



**Spacenet**

---

# ***Spacenet Security over VSAT Networks***

This document contains information proprietary to Gilat Satellite Networks Ltd. and may not be reproduced in whole or in part without the express written consent of Gilat Satellite Networks Ltd. The disclosure by Gilat Satellite Networks Ltd. of information contained herein does not constitute any license or authorization to use or disclose the information, ideas or concepts presented. The contents of this document are subject to change without prior notice.

---



**Contents**

- 1. Executive Summary ..... 1**
- 2. Terrestrial Networks and Security ..... 1**
  - 2.1 Public Internet Infrastructure ..... 1
  - 2.2 Private Networks and Security ..... 2
- 3. Spacenet VSAT Networks Overview ..... 3**
  - 3.1 Spacenet – Experienced with Secure Networks ..... 3
  - 3.2 Network Architecture ..... 4
- 4. Spacenet Layer 1 Security ..... 5**
  - 4.1 Physical Barriers to Intercepting Spacenet VSATs at Layer 1 ..... 5
  - 4.2 Inbound Channel Security Through FTDMA ..... 5
- 5. Spacenet Layer 2 Security ..... 6**
  - 5.1 Creating Secure Groups Based on Layer 2 Addresses ..... 7
  - 5.2 Enforcing Groups Based on Layer 2 Unique Identification ..... 7
- 6. Spacenet Layer 3 Security ..... 7**
  - 6.1 Issues with Outbound DVB Carrier Security ..... 7
  - 6.2 DVB Security Through Strong Encryption and Compression ..... 8
- 7. User Performance with Standard Security Solutions ..... 9**
  - 7.1 Satellite Link Security with IPSec ..... 9
  - 7.2 External Hub Interfaces ..... 9
  - 7.3 Security Options for Terrestrial Connections ..... 9
  - 7.4 Unique SSL and HTTPS Acceleration Over VSAT ..... 10
- 8. Summary ..... 10**



## **1. Executive Summary**

Traditional terrestrial networking methods have long been categorized as secure or insecure link technologies. Public TCP/IP network links are known as insecure technologies, vulnerable to IP spoofing, packet sniffing and/or session hijacking attacks. Private (Frame Relay or ATM) network links, because of their architecture, are understood to provide an inherently heightened (but not foolproof) level of security against these types of attacks. IPSEC VPNs are used in conjunction with both public network links and private network links to provide an additional layer of protection for highly sensitive data.

Through a combination of factors, Spacenet's VSAT platforms network links of equal or greater security to terrestrial Frame Relay/ATM connections incorporating IPsec VPN. All Spacenet VSAT networks incorporate built-in security functions at OSI Layer 1 and Layer 2, and configurable security at Layer 3.

Spacenet's VSAT security features include:

- Inbound transmissions secured at the OSI Layer 1 level through FTDMA frequency-hopping and time-hopping, proprietary modulation and coding, and inherent infrastructure that should be established such as a large hub dish, network basement equipment and access to network parameters
- Layer 2 security and network separation are provided through VSAT grouping, VSAT IDs and access controls based on MAC addresses
- Outbound DVB transmissions secured at Layer 3 through proprietary compression and government/military-grade encryption technology
- Additional features for enabling usage of standard secure networking protocols and technologies with minimal performance degradation.

## **2. Terrestrial Networks and Security**

### **2.1 Public Internet Infrastructure**

**In a typical public Internet infrastructure scenario, data passes in unencrypted packets from gateway to gateway across point-to-point Telco links or Ethernet LANs in data centers.** As data travels between two remote locations, it will often pass through the networks of two or more Internet Service Providers, from local ISPs to backbones. In this scenario, data transmissions are vulnerable to interception or attack from a variety of methods – primarily sniffing, spoofing and session hijacking.

“Packet sniffing” involves an intruder capturing a copy of each data packet as it crosses a LAN or other link (usually done by means of compromising security on a

router or server already on the network and surreptitiously adding the “sniffer” software to it). “Spoofing” entails using low-level manipulation of TCP/IP packet headers to allow a malicious user to masquerade as a different network host (thereby intercepting data intended for the original target). By combining these two techniques, a sophisticated attacker can “hijack a session,” taking over an in-progress communication stream between two computers by masquerading as one of the two.

**As a result of these data interception risks, unencrypted use of public Internet links is considered inherently insecure and not to be trusted with sensitive commercial or government/military data.** The conventional response to this has been the development of IPsec-based VPNs and other encryption/authentication technologies (such as PGP for e-mail, or HTTPS for web traffic) to safeguard important data. However, public Internet links, because of their fundamentally insecure architecture, are still not considered to be optimally secure solutions even when VPNs or other security measures have been applied.

## **2.2 Private Networks and Security**

**Unlike public Internet links, private network technologies such as Frame Relay and ATM are typically viewed as a “secure” terrestrial broadband networking platforms.** They are also widely seen as being “mature” or “well-tested,” having been available commercially since the early 1990s.

Frame Relay and ATM were designed with several emerging telecom needs of the late ‘80s and early ‘90s in mind, including the growing importance of packet data-based LANs, reducing the protocol overhead of X.25, and interoperability with heterogeneous networking/protocols environments.

**These private networking technologies use a shared networking environment.** Rather than provisioning a circuit for full-time use by one customer, carriers provide “clouds” of capacity through which “virtual” circuits connect two points. Every packet carries a unique identifier (Frame Relay DLCI or ATM VPI) which is unique to its virtual circuit and prevents outside access, thereby creating an effectively private network within the shared cloud.

A customer maps one or more virtual circuits (Permanent Virtual Circuits, or PVCs) from their location to whichever destinations in the cloud they wish to reach (their ISP’s connection into the cloud, another office location, etc.). The “size” of PVC is measured by its Committed Information Rate (CIR). Users can receive more bandwidth than their CIR if it is available (this potential maximum is sometimes referred to as the “burst” rate), but the amount of the CIR is the minimum that they are guaranteed to receive.

These PVCs are purely logical constructs and do not represent physically dedicated bandwidth allocations; these networks handle burstability very well, since bandwidth



within the network that is not being used by one customer is therefore available to another customer.

**Because of their cloud-and-PVC architecture, these private networking technologies are widely considered to be appropriately secure platforms for Intranet and sensitive/proprietary data applications.** For high-sensitivity data requiring additional levels of protection against packet sniffing or other network intrusions (financial and medical data, etc.), IPSec and other encryption technologies can be layered on top of private networks for high-grade security able to meet the highest commercial and government standards.

### 3. Spacenet VSAT Networks Overview

#### 3.1 Spacenet – Experienced with Secure Networks

**Spacenet, a US-based company, is a Federal Communications Commission-licensed and regulated communications carrier, providing data communications services to businesses via satellite.** Spacenet utilizes VSAT (Very Small Aperture Terminal) platforms manufactured by Spacenet's parent company, international satellite hardware manufacturer Gilat. VSAT networking is widely recognized as a mature technology, having been in active use in hundreds of thousands of sites for more than 15 years.

Spacenet/Gilat's VSAT platforms – Skystar Advantage (for IP and legacy data), Skystar 360E (IP data), Faraway and Dial@way (telephony) – provide a flexible range of services and applications to meet almost any requirements. These networks serve nearly 300,000 sites worldwide, providing broadband connectivity for interactive transactions, batch file transfers, data/media broadcasts, and broadband Internet access and voice communications, among other applications. Spacenet has installed over 50,000 VSATs in the United States for companies and entities that span multiple industries such as retail petroleum, restaurant, freight, department stores, insurance, Federal and State government agencies, and the US Postal Service.

**These Spacenet VSAT installations have been used for many years by governments and leading commercial enterprises for the transmission of proprietary, secret or otherwise highly confidential data.** In nearly all of these cases, these organizations have considered Spacenet's VSAT networks to be secure enough "out of the box" to transmit their most sensitive data *without* any additional encryption/VPN measures – a recognition of Spacenet's long-standing reputation for delivering highly secure standard solutions. In those cases where additional encryption support has been requested, Spacenet has been able to integrate this security functionality into the customers' service with little or no degradation to performance.

### 3.2 Network Architecture

The “star” topology of a Spacenet VSAT network is well suited for use in configurations where corporate/government headquarters or data centers communicate with tens, hundreds or thousands of geographically dispersed locations.

A network consists of the following components:

- A master earth station and control facility, or “hub” (for redundancy purposes, a network may have multiple backup hubs)
- A number of VSATs, located at the customer's remote sites

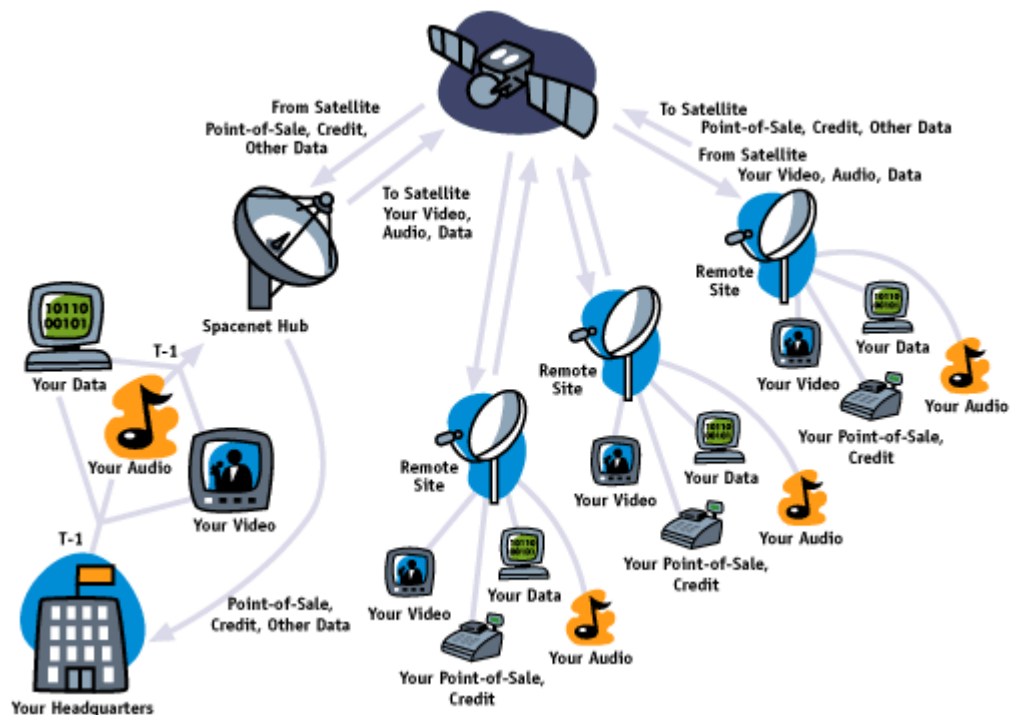


Figure 1 Typical Spacenet corporate network diagram

In a typical Spacenet network, many remote locations with end-user terminals can be connected through VSATs to a centralized processing center (hub) or to other remote locations through the hub. Data transfers are typically asymmetric, with hub-to-VSAT (“outbound”) communications having greater bandwidth available than VSAT-to-hub (“inbound”) communications. The hub consists of baseband equipment, an RF Transceiver (RFT) and an advanced object-oriented Network Management System (NMS).



## **4. Spacenet Layer 1 Security**

### **4.1 Physical Barriers to Intercepting Spacenet VSATs at Layer 1**

**It is essentially impossible to intercept Spacenet VSAT inbound transmissions, because of the physical requirements and multiple levels of time and frequency synchronization involved in the transmission/reception process.** To even attempt to intercept these transmissions, a very large receiver dish (6 meters or larger) must be used to intercept the signal. Beyond that, a potential intruder must have access to all of the physical configuration parameters (such as timing information and frequencies) on the hub. Additionally, they must also know and implement all of the proprietary modulation and channel coding algorithms used by Spacenet.

Even if an intruder is able to physically replicate the entire Spacenet hub and have access to the unique hub configuration parameters, they would not be able to intercept and decode the inbound transmissions because of each hub's unique time synchronization. This feature also ensures that different Spacenet customers cannot use their hub equipment to intercept transmissions of other customers.

It is also impossible to intercept the inbound transmissions using off-the-shelf receivers because of the proprietary burst transmissions, channel modulation, and channel coding. To overcome this, an intruder would therefore need to develop and build an entirely new system, incorporating all of the elements and parameters discussed above.

### **4.2 Inbound Channel Security through FTDMA**

**If a hostile party is able to acquire the necessary equipment/installation parameters and modulation/coding schemes to intercept Spacenet inbound transmissions, they will still face significant barriers to capturing any actual data stream because of Spacenet's unique inbound access scheme.** Using frequency-hopping mechanisms similar to those employed by military EW (Electronic Warfare) systems, the network access scheme developed by Gilat's founders (Israeli Defense Force veteran senior technologists) effectively prevents outsiders from intercepting VSAT-to-hub data transmissions.

**The Gilat VSAT inbound channel architecture is based on a patented two-dimensional (time and frequency) access scheme.** This scheme combines TDMA and FDMA to provide easy traffic expansion at a particular site without requiring extensive channel traffic loading analyses and subsequent VSAT channel balancing. The bandwidth is divided into frequency slots, while the time domain is divided into time slots. (See Figure 2 VSAT Random Access (RA) Mode

**Time synchronization ensures that only VSATs that are part of a specific network (“network members”) can communicate with the hub.** Each VSAT goes through a special process of initialization that synchronizes the VSAT to the particular hub time division methodology and frequencies. Specific parameters are defined for each VSAT so the hub can recognize each one of the network’s members. Only VSATs belonging to a particular hub can transmit and only that particular hub can receive them.

Multiple VSATs share the same satellite channel inbound bandwidth on a Time Division Multiple Access (TDMA) basis using a modified Slotted ALOHA access scheme. This is a “contention” access scheme, in which each VSAT transmits a burst at a randomly selected frequency within the available predefined bandwidth. If a collision occurs, the data packets are retransmitted immediately at an additional randomly chosen frequency on a subsequent time slot to minimize the chance of a second collision. This process of randomly choosing a frequency for each transmission is called “frequency hopping.”

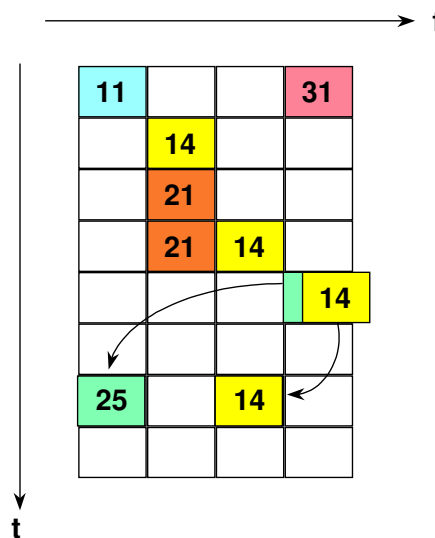


Figure 2 VSAT Random Access (RA) Mode

In addition to its security benefits, the frequency hopping mechanism also increases immunity to satellite interference. Since each VSAT can transmit over multiple frequencies, interference on a specific frequency (or group of frequencies) will not prevent the VSAT from transmitting.

## 5. Spacenet Layer 2 Security

**Spacenet’s Layer 2 security technologies, part of Spacenet’s hub architecture, ensure that multiple customer networks cannot interfere or been seen by each other (even in a shared environment), as well as restricting communications to authorized VSAT units (authenticated by VSAT ID and unique MAC address).**

This secure Layer 2 architecture also extends to the edge of the customer's private network, allowing data to pass directly from one secure environment to another.

### ***5.1 Creating Secure Groups Based on Layer 2 Addresses***

**VSATs can be grouped together on the NMS based on their Layer 2 address to form regions (each region is typically a separate customer).** VSATs within each region can communicate among themselves through an internal Layer 2 routing implemented by the Hub Basement Equipment. Traffic between VSATs on one region to VSATs in another region is automatically blocked. Customer separation is maintained towards the terrestrial lines through VLAN tagging, support of multiple routers, or VPN tunneling (see below).

### ***5.2 Enforcing Groups Based on Layer 2 Unique Identification***

**To prevent unauthorized access to network regions, groups created by the NMS can be enforced through verification of the unique Layer 2 MAC addresses of the VSATs authorized as group members.** Only VSATs identified by MAC address as being part of a network group are able to receive transmissions intended for that group.

Within the network, remote terminals are also identified by the NMS with a unique VSAT ID which is assigned when the VSAT is commissioned and added to the network. Spacenet VSAT networks are therefore not vulnerable to spoofing attacks (and hence to session hijacking attacks) because of these "anti-cloning" measures implemented in each VSAT network at the NMS level.



## ***6. Spacenet Layer 3 Security***

### ***6.1 Issues with Outbound DVB Carrier Security***

The outbound (hub uplink) direction physical layer is based on the DVB (Digital Video Broadcast) and DVB-S standards, using QPSK modulation with Viterbi and FEC coding. DVB is a mature, widely used open standard, and using DVB for the outbound layer provides performance advantages as well as easy interoperability with existing standards-based networks.

**However, DVB does not incorporate security extensions and hence the signals can be received by any DVB-compatible receiver with the appropriate physical**

**configuration.** As a result, these communications are insecure at the Layer 1 and Layer 2 levels and Spacenet has developed a solution for this issue by providing security through encryption at Layer 3.

## **6.2 DVB Security through Strong Encryption and Compression**

**Spacenet has developed an advanced outbound encryption implementation for its VSATs using the Rijndael fast symmetric encryption algorithm to ensure data security on the DVB-S outbound channel.** This algorithm is a 128-bit block cipher that was recently adopted by the National Institute of Standards and Technology (NIST) as the new Advanced Encryption Standard (AES). This new standard will replace the aging DES standard (adopted in 1977) as a Federal Information Processing Standard used by all federal agencies to protect sensitive unclassified information. This algorithm is a public algorithm designed to protect sensitive government information well into the 21st century.

A 1024-bit Diffie-Hellman public key algorithm is used to exchange symmetric keys between each VSAT and its hub. Keys are never stored physically on a hard disk or fetched from remote servers.

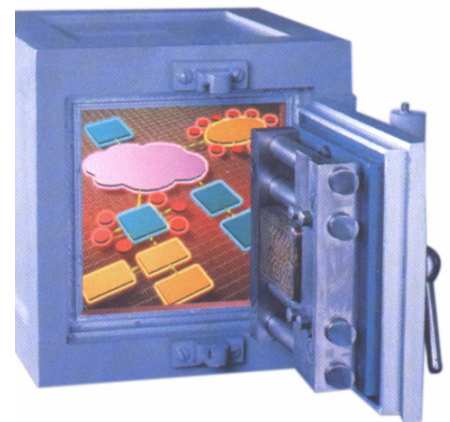
**Compression and encryption is also implemented in software on both the VSAT side and Hub Basement Equipment side.**

Spacenet NMS is used to configure compression and encryption on a network-wide basis, as well as on each individual VSAT.

Upon initial end-to-end connection across the network, the VSATs initiate an encryption key exchange using the public key algorithm with the hub.

After successfully exchanging keys, the hub compresses and encrypts outbound all user data or selected TCP sockets. In addition, the VSAT can compress all inbound user data or selected TCP sockets. The NMS allows selection of sockets for each VSAT in the network based on IP address, IP subnet mask, and a TCP port range. The NMS is also capable of enabling or disabling compression and encryption network-wide.

**Spacenet's fully configurable encryption methodology also allows clients to dynamically balance their network performance (throughput) against various levels of security – for example, customers can choose encryption optimized for maximum security (Rijndael) or a reduced run-time version optimized for throughput.** This choice may also be applied selectively, based on the selected TCP sockets.





## **7. User Performance with Standard Security Solutions**

In addition to the built-in Layer 1-3 security technologies in Spacenet's VSAT communications, additional services are available for implementing or accelerating secure interconnectivity solutions.

### **7.1 Satellite Link Security with IPSec**

**When additional security is required above and beyond that offered by Spacenet's standard VSAT service, Spacenet can implement IPSec-based encryption on top of the VSAT network – with little or no performance degradation.** Gilat/Spacenet is the leader in developing technology to add this additional high security layer with no significant decrease in performance.

This technology may be implemented in several forms, from software solutions (acting as a shim in the Win32 TCP/IP stack) to external hardware solutions. Additional information on our advanced IPSec-over-VSAT technology work is available from authorized Spacenet personnel and will be covered in-depth in a forthcoming technical document.

### **7.2 External Hub Interfaces**

**The nature of security for the link from the hub to the customer's network is determined by the architecture and type of the customer-hub connection.** The three common scenarios are:

- a) VSAT traffic is forwarded to a customer's Frame-Relay or ATM cloud via direct VLAN to PVC mapping.
- b) VSAT traffic is forwarded to the customer's network via a dedicated router and backhaul.
- c) VSAT traffic is forwarded via VPN directly to the public Internet.

### **7.3 Security Options for Terrestrial Connections**

Spacenet customers can choose to operate their own hub or (more typically) use Spacenet's existing hub infrastructure. Customers may choose to provision their own terrestrial connectivity to their hub or may elect to have Spacenet to manage these services. Spacenet hubs can support a wide range of terrestrial connectivity options, including frame relay, ATM, or point-to-point connections of any size (as well as using security mechanisms of any type).

If the customer is using Spacenet hub infrastructure and is using public Internet links for connectivity between the Spacenet hub and the customer central data center,



Spacenet can provide “secure backhaul” service for added security. Through this service, an IPSEC VPN tunnel is created between the Spacenet hub and the customer location for end-to-end data security; customers may manage their own backhaul VPN or may choose for Spacenet to provide VPN maintenance as well as setup, equipment and maintenance.

#### **7.4 Unique SSL and HTTPS Acceleration over VSAT**

**Spacenet, unlike competing VSAT providers, is also able to easily interoperate with the common web security standards SSL (Secure Sockets Layer) and HTTPS (Hypertext Transfer Protocol – Secure) without any significant loss of performance.** Through the use of proprietary Gilat technology, Spacenet is able to effectively accelerate SSL/HTTPS web transactions through the initiation of separate SSL sessions on the user PC/VSAT and Hub Basement Equipment/remote site sides of the satellite link. This technology provides high levels of latency reduction, and also includes solutions for SSL certificate generation so that users do not receive certificate authentication warnings.

### **8. Summary**

All Spacenet VSAT networks employ a broad variety of encryption, frequency and packet obfuscation, and other techniques to provide a secure broadband networking environment. Together with Spacenet’s terrestrial and hub-based data security technologies, the combined effect is to provide communications with security that is equal or greater than that of traditionally “secure” terrestrial networking platforms such as Frame Relay. Spacenet’s VSAT networks have been recognized for many years by large commercial and government customers as mature, secure solutions that have stood the test of time.

With Spacenet’s unique inbound frequency-hopping multiple access scheme, VSATs burst inbound at randomly selected frequencies – making it essentially impossible for outsiders (even with Spacenet equipment) to piece together an entire data stream. Proprietary MSK modulation and channel coding are also used for additional inbound data transmission security. Spacenet’s design for protected outbound DVB employs advanced Rijndael encryption, rendering any attempt to decrypt an intercepted signal into such a computationally intensive task as to be functionally useless. Spacenet shared hubs can separate private address networks at layer 2 for security, and hub-to-datacenter connections via VPN or Frame Relay complete the end-to-end security model.

Beyond these elements which are part of the basic Spacenet VSAT network architecture, additional security can be added to a network in the form of IPsec encryption – and Spacenet’s efforts in implementing IPsec over VSAT without performance degradation are unmatched by any competing service. Together, these



**Spacenet**

measures make Spacenet VSAT networks true high-security solutions for corporate, government or military communications networks.