ETM® (Enterprise Telephony Management) System

Technical Discussion

Release 7.1.x

A product brief from SecureLogix Corporation
Contents

ETM® (Enterprise Telephony Management) System Technical Overview ......................................................... 1
  Introduction .................................................................................................................................................. 1
  System Components .................................................................................................................................. 3
  Distributed System .................................................................................................................................... 4
  Unified Communications Support ............................................................................................................. 5
ETM® System Application Suite..................................................................................................................... 6
  The Performance Manager ......................................................................................................................... 7
  The Directory Manager ............................................................................................................................... 9
  Voice Firewall .......................................................................................................................................... 10
  Voice Intrusion Prevention System (IPS) .................................................................................................... 12
  The Usage Manager ................................................................................................................................. 14
  Call Recorder .......................................................................................................................................... 16
  Syslog Alert Tool ..................................................................................................................................... 18
ETM® Platform Appliance and VNM&S Application Technical Discussion ....................................................... 19
  Voice Network Circuit Type Support .................................................................................................... 20
  Supported Platforms ................................................................................................................................. 21
    SecureLogix® Communications Appliances .......................................................................................... 22
  Other Supported Platforms for the ETM® VNM&S Applications ................................................................. 24
  Application Appliances ............................................................................................................................. 24
ETM® Appliance and VNM&S Design ........................................................................................................... 25
  ETM® Analog Appliance Details ................................................................................................................ 25
  ETM® Digital TDM Appliance Details ....................................................................................................... 26
  ETM® Inline SIP Application Details ........................................................................................................ 29
  Unified Trunk Application (UTA) Details .................................................................................................... 31
ETM® Appliance Application Reliability ......................................................................................................... 33
  TDM Appliances ...................................................................................................................................... 33
  Inline SIP Application ............................................................................................................................... 34
  UTA ......................................................................................................................................................... 35
  Signaling and Phone Number/URI Access .................................................................................................. 36
  UTA ......................................................................................................................................................... 36
  TDM and SIP .......................................................................................................................................... 36
  Call Type Determination ............................................................................................................................ 37
  Policy Execution ....................................................................................................................................... 38
    Firewall Policy Execution ......................................................................................................................... 38
    IPS Policy Execution ............................................................................................................................... 39
    How Spans Monitor Calls ......................................................................................................................... 39
  Caller ID Authentication (CIDA) ................................................................................................................ 40
  Local ETM® Appliance Application Storage .............................................................................................. 41
  ETM® Appliance Access ............................................................................................................................. 41
ETM® Server Technical Discussion ................................................................................................................. 42
  ETM® Appliance and VNM&S Application Configuration Management .................................................. 43
  ETM® Database ....................................................................................................................................... 43
  SMDR/CDR ............................................................................................................................................. 44
  Tracking Events ...................................................................................................................................... 45
  Data Network Traffic ................................................................................................................................. 45
    Data Network Traffic Between the ETM® Server and Appliance Applications ...................................... 45
Other Types of Data Network Traffic..................................................................................................................47
Report Server Implementation................................................................................................................................48
ETM® Client Technical Discussion ......................................................................................................................48
ETM® System Security ........................................................................................................................................49
ETM® Client & Server Security ...........................................................................................................................52
ETM® Voice-Network Monitoring & Security (VNM&S) Application Security .....................................................52
Introduction

Strong security against the growing tide of attacks targeting enterprise Voice and Unified Communications (UC) resources has never been more business-critical. Real-time, interactive communications such as Voice/UC represent a large quotient of enterprise interactions, transactions, networks, systems, and applications, and these critical resources face a host of security and abuse threats. While Voice Network security has always been and remains a serious issue in legacy voice networks, the adoption of VoIP/UC has made it an even larger problem. The transport mechanism itself is not the real target; rather, VoIP has made some newer attacks, such as Telephony Denial of Service (TDoS), more practical and also made it easier to execute the same sort of inbound, application-level attacks that have been serious threats for years financial fraud/social engineering, call pumping and toll fraud, harassing calls, voice SPAM and phishing. In addition, other forms of threats and misuse/abuse exist as always, whether or not VoIP is used, such as internal abuse of outbound toll services, unauthorized access to voice systems, and large-scale outsider theft of outbound toll services via compromised IP-PBXs or voice gateways.

These types of voice attacks cannot be adequately addressed with traditional IP firewalls or Session Border Controllers (SBCs/eSBCs), which function at the transport layer or offer only static routing tables that must be manually maintained. Universal, real-time, adaptive UC application-layer security and call control policy is required to adequately address these and other threats. Failure to manage these security issues compromises enterprise productivity, information security, and regulatory compliance, and results in:

- High-profile service outages (TDoS attacks)
- Loss of contact center uptime and impaired customer response times/satisfaction (TDoS attacks and negative-value calls)
- Financial fraud against the enterprise and/or its customers (Social engineering and other fraud schemes)
- Theft of proprietary information and increased compliance costs (Unauthorized access to sensitive resources)
- Financial exposure from theft and/or abuse of toll service (External and internal)
- Loss of safety and business productivity (Harassing and malicious calls)
In addition to the host of security and abuse threats, Voice Network management challenges abound, including:

- Network optimization.
- Resource utilization monitoring.
- Trunk status and Quality of Service (QOS) monitoring.
- Call accounting.
- Cost accounting.
- Voice Over IP (VoIP) migration planning.
- Tracking of busy and unanswered calls on key lines, such as Customer Service and call center lines.

The ETM® System addresses these threats and challenges. The ETM System includes Voice-Network Monitoring & Security (VNM&S) applications deployed via software or hardware on customer-premises voice networks. These VNM&S applications monitor and control voice lines in real time and are controlled by a central ETM Management Server that can be managed from any number of distributed ETM Client applications. The applications deliver configurable real-time alerting and call-access control (CAC) for issues and calls of interest. Each ETM Client can be used to manage multiple ETM Servers and hundreds of distributed VNM&S applications, with both IPv4 and IPv6 supported. All call data, security tracking, and monitoring data for every call seen by the ETM System is stored in a secure, central relational database for enterprise-wide reporting.

The ETM System supports a number of powerful security and management applications and is upgradable to allow for expansion to support future applications.

Figure 1 provides a high level overview of one configuration of ETM System components:
A high-level description of the ETM System components is as follows:

- **ETM® Voice-Network Monitoring & Security (VNM&S) Applications** — ETM VNM&S applications support a wide variety of hardware platforms and TDM and VoIP protocols and can be deployed in various configurations and hardware platforms appropriate to your voice network. These ETM VNM&S Applications continuously patrol all signaling and bearer traffic (optionally in some configurations), and use an expandable policy engine to examine calls and take actions based upon user-defined rules. Actions include logging, alerting, call termination, call redirection*, call recording, and outbound CPN masking*. These ETM Applications are remotely managed and can be remotely upgraded with new software and applications.

  *Supported on most applications.

- **ETM® Server Applications** — The ETM Server Applications consist of processes that collect data from ETM VNM&S Application, maintain system configuration and policy data, store all call and policy data in a central relational database, and generate reports. The ETM Server Applications are centrally managed by one or more distributed, authorized ETM Client Applications. The ETM Server consists of the ETM
Management Server, an Oracle Relational Database Management System (RDBMS) server, and the ETM Report Server. These processes can run on one or multiple physical servers to allow the system to be configured to meet customer requirements.

- **ETM® Client Applications** – The ETM System Console is the client GUI that connects to the ETM Server to monitor and control the entire ETM System. All security, management, and real-time visibility functions are available via this client and the other ETM Client Applications launched from this master client. The ETM Client Applications provide a visual representation of all ETM System hardware and each monitored circuit. Additional “drill down” features are available for status review and diagnosis of problems. These client applications also include tools for Appliance Application and Server administration, log review, call monitoring, viewing of real-time alerts, and user account configuration. All security, management, policy enforcement, and real-time visibility functions are accessed via this client, which allows login to multiple ETM Servers and access to common tools that operate across ETM Servers. Additionally, these client applications provide the user interface framework into which additional security and management applications are integrated.

- **ETM® Application Appliances**—ETM Application Appliances provide large local Call Recorder storage. ETM Application Appliances support remote management and upgrade.

- **ETM® Web Portal**—The ETM Web Portal provides a secure, remote means of access to Call Recordings and certain ETM System Reporting features from an Internet Explorer web browser. Authorized users can schedule automated reports, view generated reports, and access call recordings, all via a secure web interface.

**Distributed System**

The ETM System is fully distributed; the components communicate via TCP/IP, with both IPv4 and IPv6 supported. The ETM Server can manage one to many VNM&S Applications. The local Client on the ETM Server system and any remotely installed, distributed Client Applications can be used to manage one or multiple instances of the ETM Server. All policy, configuration, and software upgrades can be downloaded from the ETM Server via the ETM Client to all managed VNM&S Application. Each link between components of the ETM System can be protected with strong authentication and Triple DES (3DES) encryption.

Figure 2 is an example in which one ETM Server manages multiple distributed VNM&S Applications, with multiple available distributed ETM Clients.
Unified Communications Support

The ETM System supports both circuit-switched and packet-switched trunk interfaces. While circuit-switched networks are still prevalent, many enterprises are beginning to plan and execute a migration to Unified Communications (UC) using VoIP for the voice network. The ETM System offers several solutions that support SIP trunks from the carrier, providing all of the functions of the ETM System for both TDM and SIP calls, including termination of unauthorized calls. Additionally, one implementation of the VNM&S Application supports both TDM and multiple VoIP protocols simultaneously.

Each ETM Application allows unified security, management, and reporting, independent of the underlying transport. VoIP support is integrated throughout the ETM System to ensure that enterprises can seamlessly transition from a circuit-switched to a VoIP network without compromising security.

Figure 3 illustrates the ETM System’s management and security applications’ support for both circuit-switched and packet-switched trunks.
ETM® System Application Suite

The ETM System offers several bundled and optional voice network monitoring, security, and management applications. These include:

- **Performance Manager**—Provides real-time visibility into trunk health and status, VoIP QoS alerts, and secure, remote management of distributed telecom resources.

- **Directory Manager**—Used to manage the directory of phone numbers and VoIP Uniform Resource Identifiers (URIs) accessible to all of the ETM Applications.

- **Voice Firewall**—Provides voice-network access and usage monitoring and real-time attack detection and mitigations for individual calls via blocking, alerting, or call redirection. Policy Rule settings include any combination of called and calling number, call direction, duration, time of day, call type, mid-call DTMF digit patterns, certain VoIP attributes, or specified audio patterns.

- **Voice IPS**—Provides for real-time call-pattern anomaly monitoring, attack detection, and mitigation for toll fraud, war dialing, TDoS attacks, and service abuse/misuse via blocking, alerting, or call redirection.

---

Figure 3 - Firewall Policy defined to protect both circuit-switched and SIP trunks
IPS Policy settings include any combination of call counts of both specified phone numbers or previously unknown numbers, cumulative cost, time of day, call type, cumulative call duration, mid-call DTMF digit patterns, lack of expected DTMF digits, Service Types (such as Long Distance or International calls), termination disposition, direction, and specified audio patterns.

- **Call Recorder**—Provides Policy-based call recording of targeted calls of interest. Rule criteria include any combination of called and calling number, time of day, call type, and direction. Recorded calls can be remotely accessed from a secure, browser-based Web Portal.

- **Usage Manager**—Provides enterprise-wide call-accounting, QoS, and voice-network security/monitoring reporting, with both ad-hoc and scheduled reporting options. Generated reports can be remotely accessed from the Usage Manager client application or from a secure, browser-based Web Portal.

- **Syslog Alert Tool**—The SecureLogix Syslog Alert Tool automatically notifies a workstation user when a system event and/or policy alert, such as a 911 call, is received from the ETM® Syslog Server.

**The Performance Manager**

The ETM Performance Manager provides unified, real-time, PBX- and media-independent monitoring and a consolidated, comprehensive view of voice service performance across the enterprise. It provides a consolidated, dashboard view of any hybrid network mix of multiple-vendor systems, trunking protocols, and TDM/VoIP media types found in today’s converging networks. The real-time console provides up-to-the-minute alerting on QoS events, changes in operational status of the network, and violations of established security and usage policies. Additionally, console, email, syslog alert, or SNMP trap notifications can be assigned to any monitored event.

Some of the key features the Performance Manager provides include:

- **Centralized, Real-Time Health and Status**—Real-time, enterprise-wide, single-view health-and-status monitoring of TDM & VoIP signaling error conditions on all monitored circuits.

- **Real-time Notification of Availability and QoS**—A wide variety of telecom events can be configured to generate real-time notifications when line errors impact service quality or availability.

- **Call Monitor Real-Time Call Display with Call Termination**—The Call Monitor displays active call information with call-type data on all inbound and outbound calls. The Call Monitor can be configured to view an individual channel, Span, group of Spans, or all Spans enterprise-wide. Suspect calls can be manually terminated in real time by right-clicking the call in the Call Monitor.
• **VoIP Codec Configuration and Monitoring**—A **VoIP Codec** GUI includes more than twenty predefined, ITU-standard codecs to allow you to establish QoS thresholds that include values for packet loss, delay, and jitter and to be alerted if these thresholds are exceeded.

• **Caller ID Masking and Call Redirection**—Allows Policy-based, granular, source-dependent generation of the Calling Party Number (CPN) to be reported for outbound calls and allows inbound and outbound redirection of calls. *(Redirection on all but T1 and Analog Spans; masking on all but UTA.)*

• **Logical Span Groups**—Fully logical Span groups allow for independent grouping of Spans (regardless of PBX configuration) to support trunk groups and distribute security and usage policies. Spans from different ETM Appliances and PBXs can be grouped and managed as a unit.

• **Troubleshooting Tools**—Alarm icons alert to circuit errors and an easy-access health-and-status display provides details. Distinct color-coded icons, logical grouping of functions, and automatic diagnostic log filtering allow you to quickly isolate potential line errors, immediately determine the severity of errors, and gain vital troubleshooting information. A command-line interface provides quick access to Span/trunk diagnostics to aid in faster resolution of circuit issues with the service provider.

• **Visibility of Telecom Signaling**—Allows verification of purchased services such as DID (Direct Inward Dial) and DNIS (Dialed Number Identification Service) and operation of automatic dialers in call center environments.

• **Policy Applications Interface and Monitoring Tools**—The Performance Manager provides the interface to the Voice Firewall, Voice IPS, and Call Recorder applications; CPN masking, call redirection, and billing plans; and tools for call monitoring, log review, and diagnostic analysis.

Figure 4 shows several Performance Manager screens. At the left is the graphical tree representation of the ETM System Policies, Span Groups, telco configuration and monitoring, and ETM Appliance configuration and monitoring. Additional “drill down” features are available from the tree pane and main menu for review of the status of Cards/Spans, circuits, and active calls. A **Performance Monitor** tool shown in Figure 5 is accessed from the ETM System Console; it shows only resources with error conditions, and provides drill-down access to the affected resource.
The Directory Manager

The Directory Manager is used to manage the directory of phone numbers and VoIP Uniform Resource Identifiers (URIs) available to all of the ETM Applications. These Directory “objects” and their associated information are used in policies and reports and to annotate real-time notifications (such as for 911 calls), real-time display of call data, log data display, policy generation, and reporting.

The Directory Manager acts much like a phone book by providing a linkage between a phone number and/or URI and a real world entity. For example, the Directory Manager might have a “listing” for 555-1234 or 5551234@mycompany.com to be associated with “John Doe in Marketing that works for Mary Smith located in Building 2 at the San Antonio site.” The Directory Manager is typically populated from an existing enterprise database, and also accommodates manual entry. The Directory Manager also provides a powerful import and
reconciliation tool that allows the Directory Manager to stay in sync with the enterprise LDAP or similar repository, and for importing specialized lists, such as the SecureLogix proprietary National Harassing Caller List. Figure 6 shows a sample Directory Listing in the Directory Manager GUI.

![Figure 6—Directory Manager]

**Voice Firewall**

ETM Voice Firewall Policies allow you to accomplish one or more of the following actions for a given call:

- Allow, terminate, or redirect the call.
- Log the call as triggering a firewall rule, with associated data.
- Alert one or more personnel and/or network monitoring (NMS)/security information event management (SIEM) systems through real-time desktop alert, email, syslog alert, or SNMP trap. Filtering options target alerts to appropriate recipients.

As shown in Figure 7, a Policy contains some number of user-defined Rules. Each Rule can specify any combination of the following call criteria: call direction (inbound or outbound), called and calling numbers, call type, time of day, call duration, certain VoIP call attributes, mid-call DTMF digit patterns of interest, action to be taken against matched calls (allow or terminate), Tracking and alerting actions for matched calls, and which
of the available Span Groups to install the Policy on. Rules are evaluated for every call monitored by the ETM VNM&S application on which the Policy is installed. Call parameters are compared to the criteria specified in each rule in numerical sequence. If a match occurs, the application performs the specified action (allow or terminate) and the ETM Server executes the specified Track Action (log, generate a screen alert, send an email, and/or send an SNMP trap or syslog alert). If no user-defined rule matches the call, the call is allowed by the “implied” Catch-All Rule (the last Rule in every Firewall Policy) that allows all calls that do not match a previous rule. 911 calls always match the implied Emergency Rule (the first rule in every Firewall Policy), which always allows any outbound call beginning with the digits 911, regardless of any other dialed digits.

A call must match all of the parameters in the Rule before it is considered to match the Rule. When all of the parameters of a Rule match, the Rule is said to fire.

Once defined, Voice Firewall Policies are installed it on the ETM VNM&S Applications securing the voice network. The VMN&S Applications then enforce the Policy in real time, and send all call and Policy enforcement data to the ETM Server, which generates any defined alerts, and stores all call and Policy data in the central ETM Relational Database.

Figure 7—Voice Firewall Policy
Details about how call parameters are determined and used for Policy are discussed later in this document in the “ETM® Platform Appliance and VNM&S Application Technical Discussion.”

You can build any number of Policies as appropriate to your enterprise. For example, you can develop specific Policies for trunk groups or sites, or you can build one large Policy in which some Rules apply to different trunk groups/sites. You also can pre-build multiple Policies to address various security and management concerns, so that they are available to be installed immediately as security conditions change, such as evidence of an attack or virus.

**Voice Intrusion Prevention System (IPS)**

The ETM Voice Intrusion Prevention System (IPS) provides real-time detection and prevention of threatening or abusive call patterns, including toll fraud, TDoS attacks, modem war dialing attacks, service abuse, and other pattern-based attacks.

Voice IPS Policies allow you to establish real-time thresholds for a variety of service types, such as long distance or international calls, and for specified call count thresholds from known or unknown source numbers, accumulated call duration, accrued toll charges, mid-call DTMF digit patterns, and audio signatures. Voice IPS Policies can terminate malicious or abusive call activity in real-time, limiting an organization’s financial exposure to toll fraud. The application also includes a real-time viewer that displays the values for all set thresholds, including current call counts (with the offending source number for rules counting previously unknown numbers), current cumulative call duration, and current accrued toll charges, for all configured Policy Rules.

Usage Manager reports help determine historical baselines and expected call activity and expenses for defining appropriate call pattern thresholds in IPS Policies. Historical baselines can be calculated using min, max, mean, and standard deviation. Voice IPS call count, cumulative call duration, and accrued cost are recorded in the database, providing a historical summary of each rule interval. These rule summaries can be used to generate historical reports very quickly to identify appropriate baselines.

Figure 8 demonstrates how a Voice IPS policy can be structured to monitor a variety of calling patterns on the enterprise voice network.
Figure 8—Voice IPS Policy

Figure 9 demonstrates how the summarized results for a Voice IPS Rule can be plotted with standard deviations to facilitate threshold selection.

ETM® System

Figure 9—Voice IPS Report
The Usage Manager

The Usage Manager provides reporting access to the ETM Relational Database that stores all of the CDR, call type, codec, Voice Firewall and IPS policy processing, trunk status, QoS statistic, resource utilization, and network security event data captured by the ETM System. The Usage Manager GUI, shown in Figure 10, provides an extensive set of predefined report templates and a powerful, integrated report editor for modifying existing templates or defining new reports. Report data can be formatted, grouped, charted, and filtered in a variety of configurations, offering exceptional flexibility in reports design and analysis. In addition to the Usage Manager’s powerful reporting capabilities, the published ETM Database Schema allows for reporting access to the ETM Database by third-party tools, and SecureLogix offers Managed Services that provide more in-depth Business Intelligence (BI) reporting and analytics.

Figure 10—Usage Manager

Fully customizable billing plans and user/extension Directory support allow for highly accurate cost allocation or bill verification auditing and call accounting. Integrated North American and International location databases provide detailed identification of called/calling party country and city-state information.
Regular updates to the location databases are available from the SecureLogix Support Web site. Figure 11 is a sample report showing International call details, including calling party location information.

**ETM® System**

<table>
<thead>
<tr>
<th>Start Time</th>
<th>In/Caller</th>
<th>Internal Number</th>
<th>External Number</th>
<th>External Number</th>
<th>External Number</th>
<th>Duration</th>
</tr>
</thead>
</table>

**Figure 11—Sample Detailed Usage Manager Report with Location Data**

Reports can be previewed, printed, and saved to a variety of formats, including Portable Document Format (PDF), PostScript (S), Hypertext Markup Language (HTML), Rich-Text Format (RTF), and Comma-Separated Values (CSV). Reports can be distributed via email, saved in the Usage Manager tree pane, or stored on a network share for enterprise-wide access.

The Usage Manager also provides a flexible scheduling tool that allows reports to run automatically on a regular basis (daily, weekly, monthly, quarterly, etc.). These Scheduled Reports can be automatically distributed via email, saved in the Usage Manager tree pane, or stored on a network share for enterprise-wide access.

A web-browser interface is available for remote access to reports saved to the Usage Manager tree pane.
Call Recorder

The ETM Call Recorder provides policy-based recording of the audio and data content of targeted calls of interest: For example, Call Recorder Policy Rules can specify:

- Record all inbound calls to the Call Center for quality assurance and security monitoring.
- Record calls on selected fax, modem, or STU-III lines to verify that classified or sensitive information is not being disclosed.
- Record calls from/to customer support lines, to provide an audit trail.
- Capture threatening or harassing calls for investigation.
- Ensure that calls to sensitive extensions are never recorded, or are flagged as sensitive.

Since the recording is policy-based, no user intervention is needed to begin recording—recording begins automatically at the start of a call for the specified extensions and call direction. A user-definable blacklist/whitelist function enables you to ensure that calls to protected or sensitive extensions, such as pharmacy lines, are never recorded regardless of policy settings, or are flagged as sensitive and stored separately in a secure directory on the Collection Server for access only by authorized HIPAA-trained personnel.

The Call Recorder uses the same policy-based call selection paradigm and many of the same data fields as the Voice Firewall and Voice IPS to select the calls of interest. A Call Recorder Policy uses any combination of the following call attributes to specify the calls to record: call direction (inbound, outbound); source and destination; call type; and time of day. You can also write Rules to specify calls not to be recorded, using those same criteria.

Call Recordings are stored on a Call Recorder Cache (CRC), and optionally can be transferred to a Collection Server application for long-term storage. From these storage locations, recordings can be remotely accessed via the secure browser-based Web Portal.

In addition to specifying the calls of interest, the Call Recorder Policy allows a priority to be assigned to each recording. The Priority setting governs the order in which calls are transferred from the CRC to the Collection Server, if one is used, and for deleting recordings from the CRC when disk space limits are reached. It does not affect whether calls are recorded. Figure 12 shows a sample recording policy.
The Call Recorder uses a distributed architecture, illustrated in Figure 13.

The Call Recorder architecture comprises the following components:

- **The ETM Server** to manage the Recording Spans and the Call Recorder Cache (CRC) application(s), and to provide recordings to the Web Server for access via the Web Portal.

- **The Call Recorder application**. Installed on the ETM Server and accessed via the Performance Manager; used to define, manage, and install Recording Policies; and specify the optional .wav greeting file to be played to callers on Analog recording Spans.

- **One or more recording-enabled ETM Spans** to transfer calls to a CRC application, where they are recorded in real time. All Span types can be recording-enabled via software. Analog Spans in the ETM
1012/1024 Appliances can optionally play an announcement at the start of the call. Digital Spans rely on the announcement capability of the PBX.

- **A Call Recorder Cache (CRC) application** to which the recording Spans transfer information to be recorded. The CRC application can run on the 1024, 1090, 1060, or 5160 Appliances and on the UTA and inline SIP applications.

- **The ETM Web Portal** to locate and access call recordings stored on the CRC or Collection Server.

- **(Optional) A Collection Server** for large offsite storage of call recordings. The Collection Server is a Windows application that runs on Windows 2003 or later. When a Collection Server is used, CRC applications send the audio files and associated call data for the recorded calls at user-defined intervals to the Collection Server for storage. The Collection Server runs a call record filter to convert each recorded call’s audio file and call data from its received format to a final format that is compatible with third-party playback and analysis tools such as TSAP and Windows Media Player.

For more details about Call Recorder, see the *ETM® Call Recorder Technical Discussion*, published under separate cover.

### Syslog Alert Tool

The SecureLogix Syslog Alert Tool automatically notifies a workstation user when specified system events and/or policy alerts, such as a 911 call, are received from the ETM® Syslog Server. When a user logs in to a workstation on which the Syslog Alert Tool is installed, the program automatically launches and runs continuously as a background process.

When a system event and/or policy alert, also referred to as a syslog alert, is received, all of the following actions occur:

- An audible tone sounds.
- The **SecureLogix® Syslog Alert Tool** window and the **Acknowledge Alert(s)** window are both proximately displayed in front of all other currently running applications with detailed information about the syslog alert.
- The Syslog Alert Tool icon in the system tray displays a “New Alert(s) Received” message.
- The alert is written to an alert log text file.

The Syslog Alert Tool is shown in Figure 14.
The workstation user reviews alert details and acknowledges the alert(s) in the **Acknowledge Alert(s)** window. After acknowledging alerts, the **SecureLogix Syslog Alert Tool** window remains displayed in front of all other windows showing acknowledged alerts for the current user session.

If alerts are not acknowledged, any new alerts that occur are added to the **Acknowledge Alert(s)** and **SecureLogix Syslog Alert Tool** windows with the most recent alert highlighted.

After all alerts have been acknowledged, the **SecureLogix Syslog Alert Tool** window can be closed to the system tray. When a new alert is later received, the **Acknowledge Alert(s)** and **SecureLogix Syslog Alert Tool** windows are both again prominently displayed.

All syslog alerts received by the Syslog Alert Tool are added to a daily alert log text file allowing system administrator to view historical alert details.

**ETM® Platform Appliance and VNM&S Application Technical Discussion**

The ETM VNM&S Applications run on a variety of hardware platforms, including SecureLogix Communications Appliances (all application types), SRE-V modules in a Cisco Integrated Services Router (ISR) G2 (inline SIP or the Unified Trunk Application [UTA]), or COTS hardware that meets minimum system and resource requirements (UTA). UTA also supports virtualization.
Voice Network Circuit Type Support

The ETM System supports the following types of voice circuits and signaling types:

- **VolP**—The ETM System supports VolP with both an Inline SIP Application and UTA.
  
  - The ETM Inline SIP Application support SIP trunks from the carrier. These Applications are installed logically inline, enabling call termination. The SIP Application supports the following SIP specifications: RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3311, RFC 3325, RFC 3389, RFC 3550, RFC 3551, RFC 4566. This Application can be installed on the SecureLogix 5000-Series SIP Appliance, and SRE module in a Cisco ISR Router, or on COTS hardware that meets minimum system and resource requirements.
  
  - The ETM Unified Trunk Application (UTA) supports a variety of VolP Protocols along with TDM and functions in conjunction with the Cisco Unified Communications (UC) Gateway Services API available in recent versions of iOS for Cisco ISR G2 or ASR. This integration allows full call monitoring and call control, including call termination and redirection. It can be installed on a SecureLogix 5000-Series UTA Appliance, an SRE-V module in the ISR, or COTS hardware that meets minimum system and resource requirements. Virtual deployments are supported.

- **Analog**—Analog support is available on the ETM 1000-Series Communication Appliances. These support loop start, ground start, and reverse battery loop start trunks. They support FXS and FXO.

- **T1 CAS**—T1 CAS support is provided by either UTA or the ETM 1090, 2100, and 3200 digital Appliances.
  
  - When used with UTA, the physical connection is governed by the router and transparent to UTA.
  
  - The digital appliances support Super Frame and Extended Super Frame framing formats. Supports Alternate Mark Inversion and Bipolar 8 Zero Substitution line coding. Supports ground start, loop start, wink start, immediate start, and asymmetrical signaling. Supports various cable lengths (line build outs). Supports DTMF and MF digit detection. For fractional T1s, the Appliance can ignore non-voice channels.

- **E1 CAS**—E1 CAS support is provided by either UTA or the ETM 1090, 2100, and 3200 digital Appliances.
  
  - When used with UTA, the physical connection is governed by the router and transparent to UTA.
  
  - The digital appliances support CAS signaling on a 30-channel E1 Span. Supports the CRC4 Multiframe and Non-CRC4 Multiframe framing formats. Supports Alternate Mark Inversion and High Density
Bipolar Order 3 line coding. Supports the R1 signaling type only. Supports MF and DTMF digit detection.

- **T1 PRI**—T1 PRI support is provided by UTA and the ETM 1090, 2100, and 3200 digital Appliances.
  - When used with UTA, the physical connection is governed by the router and transparent to UTA.
  - The digital appliance supports a 24-channel T1 Span using PRI signaling (often referred to as ISDN PRI). Supports the DMS100, ATT 5ESS, ATT 4ESS, and NI-2 variants. Supports Non-Facility Associated Signaling (NFAS). NFAS allows multiple PRI Spans to be controlled from a single D channel. Supports use of backup D channels.

- **E1 PRI**—E1 PRI support is provided by UTA and the ETM 1090, 2100, and 3200 digital Appliances.
  - When used with UTA, the physical connection is governed by the router and transparent to UTA.
  - The digital appliances supports a 30-channel E1 Span using European variants of ISDN PRI. Supports the NET5 and QSIG protocol variants. Certification testing was only performed against the NET5 protocol version, as customer demand for the other protocol variants is limited due to the widespread standardization on NET5. Support for DASS2 and DPNSS is also provided.

- **T1/E1 SS7**—Both fully associated and dedicated SS7 signaling are supported by the ETM 3200 Appliance.
  - For fully associated SS7 signaling Links, each SS7 Bearer Span provides support for up to two fully associated SS7 signaling links, allowing SS7 signaling links and bearers to be managed on the same Card. For dedicated SS7 Cards, the cPCI Card sets support 1 to 4 ANSI SS7 signaling links carried over a single DS1. The signaling links may be 56Kbps or 64Kbps (but must all be the same). This Card set is only packaged in the ETM 3200-Series Appliance. Note that in this configuration, the Card set cannot process bearer Spans, but can communicate signaling information to the other Card sets managing the bearer Spans.

**Supported Platforms**

Several types of ETM Appliance Application host platforms are available to suit various types of voice network environments and call volumes. The applications are remotely upgradable and manageable regardless of the hosting platform.
SecureLogix® Communications Appliances

SecureLogix Communications Appliances support the VNM&S Application. The following versions of the SecureLogix Communications Appliance are available. All are 19” rack mountable devices in 1u and 2u heights:

- **ETM® 1000-Series Communication Appliances**—The ETM 1000 Series Communications Appliances are 1u devices that support either 1 DS1 or up to 24 analog trunks. The TDM DS1 Span supports T1 and E1 line rates and either CAS or PRI signaling. The line rate and signaling type are software selectable. Available versions include:
  - 1012—Analog; 12 channels
  - 1024—Analog; 24 channels
  - 1024CR—Analog; 24 channels and local CRC
  - 1090—1 DS1 Span
  - 1090CR—1 DS1 Span and local CRC

  See “ETM® Analog Appliance Details” on page 25 for more information.

- **ETM® 2100 Communication Appliance**—The ETM 2100 Communication Appliance is a 1u device containing 1 compact PCI (cPCI) Card set that supports 1 to 4 DS1s in any combination of T1 Spans (PRI, CAS, and SS7) or E1 Spans (PRI, CAS, and SS7). This Card set includes a Digital Trunk Interface that provides the T1 or E1 interfaces, relays, and line interface units. The Card set also includes a Controller Card that provides the processors, memory, and other storage. The same chassis and Card set is used for T1 CAS, T1 PRI, E1 PRI, E1 CAS, and SS7 Spans. Each SS7 Bearer Span provides support for up to 2 fully associated SS7 signaling links, allowing SS7 signaling links and bearers to be managed on the same Card. The software supports mixing T1 or E1 circuit types on one Card set.

  See “ETM® Digital TDM Appliance Details” on page 26 for more information.

- **ETM® 3200-Series Communication Appliance**—The ETM 3200-Series Communication Appliance is a 2u device with 1 to 4 cPCI Card sets that each support 1 to 4 DS1s. The total capacity of this device is 16 DS1s in any combination of T1 Spans (PRI, CAS,
and SS7) or E1 Spans (PRI, CAS, and SS7). A Card set can also be used for one dedicated SS7 signaling link, or can support SS7 bearer Spans with fully associated signaling links. The chassis is cPCI and supports hot swapping controller Cards, power supplies, and fans. The hot swap capability enables any controller Card to be removed and replaced without impacting the operation of other Cards. During hot swapping, the Digital Trunk Interface is not affected, so the Spans continue to allow traffic. The power supplies are N+1 redundant and the device can operate with a single power supply. Both AC and DC power supplies are available. The available versions include:

**3200AC**—1 to 16 T1 or E1 Spans (CAS, PRI, or SS7)

**3200DC**—1 to 16 T1 or E1 Spans (CAS, PRI, or SS7)

See “ETM® Digital TDM Appliance Details” on page 26 for more information.

- **ETM® 5000-Series SIP Appliance**—ETM Inline SIP application functionality for carrier SIP trunks is provided by a set of integrated, modular software components that run on server-class platforms running a tailored version of the Linux operating system. These modular components include: a highly reliable inline Signaling Proxy, a highly reliable inline Media Proxy, and a Call Processor. The Call Processor interfaces with the ETM Server for all of the components in the SIP application, tracks call state, executes policy, and logs call events and other events. The SIP Signaling Proxy interfaces with the SIP Trunk (signaling) and acts as a logical endpoint to both ends of the SIP Trunk to extract signaling information from the trunk, enable media processing, and enable call termination. If media processing is enabled, the Media Proxy interfaces with the media carried on the SIP trunk and enables codec-based call type determination, media tracking, and call recording. Small, large, and enterprise versions are available. See the **ETM® 5000-Series SIP Appliance Technical Specification** data sheet for call capacities for each platform.

  See “ETM® Inline SIP Application Details” on page 29 for more information.”

- **ETM 5000-Series UTA Appliances**—The same physical hardware as the inline SIP appliances, configured to support UTA in conjunction with either a Cisco ISR G2 running iOS version 15.2(2)T or later or an ASR running iOS version XE3.8 or later. Small, large, and enterprise versions are available. Up to 15 instances of UTA can be virtualized on this platform, depending on the model used. See the **ETM® 5000-Series UTA Appliance Technical Specification** data sheet for call capacities for each platform.

  See “Unified Trunk Application (UTA) Details” on page 31 for more information.
Other Supported Platforms for the ETM® VNM&S Applications

- **SRE-V Modules for Cisco ISR G2**—UTA and the inline SIP application are both supported on SRE-V modules in an ISR G2. UTA requires iOS version 15.2(2)T or later on the router. Call capacities depend on the capabilities of the selected router.

- **COTS Hardware**—UTA can run virtually in a VMWare environment on COTS hardware that meets minimum resource requirements, such as the Cisco UCS family of servers. Call capacities depend on the capabilities of the selected router with which the application is interfacing, with the UC Gateway Services API enabled.

Application Appliances

ETM Application Appliances are used to supply call recording storage for the Call Recorder. Two are available:

- **ETM® 1060 CRC Appliance**—The ETM 1060 CRC is used to support the Call Recorder add-on application for customers requiring JITC-certified equipment. The 1060 CRC records and stores calls from multiple Recording Spans. This Appliance has no Spans and cannot monitor calls or execute a Recording Policy. It simply stores calls and optionally transfers them to a Collection Server. Each 1060 CRC supports:
  - 32 voice Spans (3200-, 2100-, or 1000-Series Hybrid)
  - Up to 120 simultaneous recordings
  - 2,000 hours of recording storage
  - Compression and encryption to the Collection Server

- **ETM® 5160 CRC Appliance**—The ETM 5160 CRC is used to support the Call Recorder add-on application for customers not requiring JITC-certified equipment. The 5160 CRC records and stores calls from multiple Recording Spans. This Appliance has no Spans and cannot monitor calls or execute a Recording Policy. It simply stores calls and optionally transfers them to a Collection Server. Each 5160 CRC supports:
  - 32 voice Spans (3200-, 2100-, or 1000-Series Hybrid)
  - Up to 200 simultaneous recordings
- 6,826 hours of recording storage
- Compression and encryption to the Collection Server

**ETM® Appliance and VNM&S Design**

All ETM Appliance and VNM& Applications use a tailored version of Linux. The version used includes the basic kernel and networking support. Networking support includes TCP/IP sockets and required network services (ICMP and ARP), which are used to communicate with the ETM Server and other Appliances (for NFAS and SS7). A custom and very restricted version of Telnet is provided as an optional service on TDM appliances and can be used to directly manage the Appliances from authorized Clients only. (For security reasons, Telnet access is disabled by default). SIP and UTA support SSH, which is also disabled by default. The Appliance uses the “IP Tables” capability provided by Linux to discard any IP packet that is received from a host with which the Appliance is not programmed to communicate.

All Appliance software is fully upgradeable. The operating system and application software, boot software, Digital Signal Processor (DSP) software (if applicable), and Field Programmable Gate Array (FPGA)/Programmable Logic Device (PLD) software (if applicable) are remotely upgradeable via the ETM Server and ETM Client.

**ETM® Analog Appliance Details**

The ETM 1012 and 1024 Appliances are designed for analog trunks. Relays are used in these Appliances to maintain a continuous circuit during normal operation and during power loss. The relays are only engaged for a few seconds when an ETM Policy directs termination of a call. During normal operation—even if power is removed—there is a continuous circuit through the Appliance. Figure 15 below illustrates this design. This Appliance adds no latency to the signal. These Appliances are deployed on the trunk side, between the CO and the PBX. They can also be deployed on analog circuits that connect directly to stations (typically remote access Servers or fax machines). However, these Appliances do not support vendor-proprietary digital station circuits.
ETM® Digital TDM Appliance Details

The ETM 1090, 2100-, and 3200 Platform Appliances for digital trunks should be installed between a Channel Service Unit (CSU) and the PBX. While these Appliances provide surge protection, the CSU is typically required for loop-back testing at the edge of the demarc by the local phone service provider. These Appliances can also be deployed outside an integral CSU if an equivalent Network Interface Unit (NIU), such as a “Smart Jack,” is provided. If the Appliance is deployed in a location where loop back codes/tests are sent, it detects this condition and transparently passes through the loop back codes/test. The Appliance does not attempt to process any signaling or audio on the circuits during loop-back testing.

For all digital TDM interfaces, relays are present and remain disengaged when the power is off, the Appliance is booting, or if the Appliance is taken off-line. In the disengaged state, there is a continuous circuit through the Appliance and absolutely no latency is added to the signal. The failsafe circuitry does add a small amount of resistance to the circuit, so the configuration should always be tested when circuit values such as signal strength or cable length are changed.

When the digital TDM Appliance is booted and ready to begin processing, the digital interface engages relays and routes the signal through several components. The signal is terminated by a Line Interface Unit (LIU), provided to the digital Appliance for processing, and regenerated by a second LIU. If power is interrupted, the digital Appliance is rebooted, or if the interface Span is taken off-line, the relays disengage with no loss of voice service.
When the digital TDM interface relays are engaged, the bearer/audio data is terminated and regenerated by the LIUs. This adds less than 1 millisecond of latency to the data. This is similar to the latency added by a CSU. A copy of the bearer data is provided to the DSP, which monitor the data for tones and call type. This processing is not inline and therefore adds no additional latency to the bearer data.

The digital TDM signaling data is terminated by an LIU, copied or passed inline to the microprocessor, and regenerated by the LIU. For T1 PRI, the signaling, in the form of D-channel messages, is passed to the microprocessor, which regenerates new D channel messages. This path adds some additional latency (less than 15 milliseconds) to the signaling, but does not affect the circuit or calls. This design is necessary to support call termination. Figure 16 illustrates this signaling path design.

On T1 CAS, a copy of the A-B bits is passed to the microprocessor. When call termination is needed, a command is sent to the LIU to generate the appropriate A-B bits. Figure 17 illustrates this signaling path design.
On SS7, a copy of the signaling is made for the microprocessor. Figure 18 illustrates this signaling path design.

Figure 17—T1 CAS Signaling Path Design

Figure 18—SS7 Signaling Path Design
On SS7, when call termination is needed, tones are played on the appropriate bearer Span and DS0. Figure 19 illustrates this design.

---

**ETM® Inline SIP Application Details**

The ETM Inline SIP application is installed logically inline on the enterprise SIP trunk. Call termination on the inline SIP Application proceeds as follows: On receipt of a command to terminate a call (or termination due to a reject rule), the Signaling Proxy statefully terminates the call by sending out call teardown messages to the SIP Trunk endpoints. Termination is performed in a stateful manner to facilitate proper call teardown and perform any necessary re-transmissions. In addition to terminating calls via SIP signaling, the Signaling Proxy also prompts media connections to be torn down in the Media Proxy, if media processing is active. Figure 20 illustrates this design.
Component Communication

The Call Processor, Signaling Proxy nodes, and Media Proxy nodes communicate via socket connections to enable the choice of combined deployment on fewer hardware platforms or distributed deployment across more hardware platforms. The hardware platforms hosting the SIP application components are interconnected using a private network, with the option of using IPSec to encrypt communication between components.

Call Load Capacity

Call load capacity scales according to the capacity of the hardware platforms chosen for a given deployment. See the ETM® SIP Application Technical Specification for a description of call capacity for each hardware platform.

Logically Inline Deployment

The ETM SIP application is installed logically inline (by IP address) with the SIP trunk signaling and media. It has defined IP addresses and acts as a SIP trunk endpoint to the local enterprise proxy and the remote service provider proxies. These are configured to route all SIP traffic on the specified trunk through the ETM SIP Appliance application, which proxies messages between the Enterprise’s SIP Trunk endpoints and the Service.
Provider. The primary benefit of being logically inline is that the SIP application need not sit physically inline on a chokepoint link. This enables the application to see all signaling and media traffic regardless of its physical location, reduces the scope of the traffic that must be processed, and enables clean and effective call termination. However, since the application is inline, it must be deployed in a redundant manner to prevent loss of service, with one or more backup Signaling/Media Proxies ready to seamlessly take control if the processing Signaling or Media Proxy becomes unavailable.

**Latency**

The ETM SIP Appliance application introduces extremely minimal latency to packets it processes so as not to impair voice quality. Latency limits are as follows:

- **Signaling packets:**
  - Invite message: < 3 ms
  - Non-Invite message with SDP: < 1 ms
  - Non-Invite message without SDP: < 500 µs

- **Media packets:** No more than 100 µs.

**Unified Trunk Application (UTA) Details**

The ETM Unified Trunk Application (UTA) is an implementation of the VNM&S Application that is integrated with the Cisco ISR G2 family or the ASR family via the Cisco UC Gateway Services API available in recent versions of the router iOS. UTA can be deployed on a variety of hardware platforms: an SRE module installed in the ISR and running SRE-V, on an ETM 5000 Series UTA appliance, or on customer-supplied COTS hardware that meets minimum system and resource requirements, such as a Cisco UCS. When deployed on a 5000-series UTA appliance or COTS hardware, UTA supports virtualization of either a single instance with call capacity stated for the selected 5000-Series Appliance, or of up to 15 instances on appropriately sized hardware (up to 50 calls per instance in this model). See the SecureLogix® 5000-Series UTA Appliance Technical Specifications for call capacities.

Figure 21 provides a high-level overview of a sample ETM System UTA deployment.
The integration of ETM UTA with the Cisco router decouples the ETM Application from network and signaling specifics for both VoIP (Voice over Internet Protocol) and TDM (Time Division Multiplexing) traffic, providing full ETM System functionality without the need to be inline. Policy decision processing is performed by the ETM System, and Cisco routers, gateways, and software ensure network connectivity and integrity across various telephony protocols.

UTA is not inline with either signaling or media. Signaling and call information is exchanged through Web Services calls with the iOS API, and the API forks a copy of the media and sends it over a socket connection to the UTA Media Proxy (MP). The API also provides call state, call control functionality, and trunk status to UTA. See the section on UTA reliability on page 35 for additional details about this message flow.

When UTA is installed on an SRE module, Cisco SRE-V is used as the hosting environment to embed ETM UTA into the routers. The Cisco SRE-V hosting environment provides the infrastructure to securely host, install, upgrade, and manage the application. This integrated solution complements the existing ETM hardware instrumentation strategy by extending the ETM Appliance further out into the network to provide cost-effective management and security. This enhanced visibility further strengthens the Cisco Borderless Networks initiative that enables organizations and individuals to communicate anytime, anywhere, in any way they wish.
**ETM® Appliance Application Reliability**

All ETM Appliances and appliance software are designed to be highly reliable to ensure voice network security and monitoring is continually available and that voice network operation is not impacted. Details for each appliance application are provided below.

**TDM Appliances**

The ETM® TDM Appliances are installed inline between the CO and the PBX. Because of this deployment, it is essential for the Appliances to be reliable to avoid impacting voice trunk operation, and to perform necessary security and monitoring functions. To this end, reliability is the primary requirement driving the Appliance design. The use of custom hardware allows an inline but fail-safe architecture, and maintains the 99.999% reliability of voice networks. The hardware is highly reliable; the cooling fans are the only moving parts.

All ETM Communications Appliances are designed to be very reliable and fault tolerant. All Appliances and Card sets operate autonomously from one another. For a site with multiple Appliances and/or Card sets, there is no single point of failure—in the unlikely event that an Appliance or Card set fails, it will not impact other Appliances or Card sets. The only dependency between Appliances or Card sets is for NFAS on PRI or SS7, in
which the signaling from one Appliance or Card is sent to one or more other Appliances or Card sets. This dependency is normally mitigated by use of backup PRI D channels or SS7 signaling links.

The software that runs on the ETM Series 1012/1024/1090 Appliances and the 2100/3200 Appliance Card sets is structured so that there are multiple instances of processes for each active Span. In the unlikely event of a software issue, it only impacts processing for one Span. If a process fails, the Card software restarts it. If the issue is severe, the Card generates a “panic,” which causes the event to be recorded, and the Span is taken out of line and rebooted.

ETM Communications Appliances include three monitoring capabilities to ensure that failures do not impact trunk availability:

1. If the device driver is processing input signaling information (PRI D-channel packets or T1 CAS A-B bits), but detects that the signaling is not being transmitted, this indicates an issue with the Span-level application software. In this case, the Card generates a system panic, which causes the Card to record the event, take the Span out of line, and reboot it.

2. Each of the main components of the ETM Card software maintains an interface to a software monitor watchdog. If a component experiences a logic or hardware error that results in an “endless loop,” the software watchdog detects the unresponsive component, logs the error, and reboots the Card.

3. All ETM Platform Appliances have a hardware watchdog that detects whether a hardware issue has “hung” the Card or a Span. In this case, the Card generates a system panic, causing the Card to record the event, take the affected component out of line, and reboot.

As described, this reboot process is transparent to the active calls. This is always verified when the Appliance is installed at a customer site.

**Inline SIP Application**

Because the SIP Application is logically inline with the SIP trunk, it has been designed to be deployed in a highly available manner to prevent loss of voice service and to ensure it continues to perform the necessary security and monitoring functions. To that end, the Signaling and Media Proxies are deployed in a redundant fashion on two or more Appliance platforms running high-availability software that provides failure detection and failover to a hot backup.

The redundant Signaling Proxies share one or more public addresses that external devices such as SIP Trunk endpoints address. The current processing (active) Signaling Proxy is configured to use these public addresses, but if a service or network connection fails, one of the redundant Signaling Proxies assumes the public
address(es) and immediately performs the Signaling Proxy function as messages arrive. Failure of a service or network connection on the processing (active) Signaling Proxy is detected within 5 seconds. Additionally, failover can be manually initiated to accommodate potentially service-disrupting activities such as maintenance or software updates. In this case, the failover to the backup proxy is immediate.

After a loss of network connectivity, restart, or reboot and the subsequent switchover of activity, the former processing (active) Signaling Proxy reconnects with the other redundant Signaling Proxies and performs any necessary synchronization to become an available node within the high availability cluster.

Like the Signaling Proxy, the Media Proxy can be highly available to ensure continued operation of the SIP Trunk. If the Media Proxy were to completely fail, any calls established through the Media Proxy would lose all media capability. If a service or network connection fails on the processing (active) Media Proxy, a redundant Media Proxy assumes the Media Proxy function. The processing Media Proxy shares connection state information with the redundant Media Proxies to allow them to immediately begin processing media packets for existing calls in case of a switch of activity. As with the Signaling Proxy, failover can be manually initiated to accommodate potentially service-disrupting activities such as maintenance or software updates.

After a loss of connectivity, restart, or reboot, a Media Proxy reconnects with the other cluster members and synchronizes its connection state information to facilitate subsequent activity switchovers.

In addition to redundancy and failover mechanisms, the SIP product was designed with reliability in mind. Software is as simple as possible with complex or nonessential tasks removed or located in other parts of the system. The software is also structured to continue working in spite of errors or configuration changes, minimizing the need for restarts.

**UTA**

Since UTA is not inline, it cannot affect call traffic if it becomes unavailable. However, it is designed to be highly reliable to ensure it continuously provides call monitoring and executes security and usage Policy.

The UTA appliance interfaces directly with Cisco router using the Cisco Unified Communication IOS Services API. The UTA appliance makes use of the Extended Call Control (XCC) and the Extended Serviceability (XSVC) interfaces. XSVC provides UTA with the telephony topology for the router; this includes the current trunk and route configuration. XSVC also provided real-time link status and configuration change notifications. XCC provided call control and real-time call monitoring. As a call is processed, the router makes two requests to UTA to determine if the call should continue. The first request is made when the call is first detected, but it may not contain the source phone number. UTA always instructs the router to continue to allow the call to progress for this first request. Once the router has both the source and the destination numbers, it makes
another request to UTA to determine if the call should progress. UTA processes the numbers against the 
installed Policy based on this request. Based on the Policy results, UTA may instruct the router to allow the call 
to continue or to end the call. If the action is to allow, then UTA can also record the call. Based on user action, 
UTA can send a mid-call terminate request to the router.

Signaling and Phone Number/URI Access

Signaling and phone number/URI access differs, depending on the ETM Application deployed. Details for each 
implementation are provided below.

UTA

UTA uses an interface to the API embedded in the iOS on the router to request normalized call signaling 
information. The integration of ETM UTA with the Cisco ISR/ASR decouples the ETM Application from network 
and signaling specifics for both VoIP and TDM (ISR only; ASR supports only SIP) traffic, providing full ETM 
System functionality without the need to be inline. Policy decision processing is performed by the ETM 
System, and Cisco routers, gateways, and software ensure network connectivity and integrity across various 
telephony protocols.

UTA is not inline with either signaling or media. Signaling and call information is exchanged through Web 
Services calls with the iOS API, and the API forks a copy of the media and sends it over a socket connection to 
the UTA Media Proxy (MP). The API also provides call state, call control functionality, and trunk status to UTA.

TDM and SIP

Spans in the ETM TDM and SIP Appliances access circuit signaling, whether SIP packets, analog or digital, in- 
band or out of band, to monitor call progress information. For example, digits are extracted from in-band data 
(DTMF or MF), out-of-band data (dial pulse A-B bits), D-channel messages, or SS7 ISDN User Part (ISUP).

On SIP trunks, destination digits are obtained from the To Header in the Invite message.

On TDM trunks, the destination digits are typically available on the line for both inbound and outbound calls. 
For analog lines with fixed telephone numbers, the outbound extension for the line can be set (since it may 
not appear on the line). Source numbers are extracted, if available as Caller ID, Automatic Number 
Identification (ANI), or Calling Party Number (CPN). For circuit types where this information is not made 
available on the line, the ETM System can obtain it through Station Message Detail Recording (SMDR) data 
generated by the PBX. Both serial and IP SMDR are supported. For outbound calls, the SMDR data can be used 
for Policy processing and stored in the database for reporting. For incoming calls, SMDR can be used to
identify protected internal extensions for call recording, but inbound SMDR is not used in Policy processing nor stored in the database. For more information about SMDR/CDR in the ETM System, see “SMDR/CDR” on page 44.

For outgoing calls on most TDM circuit types, the destination digits are collected until ringback from the CO is detected. On analog and T1 loop start and ground start calls, which do not provide answer supervision, a configurable Call Established Timeout setting is used.

The Spans use a "dialing plan" to normalize all numbers seen on the line, including E.164 numbers extracted from SIP signaling. The dialing plan understands the construction of normal, long distance, international, and special phone numbers, and converts the various types of Direct Inward Dial (DID), 7-digit, 10-digit, international, etc., numbers into fully normalized numbers that can be used in the Policy and saved in log files. Special numbers that should not be normalized include emergency numbers, information numbers, and so on. Dialing plan files for specific regions and/or trunk types (such as the DoD’s Defense Switched Network) are shipped with the product. These files exist as INI files located on the ETM Server and are customized for each customer site. The ETM Client is used to download the dialing plan files to the Spans.

Call Type Determination

Call type determination and policy processing based on call type are important functions of the ETM System.

For SIP calls, the call type is determined based on the codec used for the media/audio stream. The SIP Appliance determines call type by assigning a call type value to each codec, finding all of the codecs used in a call (and their associated call types), and then using a priority order to determine the call type applied to the overall call. For instance, a call using both a Voice and a Video codec would have an overall call type of Video (because the ETM System deems the Video portion more important and Voice is generally assumed to be part of a Video call).

UTA receives the call type derived by the API on the router.

Once a TDM or analog call is connected, the Span determines the call type by continuously monitoring the audio Pulse Code Modulation (PCM) values. The Span determines call type by monitoring the frequency and energy content of the audio data and looking for discrete tones, flag events, or sequences. The Span detects various tones/events such as ANS, CNG, 1800 Hz, V.8, STU-III, and Fax T.30 signaling flags. Finally, the Span uses the audio data classification and sequence of detected tones and flags to derive the actual call type. The call-type determination classifies the call as busy, unanswered, undetermined, voice, fax, modem, modem energy, data call, or STU-III. The busy call type is reported when a busy tone is detected. The unanswered call type is reported if the call is not answered. The undetermined call type is reported if a call connects, but is
terminated before the type can be determined. On PRI circuits, video calls are also detected by monitoring the setup messages in the D channel.

The specifics of the classification algorithms are both proprietary and not disclosed for security concerns.

**Policy Execution**

The Spans in the ETM Appliance Applications provide Policy-processing engines used by the Voice Firewall and Voice IPS to control calls.

**Firewall Policy Execution**

Voice Firewall Policy processing is performed in three phases:

- At the start of the call, *call-reject* processing is performed to determine whether the call should be allowed to proceed, strictly based on the direction, destination, and/or source, without waiting for call type to be identified. Reject rules allow rapid termination of known unauthorized calls, such as unauthorized toll calls, calls to protected sensitive numbers, or calls from known suspect callers, such as those on the SecureLogix proprietary National Harassing Callers List.

- When the call type is initially determined and each time the call type changes, the call is again processed against the Policy. For example, international faxes are often operator assisted, so Policy processing is performed at the start of the call to verify calls to the destination country are allowed. Policy processing is performed a second time with a call type of voice once the human operators begin talking. Policy processing is performed a third time once the fax transmission starts (and a fax call type is determined).

- If a Rule specifies duration, but the duration has not yet been reached, the Policy is reprocessed every 15 seconds until the call ends or the duration is reached and the Rule fires. If multiple duration Rules are arranged in descending duration order, processing continues until each duration has been reached or the call ends.

Policy processing compares the specific attributes of a call against the set of Rules. The call is compared to the Rules, one-by-one, starting at the top of the Rule set and working downward. If no matches are found, the default Rule (which allows all calls) is executed. Multiple Rules can fire for the same call if the call type changes or a duration rule is subsequently matched. However, the same Rule will never fire more than once for the same call. A single call can generate multiple alerts, emails, syslog alerts, and SNMP traps. A single call record is saved in the database, including each distinct call type and Rule fired values. As described, many calls will have multiple call types and some will fire multiple Rules.
If the call matches the criteria in the rule, the Span executes the specified action, which is to either allow or terminate the call. Specified tracking events also occur. Tracks may include any or all of the following: log the information for the Rule that fired, generate a real-time screen alert, send an email, send an SNMP trap, and/or send a syslog alert. The Appliance Application executes the Policy and allows, terminates, or redirects the call, but the ETM Server generates the Track events.

**IPS Policy Execution**

IPS Policies are processed as follows: When you install a Voice IPS Policy on a Span Group, a copy of the Policy is also installed on the IPS polling engine running on the ETM Server. This detection engine evaluates the Thresholds and maintains the accumulations on the Server. When a Threshold is met, the Rule is considered “breached.” When the Server identifies a Rule as breached, it instructs the Span to begin any specified terminations, and the Server generates any specified Track actions. By default, the polling engine executes to evaluate the Thresholds every 5 minutes. Depending on the number of Thresholds being monitored, you can change this frequency to a higher value to decrease processing load on the ETM Server computer. Or in the case of a suspected attack, you can lower the frequency for faster mitigation.

Accumulations are maintained for each Rule of each installed IPS Policy. When a call matches all of the other criteria of a Rule, the values for the call are included in the accumulated values for the Rule. A single call can count against multiple Rules if it matches the criteria; Voice IPS Policy Rules have no processing order. These accumulations are compared to the Thresholds every time the polling engine executes; if a Threshold is exceeded, a breach is recorded and specified tracks and actions are executed. The following actions are available for IPS Rules: *allow* the call that breached the Rule, *allow the calls that breached the Rule but prevent future calls* that match the Rule, or *terminate ongoing matching calls and prevent future calls* that match the Rule. As with Firewall Rules, available Tracks include logging the event, email alert, onscreen alert, syslog alert, and SNMP traps.

**How Spans Monitor Calls**

UTA receives a forked copy of the signaling and media from the router, which waits for a configurable amount of time (by default, 10 seconds) for a Policy-based reply from UTA on how the call should be routed: as dialed, redirected to a different destination, or terminated. The router then routes the call as directed by UTA.

Other Span types monitor both out-of-band and in-band call progress events to determine when the call is being established and subsequently when to start “reject phase” policy processing. For some signaling types, the Span cannot terminate calls that have not yet been answered. For these calls, the Span must wait until the call has been answered before it can terminate the call. This applies to incoming loop start and ground start
calls on either analog or T1 trunks. However, these trunks are typically not used in business environments due to their long call setup times.

A TDM Span does not “hold” the signaling or bearer traffic as the call state is being determined. This would prevent calls from occurring properly. Rather, the Span allows the calls to go through, and if necessary, terminates the call as soon as the necessary state is received. As an example, for a rule terminating unauthorized modems, the Span must wait for call-type determination of modem or modem energy before the call matches the Rule. If it is a modem or modem energy call, it is terminated within 1 second of the call type determination.

As in the case of TDM, the SIP Span does not “hold” the bearer traffic. The bearer traffic (audio data) is very sensitive to delay, so the SIP Span receives and retransmits the bearer traffic at a very low level to minimize any delays. Call signaling is less time-delay sensitive than the bearer traffic. The SIP Span performs call-reject Policy processing before forwarding the invite on.

**Caller ID Authentication (CIDA)**

The ETM System supports Caller ID Authentication through integration with TRUSTID’s solution. This licensed feature is particularly valuable in call center environments, and provides four key benefits:

- Decreases call center fraud rates.
- Increases IVR containment rates.
- Speeds the time required to authenticate callers who do reach agents.
- Provides an improved customer experience over other technologies for call authentication.

The ETM Caller ID Authentication (CIDA) feature is used in conjunction with the TRUSTID Authenticator™.

TRUSTID Authenticator is an undetectable, network-based caller authentication service provided primarily to call centers. Before an incoming call is answered, TRUSTID Authenticator determines the authenticity of a calling party’s ANI or Caller ID using proprietary and patent-pending real-time telephone network forensics.

To use TRUSTID Authenticator, inbound call information must be captured and sent to the TRUSTID Authenticator web service before answer supervision signaling is sent to the calling device. When the TRUSTID Authenticator completes its forensics, it returns the results to the system that provided the capture and the inbound call routing is then completed. The ETM System integrates with the TRUSTID Authenticator to provide this call data capture and call control.
For specified lines, the ETM Application delays answer supervision of a call and sends the TRUSTID Authenticator the called number, calling number, and ANI information for authentication. The TRUSTID response ("Credentialed" or "Not Credentialed") is returned to the ETM Server which then passes the response to the ETM Appliance to complete the call setup. Call center operators can use this response to determine appropriate handling of the call.

CIDA authentication request results can be viewed in the Call Monitor and are stored in the ETM Database for offline reporting. They are not available via the Usage Manager.

**Local ETM® Appliance Application Storage**

On all ETM Communications Appliances except SIP and UTA, the Card(s) in the Appliance have a Compact Flash device to store the Appliance software, security policy, or call log events/authentication database. The SIP and UTA Appliances have some number of hard drives for this purpose. The SRE-V and ASR implementations also provide local storage, while virtual UTA deployments provide virtual drive storage. This allows the Span to execute the current Policy even if it cannot communicate with the ETM Server. If communication with the Server is temporarily interrupted, Appliance Cards can store up to a week of call and security policy event information, depending on call load. Other implementations can store as much data as drive space is available for. This information is sent to the Server when communication is reestablished; Policy continues to be executed, although events are not logged on the Server until communication is reestablished. Specified Tracking events, such as email notifications, are generated when communication with the Server is reestablished.

**ETM® Appliance Access**

After initial configuration, once the Appliance Application has connected to the ETM Server, the Server is authoritative on the configuration. Therefore, most Appliance Application access is performed from the Server via the ETM Client. However, the ETM Appliance also provides a command-line interface (CLI) for initial configuration and for viewing/changing network parameters if the Server connection is temporarily unavailable.

On all Appliances except the SIP and UTA Appliances, a serial port on the Appliance/Card can be used to access the CLI, and must be used for the initial Appliance configuration. In addition to the serial interface, Telnet is available on TDM appliances if it is enabled, while SSH is available on SIP and UTA Appliances if it is enabled. The Performance Manager Client also provides encrypted/tunneled access to the Appliance CLI when the Appliance is communicating with the Server, and provides the GUIs used to set permanent Appliance settings,
monitor activity, upgrade Appliance software, and all other Appliance management tasks. See “ETM® System Security” on page 49 for detailed information about client/server/MNM&S Application Security.

ETM® Server Technical Discussion

The ETM Server consists of several non-interactive applications that continually execute to provide management of one-to-many ETM Appliance Applications, and to provide a connection point for one or more local/remote ETM Clients. The Server manages the Appliances by downloading policies, configuration, and software. The Server communicates with a Client GUI to allow configuration and management of the Server and Appliances, and for building and installing Policies. The Server sends data to the Client GUI for review, including logs, alerts, and report data. The Server also generates external events, including emails, syslog events, and SNMP traps. Figure 22 illustrates this data flow.

The ETM Server consists of several processes that perform separate functions. These processes are separate to allow distributed processing and increased scalability. The ETM Server comprises the following processes:

- **Management Server**—The Management Server is the primary component of the ETM Server and provides the central hub for communication between the Appliances, the ETM Clients, and the ETM Database.
• **Report Server**—The Report Server is used to access the ETM Database and produce data for reports. This data is in turn transferred to the ETM Client, where it can be viewed and printed. The Report Server can run on the same system as the Management Server or can run on a separate physical server.

• **Oracle RDBMS Server**—The ETM Management Server uses an Oracle RDBMS v10G or later for the ETM Database to store the majority of the data. Depending upon the size and complexity of the installation, the ETM Management Server can reside on the same system or communicate over the network with the Oracle RDBMS. The ETM Database can also co-reside on an existing corporate Oracle RDBMS.

The ETM Management and Report Server are developed entirely in Java, and currently run on 32 or 64-bit Windows Server 2003 or later server-class 32 or 64 bit versions and on 64-bit Red Hat or CentOS Linux. When using a Windows OS variant, all Server processes run as services and can be managed via the Windows Services Control Panel.


**ETM® Appliance and VNM&S Application Configuration Management**

The ETM Server manages one to many ETM VNM&S Applications/Cards/Spans. Appliance Application configuration GUIs in the ETM Client provide the means to manage settings, either individually or for multiple Applications at the same time. After initial configuration, the ETM Server is the authoritative source for most configuration settings for the Applications. When an Application is first configured and identified to the Server, the Server accepts the initial configuration information from the Application. After this point, the Server is authoritative on most settings and pushes its copy of configuration to the Application any time the Application connects to the Server.

The ETM Server can download new software to the VNM&S Application. The Server maintains copies of the VNM&S Application software, which can be pushed to all connected VNM&S Applications. New software includes updates, upgrades, and entirely new applications, and for SecureLogix Appliances, firmware upgrades.

**ETM® Database**

The ETM Server stores all data except startup configuration files and critical error logs in an Oracle relational database. The ETM Database is installed and configured separately from the Management Server. SecureLogix provides scripts and detailed instructions for creating an Oracle instance for use by the Management Server. Once the instance has been created, you use a utility provided with the ETM System, the ETM Database
Maintenance Tool, to create all necessary tables, along with additional configuration necessary for the Database to perform optimally with the ETM System. Once this is complete, the Server and ETM Database are tightly coupled and ready for operation. The ETM Database Maintenance Tool also provides functions for conversion of old data, fixing corrupt tables, and viewing the table structure. Additionally, the Database Maintenance Tool allows for the configuration and scheduling of several important day-to-day maintenance actions on the ETM Database, including:

- Automatic partitioning (Oracle Enterprise Edition)
- Maintenance of indexes
- Maintenance of table statistics necessary for optimal performance

Detailed administration of the RDBMS can be performed as necessary with the appropriate tools provided with Oracle. SecureLogix has configured the ETM Server to use features in Oracle such as partitioning and index-organized tables to minimize space requirements while supporting data storage and retrieval. Data storage is only limited by physical requirements. The Server uses a number of proprietary features of the Oracle RDBMS to optimize its performance.

If the ETM Server cannot access the ETM Database, it enters “standby” mode until the database is available. In this case, the Server closes the connections to the database, active ETM Client sessions, and all ETM Spans. Users who are logged in through the ETM Client are notified. The Spans continue to execute policy and store events locally until the Server reestablishes the connection to the ETM Database. The Server automatically attempts to reestablish this connection. When successful, the Spans reconnect and users are able to log back in.

**SMDR/CDR**

Outbound SMDR/CDR can be used to obtain data not available on the line to inline ETM applications. This most commonly includes source numbers for outbound calls, but may also include site-specific data such as authorization codes and internal extensions for which calls are not to be recorded. An Auxiliary port that can read the PBX SMDR serial data stream is present on all TDM Appliance Cards. Alternatively, the Appliance applications can receive SMDR via a TCP/IP feed if one is available. The Card or SIP application encrypts and routes the SMDR data to the ETM Server. The Server accepts SMDR from multiple Cards/applications, one per Switch. This data is cached and correlated to calls seen the by the Spans. Specific information is extracted from the SMDR, including source numbers for outbound calls and long distance authorization codes. This phone
number data is sent to the Spans for Policy execution and all of the data can be used to augment the call logs in the database.

Additionally, the application can import CDR data files from Cisco Call Manager or other PBXs to provide for station-side CDR reporting. *(Not used in Policy processing).*

Inbound SMDR can be used to identify specific protected internal extensions to which calls are never to be recorded. Inbound SMDR is not used in Policy processing nor stored in the database.

The Server uses PBX-specific configuration files to define how to parse SMDR data. In order to properly process SMDR, the ETM Server requires the appropriate configuration file. SecureLogix provides SMDR files for major PBXs. For PBXs that are not supported by an existing configuration file, SecureLogix can obtain a sample of the SMDR data and generate a configuration file.

**Tracking Events**

The ETM Server accepts events from the ETM VNM&S Applications and generates Tracking events. The Server generates real-time screen alerts, emails, syslog alerts, and SNMP traps as soon as it receives the Rule trigger message. This means that the event may not include some information, such as the end time, duration, and for certain calls and in some cases, the source number. The Server logs the event when the call is complete, which is when all information is available. An optional Track Refire setting is available to resend the Track once all information is available.

A Version 2 MIB is provided that defines the SNMP traps generated by the ETM Server.

**Data Network Traffic**

**Data Network Traffic Between the ETM® Server and Appliance Applications**

The network load between the ETM Appliance Applications and ETM Server depends on the call traffic. Several major types of messages are exchanged between the Appliance Applications and the Server:

- **Call messages**—All calls seen by the Appliances are reported to the Server. Multiple messages are sent for each call, including call start (off-hook), call connected, call type change, call end, and optionally, mid-call DTMF digits and several SMDR messages. The total number of bytes sent for a normal call is 600. Details for each application type are provided below.

- **SIP or UTA Span-to-Server network load**—The SIP and UTA Span-to-Server network load can be calculated using the following simple equation:
NumberofCalls * 600 / AverageCallLengthInSeconds

TDM Span to Server network load—The TDM Span-to-Server network load can be calculated using the following, slightly more complicated, equation:

\[(\text{NumberOfChannels} \times \text{PercentUtilized}) \times (\text{NumberOfBytesPerCall} + \text{SMDRBytesPerCall}) / \text{AverageCallLengthInSeconds}\]

The TDM Span-to-Server network load calculation is more complicated than the SIP calculation due to the variable number and utilization of channels, and the potential usage of SMDR.

- **NumberOfChannels**—The number of channels from a Span that is collecting information. T1 Spans carry 24; E1 Spans carry 30; Analog Spans carry 12.

- **PercentUtilized**—The average load on the telecommunications trunk. Industry norms are to operate a trunk at 90% utilization during peak times, and drop below 10% during off hours.

- **NumberOfBytesPerCall**—The average size, in bytes, of the sum of messages created by a call. 600 bytes is the average total of all messages generated by a call.

- **SMDRBytesPerCall**—The average size, in bytes, of the sum of SMDR messages created by a call, assuming SMDR is active for both inbound and outbound calls. 300 bytes is the average total of all SMDR messages for a call.

- **AverageCallLengthInSeconds**—The average length of all calls in seconds. This number affects the total load on the network most dramatically. Since the majority of messages per call are generated at the beginning and end of a call, the longer the average call length, the lower the load on the network, because fewer call start and end events are occurring.

In a scenario of 100 DS1 TDM Spans, the peak network load would be calculated as follows:

- \((2400 \times .90) \times (600 + 300) / 60 = 32,400\) bytes per second
- **NumberOfChannels**= 2400 (100 * 24 channels each -- assuming all DS1)
- **PercentUtilized**= 90%
- **NumberOfBytesPerCall**= 600
- **SMDRBytesPerCall**= 300
- **AverageCallLengthInSeconds** = 60
This load represents about 0.25% (less than 1%) of a 100 MB Ethernet network. This load is a worst case, assuming SMDR, high utilization, and many short calls. Actual utilization during peak times, and especially during off hours, will be lower. This load only includes the payload information. Overhead for Layer 2-4 packets is not included.

- **SMDR**—If the system is using line-side SMDR, the Card connected to the PBX SMDR serial port sends a call record for each call of interest (normally only outbound calls) to the Server. The number of bytes for each call varies by PBX, but typically is between 200 to 400 bytes. While SMDR is not required, it can sometimes provide information not available to the Card/Span on the trunk.

- **Health and Status**—By default, every 60 seconds, the Card/Span sends a “heartbeat” and other information to the Server to indicate the Card/Span and telecom trunk state. You can specify a heartbeat interval other than the default; the heartbeat message is approximately 50 bytes long.

**Other Types of Data Network Traffic**

In addition to the call traffic between the Appliances and Server, periodic traffic occurs when configuration, policy, and software is downloaded to the Appliances. This type of traffic is uncommon and typically under the control of users.

Appliance-to-Appliance traffic exists only with PRI (when NFAS is used) and SS7 signaling. In this case, the Appliances monitoring signaling sends information to the Appliances monitoring the bearer Spans. The traffic level is small, even with busy trunks. A 40-byte message is sent from the signaling Appliance to the bearer Span at the start of the call, and another 40-byte message is sent at the conclusion of the call.

If the ETM Server and Oracle RDBMS are executing on separate computers, a significant amount of traffic is generated between the systems. The Server inserts call record data into the Oracle database and the load depends heavily on call volume. The Server also extracts data from the Oracle database for presentation to the user and reports. This connection is normally on a high speed internal LAN so bandwidth usage is not an issue.

The ETM Server and ETM Client only communicate if the client is executing. When the client is executing, network load depends primarily upon which tools are displayed. The only client tools that add significant load to the network include

- **Call Monitor**—This tool displays the status of active calls. It essentially duplicates the traffic sent from the Appliances to the Server for the Spans being monitored, but in a slightly less compact form.
• **Policy Log**—This tool can be used to view logged events in real-time. If many events are being logged, the network traffic from the Appliances to Server is duplicated (extreme case is when all calls are logged pursuant to the security policy, which is not recommended).

• **Alert Tool**—This tool is used to display real-time alerts. If many events trigger alerts, the network traffic is high.

• **Reports**—Generation of a large, detailed ad-hoc report involves sending significant amounts of data from the Report Server to the ETM Client.

• **Web Portal**—When you download calls from the Web Portal, secure HTTP traffic is generated based on the size of the call data requested.

**Report Server Implementation**

The Report Server provides access to the log data in the database for generating reports. The Report Server is a separate process that can be executed on the same or a separate system from the ETM Server. The Report Server accepts requests from the Usage Manager Client, communicates with the ETM Database, and sends the appropriate filtered and formatted report to the ETM Client. The Report Server supports multiple simultaneous Usage Manager client connections.

A simple additional process called the Report Server Activator is used to start the Report Server on demand. The Report Server only runs when it is creating a Report. When a Report is complete, the Report Server idles, which allows the system to free any resources consumed when running large Reports.

**ETM® Client Technical Discussion**

Several ETM Client applications are provided with the ETM System. The primary ETM Client is the ETM System Console, which is the "launch pad" you use to access and administer all features of the ETM System. This client provides a GUI that allows you to log into the ETM Server to access all of the ETM System applications. The client is developed entirely in Java and runs on Windows Vista or later 32 or 64 bit versions, and 64-bit Red Hat or CentOS Linux.

A web-based client called the ETM Web Portal is provides web-based access to view and schedule reports, and to access call recordings saved by the Call Recorder. The Web Portal supports the Internet Explorer v5.0 or later web browser. The Web Portal web server components support Windows Vista or later 32 or 64 bit versions (not on Linux).
The Java client application is a separate process that can be run on the same system as the Server or can be run remotely on any system with network connectivity to the Server. The Web Portal can be accessed from any computer with the Internet Explorer browser and web access to the Web Portal server host.

The client applications do not directly access the ETM Database. All access to the database is through the ETM Server.

When a client is started, it initially is not connected to any Server. The client must first be configured with the IP address, port number, and DES key of the Server to enable connection. (For the Web Portal, this information is supplied to the web application, which controls access to the ETM Server.) The client then stores this information to allow subsequent connections. The Server maintains a list of authorized remote client IPs from which it accepts connections; all other connections are refused.

User accounts control login access. When a valid username and password pair are provided, the client connects to the Server and the user is given appropriate access to the system features, based on the user permissions for the account. The Server provides an “admin” user for client login that is initially used to create new users and assign the appropriate access rights. Multiple users can simultaneously log in via the client to a given Server. The Server and client provide granular locking mechanisms to prevent multiple users from changing the same object, policy, or file at the same time. There is no “hard limit” to the number of users who can log in from multiple, but there is a practical limit based upon the Server machine performance.

Communication between the Server and client can be encrypted with FIPS 140-2 certified Triple DES. See “ETM® System Security” below for detailed information about client/server/VNM&S Application Security.

ETM® System Security

The ETM System employ encryption to secure component communication as follows:

- **The ETM® VNM&S Applications** use a C-language Triple DES implementation
- **The ETM Management Server** that functions as the middle-man between the appliances, Client and Database uses a Java Triple DES implementation
- **The ETM System Console Client** that provides the only means to access the ETM Server uses the same Java Triple DES implementation as the ETM Server

In all three cases, the cryptographic module is used to secure data that is sent between ETM System components using TCP/IP network sockets. The encryption module in each component is not user-accessible.
In both the C language module and the Java module, the only user access to settings in the cryptographic module is via the Client GUI or authorized, password-controlled CLI mode for the following settings:

- Specification of the DES passphrase.
- Specification of which level of encryption to use after the initial ETM component handshake, which is always encrypted using Triple DES regardless of this setting (user settings include No DES, DES, 3DES).

Internally, the cryptographic module converts the DES passphrase to a DES key schedule and sets up the initialization and feedback vectors. The C language and Java implementations each contain initialization, encryption, and decryption routines.

The cryptographic modules only work in the following configuration and have only been certified in this configuration:

- Cipher Feedback Mode (CFB)
- 64 bits of feedback
- 64 bits of initialization vector
- 3 unique keys (3DES) - the ASCII string provided by the user is converted to 3 keys
- DES "weak key" checking is performed and logged - See Schneier's Applied Cryptography pg. 280

The ETM System Cryptographic Module is Federal Information Processing Standards (FIPS) certified and is listed on the FIPS/NIST web site. In addition, the ETM System's encryption implementation has been Common Criteria certified and independently tested, and has undergone testing and scrutiny by the U.S. Air Force Information Warfare Center.

Detailed documents were prepared regarding the ETM System’s use of encryption and the software sources were submitted for external review. The documents and software sources were reviewed during the Common Criteria evaluation and were reviewed by the US Department of Commerce Bureau of Export Administration (BXA). SecureLogix received permission for international export of the DES and 3DES ETM Systems. These documents contain many pages; what follows is a brief summary:

Encryption is only used to transmit data over network sockets once an authenticated connection has been established. An encrypted 3-message handshake is used to authenticate the ETM server and the ETM VNM&S Application connection. The sequence of events is as follows:
1. The ETM Server establishes a TCP/IP listener socket on a known, configured port. The VNM&S Applications always initiate the connection to the ETM Server on this port, because no listeners are implemented on the ETM VNM&S Applications to prevent any connection hijacking by rogue server applications. A port sweep of an ETM VNM&S Application will detect very few services. The ETM Server must be configured to accept connections from the ETM VNM&S Applications authorized to connect to it. It rejects connections from unauthorized applications.

2. After the ETM Server accepts the socket connection, the VNM&S Application converts the shared secret DES passphrase to a DES key schedule. The application then sets up the initialization vector and the cipher feedback vector. This is performed automatically and internally by the software via a function call to the initialization routine within the cryptographic module. The user simply configures the IP address of the ETM Server, the DES passphrase, and the DES level during initial installation of the VNM&S, Server, and Client.

3. The VNM&S Application then generates a Link Establishment message containing the eth0 MAC address of the host appliance and several other pertinent pieces of information about the application. The Link Establishment message also contains a random string which is dependent on time (the appliances contain a battery to ensure correct/advancing time) and the number of logged events. The VNM&S Application maintains a 64 bit unsigned number in non-volatile storage. This number is used to uniquely identify each message transferred to the ETM Server. The VNM&S Application uses time and this 64 bit number to generate a concatenated random string, to ensure this sequence is not vulnerable to playback attacks.

4. The Link Establishment message is encrypted with Triple DES and sent to the ETM Server.

5. The ETM Server must decipher the message with the same shared secret DES key used to encrypt the message. If the VNM&S Application and Server are out of sync on the DES passphrase, then the ETM Server cannot decipher the Link Establish request from the VNM&S Application and rejects the connection.

6. If the keys are in sync, the ETM Server deciphers and extracts the random string from the VNM&S Application. The ETM Server then generates its own internal random string and then encrypts using Triple DES and sends a Link Established Ack message to the VNM&S Application. This message contains the ETM Server-generated random string and the random string provided by the VNM&S Application.

7. The VNM&S Application does not process messages received on the TCP/IP socket until it receives a Link Establishment Ack message from the ETM Server. The VNM&S Application verifies that the ETM Server
deciphered the Link Established message, extracted the random string, and sent it back to the appliance. If the VNM&S Application does not receive its random string back, it disconnects from the ETM Server.

8. The ETM Server then waits for the VNM&S Application to decipher its Link Establishment Ack message. If the Application is unable to decipher the ETM Server’s random string and send it back in the Application Establishment message, then the ETM Server disconnects from the VNM&S Application.

**ETM® Client & Server Security**

Access to the ETM® Client is only allowed for authorized users and access is controlled by user accounts with granular permissions. User identification and a password (local ETM System credentials, CAC card, or LDAP authentication) are required to log into the system, and only authorized ETM Clients can connect to a given Management Server.

Since both the ETM Server and Client Applications run on general-purpose systems, SecureLogix follows and recommends accepted industry best practices for the configuration and set up of these systems. Obviously, these practices include keeping all system patches up to date and eliminating any services running on those systems that are not required to support ETM System operation. SecureLogix continuously monitors industry sources for information on security advisories and issues associated with supported systems and passes along this information to customers as they are identified.

**ETM® Voice-Network Monitoring & Security (VNM&S) Application Security**

Access to the ETM VNM&S Application is only allowed for authorized users. User identification and a password are required to log into the Applications. A separate “enable” password is required to make changes to configuration settings on the application from a direct console connection, which can be locked out completely. The Application can be placed into one of three security modes, “low”, “medium”, and “high”, which control the manner in which security settings can be changed (through Telnet/SSH, through the ETM Client GUI, or requiring change to these settings directly on the appliance through the console port interface).

The only TCP/IP service other than ICMP and ARP running on the Application is the Telnet or SSH server, which by default allows no access. Availability of the Telnet/SSH server can be enabled and disabled. Telnet/SSH connections are only accepted from authorized users from user-defined authorized client IP addresses. The only other forms of TCP/IP communication are through a configurable port used by the ETM Server. A single port is used to simplify operation through enterprise IP firewalls.

To access the ETM Server, the VNM&S Application must be configured with the server IP address, port and DES key. Initial communication with the Server always uses Triple DES encryption to validate the connection,
regardless of user-defined post-connection security settings. Subsequent communications are encrypted based upon security settings. Communication can proceed with no encryption, with DES, or with 3DES. The VNM&S Application always initiates the connection to the Server, and validates that connection with an encrypted message sequence, eliminating the possibility of a rogue “server” connecting to a VNM&S Application and thereby potentially impacting voice service or security.

Finally, the VNM&S Applications run a hardened version of the Linux operating system with most ancillary services completed removed to prevent their being inadvertently or maliciously enabled. The Linux kernel also runs the IP Tables firewall and is configured to ignore any port scans or other service requests that do not come from an authorized IP address.