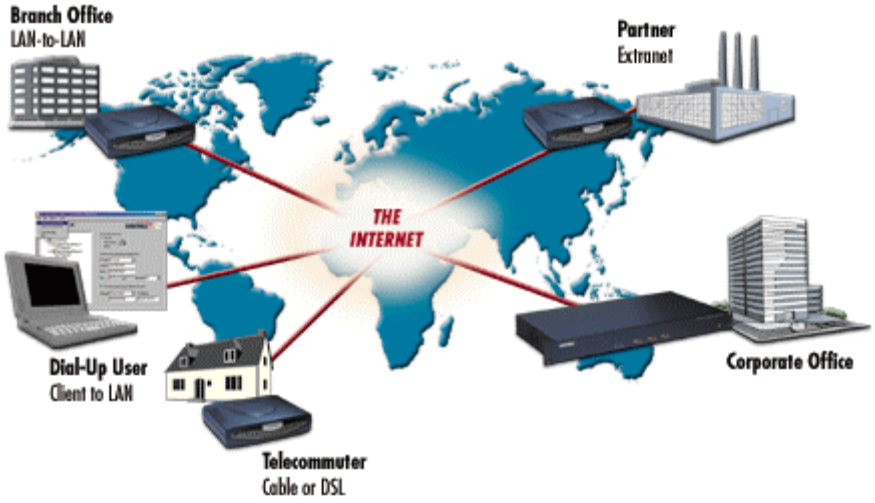
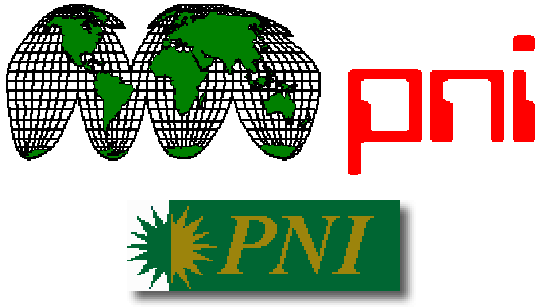
PRODUCTIVITY NETWORK, INC.

Information Technology



VPN Overview



1031 Revere Court
Lombard, IL 60148
Phone 800.828.6826 • Fax 630.495.2427
9051 Park Avenue
Houma, LA 70363
Phone 800.828.6826 • Fax 504.876.0299
http://www.pninc.com
info@pninc.com

Overview

Requirements for setting up a remote access VPN at client hospitals.

This overview describes the use and setup of a Virtual Private Network (VPN) between client networks. A VPN allows users at various remote sites to access a corporate network as though they were physically located at the corporate headquarters and logged into the corporate network. A VPN is unique in that it avoids the high cost of direct dial networks by taking advantage of the public Internet. The availability of relatively low-cost ISDN or Digital Subscriber Line (DSL) technology makes the Internet an attractive communication medium for businesses. Figure 1 shows how branch offices, telecommuters, business partners and

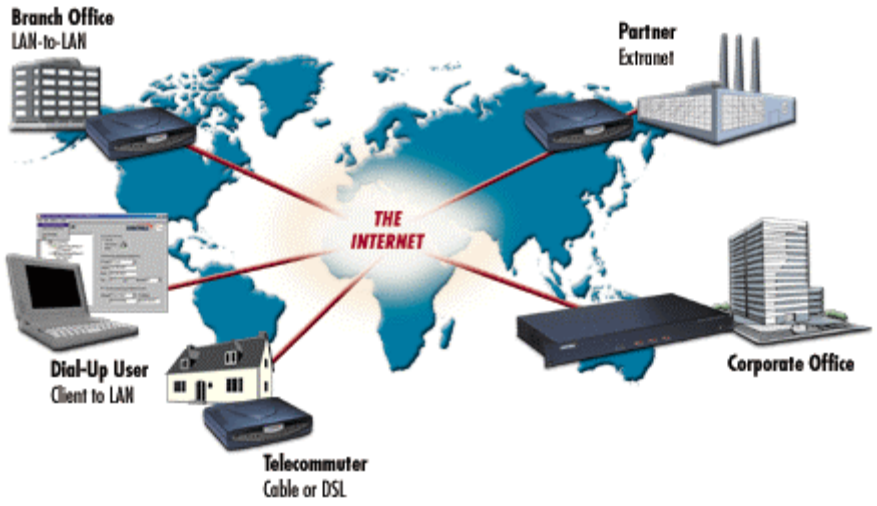


Figure 1: VPN concept using the public Internet.

others can access the corporate network using the public Internet. In this concept, PNI is the business partner accessing the corporate network via the public Internet using a VPN. PNI staff can remotely access the patient accounts as though they were on-site at the corporate hospital.

This approach is not without challenges, however. Since the Internet is a public network, care must be taken to protect sensitive corporate data. Additionally, since the corporate network is exposed to the public Internet, the network itself must be protected from intrusion. Modern Internet firewall technology provides both network protection and data security through VPN access. All SonicWALL Internet appliances are ICSA-certified firewall devices and include VPN capability and strong authentication using digital certificates signed and verified by a third-party. This combination provides the highest level of protection for corporate networks and data.

VPN Definition

What is a Virtual Private Network?

A Virtual Private Network[1] (VPN) moves your private data securely over the public Internet. This allows your business network resources to be available to telecommuters, remote workers, branch offices, consultants, contractors, and partners. Virtual Private Networking uses data encryption and the Internet to provide high-performance, secure communications between sites without incurring the high expense of leased site-to-site data communication lines. VPN isn't new, large enterprises have been using it for years, but thanks to the affordability of broadband, the benefits of Virtual Private Networking are now available to small and medium size enterprises.

A VPN delivers these benefits to your business:

- Allows people to telecommute enables your business to share in their productivity gains. With fewer meetings, less interruptions, and no commute, employee productivity dramatically improves.

- Eliminates the need for maintaining expensive dedicated site-to-site data communication links or multiple telephone lines with modems and paying telephone company usage costs to support dial-up connections to your office network. With a VPN, broadband and dial-up telecommuters, remote workers, and branch offices all use the Internet to connect to your main office network.

Virtual Private Networking (VPN)

Today's business environment requires real-time collaboration among geographically dispersed people and offices. A VPN (Virtual Private Network) is part of your business security package if you plan to allow partners, clients, telecommuters, and remote workers access to your company network resources. A VPN uses data encryption and the Internet to provide high performance, secure communications between sites without incurring the expense of leased site-to-site lines, or modem banks and telephone lines.

A VPN enables your organization to establish secure communications in a manner that is transparent to end-users. A VPN can connect individual telecommuters to the office network, creating a separate, secure tunnel for each connection or connect remote office networks together as a LAN-to-LAN connection over the Internet using a single data tunnel. A VPN enables

[1] This section taken from the SonicWALL white paper *Security Issues and Solutions for Small and Medium Business* and used with permission.

geographically dispersed people and offices to securely link up over the Internet to access business-critical information on the company network.

Internet Protocol Security (IPSec) is a robust standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity, and authentication. Digital certificates add even more security to VPN connections by allowing businesses to authenticate individuals wanting access to confidential company resources. For example, digital certificates can be used to authenticate a remote user before granting access to highly confidential information, such as medical records distributed over a VPN, which connects doctors, insurers and patients.

For More Information

If you are interested in more detailed or technical information about establishing a VPN within your corporate intranet or providing PNI with secure access to your patient accounts, please contact PNI using any of the methods on page 1.