SAND REPORT

SAND2003-0285
Unlimited Release
Printed February 2003

Experiences from Evaluating Telephone Firewall Systems

Jack A. Hudson and Gerald F. Rudolfo

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94-AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2003-0285
Unlimited Release
Printed February 2003

Experiences from Evaluating Telephone Firewall Systems

Jack A. Hudson
System Security Research and Integration Department

Gerald F. Rudolfo
Telecommunications Operations Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0806

Abstract

Communication networks, both data and telephone, are subject to attack by malicious individuals. One goal of the owners of communication networks is to defend the networks from attackers. For several years, firewalls have been used on data networks to help provide protection from attackers. Until recently, there was no comparable system to use with a telephone network. Several vendors have recognized the need for systems to protect telephone networks and have developed products to improve the security for telephone networks. Sandia evaluated the capabilities of commercial telephone firewall products. Based on the evaluation of the telephone firewall products, Sandia installed the SecureLogix TeleWall system at both the New Mexico and California sites. Sandia is currently in the early stages of applying the capabilities of the SecureLogix telephone network firewall system to the environment at Sandia. Any site that has invested in computer network security protection through the implementation of firewall and intrusion detection systems should also implement appropriate telephone network protection through a telephone firewall system.

Acknowledgement

The authors thank and greatly appreciate the patience and thoroughness of John Abbott, Deborah Hansknecht, Larry Tolendino, and Frank Mason who read drafts of this report, identified and corrected numerous typographical errors, and made valuable suggestions that contributed to the clarity of the final version of this report.

Experiences from Evaluating Telephone Firewall Systems

Table of Contents

Figures

Experiences from Evaluating Telephone Firewall Systems

Introduction

The communications networks at Sandia National Laboratories are constantly under attack from outsiders. Sandia is targeted by the attackers due to the type of work performed by the Department of Energy laboratory and because of the notoriety that an attacker would achieve by successfully attacking any Sandia communication network. Sandia has put in place a number of defenses for the data networks to provide protection against attackers. Defending data networks has been a research topic for many years, and many companies have developed products to assist in defending data networks from attackers. Until recently, there were no products to assist in defending telephone networks. One vulnerability is a computer system with an auto-answer modem where the computer system is also connected to a corporate computer network. By attacking the modem and subverting the connected computer, an intruder could achieve a backdoor entry to the corporate LAN. Tools are available to test for modem vulnerabilities in a telephone network by automatically dialing against a telephone network. The automatic dialing systems identify only modems with auto-answer enabled and that are powered-on at the time of the test. Some of the automatic dialing systems even attempt to break into computer systems if connection with a modem is achieved. The automatic dialing only provides information about equipment connected to the telephone network and does not provide any real-time protection from attackers. To provide a capability for real-time protection of a telephone network, telephone firewall systems have been developed for telephone networks. With a telephone firewall a site can implement and enforce rules for allowed and disallowed telephone call traffic (e.g. no inbound modem calls are allowed). After a market survey and product evaluation Sandia installed a telephone firewall system at both the New Mexico and California sites.

Background

Sandia works very hard to protect and defend the corporate data networks through various defensive measures and equipment. Sandia developed a Detect, Delay, Respond approach and implemented Rapid Response teams to address attacks on the communication networks. Sandia collaborates with many organizations to share ideas about methodologies and approaches for defending the data networks. One collaboration partner is the Air Force Information Warfare Center (AFIWC) in San Antonio, Texas. The initial collaboration with AFIWC included discussions about their approaches and ongoing research activities directed towards protecting both data networks and telephone networks. Since Sandia had already implemented several approaches for protecting the computer networks, Sandia management decided to investigate telephone firewall equipment and to use the expertise of AFIWC in the area of telephone firewall technology. Telephone network firewall equipment only recently became commercially available; however, a number of organizations have deployed the equipment to improve telephone network security. Telephone firewall equipment provides an approach to perform an active defense of the telephone network as well as an opportunity to gain additional knowledge about the telephone traffic, in particular the use of modems, on the Sandia telephone network.

Telephone Firewall Involvement by Sandia

A few years ago, AFIWC decided to pursue the concept of a telephone intrusion detection system with Applied Signal Technology, Inc. (Sunnyvale, CA), a company with considerable experience in signal processing and signal reconnaissance. AFIWC established with Applied Signal Technology, Inc., a contract to develop a Telephone Intrusion Detection System (TIDS). AFIWC desired to have equipment that could provide real-time indications of attacks on their telephone network. By 2000, AFIWC was evaluating the equipment that Applied Signal Technology had developed and was working with Applied Signal Technology on modifications and improvements to the equipment.

In the early fall of 2000, Sandia personnel met with AFIWC in San Antonio to discuss computer and telephone network security topics. A follow on meeting with AFIWC personnel was held at Sandia in December 2000. As a part of this meeting, AFIWC invited a representative from SecureLogix (San Antonio, Texas) to attend. SecureLogix is a company that was formed to address telephone network security issues. The SecureLogix representative gave a technical presentation about telephone network security and the SecureLogix TeleWall telephone firewall product. AFIWC described their experience with the TIDS equipment that they examined in their laboratory. Following the meeting with AFIWC, Sandia began discussions with AFIWC and Applied Signal about evaluating one of the Air Force TIDS units and discussions with SecureLogix about evaluating a TeleWall system.

From researching commercially available systems for protecting telephone networks, there appeared to be (in early 2001) three vendors with potential solutions.   The vendors were Applied Signal Technology, SecureLogix, and Sentry Telecom Systems (Burnaby, B.C., Canada).

Telephone Firewall Vendors

Applied Signal Technology

Applied Signal Technology developed the Telephone Intrusion Detection System (TIDS) under contract from the Air Force. Applied Signal Technology referred to the system as the Model 2600 Modem Sentry. In April 2000, Applied Signal Technology created a wholly owned subsidiary, eNetSecure, Inc., with the objective to market the Model 2600 Modem Sentry under the product name, IceMon. eNetSecure sold one IceMon system to the NASA Ames Research Center (Mountain View, CA). In March 2001, Applied Signal Technology made a corporate decision to reintegrate eNetSecure into the parent company.

Sandia began initial discussions with eNetSecure in December 2000 about evaluating an IceMon system and met in Albuquerque with eNetSecure personnel in January 2001. After eNetSecure was reintegrated into Applied Signal, discussions about the IceMon continued with Applied Signal. Eventually an agreement was made with AFIWC and Applied Signal Technology to borrow a TIDS from AFIWC and to install the system at Sandia in June 2001. A contract was placed with Applied Signal Technology for technical support during the installation and evaluation of the system.

SecureLogix

Following the meeting with AFIWC in December 2000, Sandia initiated discussions with SecureLogix about evaluating a TeleWall system, and the conversations with SecureLogix continued during the late winter 2001-2002. In March, an agreement was negotiated with SecureLogix to install the TeleWall equipment at Sandia/NM in April 2001 for a formal evaluation period of three months.

Sentry Telecom Systems

Sentry Telecom Systems was contacted about their telephone firewall product, Phonewall. The Phonewall was developed originally by MPR Teltech Ltd., a member of the BC Telecom Group, a major telecom company in Canada. Sentry Telecom Systems was formed to attempt to commercialize the Phonewall product. Since the Phonewall product from Sentry Telecom Systems did not provide support for the PRI (Primary Rate Interface) spans used for the majority of the spans at Sandia, no product from Sentry Telecom Systems was evaluated.

Attributes/Characteristics of the Telephone Firewall Systems

General Attributes/Characteristics of TIDS and TeleWall

Each of the two telephone firewall systems evaluated, TIDS and TeleWall, monitor in real-time the telephone spans connected to a facility; however, the systems differ in several areas including specific capabilities and how each system is connected to the telephone network. Both systems do have several general characteristics in common.

Both of the systems connect to the spans between the central office (CO) telephone switch and the local telephone switch. The systems were designed to monitor telephone lines to provide a capability to increase the security for a telephone system. Both systems are designed not to disrupt telephone traffic in the event that a telephone firewall unit loses power.

Both of the telephone firewalls identify attributes of each inbound and outbound telephone call. These attributes include information a site typically retains already about each call (e.g. source telephone number, destination telephone number, date, time, direction of call, etc.). While a site normally obtains information about the telephone calls from the telephone switch, the telephone firewalls derive the same information by analyzing the signal channel for the telephone calls. Note that telephone traffic information obtained from the telephone switch should include information about both on switch and off switch telephone calls. The information obtained by the telephone firewalls only describes off switch telephone calls, since the firewalls are connected between the local switch and the central office.

Both telephone firewall systems also use digital signal processing technology to analyze the voice channel of the telephone calls. The types of telephone calls that the equipment detects include voice, modem, FAX, and STU. A digital signal analysis of the voice channel and algorithms that are proprietary to each vendor are used to determine the type of a telephone call. The equipment attempts to determine if a call is modem, FAX, or STU, and if the call is not one of the known types, then the call type is defaulted to voice. Each product implemented different approaches for using the call attributes (e.g. source number, destination number, type of call, etc.) in conjunction with rules defined by a site to provide additional security for the telephone network.

Characteristics of the TIDS from Applied Signal Technology / eNetSecure

The TIDS (Model 2600 Modem Sentry) from Applied Signal Technology is built from a specially packaged, rack mountable, Windows NT based personal computer. Applied Signal Technology adds in-house developed custom hardware and software to the system. The hardware includes signal analysis and span connection peripheral cards, and the software includes custom application software. The system uses a Microsoft Access database to record information about the calls.

A single TIDS can monitor up to 12 spans. For each span to be protected, a tap connection is made to the span and located between the central office and the local telephone switch. The tap connection is designed to provide appropriate isolation from the telephone signals for the TIDS system. Since the connection is merely a tap connection rather than an in-line connection, in the event of power failure, there is no disruption of the telephone service. The TIDS is primarily a telephone network traffic analysis system rather than a telephone firewall. This is primarily due to the tap connection to the span and the lack of a direct way for the system to terminate undesired calls.

All traffic information is logged to the local disk on the PC. The TIDS system administrator may elect to have modem traffic recorded on the local disk. A parameter set by the system administrator determines the length (in minutes) of each modem session to record to the disk on the PC.

The quotations below were copied from the Applied Signal Technology/ eNetSecure corporate information (website and printed) about the TIDS [IceMon] and are included to provide the reader with basic information provided by the vendor about the system:

> “IceMon, …is a comprehensive Telecommunications Intrusion Detection System (TIDS) that monitors and protects your telecomm systems and provides a graphical real-time tool to view activity and historical data.”
>
> “The system scales from 2 to 12 T1 lines in a 7"-high rack mount chassis installed on the company telephone switch. It operates passively, leaving all communications free from interference and eliminating the risk of letting sessions pass unmonitored during periods of system overload.”
>
> “IceMon passively monitors all incoming and outgoing phone calls to identify possible intrusion activity through dial-up modems. Additionally, IceMon demodulates the data allowing you to view the content.”

> “IceMon monitors dial-up modem, fax and voice sessions passing through the enterprise phone network, the ‘back door’ that is considered the most likely source of security violations.”
>
> “The system automatically classifies each call as modem, fax or voice; identifies all unauthorized modems; and creates a record identifying key data for each session such as time of call, calling party number, answering party number and call type. This record is archived for historical analysis by the telecom or IT security specialist. The system can be configured to alert the appropriate personnel to suspicious conditions, such as any faxes sent between 12 midnight and 6 a.m., voice lines that are being used to send data, or war dialing indicating an intrusion effort. Intrusion activity reports can be generated upon request or at scheduled intervals.”
>
> “The system identifies the origin and destination of each communication, generates real-time alarms in the event of suspicious activity, and then archives and reconstructs the file, identifying the precise content transmitted or received. Data is automatically reconstructed, including the TCP/IP packets that are the basis of many sophisticated network attacks. Fax recovery is optional.”
>
> “… ability to recover the contents of transferred files or email messages, trace web traffic, and document password cracking attempts is a first in the commercial market. Captured session data can be used to establish the nature of the violation as well as to provide evidence for disciplinary action or legal proceedings.”

Since the TIDS was based on a personal computer, the system interface was through either a directly connected monitor or through a client system [desktop workstation] using the RemotelyAnywhere commercial software package that was supplied with the TIDS to communicate across a LAN to the TIDS.

The TIDS is connected to the telephone span via a passive, tap connection; hence, the TIDS does not have direct control over a telephone call. Applied Signal proposed providing call termination capability based on firewall rules by having the TIDS issues commands to the telephone switch through the use of communication to the telephone switch management control system.

Characteristics of the TeleWall system from SecureLogix

After Sandia completed the evaluation of the SecureLogix telephone firewall (TeleWall) system, SecureLogix re-engineered their telephone firewall system to newer model hardware with appropriately upgraded software. The TeleWall system is described below, since that was the system evaluated at Sandia/NM.

The new version of the hardware and software is referred to as the ETM (Enterprise Telephony Management) system.

The TeleWall system from SecureLogix consists of one appliance for each span to be monitored (either PRI or T1), management server software, and client desktop software. The appliances are custom designed by SecureLogix with appropriate custom software. Each appliance is connected in-line between the central office and the site telephone switch. The information (signal and voice channels) on the span passes through the TeleWall appliance. A TeleWall appliance is connected to the span through an electro-magnetic relay. In the event that power is lost, the TeleWall appliance switches itself off-line and telephone traffic is not disrupted.

A TeleWall appliance gathers attributes of each telephone call on the span to which it is connected. The attributes include typical information (e.g. source number, destination number, start time, stop time, etc.) as well as the type of call (i.e. voice, modem, FAX, STU), span identifier, and other appropriate information. The appliance saves the information in local memory. When a call is completed, the appliance completes the data information item for the call.

The appliances are connected to the computer network, and the management application software runs on a server located on the computer network. The management server communicates over the computer network with the appliances and with users connected from client systems on desktops. On a regular time interval the management server interrogates the appliance to retrieve the stored telephone call information. All permanent information storage is on the management server. After the management server retrieves call information from an appliance, the management server inserts additional information about a call such as the time the information was stored on the management server and any identifying text string that should be associated with a telephone number. The management server then saves the information. (Note that with the new version of the SecureLogix telephone firewall system, the data is stored in a database that is either on the management server or on a separate database server.) If necessary, a system administrator can communicate directly with an appliance either via a telnet connection across the network or via a console physically connected to the appliance.

The appliance runs a modified version of Hard Hat Linux 2.4 where the unnecessary operating system and networking services components were removed. The appliance has a CPU and digital signal processor, 16 MB of RAM, 128KB of SRAM (NVRAM) (for configuration parameters), and 8 MB of compact flash (for telephone traffic information, policy [firewall rules] information, Linux libraries, etc.)

The TeleWall supports firewall rules that are similar to rules used in a computer network firewall. The firewall rules are entered into the management server through a GUI running under the TeleWall client on a desktop. The person entering the firewall rules must also have logon authorization to enter and/or modify firewall rules. After the new firewall rules are entered into the management server, the person must push the new firewall rules to the intended appliances to activate the new firewall rules. An administrator could create a set of firewall rules for supporting a specific situation, and the rules could be saved and then pushed to the appliances when necessary.

Installation of the Telephone Firewall Systems

General preparation for the telephone firewalls involved working closely with the technicians who oversee the operation of the Sandia/NM telephone switch. Several issues were addressed including space and power. Both telephone firewall systems are rack mounted and require standard 120 v AC power. The telephone switch facility has available the appropriate power that is also conditioned and uninterruptible; however, additional circuits and power outlets had to be installed for the firewall equipment. Since the existing equipment racks in the telephone switch facility are designed to support typical telephone equipment, and the telephone firewall equipment is designed for standard electronic equipment racks, appropriate spacers had to be ordered for mounting the telephone firewall equipment.

Installation of the TIDS

Applied Signal Technology designed the TIDS to work with the defined standards for telephone span signaling; however, Applied Signal requested an opportunity to verify the span signaling prior to the installation of the TIDS at Sandia/NM. Applied Signal Technology sent a signal recording unit to be used to monitor the signal channel of a telephone span at Sandia. Sandia recorded a brief (approximately 1 minute) session of the span signals. Sandia repeated the recording on a second span. The signal recording unit was returned to Applied Signal Technology, and the company determined that there were no non-standard signals used on the spans where the signals were monitored. The design of the IceMon appeared to be compatible with the signaling on the telephone spans at Sandia.

Since the TIDS is connected to a span using a passive tap connection, the TIDS is normally connected to the spans by using regeneration equipment consisting of a signal amplifier and an isolation resistor. The amplifier boosts the strength of the signals on the span for the TIDS, and the resistor isolates the TIDS from the spans. The AFIWC personnel loaned one set of signal regeneration equipment, and Applied Signal Technology loaned another set of the same equipment.

The diagram below shows how the TIDS/IceMon was connected to the Sandia/NM telephone PRIs and T1s. The single system only supported twelve spans, so not all of the thirty-one Sandia spans were connected to the TIDS/IceMon.

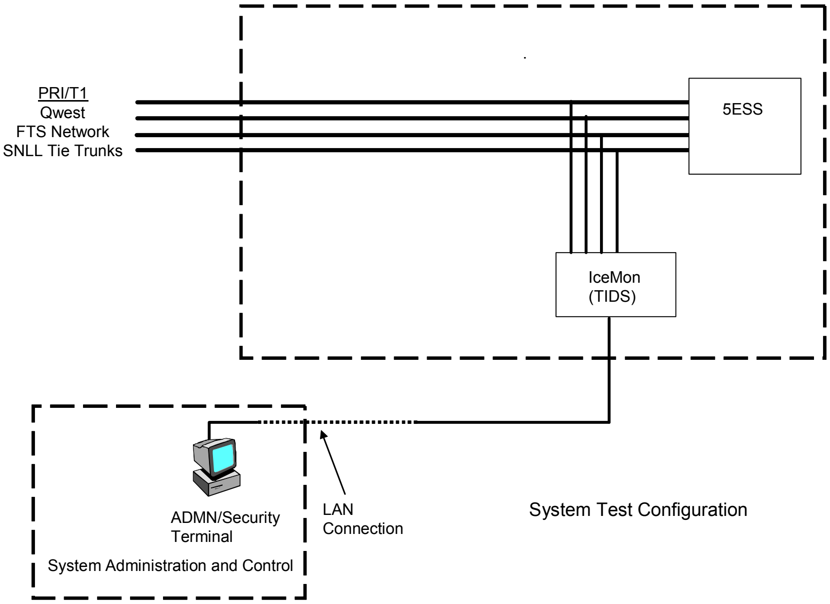

Figure 1. IceMon (TIDS) Installation Configuration.

Personnel from the Air Force installed the TIDS and the necessary signal regeneration equipment at Sandia in early June 2001. The Applied Signal representative was on-site during the installation of the TIDS. The single TIDS was capable of monitoring twelve telephone spans. Since the Sandia/NM telephone switch has thirty-one spans, the twelve spans that were selected for monitoring included a mixture of commercial, FTS, and CA spans. After the TIDS was installed, the Applied Signal Technology representative performed the initial checkout of the system and provided training on the TIDS.

The initial checkout of the TIDS equipment determined that there was a problem with the LAN interface. The lack of the LAN connection prevented the system from being accessed from a remote client. The training in the use of the TIDS was conducted from the TIDS console.

The following day, Applied Signal Technology, attempted to perform diagnostic work on the TIDS via telephone requests to Sandia personnel. After several tests were run, Applied Signal Technology decided that the TIDS mother board needed to be replaced. Applied Signal shipped in a replacement motherboard, and Sandia personnel installed the board. After the installation of the new motherboard, the LAN connection worked correctly.

Installation of the TeleWall

The evaluation agreement with SecureLogix, provided that a TeleWall system (both hardware and server software) would be installed at Sandia and would provide protection for the primary spans connected to the Sandia/NM telephone switch. Sandia acquired a new Sun Netra server to support the management application for the TeleWall system.

Prior to installation of the system, SecureLogix provided a relatively extensive Site Survey questionnaire and a Trunk Information form to be completed by Sandia to assist SecureLogix in developing the installation procedure. From the information supplied by Sandia, SecureLogix followed up with several questions about the telephone switch at Sandia/NM.

The system was installed at Sandia/NM in mid-April 2001 on thirty-one telephone spans connected to the Sandia/NM telephone switch.   SecureLogix installed the system over three consecutive days, and SecureLogix provided two days of training the following week.

The TeleWall appliances were connected in-line with the Sandia/NM telephone PRIs and T1s according to the diagram below.

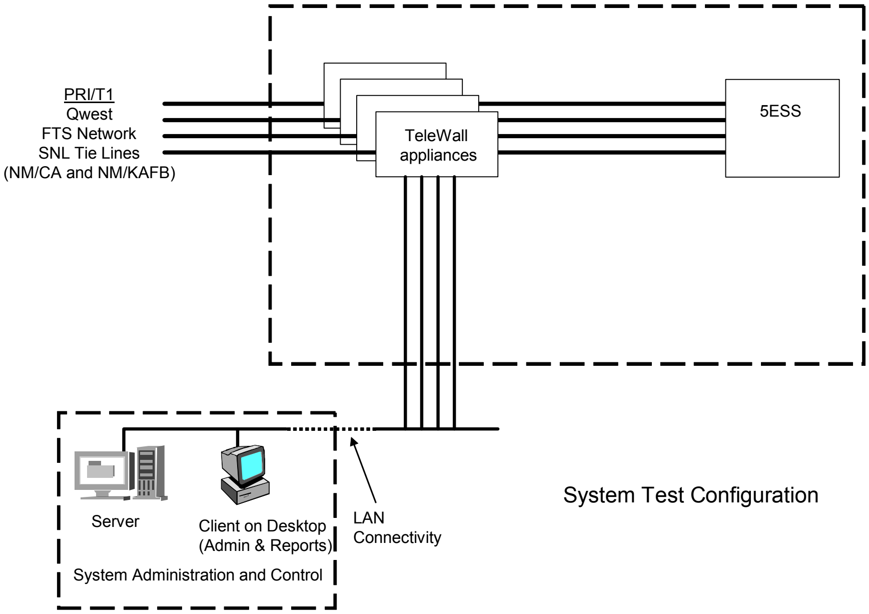

Figure 2. TeleWall Installation Configuration.

The installation of the system by SecureLogix personnel in April 2001 went relatively smoothly. SecureLogix personnel installed the equipment in the racks and configured the equipment for the Sandia/NM spans while another SecureLogix employee directed the installation of the management application software.

The software installation on the management server encountered some problems with the server configuration. This was the first time the SecureLogix installation team had worked with a Sun Netra where there was not a directly connected console, keyboard, or mouse. After several false starts, the software installation was completed on the management server. The client software was also installed on two desktops to be used as the client workstations.

By late in the afternoon on the first day, the appliances were in the racks, preliminary cabling was completed (LAN connection to appliance, and pig tail connections to appliances), and the management server was ready to begin communicating with the appliances. The telephone switch personnel disabled the first commercial span, and as soon as all calls on the span were completed the SecureLogix personnel rewired the span connection to go through the

TeleWall appliance. This same procedure was followed for the remainder of the lines.

A minor configuration problem was encountered when the tie-line to the Sandia/CA telephone switch was connected to the TeleWall appliance configured for that span. The tie-line to Sandia/CA would not go back into service. While the problem was analyzed, the appliance was left in the circuit but in an off-line status. For all spans except the two spans to Sandia/CA, the far end of the span is the “Central Office”. For the tie-lines to Sandia/CA, the telephone switch at Sandia/NM serves as the CO end. There is a difference in the signaling/handshake depending on whether a telephone switch is the CO or the secondary end of a span. Once the determination was made that the Sandia/NM end performed the CO function, the configuration was updated in the appliance, and the appliance was brought on-line to provide firewall capability for that span.

Idiosyncrasies of the T1 connection between the Sandia/NM switch and the Kirtland AFB switch necessitated some customization of the configuration for that span.

Evaluation of the Telephone Firewalls

Test Plan and Testing Procedure

Before any equipment was installed at Sandia/NM, a test outline was developed. After the vendor information was studied, other items were added to the original test outline, and an attempt was made to develop a formal test plan. The development of a rigorous test plan was hampered by the lack of formal test equipment at Sandia/NM. For example, no equipment was available to perform formal testing of modem identification. The test plan attempted to quantitatively verify as many vendor feature claims as possible. In addition, an overall qualitative evaluation of each telephone firewall system was performed in regards to design, usability, and ability of the systems to provide the necessary functionality.

General Areas for Evaluation

The areas examined during the evaluation of the telephone firewalls included aspects of the systems that could be addressed without the necessity of having a formal test laboratory.

1. System Administrator Interaction
   a) Ease of use / user friendliness

b) System setup and configuration
c) Screens; logical connection of menus and submenus
d) Speed of processing of configuration changes
e) Report generation
f) Access controls implemented for protecting system control, administration, and data storage including protections against both external and insider access

2. System operations
   a) Control of multiple spans from a single user terminal
   b) Secure communications between user terminal and units
   c) Provision for autonomous operation of systems
      - Length of time autonomous operation is sustainable
      - Method for updating the stored information/database updated and the update interval
      - Provision for authenticated communications with server
      - Access control mechanisms
   d) Capabilities for control of server/client
   e) Effects of power loss
   f) Ability to isolate system from spans
      - How is this initiated or accomplished?
      - Type of connection (i.e. bridge (isolated tap) connection vs. in-line connection)
   g) Ability to control operation by channel within span
      - Ability to turn off monitoring by PRI/channel
      - Ability to control recording by PRI/channel
      - Ability to control content of data recorded by channel
3. Handling of identification of call type
   a) Ability to distinguish voice, modem, FAX, STU
   b) Alert notification mechanisms (e.g. log, e-mail, etc.)
   c) Capability for detecting war dialing
4. Overall security provisions and philosophy
5. Data/information handling
   a) Information storage format
   b) Report generation capability
   c) Capability for handling condition when disk full
   d) Controls to protect data from alteration
   e) Whether there is a delay before data is available for analysis
6. System maturity (e.g. production level, provisions for system update, etc.)

Evaluation of the TIDS

The TIDS (IceMon) system was installed at Sandia/NM and connected to twelve PRI spans in June 2001. The system was evaluated for approximately two months (June 2001- mid August 2001). No telephone test equipment or load simulation equipment was available for performing any quantitative testing.

The IceMon system was connected passively to the twelve PRI spans using isolation resistors and signal amplifiers. The system (either with or without power) did not appear to cause any problems with the PRI spans and appeared to operate in the desired passive mode. The system identified calls as voice, modem, or FAX. The system demodulated modem sessions and recorded the information on the system disk. The installed system did not include a capability for demodulating FAX sessions.

Without access to appropriate test equipment it was not possible to verify that the IceMon correctly identified all voice, modem, and FAX calls. Since only 12 PRI spans were monitored, no attempt was made to identify all telephone lines with unregistered modems.

Reports produced by the supplied report generation tool retrieved information from the system database and identified source and destination telephone numbers as well as start of call (date and time) and end of call (date and time). A small number of demodulated http sessions were examined to verify that demodulation occurred; however, no attempt was made to verify other aspects of the demodulated information. The current corporate approach to information security at Sandia does not include monitoring, reconstructing, and analyzing modem sessions, and the demodulation feature is not a current Sandia requirement. No attempt was made to verify that the system could generate real-time alarms for suspicious activity due to concerns about other aspects of the IceMon system.

The system generally performed as described in the Applied Signal Technology corporate information. However, the system appeared to be in a very early stage of development and would not be easy to use in the production environment at Sandia/NM. During the training on the equipment, the vendor described several existing problems that were known by the vendor and that the vendor planned to resolve later in the development of the product. The problems described by the vendor were observed during the operation of the equipment at Sandia.

The IceMon crashed occasionally, which stopped the security monitoring of the spans until the system was restarted through manual intervention to reboot the system. The system also filled the logging disk with demodulated modem sessions, and the system did not provide any capability for automatically handling the occurrence of a filled disk. When the system filled the disk, the system stopped security monitoring of the spans. Manual intervention was required to clear the disk containing the demodulated sessions and to restart the IceMon system. Both of these problems were described during training.

The modem report tool provided as a part of the IceMon report generation capability was used to produce a report of calls that the IceMon system identified as modems. Some modem calls identified by the IceMon were on telephone lines not previously registered for modem use, and some of the telephone lines were determined to have an unregistered modem connected. However, for some of the calls that the IceMon characterized as modem traffic no on-site modem could be identified, and there was concern about the accuracy of the identification algorithm.

From the data in the report, a larger number of short duration (0 to several seconds) calls were categorized as modems than anticipated. Studying other records for the identified telephone numbers residing on the telephone switch showed that some telephone numbers did not appear to have any other modem usage indications. Several of the off-base numbers associated with the calls identified by the IceMon as modem were investigated. The investigation determined that several of the off-base numbers responded with tone/message combinations (e.g. voice-mail, answering machine, and automated operator), and there is a concern that in some cases the system was prematurely and inaccurately categorizing calls as modems. The call record database with over 830,000 records produced by the IceMon was examined further and found to contain 64 calls of zero length duration and 882 calls of 1 second duration categorized as Bell 103, V21, or V27TER modems (IceMon codes 9218, 9219, and 9232). No attempt was made to analyze the 0 and 1 second calls in any more detail or to run any controlled tests. However, these calls appeared to be too short for the type of call to be determined accurately.

The IceMon provides firewall [call blocking] capability by issuing commands directly to the management port on the telephone switch. This provision was not tested since external access to the management port on the Sandia/NM telephone switch is not allowed due to security concerns.

To monitor the thirty-one spans at Sandia/NM would require three IceMon systems, because the IceMon supports a maximum of twelve spans per system. Since each IceMon system is independent and logs the telephone call information data on the self-contained disk, the management and administration of three systems would be a challenging effort, and data report generation would require interfacing with three separate IceMon systems. There is no provision for integrating data from the three systems into a single report or for displaying a status of three systems on a single monitor. A system that would handle all spans (regardless of the number) in an integrated system would be significantly easier to use and much more desirable.

The RemotelyAnywhere commercial software supplied with the TIDS provided remote access from an office desktop workstation across a LAN to the Windows desktop on the TIDS; however, the access was a bit cumbersome and was slow at times. The RemotelyAnywhere software was not able to support a desktop workstation with an HDTV aspect ratio monitor. The RemotelyAnywhere software was not the current version available from 3AM Laboratories PL, Hungary, and a newer version of the software might have resolved the problem encountered with one computer monitor. The IceMon system designers expected the system to be on a small, limited access network, and only incorporated minimal access control mechanisms (e.g., a password).

The TIDS/IceMon appears to be in an early stage of development as a prototype system and provides opportunities for improvement in the user interface software and in the robustness of the software system. Many of the commands were quite cumbersome, and the system did not recover well from various situations (e.g. full disk). The IceMon modem identification data did not appear to accurately characterize the traffic at Sandia due to the significant number of very short calls identified as modems. Formal testing of the modem identification algorithms would be recommended for this equipment. The IceMon system, as evaluated, does not have an immediate application at Sandia since the demodulation capability is not a current requirement, and the use of the telephone switch management port to implement firewall rule call blocking precludes the use of the firewall capability. Allowing the TIDS to issue commands to the telephone management port was viewed as an unacceptable security risk. The TIDS appears to be better suited to an environment that desires span -monitoring rather than firewall protection.

Evaluation of the TeleWall

The TeleWall system from SecureLogix was evaluated at Sandia/NM from April through July 2001. Thirty-one appliances were installed to provide firewall capability on all spans connected to the Sandia/NM telephone switch (i.e. twenty-one commercial PRI spans, seven FTS PRI spans, two PRI spans to the Sandia/CA telephone switch, and one T1 span to the Kirtland AFB telephone switch). The equipment appeared to perform generally as the manufacturer claimed. Since Sandia does not have an appropriate test capability for generating simulated telephone calls, all aspects of the equipment were not tested. Testing included observations from using the equipment under normal operational loads at the Sandia/NM facility and with scenarios that did not require special test equipment (e.g. load generators, simulation of standard modems).

After the TeleWall system was operational, Sandia began testing to explore the product capabilities as documented in the vendor information and through specific tests as described in the test plan. The first test was a power-off test of the TeleWall system. The test verified that the TeleWall system did not interrupt telephone service when the system lost power.

One appliance needed to be replaced during the evaluation period. During the evaluation period, the vendor supplied a new version of the appliance software to correct a problem with displaying the 7-digit expansion of the 5-digit calling used by Kirtland AFB on the T1 span to the Kirtland AFB telephone switch. When an attempt was made to load the software into the appliance for that span, the appliance hung in an initialization loop, and control could not be regained. SecureLogix replaced the appliance. The software was successfully loaded into the replacement appliance.

The appliance on each span gathers information about the call traffic on that span. The TeleWall management server and the appliances are connected to a LAN. The TeleWall management server retrieves the call traffic information from the appliances across the LAN and stores the call traffic information in two files. The first file, the Audit Log, contains an entry for every call between an off-site telephone and a telephone on the telephone switch. The second log (Security Log) contains an entry for all calls that trigger a firewall rule where the logging function is requested. The Security Log also contains an entry for every call that changes type (e.g. from voice to modem) during the call.

A set of simple firewall rules was implemented to use the firewall to identify modem and FAX traffic. Rules were implemented to allow all modem calls to the modems used to access the corporate network. Additional rules were inserted to allow all other modem and FAX calls, but to save the call information in the Security Log. Additional simple rules were implemented to test controlling access to two special sets of modems. The two sets of modems are for special applications, and only a limited set of off-site numbers are allowed to access the modems.

After the TeleWall system was in operation and the firewall rules implemented, the Security Log was examined using the report generation capability provided with the TeleWall system. The report generation capability provides a set of typical reports, and the report generation tool provides an easy means for a site to modify and customize the provided reports and to generate new reports. Reports were used to identify modem traffic. The reports showed that the TeleWall system was identifying many inbound and outbound modem calls to telephones not registered for modem use. The reports can retrieve information from either the Audit Log or the Security Log. A date and time interval can be specified. The report generator also provided a capability for producing graphs of the retrieved data.

The system provided a simple disk management process. A site can set a threshold value for the call log storage area. If the amount of disk space for the call logs exceeds the threshold value, then the system deletes the oldest files until reaching a lower threshold set by the site. The deleted logs are lost, but the system continues to operate without losing new data.

Without appropriate testing equipment, the accuracy of the modem detection by the TeleWall system could not be verified; however, examination of reports from the TeleWall system and comparison against the corporate dial-up access lines for the computer network appeared to reflect traffic observed by the dial-up equipment. A comparison with other monitoring equipment produced a high level of correlation in identified modem calls for calls to numbers that were known to have modems and for numbers that could be confirmed to have modems.

Some discrepancies were observed with the TeleWall system categorizing some low speed STU calls as modem calls. At the recommendation of the vendor, a TeleWall configuration option was changed, and the configuration change appeared to provide more accurate identification of low speed STU calls.

The telephone firewall capability was tested by entering a firewall rule into the system to block voice calls to a telephone and then verifying that the calls were blocked. As noted earlier, rules were also entered to protect two sets of special service modem numbers. Each set of numbers had a limited list of off-site numbers that were allowed to call the on switch numbers. Based on the telephone firewall rules, the TeleWall system blocked non-approved calls to the designated telephone numbers, logged the blocked calls in the security log, and generated e-mails to the responsible parties as directed by the structure of the entered rules.

Sandia uncovered a problem with how the TeleWall system handled items referred to as “phone objects”. To implement firewall rules that relate to specific telephone numbers, phone objects are created for each telephone number (or block of telephone numbers). The telephone object includes the specific telephone number (or group of numbers) and a text field [name of object] to be associated with the telephone object. When the initial firewall rules failed to perform correctly, it was determined the system did not properly handle a telephone object that contained a comma in the name of the telephone object (e.g. “Doe, John A. “). SecureLogix had not encountered that problem before; however, after confirming the problem, SecureLogix recommended using a hyphen rather than a comma until the problem could be corrected in a future release of the software.

When the application of a firewall rule based on date and time was tested, the system failed to correctly implement the firewall rules. The vendor confirmed a problem in the software and supplied a revised version of the software. The test was successful when repeated.

The management application for the TeleWall system communicates across the computer network with all the appliances. A client application runs on a desktop and communicates across the computer network with the management application. The client application has displays for observing and managing all installed appliances. The displays were comprehensive, reasonably intuitive, and easy to use. There was extensive on-line documentation about the system.

Several security features were incorporated into the TeleWall system. These features allow a site to restrict access to the appliances and management application to only approved IP addresses and authorized users. Encrypted communication is used to protect the transmission of passwords and data. A site may also set specific capability privileges for individual users. The details of these and other security features are described in the equipment documentation. The design of the system does not appear to introduce any additional vulnerabilities that an attacker could exploit (e.g. denial of service attack, etc.)

The TeleWall system performed very well and appeared to be well designed and engineered including the hardware and packaging, the software system, the user interface, and the security features. The client software provided a very nice interface to the system and was relatively robust. Several problems with the TeleWall software were identified during the evaluation period; however, SecureLogix responded quickly with either a solution or a temporary work-around. The TeleWall system performed well under all tests based on observations and analysis of reports requested from the system.

Operational Issues Resolved with the SecureLogix Telephone Firewall System

During the TeleWall evaluation period, the TeleWall system provided information that assisted in resolving several telephone network operational issues. The TeleWall system provided insight that was either unavailable or not easily attainable from the telephone switch.

Videoconferences are established between the Sandia California and New Mexico sites. There was concern that bills for the calls appeared to be higher than expected. With the TeleWall system it was determined that the wide-band connections were not being dropped at the appropriate times and were continuing to stay active, which generated higher bills for the service than appropriate.

Prior to the installation of the TeleWall equipment, there was an intuition that calls from the Sandia New Mexico to the California site were not being routed appropriately (i.e. first to tie-lines, then onto FTS, and as a last resort onto commercial lines). The TeleWall system confirmed that there was a problem with call routing at the NM switch. Sample calls were placed and tracked with the TeleWall system. Based on the observations, the programming in the Sandia/NM telephone switch was changed to provide appropriate call routing to Sandia/CA.

Several incidents of improper use of the Sandia telephone system were confirmed through the implementation of appropriate diagnostic rules in the telephone firewall. The improper use was handled through defined corporate processes.

A question was raised about whether there was excess capacity in the commercial telephone circuits, since decreasing the number of commercial spans could reduce lease costs. An analysis of peak level use of the commercial telephone circuits determined that there is only a small amount of excess commercial circuit capacity during peak call situations.

After several individuals complained about receiving single page, blank documents via FAX, the FAX traffic was investigated using the TeleWall system. Careful analysis of the call information from the TeleWall system determined that an external individual (or individuals) were randomly dialing numbers on the Sandia telephone switch and as soon as a FAX machine responded, the call was terminated. All the calls originated from numbers with the source number blocked. It was impossible to determine whether the external calls were attempts to identify modems for hacking purposes or to identify FAX numbers to sell to FAX spammers.

Collaboration with SecureLogix

During the equipment evaluation period, Sandia identified a number of topics about the TeleWall system that were discussed with SecureLogix. SecureLogix was a very cooperative vendor and even enthusiastic about discussing observations made by Sandia. SecureLogix was very interested in receiving feedback on their product and actually requested recommendations from Sandia about changes and desired new features. Sandia identified several problems with the system that were unknown to SecureLogix and that in general, no other sites had reported. Sandia also provided SecureLogix with several recommendations for improving the usability of the system

Sandia collaborated with SecureLogix in examining call type recognition for different situations of FAX and STU activity. This involved running several controlled tests and documenting the results for SecureLogix.

From analyzing the error logs produced by the system, the appliance software appeared to have a memory leak. Error log entries indicated that the appliances had buffer availability problems after running for many days, and eventually an appliance would restart itself when no buffer space was available. SecureLogix confirmed the problem and had received a similar report from an installation in Europe. SecureLogix supplied a new version of the appliance software.

Following the evaluation period, Sandia continued to provide feedback and recommendations to SecureLogix. Activities following the evaluation period will be documented in another report.

Recommendations for Sites Considering Telephone Firewall Installations

General Considerations for Sites

The decision to install a telephone firewall is not necessarily an obvious one to make. While the telephone firewall equipment does provide an opportunity for a site to improve overall network security by providing telephone network security, each site must carefully determine the specific reasons for installing a telephone firewall. A telephone firewall provides the potential benefit of improved security through the opportunity to implement controls on the use of the telephone network. However, there is an associated cost for the initial purchase, the annual mortgage for maintenance and support, the additional personnel to administer the firewall system, and planning for future system replacement as new technologies emerge.

The firewall equipment can provide improved security through additional protection for the telephone network and improved policing of the use of the telephone system. A site needs to determine if these benefits are applicable to the situation at the site and whether the security improvements are worth the additional investment and increased on-going costs. For example, if the site has a casual use policy for the use of telephone and FAX, then there may be very little to be gained by significantly increasing the effort for policing telephone system usage regarding misuse. If a site desires to use the telephone firewalls to improve modem security then the site should ensure that appropriate corporate policies are in place to clarify the use of modems on the corporate computer systems and computer networks.

The site should analyze existing corporate policies and determine whether the policies reflect the desired level of security and use for telephone, FAX, modem, and STU. Particular aspects of policies to be considered include registration for modem, FAX, and STU, security issues with outbound versus inbound modems, modems configured to allow auto-answer versus disabling the auto-answer feature, use of modems and FAX during non-working periods, etc.

If a site has written policies in place regarding modem use and personnel are available to administer a telephone firewall, then a properly installed and managed telephone firewall system can improve the existing level of security.

A site needs to determine whether other organizations are supported by the telephone switch or the telephone spans. If other organizations are supported, then implementation of security and telephone use policies may need to be negotiated with the other organizations that are supported by the telephone system to avoid implementing on the telephone firewalls policies that negatively impact the other organizations.

The site should examine what measures are currently in place to implement existing policies for telephone security and use. Typical measures include a modem registration procedure, the use of an automated dialing system to attempt to identify modems on computer systems, and on-going analysis of telephone call records to identify misuse. The site should then decide whether implementing a telephone firewall system provides improvements to the existing security measures.

A site can use the telephone network firewall system to implement telephone usage and security policies through firewall rules applied to specific telephone numbers where the firewall rules restrict the type of use (i.e. voice, modem, FAX, and STU), direction of use (inbound and/or outbound), and time of day/day of week use. However, the site should be aware that only calls off switch are processed by the telephone firewall, since the telephone firewall is connected into the telephone spans between the Central Office and the site operated telephone switch.

Assuming that a site determines that the acquisition of a telephone firewall makes good business sense, then the site should identify the telephone spans to the facility that should be protected. For example, if the site plans to deploy telephone firewall systems at multiple locations that share tie-lines between the locations, then it does not necessarily make good business sense to pay for telephone firewall equipment to monitor both ends of each tie-line. Spans assigned to dedicated activity may not need to be protected by telephone firewall equipment either.

The site should begin identifying specific telephone numbers to protect. These numbers may include known corporately supported modem connections to the computer networks, modem connections used by support technicians to work on vulnerable equipment, etc.

While waiting for the telephone firewall equipment to be installed and brought into production, the site should begin developing statements to notify employees that additional security protection will be implemented on the telephone system. Many individuals are very sensitive to the issue of telephone call monitoring. By notifying the employees about the installation of telephone network firewall equipment and how the new equipment will be used, the site can minimize the employee concerns. The site should be careful to use non-threatening and non-alarming statements. For example, avoid the use of terms that might lead to the feeling that “Big Brother” is now watching such as “monitoring calls” and “recording information” that may lead employees to believe that conversations are being monitored and recorded. Alternative wording that could be used includes – “gathering information about telephone traffic” and “saving information about call attributes”. Also indicate that information about the telephone traffic is gathered already (e.g. source, destination, date, time, etc.) and that to enhance protection of the telephone and computer networks the type of the call (voice, modem, FAX, STU) will be included in the information that is gathered.

After a Site Installs a Telephone Firewall

Once a telephone firewall system is installed, the site should spend a period of time learning about the equipment and learning about the characteristics of the telephone traffic at the site. Consider having on-site training so that the training is convenient to personnel. The savings in travel costs may allow additional personnel to attend training. The classroom training will be conducted on a demonstration system set up to provide a simulated environment. Outside of classroom time, the students can apply their new knowledge to the production system to increase their understanding of the capabilities and use of the new equipment.

An initial set of telephone firewall rules can be implemented to gather initial data about the telephone traffic at the site. Implement rules to allow modem traffic to corporate computer network dial-up modems and to allow and log all other modem, FAX, and STU traffic. If there are specific telephone numbers with modems that can be identified as benefiting from protection a few simple rules can be implemented as part of gaining understanding about the telephone firewall system. For example, if there is a modem that must be accessed by technicians responsible for on-call support of specific equipment, then the telephone firewall equipment can be used to restrict access to the modem line to only the home telephone numbers of the responsible technicians.

The site should not immediately implement telephone firewall rules to block modem traffic. There may be modems at the site that are attached to and provide support for critical systems such as power, heating, ventilating, and air conditioning, etc. that should not be disrupted or blocked. A site should initially use the telephone firewall equipment to gain an understanding about the characteristics of the telephone traffic at the site, and this approach is very important for helping to begin to identify corporate telephone lines with special modem equipment that must not be blocked.

From the initial set of simple firewall rules, the site can begin gathering information about the telephone traffic at the site. The site should publish notifications to the employees about the new equipment and describe the intended use of the equipment, as noted above, with any announcements carefully worded to avoid potentially inflammatory wording. By keeping the initial notifications to employees simple, the site may avoid having employees change their habits for using modems, etc. Thus the initial information gathered by the telephone firewall system will more closely reflect actual telephone traffic prior to the installation of the telephone firewall system.

Simple reports can be produced to provide information about the telephone traffic. Gathering information about modem traffic may provide a surprise to the site by the volume of modem activity (both inbound and outbound) detected. From the identified modem traffic, the site may choose to attempt to identify the remote numbers that are being called from the telephones at the site. Off-site numbers can often be identified through reverse telephone look-up Internet sites and through Internet searches. The site can then enter these telephone number identifiers into the telephone firewall system to use in characterizing the modem traffic from the telephones at the site.

As the site gains an understanding on how the employees are using the telephone system, particularly in regards to modems, the site should review once more the corporate policies on use of the telephone system and the use of modems, FAX's, and STU's. Once all the appropriate policies are in order, the site can implement an appropriate system for registration of modems and initiate notification to all users about the requirement to register modems. The site can also remind users of the corporate policy on appropriate use of the telephone system.

When telephone lines with modems, FAX's and STU's are registered, the telephone firewall administrator should implement rules to authorize the registered telephone lines. The site can also begin identifying the telephone lines with non-voice traffic that are not registered. Some will be for non-voice traffic that no individual appears to have ownership (e.g. a modem used for maintenance on custom equipment). The staff supporting the telephone firewall will need to persist in identifying and tracking down responsible owners for the unregistered lines with non-voice traffic.

Conclusion

A telephone firewall system is an important aspect of the overall security system for a site and provides protection of the telephone network. The ability of a telephone firewall system to restrict access to specifically identified modems decreases the likelihood that an external subversive would be able to gain control of a computer connected to both the telephone network via a modem and to the corporate computer network. An appropriately implemented site modem use policy in conjunction with telephone firewall rules may decrease the use of outbound modems to connect to Internet service providers (ISPs) and encourage the employees to access the ISPs via corporate Internet connections, where security controls for virus and abuse protections are normally in place.

A telephone firewall system that provides additional information about the span utilization may assist a site to identify both under utilized spans and spans that are close to capacity.   The telephone firewall system may also provide additional information about the status of spans and channels that will be useful for the personnel that operate the telephone switch.

Any site that has invested in computer network security protection through the implementation of firewall and intrusion detection systems should also implement appropriate telephone network protection through a telephone firewall system. Based on the evaluation of the telephone firewall products, Sandia installed the SecureLogix TeleWall system at both the New Mexico and California sites.

Distribution

1	0806	J. P. Abbott, 9322
1	0864	J. S. Ahrens, 3112
1	0812	P. P. Baca, 9334 (Verizon)
1	0812	M. J. Benson, 9334
1	9037	J. C. Berry, 8947
1	0806	C. D. Brown, 9322
1	9012	L. A. Brown, 8949
1	0812	L. D. Byers, 9334
1	0813	R. M. Cahoon, 9311
1	0809	G. E. Connor, 9335
1	0806	J. M. Eldridge, 9336
1	9012	R. D. Gay, 8949
1	9012	S. C. Gray, 8949
1	0812	M. D. Gomez, 9334
1	0806	S. A. Gossage, 9336
1	0801	A. L. Hale, 9300
1	0806	D. A. Hansknecht, 9322
1	1227	E. B. Held, 5010
1	1227	G. A. Hendrickson, 5010
1	9011	B. V. Hess, 8941
25	0806	J. A. Hudson, 9322
1	9109	M. A. Jacobs, 8949
1	0806	P. C. R. Jones, 9322
1	0812	P. L. Manke, 9334
1	0801	W. F. Mason, 9320
1	0806	M. M. Miller, 9336
1	0630	M. J. Murphy, 9600
1	0813	D. N. Packwood, Jr., 9311
1	0812	D. R. Porter, 9334 (Verizon)
1	0812	G. F. Rudolfo, 9334
1	0630	D. H. Schroeder, 9630
1	0801	M. R. Sjulin, 9330
1	0806	L. Stans, 9336
1	0813	R. A. Suppona, 9311
1	0805	W. D. Swartz, 9329
1	0812	E. C. Thompson, 9334
1	0806	L. F. Tolendino, 9336
1	0139	M. O. Vahle, 9900
1	0812	D. L. Vanhouten, 9334 (Verizon)
1	9003	K. E. Washington, 8900
1	9018	Central Technical Files, 8945-1
2	0899	Technical Library, 9616
1	0612	Review & Approval Desk, 9612 For DOE/OSTI