognized by industry analysts and customer references

Reference and Research Material

- 1- The Yankee Group, Enterprise Computing & Networking, Zeus Kerravala February 2005. Titled "Managed Broadband VPN Services Are a Low-Cost Alternative for Networking Distributed Enterprises".
- 2- Missing Link Security Services, LLC, a Whitepaper by Mark Bouchard July 2006. Titled "Meeting Branch Office Business Needs for Security and Networking."
- 3- Missing Link Security Services, LLC, a Whitepaper by Mark Bouchard August 2006. Titled "Meeting Network and Security Needs for Distributed Sites in the Retail Industry."
- 4- Cisco Systems, a Whitepaper, copyright materials 1992-2004. Titled "ENTERPRISE GUIDE FOR SELECTING AN IP VPN ARCHITECTURE-COMPARING MPLS, IPSEC, AND SSL".
- 5- Forrester Research, Business Data Services North America and Europe, Ellen Daley June 2008. Titled "The State Of Enterprise Networks and Telecommunications: 2008".
- 6- Forrester Research, "Business Technographics® March 2006 North American and European Enterprise Network and Telecommunications Survey"