

VPN Technology

Oct 2000

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 of VPNs -

First is to connect two or more geographically separated networks, such as those at main office and a remote branch office.

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 above these uses permit access to protected network resources by authorized users. SecureNet solutions are geared towards the unique requirements of each. According to industry analyst Forrester Research Inc., when comparing the traditional cost of Remote Access Server (RAS) versus today Internet-based VPN, the cost difference for example 1000 users are significant.

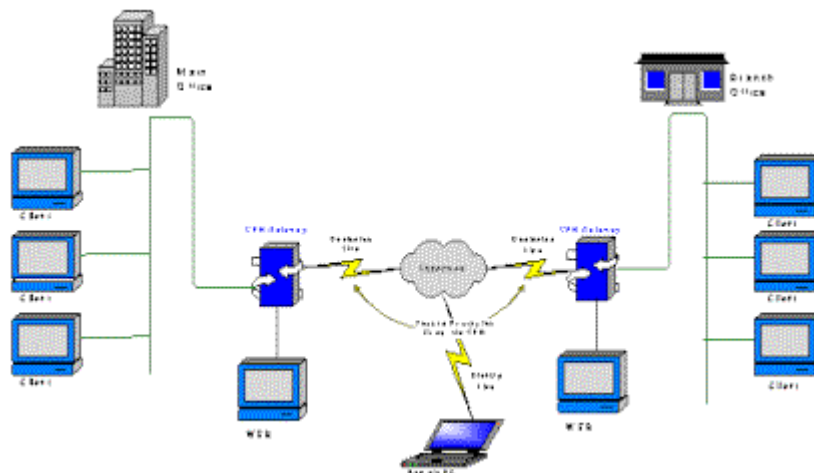
	Traditional RAS Cost	VPN Costs
Phone/ISP Charges	\$1.08M	\$0.54M
User Support	\$0.30M	\$0.00 (included in user access costs)
Capital Expenses	\$0.10M	\$0.02M
T1 Lines	\$0.02M	\$0.03M
Total	\$1.50M	\$0.59M
(Costs Per 1000 Users)		

Implementation

VPN implementations can be grouped into two Primary categories.

Remote Office VPNs between internal corporate departments, branch offices, strategic partners, customers.

Remote Access VPNs used by remote or mobile employees



Remote Office VPNs facilitates secure communications between a company's internal departments and its branch offices, strategic partners, customers. 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 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 its intended recipient.

Remote Access VPNs can allow remote users to access the company LAN through any Internet Service provider (ISP). Once connected to an ISP, user initiates a VPN link to the gateway and from then on, all office traffic is routed through the VPN.

Components

A VPN consists of two main components. One component is a VPN gateway, which has multiple network interfaces and selectively encrypts and decrypts traffic as it 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.

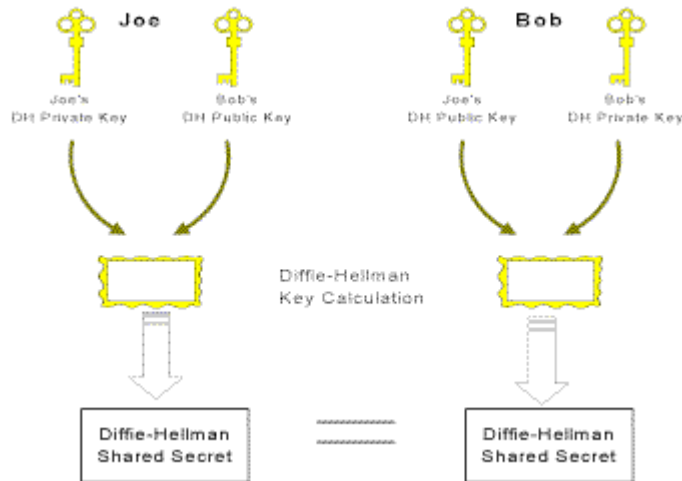
Encryption

A key component of a VPN solution is providing data privacy. Data transmitted in clear text can be viewed or even stolen through common "sniffing techniques. To ensure data privacy and to protect valuable data transmitted over unsecured channels, encryption techniques are used to encrypt or scramble clear text in cipher text. Applying mathematical algorithms, which require a key to unlock or decrypt the original data, does the encryption. Algorithms that use the same key to encrypt and decrypt data are known as "symmetric" or "private-key" encryption algorithms. Common examples include DES, 3DES, RC4.

Algorithms that use different keys to encrypt and decrypt data are known as "asymmetric" or "public-key". Common examples include Diffie-Hellman (DH), Rivest Shamir Adleman (RSA).



Private key (Symmetric) Cryptosystem



Diffie-Hellman Public Key Cryptosystem

Authentication

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 in a variety of methods like user name/password, RADIUS, or TACACS/TACACS+ servers, LDAP-compliant directory servers, X.509 digital certificate and two factor schemes such as those involving hardware tokens and smart cards.

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.

Introduction to IPSec

In 1994, the Internet Architecture Board (IAB) issued a report on "Security in the Internet Architecture" (RFC 1636). The report stated the general consensus that the Internet needs more and better security, and it identified key areas for security mechanisms. Among those were the need to secure the network infrastructure from unauthorized monitoring and control of network traffic as well as the need to secure end-to-end-user traffic using authentication and encryption.

The accepted standard for Internet-based VPNs is the Internet Protocol Security (IPSec) standard. IPSec defines the format of an encrypted and authenticated IP packet, and is required for the next generation of IP communications. To automate the management of encryption keys, IPSec is often used with the Internet Key Exchange (IKE).

Once standards-based interoperability has been established, the extranet VPN must be implemented such that external partners are granted access only to the specific resources they need, such as particular application servers. Here again is an example of the importance of integrating the enterprise VPN into your overall enterprise security policy, providing fine grained access control so that extranet partners only access authorized network resources. As you open your corporate network to increasing numbers of external users, you'll need to ensure that your company's resources are protected by a comprehensive, robust, policy-based enterprise security solution.

IPSec Functions

IPSec provides three main facilities: an authentication-only function referred to as an Authentication Header (AH), a combined authentication/encryption function called Encapsulating Security Payload (ESP) and a key-exchange function.

For VPNs, both authentication and encryption are generally desired because it is important to assure that unauthorized users cannot penetrate the VPN, and to assure that eavesdroppers on the Internet cannot read messages sent over the VPN. Most implementations are likely to use ESP rather than AH; the key-exchange function allows for either the manual or automated exchange of keys.

The current specification requires that IPSec support the Data Encryption Standard (DES) for encryption, but a variety of other encryption algorithms may also be used. Because of concern about the strength of DES, it is likely that other algorithms, such as Triple-DES, will be widely used possibly as early as this year and certainly by some time in 1999. For authentication, a relatively new scheme known as HMAC (MAC stands for message authentication code) is required.

IPSec and VPNs

The driving force for the acceptance and deployment of secure IP is the need for business and government users to connect their private WAN/LAN infrastructures to the Internet for access to Internet services and then use it as a component of the WAN transport system. Users need to isolate their networks and, at the same time,

send and receive traffic over the Internet. The authentication and privacy mechanisms of secure IP provide the basis for this.

Because IP-Security mechanisms have been defined independently of their use with either the current IP or IPv6, their deployment does not depend on the deployment of IPv6. Indeed, it is likely that we will see widespread use of secure IP features long before IPv6 becomes popular because the need for IP-level security is greater than the need for the added functions that IPv6 provides as compared to the current IP.

With the arrival of IPSec, managers have a standardized means of implementing security for VPNs. Furthermore, all of the encryption and authentication algorithms and security protocols used in IPSec are well-studied and have survived years of scrutiny. As a result, the user can be confident that the IPSec facility indeed provides strong security.