

## **VSAT Systems: The SkySecure VPN Whitepaper**

---

This VSAT Systems LLC whitepaper outlines the difficulties encountered when companies attempt to establish conventional Virtual Private Networks over a satellite link. It also outlines the steps VSAT Systems takes to eliminate or mitigate performance degradation..

Two-way satellite Internet service offers fast and reliable data transfers. All told, satellite technology works very well for browsing, e-mail, and most other Internet applications.

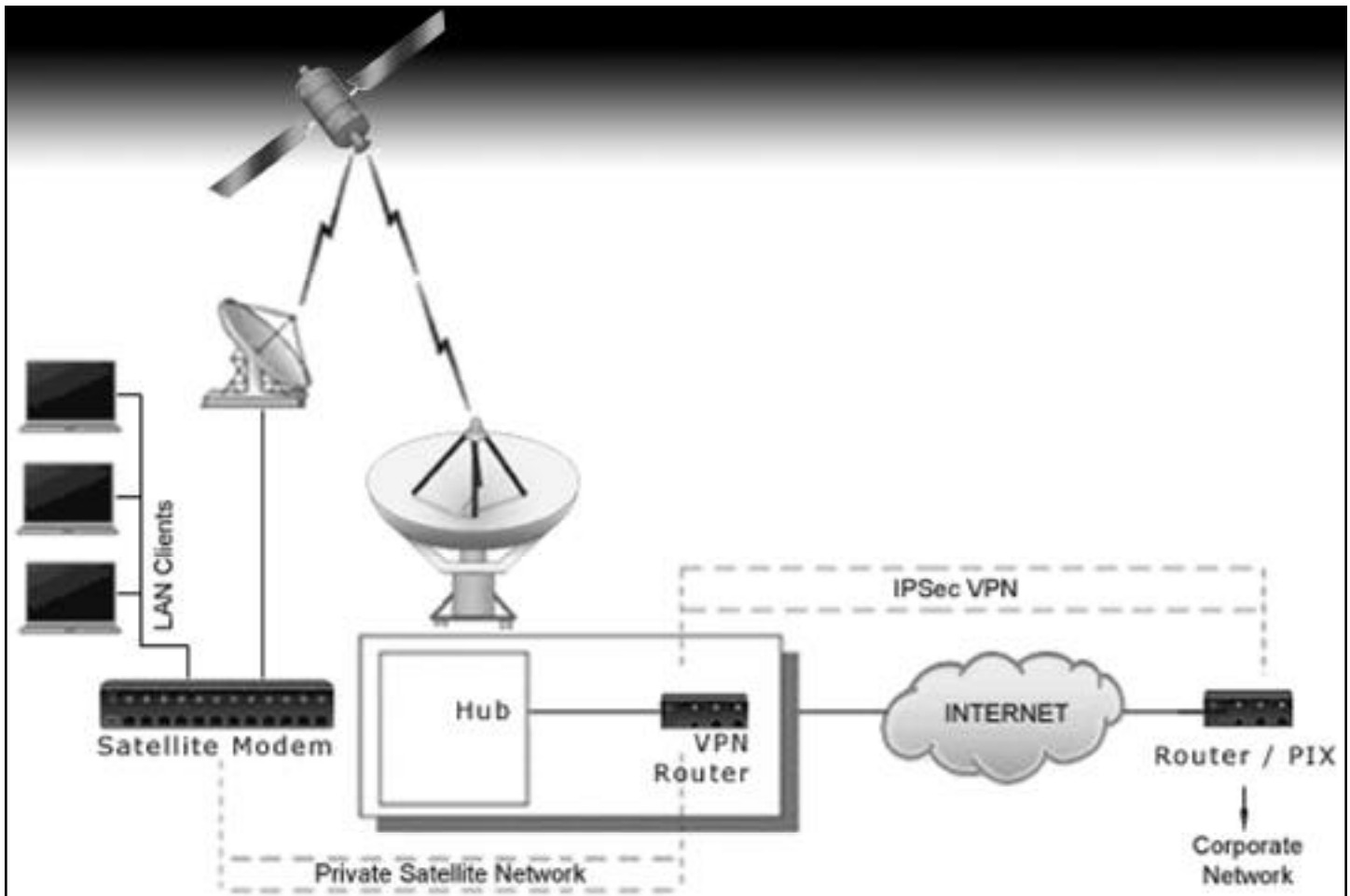
Virtual Private Networks consist of two or more computers or networks of computers that communicate securely with each other across an unsecured or public network such as the Internet. VPNs are established by using compatible encryption and decryption hardware or software at each end of the connection.

Until today, VPN has typically has a much lower performance (greater than 70 percent degradation) than traditional web browsing over the same satellite link due to factors we will be discussing here.

Today there is a growing requirement from both business and government to provide secure broadband data connections to their remote locations. Secure access at useful speed is not available with traditional dialup access and faster solutions are in ever increasing demand.

While DSL and Cable Internet are clearly the most cost effective solutions, DSL and cable do not reach a third or more of the remote locations that seek broadband service.

Enter satellites. And VSAT Systems methods for improving satellite VPN.



In order to perform properly in conjunction with traditional terrestrial networks, satellite data networks must employ special techniques to deal with the lag time caused by the 46,000 mile space segment of the connection. Even at the speed of light, it takes a few milliseconds to make this trip.

This lag time is called latency, and while not related directly to speed, latency can cause a severe speed performance problem over satellite links if not handled properly.

Here's why.

TCP/IP is the "language" of the Internet. It works by sending packets of data, and then waiting for acknowledgments of receipt. These acknowledgments signal the sender to transmit more data. If an acknowledgement does not arrive in a timely manner, TCP assumes the packet was lost or discarded due to network congestion and the packet is resent. TCP then

slows the speed at which data is being sent in order to avoid future retransmissions.

TCP works by starting a TCP/IP session slowly, and speed builds as the network's capacity to carry traffic is verified by the rate of the acknowledgments. Since TCP was designed for terrestrial networks that have less latency than a satellite network, the longer satellite latency (greater than 720ms range) causes TCP to expect an acknowledgment before the round trip to the remote site can be completed. TCP interprets this delay as network congestion, and if not corrected, this effect will cause the additional data to be sent at an ever slower rate.

In all current-generation satellite data networks, some form of IP spoofing compensates for the space-link transit time. Spoofing is accomplished by special acceleration equipment at the carrier's main satellite hub site.

---

## **Because the IP layer is left undisturbed, SkySecure offers the extra benefit of avoiding network address translation and firewall issues**

This equipment masquerades itself to the sender so as to appear as if it were the remote location, while acting as a relay or forwarder for data packets going to and from the remote satellite location.

When the spoofing equipment receives Internet traffic destined for a remote satellite location, it acknowledges receipt of the packets so more data packets will follow immediately. At the same time, the packets are forwarded to the remote site.

As “real” acknowledgments are received from the remote site, the system suppresses these acknowledgments. If the packets are not acknowledged, the system retransmits them from its buffer. In this manner, the latency is “hidden” because the acknowledgments are returned to the sender rapidly. As a result, TCP moves out of slow-start mode and builds to the highest possible speed.

In a traditional VPN-over-satellite session, the packets are encrypted and, therefore, can only be acknowledged by the VPN client software at the remote site – not by the spoofing equipment. Spoofing is bypassed, and that means acknowledgments are delayed and the slowstart data rate remains in place during the entire session. This results in substantial performance degradation.

SkySecure 3DES encryption operates at the application layer and does not encrypt the packets at the IP layer. Because the IP layer is left undisturbed, satellite TCP/IP spoofing and acceleration techniques are allowed to

function in their normal way. Thus, satellite VPN in the SkySecure example does not cause the satellite connection to suffer performance degradation.

Because the IP layer is left undisturbed, SkySecure offers the extra benefit of avoiding network address translation and firewall issues, and making use of a single port proxy to specific TCP/IP based resources.

The SkySecure server, installed in the customer’s headquarters or data center, works in conjunction with an easy-to-use SkySecure client that operates on each PC connected at the remote satellite location.

The SkySecure server allows clients to access protected services based on authenticated user identification, not on a site-to-site basis. Authentication of users, in addition to 3DES encryption, allows increased security and flexibility to network administrators.

A single-use 3DES session key is generated every time a user requests connectivity to a protected resource. SkySecure utilizes two-way authentication, meaning that not only does the SkySecure server validate the client user, but the inverse is also true. The server and client engage in a two-factor challenge/response exchange with each other to verify authenticity. A physical smartcard, virtual soft token residing on a hard drive, or biometrics device can be used with SkySecure technology. Third party authentication systems can also be integrated, including RSA SecureID®, PKCS #11, RADIUS® and LDAP.

---

## **SkySecure offers a widely deployed FIPS 140-1 validated virtual token approved for U.S. Government use.**

### **Security and Administration**

The SkySecure client, loaded on machines at remote sites, intercepts all connection requests from an end user's computing platform bound for an application running on a SkySecure protected server. The SkySecure client encrypts both session and user data with a single-use 3DES key.

After the session information is validated, a connection is made between the server and the client thereby completing the secure connection. Data packets are then forwarded to the SkySecure server at the headquarters or data center network where they are decrypted and processed. SkySecure security meets FIPS 140-1 as well as HIPAA requirements.

SkySecure interacts with a powerful, secure 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. SkySecure On-line Registration capability allows end users to securely register with the server via the Internet and begin accessing secured applications and resources within minutes.

After a user gets enabled by an administrator and launches the secure client, the secure

server pushes access permissions to the user's secure client. These read-only permissions are stored on the user's computer only for the duration of a session.

The SkySecure server loads new permissions at the beginning of each subsequent session and the system allows administrators to modify permissions in real time.

SkySecure clients run on a broad range of computing platforms including Windows, Unix, Linux and Macintosh. A Java™ version of the SkySecure client is available which eliminates the need for client software to be pre-loaded on an end users computer.

To allow secure connectivity from an end user's computing platform to a destination application, all connection requests are processed through the SkySecure client. Access to non-secure sites is not impeded. The SkySecure client only reacts to requests made to access a SkySecure protected service, in which case authentication is enforced and session and user data is encrypted with 3DES.

### **Conclusion**

By operating at the application layer and leveraging a satellite network's TCP protocol spoofing capabilities, SkySecure VPN technology is able to deliver non-degraded 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.