www.skycasters.com
800-268-8653

skycasters

Headquarters
1520 South Arlington Street
Akron, Ohio 44306

VPN over Satellite

A comparison of approaches

by
Richard McKinney and Russell Lambert

As awareness of satellite Internet access becomes more widespread, demand for secure connections from remote locations to corporate local area networks continues to increase. The high latency inherent in geosynchronous satellite connections has presented a significant obstacle to efficient virtual private network (VPN) connections over satellite.

Various solutions to carrying IP traffic over satellite have been proposed, but each one has had some limitation that prevented it from becoming widely adopted. Recently Encore Networks released their VSR-30 3DES VPN device which offers the most popular features of Internet protocol security (IPsec) appliances, but leaves the IP header unencrypted. This feature makes the VSR-30 attractive for satellite-based VPN applications because visible headers allow satellite operators to optimize throughput.

The Problem

In order for a two-way satellite service to perform properly in conjunction with traditional terrestrial networks (Internet, Intranet), satellite data networks must employ special techniques to deal with the extra 44,600 mile space segment of the connection. Without those steps, the increased latency (as a result of the time required to traverse the extra distance) would severely limit performance.

The Internet relies on the Transmission Control Protocol (TCP) to ensure packet delivery without errors. TCP works by sending a certain amount of data, the "window size," then waiting for the receiver to send an acknowledgment of receipt. With TCP, the sender cannot transmit more data until it has received an acknowledgment. If an acknowledgment does not arrive in a timely manner, TCP assumes the packet was lost (discarded due to network congestion) and resends it. When packets go unacknowledged, TCP also slows the transmission rate to reduce congestion and to minimize the need for retransmissions.

TCP/IP sessions start out sending data slowly. Speed builds as the rate of the acknowledgments verifies the network's capacity to carry more traffic. This is known as slow-start, followed by a ramp-up in speed. The speed of the connection builds until the sender detects packet loss from a lack of an acknowledgment. This allows TCP to achieve the fastest practical data transfer rate for the conditions present on the network.

Terrestrial networks typically have round-trip latencies in the range of 35 to 100 ms. Satellite networks, due to the distance of geosynchronous satellites above the equator, require 550 ms or more. Some satellite connections have much higher latencies. Depending upon the satellite hardware and subscription policy of the service provider, latencies of 800 ms to as much at 2,000 ms or more can occur.

TCP interprets the additional satellite transit time as network congestion. If uncorrected, this effect causes the network to send all additional packets at the slow-start rate.

Current satellite data networks employ a technique referred to as TCP acceleration or IP spoofing to compensate for the extra time required to transit the space segment. Special equipment at the carrier's main satellite hub appears to terminate the TCP session, so it appears to the sender as the remote location. In actuality, the device at the satellite hub acts as a relay or forwarder between the originating terrestrial location and the remote satellite unit.

When the spoofing equipment receives Internet traffic destined for a remote satellite location, it immediately acknowledges receipt of the packet to the sender so more data packets will follow promptly. This way the sender never experiences the actual latency to the remote site because acknowledgments return rapidly. As a result, TCP moves out of slow-start mode quickly and builds to the highest practical speed.

To prevent packets from being acknowledged twice, the spoofing equipment suppresses acknowledgments from the remote site. In this way, computers behind a satellite link communicate seamlessly and efficiently with servers on the terrestrial Internet.

IPsec VPNs not only encrypt the data portion of packets, they also encrypt the TCP port number and IP address of the sender's computer. (Think of the TCP port as the apartment number while the IP address is that of the

building.) Consequently, only the VPN software at the remote site can decipher where packets originated and acknowledge receipt of data.

Popular IPsec VPNs, therefore, defeat TCP acceleration over satellite links because ground stations cannot adjust the fields in the header when those fields are encrypted. This situation requires that acknowledgments transit the space segment twice (over and back) and results in substantial performance degradation. The impact on performance increases as the latency rises.

To determine the effect of latency on performance and to measure the effectiveness of an alternative VPN device, engineers at Skycasters transferred a variety of data files over a high-quality satellite link under controlled conditions and measured the results.

Test Procedure

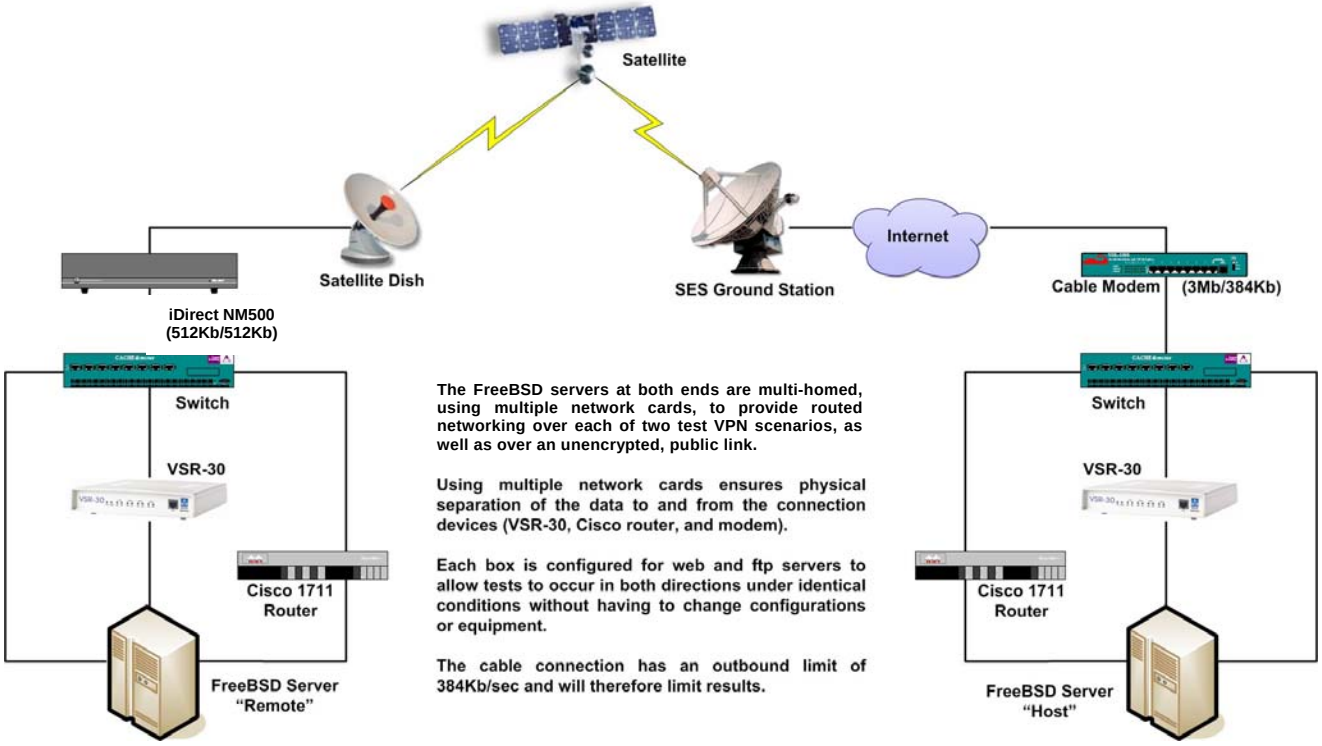
The test compared transfer rates over a Cisco 1711 IPsec VPN and an Encore VSR-30 Selective Layer Encryption (SLE) appliance to each other and to the speed of file transfers over the open Internet (unencrypted).

The data moved from remote to server, then from server to remote using FTP. Transfer rates were measured in kilobits per second (Kbps). The test utilized six different files to measure data transfers rates: 500 kilobyte, 5 megabyte, and 10 megabyte files in both compressible (text) and non-compressible (binary) forms.

Both the Cisco and Encore equipment used 3DES encryption. However, the Encore unit's SLE encrypted only the data, leaving the IP and TCP headers accessible. With the headers accessible, the encrypted packets are compatible with all types of satellite modems and all methods of TCP acceleration.

The test transferred files between two similarly configured FreeBSD computers containing three identical network cards. With three cards in each system, the computers could multi-home and physically separate data. The resulting three data paths facilitated the near simultaneous testing of the two VPN circuits and the unencrypted, clear connection.

The remote connection utilized an iDirect NetModem II commissioned for 512 Kbps/512 Kbps service to the Internet. The host side had a cable modem connection running at 3 Mbps/384 Kbps. The 384 Kbps outbound connection limited the ability to test the full 512 Kbps download capability of the satellite modem, but it did



skycasters

provide adequate results to compare relative speeds of encrypted and unencrypted data coming from the host.

The latency of the satellite link used in these tests ranged from approximately 550 ms to 625 ms. (Some satellite connections have much higher latencies. Depending upon the satellite hardware and subscription policy of the service provider, latencies of 800 ms to as much at 2,000 ms have been observed.)

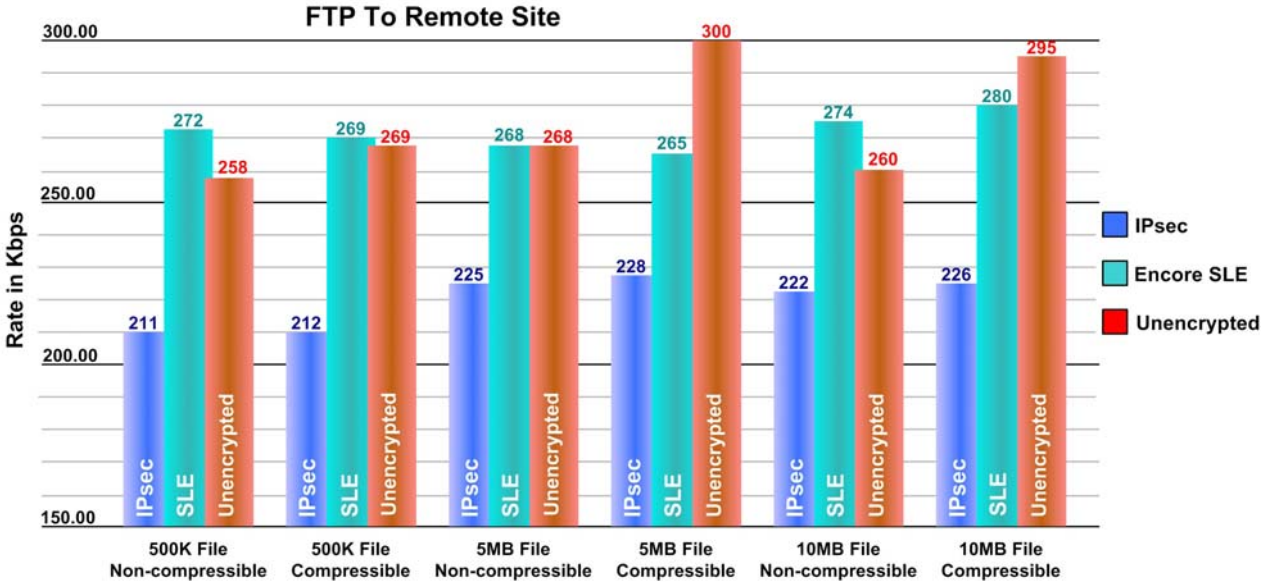
The performance of any shared bandwidth system varies throughout the day. To minimize bandwidth effects on results, five iterations of each test were run at different times. To further reduce the influence of bandwidth fluctuations, the testing sequence progressed through all six files, once in each direction, before repeating the transfer of any one file. For example, the 500 K text file ran through the SLE tunnel, then the IPsec circuit, and finally in the clear. Next a 500 K binary file passed through each circuit, and so on. Each interleaved sequence of transfers were repeated five times.

An efficient VPN solution must do more than simply transfer files proficiently. The time to establish a TCP/IP session can significantly impact how applications run across a high-latency connection. To gain an indication of the rate at which the connections could establish TCP/IP sessions, the test procedure transferred a directory file and a group of web pages back and forth.

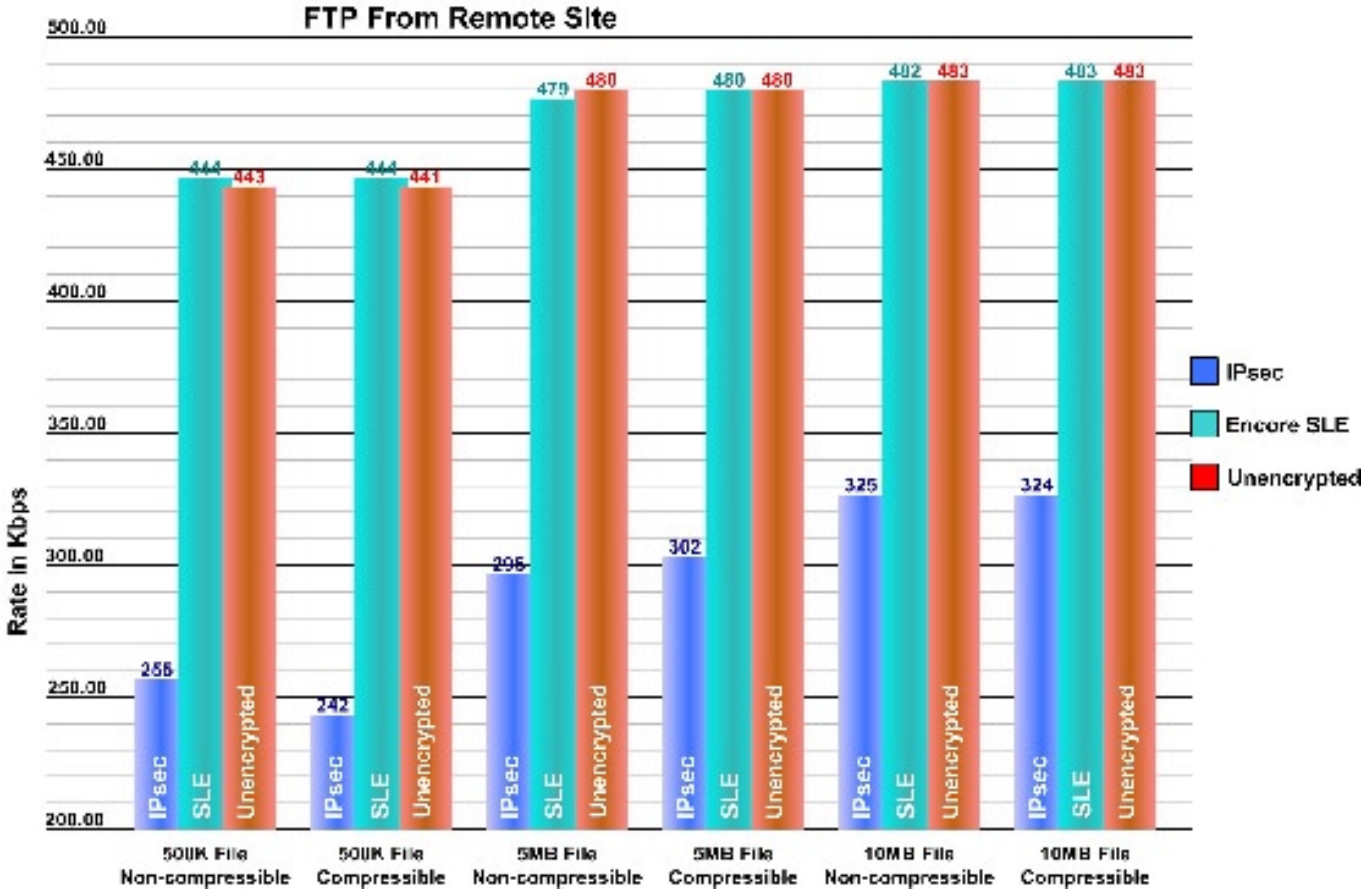
The time required to establish a TCP/IP session can have a noticeable impact on the performance of some web-enabled applications. Since each file included in a web page requires the browser to start a new HTTP connection to the server, a page with multiple graphics, framed text, or media in external files will cause a delay as multiple connections open and close. Similar circumstances occur in FTP connections as a client traverses the server's file structure if that action involves multiple files.

To illustrate TCP/IP session initiation efficiency, the test protocol included two additional procedures. First, each server transferred a directory containing files of different sizes and composition over and back across the connections using FTP. Second, the servers moved a series of web pages to and from the remote site using HTTP.

Since both FTP and HTTP must establish a new connection for each file, this procedure provided a method to assess start/restart timing issues associated with VPN tunnels extended across satellite links. For convenience, the FTP and HTTP tests measured the total time required to transfer the respective data from one side to another, not the time to reestablish each individual connection.



skycasters



Results

As the graphs above clearly indicate, the 3DES Selective Layer Encryption technology proved consistently faster than IPsec encryption in all three categories: FTP file transfer, FTP directory transfer, and HTTP web page downloads. This is as expected because SLE leaves the TCP/IP headers in the clear which allows the satellite operator to perform IP spoofing or TCP acceleration.

In half of the FTP file transfers, Selective Layer Encryption attained higher data transfer rates than the unencrypted circuit. Data moved 20% slower over the IPsec connection than it did over the unencrypted channel when moving from host to remote and 38% slower moving from the remote to the host.

Both the graph on page 3 entitled FTP to Remote Site and the one above labeled FTP from Remote Site present the mean values for five iterations of each file type.

Selective Layer Encryption also performed well in the TCP/IP intensive tests involving directories and web pages. When downloading the directory information to the remote site, SLE performed only 7% slower than the unencrypted connection compared with 25% for the slower IPsec protocol. In the opposite direction, the SLE connection completed the task only 3% behind the unencrypted connection while the IPsec circuit ran 14% slower. The graph entitled Directory Transfer on the next page illustrates mean values for five iterations.

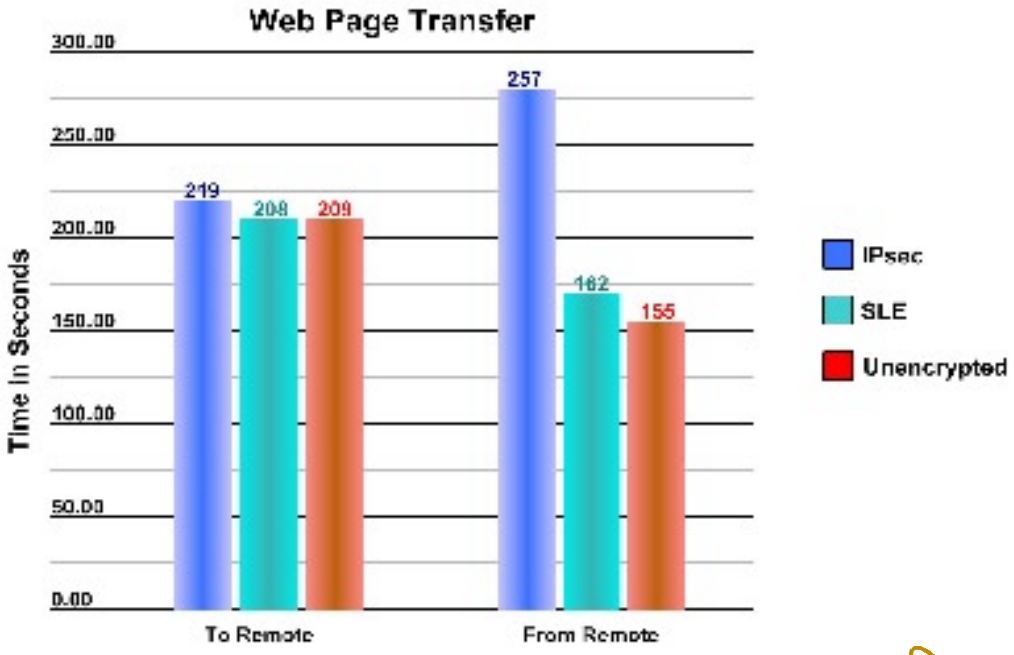
In the web page test, SLE completed the task 0.5% faster than the unencrypted circuit when moving data from the host to the remote site. Reversing direction reduced the SLE performance relative to the clear channel: SLE took 6% longer. The IPsec connection pulled down the web pages 5% slower than the unencrypted circuit going from host to remote and 66% slower when run from the remote site. As with the other graphs, the one on the next page labeled Web Page Transfers displays the mean values of five passes.

As mentioned earlier, satellite latency varies with equipment and service quality. Longer latencies, while affecting all the results, will have a more severe impact on the IPsec connection than either of the other two protocols in this test.

Conclusions

Any encryption technique over any connection imposes some performance loss. Performance also suffers as a function of increased latency. Some of the geosynchronous satellite services available today, however, have sufficiently low latencies (550 to 625 ms) that even an IPsec VPN becomes practical.

But as the results of these tests clearly indicate, IPsec encryption significantly reduces the performance of TCP/IP over a high latency connection. The Encore VSR-30 with Selective Layer Encryption technology, however, offers an efficient method to achieve fast, secure 3DES encryption when using a satellite link to access the public Internet.



skycasters