

G R O U N D  C O N T R O L

IG-VPN

Your VPN Solution over Satellite

**Using Application Layer Technology to Overcome the Impact
of Satellite Circuit Latency on VPN Performance**



Ground Control
February 2003

Abstract

This paper explains the source of severe throughput degradation experienced by IPSec and other data communication protocols over a satellite link. It describes a client/server software solution that enables highly efficient end-to-end VPN performance over satellite circuits despite lengthy signal propagation delay. Details are provided on features and functionality of this innovative technology.

Background

Virtual Private Networks

A Virtual Private Network (VPN) allows users to communicate and access information securely over the public Internet and other IP based networks. VPNs operate as seamlessly and securely as a private network, but take advantage of the low cost and ubiquitous global coverage of the Internet. Dramatic cost savings can be realized when compared to the expense of building and operating a private network since VPNs utilize the public telecommunications infrastructure instead of dedicated circuits.

Secure virtual connections or “tunnels” are established only when needed to provide network connectivity for a closed user community. IPSec (IP Security) is a protocol suite widely used for VPN solutions that allows secure exchange of data packets at the IP layer.

Using encryption and other technology, VPNs typically support four important areas: authentication, confidentiality of information, access control, and data integrity. Most VPN solutions are suited for intranet, extranet, site-to-site and remote access configurations.

Satellite Communication

Satellite communication technology has been available for many years and is an ideal medium for simultaneously disseminating information to many users, linking remote geographical locations, and providing connectivity to wide coverage areas. Via radio transmission, impressive data rates can be obtained using high capacity transponder channels.

As the demand from businesses for broadband data services increases, satellite communication is well positioned to address this need. DSL and ISDN fulfill much of the demand in a cost-effective manner, but these services are not available throughout all of North America and the world. A small satellite antenna or VSAT (Very Small Aperture Terminal) can be placed virtually anywhere to provide high-speed connectivity for remote offices, teleworkers and users.

Due to the broadcast nature of satellite systems, receiving signals can be accomplished with relative ease by a properly positioned satellite dish, associated electronics and moderate technical expertise. No wiretapping, direct connection or physical security breaches are necessary to intercept a transmission. For these reasons, it is imperative that appropriate measures are taken to protect sensitive information when communicating over the airwaves.

Satellite Signal Propagation Delay

Satellite communication technology is based on electromagnetic waves passing between earth-based antennas and a radio transceiver in space. This is the same fundamental principle used by terrestrial microwave systems, with the notable exception that signals must travel a much greater distance between satellite antennas on the ground and a repeater in orbit.

In order for a satellite in space to appear stationary relative to the earth's rotation, it is placed in a geostationary or geosynchronous orbit. This represents a distance of approximately 22,300 miles (35,880 km) from the surface of the earth, as depicted in Figure 1. Even though electromagnetic waves travel at the speed of light, roughly 186,000 miles/sec (299,300 km/sec), the lengthy distance introduces a relatively long latency period. This delay can dramatically affect performance of certain data communication protocols that were designed to operate on terrestrial based networks.

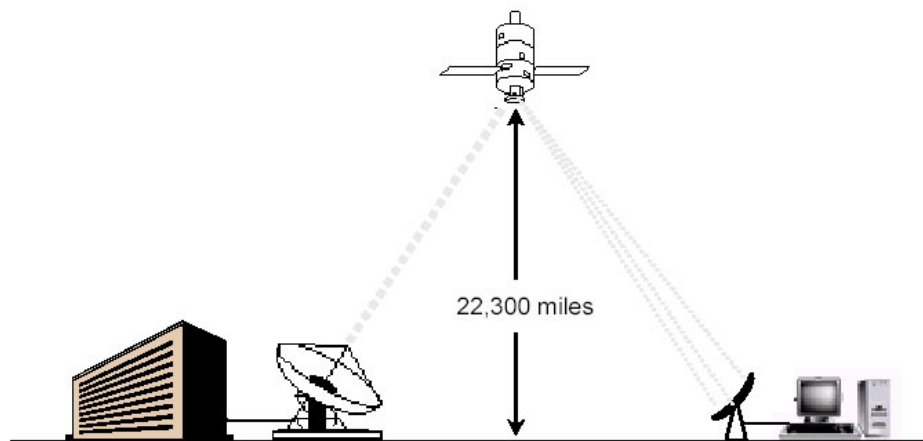


Figure 1. Geostationary satellites orbit 22,300 miles above the earth.

The time for a signal to travel from one satellite earth station to another is nearly $\frac{1}{4}$ second, which can be computed by dividing the total distance traveled by the speed of signal propagation.

$$\frac{22,300 \text{ miles (uplink)} + 22,300 \text{ miles (downlink)}}{186,000 \text{ miles/sec}} = 0.24 \text{ sec.}$$

A return transaction doubles the total transit time, increasing it to almost $\frac{1}{2}$ a second. For comparison, a round-trip terrestrial transaction using copper or fiber mediums between New York and London requires approximately 0.038 seconds, well over 10 times quicker than via satellite. Transactions requiring less distance between nodes are considerably faster. These calculations exclude additional time required for processing by electronic equipment at the originating, receiving, and repeater stations, which adds to the total delay. In practice, round trip transaction time can easily exceed 750 milliseconds.

TCP/IP over Satellite

Internet and World Wide Web connectivity is made possible through use of the TCP/IP protocol suite. TCP is a connection oriented end-to-end communication protocol that enables reliable transport of data between network nodes. In short, the protocol functions by breaking an electronic file into small packets of data, sending them along with control information, and then waiting for acknowledgements indicating they were received successfully before more data is sent. The process of sending data and receiving acknowledgements is normally rapid and quite efficient.

TCP uses a mechanism called slow-start to ascertain the maximum data rate of a channel upon initial connection setup. After sending a packet, it waits for an acknowledgement. When a response is received, an increasing number of packets are sent in the next transmission and the process continues in a similar manner. When a positive acknowledgement for a data packet is not received within a set time period, the rate at which subsequent packets are transmitted is slowed down in an attempt to optimize throughput.

There are well-understood and long-standing technological problems preventing efficient TCP communication over satellite links. TCP was designed to function most effectively on common terrestrial-based networks that exhibit much shorter round-trip latency than that of a satellite channel. In fact, the intrinsic ½ second round-trip delay for a satellite circuit (in addition to other processing time) exceeds the timeout period during which TCP expects an acknowledgement. Because of this, the protocol assumes there is network congestion and will continue sending all subsequent transmissions at a slow rate, never escaping slow-start mode.

Protocol Spoofing

Given the widespread use of TCP/IP and satellite communication technology, solutions have been developed to compensate for the effects of space segment latency. Performance enhancement proxies, most commonly in the form of TCP spoofers or accelerators, isolate the satellite portion of a circuit from the terrestrial leg, thereby avoiding adverse effects of a high latency satellite link. Spoofing allows configuration parameters, such as window size, for each portion of the circuit to be optimized independently.

TCP spoofing is accomplished by hardware or software at a local earth station that emulates TCP protocol functionality at the remote station. Packet acknowledgements are sent back to the sender by the spoofing software prior to the space segment portion of the journey. This, in effect, allows signal propagation delay to be hidden from the originator. Since packet acknowledgements are returned rapidly by a terrestrial link, TCP quickly moves out of slow-start mode and builds to a fast processing speed. Remote site acknowledgements are suppressed since they are handled by local spoofing software. Under ideal conditions, spoofing technology allows satellite users to obtain throughput performance equivalent to a comparable terrestrial circuit since the effects of signal propagation delay are essentially negated.

IPSec and Spoofing

Though IPSec VPNs are built to operate atop an IP infrastructure, they cannot capitalize on spoofing benefits due to protocol design and the manner in which encryption is employed.

Since IP Security data is transmitted using an IPSec packet type—not a TCP/IP packet format—they simply can not be interpreted by TCP protocol spoofing software. Furthermore, IPSec encrypts and encapsulates not only data, but also the TCP and IP headers that are needed in clear text by spoofing logic to function properly. An IPSec packet is depicted in Figure 2.

Due to these factors, protocol spoofing functionality is rendered useless and IPSec packets traverse performance enhancement proxies without any action being taken. They are then forced to make a time-consuming journey over the satellite channel to a receiving node where they can be decrypted, at which point acknowledgements are generated and sent back over the satellite circuit to the originator. The round-trip satellite connection adds over a ½ second delay between packet transmission and acknowledgement—a long time in the realm of electronic data communications. Since this same process takes place for every IPSec packet, the effects of propagation delay and processing time accumulate and are manifested in the form of significantly reduced throughput.

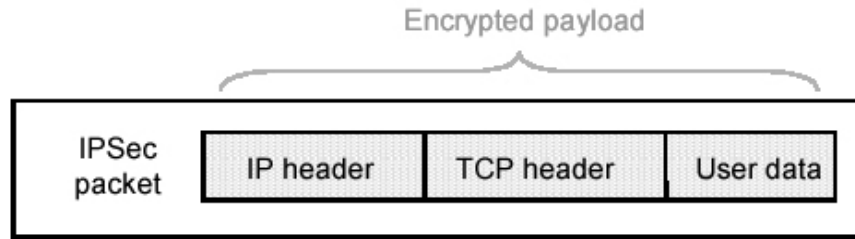


Figure 2. IPsec packets encrypt and encapsulate all TCP header information.

Due to protocol design and the laws of physics, IPsec cannot escape the adverse impact on throughput resulting from satellite circuit latency. The ability to locally spoof a remote receiver is not feasible and throughput is consequently limited by the need to acknowledge each data packet individually over a satellite link.

Application Layer VPN Technology

Ground Control's client/server VPN software circumvents performance problems experienced by IPsec and other network layer protocols when subjected to satellite circuit propagation delay. As a result of operating at the application layer, above the network level where IPsec functions, Ground Control IG-VPN technology is compatible with and takes advantage of a satellite network's existing protocol spoofing capabilities and other performance enhancement techniques.

Figure 3 provides a high level overview of the process for sending data from a user's client application to a secure server residing in a trusted environment. With Ground Control's solution, all user data and sensitive addressing information traversing the Internet is fully encrypted using constantly changing Triple DES (3DES) session keys. Only addressing information that directs a packet to the VPN proxy server is sent in the clear. At no time is an IP address of a private server exposed or transmitted in an unencrypted format.

When the VPN client on an end user's platform receives data and associated communication information (such as an IP hostname and address header) from an application, it is encrypted, packaged and prepared for transmission. This information becomes the encrypted payload of a standard TCP/IP packet destined for the VPN server. After traversing the Internet, the VPN server receives the packet, decrypts the payload, unpackages the contents and performs validity checks. Once validated, original addressing information is read and the packet is forwarded (i.e., proxied) on to the final destination. In this manner, target destination address headers and encrypted data are never visible during transport outside of a secure environment.

Once a packet is encrypted by an application layer VPN client and transmitted, it can be intercepted by a legitimate protocol spoofer that interprets the TCP control information, sends an acknowledgement to the originator, and forwards the message on to the VPN server (that will proxy it to the final destination). Immediately after the originator receives a positive acknowledgement, it transmits the next packet—while previous ones are in transit over the satellite channel—and the process continues. Since this happens rapidly, TCP quickly moves out of slow-start mode and builds to the fastest rate supported by the connection. When a packet reaches the VPN server, user data is decrypted and sent to the desired location if authorized by access controls. TCP acknowledgements returned from the receiving node are intercepted by the protocol spoofer and discarded before they can reach the originator since they would be duplicates.

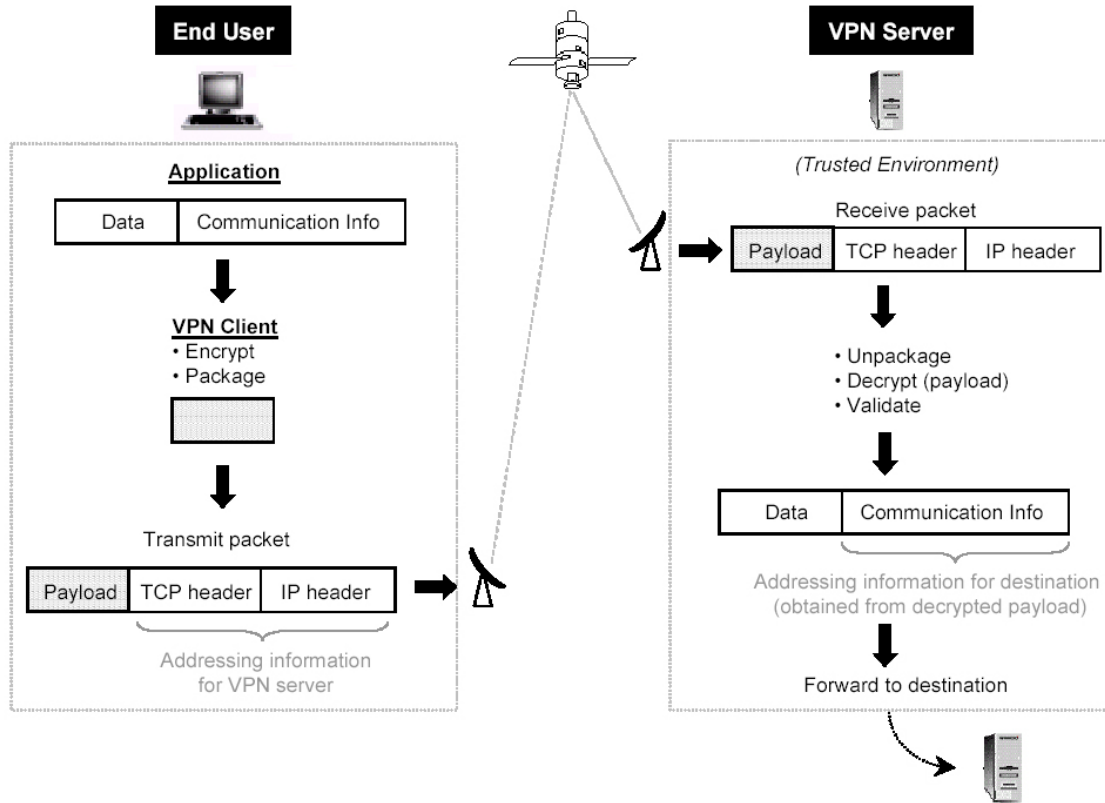


Figure 3. Ground Control's technology encapsulates sensitive control information and data into standard TCP/IP packets allowing compatibility with satellite performance enhancement proxies.

It is important to realize that encryption and VPN services are provided from an end user's system to the VPN server that is located in a trusted private network, thereby ensuring end-to-end protection. This is possible because of the client/server proxy based architecture that allows a highly secure path to be maintained from an end user all the way to the target destination.

Since application layer technology allows packets to appear as standard TCP/IP traffic, they are not subject to NAT (Network Address Translation) issues or firewall traversal problems commonly encountered with IPsec VPNs. These areas are a source of implementation and ongoing maintenance headaches that make deployment and management of a VPN a time-consuming chore requiring skilled network technicians.

Figure 4 (next page) graphically depicts the effects of TCP spoofing in a satellite network when interacting with IPsec and IG-VPN application layer protocols. To simplify, only one protocol spoofer is used in this configuration.

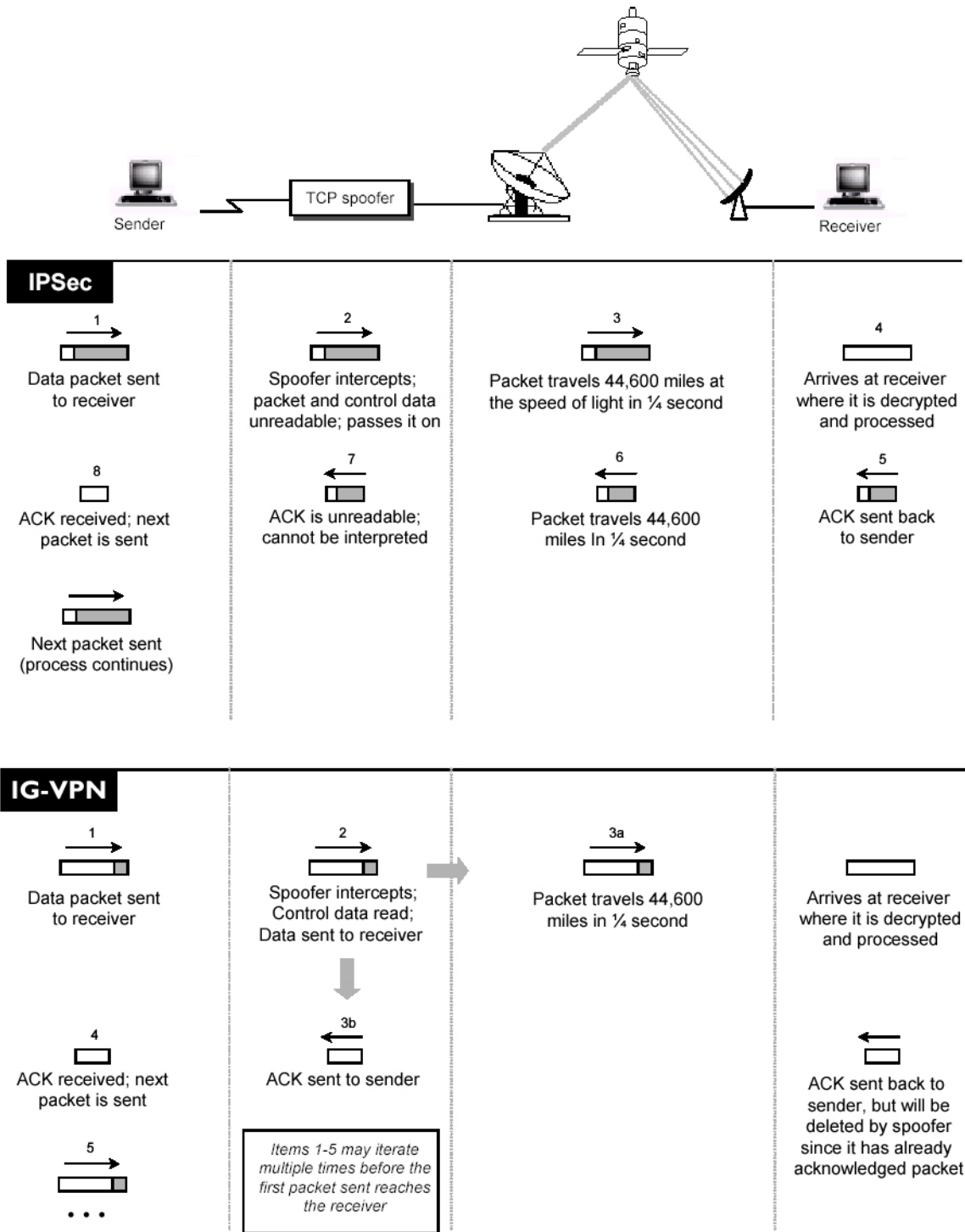


Figure 4. Effects of protocol spoofing and satellite propagation delay on IPSec and application layer VPN protocols

Hybrid or asymmetric approaches involving a combination of terrestrial and satellite circuits are not necessary. There is no need to integrate multiple technologies or components to handle encryption and/or other VPN functions in order to benefit from the performance gains.

Benchmark results to date using application layer VPN technology has shown as much as a 5:1 improvement in throughput over IPSec solutions, and performance degradation is practically negligible (less than 10%) when compared to unencrypted TCP/IP traffic over satellite.

The GROUND CONTROL IG-VPN SOLUTION

Ground Control's state-of-the-art technology is designed to protect sensitive information during transport over a public TCP/IP network, in both wired and wireless modes, from an end user's system all the way into a trusted environment. IG-VPN application layer VPN server software is the engine behind IG-VPN Client software that provides authentication, access control, encryption, key distribution, data integrity, single port proxy and other services.

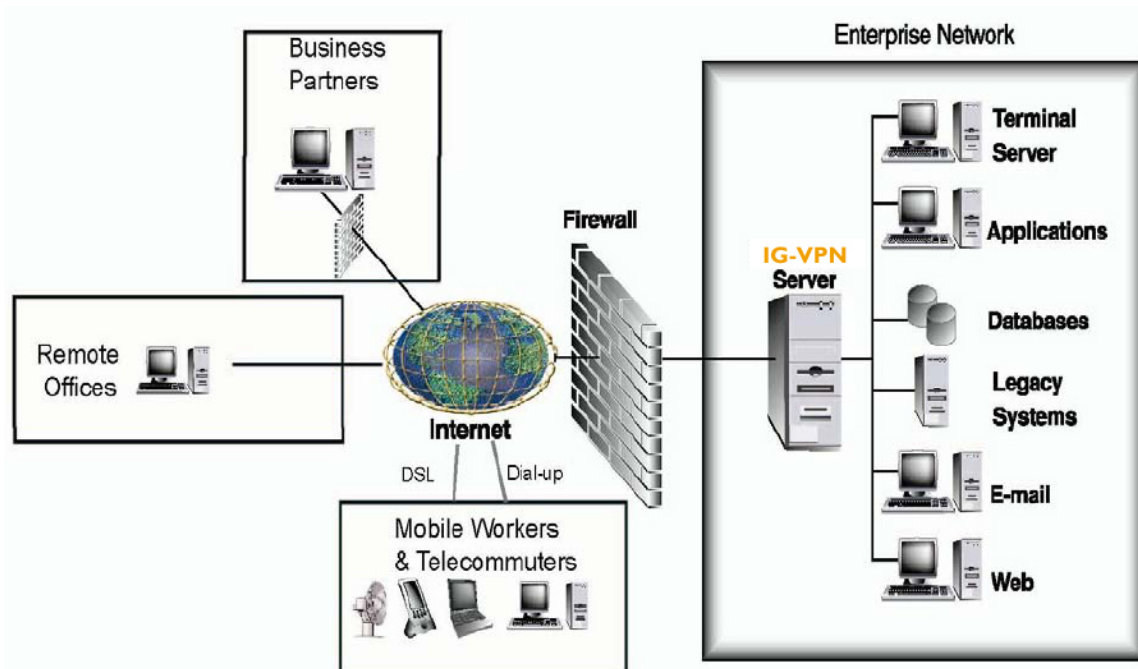


Figure 5. Ground Control client software connects over an IP network to an IG-VPN server

Application Layer and IPSec Capabilities

Through the use of application layer VPN technology, IG-VPN solutions offer benefits communicated throughout this paper that include overcoming the effects of satellite propagation delay, avoiding network address translation and firewall traversal problems, and making use of a single port proxy to provide fine-grained access control to specific TCP/IP based resources.

Access & Authentication

IG-VPN Server works in conjunction with a simple to use, non-intrusive IG-VPN client program that operates on an end user's system. VPN server software allows IG-VPN Client users to access protected services based on authenticated user identification, not an end user's source IP address or machine specific identifier.

A single-use 3DES session key is generated every time a user requests connectivity to a protected resource such as a private e-mail server or an intranet web page. By using dynamic session keys, one visit to a URL could result in multiple encryption keys being generated—one for each file contained in an HTML page. If a hacker were to intercept a data packet and invest an extraordinary amount of time, energy, and resources to decrypt the contents, their reward may be nothing more than a single image from a web page.

IG-VPN Server utilizes two-way and two-factor authentication. Two-way, or mutual, authentication means not only does the IG-VPN server validate a IG-VPN client user, but the converse is also true. The server and client engage in a challenge/response exchange with each other to verify authenticity. Two-factor authentication is analogous to a bank's automated teller machine that identifies users by something they know (a PIN) and something they have (an ATM card). A physical smartcard, virtual soft token residing on a hard drive, or biometrics device can be used with IG-VPN technology. Third party authentication systems including RSA SecureID®, PKCS #11, RADIUS® and LDAP can also be integrated.

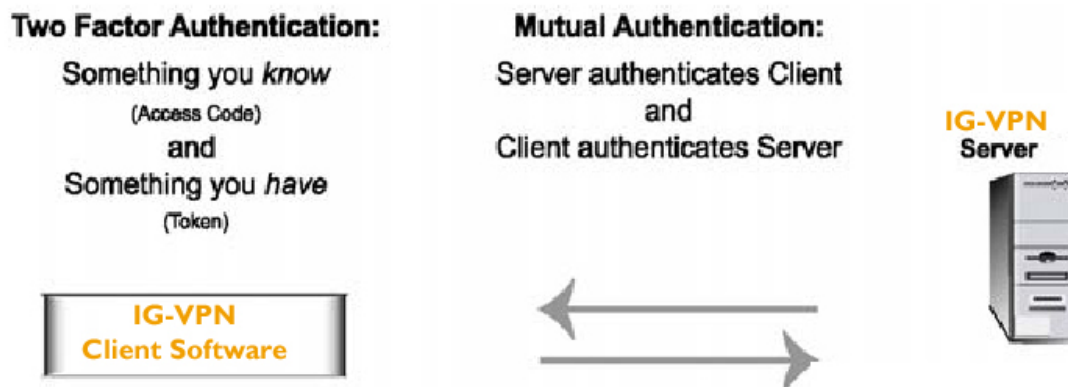


Figure 6. Both two-factor and mutual authentication is used between the client and server.

End-to-End Protection

To allow secure connectivity from an end user's computing platform to a destination application, all connection requests are intercepted by the IG-VPN client. They are ignored unless a request is made to access a IG-VPN server protected service, in which case, session and user data is encrypted with a single use 3DES key. Data packets are then proxied to the IG-VPN server residing on a private network where they are decrypted and processed. After the session information is validated, a proxy connection is made to the destination server thereby completing the secure connection.

By means of proxy capabilities and a single port presence on the network, IG-VPN is able to support fine-grained access control.

Administration

IG-VPN interacts with "SmartAdmin", a powerful Web-based administrative utility that manages users, groups, and access control lists in either a centralized or distributed manner. Four levels of administrative privileges are available. Nested group capabilities allow efficient management of large, closed user communities. Administrators with control privileges can grant specific

individuals or groups access rights to entire networks, certain applications, specific URLs, and/or other network resources.

On-Line Registration

IG-VPN's On-line Registration (OLR) capability allows end users to securely register via the Internet and begin accessing IG-VPN secured applications and resources within minutes. After a user registers, is enabled by an administrator, and launches IG-VPN client, the IG-VPN server pushes current access permissions to the user's IG-VPN client. These read-only permissions are stored on the user's computer for the duration of a session, are reloaded from the server upon each subsequent login, and can be modified in a real-time manner by an administrator.

Platform Support

IG-VPN Server and IG-VPN client are supported on a broad range of computing platforms as summarized in the figure below. A Java™ version of IG-VPN client is available which eliminates the need for client software to be pre-loaded on an end user's system. Ground Control offers a widely deployed FIPS 140-1 validated virtual token that is approved for U.S. Government use.

The Ground Control IG-VPN solution is engineered to be flexible and scalable—integrating seamlessly with existing firewalls and network infrastructures.

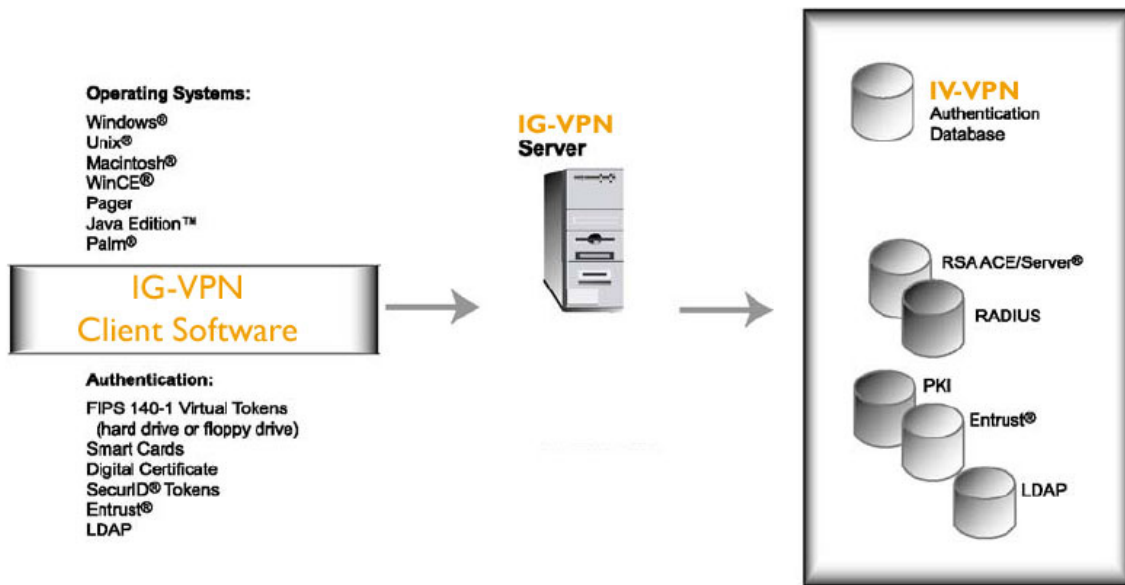


Figure 7. IG-VPN is available on a wide range of platforms and supports third party authentication methods

Conclusion

By operating at the application layer and leveraging a satellite network's TCP protocol spoofing capabilities, IG-VPN technology is able to deliver impressive throughput efficiency over high latency satellite links. Secure VPN connectivity is provided from an end user all the way into a secure environment without exposing any user data or sensitive addressing information.

IG-VPN is powerful client/server VPN software that offers many features and benefits in both wireless and wired environments.

GROUND CONTROL
241 Prado Road
San Luis Obispo, CA 39401
800-773-7168 Phone
805-542-0688 FAX
www.groundcontrol.com