



Best Practices: The Key Things You Need to Know Now About Secure Networking

Layer 1 (SONET), Layer 2 (ATM), and Layer 3 (IP) Encryption Technologies

Reaching a Balance Between Communications and Security

Threats to high-speed communications, and the sensitive data they carry, have reached a critical point, with the threats rapidly escalating in sophistication and frequency over the last several years. The loss of sensitive data has a significant economic impact. According to recent studies by the FBI and the American Society for Industrial Security, each data attack costs an organization between \$150,000 and \$400,000, with multiple attacks driving these costs into the millions of dollars per year.

The need for a secure networking environment is obvious and vital. However, enterprises have other needs to consider. At the top of this list is speed — as network users and transactions grow, so does the need for faster connectivity and processing to support data communication between headquarters and core sites. Ultimately, companies require high-speed communication channels that provide high availability, dependable quality of service, and low latency in order to support their operational processes, as well as their continuity of services planning.

Reaching the appropriate balance between enabling communication and providing adequate protection of sensitive information is one of the most significant challenges faced by today's enterprise network and security engineering groups.

SafeNet's innovative approach to obtaining this balance is through the application of security solutions that offer the flexibility to encrypt data at the Physical (Layer 1), Data Link (Layer 2), and Network (Layer 3) layers. By providing three layers of security, organizations have alternatives for protecting information without disrupting existing infrastructure and systems.

The High-Speed Network Security Challenge

The geographically disparate operations of multi-national corporations are well known, however the majority of medium and large enterprises also have networks comprised of partners, suppliers, and customers residing outside geographic and national borders. This global explosion of collaboration has saturated nearly every aspect of modern business with staggering economic implications and corresponding demands upon “the network” – the critical infrastructure upon which their business survival depends. Widely dispersed networks are more vulnerable than protected local networks. Additionally, the security and auditing methods employed to meet regulatory requirements must be extended over the widely dispersed networks in order to maintain regulatory compliance. This all results in the necessity for transparent high-speed encryption wherever there are high-speed data communications.

Although bandwidth is readily available, Service Providers do not provide data integrity for high-speed communication. Their solution has been to address security through traffic isolation or data separation. This minimal level of privacy does not protect against data disclosure caused by equipment failure, eavesdropping at switching and routing points, network misconfiguration, and so forth. Further, when multiple carriers are required to deliver regional, national, and global communications, there is generally no accountability or trust applied to the security of the end users’ data.

The best solution for data integrity is encryption—specifically, solutions designed to provide the *high speed, secure, trusted, and reliable* flow of information. Finance, government, medical, research, utility, and communications companies, to name a few, are challenged to find a high-speed encryption solution for data integrity that is effective, easy to deploy, and addresses the most common applications for high-speed communications.

Common Applications for High-Speed Communications	
Wide Area Networks (WANs)	Interconnect today’s geographically dispersed server farms and data centers while providing the backbone for high-speed Local Area Networks (LANs) or switched internetworks used to operate high bandwidth applications, such as multimedia and video conferencing.
Metropolitan Area Networks (MANs)	Serves a role similar to an Internet Service Provider (ISP), but for a consortium of users or partners providing a high-speed captive network for sharing resources, creating corporate campuses, and establishing transparent LAN applications.
Storage Area Network (SANs)	Interconnects data storage facilities or associated data servers on behalf of a large network of users. Typically, an overall solution for high-speed computing resources providing services such as VoIP (Voice over IP) aggregation, Triple Play (voice/data/video), Ethernet Video, or Wireless LANs.
Disaster Recovery	Utilizes WAN technologies to implement a high-speed, purpose-built network for the remote backup, storage, and immediate recovery of data, providing businesses with continuity of operations so that they may open their doors “the day after.”

Using the Right Encryption Technology

Factors to be considered when designing security into network architectures include the applications to be implemented, their corresponding performance requirements, the circumstances under which they will be used (WAN, MAN, SAN, etc.), and last, but clearly not least, the nature of the data itself.

Choices for network services vary from high-speed options such as ATM and/or SONET/SDH to the lease or purchase of their own fiber or private line facilities. Lower speed services are offered as Frame Relay, Internet Protocol (IP), or MultiProtocol Label Switching (MPLS) services.

Encryption solutions for Layer 1 and Layer 2 (Link, ATM, Frame Relay, and SONET/SDH solutions) are designed to secure static connections, such as site-to-site core office connections (for example, connecting a corporate office with its manufacturing facility or offshore development team).

IPSec is most commonly used to secure communications across public IP and MPLS networks (Layer 3). IPSec's strength is in its flexibility – by being both protocol and network independent. The downside to IPSec technology is an overhead burden on the network (that can be, in extreme cases, in excess of 50%), as well as its complex administration requirements.

Each of the encryption solutions serves a different purpose. Layer 1 and Layer 2 solutions are designed for high-speed inter-network connectivity. IPSec (Layer 3) is a bridging technology best suited to connecting many sites to one another across the Internet.

Enterprises will best serve their security needs by incorporating multiple encryption technologies – selecting the appropriate technology for each application. This will maximize network throughput, control security costs, simplify security management, and deliver a “best-of-breed” solution.

Layer 1 and Layer 2 encryption have the following characteristics in comparison to IPSec (Layer 3):

Performance	<ul style="list-style-type: none">▪ Most organizations carefully monitor the utilization of the network infrastructure, as building excess capacity has a direct impact on the cost of the service provisioned. Therefore, anything that increases bandwidth utilization needs to have a clear business case to support it. One of the side effects of the introduction of IPSec is the increase in overhead on the IP packets. This is dependent upon the packet size, which can be as much as 50% for small packets. VoIP introduces a large number of small packets and, for this reason, any organization that is planning its implementation needs to consider this issue carefully.▪ In certain network environments, the increase in packet size may lead to packet fragmentation, which may cause network performance issues.▪ Layer 1 and Layer 2 encryption introduces virtually no latency or overhead to the network.
--------------------	---

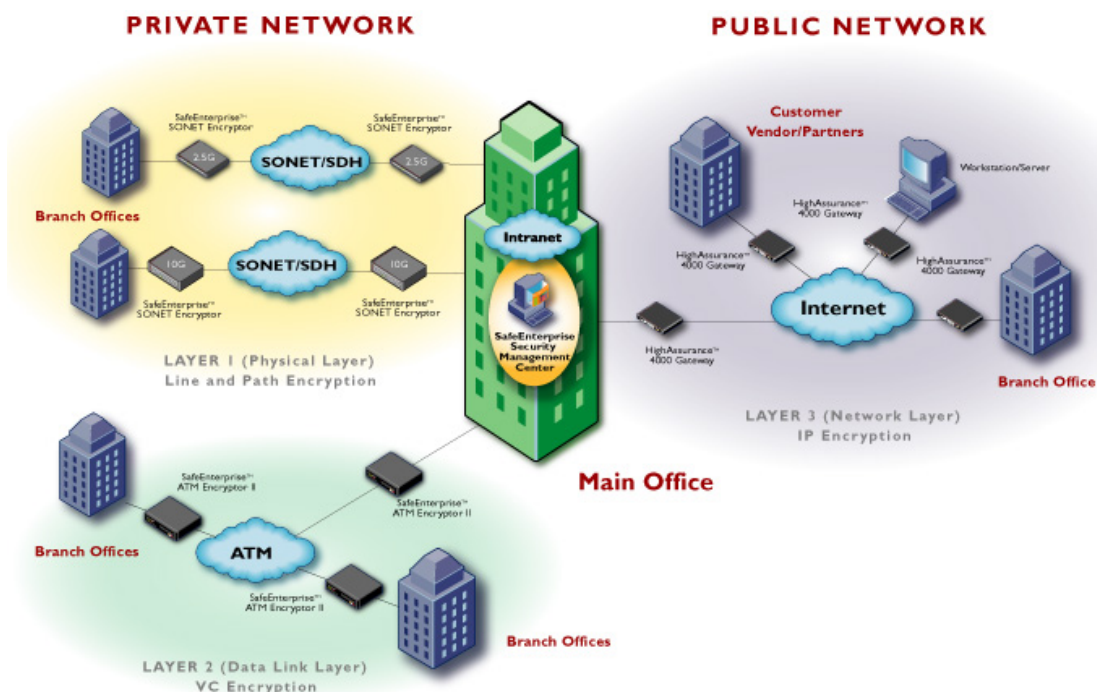
Ease of Implementation and Ongoing Management	Due to the more static nature of Layer 1 and Layer 2 connections, the implementation of these encryption devices is typically “set and forget.” They are sometimes referred to as “bumps in the wire.” Once installed, they usually require little, if any, ongoing configuration and maintenance.
Depth of Security	<ul style="list-style-type: none"> ▪ Due to its nature, this capability is nearly always implemented in highly secured hardware (FIPS 140-1 or 140-2 and/or Common Criteria 4+ Certified), and is configured once by a trusted employee, which means there is no way to bypass the connection and get information out in the clear. ▪ New encryption standards, such as AES 256, are implemented. ▪ It supports higher throughputs, such as OC192/STM64 (10Gbps).

IPSec (Layer 3) encryption has the following characteristics in comparison to Layer 1 and Layer 2 encryption:

Support for Diverse Networks	<ul style="list-style-type: none"> ▪ Has the inherent capability to supply access to other locations. ▪ Provides the ability to secure traffic in a highly selective manner. ▪ Allows the enforcement policy in a flexible and in-depth manner in order to satisfy the most stringent of fixed-site security requirements.
Commonality of Implementation	<ul style="list-style-type: none"> ▪ As IPSec is inherently a Layer 3 service, it is independent of Layer 1 and Layer 2 configurations and link types. ▪ A common method of implementation can be used across all connection types.
Depth of Security	<ul style="list-style-type: none"> ▪ The encryption occurs closer to the application. ▪ A well-understood and proven interoperability with most vendors. ▪ Rigorous scrutiny of IPSec and key exchange ensures a high level of security.

World's Only Complete Family of Encryption Solutions—from Layer 1 to Layer 3

SafeNet has developed the world's only complete family of devices for encrypting high-speed communications. Wirespeed performance, scalability, and quality of service provide operational integrity without impacting the network architecture or degrading bandwidth utilization. Customers are no longer forced to utilize inherently unsecure solutions for high-speed communications.



SafeNet's SafeEnterprise™ SONET (Layer 1) and ATM (Layer 2) Encryptors leverage fixed-frame protocols for reduced overhead and extremely low latency by offering the fastest encryption line rates on the market. Our SONET/SDH encryption scheme adds no overhead, compared to as much as 50% encryption overhead required by higher layer encryption schemes, such as IPSec, and is compatible with the majority of fiber infrastructures around the world. Available at very high speeds (OC-48/STM16 and OC-192/STM64), SafeNet SONET Encryptors provide simple, secure, and extremely fast site-to-site security, and are the ideal solution for time-sensitive, high-bandwidth applications, such as voice and video, disaster recovery, and site-to-site communications.

Our purpose-built, dedicated HighAssurance™ 4000 IPSec (Layer 3) Gateway provides better performance and security than router-based solutions because the hardware is dedicated to data encryption functions and is secured from external intervention, contrary to the intended purpose of a router. The benefits of SafeNet's dedicated IPSec security appliance versus integrated solutions include separation of security policy from networking policies, higher throughput values, lower cost of ownership over time, and higher levels of security and assurance.

SafeNet also offers Layer 2 (Frame Relay and ATM) security solutions that are compatible with MPLS (Layer 3) networks. These solutions provide low latency throughput, virtually no overhead, making best use of the available bandwidth, and have easy to manage configuration and key management systems.

The SafeEnterprise Security Management Center (SMC) provides centralized management for our entire family of Layer 1, Layer 2, and Layer 3 devices within a single product, ensuring that customers save time and reduce cost, while effectively implementing network security for the industry's strongest authentication, definition, and enforcement of security policy.

SafeNet's future product plans will mark the first time high-speed encryption has achieved interface autonomy for network security, allowing customers to add security that is independent of network infrastructures. Our upcoming development projects will also ensure customers that they have a partner that is committed to securing high-assurance communications regardless of the type of transport technology that is chosen.

Summary

With organizations expanding and becoming more geographically dispersed, the global collaboration between partners, suppliers, and customers is forcing a requirement for secure and transparent high-speed communications across the network. Enterprise network and security engineering groups must reach an appropriate balance between enabling communication while securing corporate information. Organizations also require high-speed communication links that provide reliable, trouble free, low latency connectivity in order to back up operational activities and recover from disaster. Although bandwidth is readily available, Service Providers do not provide data integrity for high-speed communication, and there is no accountability or trust applied to the security of the end users' data. The best solution for data integrity is encryption; specifically, solutions designed to provide a high-speed, secure, trusted, and reliable flow of information.

Layer 1 and Layer 2 encryption technologies, as well as IPSec, complement one another within the encryption market; however, each primarily serves a different purpose. Layer 1 and Layer 2 solutions are designed to connect networks to networks, while IPSec at Layer 3 functions as a bridging technology best suited to connecting many sites to one another across public networks. It is quite likely that many enterprises will find that their security needs are best solved by incorporating multiple encryption technologies. Therefore, it is important that the management of any solution has the ability to simultaneously and seamlessly apply and enforce connection rights and policies across multiple technologies.

SafeNet's innovative approach to the issues and technologies described above is to provide a complete family that offers the flexibility to encrypt data at the Physical (Layer 1), Data Link (Layer 2), and Network (Layer 3) layers for communication, while providing organizations with the best alternative for implementing encryption within their existing infrastructure. SafeNet offers the world's only complete solution—a family of high-speed encryption products, from SONET to ATM to IP, with centralized management.

SafeNet Overview

SafeNet (NASDAQ: SFNT) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.



www.safenet-inc.com

Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA

Tel: +1 410.931.7500 or 800.533.3958 email: info@safenet-inc.com

Phone USA and Canada (800) 533-3958

Phone Other Countries (410) 931-7500

Fax (410) 931-7524

E-mail info@safenet-inc.com

Web site www.safenet-inc.com

©2005 SafeNet, Inc. This document contains information that is proprietary to SafeNet, Inc. No part of this document may be reproduced in any form without prior written approval by SafeNet. SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The opinions expressed herein are subject to change without notice.

Australia +61 3 9882 8322
Brazil +55 11 6121 6455
Canada 613.723.5077
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852 3157 7111
India +91 11 26917538
Japan(Tokyo) +81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts) +1 978.539.4800
U.S. (New Jersey) +1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California) +1 949.450.7300
U.S. (Santa Clara, California)
+1 408.855.6000
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers
located worldwide.