



NxSSLSRV

Highlights

Completely concurrent architecture

Support for latest non-patented key exchange and encryption algorithms:

- RSA
- AES/Rijndael
- Diffie-Hellman
- DES
- Triple DES bulk encryption

High Performance Encryption

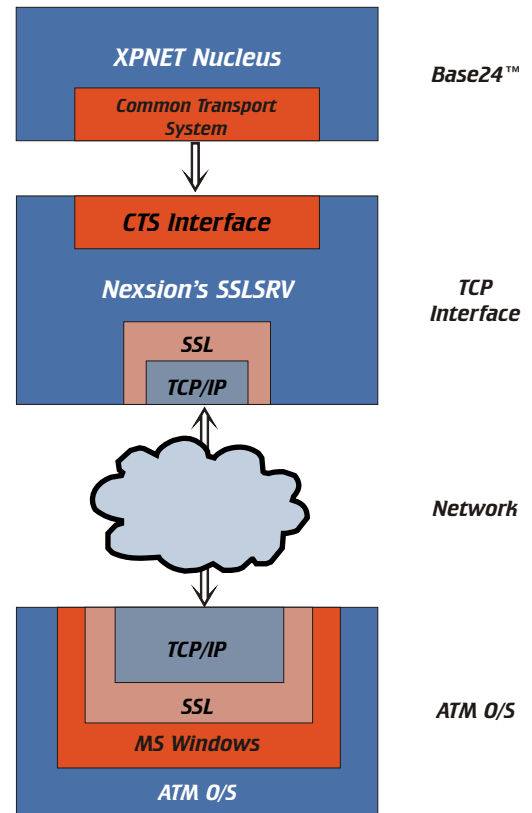
Optimized for HP NonStop instruction set and Guardian Operating System

NxSSLSRV is a plug compatible SSL server process replacement for ACI's BASE24™ TCPSRV process. This allows our customers to protect all of their TCP/IP connections with full SSL (Secure Socket Layer) support without having to change any of their current applications. NxSSLSRV is not a proxy, it runs as a integrated component of XPNET which allows our customers to uniquely identify devices by client IP address and port. NxSSLSRV is fully compatible with most web browsers and Microsoft Windows SSL.

NxSSLSRV offers concurrent secure TCP/IP connectivity between HP NonStop Systems and remote terminals such as ATMs using the well-known SSL/TLS protocol. It runs under the HP NonStop Guardian Platform. NxSSLSRV initiates the following activities:

- Initial requester-initiated session negotiation between requester and process.
- Data transformation from encrypted (requester-side) data to clear toward the Host application ("upward" data flow)
- Encryption of clear data from the Host application toward the requester ("downward" data flow)
- Completely concurrent architecture: each session is its own entity independent of others, with no theoretical limits on the number of supported connections imposed by NxSSLSRV.
- Support for the latest non-patented key exchange and encryption algorithms, including RSA and AES/Rijndael as well as the Diffie-Hellman key exchange and DES and Triple-DES bulk encryption.
- High performance encryption. NxSSLSRV has been optimized for the HP NonStop instruction set and Guardian Operating system.

The Nexsion NxSSLSRV process combines the proven reliability of OpenSSL with our proprietary high performance multi-threaded nucleus. These components combine to provide an exceptionally high performing and reliable product.



Theory of Operation

NxSSLSRV

Performance

NxSSLSRV encryption has been benchmarked on a K1000 (25 MHz R3000) system at 2.08 seconds to establish a session and a steady state of 67 Kb/second for encryption using 3-DES. From these numbers we can estimate the time on a S74000 (300 Mhz R12000) to be 91 milliseconds of processor time for a session establishment and 1.53 Mb/second for processing the 3-DES. This works out to 11 session establishments per processor per second, 7 ATM downloads per processor per second (at 225 Kb per download), or 3000 ATM transactions per processor per second.

<i>Platform</i>	<i>Session Establishment Seconds</i>	<i>Steady State Encryption (3DES)</i>	<i>Sessions Per Second</i>	<i>ATM Loads Per Second (225 Kb)</i>	<i>Transactions Per Second</i>
<i>K1000</i>	<i>2.080</i>	<i>67 Kb/Sec</i>	<i>0.5</i>	<i>0.3</i>	<i>134.</i>
<i>S7400 (est)</i>	<i>.091</i>	<i>1.53 Mb/Sec</i>	<i>11.0</i>	<i>7.0</i>	<i>3060.</i>

OpenSSL is copyright (C) 1995-1998 by Eric Young (eay@cryptsoft.com).

NonStop, Himalaya, ServerNet, and Tandem are registered trademarks of Compaq Computer Corporation.

Microsoft and Microsoft Windows are registered trademarks of Microsoft Corporation.

ACI, BASE24, BASE24-atm, BASE24-pos, BASE24-teller, and NET24-XPNET are trademarks or registered trademarks of ACI Worldwide Inc., Transaction Systems Architects, Inc., or their subsidiaries.