Building Remote Access VPNs

124 Grove Street, Suite 309
Franklin, MA 02038
877-4-ALTIGA
www.altiga.com

Building Remote Access VPNs: Harnessing the Power of the Internet to Reduce Costs and Boost Performance

Executive Summary

One of the most important trends in enterprise networking is the development of Virtual Private Networks (VPNs). VPNs can be particularly effective in providing remote access to corporate resources for business travelers, telecommuters and remote offices.

The implementation of a VPN will bring substantial cost savings over conventional solutions – up to 60% according to a 1996 Forrester Research Study. Unlike conventional remote access solutions, a VPN can leverage high speed Internet access technologies (cable modems and DSL technologies) to dramatically increase performance. Given the magnitude of these benefits, implementing a remote access VPN should be among the highest priorities for an enterprise network.

For networks with hundreds or thousands of remote users, first generation VPN servers do not provide the required scale and performance. Altiga's VPN Concentrator overcomes these limitations. The first of a new generation of broadband access servers, the Altiga solution meets the full range of VPN requirements, not only for remote access, but for business partner Extranets and other VPN applications as well.

The Altiga VPN Concentrator incorporates many design features to minimize operating costs. Features such as powerful management tools, a scaleable architecture and robust platform characteristics. The Altiga VPN Concentrator is also fully compatible with the built-in VPN capabilities of the Microsoft desktop, and requires no changes to router or authentication server configurations. The Altiga VPN Concentrator is simple to deploy.

Introduction: Using the Internet for Private Networking

The Internet is transforming enterprise networking. With its ubiquitous availability, high performance and low cost, it is creating a wealth of opportunities to operate more effectively and efficiently, and gain a competitive advantage. The most successful enterprises will be those that most effectively harness the power of the Internet.

One opportunity the Internet brings is to replace traditional private wide-area networks with Virtual Private Networks ('VPNs'). A VPN is simply defined as a service that gives its users the appearance that they are connected directly to their private network, when in fact they are connected using the public Internet. One element of the enterprise network for which the VPN approach is particularly attractive is remote access. A remote access VPN not only reduces costs associated with existing systems, it also boosts overall performance dramatically.

VPN's are built using two technologies, tunneling and encryption. Tunneling provides the ability to extend the reach of private networks to remote locations over public shared networks in a controllable fashion. Almost any application that can be run over a private line can be run through a VPN tunnel. There are several tunneling protocols in use, with the most prevalent being PPTP ('Point-to-point tunneling protocol) and L2TP ('Layer two tunneling protocol).

Encryption ensures data privacy by allowing data to be decrypted and read by only the intended recipients. The most common encryption methods are RC4, used in Windows95, and DES and triple DES, which are used by the IPSec suite of protocols. RC4, while relatively lightweight, provides protection against all but the most professional code-breakers; used over the Internet it provides considerably more security that transmitting clear data over (supposedly) private lines. DES and triple DES are the techniques used for themost sensitive commercial information.

The Growth of Remote Access

Over the past ten years, remote access has been one of the fastest growing areas of enterprise networking. The primary application is to provide seamless access to corporate resources for remote offices, business travelers, and the rapidly growing legions of telecommuters. The goal of a remote access system is to create a virtual workplace where all information workers have access to the same tools and services, and to each other, irrespective of their geographical location. Enterprises benefit through reducing travel cost and time, saving on facility costs, increased productivity and increased employee satisfaction.

Today, remote access systems are implemented using the telephone network. A typical configuration is shown in figure 1. Each remote PC is equipped with a modem, which it uses to connect via the telephone network to a remote access server on the enterprise LAN. When connected, the remote user can access the same applications as the directly connected user.

Traditional Remote Access and Remote Office Connection to Their Enterprise

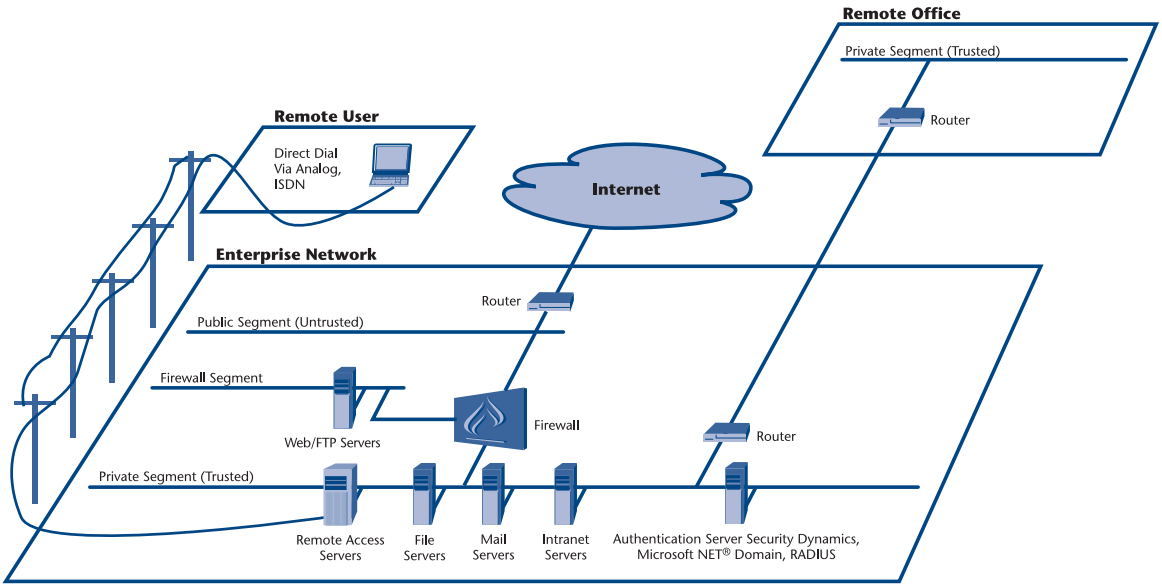

Figure 1

For all its benefits, current remote access implementations have two major limitations. First, the cost per user can be unacceptably high, with long distance charges being a major (and in some case the dominant) component. Second, access speeds over the telephone network are limited to maximum of 56Kbps, the fastest speed at which dial modems can operate.

Remote Access in the Internet Age

The Internet now brings the opportunity to overcome these limitations by implementing a remote access VPN. According a recent Forrester Research study, implementing a remote access VPN will save a typical enterprise up to 60% in telecommunications charges. The savings arise because, in all but the smallest implementation, remote access users are dispersed over a number of local calling areas. Most remote users without a VPN incur long distance charges whenever they connect. A remote user who connects for just half an hour each day will create around $60 per month in long distance charges alone, and a telecommuter connected for four hours daily will incur $480 per month in long distance charges.

In the case of a remote access VPN, however, these long distance charges are replaced by the Internet access charge, typically less than $20 per month whether used for half an hour per day, four hours per day or much more. Since the Internet access connection is usually local to the user, the telephone network charges will be covered by the flat rate local telephone tariff, which must be paid in any case.

In addition to these dramatic cost savings, remote access VPNs will bring major performance improvements. While modem speeds have more than doubled in recent years, most remote access users will testify that, even with the latest generation of 56Kbps modems, performance leaves much to be desired. In practice only applications with relatively low communications demands can be used effectively. Downloading any document with graphic content such as PowerPoint presentations, faxes and scanned documents can be frustratingly slow. Even the simplest networked application designed for local use can be very slow when accessed remotely.

The limited access speed of dial-up remote access implementations limits the number of workers who can successfully telecommute, and negatively impacts the productivity of those that do. Moreover, as application demands increase, these ‘traditional’ remote access systems have no growth potential.

However, remote access VPNs provide the opportunity for increasing numbers of remote users to take advantage of much higher performance Internet access mechanisms: cable modems and DSL (‘Digital Subscriber Link’). These access methods, which are rapidly increasing in availability, provide performance of up to 20 times the maximum 56 Kbps of the phone network. As they become available, these new access methods are typically very attractively priced with list prices of $40-100 per month.

According to Virginia Brooks of the Aberdeen Group “High speed access to remote access VPNs will transform the virtual workplace, giving the remote user capabilities virtually identical to his local colleague. Companies will gain big savings and productivity benefits from exploiting this potential.” It is important to note that there is no way for traditional remote access systems to utilize these new access techniques: a remote access VPN is the only choice.

Building a Remote Access VPN

A VPN configured for remote access is illustrated in figure 2. The two key components that differ from the traditional remote access implementation are the VPN software resident on the remote PC, and the VPN access server on the enterprise network. The authentication server can remain identical to that used for dial access.

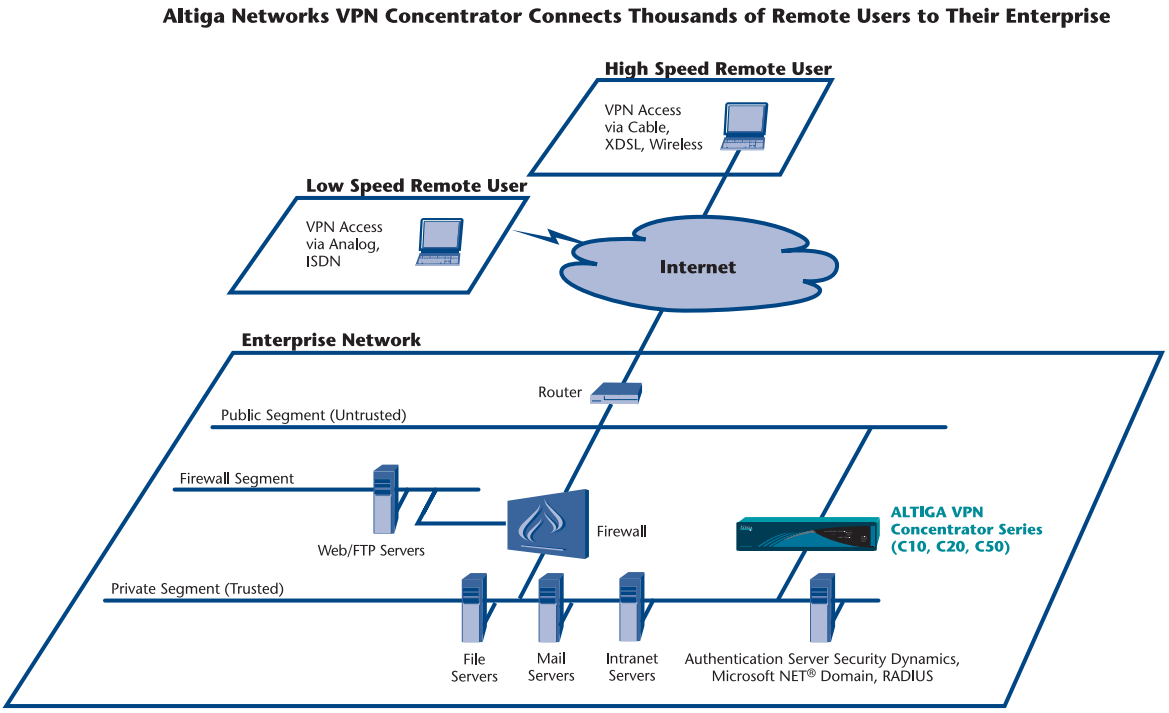

Figure 2

Increasing access speed is only a matter of obtaining a DSL or cable modem local loop from the local telephone company, Internet service provider or cable company. While high-speed access has only recently been introduced, availability is growing fast, and one or several access techniques will ultimately be available to virtually every urban and suburban business and residence.

The Remote Access Client

Today, there are competing standards and protocols for establishing secure tunnels over the Internet. Many of the solutions available today rely on proprietary client software. This issue is evolving in much the same way as direct dial remote access. At first, vendor specific PPP client software was necessary. Eventually this functionality was incorporated into popular desktop operating systems, e.g. Microsoft Dial Up Networking, Microsoft NT RAS and AppleTalk Remote Access for Macintosh. This advancement effectively removed the deployment ceiling for corporate remote access programs.

Even now, Windows 95, Windows 98, and Windows NT users can enjoy the benefits of integrated VPN client software using the Point-to-Point Tunneling Protocol (PPTP). However, for full functionality including IPSec, the most significant development in this area will be the release of Microsoft NT 5.0. Altiga's VPN Concentrator supports all standard protocols, allowing customers to preserve their hardware investment as deployment configurations change with time.

For customers who want to bridge the gap between integrated PPTP and IPSec, Altiga provides simple to use client software for unlimited distribution within a corporation. Our design criteria were ease of use and security. With this software, Altiga customers can deploy IPSec today and move to an integrated client as operating system support becomes available.

The Remote Access Server

Unlike the client, which operates a single tunnel, the central site server in a VPN has to concurrently operate hundreds or thousands of tunnels, with the associated challenges of performance and management. VPN access servers can be classified based on the number and type of remote connections they can support. Until recently, two types of access server have been available:

The VPN router is a router with the addition of tunneling and encryption support. While this type of server can be implemented without adding hardware, only a limited number of VPN connections can be supported, so it is rarely applicable to remote access applications, which require hundreds or thousands of connections. A typical application for a VPN router is to interconnect a limited number of remote offices, or to provide VPN connections to a small number of third-party networks (known as Extranets).

The VPN switch is the first generation of dedicated VPN access server that can support hundreds of VPN connections, and is therefore suitable for remote access applications. The limitation of VPN switches is that they are software based, and are limited in the sustained throughput they can support. This throughput limitation will increasingly restrict VPN Switches to small implementations as high-speed access becomes more widespread

Enter the VPN Concentrator

Advances in broadband access technology have made possible a new generation of VPN access server, the VPN concentrator. This new class is designed for large-scale operations with performance and scalability to support the hundreds or thousands of users that enterprise systems will grow to as they transition from VPN pilots to full deployment. The VPN concentrator meets the performance demands of encrypting very large numbers of users by using hardware assist for encryption processing.

As networks upgrade remote users to high speed access using cable modem or DSL access, the access server is a potential weak link. But with its ability to encrypt a broadband link at wire speed, the VPN concentrator has the performance to meet this added demand. It can provide this capability with a heterogeneous mix of connections from modem speeds to 1.5 Mbps bursts, accommodating concurrent remote clients, business partner Extranet connections and other VPN links. A comparison of the VPN concentrator with other types of access servers is given in figure 3.

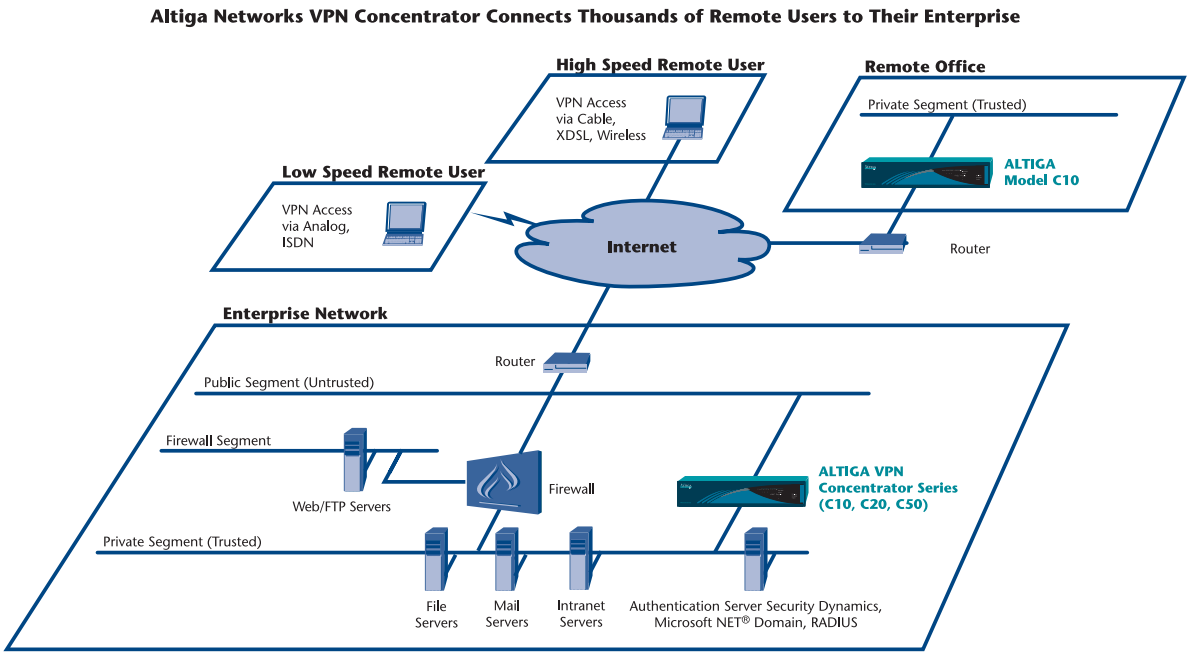

Figure 3

The first of this new generation is the VPN Concentrator from Altiga Networks. As the first true enterprise-class VPN concentrator, it provides all of the benefits of the first generation of software-based servers, but provides an unprecedented level of performance, scalability and service availability, while minimizing operating costs.

VPN Concentrator Functionality

The Altiga VPN Concentrator provides all of the capabilities required for an enterprise-class remote access VPN, while minimizing operational and administrative costs.

The VPN Concentrator supports all of the VPN tunneling and security options in the current generation of Microsoft desktop. These include PPTP and PPTP with encryption for compatibility with Windows95, Windows98 and NT 4.0, and IPSec and L2TP for compatibility with NT 5.0. Altiga is committed to maintaining full compatibility as Microsoft expands or enhances its capabilities, a commitment that is underwritten by Altiga's status as a Microsoft development partner.

Most enterprises will elect to use a dedicated authentication server. There are several available that provide varying compromises between the degree of security provided and the level of administration and user effort required to use them. The most common forms in use today are the RADIUS server and Security Dynamics' two-factor authentication , the latter providing users with smartcards as physical tokens of their identity. In the future, Microsoft's NT Domain authentication server and Microsoft's Active Directory Services are likely to gain in popularity, as they are already viewed as the emerging system for Microsoft shops. Altiga's VPN Concentrator is compatible with all of these options, and also includes an integral RADIUS server for those users that prefer not to use a separate server. In a RADIUS environment, a database of authorized users and their authentication information is held in a file server referred to as a RADIUS server. The Altiga VPN Concentrator notifies the RADIUS server when a remote user attempts to connect to the network to authenticate their identity and authorization. Two-factor authentication servers can also be accessed via the RADIUS protocol

In terms of performance, Altiga's VPN Concentrator greatly exceeds the performance of the first generation of VPN servers it supercedes. Leveraging unique hardware-assisted encryption modules, the VPN Concentrator supports up to 5,000 concurrent users, with an aggregate throughput of 50 Mbps. It is important to note that this capacity is achieved with all users employing encryption, because encryption is extremely processor intensive, and is the predominant user of system performance in a VPN access server. This performance represents at least a tenfold increase over the performance of first generation access servers.

With most networks experiencing growth in both user numbers and access speeds, scalability is an important consideration. The VPN Access Server addresses this need by implementing the encryption engine – the key determinant of system performance – in the form of field-upgradable modules. Each VPN Concentrator can support up to four modules. The system can be installed with a single module, with additional modules added as the number of users or access speeds increase. This architecture is illustrated in figure 4.

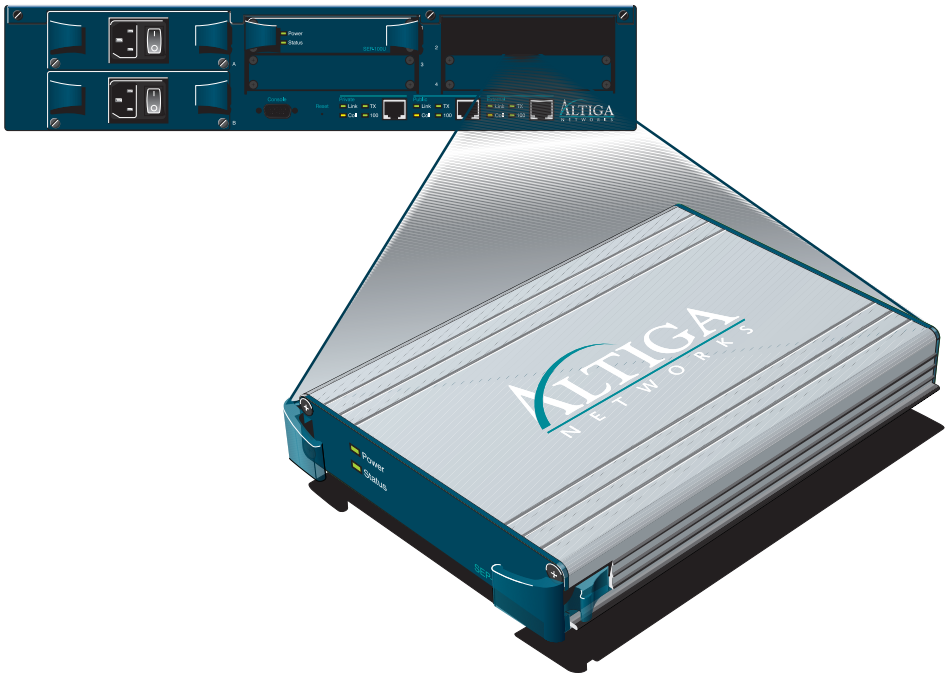

Figure 4

With increasing numbers of workers dependent on remote access, reliability has never been more important. Unlike many first-generation access servers that were built on PC platforms, the Altiga VPN Concentrator utilizes a purpose-designed platform to deliver carrier-class reliability, with easy maintenance and redundant power. From its inception, Altiga's VPN Concentrator was architected to solve the unique access requirements of both the remote user and the remote office, while allowing users to expand support as access needs grow.

Implementing a VPN with Altiga

With an average of 35% of remote access costs accounted for by network administration, a major focus in the design of the VPN Concentrator has been in minimizing operating costs.

The VPN Concentrator can be added to the existing enterprise network infrastructure as easily as adding a new host. No changes are required to existing router tables or firewall configuration. Because it works with a wide range of authentication servers, migration from dial-up remote access to remote access VPN can be made with no change to the authentication server.

Best of all, because the VPN Concentrator is designed for use with VPN facilities already integrated in Windows, client issues in deployment are limited to reconfiguring the dialer.

When the VPN Concentrator is installed, no configuration is required for remote users. Security profiles are learned from the authentication server, tunneling protocols are recognized automatically and supported in any mix, and data streams are automatically assigned to processing modules.

Management focuses on monitoring network utilization and performance. Beyond tracking critical parameters such as the number of active users, CPU utilization and throughput, Altiga's VPN Concentrator also provides unique compartmentalized management, allowing management pieces to be assigned to different people or groups. To simplify the management of a large network, the Altiga Monitoring System (AMS) simultaneously monitors multiple VPN Concentrators, using Java applets to provide 24x7 SNMP monitoring, historical analysis, capacity monitoring and alarms on key variables. The management visibility provided by this application is illustrated in figure 5

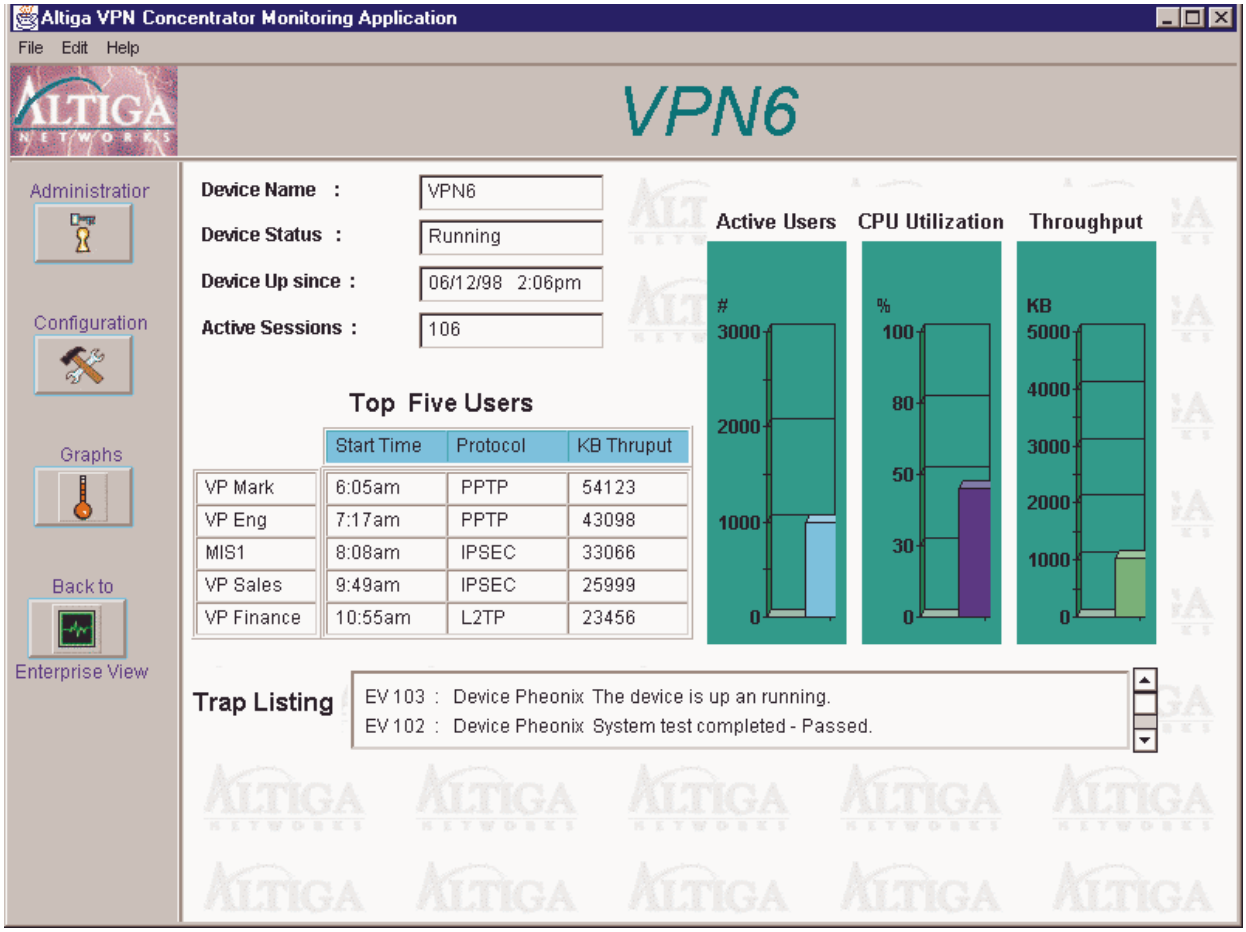

Figure 5

Standard access for both provisioning and monitoring is achieved via an HTML interface, while the system also provides full compatibility with SNMP enterprise managers such as HP OpenView, and provides telnet access as a backup. A ‘quick-start’ facility will get the VPN Concentrator up and running in five minutes. And in recognition of the increasing popularity of outsourcing networks to systems integrators or network service providers, the network management is designed to be compartmentalized between different classes of operators, with privileges assigned by the administrator.

Conclusion

Growing demand for remote access, coupled with the tremendous strength of the Internet have made implementing a remote access VPN mission critical for every enterprise network. Not only will most enterprises see a dramatic reduction in remote access costs, they also have the potential to increase access performance, and the productivity of remote users and offices.

A successful implementation of a remote access VPN has two main constituents:

- *Deployment of an enterprise-class VPN concentrator.* This will provide the performance to harness the power of the Internet, and the scalability to grow as the user base expands and their access speeds increase.
- *Selection of an authentication system that reflects an appropriate balance of the enterprises needs for security and effort.*

The first generation of VPN routers and switches cannot meet the second component of a successful implementation. Altiga's second generation VPN Concentrator is the clear choice. The Altiga VPN Concentrator meets all of the requirements of a remote access VPN: performance, capacity, scale, client mix, reliability and security. It is fully compatible with Microsoft clients and a wide range of authentication systems.

With its design for ease of implementation and management, and minimal impact on the existing network, deploying the Altiga VPN Concentrator will not only increase the productivity of the enterprise, it will also increase the productivity of the network staff.