Hewlett Packard Enterprise

NonStop cF SSL-LIB and NonStop cF SSL-AT

Easily integrate SSL/TLS into your applications

When was the last time you heard of a real bank robbery in the news? Probably quite some time ago. And how about the last time you heard of a company subject to a data breach? Well–basically data breaches costing companies tens or even hundreds of million dollars are in the news very regularly nowadays.

Financial data, personally identifiable information, personal health information, other confidential data: all kinds of sensitive data is subject to attacks from highly skilled and highly funded attackers trying to gain financial or political advantage. Data has become the new gold.

Introduction

It has become imperative to encrypt all data between communicating peers and accordingly, various security mandates like PCI-DSS, Sarbanes Oxley, and HIPAA enforce the encryption of data in transit.

SSL/TLS[1] is one of the standard protocols for providing this data-in-transit security and on the HPE NonStop, the NonStop SSL product has been available since 2010 for helping SSL/TLS enabling applications.

While in many cases HPE NonStop SSL perfectly addresses the environmental requirements, there are certain restrictions in the product. These limitations show up when running as SSL/TLS clients dealing with a high number of peers, or, when a tighter integration with the application is required. A key example of this need is the regulatory requirement to see the actual originating IP address of a request, instead of the local loopback address as seen with HPE NonStop SSL.

To overcome these limitations, Hewlett Packard Enterprise now offers two optional add-on modules, NonStop cF SSL-LIB and NonStop cF SSL-AT.

[1] SSL and TLS are used to reference both a general technology and specific protocol versions within this technology. To refer to the general technology, both terms are still used and mean the same thing—we use SSL/TLS in this document. However, when referring to the low-level protocol version within the technology itself the terms have different meaning and are used individually.

Note that all SSL protocol versions are outdated as they are no longer considered to be secure.

Purpose

The NonStop cF SSL-LIB and NonStop cF SSL-AT products provide the power of HPE's proven SSL/TLS implementation to the existing TCP/IP (socket) applications in two ways:

- If you have access to the source code of the application and if the application is implemented in native code, NonStop cF SSL-LIB allows you to add SSL/TLS encryption capabilities to the application with just a few lines of code change.
- If you do not have the source code or do not want to change it, NonStop cF SSL-AT (Application Transparent) adds SSL/TLS encryption transparently, i.e., no changes to the application or configuration are required. For example, NonStop cF SSL-AT can encrypt ATM traffic of existing ACI BASE24 installations.

Features and benefits

Proven SSL/TLS technology
The NonStop cF SSL-LIB and NonStop cF SSL-AT products share the SSL/TLS engine with HPE NonStop SSL.

Provides the high level of security your data deserves
NonStop cF SSL-AT and NonStop cF SSL-LIB support the latest version of TLS (TLS 1.2 at the time of this writing) as well as highly secure cipher suites, e.g., using AES256, RSA with up to 8192-bit keys or Elliptic Curve Cryptography (ECC) with SHA-2 Message Authentication Codes (MACs).

Tight integration of SSL/TLS into the application
Unlike a TCP/IP proxy-based solution such as NonStop SSL, both NonStop cF SSL-LIB and NonStop cF SSL-AT grant the applications full access and control to the remote IP address and port number of the connection.

Performance improvement compared to a proxy based solution
Tighter integration into the application results in less processing overhead and thus increased performance. Mileage varies but tests have shown that response times can be twice as fast compared to a TCP/IP proxy-based solution.

Plain data cannot be viewed through PTRACE
With a proxy-based approach, the plain data can be traced via PTRACE on the so-called loopback connection. While this can be avoided by properly securing the NonStop system, it remains a residual risk.

Easy to manage even in highly complex environments
Easy to manage even when running as SSL/TLS client with thousands of peers (e.g., in ATM environments).

Requirements and architecture

NonStop cF SSL-LIB
NonStop cF SSL-LIB is not just another SSL/TLS library but it was created by NonStop developers for NonStop developers in order to provide maximum ease of use. The API provided by NonStop cF SSL-LIB is oriented very closely at the Guardian Socket API. This means that the integration of NonStop cF SSL-LIB into an application is primarily a search and replace, prefixing existing Guardian socket call names with "SSL_". By design as a non-transparent library, the source code of the application parts that perform the socket operations has to be available.

NonStop cF SSL-LIB supports native mode applications written in C, C++, TAL, or COBOL.

NonStop cF SSL-AT
With NonStop cF SSL-AT, an application transparent library is provided. There is no source code change required to the application to be SSL/TLS enabled. NonStop cF SSL-AT only needs to be combined with the application by either binding it in (non-native mode) or specifying it as a user library in the application startup configuration (native mode). To provide this application transparent layer, NonStop cF SSL-AT uses the well-established intercept technology.

NonStop cF SSL-AT will work fully transparently with any object file. However, note that for non-native object files, NonStop cF SSL-AT will need to use a native mode proxy process for handling the cryptographic operations. The performance improvement and protection against PTRACE will not be present as a result.

Technical specifications

HPE NonStop cF SSL-LIB

Platform	Software	HPE Product ID
HPE Integrity NonStop L-Series systems	L15.02 or later	BE407AL
HPE Integrity NonStop J-Series systems	J06.04 or later	QSSLIB

HPE NonStop cF SSL-AT

Platform	Software	HPE Product ID
HPE Integrity NonStop L-Series systems	L15.02 or later	BE406AL
HPE Integrity NonStop J-Series	J06.04 or later	QSSLAT

Learn more at
hpe.com/info/nonstop-security

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-4338ENN, March 2016