com.forte®
better always on

SecurTN

Integrated and high-performance solution for securing terminal access to NonStop systems

Today many organizations providing enduser access to NonStop host applications via Telnet across large networks face several serious challenges. Realizing that Telnet communication is vulnerable against sniffer attacks to spy on passwords and confidential application data, security becomes a very important issue.
Furthermore, standard Telnet servers are often incapable of handling large numbers of users and sessions efficiently.

Purpose

SecurTN provides secure and manageable high volume Telnet access to applications running on HP NonStop systems. It combines the functionality of a powerful Telnet server with strong authentication, user access control, session encryption and auditing facilities in a single, integrated product.

Features

Data encryption using SSL/TLS

SecurTN takes advantage of the most widely used and accepted security protocols:
Highly Secure Connections with SSL/TLS. All standardized SSL/TLS versions up to version TLS 1.2 are supported, along with the strongest cipher suites available from the TLS 1.2 standard, like RSA or Elliptic Curve based key exchange combined with 256 bit AES in Counter mode with SHA384 MAC.
Support of Public Key Infrastructure (PKI) allows you to enforce both client and server authentification. Use of strong bit-size Elliptic Curve, RSA and DSA certificates is supported.

N E W / O P T I O N A L :
support of 3270 emulation protocol

TELSERV replacement

SecurTN fully replaces TELSERV and enhances Telnet connectivity through the following features:

- Unlike TELSERV, SecurTN supports an unlimited number of sessions per process
- Multiple TCP/IP processes and ports within a single process
- supports OSS shells using 6530, vt100 and vt220
- Support for 3270 protocol
- Pathway TERMs can be created dynamically; this significantly reduces overhead for the management of Pathway systems with many end users

Auditing

SecurTN optionally creates Audit events and writes them to an EMS collector where it can be viewed and filtered using standard procedures.

Access Control

SecurTN provides features for tight control of application access:

- Restrict services to specific IP addresses
- Strong Client Authentication through SSL/TLS
- Retrieval, display and auditing of information such as Windows user name from the workstations connecting to SecurTN

Requirements

NonStop System:
- G06.29 or later
- H06.18 or later
- J06.05 or later
- L15.02 or later

Telnet Clients:
Any TN6530, vt100 or vt220 client for unencrypted access. MR-Win6530, J6530, JPath or any other SSL/TLS-enabled TN6530, vt100 or vt220 client for SSL/TLS-encrypted access.

SecurTN

Benefits

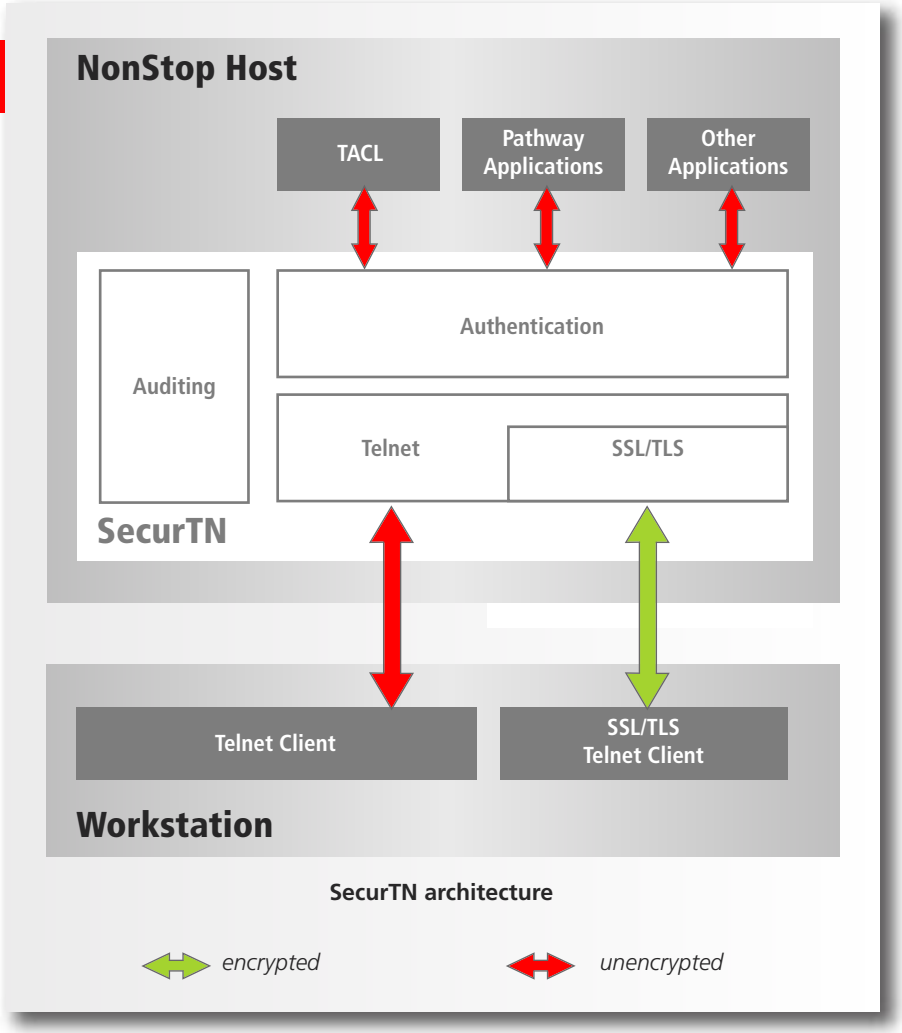
With its first release being shipped in 2001, SecurTN is **a proven solution.** Various customers around the world use SecurTN to secure Telnet access.

The **tight integration of Telnet, SSL/TLS and audit** functionality provides a single view of terminal-based access to your system.

Architecture

SecurTN has a layered architecture as depicted in the diagram.

All SecurTN layers generate audit events, which can be monitored to confirm the security process' effectiveness.



SecurTN architecture

comForte 21 GmbH, Germany
phone +49 (0) 611 93199-00
sales@comforte.com

comForte, Inc., USA
phone +1 303-256-6257
ussales@comforte.com

comForte Asia Pte. Ltd., Singapore
phone +65 6818 9725
asiasales@comforte.com

comForte Pty Ltd, Australia
phone +61 2 8514 7007
aussales@comforte.com

www.comforte.com

comforte® better always on

For distribution partners in your region visit comForte's homepage www.comforte.com