

**Stratecast Partners**

*A Division of* **FROST & SULLIVAN**

**WAN Services and Encryption:  
Protecting Data Across Public and Private Networks**

March 2005

Frost & Sullivan reports are limited publications containing valuable market information provided to a select group of customers in response to orders. Our customers acknowledge when ordering that Frost & Sullivan reports are for our customers' internal use and not for general publication or disclosure to third parties.

No part of this report may be given, lent, resold, or disclosed to non-customers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the permission of the publisher.

For information regarding permission, write:

Frost & Sullivan  
7550 West Interstate 10, Suite 400  
San Antonio, TX 78229  
United States

# Table of Contents

## **WAN Services and Encryption**

Introduction.....	4
Security Factor #1: Convergence in Public Networks .....	5
Security Factor #2: Traffic Monitoring Facilities .....	6
Voice Traffic Monitoring: CALEA .....	6
Internet Traffic Monitoring.....	7
The Significance of Authorized Interception .....	7
Security Factor #3: Corporate Exposure to Information Theft.....	7
Financial and Strategic Exposure.....	7
Regulatory Exposure .....	8
The Solution: Preventing Information Theft with SafeNet SafeEnterprise™ ATM/Frame/SONET Encryptors.....	8

## *Introduction*

Enterprise customers are aware of and concerned about the security risks involved in transmitting sensitive information over the public Internet, and they take appropriate measures to address those risks. A wide variety of Virtual Private Network (VPN) technologies and products are used to protect sessions that workers establish from their homes, hotel rooms, or via Wi-Fi services in airports. These VPN sessions are encrypted, typically using Secure Socket Layer (SSL) encoding and, in some cases, using the IP Security Protocol (IPSec).

For site-to-site communications, enterprises typically avoid the Internet and rely on circuit-based technologies including SONET, ATM, and frame relay. These long-lived circuits connect different campuses and remote locations, and sometimes connect an enterprise to its business partners. They are carried over optical fiber or copper. This WAN architecture provides several security advantages:

- The circuits do not depend on IP routers to determine the path across the network in real time. This avoids congestion and delays.
- The circuits have dedicated bandwidth, which protects them against denial of service attacks launched from other networks.
- The use of optical links eliminates the radio-frequency signals generated over electrical links. These RF signals can be intercepted and decoded without detection.

Because of the inherent strengths of circuit-based WAN services compared to premise networks, many enterprises take their security for granted. **The presumption of WAN security has always been a mistake, and is becoming riskier as public networks evolve.** Any data or voice service offered over a service provider network is subject to eavesdropping and information theft. In this paper we examine the technology and regulatory trends behind this vulnerability, the costs associated with it, and the tools that an enterprise can use to protect itself.

Three factors are involved in the new security challenge for WAN services:

1. **Network convergence:** The move from separate networks for separate services (e.g., voice versus Internet) to a single infrastructure carrying all traffic.
2. **Traffic monitoring facilities:** Federal government mandates that service providers design their networks to allow authorized law enforcement agencies to monitor voice calls, and the federal government has several initiatives to monitor Internet traffic.
3. **Corporate exposure to information theft:** As more transactions are processed electronically and as organizations rely on remote collaboration, more sensitive data is transported over wide area networks. The increase in sensitive data makes theft of information more profitable.

These three factors are inter-related, and together they are changing the privacy exposure of enterprises using WAN services.

## ***Security Factor #1: Convergence in Public Networks***

Until recently, service providers developed and deployed separate core telecommunications networks for separate services. Telephone calls were carried over a circuit-oriented network optimized for voice traffic; Internet traffic was carried over a packet-oriented network optimized for data. The voice network used allocated bandwidth, with each call given a dedicated kilobit-per second (kbps) capacity. It also used a hierarchical structure, with all telephones in a particular area code supported by the same network equipment. In contrast, the Internet relied on a “best effort” network with no top-down organizational structure. Routers forwarded Internet packets from source to destination “hop by hop.” Each router examined every packet and decided which port to send it over. Dedicated point-to-point data services for enterprises, using SONET, frame relay, or ATM service interfaces, were allocated bandwidth and carried over the voice network.

These two distinct core networks were connected to customer-facing access networks, which provided the actual service interfaces that businesses and residential customers use. Residential DSL service provides an interesting example. A single electrical line carries both traditional telephone calls, which are delivered to the core voice network, and IP over DSL traffic, which is delivered to the routed IP core.

**Maintaining and expanding these separate core networks independently is expensive and difficult.** Service providers have been working to combine them into a single, *converged* network that supports the latency and jitter requirements of voice traffic and private line services while also providing cost-effective transport for best-effort, high bandwidth IP traffic. In recent years, Multi-Protocol Label Switching (MPLS) has emerged and proven capable of meeting these competing requirements, reliably carrying diverse traffic over a single network infrastructure. Voice, private line, and Internet traffic all traverse the same set of fibers and switches, but each type of traffic is given its own bandwidth pool and forwarding priority. All the major service providers have migrated to, or are in the process of migrating to, MPLS backbones.

This migration is largely transparent to service provider customers. While the core network technology changes, the customer-facing service interfaces are preserved. Frame relay, ATM, and SONET services are re-routed from the older voice-only core network to the MPLS backbone without disturbing the connection at each end. The same service level agreements (SLAs) remain in place. The fact that the traffic is now carried across the core in labeled packets rather than allocated timeslots (SONET) or cells (ATM) is entirely hidden from the customer and does not affect the performance or reliability of the customer’s circuits.

When properly configured, an MPLS network can provide protection against congestion, denial of service attacks, and radio-frequency snooping. These advantages lead many providers to describe MPLS as ‘inherently secure.’ Unfortunately, that overstates the situation. Other forms of eavesdropping are possible, and the shift to a single infrastructure for all network services introduces new vulnerabilities for private line customers.

The MPLS switches that make the converged network possible use fiber optic ports and electrical switching. Traffic is received on one port, its label is examined, and it is then forwarded to the output port associated with that label. The label also determines which

traffic is forwarded first in the event of congestion: labels for voice or private line traffic take precedence over Internet data.

These switches typically provide diagnostic capabilities such as ‘port mirroring,’ in which all the traffic from a particular port can be copied to a second port in addition to its label-specified destination. This enables the service provider to troubleshoot network problems without disrupting service.

A second, related aspect of convergence is the emergence of Voice over IP (VoIP) protocols and services. By using IP protocols to support voice traffic, software developers promise to integrate different forms of enterprise messaging—for example, providing a single ‘inbox’ for both voice mail and e-mail. MPLS and newer routing protocols enable different categories of IP traffic to be assigned different priorities. Consequently, VoIP traffic can escape the pitfalls of ‘best effort’ service. Many different network models and business models for VoIP services are currently being explored, but the common thread is the following: VoIP telephone calls will no longer rely on traditional telephone switching systems, and will instead use IP-based servers.

## ***Security Factor #2: Traffic Monitoring Facilities***

### **Voice Traffic Monitoring: CALEA**

In 1994 Congress passed the Communications Assistance for Law Enforcement Act (CALEA), which is intended to ensure that authorized surveillance of telephone calls by law enforcement agencies is possible. CALEA has led service providers to design their voice networks in a manner that allows the interception of both call transactional information (e.g., calling number, called number, time of day and duration) and the call itself. Historically, intercepting the call itself —‘wiretapping’— involved physically attaching a device to the target’s individual telephone line. Under CALEA, the service provider enables law enforcement to intercept the call[s] at a network switch rather than an individual line.

Congress explicitly excluded Internet data from CALEA requirements. However, the emergence of VoIP telephony and the converged core network are causing this distinction to fade. Telephone calls may never traverse a traditional telephone switch in the new model. Instead, the telephone translates call signaling and voice samples to IP packets and sends those packets to servers, gateways, and remote telephones. How can CALEA requirements be supported in this environment?

The approach that many service providers are taking relies on inspecting IP headers to determine whether they contain voice signaling information, for example H.323 or Session Initiation Protocol (SIP) setup messages. If so, the setup messages are monitored to determine whether the call is subject to a CALEA intercept, and if so the information needed to perform the intercept is captured and used. Implementing this inspection process is difficult, and many service providers are choosing to outsource CALEA monitoring to a third party, for example VeriSign’s NetDiscovery Service. Switch traffic that may contain telephone calls is forwarded to the third-party data center where the inspection is performed.

**The process of monitoring potential VoIP traffic involves intercepting and examining unrelated IP packets.** Until the packet header is examined, the system cannot determine whether it contains voice traffic subject to CALEA, or (for example) e-mail traffic that is exempt.

## Internet Traffic Monitoring

CALEA applies only to voice traffic, but law enforcement agencies have other programs to monitor Internet data. One of the more prominent initiatives is the FBI's 'Project Carnivore,' in which monitoring software is deployed at an ISP to monitor all e-mail traffic to and from a particular suspect. (In January 2005 the FBI announced that it is replacing its custom-built monitoring system with a commercial off-the-shelf version.) Other intelligence agencies, both in the United States and in foreign governments, are reported to have programs for monitoring data traffic traveling over public networks.

## The Significance of Authorized Interception

For our purposes, the significance of these programs to intercept voice and data traffic on the public network is not that enterprise information may be deliberately intercepted by these agencies. There are safeguards in place to prevent arbitrary government surveillance. **Rather, our concern is that these programs have created a network infrastructure that supports such surveillance.**

In the new converged network architecture, telephone calls, Internet traffic, and private line traffic (from SONET, ATM, and frame relay services) all traverse the same core network and are switched by the same equipment. That network is designed to support traffic monitoring. Private line traffic is not legally subject to CALEA interception or Internet surveillance. **However, the software and equipment are in place to monitor any traffic on the multi-service network switch. Only the policies and personnel at the service provider, and for some types of traffic at third-party CALEA monitoring firms, prevent unauthorized interception.**

## *Security Factor #3: Corporate Exposure to Information Theft*

### Financial and Strategic Exposure

Although corporations are reluctant to disclose any network security incidents that they experience, some studies have provided useful data on the subject. The American Society for Industrial Security, now known as ASIS International, regularly surveys Fortune 1000 companies on the subject of proprietary information loss. Their 2002 report, conducted with PricewaterhouseCoopers and the U.S. Chamber of Commerce, and entitled "Trends in Proprietary Information Loss: Survey Report," is the most recent.

This survey concludes that the 138 responding companies had experienced aggregate financial losses of 53 to 59 billion dollars due to information theft in the year ending June 30, 2001. Forty percent of responding companies reported incidents of information theft. The average cost of an incident was \$404,000 in the case of research and development, and \$356,000 in the case of financial data.

A separate study conducted by the Computer Security Institute and the FBI in 2004, entitled "2004 CSI/FBI Computer Crime and Security Survey" elicited 269 responses from small to large organizations (19% had under 100 employees, 7% had 50,000 or more employees). This report attributed \$11,460,000 in losses from proprietary information theft at the responding firms. (This is a substantial undercount, since many firms were unable to assign a dollar amount to their losses.) This was the third most costly information security threat, following viruses and denial of service attacks.

**Both surveys measure only *detected* incidents of information theft, which is likely to represent the tip of the iceberg.** When customer lists, product roadmaps, strategic plans, or merger and acquisition information is intercepted by a competitor, the victim may never learn of the incident. The costs, for example in terms of lost business, will never be tallied. The strategic impact, measured in lost market share and competitive position, may be so devastating to the company that financial metrics are beside the point.

## **Regulatory Exposure**

Legislation and regulatory agency rulings are imposing new requirements on businesses to ensure the privacy of their customer and transactional data. The 1996 Health Information Portability and Accounting Act (HIPAA) introduced requirements for protecting patient medical records, with wrongful disclosure of such information carrying penalties of up to \$50,000 and a year in prison. The 2002 Sarbanes-Oxley Act mandates strong internal controls on access to sensitive financial information, and provides for penalties of up to \$5,000,000 and 20 years in prison. The loss of corporate reputation could far outweigh even these strict penalties.

**We are likely to see further regulatory action regarding corporate responsibility to protect against information theft.** Recent reports of incidents in which thousands of individual accounts containing personal information were stolen have led several Congressmen to introduce new legislation on the subject.<sup>1</sup>

### ***The Solution: Preventing Information Theft with SafeNet SafeEnterprise™ ATM/Frame/SONET Encryptors***

To briefly review the challenges examined above:

- Today's converged public network architecture carries private line traffic over the same facilities that carry voice and Internet data.
- Law enforcement initiatives against crime and terrorism direct service providers to design those facilities so that they support surveillance of voice and data traffic, sometimes with the help of third-party specialist firms.
- Legal safeguards prevent unauthorized government surveillance. However, the surveillance facilities and tools are in place, and enterprises must rely on the internal procedures of the service provider and its partners to guarantee against surveillance by rogue employees.
- The potential cost of information theft per incident is measured in hundreds of thousands to millions of dollars, with the potential for executive prison sentences.
- All networks are subject to tampering, equipment failures, and misconfiguration, which leads to data vulnerability.

### **How should the enterprise protect itself in this environment?**

The answer cannot be “avoid transmitting sensitive data over the wide area network.” The productivity gains from remote collaboration across enterprise campuses and with business

---

<sup>1</sup> *Senators Rip into ChoicePoint, Bank of America on Data Losses*, ComputerWorld, March 11 2005

partners are too compelling. The answer must instead be **“ensure that your data is safe from surveillance, regardless of your carrier’s network architecture and security measures.”** Fortunately, there are simple and straightforward solutions to accomplish this. The solutions rely on encryption: the enterprise deploys an encrypting device at each WAN access service interface, ensuring that its data and potentially voice traffic, is unreadable even if it is intercepted.

**Not all encryption systems are equal.** Encryption techniques have evolved rapidly over the past decade, driven by increasing computing power that makes once-secure techniques now subject to unauthorized decoding. The Data Encryption Standard (DES) evolved into “Triple-DES” to provide greater security, but the National Institute of Standards and Technology (NIST) recommends that DES variants be replaced with the newer and more robust Advanced Encryption Standard (AES).<sup>2</sup>

Key criteria for choosing a WAN encryption system include support for AES, line-rate performance (not always provided at higher rates, such as OC-48), support for the secure network management protocol SNMP v3, and support for the “Common Criteria” security certification standards adopted by the U.S. Department of Defense and Homeland Security. **With precisely these criteria in mind, Stratecast Partners believes that SafeNet’s SafeEnterprise series, which includes SONET/SDH, ATM, and frame relay encryptors, offers a very compelling solution to the security challenges described above.** In fact, SafeNet has been first to market with line-rate OC-48 and even OC-192 SONET encryptors.

In many other areas, implementing network and information security involves tradeoffs -- more security means lower network performance, greater complexity for users, ongoing management issues, and interoperability problems. WAN encryption involves none of these tradeoffs. **In the face of growing threats and greater exposure to interception of data on the provider network, any enterprise that is not using WAN encryptor technology must re-examine its security strategy. In this context, and based on the research and analysis conducted by Stratecast Partners, SafeNet’s SafeEnterprise ATM/Frame/SONET Encryptor series can provide tangible benefits to enterprises.**

*Michael Ladam*  
*Tier 1 Service Provider Strategies*

---

<sup>2</sup> NIST Says DES Encryption “Inadequate,” July 29, InfoWorld.