

# Virtual Private Network



*Businesses can significantly reduce communication costs and maintain security by adopting VPN technology for data transmission*

NetWolves' VPN technology provides a company with the same capability to securely connect separate business locations as private leased lines. NetWolves' VPN offers a wide range of standard features through which companies can reduce equipment costs, network expenses, and service and licensing fees. In addition, this VPN technology can be managed from a central location using NetWolves' Secure Remote Monitoring and Management (SRM<sup>2</sup>)<sup>®</sup> system.

## IPSec VPN

Data privacy is maintained through the use of tunneling protocols and security procedures sending encrypted data over the Internet. By adopting the standard practices of the Internet Engineering Task Force, NetWolves has developed a secure VPN solution using the latest encryption and authentication technologies. NetWolves' IPSec VPN is driven by a customized, fault tolerant UNIX-based operating system.

This VPN complies with IPSec standards so that changes and enhancements can be quickly developed to provide customers with the latest security innovations in response to changing threats and market demands. In addition, NetWolves' VPN technology is interoperable with many other VPN vendors including Cisco and Check Point.

## SSL VPN

NetWolves' SSL VPN enables customers to provide business partners and mobile office workers with convenient and secure access to shared network resources. While IPSec VPN and private line solutions are ideal when a secure site-to-site method of transferring large applications is required, NetWolves' SSL VPN may be a smarter choice to implement for supporting business travelers and partners who require access only to email and small files.

NetWolves' SSL VPN service leverages the power and protection afforded by the Secure Socket Layer protocol, standard with today's popular web browsers, to access vital web-enabled resource applications on a company's protected network, including common email and file-share utilities. With NetWolves' SSL VPN, customers can provide authorized users with a simple key chain USB device and unique login password. The combination of these two security features provides formidable protection against unauthorized use resulting from password theft through such means as key logging or theft of the USB device itself.

*NetWolves' VPN enables changes and enhancements to be made quickly in order to provide customers with the latest security innovations in response to changing threats and market demands. In addition, NetWolves' VPN technology is interoperable with many other VPN vendors including Cisco and Check Point.*

**IPSec provides for access control, connectionless integrity, data origin authentication, encryption, protection from replays and traffic flow confidentiality.**

**Authentication Header & Encapsulated Security Payload provide authentication, integrity and confidential security services.**

**No client software to install on remote PCs, and vital resource applications are easily maintained in a central location.**

**Secure end-to-end authentication and encryption exists from the client PC directly to resource applications.**

**Authentication via SSL proxy ensures that a trusted source is accessing the protected network.**

**Scalable with other NetWolves security services, including ICSA-certified firewall, IPSec VPN, ASURERoute, intrusion detection, congestion management, advanced routing, quality of service, content filtering, and email virus protection.**

**SSL VPN can be monitored and configured from a central location using NetWolves' Secure Remote Monitoring and Management (SRM<sup>2</sup>) system.**

**Call today to learn more about NetWolves' Intelligent Network Solutions.**