comforte

SecurCS

Adding SSL/TLS encryption to TCP/IP connectivity for NonStop systems

Today many organizations exchanging data between computer systems across TCP/IP networks are facing serious challenges. Sensitive data is sent across large networks not only by using Telnet, but also by using Client/Server protocols such as Remote Server Call (RSC),Open Database Connectivity (ODBC), IBM Websphere MQ or numerous other protocols. All those TCP/IP based access methods for NonStop systems do not come with encryption capabilities. User names, passwords, and application data are sent across the network in the clear, making the data communication vulnerable against sniffer attacks to spy out or change confidential data during transit across the network.

Purpose

SecurCS provides SSL/TLS encryption capabilities to Client/Server middleware protocols without any changes to the underlying components. It can also be used to encrypt the Telnet data stream between any standard TN6530 emulator and the NonStop TELSERV process.

Features

SecurCS takes advantage of the most widely used and accepted security protocol:
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.
Allows for enforcing strong isolation

- Access to the protocol without encryption can be disabled if required.
- Allowed remote IP addresses can be limited by implementing white lists and black lists.

Optionally, SecurCS can be used to write an **audit log** of all network traffic. This can be useful for protocols such as ODBC or Telnet when a complete byte-to-byte dump of the network traffic is desired.
SecurCS is proven to work with the following protocols: Telnet, IBM Websphere MQ, RSC, ODBC, EXPAND over IP, FASTPTCP, CORBA, Pathway iTS, OSM, Webviewpoint, Attunity, SMTP. SecurCS supports the SOCKS protocol enabling it to pass through firewalls on remote systems.
Support for IPv6: SecurCS fully supports securing IPv6 connections, be it in IPv6 only or in Dual (IPv6/IPv4) mode.

Benefits

SecurCS is **transparent to your existing communication environment** and requires no changes to your application.
With its first release being shipped in 2000, SecurCS is the first SSL/TLS implementation for the NonStop platform, making it a **proven solution** being in productive use on more than 100 NonStop sites world-wide.
Because SecurCS uses standard SSL/TLS, it **will interact with any SSL/TLS implementation on partner systems.** For instance, SecurCS can add SSL/TLS capabilities to IBM Websphere MQ version 5.1 running on NonStop systems interfacing with 5.3 implementations on other systems.

Requirements

NonStop System:

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

Partner System:
The SecurCS Remote Proxy component runs on any platform with a Java Virtual Machine for Java 1.7 or later

High flexibility in Telnet environments: comForte provides three different 6530 emulators all coming with built-in SSL/TLS. By using the Remote Proxy component SecurCS will seamlessly interact with your existing Telnet client even if it does not support SSL/TLS.
Small footprint on the NonStop system: SecurCS consists of less than 10 files to install and is easy to configure and manage.

Architecture

On the NonStop platform, SecurCS is running in native mode under the Guardian personality, resulting in optimal performance and full leverage of the NonStop advantages. SecurCS is available for all HPE NonStop platform type systems (S-Series, H/J-Series and L-Series).

On the partner platform, there is a rich set of choices: If you have an SSL/TLS-enabled solution on the partner platform (such as MR-WIN6530 or MQ version 5.3) there is nothing to install. Otherwise, the Remote Proxy component will be running on the partner platform.

SsecurCS will encrypt any protocol which is based on TCP clients connecting to a fixed number of static ports. The TCP/IP client may either reside on the remote platform (such as for Telnet, RSC or ODBC) or on the NonStop platform (such as in FASTPTCP).

SecurCS

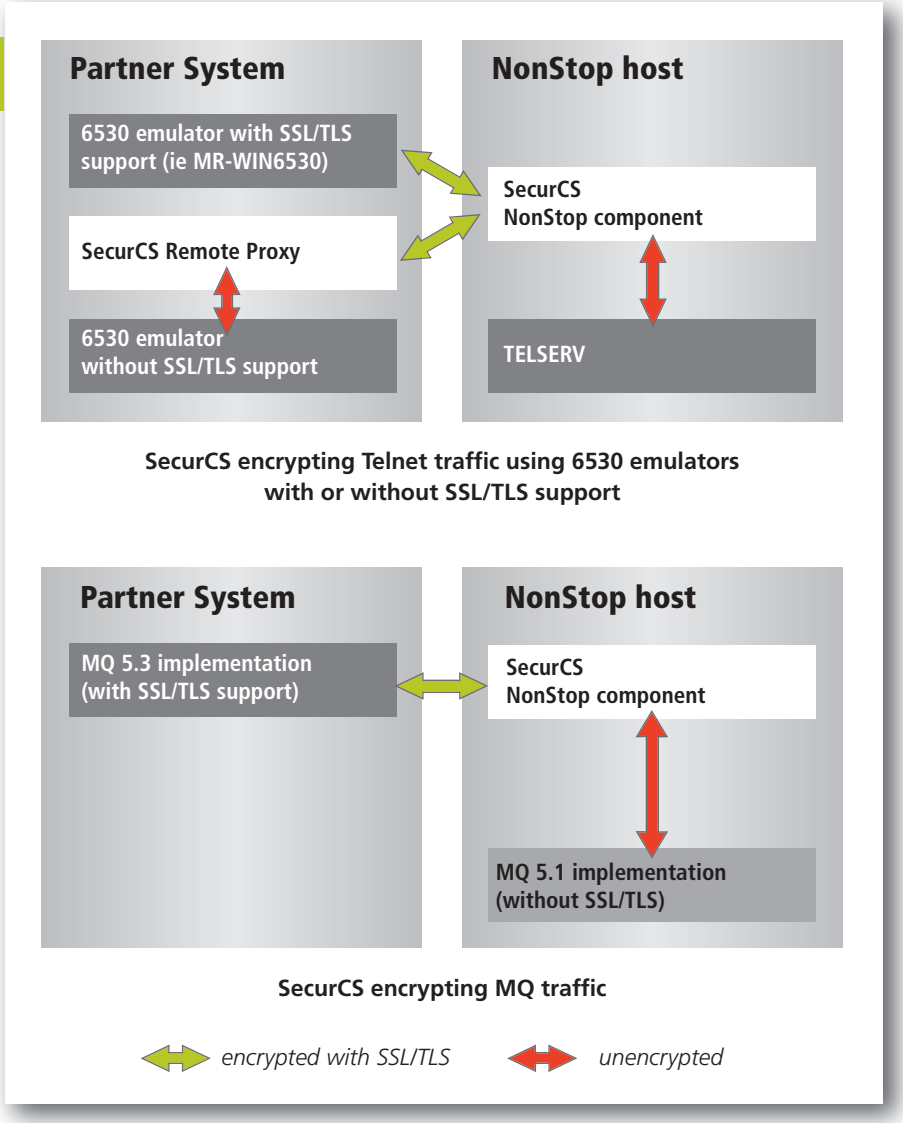
comforte 21 GmbH, Germany
phone +49 (0) 611 93199-00
sales@comforte.com

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 8197 0272
aussales@comforte.com

www.comforte.com



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