Benefits of Using VPN Technology

Introduction

Virtual Private Networks allow you to use the public Internet to securely connect remote offices and remote employees at a fraction of the cost of dedicated, private telephone lines. There are two major uses for VPNs. The first is to connect two or more geographically separated networks, such as those at a main office and a remote branch office. The second is to allow employees or authorized users to access a network from a remote PC, such as traveling laptop or home computer. Both of these uses permit access to protected network resources by authorized users. Technologic provides solutions geared towards the unique requirements of each.

Components
A virtual private network consists of two main components. One component is a VPN gateway, which has multiple network interfaces and selectively encrypts and decrypts traffic as is flows through. Two gateways can be used to establish a VPN between two remote offices. The other component is a VPN client, which is installed on a PC and selectively encrypts and decrypts traffic to and from a network protected by a VPN gateway. Technologic's Interceptor and InstaGate appliances are both VPN gateways and support third-party VPN clients.

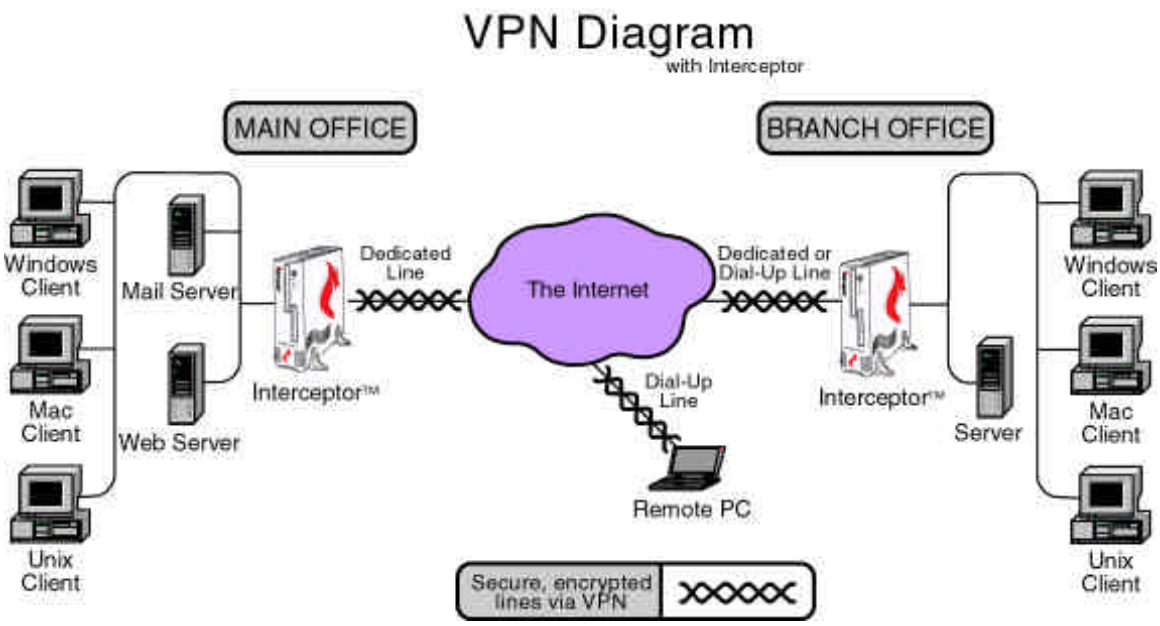
Encryption
Encryption is the process of modifying information so that it can not be read by anyone except the intended recipient. This is done by applying mathematical algorithms that require a "key" to unlock, or decrypt, the original data. Algorithms that use the same key to encrypt and decrypt data are known as "symmetric" encryption algorithms. Common examples include DES and RC4®. Algorithms that use different keys to encrypt and decrypt data are known as "asymmetric" or "public-key" encryption algorithms. Common examples include RSA and Diffie-Hellman. Technologic's products use both symmetric and public-key algorithms to create VPNs.

Authentication & Integrity
In addition to encryption and decryption, a VPN must also verify who's sending the information and ensure that it has not been modified while traveling over the Internet. The process of verifying the sender's identity is known as "authentication". Authentication can be performed with a user name and password, or with a piece of information known as a "digital certificate". A digital certificate contains encryption parameters, which can be used to uniquely identify a user or a host system. Verifying that data has not been modified by an external party is known as "integrity checking". Integrity checking is done by applying a mathematical algorithm, known as a "hash", to data before it's sent and computing the same hash when the data is received. If the two hashes map to the same result, then the data hasn't been modified. Technologic VPNs use authentication and integrity checking to verify the identity and validity of data.

Tunneling
VPNs use a process called "tunneling" to pass encrypted traffic over the Internet. Tunneling is the process of encapsulating a network packet within another one and provides the benefit of hiding the IP addresses of the actual sender and receiver as well as other protocol information (such as whether the packet contains email or web traffic). The packet that travels across the Internet is encrypted and only the IP addresses of the VPN endpoints (gateways or clients) are exposed. Technologic's VPNs also work with clients who are assigned dynamic IP addresses by their Internet provider.

Remote Office VPN

Connect Branch Offices
Virtual Private Networks are ideal for connecting two or more remote office networks together. With a VPN, employees can enjoy the benefits of intranet web sites, email, conferencing, and file sharing between geographically separated networks. Most commonly, this is used to



connect multiple branch offices to a main office and to each other. Traffic from one network is routed to a remote network via normal IP routing, but as it passes through the VPN gateway, it's encrypted and tunneled to the VPN gateway at the remote office. When the remote gateway receives the encrypted packet, it verifies the sender and integrity, then decrypts the packet and forwards the original packet, unmodified, to it's intended recipient. Because the VPN is implemented only between the two gateways, it is completely transparent to all users and applications.

IPSec/SKIP Technologies

Technologic implements Remote Office VPN using a combination of IPSec and SKIP technologies. IPSec stands for IP Security and is a VPN protocol standard being developed by the Internet Engineering Task Force (IETF). It defines the packet formats used to encrypt and authenticate information. SKIP stands for Simple Key Management for Internet Protocols and is an industry standard developed by Sun Microsystems. It is used to negotiate and dynamically change encryption keys for improved security and ease of use. Technologic's SKIP implementation is compatible with other vendors, including Sun Microsystems, Check Point, and TrustWorks.

Configuration

A Remote Office VPN requires two compatible gateway products, one at each network. Each VPN gateway has a unique certificate, which is used to identify it and exchange encryption keys with other gateways. To configure a VPN, each gateway is given information about the other gateway, the remote network, and which encryption algorithms to use. This configuration is all done through Technologic's secure, web-based management interface. After that, the two gateways automatically exchange digital certificates and the VPN is complete. Gateways can support multiple remote networks with different parameters. For example, a VPN to a branch office in the US should be configured to use the strongest encryption available, but a VPN to an overseas office may have to use weaker, exportable encryption.

Access Control

Technologic also offers two choices for access control through a remote office VPN. The first, called an "Untrusted VPN", allows you to pass all VPN traffic through the firewall's proxies to enforce access control, user authentication, and provide logging of transactions. The second choice, called a "Trusted VPN", bypasses the proxies for improved performance and flexibility. Trusted VPNs are appropriate for

branch offices where the users are employees and access control is enforced on servers if necessary. Untrusted VPNs are appropriate for business partners or consultants who need limited access to internal resources. Interceptor and InstaGate both support simultaneous combinations of Trusted and Untrusted VPNs.

Remote User VPN

Connect Remote Users
A Virtual Private Network can allow remote users to access the company LAN through any Internet Service Provider (ISP). Once connected to an ISP, the user initiates a VPN link to the gateway and from then on, all office traffic is routed through the VPN. Like the Remote Office VPN, a tunnel is created to hide the traffic, but with remote user VPN, the tunnel exists at a lower network layer. This is done by having the gateway assign a unique IP address to the client for use on the office network. VPN traffic between the client and the gateway will use the gateway's public address and the dynamic address assigned by the user's ISP. Once the traffic is decrypted by the gateway, it will use the client address that was assigned by the gateway to communicate with internal servers.

PPTP
Technologic implements Remote User VPN using Microsoft's Point to Point Tunneling Protocol (PPTP). Support for PPTP is integrated into Microsoft's Dial-Up Networking in Windows 95, 98, and NT. This means that you do not have to purchase and install third-party VPN client software for remote users. The software is bundled with Windows 98 and NT and can be downloaded free of charge for Windows 95 with the Dial-Up Networking Upgrade 1.3. Third party PPTP client software is also available for Mac OS.

Easy Configuration
Configuring Remote User VPN involves allocating a range of client IP addresses and creating user accounts on the gateway. A client IP address is assigned to a client when it connects and is returned to the pool when the session has ended. Accounts are created by setting a username and password for each user. Users can also be assigned to groups and PPTP access can be provided at the user or group level.

On the user's system, a new Dial-Up Networking entry is created with the public IP address of the gateway. To connect, the user selects the Dial-Up Networking entry and is prompted for a username and password. Windows then connects to the gateway and is assigned a new IP address on the LAN and is also provided with the address of the DNS server. The user can also set the IP address of the WINS server on the LAN, to allow network browsing and logging on to NT domain controllers.

Interoperability
As an alternative to PPTP, remote users can also use IPSec/SKIP for remote access. This requires Technologic's Remote Office VPN feature and a third party IPSec/SKIP client. Technologic has tested interoperability with clients from Sun Microsystems and TrustWorks.

Frequently Asked Questions

What VPN standards does Technologic support?
IPSec/SKIP for Remote Office VPN
PPTP and IPSec/SKIP for Remote User VPN

Does Technologic's VPN support private (non-routable) IP addresses?
Yes, both SKIP and PPTP technology use tunneling, so private IP addresses are hidden.

Does Technologic's VPN support dynamically assigned IP addresses?
Yes, both Remote Office and Remote User VPN support dynamically assigned client addresses.

What operating systems are supported by Remote Office VPN?
PPTP clients exist for Windows 95, 98, NT, and Mac OS.

Does Remote Office VPN support Microsoft Networking features like browsing, file sharing, and NT domain logons?
Yes, PPTP is integrated into Microsoft Networking to support these features.

Where can I get more information about the SKIP protocol?
http://skip.incog.com/ *and* http://www.sun.com/security/skip/

Where can I get more information about the PPTP protocol?
http://www.microsoft.com/ntserver/zipdocs/understanding_pptp.exe

What is the maximum number of users that Technologic's VPN can support?
Remote Office VPN has no limit on the number of VPN links or users.
Remote User VPN can support up to 256 simultaneous clients.

What encryption algorithms are supported by Technologic's VPN?
Remote Office VPN supports DES, Triple-DES, 40-bit RC2, 40-bit RC4 and 128-bit Safer.
Remote User VPN supports 40 and 128-bit RC4.

Is Technologic's VPN transparent to my users and applications?
Yes, Remote Office and Remote User VPNs are transparent to users and applications.