Technology Security for Corporate Office

VIRTUAL PRIVATE NETWORK (VPN) SECURITY OVERVIEW & CREATION OF PUBLIC-KEY INFRASTRUCTURE (PKI) CERTIFICATE

BY

DR. ENGR BABA J ADAMU
May 2004

Table of Contents

1 BUSINESS REQUIREMENTS

As a business grows, it might expand to multiple shops or offices across the country and around the world. To keep things running efficiently, the people working in those locations need a fast, secure and reliable way to share information across computer networks. In addition, traveling employees like salespeople need an equally secure and reliable way to connect to their business's computer network from remote locations. The requirement is to provide Corporate Users secure access to corporate network over Internet, which is very secure. One popular technology to accomplish these goals is a **VPN (**virtual private network**).**

2 INTRODUCTIONS TO VPN

Virtual Private Networks (VPNs) supply network connectivity over a possibly long physical distance. In this respect, VPNs are a form of Wide Area Network (WAN). The key feature of a VPN, however, is its ability to use public networks like the Internet rather than rely on private leased lines to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site or employee. By using a VPN, businesses ensure security -- anyone intercepting the encrypted data can't read it. VPN technologies implement restricted-access networks that use the same cabling and routers as does a public network, and they do so without sacrificing features or basic security.

VPNs support at least three different modes of use:

- Remote access client connections
- LAN-to-LAN internetworking
- Controlled access within an intranet

VPNs do not offer any network services that aren't already offered through alternative mechanisms. However, a VPN does use a unique mix of technologies that promises to improve on the traditional approaches.

Traditionally an organization that wanted to build a wide-area network needed to procure expensive, dedicated lines to connect their offices together. Only large companies could afford to purchase these lines outright, so most organizations "leased" their lines and paid a monthly charge -- sometimes thousands of dollars -- for the privilege of using cables that no one else could tap into. Leased lines, such as ISDN (integrated services digital network, 128 Kbps), are private network connections that a telecommunications company could lease to its customers.

An organization typically installs a leased-line WAN to support a long-distance intranet. Though leased lines are reliable and secure, the leases are expensive, with costs rising as the distance between offices increases. Besides file sharing and email, these WANs

provide access to intranet Web sites and videoconferencing systems. In addition, some organizations selectively open their WAN access to partners to provide extranet services. Today, the Internet is more accessible than ever before, and Internet service providers (ISPs) continue to develop faster and more reliable services at lower costs than leased lines. To take advantage of this, most businesses have replaced leased lines with new technologies that use Internet connections without sacrificing performance and security, the VPNs. Businesses started by establishing **intranets**, which are private internal networks designed for use only by company employees. Intranets enabled distant colleagues to work together through technologies such as desktop sharing. By adding a VPN, a business can extend all its intranet's resources to employees working from remote offices or their homes.

3 TECHNOLOGIES BEHIND VPN'S

A VPN can grow to accommodate more users and different locations much more easily than a leased line. In fact, scalability is a major advantage that VPNs have over leased lines. Moreover, the distance doesn't matter, because VPNs can easily connect multiple geographic locations worldwide. Several network protocols have become popular as a result of VPN developments:

- PPTP
- L2TP
- IPsec
- SOCKS

These protocols emphasize *authentication* and *encryption* in VPNs. Authentication allows VPN clients and servers to correctly establish the identity of people on the network. Encryption allows potentially sensitive data to be hidden from the general public. Many vendors have developed VPN hardware and/or software products. Unfortunately, immature VPN standards mean that some of these products remain incompatible with each other.

4 VPN'S FOR REMOTE ACCESS

A VPN can support the same intranet/extranet services as a traditional WAN, but VPNs have also grown in popularity for their ability to support *remote access service*. In recent years, many organizations have increased the mobility of their workers by allowing more employees to telecommute. Employees also continue to travel and face an increasing need to stay "plugged in" to the company network. Leased lines don't support mobile workers well because the lines fail to extend to people's homes or their travel destinations. Companies that don't use VPNs must resort to implementing specialized "secure dial-up" services in this case. To log in to a dial-up intranet, a remote worker must call into a company's remote access server using either a 1-800 number or a local number. The overhead of maintaining such a system internally, coupled with the possibility of high long distance charges incurred by travelers, make VPNs an appealing option here.

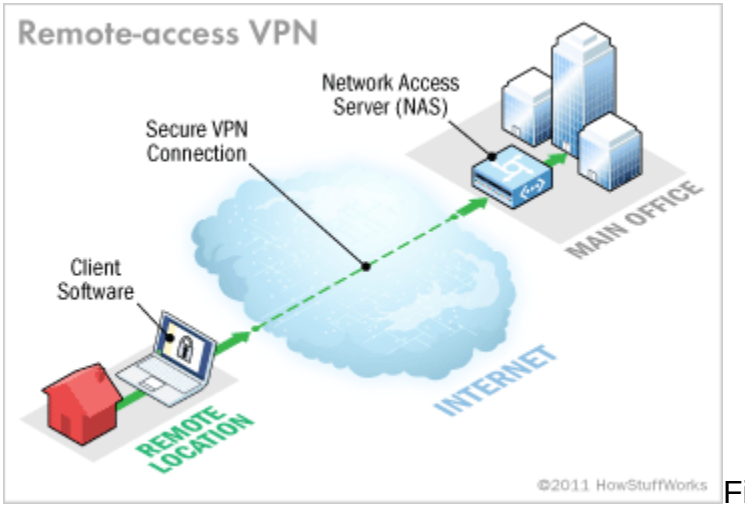

Fig. 1

As shown in Fig. 1, a remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the Internet.

A site-to-site VPN connection lets branch offices use the Internet as a conduit for accessing the main office's intranet (Fig.2)

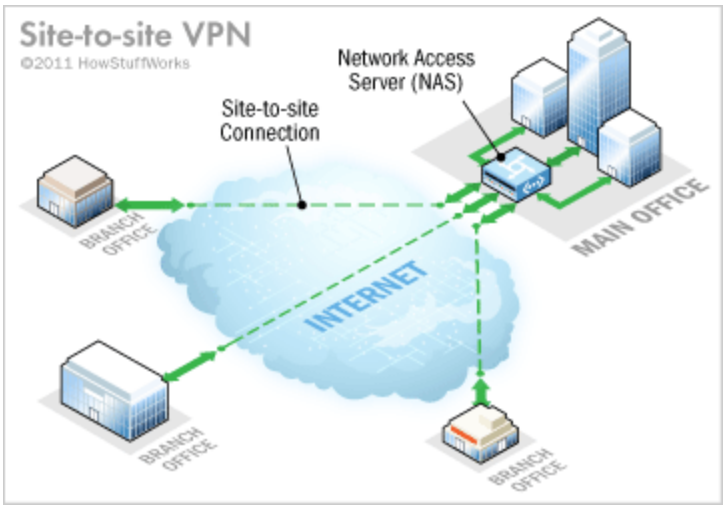

Fig. 2

Figure 3 below shows a VPN Remote Access Architecture. In a remote- access VPN, tunneling typically relies on **Point-to-point Protocol** (**PPP**) which is part of the native protocols used by the Internet. More accurately, though, remote-access VPNs use one of three protocols based on PPP:

- L2F (Layer 2 Forwarding) -- Developed by Cisco; uses any authentication scheme supported by PPP
- PPTP (Point-to-point Tunneling Protocol) -- Supports 40-bit and 128-bit encryption and any authentication scheme supported by PPP
- L2TP (Layer 2 Tunneling Protocol) -- Combines features of PPTP and L2F and fully supports IPSec; also applicable in site-to-site VPNs

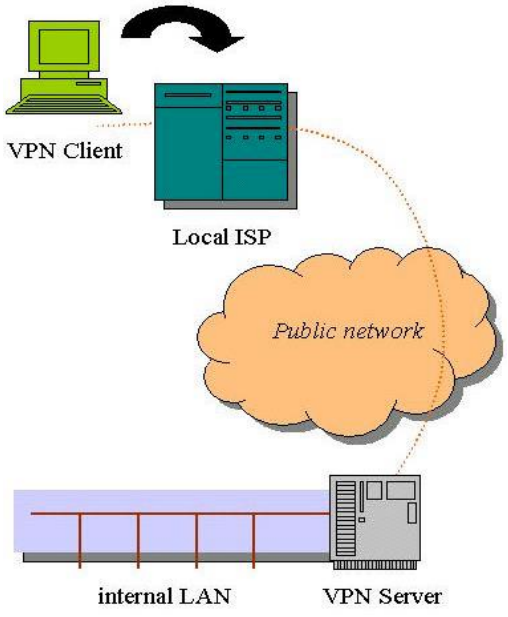

Fig. 3

5 ADVANTAGES OF VPN

VPNs promise two main advantages over competing approaches -- cost savings, and scalability (that is really just a different form of cost savings).

6 THE LOW COST OF A VPN

One way a VPN lowers costs is by eliminating the need for expensive long-distance leased lines. With VPNs, an organization needs only a relatively short dedicated connection to the service provider. This connection could be a local leased line (much less expensive than a long-distance one), or it could be a local broadband connection such as DSL service. Another way VPNs reduce costs is by lessening the need for long-distance telephone charges for remote access. Recall that to provide remote access service, VPN clients' needs only call into the nearest service provider's access point. In some cases this may require a long distance call, but in many cases a local call will suffice. A third, subtler way that VPNs may lower costs is through offloading of the support burden. With VPNs, the service provider rather than the organization must support dialup access for example. Service providers can in theory charge much less for their support than it costs a company internally because the public provider's cost is shared amongst potentially thousands of customers.

7 SCALABILITY AND VPNS

The cost to an organization of traditional leased lines may be reasonable at first but can increase exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations. If a third branch office needs to come online, just two additional lines will be required to directly connect that location to the other two. However, as an organization grows and more companies must be added to the network, the number of leased lines required increases dramatically. Four branch offices require six lines for full connectivity; five offices require ten lines, and so on. Mathematicians call this phenomenon a *combinatorial explosion*, and in a traditional WAN this explosion limits the flexibility for growth. VPNs that utilize the Internet avoid this problem by simply tapping into the geographically distributed access already available.

7a Keeping VPN Traffic in the Tunnel

Most VPNs rely on tunneling to create a private network that reaches across the Internet. Tunneling is the process of placing an entire packet within another packet before it's transported over the Internet. That outer packet protects the contents from public view and ensures that the packet moves within a virtual tunnel.

This layering of packets is called **encapsulation**. Computers or other network devices at both ends of the tunnel, called **tunnel interfaces**, can encapsulate outgoing packets and reopen incoming packets. Users (at one end of the tunnel) and IT personnel (at one or both ends of the tunnel) configure the tunnel interfaces they're responsible for to use a tunneling protocol. Also called an encapsulation protocol, a tunneling protocol is a standardized way to encapsulate packets [source: Microsoft].

The purpose of the tunneling protocol is to add a layer of security that protects each packet on its journey over the Internet. The packet is traveling with the same transport protocol it would have used without the tunnel; this protocol defines how each computer sends and receives data over its ISP. Each inner packet still maintains the passenger protocol, such as Internet protocol (IP) or AppleTalk, which defines how it travels on the LANs at each end of the tunnel. The tunneling protocol used for encapsulation adds a layer of security to protect the packet on its journey over the Internet.

To better understand the relationships between protocols, think of tunneling as having a computer delivered to you by a shipping company. The vendor who is sending you the computer packs the computer (passenger protocol) in a box (tunneling protocol). Shippers then place that box on a shipping truck (transport protocol) at the vendor's warehouse (one tunnel interface). The truck (transport protocol) travels over the highways (Internet) to your home (the other tunnel interface) and delivers the computer. You open the box (tunneling protocol) and remove the computer (passenger protocol).

 Fig 4.

A large corporation might deploy its VPN alongside other network equipment at a co-location facility or data center like the one shown in Figure 4. Source - ©iStockphoto.com/senticus

8 PUBLIC-KEY INFRASTRUCTURE (PKI) - Encryption and Security Protocols in a VPN

Encryption is the process of encoding data so that only a computer with the right decoder will be able to read and use it. You could use encryption to protect files on your computer or e-mails you send to friends or colleagues. An encryption key tells the computer what computations to perform on data in order to encrypt or decrypt it. The most common forms of encryption are symmetric-key encryption or public-key encryption:

- In **symmetric-key encryption**, all computers (or users) share the same key used to both encrypt and decrypt a message.
- In **public-key encryption**, each computer (or user) has a public-private key pair. One computer uses its private key to encrypt a message, and another computer uses the corresponding public key to decrypt that message.

Public-Key infrastructure (PKI) is the integration of software, hardware, encryption technologies and services for managing public keys. PKI provides for the four basic requirements of a secure system:

- Confidentiality to keep information private.
- Integrity to prove that information has not been changed.
- Authentication to prove the identity of the sender.
- Non-repudiation, which ensures that the information originator cannot deny
- Ownership.

How these requirements are achieved?

- Cryptography allows data to be transmitted across a vast public network such as the Internet while preserving the confidentiality of its contents.
- Integrity is ensured because only data that has not been tampered with can be decrypted.
- The trusted Certificate Authority (CA) that validates the identity of the recipient's public key preserves authenticity.
- Ownership of the data cannot be repudiated once it has been signed by the sender's public key.

There are two basic operations common to all PKI's, certification and validation. Certification is the process of binding a public-key value to an individual, organization or other entity or even to some other piece of information such as a permission or credential. Validation is the process of verifying that a certificate is still valid.

Cryptography is the essential building block of PKI. There are two forms of Cryptography that are currently in use:

- Private Key Cryptography, also known as Symmetric Encryption
- Public Key Cryptography, also known as Asymmetric Encryption

In Private Key Cryptography both the receiving and sending parties use the same key to encrypt and decrypt data. Whereas in Public Key Cryptography there are separate keys for encryption and decryption of data, these keys are mathematically related and cannot derive from one another. We will be using Public Key Cryptography for the deployment of this VPN.

9 CREATION OF PUBLIC-KEY CERTIFICATE

A public-key certificate has a special data structure and digitally signed by an authority called Certificate Authority (CA). A public-key certificate binds a public key to a user who holds the corresponding private-key so that other entities could trust subject's public-key. Public-key certificate can be used during some period of time specified in a certificate's 'validity' filed. But, for some reasons, the CA can revoke the certificate before the certificate expires. If an authority revokes a public-key certificate, users need to be able to know that revocation has occurred so they no longer use the revoked certificate. A system using a public-key certificate needs to validate a certificate prior to using that certificate for an application.

10 AUTHENTICATION USING DIGITAL CERTIFICATES

For authentication using digital certificates, there must be at least one identity certificate (and its root certificate) on a given VPN Device.

11 VPN'S AND PKI

Security offered by VPN solutions can be enhanced by integration with PKI (Public Key Infrastructure) which enforces stronger authentication, non-repudiation, and scalability. Additionally, PKI-based VPN systems can draw on the flexibility of digital certificates to establish trusted internal communications within the enterprise as well as trusted extranet connectivity among customers, suppliers, and business partners.

12 INTERNET PROTOCOL SECURITY (IPSEC)

Internet Protocol Security Standard (IPsec) is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution, or it can use simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (layer three) in OSI. IPsec extends standard IP for the purpose of supporting more secure Internet-based services (including, but not limited to, VPNs). IPsec specifically protects against "man in the middle attacks" by hiding IP addresses that would otherwise appear on the wire.

13 IPSEC AND DIGITAL CERTIFICATES

Internet Protocol Security Standard (IPSec) secures private communications on the Internet at the network level between firewalls, routers, and remote access devices. IPSec authenticates the identities of communicating parties, protects data from alteration, and safeguards information from interception using confidentiality services. IPSec is transparent to intermediary network layer devices because it is based on standard IP traffic. The Internet Key Exchange (IKE), part of the information transmission process, authenticates each side of an IPSec transaction and creates a secure path for encrypted data packets to travel to their destination on the network. In order for identity authentication to take place, every VPN device requires a unique identifier like a digital certificate. For example, the digital certificates issued by VeriSign comply with the IPSec standard.

14 VPN SOLUTION PROPOSED

After evaluating VPN solutions from various vendors iNetworks has chosen a VPN Solution from Cisco. This solution uses IPsec with Digital Certificates. This is the process every user requiring a VPN will have to follow:

1. The user downloads and installs the Cisco VPN client software and completes the certificate request form.
2. The administrator receives an email that Kaminski has requested a certificate.
3. The administrator connects securely to the On-Site Control Center and approves or rejects the certificate. If the certificate is approved, On-Site will send an email telling the user to pick up his certificate.
4. The user picks up their certificate with their browser.
5. The user can now securely connect to the corporate network from anywhere on the Internet.
6. When the user tries to authenticate with Cisco VPN Appliance, the Cisco VPN Appliance will compare the certificate against the current Certificate

Revocation List (CRL). If the cert is not on the CRL and the user is on the valid access control list, then a secure connection is created.

We have looked at the types of VPNs and the components and protocols that they use. Over time, people have developed new and better technologies to use in networks, which improves the features of existing VPNs. VPN-specific technologies, though, such as tunneling protocols, haven't changed much in that time, perhaps because current VPNs do such a good job at to keep businesses connected around the world.