VIRTUAL PRIVATE NETWORK

NEED FOR VPN???

Remote and branch office connectivity has been a staple of most IT managers for many years. Prior to VPN and other existing technologies, a company that needed to connect a branch location to their "corporate network" needed to lease a circuit from a telecommunications carrier. These lines vary in speed from 9600 bits per second to well above 1.5 million bits per second. These lines are expensive, and the longer the distance between sites the more expensive the line is. The answer to this problem is the costs of using traditional remote access technology is skyrocketing and will only get higher as more users and sites need to be connected.

The cost of ownership of dedicated remote access connectivity is divided into the following heads:

- **Equipment costs**: are only about 15 percent to 20 percent of the total cost of ownership when connecting users and sites. Equipments involved in tradional access are very complex and includes devices such as remote-access servers, access routers and WAN switches--that are to be installed, maintained and managed.

- **Recurring telecommunications costs and the operational costs:** to support the users and manage the equipment for a period of three- to five-year period

- **High management costs:** For supporting users. Each type of equipment requires a different set of management skills, which adds to the total cost of ownership.

- **Hidden Cost:** Companies also often have additional hidden costs when supporting large numbers of sites or users.

VPN has greatly reduce costs associated with Traditional remote access

VPN????????

A Virtual Private Network (VPN) connects the components of two networks together over another network. VPNs accomplish this by allowing the users to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in a private network. VPNs allow users working at home, a branch office or on the road to connect in a secure fashion to a remote corporate network or host computer using the routing infrastructure provided by a public Internet. From the end user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate Internet is irrelevant to the user because it appears as if the data is being sent over a dedicated private link. VPN technology also allows a corporation to connect to branch offices or to other companies over a public Internet, while maintaining secure communications. The VPN connection across the Internet logically operates as a Wide Area Network (WAN) link between the sites. In other words VPNs turn the Internet into a simulated private WAN. The secure connection across the Internet appears to the user as a private network connection—despite the fact that this connection occurs over a public Internet - hence the name **Virtual Private Network**.

A simpler definition of VPN could be:

"Virtual private network is defined as customer connectivity deployed on a shared infrastructure with the same policies as a private network. The shared infrastructure can be a service provider's IP, Frame Relay, or ATM backbone, or the Internet "

HOW IT WORKS????

OBSTACLES OVERCOME BY VPN!!!

- **Can handle non-IP traffic:** networks often communicate using a variety of protocols, such as IPX and NetBEUI, but the Internet can only handle IP traffic.
- **Non -Encrypted transmission of traffic:** data packets traveling the Internet are transported in clear text. Consequently, anyone who can see Internet traffic can also read the data contained in the packets. This is clearly a problem if companies want to use the Internet to pass important, confidential business information.

VPNs overcome these obstacles by using a strategy called tunneling. Instead of packets crossing the Internet out in the open, data packets are first encrypted for security, and then encapsulated in an IP package by the VPN and tunneled through the Internet.

To illustrate the concept, let's say you're running NetWare on a network, and a client on that network wants to connect to a remote NetWare server.

The primary protocol used with traditional NetWare is IPX. So, to use a generic layer-2 VPN model, IPX packets bound for the remote network reach a tunnel initiating device - perhaps a remote access device, a router, or even a desktop PC, in the case of remote-client-to-server connections - which prepares them for transmission over the Internet.

The VPN tunnel initiator on the source network communicates with a VPN tunnel terminator on the destination network. The two agree upon an encryption scheme, and the tunnel initiator encrypts the packet for security. (For better security, there should be an authentication process to ensure that the connecting user has the proper rights to enter the destination network. Most currently available VPN products support multiple forms of authentication). Finally, the VPN initiator encapsulates the entire encrypted package in an IP packet. Now, regardless of the type of protocol originally being transmitted, it can travel the IP-only Internet. And, because the packet is encrypted, no one can read the original data.

On the destination end, the VPN tunnel terminator receives the packet and removes the IP information. It then decrypts the packet according to the agreed upon encryption scheme, and sends the resulting packet to the remote access server or local router, which passes the hidden IPX packet to the network for delivery to the appropriate destination.

VPN CORE TECHNOLOGY OVERVIEW

AUTHENTICATION SYSTEM

Besides the normal tasks of maintaining remote-access server (RAS) equipment, managers often find their time consumed administering access rights and authentication privileges on several, geographically dispersed remote access servers at the same time. Enter the Remote Authentication Dial In User Service (RADIUS), a commonly used authentication system. Most remote-access equipment vendors have supported RADIUS in their remote-access servers. RADIUS has simplified administration of user authentication by maintaining a centralized database of access rights. IT managers can use a single RADIUS server to authenticate users dialing into multiple remote-access servers thereby maintaining a single authentication database. All users dialing into a network are authenticated against this database. For such centralized authentication to work, a RAS and VPN equipment must securely communicate with a RADIUS server and verify that the user meets certain conditions before allowing the user to gain access to the network.

WORKING

- A user places a call into a remote-access server and a Point-to-Point Protocol session is initiated.

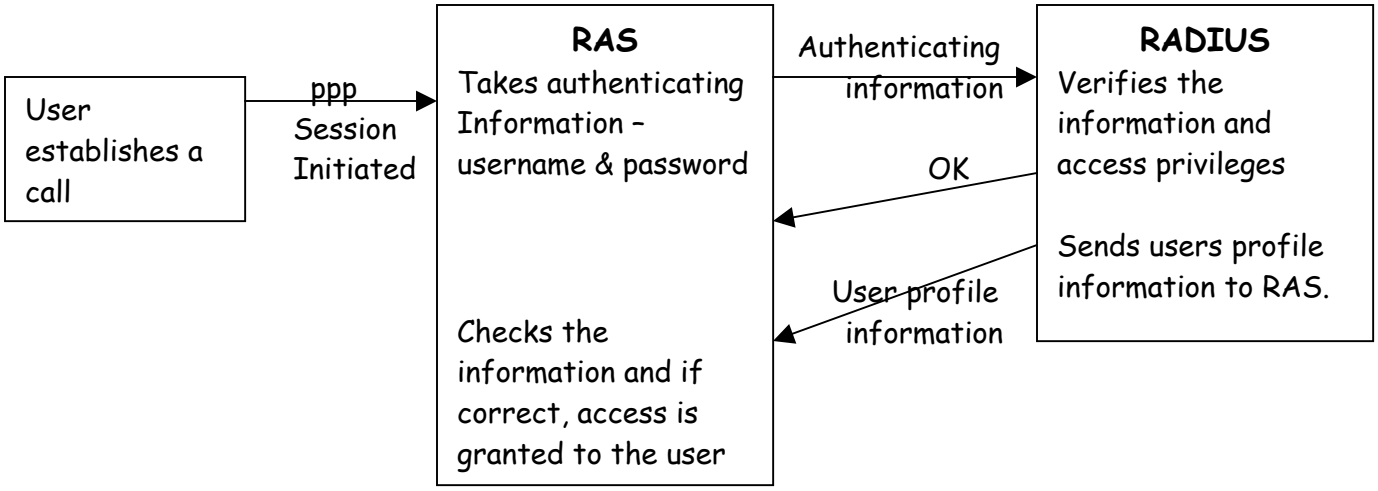
- The RAS or VPN takes authentication information, such as a user name and password, and passes this information to the RADIUS server.

- If the user is in the database and has access privileges to the network, the RADIUS server signals the remote-access server that it is OK to continue the process. The RADIUS server also sends what is called profile information about the user to the remote-access server. The profile can include information such as the user's IP address, the maximum amount of time the user can remain connected to the network and the phone number the user is allowed to dial to access the network.

- The RAS or VPN takes this information and checks to make sure the user meets all the criteria of the checklist items.

- If all the conditions are met, the PPP negotiation with the user is completed and access is granted.

- If the user does not meet all the conditions, say the person called using a number reserved for other people in the company, the call is terminated.



AUTHENTICATION PROTOCOL: PPP supports both PAP & CHAP

- **Password Authentication Protocol (PAP):** PAP is easier to use, but offers lower security. With PAP, users typically send passwords to the RAS unencrypted in plain text format. The RAS encrypts the password and sends it to the RADIUS server, which decrypts the password. The RADIUS server then validates the password against its database or against a NetWare Bindery, NetWare Directory Service or against a Microsoft NT Domain or Workgroup list.

- **Challenge Handshake Authentication Protocol (CHAP):** With CHAP, the RAS challenges the user to prove his or her identity. This is accomplished by the RAS generating a random number and then sending it to the user. The user's PPP client creates what is called a digest that encrypts the password using the "challenge." This digest is sent to the RAS, which then passes it to the RADIUS server. The RADIUS server creates a digest using its copy of the user's password. If the two digests match, it means the user is who he or she claims to be and the RADIUS server authenticates the identity. The benefit of this approach is that a user's password never passes unencrypted over the dial-up portion of the link.

TUNNELING:

Tunneling is at the heart of all VPN implementations. There are two generic classes of tunnels.

The first is end-to-end tunneling where, for example, the tunnel extends from a remote user's PC to the server that user is connecting to. In this scenario, the devices at each end of the connection must handle the establishment of the tunnels, and encrypt and decrypt the data passed between the two points.

The second type is node-to-node tunneling, where the tunnel terminates at the edge of the network. This type of tunnel could be used to connect LANs in different sites. In such a configuration, all the traffic on each LAN is unchanged. Once traffic passes through a VPN de-vice on the edge of the LAN, it is encrypted and tunneled to a similar device at the second site. At that point, it is decrypted and put onto the LAN in native format

TUNNELING PROTOCOL

L2TP: Known as the Layer-2 Tunneling Protocol, L2TP is the combination of Cisco Systems' Layer-2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP supports any routed protocol, including IP, IPX, and AppleTalk. It also supports any WAN backbone technology, including frame relay, ATM, X.25, and SONET. One key to L2TP is its use of PPTP. This Microsoft protocol is an extension of PPP and is included as part of the remote access features of Windows 95, Windows 98, and Windows NT. So, in the big picture, most PC clients come equipped with tunneling functionality. PPTP provides a consistent way to encapsulate Network-layer traffic for remote access transmission between Windows clients and servers. The L2F portion of L2TP lets remote clients connect and authenticate to networks over ISP links. L2TP can create multiple tunnels from a single client.

IPsec: As for IPsec, the full name for it is Internet Protocol Security, and it's basically a suite of protocols that provide security features for IP VPNs. As a layer-3 function, IPsec can't perform services for other layer-3 protocols, such as IPX and SNA. IPsec provides a means of ensuring the confidentiality and authenticity of IP packets. The protocol works with a variety of standard encryption schemes and encryption negotiation processes, as well as with various security systems, including digital signatures, digital certificates, public key infrastructures, and certificate authorities. IPsec works by encapsulating the original IP data packet into a new IP packet that's fitted with authentication and security headers. The headers contain the information needed by the remote end,

which took part in the security negotiation process to authenticate and decrypt the data contained in the packet. IPsec can complement other VPN protocols. For instance, IPsec can perform the encryption negotiation and authentication, while an L2TP VPN receives the internal data packet, initiates the tunnel, and passes the encapsulated packet to the other VPN end point. IPSec was developed by the Internet Engineering Task Force as a security mechanism to protect IP packets. It is commonly used in both end-to-end as well as node-to-node applications.

SOCKS 5: It follows a proxy server model and works at the TCP socket level. To use SOCKS 5, systems must be outfitted with SOCKS 5 client software along with a SOCKS 5 server. The SOCKS 5 client intercepts a client request for services. The request is sent to the SOCKS 5 server, which checks the request against a security database. If the request is granted, the SOCKS 5 server establishes an authenticated session with the client and acts as a proxy for the client, performing the requested operations. The upside to SOCKS 5 is that it lets network managers apply specific controls on proxied traffic. Because it works at the TCP level, SOCKS 5 lets you specify which applications can cross the firewall into the Internet, and which are restricted.

TYPES OF VPN

(A) On the basis of how businesses and organizations use VPNs

- **Access VPN**---Provides remote access to a corporate intranet or extranet over a shared infrastructure with the same policies as a private network. Access VPNs enable users to access corporate resources whenever, wherever, and however they require. Access VPNs encompass analog, dial, ISDN, Digital Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.
- **Intranet VPN**---Links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, quality of service (QoS), manageability, and reliability.
- **Extranet VPN**---Links customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, QoS, manageability, and reliability.

(B) On the basis of the platform

- **Hardware based:** Most hardware-based VPN systems are encrypting routers. They are secure and easy to use, since they provide the nearest thing to "plug and play" encryption equipment available. They provide the highest network throughput of all VPN systems, since they don't waste processor overhead in running an operating system or other applications.
- **Firewall-based:** Firewall-based VPNs take advantage of the firewall's security mechanisms, including restricting access to the internal network. They also perform address translation; satisfy requirements for strong authentication; and serve up real-time alarms and extensive logging. Most commercial firewalls also "harden" the host operating system kernel by stripping out dangerous or unnecessary services, providing additional security for the VPN server. OS protection is a major plus, since very few VPN application vendors supply guidance on OS security.
- **Software based:** Software-based VPNs are ideal in situations where both endpoints of the VPN are not controlled by the same organization (typical for client support requirements or business partnerships), or when different firewalls and routers are implemented within the same organization. At the moment, standalone VPNs offer the most flexibility in how network traffic is managed. Many software-based products allow traffic to be tunneled based on address or protocol, unlike hardware-based products, which generally tunnel all traffic they handle, regardless of protocol. But software-based systems are generally harder to manage than encrypting routers. Tunneling specific traffic types is advantageous in situations where remote sites may see a mix of traffic, which needs transport over a VPN (such as entries to a database at headquarters) and some that doesn't (such as Web surfing). In situations where performance requirements are modest (such as users connecting over dial-up links), software-based VPNs may be the best choice.

(C) On the basis of performance

- **Static VPNs** are up full time
- **Dynamic VPNs** operate on demand and are more commonly used for mobile workers and telecommuters.

BENEFITS

1. **Cost Savings** - If you use the Internet to distribute network services over long distances, then you avoid having to purchase expensive leased lines to branch offices or partner companies. And, you escape having to pay for long distance charges on dial-up modem or ISDN calls between distant sites. Instead, users and systems simply connect locally to their ISP and leave the rest of the journey to the vast reach of the Internet. VPN can reduce the recurring communication charges.

2. **Ideal way to handle mobile users** - VPNs allow any user with Internet access and a VPN client to connect to the corporate network and to receive network services.

3. VPNs also use encryption to **ensure the confidentiality of data** as it passes over the Internet or service provider's network. The choice of encryption technology includes
   - RSA Data Security Inc.'s
   - Rivest Cipher technology
   - DES (Data Encryption Standard)
   - Triple-DES

   And the choice of key sizes include 40-bit to 128-bit sized keys in commercial applications. The general idea is that the larger the key is, the more difficult it is to crack the code and thus the more secure the data will be. The choice of key size depends on many factors, including such obvious ones as the importance of keeping the data confidential and the security of the network that the data will pass over.

4. **Manifold Efficiency:** The effects a VPN can have on an organization are dramatic: sales can be increased, product development can be accelerated, and strategic partnerships can be strengthened in a way never before possible. Prior to the advent of VPNs, the only other options for creating this type of communication were expensive leased lines or frame relay circuits. Internet access is generally local and much less expensive than dedicated Remote Access Server (RAS) connections.

APPLICATIONS

Remote access: to give telecommuters and mobile workers a way to get back to a corporate network over the Internet or a service provider's backbone. In a remote-access VPN, a user dials into a service provider's point of presence, establishes a tunnel back to headquarters over that provider's network or the Internet, and authenticates himself or herself to gain access to the corporate network.
There are a number of reasons to use a VPN for remote access.

- Cost savings on the calls
- Savings can come from reducing the operational costs associated with supporting remote users
- Save on communications charges - VPN would eliminate the need for the T1 line for dial access.

Site-to-site connectivity: As in the remote-access scenario, branch offices are connected to corporate headquarters through tunnels that transport traffic over the Internet or via a provider's backbone. Again, as in the case of remote access, a company might be able to reduce communications costs by paying only for the access line from a branch office to the service provider's POP, rather than paying for a long distance link to headquarters. Additionally, site-to-site VPNs can cut communications costs significantly if a company has many international sites. A VPN built around a service provider with points of presence in countries where there are branch offices would allow the international sites to pay only for dedicated Internet access to that point of presence.

Extranets: The basic idea of VPN-based extranets is to use the access control and authentication services with a VPN implementation to deny or grant customers, trading partners and business associates access to specific information that they may need to conduct business. With a VPN-based extranet application, the outside party would get to the corporate firewall by tunneling across the Internet or a service provider's network. The ability to get behind the firewall is controlled by the VPN access control services. Basically, VPN authentication and access control services are used to manage such levels of access. The selling point for this VPN application is that it builds customer loyalty.

Intranet: The general idea is to use the encryption, authentication and access control services of a VPN to segment populations on a corporate network or intranet. In many situations, companies need to ensure the confidentiality of data. **For instance**, a human resources department might want to let employees check on vacation time, but not be able to see performance reviews. Or a national sales

manager might be granted access to the sales performance records of all sales associates, while each associate only has access to his or her own records. VPNs can help an IT manager establish and manage these levels of access.

ROLE OF SERVICE PROVIDERS IN VPN ARENA

The role of a Service Provider depends upon the preferences of the Client Organizations IT Manager. Some will want to off-load as many VPN and security tasks to a provider as possible while some may restrict the provider to provide access and equipments and leave the management of the VPN to the corporate IT staff. The role of the Service Provider is dependant upon the degree of involvement the IT Manager of the Client Organization wishes to have with the Service Provider. Therefore, the role of the Service Provider can range from supplying Internet access to one where the provider offers a Turnkey Solution.

BASIC OPTION: Sets up remote users with VPN client software and then puts VPN equipment in branch offices. The IT staff must manage the equipment and VPN services such as user authentication and encryption key distribution. The provider is not involved in managing the VPN at all. The provider is not involved in managing the VPN at all. This approach is generally regarded as an economical one. A company pays for an Internet access line to headquarters and branch offices. Users, in turn, each get an unlimited access, flat-rate monthly ISP account.
One potential problem with this approach is that with a flat-rate ISP account, there is no distinction between a VPN user dialing into the service provider for business or a teenager surfing the Web and chatting with friends.

PREMIUM OPTION: In contrast to the flat-rate service, a premium service provides performance guarantees. These guarantees typically come with some financial incentive for the user organization. If the provider fails to meet promised service level agreements (SLA's) for latency across its backbone or network availability, the customer gets a credit on its monthly bill. With SLAs in hand, some providers are offering premium usage-based user accounts that deliver much better performance than flat-rate monthly ISP accounts. Such services cost more than a flat-rate service but deliver the performance that would be required for business applications.

MANAGED SERVICES OPTION: Certain providers offer services that include access in addition to the VPN equipment. In essence, the IT manager leases the equipment from the Service Provider or the price of the equipment is built into the monthly service fee. In addition to equipments and access the Service Providers provide the Organizations employees with the training on the use of the

equipments. In addition, the Client no longer needs to dedicate resources to manage the equipments on a day-to-day basis, and the provider can typically upgrade the equipment over time.

BEYOND MANAGEMENT OPTION: Service providers can also play a role beyond the management of access equipment. However, as more companies look to their VPNs for e-commerce applications, IT managers may want the service provider to play a bigger role in security services. Here the Service Providers play a major role from beginning to end. The provider in addition to providing access, equipments, training, hardware and software upgrades also manage the security aspects for the Client Organization. The security portfolio includes managing firewalls and scanning e-mail messages and attachments for viruses, managing traffic etc.

WHY OUTSOURCING??????

Outsourcing because IT managers are trying to find ways to reduce the total cost of supporting ever-increasing numbers of remote users be they telecommuters, travelers or just users in other sites. Acc. to the Gartner Group, enterprises are increasingly turning to service providers to configure, own and manage their remote communications infrastructures.

1. **Low cost of ownership:** Outsourcing remote access to a VPN reduces the total cost of ownership of remote access: means no more modem pools to maintain, no more remote access servers to manage and no more WAN equipment such as Channel Service Units/Data Service Units associated with these devices.

2. **Introduction to new services:** Some companies have found that outsourcing remote access has allowed them to bring in-house other services that have previously been outsourced.

3. **Staffing Issues:** One component of the total cost of owner for remote access is staff training. Using a VPN approach, a company could out-source its remote access communications to a service provider. And this can help reduce training costs. Essentially, the service provider is responsible for the management of the equipment. As a result, there is no need to train staff in the use of the equipment.

4. **Low employee turnover:** Outsourcing remote access to a VPN eliminates the staff churn problem. The service provider is responsible for managing the equipment and for training its own people on the equipment.

5. **Concentrate on competitive advantage:** IT managers also may find that when outsourcing a VPN to a provider, they can off-load other management tasks, again freeing up staffers' time for other projects.