

electronic design

TechView: **COMMUNICATIONS**

SSL NIC Has A Knack For Instantly Securing Transactions



Louis E. Frenzel

*Communications
/Networking Editor*



lfrenzel@penton.com

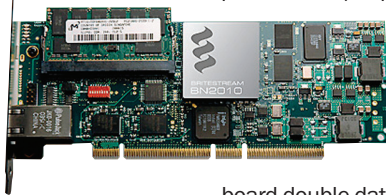
Secure-socket-layer (SSL) software ties up servers and slows transactions. But Britestream Networks' self-contained BN1010 PCI bus network interface card (NIC) can speed things up.

SSL and transport layer security (TLS) are the de facto methods of securing Internet data for e-commerce, online bill payments, and Web services. Recently, SSL also has been replacing IPsec as the security method of choice for virtual private networks (VPNs). Virtually every browser has built-in SSL software. The software is used at the servers, too.

Though this works well, SSL software ties up the processor in the server. It really

delays transactions, especially if many transactions must be processed concurrently. Hardware is the answer, which is where the BN1010 steps in.

The BN1010 operates as a standard 10/100/1000 Ethernet NIC. SSL-encrypted data received at the NIC is decrypted and sent to the host system via the 32/64-bit PCI/PCI-X compatible bus as standard plaintext TCP/IP packets. Designated



plaintext TCP/IP packets received from the host are encrypted and transmitted out of the network as SSL-

secured traffic. The on-board double-data-rate SDRAM memory stores the TCP and SSL state information.

The BN1010 totally offloads all SSL operations, freeing the server CPU to handle the transaction rather than deal with SSL overhead. As a result, the NIC provides up to 10,000 SSL transactions per second (TPS) and can maintain up to 100,000 simultaneous connections. The full duplex throughput is 300 Mbits/s.

At the heart of the NIC is the company's previously announced BN2010 SSL security ASIC. This huge chip incorporates nine ARC processors and massive logic to handle in-stream SSL processing. The internal processors proxy the TCP/IP connections between clients and servers. Also, the chip supports 1-, 2-, and 4-kbit RSA keys. There's on-chip storage of the private keys as well.

The chip includes FIPS-certified (Federal Information Processing Standard) bulk encryption and secure hash algorithms. Extensive FIPS-140 support also is provided. By integrating the TCP and encryption on the same chip, the data is processed directly in the network stream, freeing the server CPU resources. The whole effect is as if a dedicated SSL appliance were connected in front of a Web server farm or networking platform to completely and independently process SSL.

The BN1010 is available now for \$995 in 10,000-unit quantities.

Britestream Networks Inc.

www.bristream.com **ED Online 9218**

Copyright © 2004 by Penton Media, Inc.



BRITESTREAM

Britestream Networks, Inc.
12401 Research Blvd.
Building 2 Suite 275
Austin, TX 78759
Phone: 512-250-2129
Email: info@bristream.com
www.bristream.com