
Enterprise Telecom Management Solutions

A Corporate Whitepaper by
Kirk Vaughn,
Senior Product Manager
VoIP Technologies



Executive Summary

Voice over Internet Protocol (VoIP) is possibly the most disruptive technology and enhancement that the enterprise communications network has ever seen. This technology forces the convergence of two physically separate networks into one, and is driving organizational convergence as well. VoIP forces CIO's to consolidate what was once three autonomous organizations—telecommunications management, data communications management, and IT security—into one organization. The new converged network needs to be managed as a single homogenous network, and accomplishing this is the charter of this new organization. The question is: How?

Tools are available, but they generally come packaged in expensive purpose-built wrappings, and are usually "left-overs" from the old legacy organization. Security has its own set of tools. As does Telecom and Datacom management. Complicating matters further, the legacy Public Switched Telephone Network (PSTN) equipment and services cannot be completely eliminated. This creates a "hybrid" network consisting of legacy Time Division Multiplex (TDM) equipment that must be integrated with the new converged data network. What is sorely missing is an appropriately scaled, yet integrated system for providing end-to-end, multi-vendor management and security of the new hybrid voice infrastructure.

The SecureLogix® ETM® Hybrid Telecom Firewall platform is purpose-built for managing this environment. It combines applications and tools in the areas of application security, accounting, and performance management, and provides a level of visibility and control that has never been available before. SecureLogix recognizes that a long migration period is necessary for VoIP, and has developed the ETM System to assist the enterprise telephony manager during this period. This document discusses the requirements for a hybrid voice management solution, and details the capabilities offered by the SecureLogix ETM Hybrid Telecom Firewall for satisfying these requirements.

Table of Contents

1. Introduction
2. Requirements for a Voice Management Solution
3. The SecureLogix® ETM® System
4. The ETM® System Fulfills the FCAPS Challenge
5. Summary

1. Introduction

As VoIP is introduced to the enterprise in large volumes, the management challenges that VoIP imposes must be addressed. Most enterprises that have deployed VoIP have done so in small incremental steps, usually by creating VoIP "islands" connected to the rest of the world through the PSTN. This makes the network easier to manage, and if problems arise from the deployment, they can be easily isolated and resolved. As the deployment grows in size and complexity, and as more of the legacy TDM network is migrated over to Internet Protocol (IP), managing the network as a single entity becomes more complicated. Voice communications is by far the most important

"application" running on the enterprise data network, and it has unique real-time characteristics that must be preserved and maintained. Additionally, voice communications carries with it an expectation for high quality, availability, and privacy that was created over the years by the legacy circuit-switched network.

VoIP is certainly important enough to an enterprise's operation to deserve its own set of management tools. When searching for these tools, the enterprise telephony manager generally starts by either looking to the Private Branch eXchange (PBX) or VoIP system vendor for management solutions, or evaluating the wide array of specialized network management platforms targeting the data network or carrier environment. It is immediately obvious that these options have their shortcomings. They are expensive, they don't properly scale to the enterprise environment, and they aren't integrated at the console level. Ideally, what is needed is an integrated platform containing the key features from each of the five necessary management system categories, as defined by the International Telecommunications Union (ITU) in its FCAPS Network Management System (NMS) model. This includes Fault, Configuration, Accounting, Performance, and Security Management. To meet this need, a platform would need to consist of an integrated subset of each of the "point-systems" that are purpose-built for these functions, in a scaled-down platform designed to meet the needs of the enterprise environment.

Additionally, we must remember that the enterprise network is now a hybrid mix of vendors, technologies, and transport types. The ideal solution must include an integrated and scalable platform designed to cover the entire enterprise telephony network, regardless of whether an enterprise is dealing with a traditional voice network, a VoIP network, or a hybrid mixture of both. This whitepaper discusses the generic requirements for such a platform, and details the SecureLogix® ETM® Hybrid Telecom Firewall platform as a solution to these requirements.

2. Requirements for a Voice Management Solution

The FCAPS model for Network Management, as defined by the ITU and standardized by the International Standard's Organization (ISO), consists of five major categories. This model was developed as a framework to help operators with large-scale networks build a network management strategy to support multi-vendor, multi-technology environments. The model covers the basic elements of a network management strategy, and provides a consistent framework for prioritizing functions and responsibilities.

The first two categories are Fault and Configuration Management. These categories consist of basic functions required to setup and manage any network. As a result, these two are always included as basic capabilities of the supplied network infrastructure. For example, it is considered standard practice for data network and voice network equipment to come equipped with Element Managers (EM) capable of collecting and sending alarms from the managed equipment. These alarms may be stored and displayed on the EM console, or alternatively sent upstream using Simple Network Management Protocol (SNMP) commands to an external fault management

system such as HPOpenview®. In this manner, a single network operations group (i.e., NOC) can manage and coordinate the resolution of alarms from a central position in the network. It is also standard for EMs or “craft” ports to be used for establishing and maintaining configuration settings on the equipment. Sometimes, an overlay configuration manager is used to centralize the configuration process if one is not already provided with the system. In short, Fault and Configuration Management are functions that benefit from centralized management, and they have been satisfactorily addressed by the infrastructure providers. The convergence of the various technologies into a hybrid network does not appear to have a significant impact on the NOC’s ability to manage Fault and Configuration functions. Therefore, there is no need for a detailed discussion of these two functions in this document.

The FCAPS functions that must be carefully addressed for the new hybrid network are Accounting, Performance, and Security Management. These functions have enormous challenges in this new architecture, as they all require a single end-to-end view of the network in order to be effective. To understand why this is important, we must first understand the responsibilities for each of these three categories of management:

Accounting Management involves collecting and tracking network resource usage metrics and reporting utilization costs to the appropriate parties. Accounting Management Systems (i.e., billing systems) should have the capability to not only track high-cost resources (e.g., long distance, international, and 900 toll numbers), but also to report, and track enterprise and departmental usage of the resources. Additionally, usage and cost reporting needs to be consolidated from across the entire voice network, independent of vendor or implementation—not segmented between the legacy PBX and VoIP networks.

Performance Management comprises gathering and analyzing critical end-to-end network performance metrics under both normal and degraded conditions. This includes collecting statistical data from both within the network protocols (i.e., RTCP or D-channel analysis), and by actively monitoring the traffic. Active monitoring techniques include real-time analysis on a channel or packet basis, or using synthetic transactions to monitor network capabilities and performance. Performance Management also includes setting thresholds and providing reports and alerts to other systems, such as sending SNMP traps to the alarm manager, when network performance degrades below acceptable levels.

Security Management entails minimizing and attempting to eliminate unauthorized access to the voice and data network through vulnerabilities in the traditional voice and VoIP networks. It involves monitoring and controlling access to specific network resources and applications, ensuring access is limited to only legitimate use by authorized internal and external users, providing controlled access to key resources, and providing notifications (alarms) when breach attempts occur. Security Management also includes implementing prescribed corrective actions when violations of established security policy occur, such as termination of active phone calls or denial of access to phone calls in violation of policy.

To satisfy each of these functions on a single system, it is important for a Hybrid NMS system to have the following capabilities:

Accounting

- Provide access to call details for all calls—both internal and external
- Use centralized database for collecting call records across all systems—both TDM and IP
- Generate both departmental and enterprise-wide reports
- Correlate, cross check, and verify records received from multiple sources

Performance

- Provide end-to-end measurement of application performance across disparate networks and boundaries (i.e., PSTN, WAN, LAN, Core)
- Perform real-time (active), as well as historical (passive) measurement techniques
- Measure performance at key points in the network—not just end-to-end
- Identify and alert on degrading conditions that will soon affect performance—pro-active vs. reactive service
- Integrate with the Fault Manager to provide alerts on network performance issues
- Include a “human perception” correlation factor in the calculation for establishing application performance—for use in addition to network performance statistics

Security

- Secure vulnerabilities in PSTN access and IP networks
- Protect network from attacks exploiting VoIP protocol vulnerabilities
- Provide edge security to control access at boundaries of IP network
- Provide Call Admission Control (CAC) at the network edge and critical internal network boundaries
- Detect and thwart malicious call patterns or those which might indicate toll theft or fraud

Security is an important piece of this model. It cannot be ignored or addressed separately due to its enormous impact on the network’s ability to perform and deliver critical real-time services, such as VoIP. Based on interviews with companies that have installed VoIP, Forrester found that most companies fail to consider the unique vulnerabilities caused by integrating voice into a converged network prior to deployment. Although most companies take major steps to regularly upgrade their data networks to prevent attacks, many fail to recognize the need to add additional security measures when adding voice traffic to the data networks. Only 25% of the companies interviewed upgraded or replaced firewalls and just 22% changed to secure gateways. Companies that do not address security requirements...risk exposing their data networks to malicious attacks from external or internal sources.[1]

3. The SecureLogix® ETM® System

The SecureLogix® ETM® System has its roots in traditional voice telecom system security and management, but its design allows its inherent real-time management and security capabilities to be logically extended and expanded to VoIP services, providing unified management and security for any mixture of legacy voice and VoIP traffic. The ETM System consists of in-line appliances, management servers, and an application suite that meets each of the key management capabilities required in the FCAPS management model.

ETM® Platform Appliances

The highly expandable, remotely managed ETM Appliances are vendor-independent, solid-state devices installed in-line on the telecommunications circuits between the PBX and Central Office (CO), and on critical VoIP network segments, to continuously monitor and control all enterprise communications in real time. The devices are centrally managed and remotely upgradeable. In environments comprised of a hybrid mix of legacy and IP services, the ETM Appliances support ETM Management and Security Applications for either or both services, allowing telephony managers to manage and secure all enterprise voice communications with one integrated, robust and scalable system.

The appliances host a growing suite of first-of-kind applications, including a hybrid Telecom Firewall, Telecom VPN, Call Recorder, Usage Manager, and Infrastructure Manager to provide:

- Visibility and control of voice network access and usage
- Continuous call monitoring with stateful inspection
- Policy-based operation with real-time alerts (console, email, pager, SNMP traps)
- Real-time call-type detection at the network edge (voice, fax, modem, video and STU-III)
- Support for a variety of circuit types (IP, T1, ISDN PRI, European PRI, and analog)

Figure 1 illustrates deployment of the ETM System in a Campus VoIP scenario. Appliances are installed on TDM circuits between the PBX and CO, and on critical VoIP network segments, including in front of the Call Server (IP PBX). The hybrid Telecom Firewall application blocks inbound attacks through the legacy phone network and the VoIP WAN links, internal attacks against the Call Server, toll fraud, and DoS attacks against critical resources. Recommended locations for appliances on VoIP network segments vary with each deployment scenario (Campus, IP Centrex, End-to-End VoIP), but include in front of Call Servers, on the perimeter in an IP Centrex environment, on the WAN perimeter, and on the IP trunking perimeter.

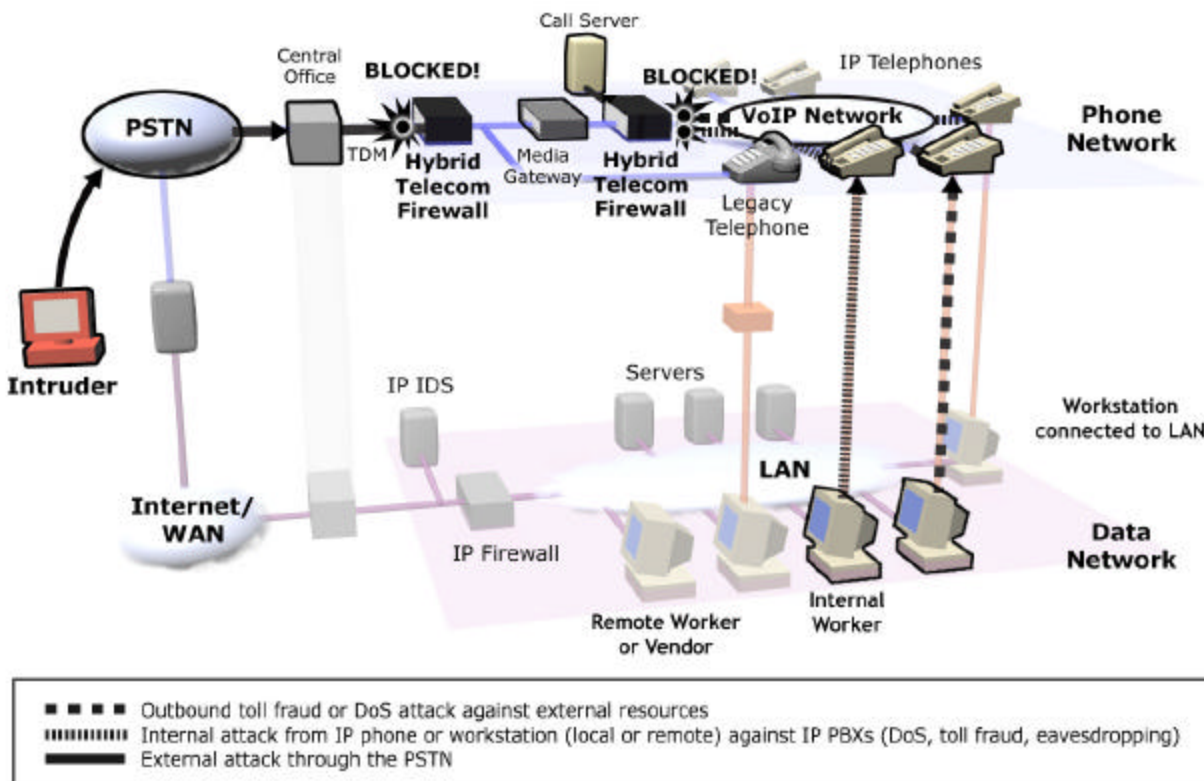


Figure 1 – ETM® Hybrid Telecom Firewall

ETM® Application Suite

The ETM Application Suite provides patented and patent-pending technologies to bring unified management and security intelligence to legacy voice and/or VoIP networks. To meet the enterprise's needs, whether dealing with a legacy voice network, a VoIP network, or a hybrid mixture of both, the management and security applications discussed below monitor and control access to specific network resources, collect and track network resource usage metrics, collect and analyze network performance metrics, provide associated alarms and alerts, and provide consolidated cost and utilization reporting. Additional applications provide encrypted communications and call recording on the legacy voice network.

ETM® Telecom Firewall

The ETM Telecom Firewall complements traditional data firewalls (which are designed for non-real-time IP traffic), by providing seamless, unified security for all real-time enterprise voice communications—both TDM and VoIP.

The ETM Telecom Firewall detects, logs, and controls all inbound and outbound voice activity based on administrator-defined, automated security policies (see Figure 3). The Telecom Firewall's granular usage policies can prevent abusive or malicious use of the enterprise telecom resources by both internal and external callers, and reduce the costs of voice network infrastructure, service, and management.

The ETM Telecom Firewall is designed to close the security gap left by the traditional data firewall's inability to monitor VoIP signaling or media for attacks against the voice network. This shortfall forces traditional data firewalls to either block the call or open several ports per call without determining whether the packets were legitimate, leaving the VoIP network vulnerable to attack. The Telecom Firewall provides in-line signaling and media inspection, transparently passing allowed signaling and media through to their destination, but cleanly terminating disallowed call activity. Additionally, while most data firewalls slow data transfer, impeding the flow of traffic and adding an unacceptable latency to VoIP's real-time media packets, the ETM Telecom Firewall meets VoIP's unique, real-time performance requirements.

Anomaly Detection and Prevention

The ETM Telecom Firewall performs call pattern anomaly detection and prevention, monitoring voice traffic for abusive call patterns, such as war dialing, toll fraud, and password guessing, second dial tone-type loop back calls (i.e., an inbound call that is routed outbound to a toll number), and abusive Dual Tone Multi-Frequency (DTMF) tone sequences, such as strings of tones close similar to known passwords.

The Telecom Firewall also performs packet-level anomaly detection, monitoring VoIP traffic for packets that are too large, too frequent, use signaling commands that are out-of-specification, or contain known Denial of Service (DoS) or other attack signatures. When anomalous activity is detected, the hybrid Telecom Firewall can terminate the call and send associated notifications (alerts) to designated systems and personnel, in accordance with security policy. Figure 3, Rule #6 shows an example Packet Anomaly rule for the Telecom Firewall.

QoS Monitoring

The ETM Telecom Firewall is designed to function as both a signaling firewall, and a media firewall. When properly located in an enterprise network, such as on a monitored boundary connection or in front of a media gateway resource, the Telecom Firewall provides visibility into media stream activity as it traverses the enterprise. This visibility allows measurements and analysis to be conducted on network performance as the network reports it on an end-to-end basis, using RTCP statistics as reported by the VoIP endpoints. By combining Quality of Service (QoS) statistical reporting with policy-based thresholds and real-time alert capabilities, the ETM System provides additional control and visibility into network performance above what is available in traditional enterprise voice management systems.

Future capabilities are expected to include an active measurement capability using Mean Opinion Score (MOS) technology as defined in ITU specification G.107. By using an active capability, performance metrics can be measured at various points in the network, in real time, instead of relying on reported data in an end-to-end fashion. QoS issues may be caused by a single breakdown in one area of the network. By segmenting the QoS measurements into several parts, it is easier to identify the trouble-spots and isolate them. Additionally, MOS addresses QoS at the application level, and adds a "Human Perception" factor to the calculation on top of what is measured at the network level. This provides a better overall indication of voice quality, as the customer perceives it. Policies can be developed to take certain actions based on the MOS scores, such as sending real-time alerts (email, page) to key personnel, or SNMP alarms to the enterprise alarm management system. With the use of the centralized ETM Management Server and database, it is possible to correlate measurements from various points in the network and identify conditions which are degrading over a period of time. The appropriate personnel may be notified with real-time alerts, or reports detailing these conditions may be generated and distributed as needed.

ETM® Infrastructure Manager

The ETM Infrastructure Manager provides real-time, enterprise-wide visibility and control over telecom resources, including centralized health-and-status monitoring of legacy voice trunks and VoIP segments, with unified management of geographically distributed ETM Appliances and security/usage policy sets from a single console.

The ETM Infrastructure Manager supports real-time, enterprise-wide health-and-status monitoring of telecom signaling error and availability conditions on TDM trunks and monitored VoIP segments, with problem diagnosis tools and automated alerting capabilities. For the first time, telephony managers can assume a real-time, proactive Service Level Agreement (SLA) enforcement position with their telecom service providers.

The Infrastructure Manager also provides a real-time call monitor that tracks all active calls across the enterprise, both legacy and VoIP, and enables manual termination of unauthorized, threatening or suspect calls.

Troubleshooting Tools

The Telecom Firewall is designed to obtain in-line access to real-time data from the network, application signaling, and the corresponding voice media. This places the ETM System in the optimum position for detection and analysis of network and voice application issues. The centralized management console provides the ability to launch PING and Traceroute commands on any IP endpoint from any ETM Appliance in the network, allowing the network administrator to segment his network and isolate faults. Additionally, a signaling packet sniffer is available on each appliance to textually display the application signaling packets as they traverse an appliance in the network. This provides real-time visibility into the application to help isolate application-level faults.

Figures 2, 3, and 4 illustrate the Infrastructure Manager user interfaces, which seamlessly unify security and visibility for any mixture of legacy and VoIP traffic.

Figure 2 illustrates the user interface at a unified Infrastructure Manager, which provides access to the enterprise policies for the hybrid Telecom Firewall. Figure 2 also currently displays a portion of the firewall policy, containing both traditional voice and VoIP rules.

Figure 3 illustrates a simple hybrid Telecom Firewall policy (partially shown in Figure 2), which may include legacy and/or VoIP rules. In this illustration, rules 1 through 4 and 7 apply to traditional voice communications; rules 4 and 7 apply to VoIP activity; and rules 4 and 7 apply to both traditional voice and VoIP communications.

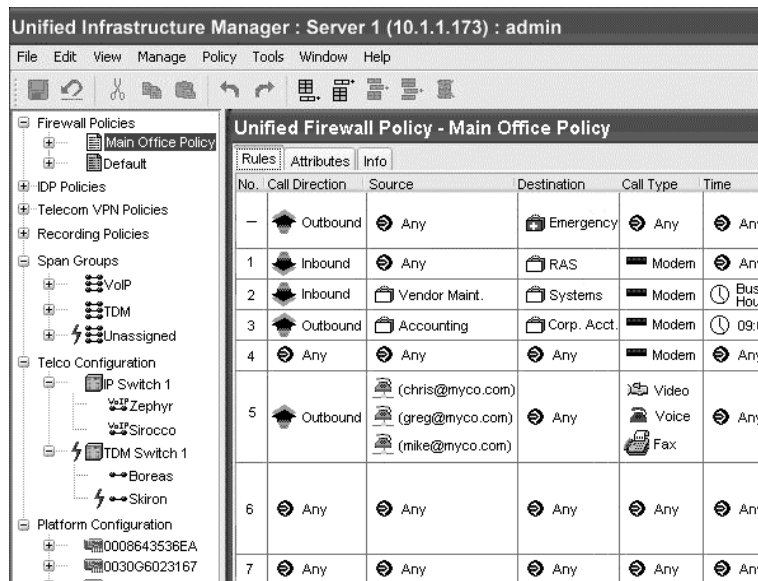


Figure 2 – Unified Infrastructure Manager

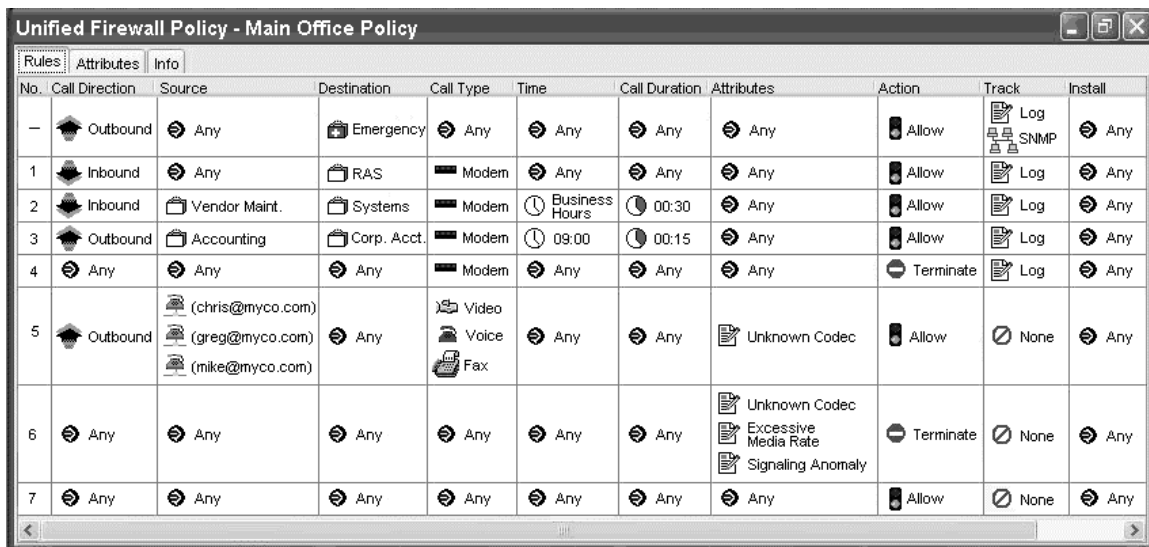


Figure 3 – Hybrid Telecom Firewall Policy

Span	Chn	Direction	Source	Dest	Codec	Start	Connect	End	Dura	Type	Track	Rate In	Rate Out	Bytes In	Bytes Out	Packets In	Packets Out
Skiron	8	Inbound	+1(512)9833808	+1(210)5554894		17:14:24	17:14:24	17:14:24	00:00:00	Modem	Terminate						
Skiron	10	Inbound	+1(204)2892305	+1(210)5554896		17:14:24	17:14:24	17:14:24	00:00:00	Voice	Terminate						
Boreas	13	Outbound	+1(210)5554892	+1(045)2235413		17:13:58	17:13:58		00:00:38	Fax	Log						
Boreas	14	Outbound	+1(210)5554880	+1(412)4428524		17:13:35	17:13:35	17:14:18	00:00:43	Modem	Log, SNMP						
Boreas	15	Outbound	+1(210)5554892	+1(723)4428512		17:14:24	17:14:25		00:00:10	Modem							
Boreas	17	Outbound	+1(210)5554001	+1(045)2235413		17:13:54	17:13:55	17:14:17	00:00:23	Voice	Log						
Boreas	19	Outbound	+1(210)5554893	+1(210)5557325		17:14:14	17:14:15		00:00:20	Fax	Log						
Boreas	20	Outbound	+1(210)5554885	+1(723)4428510		17:14:21	17:14:22		00:00:13	Modem							
Boreas	22	Outbound	+1(210)5554084	+1(718)4582121		17:14:15	17:14:16		00:00:19	Fax							
Boreas	23	Outbound	+1(210)5554871	+1(045)2235423		17:13:56	17:13:56		00:00:38	STU	Log						
Boreas	24	Outbound	+1(210)5554076	+1(418)2557510		17:13:50	17:13:58		00:00:36	STU	Log						
Zephyr	1	Inbound	bmysa@psre.com	baryn@nyco.com	GSM	17:13:52	17:13:52		00:00:42	Voice		8.3 K/s	8.4 K/s	338.4 K	344.4 K	0	111
Zephyr	2	Inbound	hegerb@kping.com	susan@nyco.com	G723	17:13:53	17:13:53		00:00:41	Voice		8.3 K/s	8.3 K/s	330.1 K	330.1 K	99	0
Zephyr	4	Outbound	chris@nyco.com	ralon@gyser.com	PCMU	17:13:54	17:13:54		00:00:40	Voice		8.3 K/s	8.3 K/s	321.8 K	322.3 K	87	0
Zephyr	5	Inbound	macon@talon.com	sehr@nyco.com	G723	17:13:55	17:13:55		00:00:39	Voice		8.3 K/s	8.3 K/s	34.9 K	34.9 K	0	0
Zephyr	6	Outbound	greg@nyco.com	wilson@vln.com	G723	17:13:56	17:13:56	17:14:14	00:00:16	Voice		8.8 K/s	8.8 K/s	141.3 K	141.3 K	0	0
Zephyr	7	Outbound	mike@nyco.com	vdh@emline.com	G723	17:13:56	17:13:56		00:00:38	Voice		1.1 K/s	1.1 K/s	41.8 K	40.8 K	0	0
Zephyr	8	Outbound	shp@nyco.com	nyvys@usst.com	G723	17:13:58	17:13:58		00:00:36	Voice		8.9 K/s	8.9 K/s	32.1 K	32.1 K	0	0
Zephyr	10	Inbound	lrysch@zfp.com	seang@nyco.com	GSM	17:14:01	17:14:01		00:00:33	Voice		8.8 K/s	8.8 K/s	280.8 K	280.8 K	0	0

Figure 4 – Real-Time Unified Call Monitor

Figure 4 illustrates the Infrastructure Manager’s unified Call Monitor, which provides a real-time display of traditional voice and/or VoIP activity. The administrator can focus the tool on specific legacy spans and channels, or VoIP Network Interface Card (NIC) pair and VoIP session to support very granular monitoring of call traffic.

ETM® Usage Manager

The ETM Usage Manager is a powerful reporting, analysis and management tool, enabling a full Return on Investment (ROI) through reduced phone bills, automated utilization and call accounting reports, and detailed telecom security audits.

The Usage Manager's analysis engine collects and compiles Call Detail Records (CDR) with call-type information on all inbound and outbound transmissions, along with health and status conditions on all trunks across a distributed enterprise, regardless of PBX type or transport type, and sends this information 3DES encrypted to a central relational database. Enterprise-wide reports can be generated from one centralized management console or any number of provisioned client consoles.

The report writing tool provides unified enterprise-wide visibility into telecom resource utilization and capacity planning issues, legacy voice and VoIP network usage, abusive and costly calling patterns, toll fraud incidence, and telecom/data network security issues.

In the early stages of a planned migration, the Usage Manager can be used to properly dimension VoIP media gateways by providing a precise breakdown of busy hour call traffic. Additionally, reports can be generated to show the percentage of calls that are over fax or modem lines, which will most likely require dedicated PSTN facilities. It is

also possible to differentiate inter-office calls from public calls, to give a better estimate of IP WAN utilization in the case that IP trunking is used to connect campuses within the enterprise. By understanding the ratio of fax and modem calls to voice calls, and the ratio of inter-office to public PSTN calls, the media gateway can be properly dimensioned to handle the voice traffic between the enterprise and the PSTN.

Figures 5 and 6 illustrate unified enterprise-wide visibility into legacy voice and VoIP resource utilization reports.

Figure 5 illustrates a resource utilization report sample showing busy hour call attempts on the legacy voice trunks, as an example of what can be visualized when dimensioning VoIP media gateway platforms and trunking.

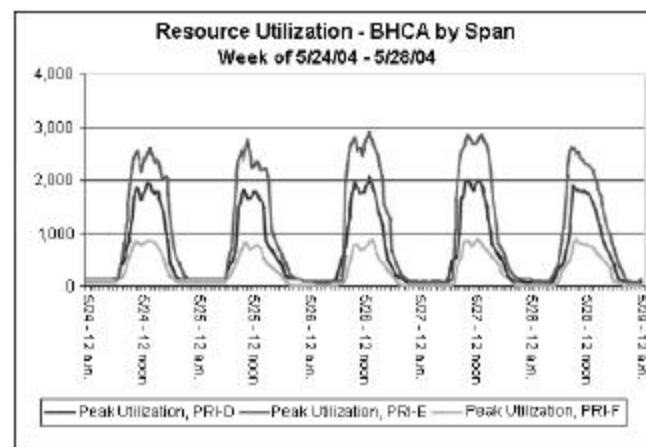


Figure 5 – Busy Hour Call Attempts Report Sample

Figure 6 illustrates a resource utilization report sample showing a comparison of office-to-office communications on legacy voice trunks vs. IP trunking.

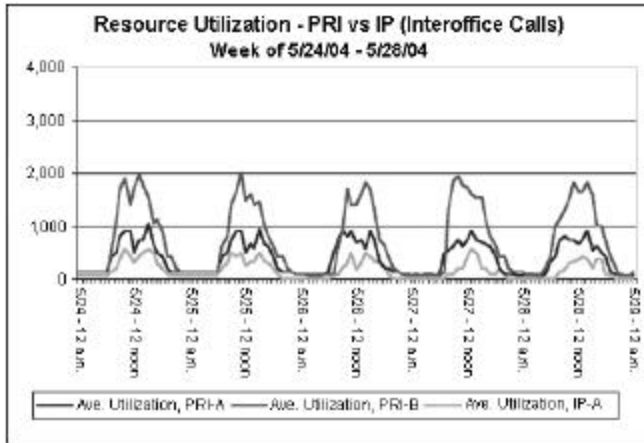


Figure 6 – Legacy vs. IP Utilization Report Sample

Figure 7 illustrates the ETM System’s central management and consolidated reporting from geographically distributed appliances deployed across a hybrid mix of legacy and VoIP

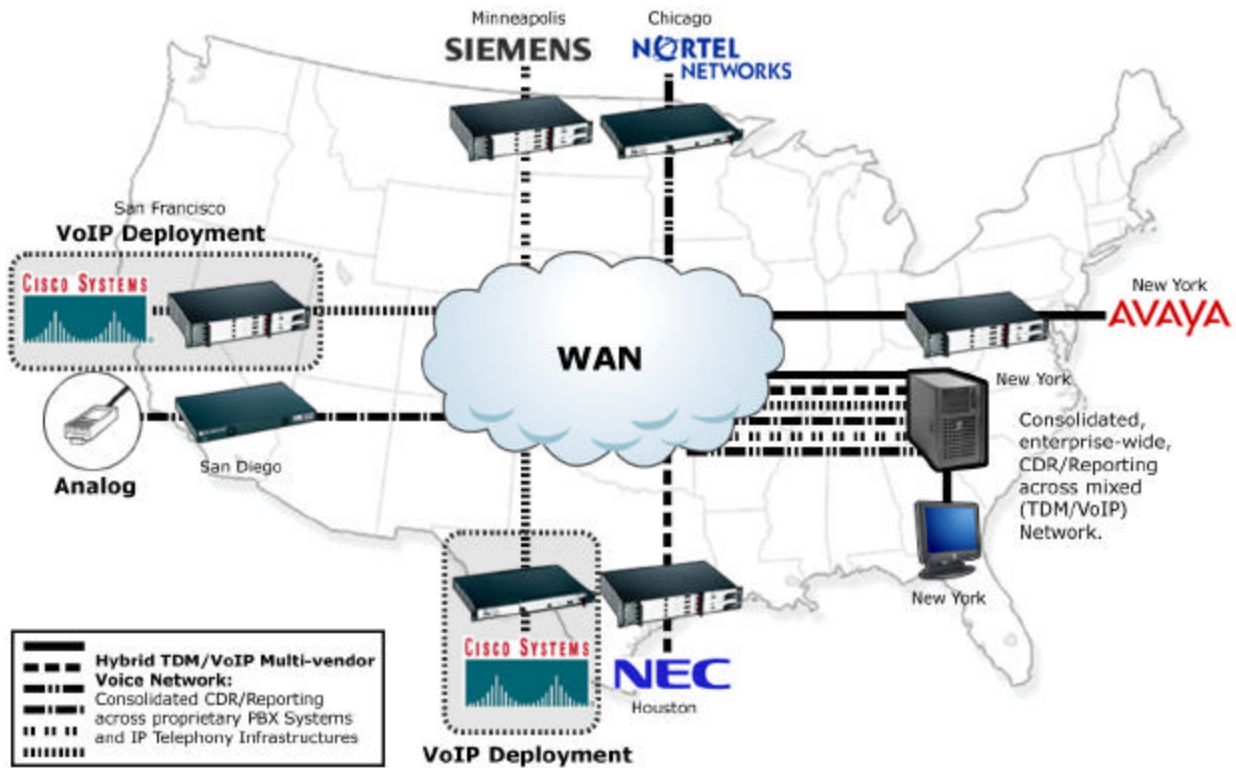


Figure 7 – ETM® System Unified Reporting Across a Multi-Vendor Environment

services, independent of multiple proprietary PBX and IP PBX systems. (No endorsement is implied by use of vendor name in illustration.)

ETM® Telecom VPN

The ETM Telecom VPN enhances the security strategy for any enterprise. Communications through public infrastructure like the Internet and PSTN are at risk for interception, eavesdropping and/or vandalism. Telecom VPN provides enterprise-wide call confidentiality for voice, fax and modem calls made over the PSTN. Accordingly, many organizations secure their data transmissions through the Internet with data VPNs. The ETM Telecom VPN adds similar protection to legacy voice network transmissions.

Unlike voice encryption technologies that require separately deployed desktop devices, the ETM Telecom VPN sits at the edge of the legacy voice network to inexpensively encrypt communications from PBX-to-PBX. The Telecom VPN is transparent to the user, with no noticeable impact on voice quality, and does not require user interaction in order to encrypt a call. The VPN provides a policy engine which allows policy-based encryption on a per-call basis, enforceable on an individual station, department, or enterprise level.

Figure 8 illustrates the Telecom VPN transparently encrypting a call made to a destination that also has encryption capability. However, the Telecom VPN allows a call to proceed in the clear if the call is to a destination that does not have encryption capability.

ETM® Call Recorder

The ETM Call Recorder provides security monitoring of specific source and/or destination numbers with policy-based call caching and aggregation of specific voice, fax, and modem calls. The application records audio content in accordance with the policy, then transmits the copy to an analysis site for review, analysis, and storage. This capability is useful for conducting investigations such as recording the audio content of calls from specified locations in order to perform Communications Security (COMSEC) monitoring.

The Call Recorder also facilitates compliance with new regulations, such as those impacting the medical community that may require patient privacy be ensured by either encrypting or monitoring faxes. Allowed modem sessions and fax transmissions are recorded based on policy, then transmitted to the analysis site for reconstruction, review, analysis, and storage.

ETM® Management Software

Client and server software is used to manage and monitor distributed ETM Appliance operations, providing telephony managers with real-time visibility and control over the entire ETM System with:

- Centralized platform administration and monitoring
- Real-time telecom and VoIP health and status alerts
- Distributed policy, software and firmware updates
- Relational database capture for call detail records
- 3DES encrypted communications between the ETM Client, Server, and Appliances

The ETM System is centrally managed, remotely upgradeable, and scalable to meet the needs of geographically, or even globally distributed enterprises. Larger enterprises with multiple management servers can receive consolidated screen alerts to a single console. This aids in the centralized monitoring and support of a larger number of servers, regardless of their geographical locations.

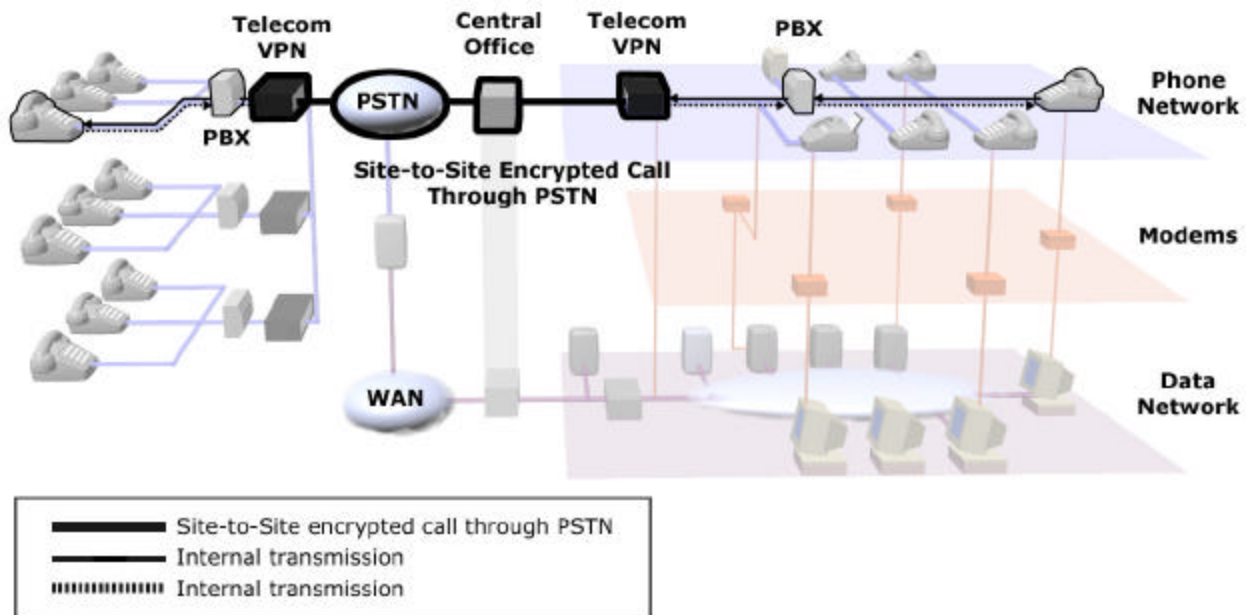


Figure 8 – VPN for the Legacy Voice Network

Figure 9 illustrates a geographically distributed deployment of the ETM System. In environments with a hybrid mix of legacy and IP services, each ETM Appliance can support applications that provide management and security for either or both legacy and VoIP services.

4. The ETM[®] System Fulfills the FCAPS Challenge

The ETM[®] System is well suited for satisfying the primary requirements for enterprise telephony management as outlined in the ITU's FCAPS model. It provides a robust, integrated, centrally managed approach to covering the important aspects of FCAPS as it relates to enterprise voice network management, including the complex world of traditional voice and VoIP security management. The ETM Solution uses application security techniques to secure the network from application-layer attacks, and provides additional user-level security to detect unauthorized or malicious user activity on the network.

The ETM Solution, with its centralized relational database, is capable of providing a CDR management solution for multi-vendor hybrid environments. The call accounting, reporting, and utilization measurement capabilities satisfy the Accounting responsibilities of the model.

Performance Measurements are accomplished on the VoIP network with the QoS reporting tool, and will soon be enhanced with an MOS-based active measurement tool. This feature allows an enterprise to use policy-based controls to alert on degrading conditions, or send upstream SNMP alarms when critical QoS issues are detected.

Security is one of the more difficult areas of FCAPS to address. The ETM System enhances the existing data network security platform with voice application security tools. It provides protection from IP-based attacks on the voice system, and prevents modem attacks through the legacy voice network onto the data network. User-level security is provided to protect against abusive behavior from internal "trusted" users. This includes traffic that is traveling across the IP network, the TDM network toward the PSTN, and any independent TDM facilities that are used for modem and fax support outside the VoIP network.

Without trying to replace all of the features of the purpose-built FCAPS management systems, the ETM System succeeds in supplying enhanced features for managing the enterprise voice environment, while providing enhanced application-level security to complement the existing data network security platforms.

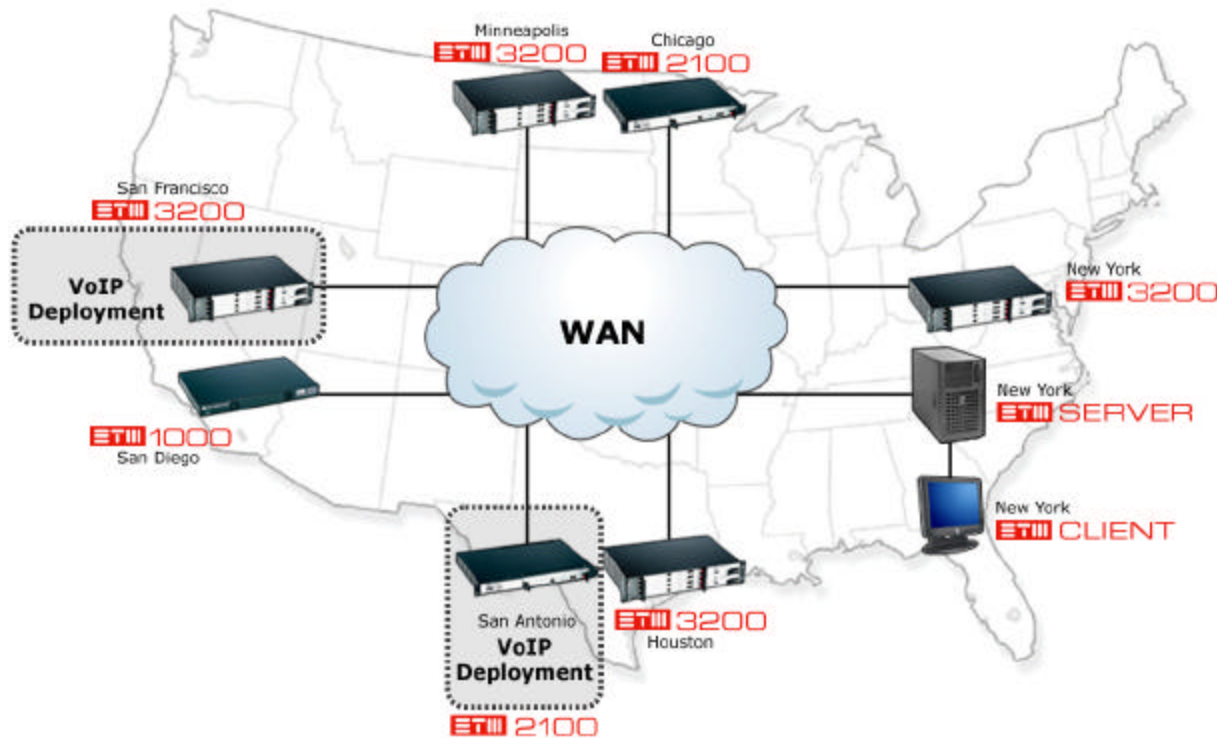


Figure 9 – Centralized Unified Voice Management for Distributed Enterprises

5. Summary

The reality for enterprise communications is that hybrid TDM and VoIP based networks exist and must be managed as a single entity. The tools to manage this hybrid network are available, but they generally come packaged in expensive purpose-built wrappings, each with their own specific purposes in satisfying the FCAPS model. Large enterprises have the most flexibility in terms of resources and budget for installing these purpose-built management systems, but even they must take a step back and decide if this is the right approach. What is needed is an appropriately scaled but integrated system that addresses all aspects of the FCAPS model for providing end-to-end multi-vendor management and security of the voice infrastructure.

The ETM[®] System is built specifically for this purpose. It is the only system that combines many of the most desired FCAPS features in one platform, and is also the only platform that can perform across both TDM and VoIP networks.

The ETM System cannot do everything by itself however, and will certainly require support from other management systems. For example, fault management is a key

component of the FCAPS model, and the ETM System does not attempt to replace a well-designed fault management system such as the HPOpenView[®] management product. It can however, enhance the capabilities of fault management by monitoring other aspects of the network and its performance that might be overlooked by traditional enterprise network management systems.

The ETM System can also enhance the Alarm Management system with remote IP-specific troubleshooting tools manageable from a central location. A data security platform is also required to protect the network from lower-layer network attacks. This includes traditional data firewalls at perimeter locations and adjacent Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) with application filters for virus protection.

If it is determined that the security and management of hybrid networks is an important aspect of a VoIP migration strategy, then a system like the SecureLogix[®] ETM[®] System, which uses an integrated, scaleable approach to addressing the security and management issues of the converged networks should be seriously considered.

For more information on the ETM System , please visit the SecureLogix website at www.securelogix.com

Appendices

Appendix A: The ETM[®] System and the FCAPS Model

The tables below illustrate how the capabilities of the ETM System meet the key tasks of the five FCAPS model categories. The Fault and Configuration Management categories are included to show how the ETM Management System fulfills these obligations for its own environment. Also included is the real-time alert capability for feeding SNMP alarms to give the alarm manager additional visibility to any detected network faults.

Table 1 illustrates how the ETM System meets the FCAPS Fault Management requirements for Fault Management (i.e. monitoring, collecting, analyzing, correlating and troubleshooting network problems).

FCAPS: Fault Management	
Fault Management Tasks	ETM[®] System Feature Description
Alarm monitoring, collection and analysis	<ul style="list-style-type: none"> · The Infrastructure Manager allows the telephony manager to define and configure measurable thresholds for span/trunk error conditions. · Real-time alerts such as email, pages and SNMP traps can then be generated when line errors start to impact resource availability. · Color-coded alarm icons quickly identify telecom or ETM Appliance issues, including blue alarm icons for CO-side telecom issues and red alarms for PBX-side issues. A right click on the alarm pulls up filtered diagnostics specific to the span and the alarm. · SNMP capability is provided for alerting on performance thresholds and security breaches.
Trouble detection	<ul style="list-style-type: none"> · VoIP networks can be further analyzed with PING and Traceroute commands launched from the distributed ETM Appliances, to provide remote troubleshooting capability. · A packet sniffer is supplied on each appliance to analyze packet signaling flows, and if desired, provide a textual display of the packets, as they cross each appliance boundary. · Telecom management and IT security personnel are provided the same level of notification when security or resource-availability policy rules are triggered, including real-time notification via console, email, pager or SNMP trap. · Larger enterprises with multiple management servers can receive consolidated screen alerts to a single console. This aids in the centralized monitoring and support of a larger number of servers, regardless of their geographical locations.
Trouble correction	<ul style="list-style-type: none"> · The ETM Appliance can be remotely rebooted and managed.

Table 1 – The ETM[®] System Meets FCAPS Fault Management Requirements

Table 2 illustrates how the ETM System meets the FCAPS Configuration Management requirements of identifying and tracking network resources and orderly change management and upgrade of ETM System components.

FCAPS: Configuration Management	
Configuration Management Tasks	ETM® System Feature Description
System turn-up	<ul style="list-style-type: none"> The ETM System provides highly secure, scalable, remote management of platform components, including distributed policy update and mass update of appliance applications software, firmware, and boot code. Updates can be applied to hundreds of remote appliances with minimal interaction by operations personnel beyond reviewing the update log to ensure that all devices have been updated and are operational.
Network provisioning	<ul style="list-style-type: none"> The ETM System is perfectly suited for analyzing usage patterns across the PSTN, providing vital details to assist with the dimensioning of a customer's VoIP network. The ETM Usage Manager provides a report summarizing the call loads on the PSTN interconnections, peak usage, and identifying all detected modems and faxes in the network.
Database handling	<ul style="list-style-type: none"> An Oracle® relational database allows statistical collection, analysis and historical record keeping.

Table 2 – The ETM® System Meets FCAPS Configuration Management Requirements

Table 3 illustrates how the ETM System meets the FCAPS Accounting Management requirements of collecting resource utilization metrics and enabling billing of end users and departments for their usage of network.

FCAPS: Accounting Management	
Accounting Management Tasks	ETM® System Feature Description
Service usage tracking and reporting	<ul style="list-style-type: none"> Infrastructure Manager provides real-time enterprise-wide visibility into the use of voice network, reducing manpower required to manage the network. The ISDN-PRI Appliance detects and logs Wideband Video traffic to allow monitoring of video usage, and facilitate detailed resource utilization. VoIP call types are detected by identifying codec type. Codec definitions can be customized as needed A batch scheduling feature allows reports to be set up and run overnight and during other non-peak periods. This includes scheduling daily, weekly, or monthly detail and summary reports as required. On-demand report generation is also supported Multiple reports show the usage as a percent of single trunks, trunk groups, and arrays enterprise-wide. Reports include graphs by minute, hour, or day, trend lines for planning, and call detail records.

FCAPS: Accounting Management	
Accounting Management Tasks	ETM® System Feature Description
Services billing	<ul style="list-style-type: none"> Personal Identification Number (PIN) codes can be extracted from Station Message Detail Reporting (SMDR) and saved in the audit logs for processing with pre-defined reports, allowing reports generation for department-level billing.

Table 3 – The ETM® System Meets FCAPS Accounting Management Requirements

Table 4 illustrates how the ETM System meets the FCAPS Performance Management requirements of collecting, analyzing and reporting on end-to-end network performance metrics.

FCAPS: Performance Management	
Performance Management Tasks	ETM® System Feature Description
Data collection	<ul style="list-style-type: none"> The Health and Status display includes resettable counters for all of the various monitored TDM line conditions, such as CRC errors, frame slips...etc. VoIP reports are collected on jitter and packet loss in VoIP media streams (as reported in RTCP). Future enhancement to include active measurements and calculation of a Mean Opinion Score (MOS) to apply against policy-based thresholds. This MOS can be calculated at the appliance level at various points in the network, and applied against policy thresholds established for each appliance.
Report generation	<ul style="list-style-type: none"> A batch scheduling feature allows reports to be set up and run overnight and during other non-peak periods. This includes scheduling daily, weekly, or monthly detail and summary reports as required. On-demand report generation is also supported Multiple reports show the usage as a percent of single trunks, trunk groups, and arrays enterprise-wide. Reports include graphs by minute, hour, or day, trend lines for planning, and call detail records.
Data analysis	(See Report generation above)

Table 4 – The ETM® System Meets FCAPS Performance Management Requirements

Table 5 illustrates how the ETM System meets the FCAPS Security Management requirements of monitoring and controlling access to specific network resources and applications, limiting access to only authorized internal and external users, as well as implementing prescribed corrective actions when violations of established security policy occur.

FCAPS: Security Management	
Security Management Tasks	ETM[®] System Feature Description
Network Edge (NE) access control	<ul style="list-style-type: none"> · The Call Monitor screen can be focused on a specific span and channel, or VoIP NIC pair and VoIP session to support very granular traffic monitoring. · Calls can be manually terminated from the Call Monitor. Manual termination can be very effective when an alert is generated that does not block a call, but upon inspection the administrator determines it should be terminated. · One-click class restrictions/call blocking allows the administrator to secure the network by controlling which calls are allowed or terminated, based on: <ul style="list-style-type: none"> · Call type · Source phone number · Destination phone number · Date/time · Call direction (inbound / outbound) · Call duration · The ability to define which calls are allowed into or out of the organization effectively eliminates security and resource abuse threats such as: <ul style="list-style-type: none"> · Unauthorized modems accessing the data network · Misuse of fax lines · Voice or modem calls to restricted equipment such as PBX or VoIP server maintenance ports · Call type recognition allows creation of specific rules that allow some call activities while terminating others. This can effectively force use of the secure Remote Access Server (RAS), eliminate administrator-configured remote access points and prevent fax misuse. This level of detail in policy rules is not possible on PBX's, which don't support call type recognition on a per call basis. Supported call types include: <ul style="list-style-type: none"> · Voice · Fax (now includes support for V.34) · Modem · Video (wide band) · STU-III Secure Phones · Unanswered · Busy · Undetermined · Discriminating between modems and STU-III allows policies that: <ul style="list-style-type: none"> · Allow STU-III secure calls while terminating modems · Enable detailed STU-III utilization reports showing number of secure calls by group over a period of time · Improve Secure Telephone Unit (STU)-III call type discrimination, to include older, 2400-baud devices.

FCAPS: Security Management

Security Management Tasks	ETM® System Feature Description
	<ul style="list-style-type: none"> · VoIP Codec's are detected and used to determine call type of associated media: <ul style="list-style-type: none"> · Compressed or uncompressed voice · Fax · Video · Call rejection allows calls to be terminated before the call type is established. Calls can be terminated based on direction, source phone number, destination phone number and time, or based on the absence of caller ID (CID) information. This feature allows unwanted calls, including international calls, calls to/from competitors, recruiters, telemarketing, etc. to be immediately terminated. · In VoIP, call flows can be managed to insure that network resources and critical network bandwidth are not overloaded. · ETM Telecom Firewall monitors the entire duration of a call, maintaining the call session state. If the call state changes during the call (e.g., from voice to modem), the security policy is re-evaluated to ensure that the call is still allowed to continue. · With VoIP systems, the ETM Telecom Firewall detects changes in codec type and adjusts accordingly.
NE function enabling	<ul style="list-style-type: none"> · Multiple reports are available which help identify potential toll fraud and support call detail-auditing functions. · Reports include charts to show highest incidents or use and call detail records to support further research or investigations. Examples of the information provided by this category of reports includes: <ul style="list-style-type: none"> · All calls during non-business hours: <ul style="list-style-type: none"> · International · Long distance · Calls over 30/60 minutes · Possible Toll Fraud: <ul style="list-style-type: none"> · Inbound DISA calls · Inbound voice mail calls · Outbound voice mail calls · Long distance minutes · Long distance numbers · Multiple reports to show security policy implementation and tracking results. Reports include charts to show highest incidents of use and call detail records to support further research or investigations. Examples of the type of information this category of reports provide includes: <ul style="list-style-type: none"> · STU Calls: call detail including time, duration, source, destination, and inbound STU calls. · Calls Terminated by Call Type: call detail including time, source, destination, inbound/outbound and trunk group. · Tracked Calls by Call Type: calls that generate alerts, emails or pages and the various tracks they fire on, including trends and call detail records.

FCAPS: Security Management	
Security Management Tasks	ETM[®] System Feature Description
Access logging	<ul style="list-style-type: none"> · Authorization, Authentication, Accounting (AAA) services provides additional security for authorized modems and other limited access services by forcing users who wish to utilize protected inbound or outbound systems through a distributed authentication server. Available in dual-port models, the AAA Server operates solely in voice mode, prompting the remote caller for a valid user-id, PIN code and destination number prior to allowing any connection attempts to the requested system. · AAA Servers run an embedded, real-time version of Hard Hat[®] Linux. Supporting fully distributed operations, the systems can be installed in strategic locations and linked to an ETM Management Server for remote configuration and software updates via connection to the IP network. · AAA services is applicable to VoIP networks when using a Hybrid analog/VoIP appliance such as the 1012/1024. By selecting the hybrid approach, AAA appliances can be used to grant access to certain analog ports for modem usage. AAA is managed as an adjunct service to the VoIP security and management services. This is a key component to the hybrid story.
User-level access monitoring	<ul style="list-style-type: none"> · The ETM System utilizes the same access control features found on traditional IP security devices used to restrict visibility and control to authorized personnel: <ul style="list-style-type: none"> · User accounts based upon username and passphrase · Enforcement of passphrase aging (maximum and minimum) and passphrase uniqueness · Real-time account disabling and lockout · Privilege limits varying from "view only" to full administrative rights

Table 5 – The ETM[®] System Meets FCAPS Security Management Requirements

Appendix B: Acronyms

3DES – Triple Data Encryption Standard
AAA – Authorization, Authentication, Accounting
CAC – Call Admission Control
CDR – Call Detail Record
CID – Caller ID
CO – Central Office (carrier or telephony provider)
DISA – Direct Inward Service Access
DoS – Denial of Service
DTMF – Dual Tone Multi-Frequency
EM – Element Manager
FCAPS – Fault, Configuration, Accounting, Performance, Security management
IDS – Intrusion Detection System
IP – Internet Protocol
IPS – Intrusion Prevention System
IPT – Internet Protocol Telephony
ISO – International Standard's Organization
ITU – International Telecommunications Union
LAN – Local Area Network
MOS – Mean Optical Score
NE – Network Edge
NIC – Network Interface Card
NMS – Network Management System
NOC – Network Operations Center
OSI – Open System Interconnection
PBX – Private Branch eXchange
PIN – Personal Identification Number
PRI – Primary Rate Interface
PSTN – Public Switched Telephone Network
QoS – Quality of Service
RAS – Remote Access Server
RTCP – Real Time Control Protocol
SLA – Service Level Agreement
SMDR – Station Message Detail Reporting
SNMP – Simple Network Management Protocol
STE – Secure Telephone Equipment
STU – Secure Telephone Unit
TDM – Time Division Multiplex
VPN – Virtual Private Network
VoIP – Voice over Internet Protocol
WAN – Wide Area Network

Reference

[1] Herrell, Elizabeth, *Resolving Security Risks for IP Telephony; What Companies Need to Consider when Deploying Voice on Data Networks*. Forrester Research, Inc., August 23, 2004.

SecureLogix, SecureLogix Corporation, ETM, the ETM Emblem and the SecureLogix Diamond Emblem are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

© Copyright 2004 SecureLogix Corporation. All Rights Reserved. U.S. Patents No. US 6,249,575 B1, US 6,320,948 B1, US 6,542,592 B2, US 6,687,353 B1, US 6,700,964 B2, US 6,718,024 B1, US 6,735,291 B1, and US 6,760,420 B2. U.S. and Foreign Patents Pending.



13750 San Pedro, Suite 230 • San Antonio, Texas 78232 • PH: 210.402.9669 • FX: 210.402.6996 • TF: 800.817.4837
www.securelogix.com
