CAIL Security

Overview

To quickly and easily have more trusted systems, comply with security regulations, and better assure information privacy, CAIL provides industry standard SSL and SSH based solutions. And for those who are still using them, we are continuing support for our “classic” PCProxy and PCSST products.

CAIL / SSL Encryption

The CAIL / SSL Security Facility provides corporations with a way to secure almost any TCP/IP based data streams between the PC and NonStop host, between NonStop hosts, and from/to the NonStop host to/from other systems that support the SSL standard.

This is a Proxy based solution, providing secure sessions without any changes to application programs other than to reconfigure the IP Address and Port Number to which the application normally connects.

All NonStop modules are available for both K & S series systems, and for new Itanium based Integrity NonStop Servers and Blades. These are native Guardian based programs, thereby removing the need for OSS. The CAIL / SSL Security Facility includes four proxies for the NonStop host:

- SSLPrxy: Server proxy secures incoming telnet and any other socket based communications coming from the PC, other NonStop hosts, or from other systems that support SSL secured connections.

- SSLPrxc: Client proxy secures outgoing telnet and any other socket based communications going to other NonStop hosts, or to other systems that support SSL secured connections.

- SSLFTPS: Server proxy secures incoming FTP communications coming from the PC, other NonStop hosts, or from other systems that support SSL secured FTP (FTPS) connections.

- SSLFTPC: Client proxy secures outgoing FTP sessions to other NonStop hosts, or to other systems that support SSL secured FTP (FTPS) connections.

All PC modules run as a service which can be configured to start automatically when the PC is turned on, thereby avoiding the need for the user to even be aware that the sessions are secured. One service can run multiple proxies, for both Telnet or FTP sessions, or for any other applications that communicate with the NonStop host via socket based TCP/IP. The CAIL / SSL Security Facility includes two proxies for the PC:

- PCSSLPrxy: Client proxy secures outgoing telnet and any other socket based communications going to NonStop hosts, or to other systems that support SSL secured connections.

- PCSSLFTPPrxy: Client proxy secures outgoing FTP sessions to other NonStop hosts, or to other systems that support SSL secured FTP (FTPS) connections.

Features

- Easy installation, with PC utility to transfer host modules. Can be active in minutes
- Support for Client and Server Certificates
- Optional User database to easily add / remove User access
- Optionaly verify SSL client certificates username and serial number against database
- Two factor authentication – Username/Password and client certificate
- Logging with time of connection and disconnection, and Users IP address; useful for auditing purposes
- All native binaries: code 700 for K and S-Series, and code 800 for Itanium based systems including Blades
- Not a direct port: enhancements made to improve performance and reduce CPU usage
- Regular updates to the latest release of OpenSSL
- Instruction on how to “lock down” Telserv and FTPServ so they can’t accept non-secure connections
- Only minor changes to scripts that transfer files in clear text now, since the built-in NonStop FTP client is used

The following diagrams provide an overview of how the system works. Figure 1 represents an SSL Proxy scenario, while Figure 2 represents an SSL FTP Proxy scenario.

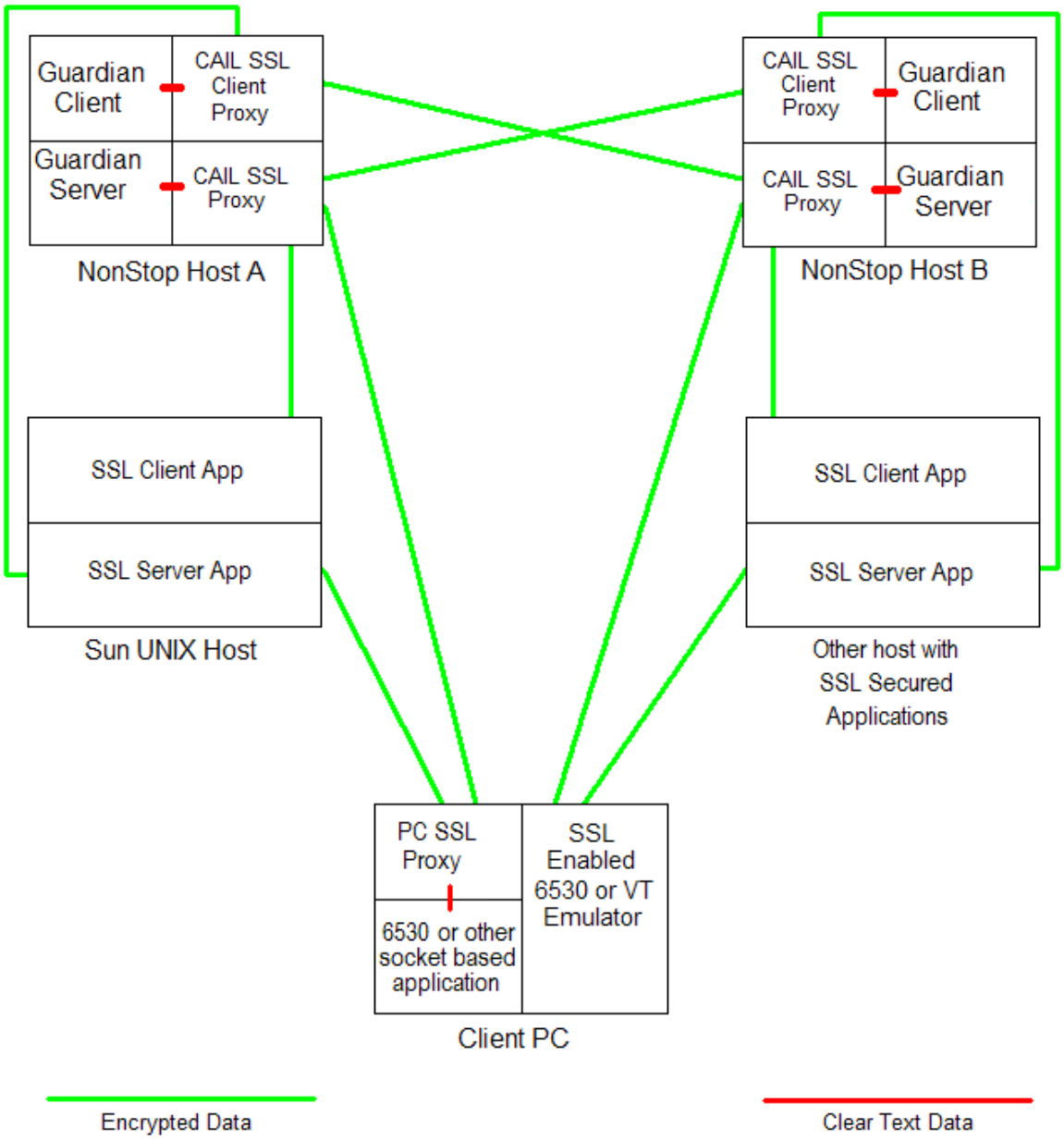

Figure 1 – SSL Proxies

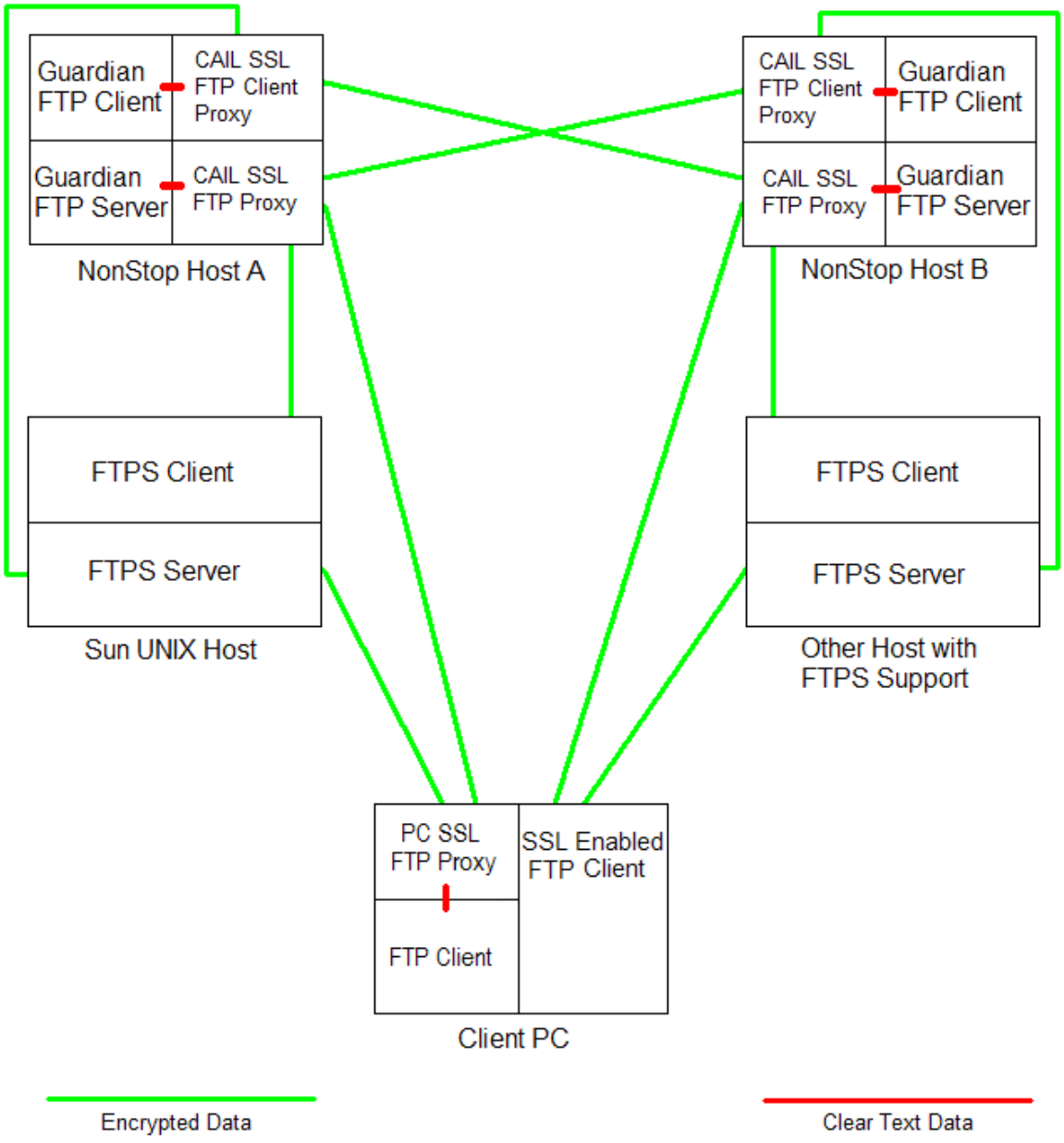

Figure 2 – SSL FTP Proxies

CAIL / SSH Encryption

SSH is a suite of network connectivity tools that increasing numbers of organizations are coming to rely on. CAIL / SSH encrypts all traffic (including passwords) to effectively protect your data-in-motion. Additionally, CAIL / SSH provides secure tunneling capabilities, as well as a variety of authentication methods.

CAIL / SSH includes SCP (Secure Copy Program), which is an RCP like client that can be used for file transfers over the network. SCP uses SSH to secure data connections, and supports large file (2GB+) access.

SFTP (Secure File Transfer Program) is an FTP like client that can be used to secure file transfers over the network. SFTP now supports direct access to the GUARDIAN and OSS file systems. The new SFTPG client accesses the guardian filesystem directly for copying files to and from the system. This also supports large file access for OSS.

SSHD (Secure Shell Daemon) is the daemon program for SSH. It handles key exchange, encryption, authentication, command execution, and data exchange.

Together these programs replace the UNIX rlogin and rsh programs, and provide secure encrypted communications between two untrusted hosts over an insecure network. The programs are intended to be as easy to install and use as possible.

Features

- High performance and low CPU overhead
- Scalable across all CPUs in a 16 node system.
- Full replacement for telnet, rlogin, rsh, rcp, and ftp
- Instruction on how to “lock down” Telserv and FTPServ so they can’t accept non-secure connections
- Automatic authentication of users, no passwords sent in cleartext
- Encryption and compression of data for security and speed
- Multiple built-in authentication methods, including passwords, public key, SecurID, and host-based authentication
- Support for multiple public key algorithms, including DSA and Diffie-Hellman key exchange
- Multiple ciphers for encryption, including 3DES, Blowfish, Twofish and AES
- Guardian SFTP server for accessing the guardian file system directly