Hifn 7711

Encryption Processor

Compression

- LZS
- MPPC

Encryption

- DES
- Triple-DES
- ARC4*

Authentication

- SHA-1
- MD5

Interoperate with Everything Compress, Encrypt and Authenticate IPSec Data Packets

Supports More Algorithms and Protocols than any Other Chip

Only Hifn™ security processors offer designers on-board ARC4,* LZS and MPPC. Plus, you get DES, 3-DES, SHA and MD5 encryption and authentication algorithms in our 7000 family of products.

IP Compression is a Security Essential

Data compression doubles bandwidth and reduces performance-killing packet fragmentation. The 7711 supports compression within Layer 3 IPSec or Layer 2 PPP. To add built-in PCI support, choose the 7751. Either way, you'll get single-pass compression, encryption and authentication, dramatically reducing demands on the CPU and system bus.

Build Fast VPNs Fast

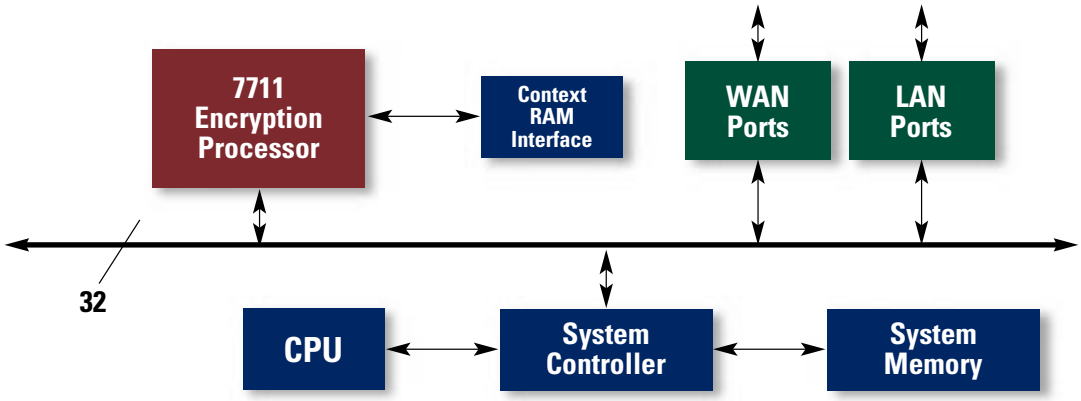
You can program the 7711 to support Layer 3 IPSec and protocols such as Layer 2 PPP compression. The 7711 is perfectly complemented by IPSECure software and our 6500 Public Key Processor. IPSECure is Hifn's software toolkit for VPN developers who need to implement IPSec and IKE in a hurry. Add our blazing fast 6500 Public Key Processor for a truly comprehensive VPN construction kit.

Support Up to 12 T1 Lines With Your VPN Gateway Application

The robust performance of 7711 lets you support up to 12 full duplex T1 lines. Plus, you can maintain separate compression histories and encryption keys for each concurrent session. So you can support both Layer 2 and Layer 3 sessions simultaneously. High-performance compression, encryption and authentication: That's the 7711.

Complete Documentation Suite

The 7711 is ideal for embedded systems, with its dual DMA slave interface and easy programming. For ease of programming, you get a bound Reference Kit, which includes a complete suite of documentation, pocket guide, and reference software. Optionally, you can also buy a Hardware Reference Board.



System Block Diagram

Hifn

Intelligent Secure Networking

Hifn 7711

Enryption Processor

Supports Layer 3 and Layer 2 protocols.

IPSec (Layer 3)

RFC 2401 – IP Security Architecture

RFC 2393 – IP Payload Compression

RFC 2406 – IP Encryption

RFC 2402 – IP Authentication

RFC 2395 – IP Compression/LZS

RFC 2405 – DES-CBC Cipher Algorithm

RFC 2403 – HMAC-MD5

RFC 2404 – HMAC-SHA-1

PPP (Layer 2)

RFC 1962 – Compression Control Protocol

RFC 1967 – PPP LZS-DCP Compression

RFC 1974 – PPP LZS Compression

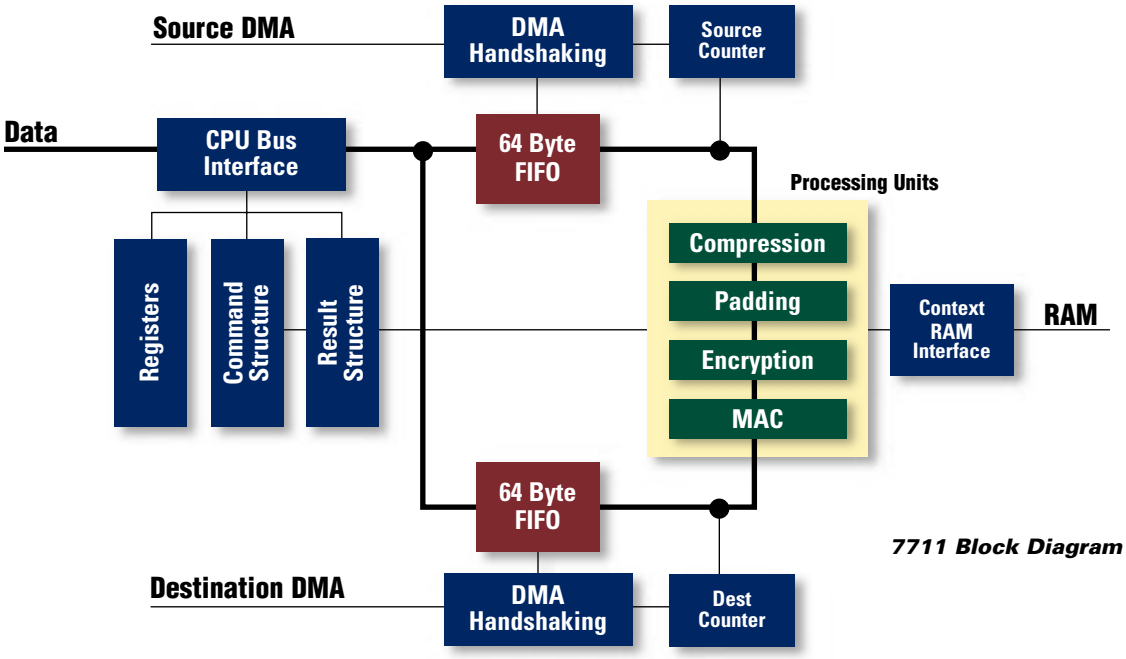
RFC 2118 – Microsoft Point-to-Point Compression (MPPC)

Hifn
Intelligent Secure Networking

750 University Avenue
Los Gatos, CA 95032
408.399.3500 tel
408.399.3501 fax
info@hifn.com
www.hifn.com

Features

- 32 bit, 33MHz DMA slave interface
- DES, Triple-DES, ARC4,* LZS, MPPC, SHA-1, and MD5 algorithms
- 80 Mbps peak 3-DES performance
- Pipelined operations without CPU intervention
- Supports more than 2,000 sessions
- 3.3V operation with 5V tolerant I/O's



7711 Block Diagram

Hifn Product Selection Guide

Encryption Products

Hifn Products	Delivered Mode	PCI	LZS	MPPC	DES 3-DES ARC4*	SHA MD5	RSA DSA
6500	Silicon	■					■
7711	Silicon		■	■	■	■	
7751	Silicon	■	■	■	■	■	
7811	Silicon	■	■	■	■	■	
7851	Silicon	■	■	■	■	■	
7901	Silicon		■	■	■	■	■
7951	Silicon	■	■	■	■	■	■
IPSECure**	Software		■		■	■	■

**IPSECure does not include ARC4*.

Compression Products

Hifn Products	Delivered Mode	PCI	LZS	MPPC	ALDC
9600	Silicon		■		
9602	Silicon				■
9603	Silicon		■		
9610	Silicon		■		
9710	Silicon		■		
9711	Silicon		■	■	
9751	Silicon	■	■	■	
LZS-221	Software		■		
MPPC	Software			■	

Ordering Information

Part Number	Package
7711 PT6	144-pin TQFP
7711 MREF	Reference Design kit

Documentation:
Network Security Data Book
7711 Reference Kit Literature