Customize Virtual Private Networks with Spartan-IIE FPGA Solutions

Spartan-IIE FPGA solutions can help you to customize your virtual private network for highest performance, greatest security, and lowest cost.

by Amit Dhir
Manager, Strategic Solutions
Optical/Wired Networks
Xilinx, Inc.
amit.dhir@xilinx.com

The worldwide VPN (virtual private network) market will reach $32 billion by 2003, up from $3 billion in 2000, according to Infonetics Research. VPNs provide highly secure, temporary, point-to-point "tunnels" through the public Internet. These tunnels are created on demand and are removed when a session ends. VPNs offer you the following advantages:

- Lower operating costs
- Extendable networks to respond to changing business demands
- Anywhere, anytime access to e-mail, intranet, and other shared applications.

Essentially, VPNs are private networks deployed over public networks that provide similar levels of privacy, security, quality of service (QoS), reliability, prioritization, end-to-end management, and manageability as local area networks (LANs).

With Spartan™-IIE FPGAs, the right software, and Internet gateways, you get secure data encryption and packet authentication even over the wide-open public Internet.

Furthermore, compared to leased line networks, Xilinx-enabled VPNs are:

- Simpler to set up and easier to administer
- More dynamic and extendable
- Less expensive to create and deploy
- More accessible anywhere, anytime.

How Do VPNs Work?

VPNs use the bandwidth of public, packet-routed networks – typically the Internet or a service provider's backbone network (Internet Protocol, frame relay, or ATM). Corporations have company headquarters, remote offices, mobile workers, independent contractors, and business partners connected to a network service provider's local points of presence (POP). Remote users and the company's LAN(s) connect to the provider's network using dial-up, DSL, cable, ISDN, T1/T3, and wireless.

The key to VPNs is "tunneling" – the practice of repackaging data from one network to another. At the originating end of a tunneled transmission, a data packet is "wrapped" or encapsulated with new header information that allows an intermediary network to reorganize and deliver the packet. At the terminating end, the terminal protocol "wrapper" is removed, and the original packet is delivered to the destination.

Tunneling does not ensure privacy or security – just delivery. To secure a tunneled transmission against interception and tampering, all traffic must be encrypted. Therefore, VPNs must include additional functional features to enhance transmission security, ensure quality of service (QoS), and protect the VPN perimeter with a firewall.

Security and privacy features include tunneling itself, data encryption, packet authentication, firewalls, and user identification. Tunneling uses IPSec (Internet Protocol Security), and encryption uses DES (Data Encryption Standard), Triple DES, and Diffie-Hellman cryptographic algorithms.

VPN QoS and bandwidth management make possible delivery of high transmission quality, mission-critical applications (such as financial reporting and order processing), and real-time voice/video applications (such as distance learning and videoconferencing). Packets are tagged with priority and time sensitivity markers to allow traffic to be routed based on delivery priorities. Tagged packets take precedence over bandwidth-consuming applications (such as Web surfing).

Network management features simplify the addition, deletion, or changing of users; software upgrades; and policy management for security and QoS assurance. These features make scalability and interoperability possible.

Xilinx Spartan-IIE FPGAs – Providing Encryption with Flexibility

VPN gateways secure Internet-based communication, perform user identification, authenticate data integrity and confidentiality, and reject all non-tunneled IPSec traffic. Encryption and authentication lie at the heart of VPN products, and speeding up the processing of encryption algorithms boosts the performance and scale of VPN solutions.

Spartan-IIE FPGAs programmed with proprietary and/or standard encryption cores provide flexibility without compromising cost or performance – and reducing time to market.

Implementing encryption in programmable hardware significantly improves performance over software solutions. By using parallel computing, FPGAs encode and decode larger transmission blocks more effectively. The encrypted key can be changed within the FPGA fabric, and if a key is ever broken, the Xilinx Spartan-IIE solution can be reconfigured instantly with new algorithms.

Spartan-IIE FPGAs give you the power to to choose and optimize just the right feature set and intellectual property cores you need to implement your designs. You can integrate functionality, such as PCI, memory controllers, and other components, within the Spartan-IIE device to customize your product and reduce costs. This flexibility comes at a significantly lower cost compared to ASSPs (application specific standard products).

Conclusion

VPNs improve the productivity of remote workers and hence, their organizations. VPNs promote flexible work styles, extend workplaces beyond office walls, connect remote offices with the headquarters, and foster competitive advantages with strategic partners – all at reduced costs, compared to other options.

Using the Internet and/or service provider backbones to transfer confidential data requires state-of-the-art encryption and privacy solutions. Spartan-IIE FPGA-based encryption and security give you the scalability and flexibility you need to implement the perfect virtual private network for your enterprise.