# VOICE FIREWALL

Secure your voice network edge
and prevent financial losses.

SecureLogix®

The ETM® Voice Firewall secures your critical networking resources and lowers telecom expenses by protecting your enterprise voice network/UC edge from TDM and VoIP attacks, disruption, and service abuse.

**The Voice Firewall logs, monitors, and controls all inbound/outbound voice network activity** on a per-call basis through user-defined call access control (CAC) policies. These granular security and usage policies alert or prevent abusive or malicious use of your enterprise voice resources by internal or external callers.

**The Voice Firewall solves a host of real-world voice application security issues, enabling a large and immediate ROI** while providing an elegant, cost-effective, easy-to-manage path to full Unified Communications (UC) security. It prevents data network penetrations over modems, attacks on telephony systems and other key infrastructure, unauthorized Internet sessions on phone lines, data leakage, harassing/threatening calls, long distance abuse, calls to/from restricted parties, and other forms of phone line disruption, misuse and abuse. Companion SIP application security software will be available to augment the Voice Firewall's VoIP security capabilities and secure your migration to VoIP/UC by alerting and blocking VoIP/SIP-specific application threats such as flood DoS, fuzzed messages, directory scanning, and zero-day attacks.

**The ETM® System Voice Firewall supports and unifies TDM and VoIP security, and works across any network mix of IP-PBX switch vendors.** The system's Unified Communications Policy Management™ capabilities allow for the creation, remote distribution, and monitoring of consistent voice security and usage enforcement policies across a heterogeneous enterprise voice/UC network from a single administrative console. It truly unifies the security of voice/UC traffic and infrastructure across the entire enterprise. The Voice Firewall is a critical component of your regulatory information security compliance measures, providing application-layer security to real-time media that works side-by-side with your data firewall, helping complete the security of your corporate electronic perimeter for 360-degree protection and monitoring.

## Prevent malicious or unwanted voice traffic to dramatically boost your security, compliance, and cost reduction efforts.

### PROBLEM

### VOICE FIREWALL SOLUTION

### SECURITY BREACHES

Prevents network security breaches that result in network resource corruption, lost/stolen information, financial losses, and business operation disruption by alerting and/or blocking:

- Penetration attacks against the corporate data network via unauthorized inbound modem calls.
- Unauthorized outbound modem calls and private ISP dial-up connections that open security back doors into networking resources.
- Telecom system tampering, restricted long distance (LD) access, and voice mail/ IP-PBX attacks.
- Virus infections and restricted file transfers over dial-up connections.

### SERVICE ABUSE

Prevents misuse of corporate voice services that poses a security, safety , or legal threat including:

- Unauthorized employee dial-up Internet use and restricted web content over phone lines.
- Harassing, threatening, and caller ID (CLID) blocked calls.
- Inbound social engineering/identity theft calls from known perpetrators.
- Other restricted inbound and outbound calls.

### DATA LEAKAGE

Extends data leakage protection (DLP) to voice lines and communications, including data file transfers via modems and faxes of proprietary information.

### EXPENSES & FINANCIAL LOSSES

Reduces telecom expenses by detecting and blocking unauthorized or abusive use of corporate phone service and resources including:

- Unauthorized employee ISP dial-up connections and restricted Internet access.
- Data file transfers/faxes of restricted, proprietary information over phone lines.
- Internal voice service misuse/abuse.
- Non-business LD and international calling.
- Restricted toll calls to pay-per-call services (e.g., 1-900, 1-XXX-976).
- Directory assistance calls, connection fees, and out-of-service toll charges.
- LD and modem calls on fax lines.
- Long duration LD from common resource areas.
- Fax and VoIP spam.
- And much more.

### INVESTIGATIONS & LEGAL RISK

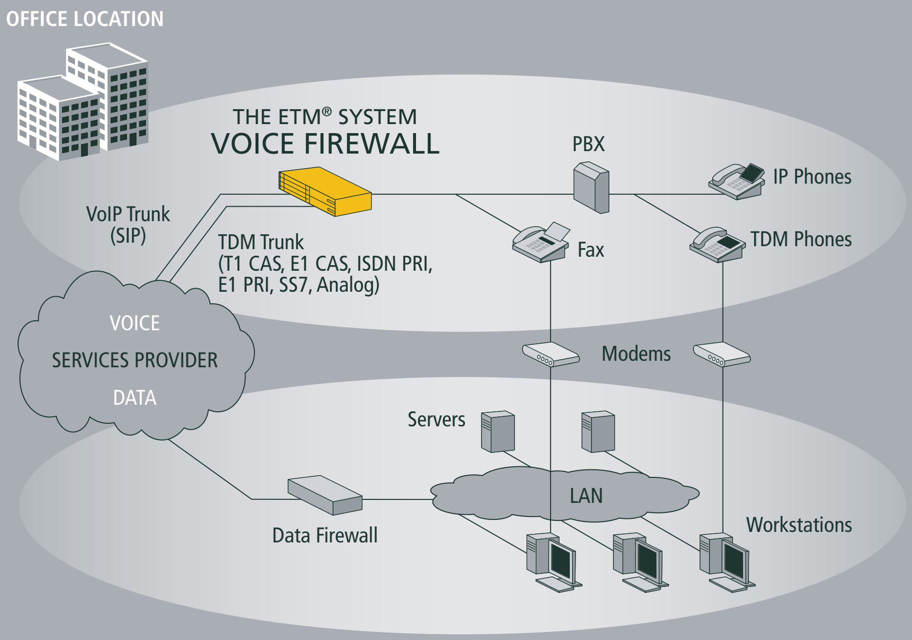
Decreases legal risk and liability exposure, and aids security investigations by tracking and alerting key calls of interest such as:

- 911 emergency calls, or other key calls of regulatory, legal, or business interest.
- Calls to/from employees or outside parties under investigation for fraudulent, threatening, or illegal conduct.
- Calls to/from restricted trade embargo-listed countries or other outside parties under suspicion for threatening activity.

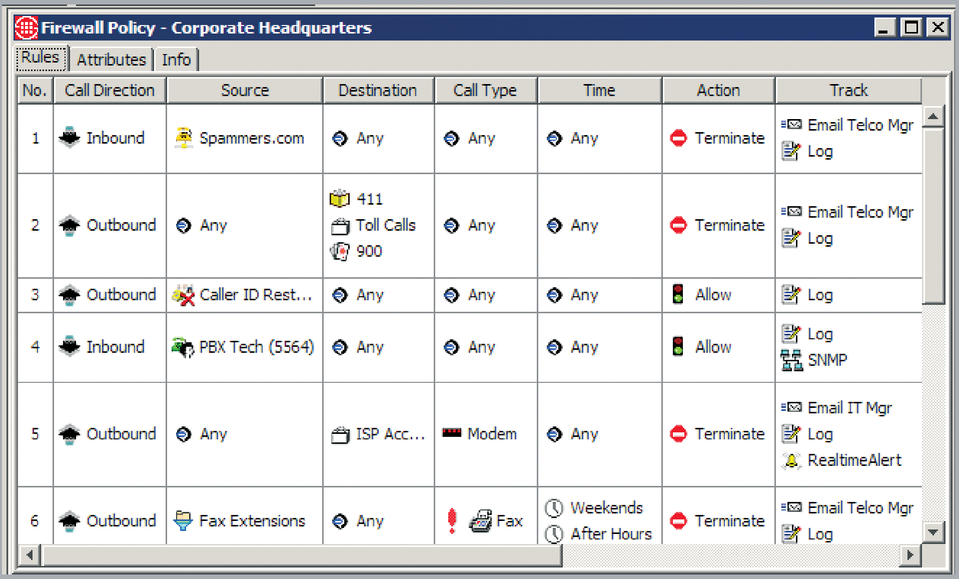
### COMPLIANCE

Adds security to voice lines to help complete the protection of your corporate network perimeter and strengthens regulatory security compliance.

## Secure your voice network edge for complete, 360° perimeter protection.



Most organizations have deployed traditional data network firewalls to guard against network-level IP threats to data networks. However, without a Voice Firewall, your enterprise is open to a host of real-time voice/UC security threats, including voice fraud and modem connection back doors into data networks through unsecured enterprise phone lines. Additional SIP security software will also protect against SIP specific application threats.



| No. | Call Direction | Source | Destination | Call Type | Time | Action | Track |
|---|---|---|---|---|---|---|---|
| 1 | Inbound | Spammers.com | Any | Any | Any | Terminate | Email Telco Mgr<br>Log |
| 2 | Outbound | Any | 411<br>Toll Calls<br>900 | Any | Any | Terminate | Email Telco Mgr<br>Log |
| 3 | Outbound | Caller ID Rest… | Any | Any | Any | Allow | Log |
| 4 | Inbound | PBX Tech (5564) | Any | Any | Any | Allow | Log<br>SNMP |
| 5 | Outbound | Any | ISP Acc… | Modem | Any | Terminate | Email IT Mgr<br>Log<br>RealtimeAlert |
| 6 | Outbound | Fax Extensions | Any | ! Fax | Weekends<br>After Hours | Terminate | Email Telco Mgr<br>Log |

SAMPLE VOICE FIREWALL POLICY

The firewall policy GUI is similar to those found in industry-standard IP-data firewalls. The above rule set automatically terminates threatening and abusive call activity such as restricted employee calls to ISPs over unauthorized modems (Rule 5), non-fax calls on dedicated fax lines during non-business hours (Rule 6), inbound VoIP spam (Rule 1), and toll calls such as 411 and 1-900. (Rule 2). The policy also sends real-time alerts via email to certain security and telecom management personnel when these types of abusive calls occur.

Deliver unified voice/UC network access and usage policies across your multi-vendor, mixed TDM and VoIP enterprise.

| FEATURE | FUNCTIONALITY |
|---|---|
| Enterprise-Wide Security & Usage Policy Enforcement | Secure and control your voice network by prescribing which inbound and outbound calls are allowed, terminated, and alerted with real-time, inline, usage monitoring/call blocking policy enforcement. |
| Continuous Call-Type/ Codec Monitoring | Restrict or monitor calls by call type or call type associated with a VoIP codec. Inline ETM Appliances continually monitor all signaling for call-type changes. Mid-transmission changes are logged and the call is re-evaluated against the active firewall policy. |
| Rule-Based Security Policy GUI | Construct security and usage policies of individual rules in an easy-to-use graphical user interface, similar to those in industry-standard IP firewalls. Specify different call criteria in each rule to cover all of your voice network restrictions. |
| Granular Policy Construction | Construct rules to alert and control call activity by specifying any combination of policy fields— call type; absence or blocking of caller ID, call source and destination numbers; call direction; time of call; call length; and certain VoIP call attributes, such as excessive media rate. |
| Centralized or Distributed Policy Administration | Administer enterprise-wide, departmental, or station-specific security and usage policies from one central management console or from multiple distributed consoles. |
| Policy-Based AAA Services | Secure access to authorized modems and other restricted services to authenticated users only. Authorized users of protected inbound or outbound systems authenticate to a distributed AAA Server Appliance running in IVR mode. |
| Real-Time Alerts and Call Termination | Configure policy rules to send a real-time security event alert via console message, email, and/or SNMP trap. Rules can also be configured to automatically terminate calls that match specified criteria—call type, time, source/destination, and more. |
| Wildcards, Phone Numbers & VoIP Addresses | Use wildcards to restrict inbound or outbound calls associated with a specific country, area code, city code, or VoIP domain. Use phone number groups, ranges, and filters to restrict PSTN or VoIP calls. |

SecureLogix®

SecureLogix Corporation

13750 San Pedro Ave.
Suite 820
San Antonio, TX 78232

1-800-817-4837
securelogix.com

Other ETM Applications

Usage Manager
Performance Manager
Voice IPS
Call Recorder