

Using VPN (Virtual Private Networks) over Satellite

Executive Summary

This paper discusses the usage of VPN (proprietary or IPSec) over two-way satellite networks and identifies the solutions possible to increase performance and provide an effective environment for VPN communications.

Characteristics of satellite networks

Satellite communication is an ideal method of providing connectivity to wide geographical areas. It provides a useful and unique alternative to private circuits, ISDN, xDSL and cable modem where these technologies cannot reach or are inappropriate. Using modern satellites very high data rates can be obtained offering a range of connection speeds equivalent to those from dial-up to international data trunking.

Geostationary Satellites are located 36,000 km from the Earth and despite the very high speed of transmission (300,000 km/s) the path the signal must travel is affected by a delay of around 0.25 of a second (twice this for a round-trip). This delay is the most significant difference between satellite and terrestrial for data communications, especially for the Internet protocols TCP/IP.

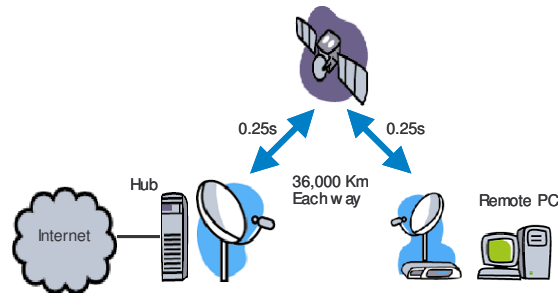


Figure 1. Typical Satellite connection

How TCP/IP works

Applications, such as web browsing or email send and receive information over the Internet as packets of data. These packets are built up in a stream or in bursts which include information or data from the application and control information about the data stream itself. This control information is stored within packet headers to ensure that all packets are sent and received to and from the correct addresses, in the correct order and with no errors. The control information is used to resend, synchronise and correct any packets that go astray during transmission. The packets are made up of application data and headers from the TCP protocol and IP protocol, as shown in Figure 2.



Figure 2. Simplified IP data packet

Why VPN is important

Because a TCP/IP data stream has these fixed attributes it is possible for the security of the data within each packet to be compromised. It is possible to intercept each packet, read the data, reassemble it and then send it on its way. For the majority of traffic that traverses the Internet this is not an issue. However, for businesses that want privacy and protection from attack it is critical. Therefore the use of VPN (Virtual Private Networks) has become commonplace across the Internet, especially where business is conducted across multiple sites nationally or internationally and increasingly as we adopt working from home as an acceptable alternative to lengthy and expensive commuting. VPN also protects the ingress of unwanted visitors to private networks that have connections to the public Internet. The VPN server acts as a secure gateway to allow remote access from multiple sites into a private network.

A VPN is used to encapsulate and protect the TCP/IP stream from interference, snooping, hijack or attack. In essence, it provides a secure “tunnel” from one end point to another across a public network, see Figure 3.

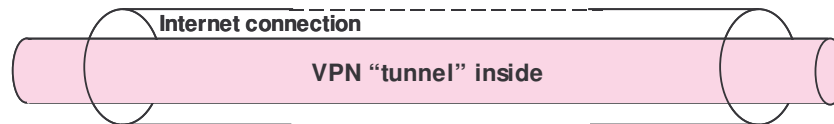


Figure 3. The VPN tunnel

At a packet level, VPN performs two functions. The TCP/IP data stream is encrypted so that the data cannot be read, it also adds additional header information so that any packets transferred that are lost or arrive out of order can be retransmitted. This replication of TCP/IP function introduces a processing overhead and therefore the performance over a VPN connection is always slightly less than a normal TCP/IP connection.



Figure 4. VPN at the packet level

This difference in performance is not significant and so VPN has become an established method of creating private networks over public networks such as the Internet.

Using VPN over satellite connections

The protocols used over the Internet (TCP/IP) were designed for reliable end-to-end data delivery over unreliable and congested networks. On a satellite connection the circuit is not congested in the same way a terrestrial connection may be; there is less retransmission and recovery. However, satellite presents a high latency (delay) medium and TCP responds in different ways to this delay. To begin a data transmission, TCP uses a slow-start mechanism to determine the congestion on the network. A delay over satellite is interpreted as congestion and therefore the slow-start mechanism remains in force for the duration of the transmission. Combined with the need to make frequent acknowledgments for the receipt and transmission of each

packet this leads to a very inefficient use of a medium that is inherently reliable and uncongested.

To overcome the limitations of TCP over satellite the providers of satellite equipment and services pass TCP and other application layer protocols through Performance Enhancing Proxies (PEP) that accelerate this traffic over the satellite connection. The PEP performs a number of functions such as reducing window sizes for packet transmissions and selectively suppressing the need for acknowledgments in the data stream. See Figure 5. Additional techniques such as caching and web-page acceleration (sending a pre-built web-page rather than downloading each element through multiple “get” messages) are also used to improve performance.

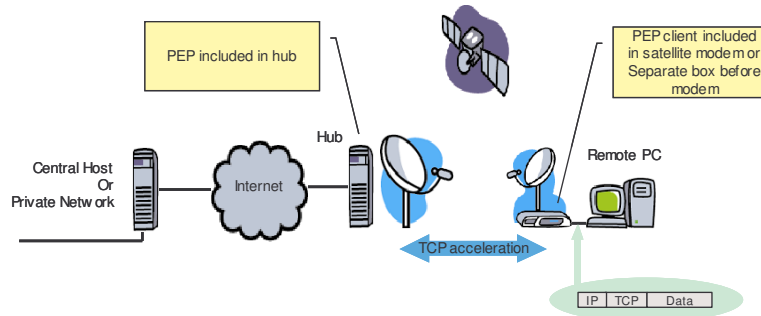


Figure 5. TCP acceleration through Performance Enhancement Proxy

The performance enhancement techniques used to accelerate TCP actually modify the TCP headers in each packet. When an IPSec VPN is used, the TCP headers are encapsulated within the VPN data stream and cannot be accelerated. The performance of the VPN is therefore affected and appears significantly less than accelerated TCP. See Figure 6.

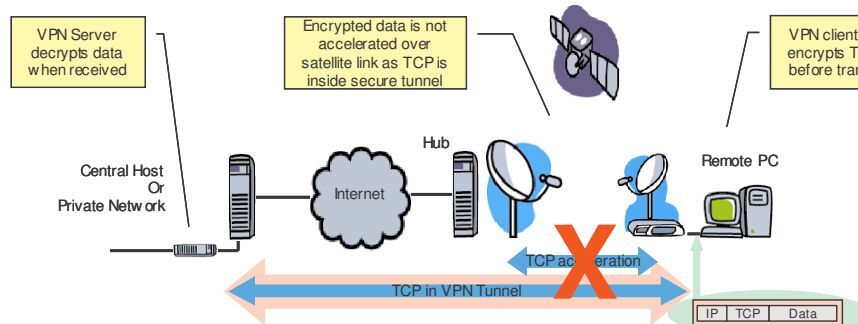


Figure 6. IPSec VPN with no TCP acceleration

In conclusion, VPNs do work over satellite connections. Whether the speed is acceptable for a particular user application is another matter and any degradation from normal TCP/IP performance is seen as unacceptable. In order to enhance the performance of VPN over satellite there are a number of alternatives available.

Improving VPN performance

The function of VPN over satellite is directly related to the implementation of the various methods to improve the performance of encapsulated TCP. Satlynx has tested many of these and has concluded that the selection of the right or optimal method

depends much upon the application, customer requirement and budget available. Satlynx does not generally prescribe any one solution from a 3rd party supplier but instead approves the solutions that it tests and finds acceptable and compatible with its networks.

More bandwidth

Whilst it is true that more bandwidth will improve performance there are always physical and economic constraints on this solution. Additionally, the increase in demand for the bandwidth required to transmit the protocol overhead will increase volume consumption.

Regardless of the bandwidth available there will always be a limitation from the high latency (round trip delay) of transmission over satellite. This will ultimately provide a ceiling beyond which more bandwidth will not be able to improve the performance.

Changing the parameters of transmission

The operation of TCP is defined by a complex parameter set that defines attributes such as packet size, window size, timeout, acknowledgments, buffer size and so on. These attributes determine the performance of the protocol and ideally should be tuned to match the operating system of the processor and the type of network connection.

Changing these parameters requires matching the parameters at either end of the connection to get the full benefit of the performance improvement. Some parameters may be changed independently. There is no single definitive source of this information as any changes that can be made will depend upon the users local environment. Further information can be obtained from these locations:

Source	Reference	Subject
Speedguide	http://www.speedguide.net/articles.php?category=52	Windows/TCP
Microsoft	http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/tcpip2k.msp	Windows 2k
IETF	http://www.ietf.org/rfc/rfc2488.txt http://www.ietf.org/rfc/rfc2760.txt	TCP

Table 1. Further information on TCP optimisation over satellite

Application layer security

A relatively easy and cost effective way to implement VPN over satellite is to encrypt just the data packet and not the TCP or IP headers. This method already provides a good level of security which for many small businesses and individuals, especially where no IPSec VPN solution exists or where there is no predefined technology or vendor choice.

In a typical configuration client software resides on a remote PC and creates the VPN by encrypting data from the applications before passing it on to TCP for transmission across the network. Therefore, the TCP and encrypted data can be accelerated over the satellite connection. At the other end of the path a VPN server will terminate the VPN tunnel and pass the data on safely to its destination within a secure network or directly to a host. See figure 7.

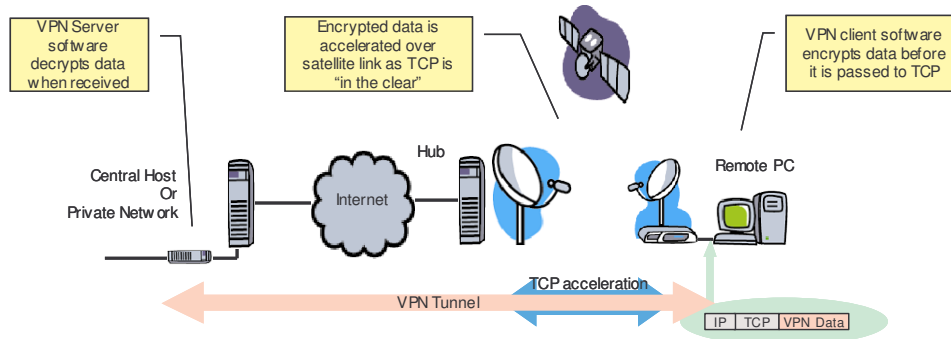


Figure 7. VPN at the application layer

There are many providers of this technology, some implement a client/server pair as software and hardware, others implement a hardware gateway pair; the solution chosen depends upon the configuration required at the remote site (single PC or LAN).

Accelerating before encrypting

Another alternative for improving VPN performance over satellite requires the full encryption of the TCP data stream so that both data and protocol headers are secure. This is particularly important in cases where an enterprise has a predefined technology choice (such as IPSec), vendor procurement or security policy that requires the highest level of VPN security possible.

The method used here is to accelerate the TCP before passing the data stream on into the IP layer for encryption. See Figure 8.

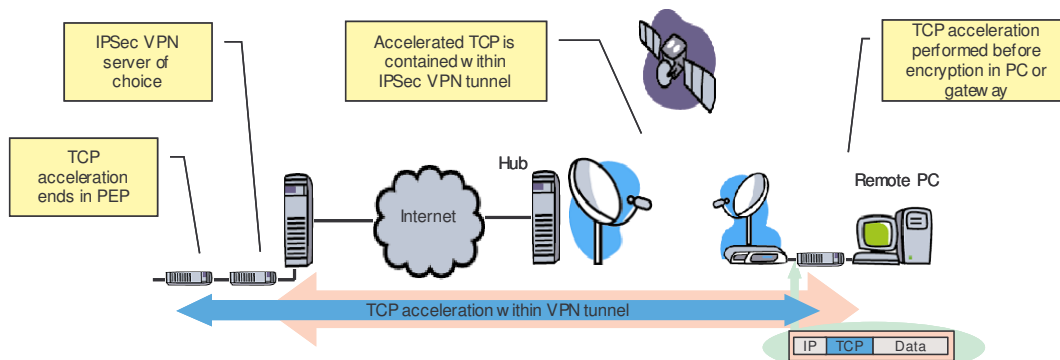


Figure 8. Accelerating TCP before the IPSec VPN

This solution comprises an acceleration or Performance Enhancement Proxy that is operated by the user, rather than embedded within the VSAT and hub. Again, There are many providers of this technology, some implement a client/server pair as software and hardware, others implement a hardware gateway pair; the solution chosen depends upon the configuration required at the remote site (single PC or LAN).

Conclusions

This paper has discussed the characteristics of satellite networks, how TCP works and why VPN is deployed over public networks to make communications and gateway servers more secure and resistant to attack. The operation of VPN over satellite connections has been explained and different solutions presented to illustrate how a degree of fine-tuning of these solutions is required, according to application and budget.

The various solutions discussed are all available on the market and have been tested by Satlynx. As most customers' networks are unique there is no single or universal solution that can be prescribed for all, especially when satellite is often used to complement existing terrestrial networks where IPSec VPN is already in use.

Accordingly, Satlynx has chosen to give its customers an informed choice along with a range of tested and approved solutions. Satlynx continues to monitor the availability of various available VPN solutions to test and approve the most promising alternatives for use on its networks. Given the ever-changing nature of technology the list of approved and recommended products is available from Satlynx on request.