

IPSec VPNs Over Spacenet VSAT Networks

This document contains information proprietary to Spacenet Inc. (Spacenet). It may not be reproduced in whole or in part without the written consent of Spacenet. The disclosure by Spacenet of information contained herein does not constitute any license or authorization to use or disclose the information, ideas, or concepts presented.



Contents

1. Executive Summary	1
2. Challenges with VPN Over VSAT Networks	1
2.1 Satellite Networks and IPsec VPNs	1
2.2 Spacenet Standard Acceleration Technology	2
2.3 IPsec and VPNs	2
2.4 Spacenet's TCP Acceleration Technology and VPNs	3
3. Spacenet's VPN Over VSAT Solution	4
3.1 Solution Overview	4
3.2 Software VPN Implementation	5
3.3 External ("Embedded Unit") Device VPN Implementation	5
3.4 Integrated Device VPN Implementation	6



1. Executive Summary

Spacenet's VPN accelerator provides the technology necessary to deliver high levels of performance for VPN connections over VSAT networks. This accelerated VPN over VSAT solution is the first to enable IT managers to provide a unified security solution with ubiquitous availability for their LAN/WAN and remote users.

Most VSAT systems include some form of network "acceleration" technology to combat the inherent round-trip latency of communications between terrestrial and geosynchronous-orbit devices. The nature of IPSec, however, runs counter to most existing acceleration methods and significantly decreases their effectiveness. The resulting lack of acceleration has often resulted in poor performance of critical applications over VPN over VSAT.

Gilat has developed proprietary new technology which enables integration of IPSec VPNs into VSAT networks with no significant loss of performance. The Gilat VPN acceleration method is accomplished through hardware and software solutions that create VPN tunnel start/end points where they are able to take advantage of Spacenet TCP acceleration technologies.

This solution will be offered in three different forms: a Win32 PC software add-on, as an "embedded unit" that can be added into a network with an existing IPSec gateway, or with an integrated "embedded box" and IPSec gateway in a single unit. Testing of the technology has shown a significant improvement in VPN throughput over VSAT links (increasing outbound throughput from a maximum of 100 kbps to 1 Mbps or higher).

2. Challenges with VPN Over VSAT Networks

2.1 Satellite Networks and IPSec VPNs

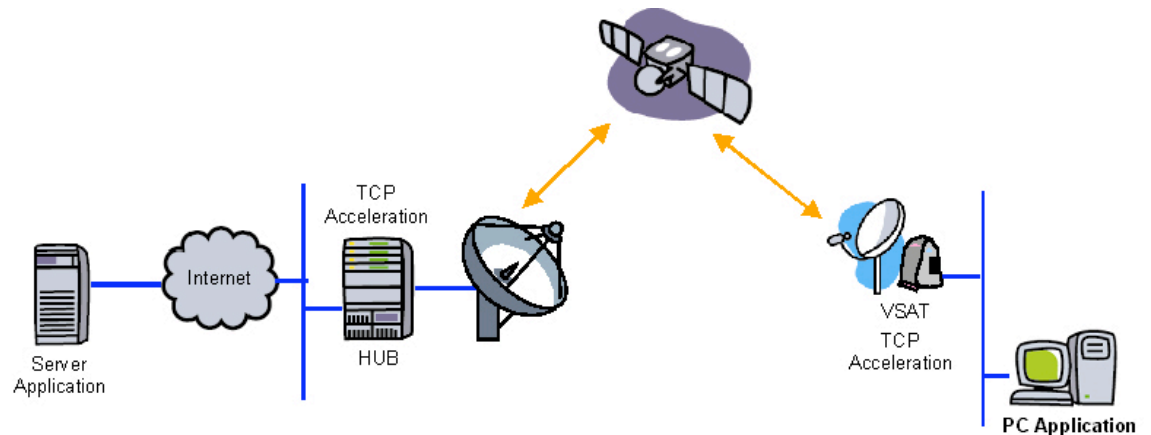
All VSAT networks experience a certain amount of latency due to the amount of time needed for a signal to travel between a terrestrial location to a satellite in geosynchronous orbit 22,300 miles above the Earth and then down to a terrestrial hub dish. While this latency does not limit raw bandwidth speeds, it does create a functional slowdown for "chatty" applications and protocols which "talk" back and forth frequently and must wait for each side to reply back before they continue. Most satellite network operators implement some form of data "acceleration" of some sort over their satellite links in order to combat this latency (see below).

However, the nature of standard IPSec VPNs interferes with these acceleration technologies, resulting in massive performance degradation of satellite links when VPNs are being used. This paper will address the advances that Spacenet has made in the development of technologies which will significantly improve

performance of VPN tunnels over VSAT links and enable seamless VPN solutions using VSAT networks.

2.2 Spacenet Standard Acceleration Technology

Spacenet has always been the leader in implementing acceleration technologies designed to solve the VSAT latency challenge and provide users with high-quality broadband experiences over satellite networks. The illustration below shows a typical Spacenet VSAT network, including the “TCP Acceleration” software and hardware devices placed on each end of the connection.



This Spacenet acceleration technology works through emulating a destination computer in order to send TCP acknowledgement packets “locally” and avoid satellite link delay. The acknowledgement packets sent by this acceleration technique “tricks” remote computers into sending follow-up packets immediately rather than waiting for an acknowledgement to reach the destination computer over the satellite link and then make the return trip as well – effectively “accelerating” the data stream.

Spacenet also employs proprietary technology designed specifically to accelerate web browser HTTP GET requests and dramatically increase the speed of web surfing. Through the combination of these web and TCP accelerator technologies, common Internet applications are significantly accelerated and the user enjoys a high-quality broadband experience.

2.3 IPsec and VPNs

Standard VPNs encrypt IP packets using IPsec (IP Security Protocol), the current de facto standard (and future IETF standard) for secure Internet communications. IPsec is a set of extensions to the existing IP protocol which add cryptographically-based authentication, integrity, and confidentiality services at the IP datagram layer. IPsec

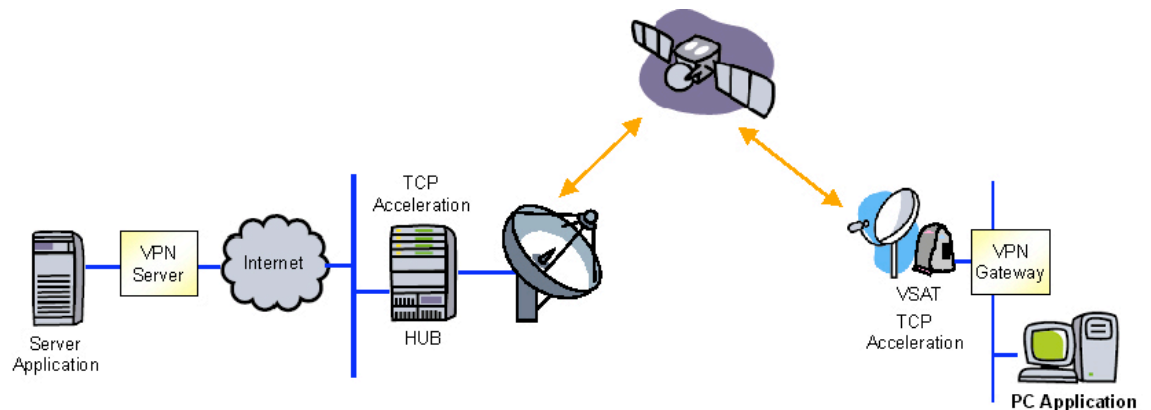
provides a basis for interoperably secured host-to-host pipes, encapsulated tunnels, and Virtual Private Networks (VPNs), thus providing protection for client protocols residing above the IP layer.

The protocol formats for IPsec's Authentication Header (AH) and IP Encapsulating Security Payload (ESP) are independent of the cryptographic algorithm, although certain algorithm sets are specified as mandatory for support in the interest of interoperability. Similarly, multiple algorithms are supported for key management purposes (establishing session keys for traffic protection), within IPsec's IKE framework.

As part of its function, IPsec encrypts whole IP packets (including both the user data payload and the original TCP/IP headers) and places the encrypted data with the new IPsec packet's ESP. This action (necessary to IPsec's operation) is what causes the current conflicts with VSAT acceleration technologies.

2.4 Spacenet's Acceleration Technology and VPNs

When VPN connections are used, Spacenet's acceleration components (the VSAT IDU on the customer side and the HPS [Hub Protocol Server] at the hub location) are able to perform their operations on the IPsec authentication header but are unable to read the original IP header (now encrypted and put inside the IPsec ESP) in order to send an accelerated acknowledgement. This effectively "breaks" the standard acceleration system and does not allow it to provide its normal benefits.

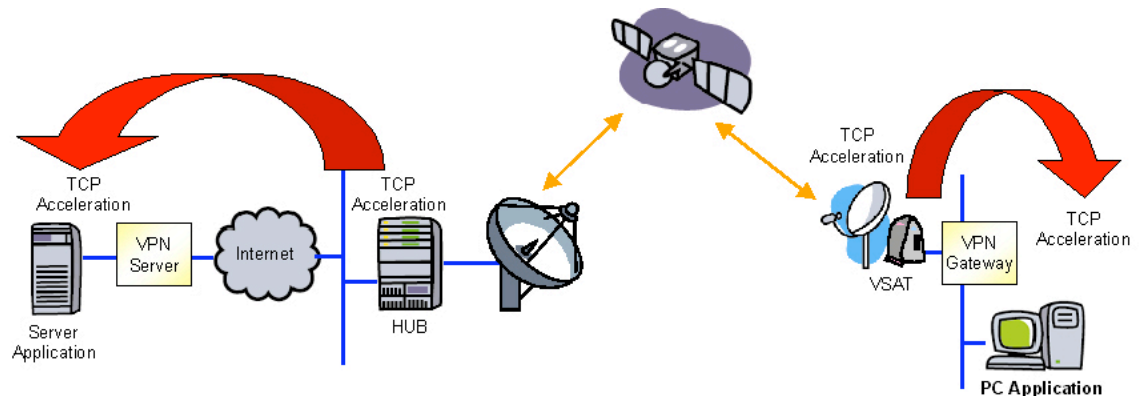


As a result, typical throughput over a VSAT link is adversely affected. Preliminary testing of unencrypted VSAT vs. VPN-over-VSAT networks showed a decrease in outbound throughput of 90 percent or greater, with a functional limit of 100 kbps. In addition, the encrypted packets are not able to be assigned rate control/priority designations based on destination or application by the Spacenet network.

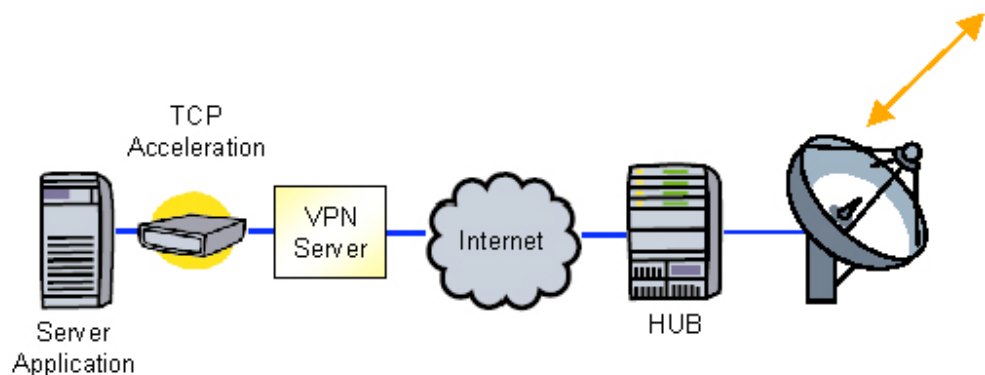
3. Spacenet's VPN Over VSAT Solution

3.1 Solution Overview

Spacenet's solution to this dilemma involves the movement of the TCP acceleration devices from a position in the network flow *after* IPSec encryption has been done to a position in the network *before* IPSec encryption is performed. This movement of acceleration devices to locations between the network application and the encryption/IPSec tunnel device allows the acceleration techniques to work properly, and re-enables rate control/priority features.



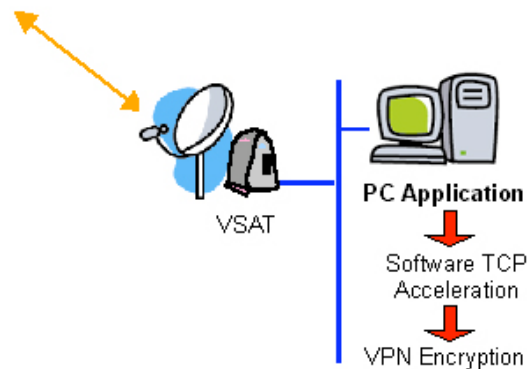
On the client side, the solution intercepts TCP packets before they reach the IPSec encryption device. Only after this is done (in the Win32 TCP/IP stack for software VPN clients, or using an external “embedded unit” for hardware-based VPN solutions) is the packet forwarded on to the VPN device. This solution is available in three different client-side implementations.



All three implementations require a server-side Spacenet TCP acceleration embedded unit. This unit, a “lite” version of the Spacenet Hub Accelerator implemented on a Sun Solaris-based server, is placed on the customer network between the server or Intranet and the VPN gateway.

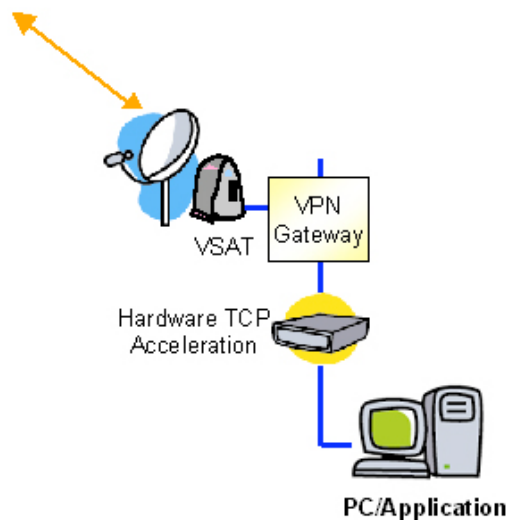
3.2 VPN Client Implementation

The VPN client implementation is a software-based solution for users whose VPN access relies upon client software on their PC. For systems using a software-based VPN solution (the VPN tunnel begins at the user's PC), Spacenet software can be installed on each user's computer to accomplish the TCP acceleration at a software layer just above the VPN encryption layer.



The software solution is compatible with all other client software VPN solutions (Cisco, etc.). This software is available for use with Win32 (Windows 95/98/ME/NT/2000/XP) systems.

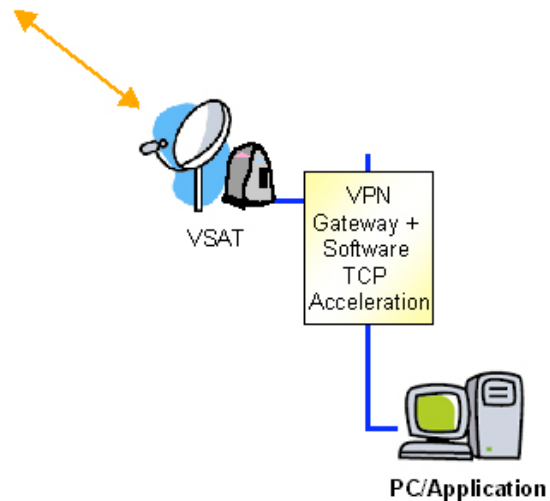
3.3 External ("Embedded Unit") Device VPN Implementation



In this implementation, a dedicated "acceleration server" or "embedded unit" is physically added to the client-side network to handle acceleration tasks before data reaches the network VPN gateway. This "embedded unit" is essentially a streamlined version of the Hub TCP Accelerator running customized acceleration software on a Sun Solaris-based server. A primary advantage of this solution is that it does not require any software to be installed on the client computer.

3.4 Integrated Device VPN Implementation

The integrated device solution is similar to the “embedded unit” implementation, but uses custom software to be installed onto the user’s VPN gateway.



This effectively combines Spacenet Hub Acceleration and VPN router functionality on the customer’s existing Cisco, Lucent or other VPN gateway, eliminating the need for a separate physical server for acceleration tasks. This solution also does not require any software to be installed on the client computer.

4. Summary

VPN tunnels have long posed a performance problem for VSAT networks. Spacenet has taken the lead in the development of acceleration technologies that will deliver a quality broadband VPN experience over VSAT. This technology is being implemented in a variety of ways to meet all customers’ needs, and represents a significant step forward for customers’ ability to integrate their existing security solutions with VSAT networks.