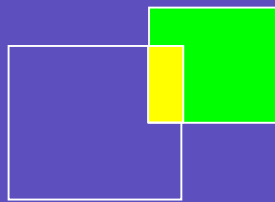




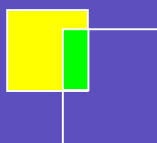
March 28, 2002



**Colorado Office**  
1317 Cherry Street  
Denver, CO 80220  
303.355.1982

**Oklahoma Office**  
1307 South Boulder Avenue  
Suite 120  
Tulsa, OK 74119  
918.382.0007

**Texas Office**  
2208 Columbia Drive  
Flower Mound, TX 75028  
972.874.7791



# Building the Business Case For IP VPNs

Prepared for:



The Strategic Catalyst™  
**TeleChoice**  
for the Telecom Industry

## The Business Case for IP VPNs

In these times of cost control consciousness yet exploding demand for the support of IP applications, a growing number of enterprises find the ongoing adaptation of their legacy infrastructures an increasingly painful experience. While such networks—frame relay, private line, etc.—have proved to be successful over the years as reliable transport, in today's increasingly networked economy the cost structure and scalability limitations force enterprises to consider alternatives.

Rising to the top as the alternative to today's legacy infrastructure, IP networks address the ongoing networking needs of the enterprise. However, native IP is often not acceptable. Whether delivered across the Internet, broadband access, or a private carrier IP network, many businesses require that the transport be secured in this open environment. It is the IP VPN that has been tagged by the industry and early enterprise adopters as the mechanism for layering transport security upon the network. This paper provides a high-level examination of both the qualitative networking benefits as well as the financial business case associated with making a transition to an IP VPN.

### New Networking Requirements

Until more recently, the methods for supporting enterprise data networking requirements largely consisted of legacy technologies such as private line and frame relay. Services built on these technologies have their advantages as well as challenges as shown in the following table:

Technology	Advantages	Challenges
<b>Private Line</b>	Dedicated circuits provide greatest degree of enterprise control, best quality of service, and high level of security.	<p>Most costly alternative.</p> <p>Difficult to scale, requires dedicated circuit for each site-site pair.</p> <p>Difficult to manage, especially as network complexity increases.</p>
<b>Frame Relay</b>	<p>Enterprises leverage the virtual nature of Frame Relay to provision their networks more easily and at a lower cost than private line networks.</p> <p>Even though a public infrastructure, traffic is isolated. Enterprises perceive it as secure and reliable.</p>	<p>Though less costly than private line, it is still more costly than IP networks.</p> <p>Does not scale well and difficult to manage Permanent Virtual Circuits (PVCs).</p> <p>Single-carrier network architecture susceptible to outages.</p> <p>Connectivity challenges to external entities either for Extranets or basic Internet access.</p>

Enterprises leveraging data networks based on these technologies find that the disadvantages can be a real hindrance in keeping up with current trends impacting the industry:

- **Cost Pressures.** A pervasive need exists in every sector of the economy for enterprises to reduce costs, improve efficiency, and increase performance.
- **Abundant, Relatively Cheap Bandwidth.** There is a growing supply of lower-priced bandwidth, such as broadband Internet access through DSL and/or Cable.
- **Increased Deployment of IP-based Software Applications.** Whether client server- or Web browser-based, business-critical applications such as ERP and CRM are moving to an IP-based model. Enterprises increasingly place importance on even basic applications such as email and web browsing.
- **Growth of Internetworking between Enterprises.** Business-to-business e-commerce and e-business are becoming a tactical necessity and not just a strategic differentiator.

With such challenges and trends impacting the legacy environment, many enterprises will look to a new solution: The IP VPN.

## The IP VPN Solution

An IP VPN consists of a layer of security, traffic segregation, and control imposed on a public IP network to create a data network that is, in effect, private. IP VPNs may be end-to-end with Customer Premise Equipment (CPE)-based IPsec or SSL encryption solutions, or they may be delivered from the service provider's network using MPLS and/or again IPsec at Layer 2 or Layer 3. Hybrid solutions can also exist wherein some sites leverage a network-based solution and other sites leverage CPE for end-to-end encryption or an on-premise firewall where required. Many options exist, each with various strengths and weaknesses that allow the enterprise to align a solution with its specific needs and requirements. Currently, however, the vast majority of IP VPN deployment is accomplished via CPE and is the implementation methodology that is the focus here.

## Why Traffic Needs to Be Secure

Legacy networks have traditionally been perceived as secure, but the degree to which they are truly or highly secure is open for debate. Examples include attacks on the last mile such as physical wire-tapping or the potential for inadvertent, inaccurate provisioning by a service provider's network technician—directing circuits to the wrong location. Also, the potential for social engineering attacks always exists (e.g., an individual with malicious intent providing forged credentials to enter a provider Point of Presence).

Such are the possibilities within the “closed” legacy networking world, but by its very nature the IP world is typically “open,” adding to the list of concerns and increasing the security requirements for many enterprises. Traffic traversing the public network can encounter potentially harmful events along the way from where it originates to where it terminates. For many enterprises, additional security precautions may also be required—even when using single-carrier private IP networks. As an example, some industries are becoming regulated in the way of information confidentiality, which many enterprises interpret as a need for end-to-end encryption.

## How Are IP VPNs Secure?

The majority of CPE-based IP VPNs draws upon the IP Security (IPsec) standards for encryption and tunneling. IPsec tunnels establish a secure connection between endpoints while encryption encodes packets to ensure confidentiality of data in transit. IP VPNs generally involve firewalls at the enterprise’s perimeter networks to protect internal LANs, applications, and services from unwanted and/or malicious traffic or users. Furthermore, IP VPNs leverage authentication techniques to validate the identity of users/hosts on the network based on access rights and lists controlled by the network manager.

## What’s in It for the Enterprise?

Many obvious benefits to IP both drive and respond to the networking trends outlined earlier. IP VPNs allow the enterprise to leverage these benefits but in a more secure manner. Specifically, IP networks benefit the enterprise through:

- **Any-to-Any Connectivity.** IP was designed for simplified, ubiquitous connectivity between all locations on a network. Enterprises can connect remote and central locations via site-to-site VPNs or remote dial networking. IP allows routing of traffic between sites simply, and IP VPNs secure this traffic. This also applies to connecting with external entities.
- **New Application Enablement.** IP enables the creation of software applications for transmission of data. New applications have emerged or increased deployment, such as email, instant messaging, and web browsing. Additionally, IP provides a mechanism for new multimedia applications, such as voice communication, streaming media, and content distribution/delivery.
- **Flexibility in Network Design.** Enterprises can transition their networks from the traditional central hub-and-spoke design to a more meshed topology for more peer-to-peer applications.

## The Economic Benefits of IP VPNs: A Closer Look

Enterprises that harness the power of IP networks can position themselves for greater revenue opportunities through areas such as e-commerce/e-business. However, cost savings are potentially an even greater factor and motivator for enterprise adoption of IP VPNs in today's economic environment. Not every enterprise's business model is conducive to driving additional revenue from e-business, but virtually all can realize cost reductions and efficiencies, some of which are listed below:

- **Bandwidth Savings.** The specific per site savings from a bandwidth perspective will vary depending upon implementation options such as carrier-managed solutions versus a Do-It-Yourself (DIY) approach and public Internet-based transport versus private IP carrier infrastructure.
  - ✓ *Lower Site-to-Site Connection Charges.* In the legacy world, the connection between each site requires a dedicated circuit or PVC. IP networks avoid these costly connections by providing access to the entire network at one site for one price. In addition, IP connectivity when compared to legacy connectivity at the equivalent speed is typically priced much more aggressively by service providers.
  - ✓ *Remote Dial Savings.* DIY remote access solutions have been cumbersome to maintain and highly costly in telecom charges. Moving from domestic and international long distance toll charges, 1-800, and calling cards to flat rate or usage-based VPN utilizing nationwide local access numbers can reduce cost per user from 30% to 70%.
  - ✓ *Access Convergence.* Combining Internet and internal traffic on a single network connection reduces complexity and the cost of managing multiple connections. Multi-service networks using converged voice and data will further reduce bandwidth costs.
- **Operational Cost Reduction.** Adding a new site to an IP VPN can be less costly than adding a legacy network location. For each new legacy site, one or multiple PVCs are also required for connectivity, which means added bandwidth provisioning expense and ongoing monthly expenses.

Additionally, enterprises migrating to an IP VPN may potentially realize "soft-cost" savings in areas such as:

- **The Addition of a New Site.** Adding a new site to an IP VPN can require less time to provision and set up compared to a legacy solution.
- **Reducing Management Time.** This would be reducing the management time associated with moves, adds, or changes with, for example, PVCs. Managing IPsec tunnels can be a similar task, but many vendors offer network management tools that greatly facilitate provisioning a partially meshed or fully meshed network through a graphic interface.

- **Interconnecting with External Parties.** Enterprises connecting with business partners or customers can find shorter provisioning time and more flexibility in connecting multiple sites with an IP VPN than by legacy services. Additionally, in the Frame Relay world this would usually require that both parties subscribe to the same carrier. Through the flexibility of IP VPNs, each party can select its own provider of choice.

## The Cost of Migration

Despite the comparative cost savings of IP VPNs, enterprises currently using legacy infrastructure will incur costs associated with migration. Some of the anticipated costs are depicted in the following table:

Cost Element	Description
<b>Security Equipment</b>	Any new equipment required to support the IP VPN. These costs may vary based on vendor solutions (i.e., software solutions on server platforms, integrated appliance and/or security systems, the number of such systems, etc.)  Additional devices may be desired for redundancy at critical locations.
<b>Installation and Configuration</b>	Labor expense related to physically installing the network devices, the network access links/related equipment, as well as the creation of security policies and configuring the security solution to support these policies.
<b>Network Management</b>	Changes to an existing network management system may be required, including the addition of element management tools required to control the CPE devices. The DIY enterprise would purchase these items while an enterprise outsourcing network management would incur additional monthly recurring charges.
<b>VPN Expertise on Staff</b>	The DIY enterprise will incur costs related to finding, hiring, training, and retaining employees with network security expertise.
<b>Service Charges for Parallel Networks</b>	Enterprises that do not switch their network all at once will have overlap of legacy and IP infrastructure to maintain connectivity for sites that have not migrated. Some may leave the legacy network in place for several months as an emergency backup.

## Frame to IP VPN Migration Scenarios

To provide some context to the economic potential of IP VPNs, the following section analyzes two example scenarios. Scenario A is an apples-to-apples comparison of moving to IP at equivalent bandwidth levels to the legacy network while Scenario B represents migration to greater levels of bandwidth at remote locations.

	Legacy Network	IP Network	Change
<b>Scenario A: Direct One-to-One Comparison</b>			
Small Site Bandwidth (8 sites)	56-64 Kbps	56-64 Kbps	No Change
Monthly Cost/Site	\$280	\$75	Save \$205
Medium Site Bandwidth (2 sites)	384 Kbps	384 Kbps	No Change
Monthly Cost/Site	\$1,150	\$190	Save \$960
Central Site Bandwidth (1 site)	T-1	T-1	No Change
Monthly Cost/Site	\$3,275	\$1,570	Save \$1,705
<b>Total Annual Costs</b>	<b>\$93,780</b>	<b>\$30,600</b>	<b>Save \$63,180</b>
Time to pay back initial hardware investment (\$6,000 to \$10,000): 1.1 – 1.9 Months			

In this direct comparison, the costs of IP VPN represent roughly one-third of those of the legacy network. This example does not include network management, installation expense, time to migrate multiple networks, etc. The initial hardware purchase is based on average pricing for NetScreen appliances while the bandwidth rates are based on averages derived from multiple carrier offerings.

In what is proving to be a likely scenario, enterprises will increase their bandwidth per location as they migrate to lower-cost bandwidth services (such as DSL), as outlined below:

	Legacy Network	IP Network	Change
<b>Scenario B: More Bandwidth for Incrementally Less</b>			
Small Site Bandwidth (8 sites)	56-64 Kbps	384 Kbps	320 Kbps
Monthly Cost/Site	\$280	\$190	Save \$90
Medium Site Bandwidth (2 sites)	384 Kbps	512 Kbps	128 Kbps
Monthly Cost/Site	\$1,150	\$235	Save \$960
Central Site Bandwidth (1 site)	T-1	FT-3 (3-6 Mbps)	1.5–4.5 Mbps
Monthly Cost/Site	\$3,275	\$5,574	Add (\$2,299)
<b>Total Annual Costs</b>	<b>\$93,780</b>	<b>\$90,768</b>	<b>Save \$3,012</b>
Time to pay back initial hardware investment (\$6,000 to \$10,000): 23 – 39 Months			

Again, the initial hardware investment is based on average pricing for NetScreen security appliances while the bandwidth rates are based on averages derived from multiple carrier offerings.

In this “apples-to-oranges” scenario, the enterprise saves a modest amount and takes longer to pay back the initial investment. However, this calculation does not include the potential upside of soft cost savings (noted above), as well as the fact that the enterprise enjoys more bandwidth at each location for roughly the same price it paid for frame relay services. With this additional bandwidth, the enterprise may deploy more robust applications and allow more users to have concurrent access—benefits that the 64 Kbps network most likely could not support. Plus, the recurring cost of IP networks would be much less than that of upgrading the frame relay network to these higher speeds.

Although the two scenarios resulted in annual savings, not all enterprises will achieve cost savings when migrating to an IP VPN. Network configuration, equipment choices, bandwidth requirements, and geographic considerations among others will also have an impact on the bottom-line analysis. However, even in scenarios where hard cost savings are not realized or only realized to a small degree, the qualitative benefits of an IP VPN as discussed previously may more than make up for the added cost.

## Summary

IP VPNs provide enterprises a secure, flexible, and generally cost-effective means of leveraging IP networks for their business communication requirements. Cost savings may be obtained from reduced bandwidth charges and operational efficiencies to “soft” costs associated with shorter provisioning times, reduced management expenses, and internetworking with business partners.

When considering migration options, it is important to make an apples-to-apples comparison for one-to-one cost analysis, as well as an apples-to-oranges view to determine what additional functionality can be added and, in most cases, for incrementally less cost. It is also important to keep in mind those business benefits of an IP VPN that cannot generally be reflected in a hard numbers analysis.