CONNECT | MANAGE | PROTECT

WHITE PAPER:

SageNet VSAT Security Features and Technology

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com

VSATSecurityWP060321

CONNECT | MANAGE | PROTECT

INTRODUCTION

Organizations in every industry must meet network security requirements to protect critical data transmissions. Security threats can impact bottom-line profitability, can compromise customer and stakeholder confidence and can affect an organization's viability. In addition, industry regulations require that enterprise and government organizations protect against interception of commercially sensitive data pertaining to its customers and business partners.

Many organizations depend on SageNet to provide satellite, wireless and wireline communication networks to support their mission-critical data, video and voice applications. SageNet has over 30 years' experience supplying satellite-based Very Small Aperture Terminal (VSAT) networks to security-conscious enterprise and government customers to meet their security requirements. SageNet's security solutions cover the transportation of data at all network levels to provide a full security suite to our customers.

This white paper provides an overview of SageNet's security advantages for satellite-based VSAT networks as well as networks supporting wireline and wireless communications, including:

- Network Security
- Transmission Security
- AES Encryption
- Accelerated VPN and VLAN Tagging
- Physical Teleport Security
- Level 1 PCI DSS Compliance

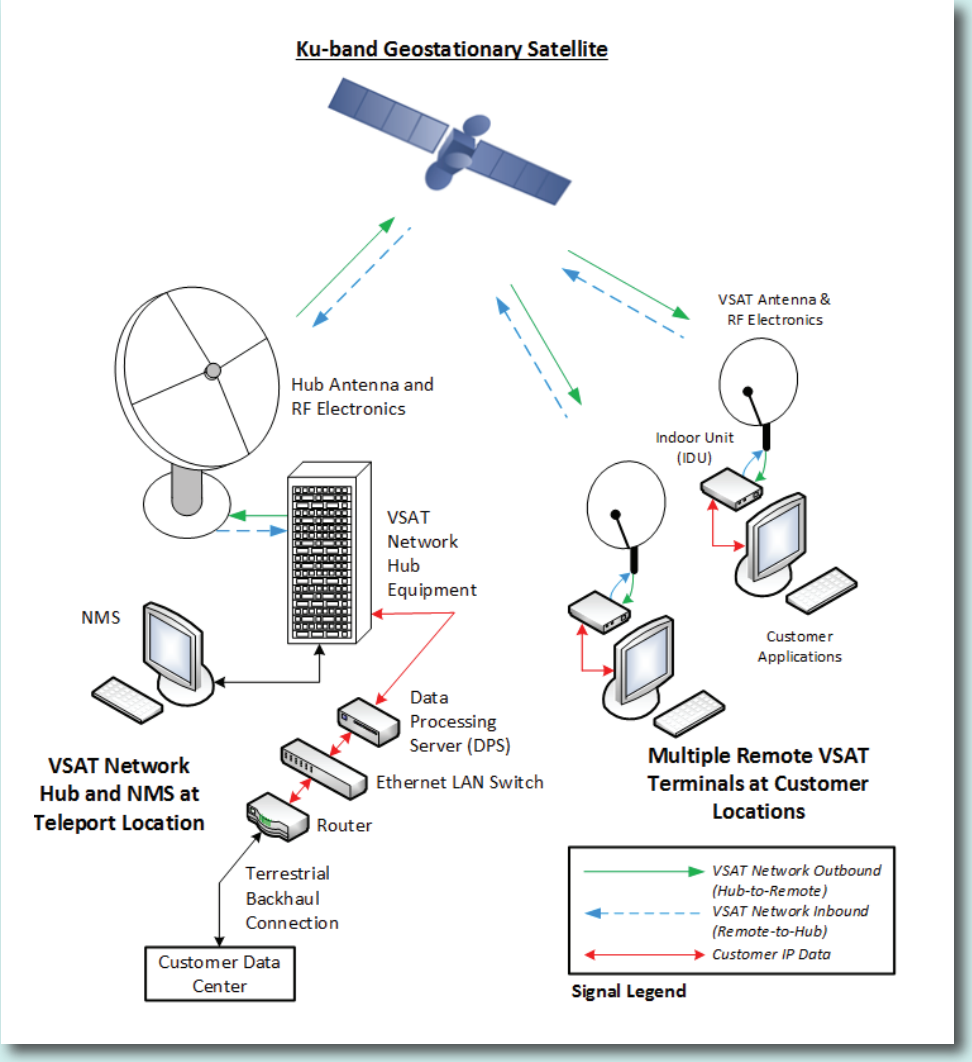
SAGENET NETWORK SECURITY FEATURES AND TECHNOLOGY

SageNet's satellite network solutions offer security advantages over competing technologies, including wireline networks, since VSAT networks can be a completely private network that does not need to traverse the public Internet. In a typical public Internet infrastructure scenario, data passes in unencrypted packets from gateway to gateway across point-to-point telco links or Ethernet Local Area Networks (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 (ISPs) from the local ISPs to high-capacity Internet backbones. In this scenario, unencrypted data transmissions are vulnerable to interception or attack from a variety of methods – primarily sniffing, spoofing and session hijacking.

As a result of the 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. To safeguard important 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. However, because public Internet links provide a fundamentally insecure architecture, they are still not considered to be optimally secure solutions even when VPNs or other security measures have been applied.

The below figure shows a typical SageNet VSAT network implementation of a hub earth station at a SageNet teleport connected to multiple remote VSAT earth station terminals at customer locations operating with a geostationary satellite. Since the assigned VSAT network geostationary satellite remains fixed relative to the earth's rotation, SageNet's VSAT networks do not require the remote VSAT terminals to track the satellite position. The remote VSATs typically use a 1.2-meter diameter antenna.

Typical SageNet VSAT Network Diagram



TELEPORT SECURITY

SageNet owns and operates secure teleports in Marietta, GA and Chicago, IL and also offers teleport services via a partner in Santa Paula, CA. Each teleport location supports Ku-band satellite VSAT network services focused on what it does best and its key competencies:

- The Chicago, IL teleport has a proven track record for reliable legacy platform hub operations and data center support services.
- The Marietta, GA teleport uses state-of-the-art technology to maintain high availability hub services for tens of thousands of remote VSATs supporting all generations of VSAT technology and equipment hosting and data center support services.
- The Santa Paula, CA teleport offers geographic diverse hub services in a dry location for increased network availability.

SageNet Teleport Security Features

- Biometric security protection
- State-of-the-art power generation with uninterruptible power supply
- Parallel diverse vendor and path backhaul connectivity
- Modern fire-suppression
- Hot & cold standby equipment redundancy features

SageNet's three teleport facilities contain multiple levels of security. All facilities have cameras located on the exterior of the building. Everyone gaining access to the facility is met at the door and all visitors must sign in and out of the facility. Additionally, the teleport facility is gated, locked and manned with technical support personnel 24 hours a day, seven days a week and 365 days a year.

Critical large Ku-band hub antenna installations at the teleports are protected by high fences and are capable of withstanding hurricane force winds and several feet of flood waters. All hub building access is controlled externally by card key access and again at the entrance to critical Network Management Centers (NMCs). Access to the NMCs is limited to authorized personnel only. Each location utilizes the combined approach of pre-action sprinkler systems and FM200 for fire protection and prevention.

VSAT TECHNOLOGY OVERVIEW

Physical Layer (Layer 1)

At the physical layer, security is implemented through network specific and secure Ku-band radio frequency transmission plans, modulation and coding schemes supporting satellite connections for the outbound (hub-to-remote) and inbound (remote-to-hub) links. Proprietary data scrambling in the modulator and descrambling in the demodulator is also implemented in all VSAT networks. The SageNet VSAT network physical layer complies with ETSI DVB-S2 or DVB-S2X standard for the outbound and DVB-RCS for the inbound link. Due to the secure radio frequency link characteristics, it is very difficult for a rogue element to join the network, but theoretically possible. Further security and privacy are provided at the data link layer to address potential security threats.

Data Link Layer (Layer 2)

Authentication is performed at the data link layer. Each remote VSAT IDU authenticates with the VSAT Network Management System (NMS) at the hub using its Ethernet port MAC address. The NMS is updated with the VSAT MAC address either manually or automatically during the VSAT commissioning process. If authentication fails, the remote VSAT turns off inbound data transmissions toward the satellite and disables LAN data transmission and reception. If authentication succeeds, the remote VSAT can have full network access, or restricted access, as configured by the network operator. The authentication of each VSAT transmitting and receiving data over the satellite network provides proof of the integrity and origin of customer data. This provides a high level of assurance that data being transmitted or received by a remote VSAT terminal is genuine.

VSAT network data transmitted over the satellite does not contain the source IP address and destination IP address of each packet; it contains only a unique VSAT identification (ID) and a session identifier that is dynamically built when two end devices start to communicate. Ethernet, IP addresses and TCP/UDP headers are removed from the user data packets and fragmented into transmission blocks with each transmission block encapsulated by a proprietary frame. The SageNet available 256-bit AES encryption feature is embedded in the hub and the VSAT software, providing bi-directional unicast and multicast encryption.

AES Encryption

SageNet's data encryption solution is a complete integrated sub-system that provides enhanced security without compromising performance and bandwidth efficiency. The SageNet encryption solution is embedded in the software in the SageNet provided hub baseband equipment and remote VSAT terminals. The SageNet VSAT network encryption solution uses dedicated hardware-based modules that work in conjunction with the TCP and HTTP acceleration modules to mitigate the latency challenges that may be encountered by geostationary satellite communication networks.

The SageNet encryption solution is based on the Advanced Encryption Standard (AES) from the National Institute of Standards and Technology (NIST) under FIPS 197 that standardized encryption on the Rijndael algorithm. AES is currently one of the most popular standards implemented for symmetric encryption. The SageNet offered encryption solution provides two main functions:

- **Encryption of user data traffic** – Supports encryption of all customer unicast and multicast traffic between the hub Data Processing Servers (DPS) at the SageNet teleport and remote VSAT Indoor Units (IDUs) at the customer locations.
- **Encryption key management** – Supports all functions that are responsible for generation, periodic refresh, exchanging, and distribution of encryption keys between the remote VSAT IDUs and the hub baseband equipment at the SageNet teleport facility.

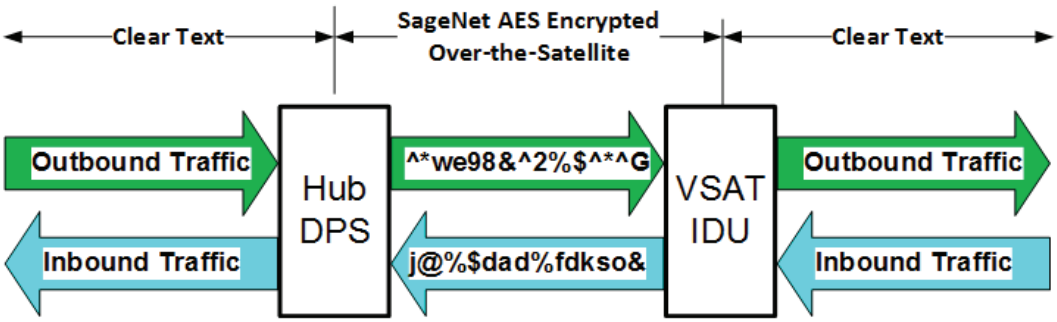
Available Security Features

- AES 256-bit encryption
- Support for bi-directional unicast and multicast encryption
- Key management protocol for automatic generation and periodic refreshing of multicast and unicast session keys
- Powerful dedicated hardware-based encryption processor module at the SageNet teleport hub
- Embedded hardware-based encryption engine at each remote VSAT IDU
- Integrated TCP and HTTP acceleration
- VSAT IDU IPsec Client, ACL firewall and X.509 terminal authentication

VSAT network encryption is implemented between the Data Processing Server (DPS) at the hub and the remote VSAT IDUs at the customer locations enabling encryption of all user data traffic - inbound and outbound connections, unicast and multicast applications - transmitted over the VSAT network satellite links. The basic encryption operational principle is that once customer data traffic enters the VSAT network, at both the hub and remote locations, it is encrypted before being transmitted over the satellite link. On the receiving side, the customer traffic is decrypted and is forwarded out of the VSAT network to the destination.

The SageNet VSAT network encryption solution also supports a hybrid network configuration where some VSATs are operating in a secure mode (encryption is enabled) while others are not (encryption is disabled). To achieve high throughput the implementation of encryption is based on hardware encryption engines that perform all necessary cryptographic operations. At the remote VSAT terminals all cryptographic operations are performed in the embedded security engine hardware chip in the VSAT IDU. At the VSAT network hub, each Data Processing Server (DPS) module has a hardware security engine available to support encryption.

Encryption Solution Concept



When a remote VSAT terminal is configured to operate in a secure mode, all customer data traffic that is transmitted over-the-satellite interface is encrypted. Following the VSAT network Layer-2 Link-Connect process, the remote VSAT initiates a procedure to exchange with the hub DPS module all the necessary parameters to secure Layer-3 communications (this group of parameters is called “SA” or Security Association). The following actions occur during this process:

- The remote VSAT and the hub DPS exchange a unicast encryption key using Diffie-Hellman algorithm, which enables two parties to exchange a shared secret (i.e. encryption key) over a non-secure medium. The encryption key is unique per remote VSAT terminal.
- The remote VSAT sends to the hub DPS the encryption key lifetime, which determines how long a key will be used. When the key period expires the remote VSAT initiates a Security Association (SA) refresh procedure to exchange a new key with the hub DPS.
- For multicast applications the hub DPS sends to the remote VSAT a broadcast key, which is used by the hub DPS to encrypt multicast keys before they are transmitted to all remote VSATs scheduled to receive the multicast transmission. The multicast keys are used to encrypt outbound multicast packets.

Shortly before the unicast key expires, the remote VSAT initiates a procedure to exchange a new unicast key with the hub DPS – as done in the initialization procedure. The unicast encryption key is used to encrypt all unicast and inbound multicast customer traffic between a remote VSAT and the hub DPS. When operating in secure mode, customer traffic can pass only after both hub and remote VSAT locations have valid keys. If, for any reason, a key is not valid then both the remote VSAT and hub DPS block customer data traffic over the VSAT satellite network.

VLAN Tagging

Virtual Local Area Networks (VLANs) provide additional flexibility and security to SageNet's VSAT networks.

The VLAN Challenges and Solutions

SageNet's customers operating with shared VSAT network resources need to be isolated from other shared VSAT network customers as if each had their own secure, point-to-point connection through the common media. This situation presents many technical and administration problems, some of which are addressed in this section.

Duplicate IP Addresses

Unless all IP addresses are unique, data can be duplicated and/or corrupted. How do you ensure no two devices in the different departments and companies sharing the VSAT hub do not have duplicate IP addresses?

One way is to enforce an IP address numbering scheme. However, this may be unacceptable for some customers who already have their private IP address mapping structure in place. SageNet's answer is to support end-to-end IEEE 802.1q tagging, which gives each VLAN a unique identity. Now, duplicate IP addresses can coexist in the system when assigned to different VLANs.

Tagged Mode

In the tagged mode, the remote VSAT adds a VLAN tag based on a predefined configuration from the VSAT Network Management System (NMS). This mode is used to create groups of remote VSATs, with each group associated to a different VLAN ID. The VLAN tagging provides complete separation between two or more remote VSAT groups, so each group can be associated to totally different customers.

Furthermore, each remote VSAT can be configured to support multiple Virtual Routing and Forwarding (VRF) configurations with each one utilizing a different VLAN. This allows multiple entities to share a single remote VSAT IDU by running different applications on separate VSAT LAN interfaces, while allowing duplicate IP addresses between the different LAN segments of a single VSAT IDU. An example of a typical implementation where this is useful is where one remote VSAT IDU LAN port supports a customer's corporate network applications. On the same remote VSAT IDU, a second LAN port supports the customer's vendors that require secure connectivity for their applications, but the vendors are not allowed access to the customer's corporate LAN segment. SageNet offers several different VSAT IDU models that support multiple 10/100/1000 Base-T (RJ-45) Ethernet LAN ports capable of IEEE 802.1q VLAN tagging.

At the VSAT network hub, a VLAN switch separates the IP traffic into different physical Network Interface Cards (NICs) according to the VLAN tagging scheme. The VLAN switch is connected to the VSAT network hub by a single LAN segment using VLAN tagging. There can be multiple virtual LANs on the customer facing side of the VSAT network hub VLAN switch. At the hub, the VLAN switch segment facing the VSAT network baseband equipment (typically the VSAT network DPS) supports multiple physical LAN segments - each of which is a virtual LAN on the VSAT network. Thus, the VLAN switch provides a physical separation between different customer networks and equipment at the VSAT network hub. This enables multiple VLANs belonging to multiple different SageNet customers to share hub VSAT network components and satellite space segment in a shared and secure VSAT network implementation. SageNet also offers customers VSAT network services with dedicated VSAT network hub components and satellite space segment resources.

Central System Administration

Data networks are dynamic, continually evolving to meet the requirements of new customer applications, added nodes and services. SageNet's unique NMS enables central configuration, reconfiguration and management of every network component, which is a compelling benefit for most VSAT networks.

Central Management of All Remote VSAT IDUs in the Network

SageNet's hub-based NMS provides a central management system for the VSAT network. Remote VSAT IDUs are frequently installed at locations without personnel with technical expertise. When VSAT network configuration changes are needed, the changes must be executed on all or some of the remote VSAT network IDUs using the NMS located at a SageNet teleport facility. As the number of remote VSATs in a network is typically large (hundreds to thousands), it is not practical to modify the configuration of the remote VSAT IDUs one at a time using the NMS. Fortunately, the SageNet VSAT network NMS can update the remote VSAT IDU configuration by customer designated groups of remote VSAT IDUs. Here are a few examples where group-based configuration updates are useful: firewall rules, Quality of Service (QoS) configuration, routing protocol configuration and many more.

Dynamic IP Addresses

One requirement in IP data communication networks is the ability to dynamically assign IP addresses on demand without administrative intervention. SageNet VSAT networks support two methods:

- **DHCP Relay** - The remote VSATs relay all requests from their local DHCP clients to a DHCP server in the network located at the VSAT network hub.
- **Embedded DHCP Support** - Embedded DHCP servers in the remote VSAT IDUs provide the IP addresses based on a list that was provided to each remote VSAT's DHCP server from the NMS.

PAYMENT CARD INDUSTRY SECURITY REQUIREMENTS

The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding credit cardholder information for all credit card brands. The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites, mobile applications and retail POS systems that process credit cards over the Internet.

SageNet's satellite VSAT networks, managed wireline networks, and data centers that require PCI DSS compliance have undergone a PCI DSS assessment as a Level I service provider since 2009 and continue to be assessed and certified annually. For years, SageNet's networks have been trusted by many of the world's largest retailers for mission-critical transactions. PCI certification provides an additional layer of confidence to SageNet's customers in the retail, hospitality, financial services industries, or any customer application supporting financial transactions. SageNet's PCI-compliant network architecture helps companies meet network requirements and ensures a trusted and secure managed application routing environment.

In addition, SageNet is an active member of the PCI Security Standards Council and participates in the development of the latest payment card security standards from the Council. As a Participating Organization, SageNet is adding its voice to the process and ensuring that the SageNet-provided satellite based VSAT networks, wireline networks, wireless networks and hybrid networks will meet the highest standards set for payment card data security.

CONCLUSION

SageNet has more than 30 years of experience supplying satellite and hybrid networks to security-conscious business and government organizations as well as a long history of providing secure solutions that meet or exceed customer and industry standards. SageNet's customers rely on their networks to securely transport mission critical application data to and from multiple locations. The applications transported over these networks are as varied as the industries our customers represent and include nightly polling, help desk remote control, content delivery, streaming video, SCADA, M2M, IoT, credit/debit, check authorization, automatic teller machine transactions, inventory management, interactive distance learning and Internet/Intranet access. SageNet assures the highest standards for consistent ongoing service and availability, and through our advanced technology features, SageNet provides customers the highest level of network security and reliability.

About SageNet

SageNet today is the result of the 2013 merger between SageNet of Tulsa, LLC (founded in 1998) and Spacenet Inc (founded in 1981). With a rich history of innovation, SageNet has a track record of intelligent growth, both organic and through acquisition.

SageNet is a leading managed services provider specializing in connectivity, cybersecurity and digital signage. The company connects, manages and protects technologies and devices across widely distributed enterprises. SageNet's people, processes and technologies, coupled with its collaborative approach, empowers customers to achieve their core business objectives.

The company offers world-class service and support via its US-based 24/7/365 Network Operations Centers (NOCs) and Security Operations Centers (SOCs), geographically diverse teleports, a central National Logistics Center, multiple data centers, and a nationwide field service organization.

What makes SageNet unique is its Why: SageNet is passionate about Trusted Connections. This is a two-fold calling. First, the company creates trusted, reliable and secure technological connections for its customers. Second, and perhaps even more importantly, SageNet works tirelessly to build trusted human connections with its customers, partners and communities. The company believes that by creating, discovering and nurturing these trusted connections, SageNet enhances the world that connects us all.

With a three-decade track record in managed services, SageNet boasts a long-term customer base that includes the nation's largest retail, financial, healthcare, utilities and energy organizations. SageNet manages communications for more than 220,000 endpoints. Headquartered in Tulsa, SageNet has regional offices in Washington, D.C., Atlanta, Philadelphia, and Chicago.