

VPN Introduction

1. GENERAL DEFINITIONS

A Virtual Private Network is a communication environment where access privileges are restricted to permit peer communications only within defined community of interest and is constructed through a means of a common communication medium with the associated network services. VPN offers solutions to the today's communications in the following ways:

A number of technologies must be integrated to provide "true" Virtual Private Network" solutions. They range from simple dial or leased line access for encryption, policy management, directory integration and system management. The successful network service provider will provide a unique set of technologies, integrated to meet the corporation and enterprises to offer VPN services. The technical components from the remote site/user, system access, core network and value-added services are illustrated in Figure 1.

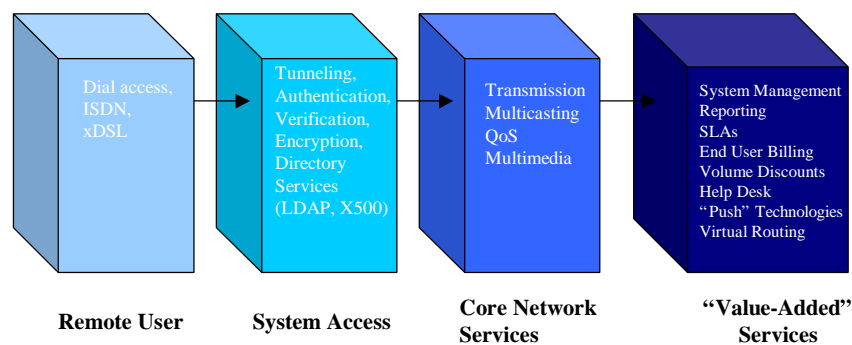


Figure 1: Technical components to offer VPN services

VPNs products and services provide the opportunity for network service providers to secure and expand their customers' base in an increasingly competitive telecommunication. Through the VPN, the corporate can provide but not limited to the following services:

- Packet telephony services
- Multimedia applications (e.g. video-telephony, video-conference and interactive learning)
- Database access
- Internet and Web access
- Electronic messaging
- Inventory management
- Customer service
- Collaboration
- Publishing

- Electronic commerce
- Y2K Updates

2. KEY REQUIREMENTS OF A WELL-DESIGNED VPN

The key requirements of a well-designed VPN must include the following attributes:

- **Any-to-Any Connectivity:** It must have the capabilities to provide access and communication among two or more sites. Therefore the chosen networking is an important factor for the any-to-any connectivity.
- **Scalability:** Scalability must include ways to expand the capacity of the existing devices in the network. As an example, in the case of a remote site requiring more connections, another hub can be inserted within the existing architecture. Scalability allows business expansion and eliminates forklift upgrades and usually provides load balancing and redundancy. Scalability greatly depends on the networking technology used to implement VPN services.
- **Network Resiliency:** One of the challenges that the service providers face is the network availability. It is therefore important for the VPNs to provide mechanisms for error diagnosis and recovery mechanisms in an efficient way.
- **Reliability and Flexibility:** Reliability and Flexibility in a VPN, means availability of services at all times, similar to the telephone network. This means that redundancy features (e.g. RAS) must be added to allow automatic recovery of failed devices. Additionally, VPN should offer flexibility to the corporate sites by taking advantage of the offered services.
- **Usability:** The VPN must be very easy to use and understand. For a VPN solution to be successful, the end users of the VPN must use their services without realizing it. The VPN must be transparent to the end-user when tunnels are established and torn down.
- **Management Capabilities:** This is essential for cost-effective provisioning, management and billing with advanced monitoring and automated flow-through systems to quickly roll out new service and support of Service-Level-Agreement (SLA).
- **Quality of Service:** It ensures prioritization of mission-critical or delay-sensitive traffic and manages congestion across varying bandwidth rates.

3. VPN USER CATEGORIES

The following categories seem to benefit for the deployment of VPN:

- **Remote User Access.** Remote access is referred to the access of the enterprise Intranet from the remote users without dialing in a RAS located within the corporate headquarters. Such users can be classified in the following categories:

1. Mobile workers and business travelers. For this category, access is granted by limiting the authentication process to user name and password. These are the classic road warriors who need access to the enterprise's resources. Mobile users require self-contained technology on their laptop such as PCMIA modem and dial-up client software.
2. Telecommuters work one or more full days a week from home. These types of remote access users have higher demands than the previous category. Such demand can be accomplished through the use of higher bandwidth connections such as ISDN for dial-up. Telecommuters require corporate and Internet accesses and may use a separate phone/fax line for work.
3. Home workers use their PC occasionally from home for short period of time such as weekends and/or evenings, additionally to their main daily activity at the corporate site.

Figure 2 illustrates a typical distribution of user types.

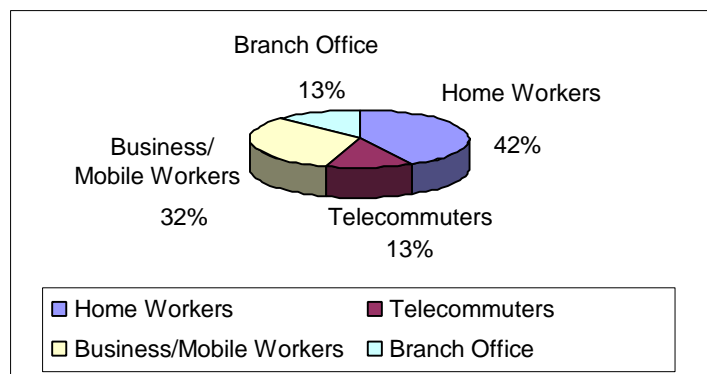


Figure 2: Typical users of remote access

Remote access to information is a strategic corporate necessity. The deployment of VPN benefits the company in the following way:

- ✓ Arms employees with up-to-date information, enabling them to make the most informed decisions available.
- ✓ Streamlines access to information through Internet and intranet connections
- ✓ Reduces networking costs by using mainly Internet to replace in-house WAN and dial-up networks.
- ✓ Extends the workplace beyond the office walls to allow people to be fully productive at home and on the road.
- ✓ Provides an edge in recruiting employees looking for flexible work styles such as telecommuting and job sharing.
- ✓ Competitive advantage by creating closer links with customers, suppliers and employees

- **Branch Offices:** Small businesses requiring access to a central site is also an important category where VPN can be deployed. The number of individuals in the office and the data rates of the connections vary depending upon the nature of the work.
- **Business partner/supplier network (Extranets):** The Internet activates new era in business partner communications. The clunky Value-Added Networks (VANs) of the past, which were typically set-up for only a few large customers and suppliers of the company, have now been superseded by simpler and cost-effective methods. As an example, supplier and/or customer can use Internet connection by securing the link to the enterprise network and use authenticating mechanism of the transmitted data, as illustrated in Figure 3.

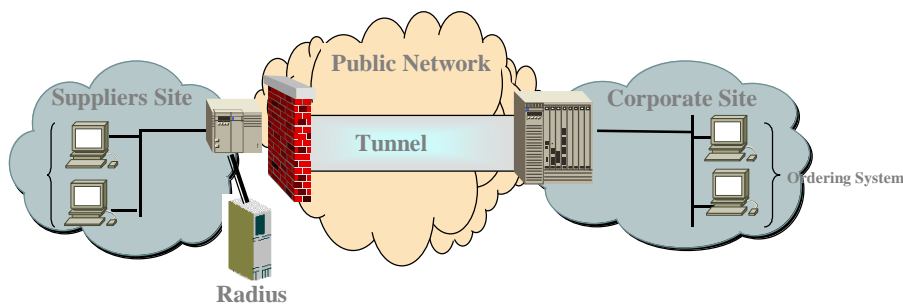


Figure 3: Typical Extranet example

This scenario represents the most recent trend for VPN usage. Companies can grant their partners temporal and limited access to their Intranet enterprise network. The wide availability of the Internet and its relatively small costs together with mature IP-VPN technology shall allow fully functional e-business applications including initial contact of customer, sales negotiation, as well as order process and on-going support. Similar to the remote access, the company pays for dial-in access from. A VPN around a service provider with POP in countries where there are branch offices would allow the international sites to pay only for dedicated Internet access to that POP. This would be much less expensive than the payment of a long distance link. It is difficult to estimate the cost savings of using VPN versus another networking technology. Since the inception of the Electronic Data Interchange (EDI), corporations have sought ways to streamline inventory and distribution cycles. Bar EDI and fueled efficient distribution by enabling trading partners to communicate in a fast way. VPN represents the opportunity for corporations to extend beyond themselves to multiple organizations, which must collaborate, communicate and exchange documents to achieve joint goals, not just transmit purchase orders and invoices. Apart from EDI, other important activities of an Extranet involve electronic commerce and supply-chain management. Online products are handled differently than traditional ones. A company sends out a description of a product

with appropriate modifications to meet individual needs; prompting the vendor to order additional parts and/or services from their supplier chain; and the product is shipped directly from the factory floor to the buyer's business.

- **Building Virtual Collaborative Group in a Private Network:** For example, IT managers of big companies have tried to segment the employees of the company using the Virtual LANs (VLANs) technology. However, the problems encountered with VLANs technology is that many products are proprietary-based and lack interoperability. VPNs can replace VLANs by creating an environment which is analogous to physically segment
- **Site-to-Site connectivity:** The next general application of VPNs is for site-to-site connectivity. Similar to the remote-access scenario, branch offices can be connected to the corporate headquarters. This can be addressed using ATM, Frame Relay, Leased Lines, the public Internet or a private Intranet network technology. The advantages, which are offered to the company, are the following:
 - ✓ The communication costs are reduced since the company pays only for the access line from the branch office towards the service provider's POP. As an example, using VPN technology for site-to-site connectivity, a branch office can remove the dedicated lines and move the traffic over the existing Internet access connection. Devices such as remote access servers, access routers may not be useful. Such equipment is expensive to manage and maintain.
 - ✓ VPNs allow flexibility in terms of moving easily from one provider to another by taking into account factors such as price, performance and offered services.
- **VPN to the Internet Service Providers:** Virtual Private Networks allow service providers to build innovative and highly profitable adjunct services which will grow customer base, eliminate churn and position the provider to enter in new markets. Such services may include:
 - ✓ Managed services offered to enterprises
 - ⇒ Customer premises equipment
 - ⇒ Security services
 - ⇒ Directory integration with Domain Name servers
 - ⇒ Software distribution services
 - ⇒ Asset management services
 - ✓ Consulting services
 - ⇒ Network troubleshooting
 - ⇒ Network design
 - ⇒ Network planning
 - ✓ Extranet "affinity" program

- ✓ Wholesale access to junior providers
- ✓ New Customer premise equipment offerings and programs

4. TECHNICAL ISSUES

A number of thorny technical and support issues therefore confront the corporation seeking to implement, which provide the remote access workers. These issues are the following:

- Access speed and technology
- Capitalization of central site equipment (It has been estimated that it costs more than \$200,000 in equipment to support 2,000 remote users)
- Integration of multiple protocols (TCP/IP, IPX, AppleTalk)
- Authentication
- Encryption
- Directory services
- Quality of Service mechanisms for multimedia applications
- Help desk support
- TCP/IP address management
- End user billing

4.1 Networking options

Traditionally, VPN had been provided in the form of packet switched services such as Frame Relay, X.25 or leased lines. Now, with the advent of the Internet it is possible to offer VPN services over the Internet. Figure 4 illustrates the possible networking technologies, which can be employed to implement VPN services.

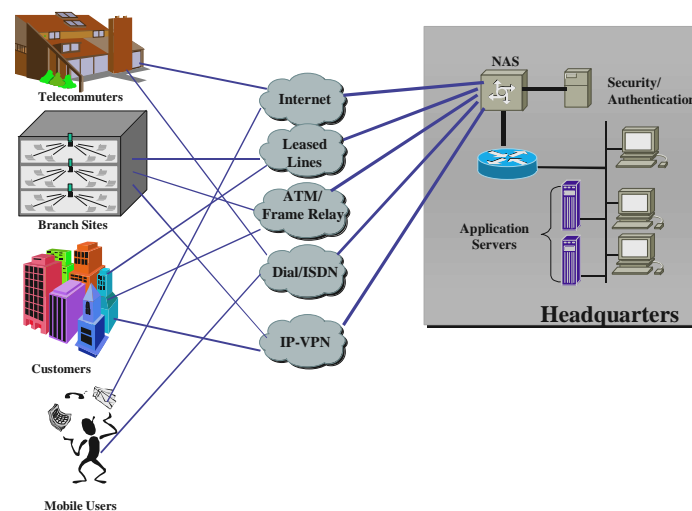


Figure 4: Use of different technologies to implement VPNs

The pros and cons of each networking technology are summarized in Table 1:

| Technology | Ubiquity | Cost | Internet Security | Efficiency | Guaranteed Service Levels |
|---------------------|-------------------|----------|-------------------|------------|---------------------------|
| ATM/ Frame Relay | Low- Moderate | Moderate | High | High | Yes |
| Public Internet | High | Low | Low | Moderate | No |
| IP VPNs | Moderate- High | Moderate | High | High | Yes |
| Leased-Lines | Low- Moderate | High | High | Low | Yes |

Table 1: Comparison of different networking technologies to create VPN services

The most common way for the remote user is to implement a VPN network using the Internet technology. Such a network can be based either on Intranet managed by the enterprise or using the public available Internet, through an Internet Service Provider. The pros and cons of each approach are illustrated in Table 2.

| Internet VPN | Intranet VPN |
|--------------------------------------|---|
| Public Internet-based | Provided by a single ISP controlling all access and backbone facilities |
| Ubiquitous connectivity | Configuration of path establishment |
| Throughput and latency varies | Tight throughput and latency |
| Constrained by lack of inter-ISP SLA | Enables SLAs to be delivered |

Table 2: Internet VPN versus Intranet VPN

It becomes apparent that Intranet VPN imposes constraints especially to mobile workers and travelers who may move to an area with no POP by the chosen ISP. Therefore, the Internet VPN is a more global solution.

4.2 VPN system Access Architecture

There are two basic VPN architectural choices:

- Service provider independent model. In this scenario, a VPN-enabled client initiates the tunnel, through the public network (e.g. Public Internet), to the corporate network. This can be accomplished by establishing a PPP session to the POP of a local ISP. The ISP takes over the responsibility. The advantage for the ISP, the tunnel is simply data and there is no requirement for special handling. However, the disadvantage this approach is that the client must be VPN-enabled. The larger the number of remote users, the bigger the investment thus increasing the expenses of the company to support the remote users. Such a configuration is illustrated in Figure 5.

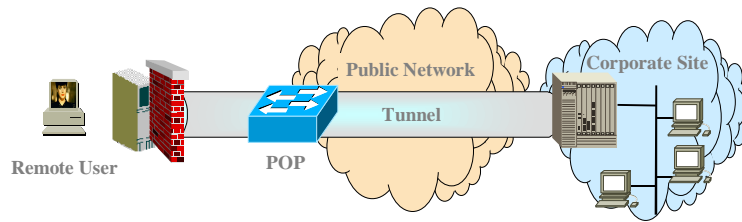


Figure 5: Service provider independent tunneling

- In the service provider dependent model, the corporate site signs an agreement with an operator such as ISP. The corporate user dials into a local POP with a PPP client and the tunnel session is initiated at the POP. The crucial difference is that the client can be any PPP client. Such a solution is illustrated in Figure 6.

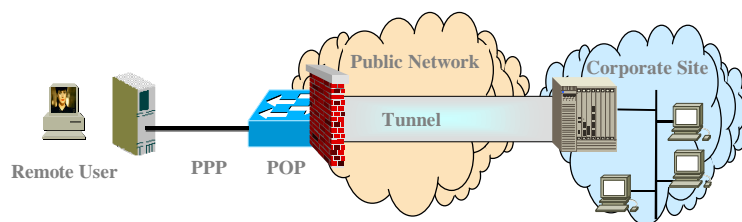


Figure 6: Service provider dependent tunneling

Comparison of the two approaches: The Service provider dependent model, eliminates the need for expensive deployment of new software to remote clients. Most end users prefer not to become involved with configuration firewalls, encryption software etc. This makes the Service Provider Dependent model particularly attractive for big companies with large number of remote workers and sites. The main disadvantage of this model is that access from the remote sites/users may be slow due to network overload. Additionally, the lack of POP in certain areas may be a drawback for travelers who find themselves unable to access the provider's network. Additionally, authentication is critical when using the service provider dependent model. In this model, the IT manager of the corporate site must monitor how remote users/sites are authenticated. If the service provider controls all user names and passwords, then all possible modifications (e.g. additions, deletions) must be accomplished through the service provider. On the other hand, the service independent other hand, relies on the VPN model. Additionally, since VPN software is on the client the remote site/user can use service provider with the POP. This is important also for travelers who may use the ISP with the closest POP.

4.3 Tunneling

VPNs are built upon the notion of efficiency and security data tunneling from one point to another. By using the tunneling concept, the remote access server of the network provider

wraps the user data inside packets of format depending on the employed technology by the network provider. Since Internet will be dominated as the technology where VPNs will be built. In this case, the user data are conveyed within an IP packet which are routed through the carrier's network or even across multiple networks up to the tunnel endpoint where the packet is unwrapped and sent towards its destination. Tunneling employs point-to-point session protocols to replace switched connections, linking data addresses over a routed network.

There are two major tunneling categories namely layer 3 and layer 2 tunneling. Their major difference regards the location where the tunnels are initiated and terminated. Layer 3 tunneling terminates the layer 2 connection at the RAS. It carries only the Layer 3 payload through the tunnel to the tunnel endpoint either in the enterprise network or at a router residing in the service provider's network. On the other hand, layer 2 tunneling carries the entire PPP frame over the service provider's backbone to a predefined endpoint. Table 3 briefly outlines the two tunneling types.

| Tunneling Type | Pros | Cons |
|--------------------------|---|---|
| Layer 2 tunneling | Simplicity, End-to-end encryption, Bi-directional tunnel set-up | Standards not finalised yet, Scalability issues Reliability issues Limited to PPP payload types Questions on security |
| Layer 3 tunneling | Scalability, Security, Reliability | Limited vendor participation Complex to develop |

Table 3: Layer-2 versus Layer-3 tunneling

There is a number of tunneling standards:

- L2F (Layer 2 Forwarding)_ which has been developed by Cisco, Nortel and Shiva.
- PPTP(Point to Point Tunneling Protocol): PPTP operates at layer 2 of the OSI model. It has been designed to work on the client-server basis and that is the reason why it can be employed for a single point-to-point connection.
- L2TP (Layer 2 Tunneling Protocol). It is a hybrid of L2F and PPTP. Like PPTP, it operates at layer 2 of the OSI model thin the tunnel and has been designed for a single point-to-point client-server connection. Multiple protocols can be encapsulated within the tunnel.

4.4 QoS

One other major concern is the challenging of QoS handling in VPN. MPLS tackles the problem of “how to make IP and data link technologies (e.g. ATM, FR, WDM) to interoperate by integrating the label swapping forwarding paradigm with network layer routing. MPLS groups packets in an IP session into a single flow at the network layer and then tags each session to expedite its passage through the router along the path. After the path is established, MPLS maps it onto a dedicated data link for delivery. Apart from MPLS, a QoS model must be adopted which alleviates the drawbacks of the Integrated Service Model. In contrast to IntServ model, DiffServ tags packets to identify whether they are voice, video, or data and then instructs the routers to service them according to the assigned classes. This is important for services with real-time flow such as VoIP, video on demand etc.

4.5 Security

Given a tunnel that defines a method for carrying private information across the shared network, encryption can be used to protect the contents of the tunnel. VPNs support standard forms of cryptography, including public key cryptography and DES (Data Encryption Standard) cryptography.

Compared to public key cryptography, DES is a symmetric crypto-system. When used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message.

While DES is CPU intensive, public key cryptography is 1000 times more expensive in terms of CPU cycles. Hence, public key technology is best used as a secure alternative to password-based authentication and for key distribution. DES should be used for bulk data encryption.

If another learns a valid user’s private key, then the user can be spoofed. Due to the requirements to control and distribute keys, a significant management infrastructure is required to control the technology:

- Certification Authorities are employed to vouch for the validity of keys
- X.509 Certificates provide a standardised way of representing names and associated public keys
- Certification Revocation Lists contain certificates and their associated keys
- An X.500 server provides a publicly accessible database for storing certificates and CRLs.

When layer 3 tunneling is employed there are certain mechanisms to prevent eavesdropping. IPsec is a standard-based technology that governs security management in IP networks.

Additionally, IPsec provides a standard way to exchange public cryptography keys, specify an encryption method (e.g. data encryption standards (DES) or RC4) and specify which parts of packet headers are encrypted. This is particularly important for emerged application such as the electronic commerce.

4.6 Authentication, Authorization and Accounting

One of the most popular mechanisms for the remote dial-in users is the provisioning of Authentication, Authorization and Accounting. Such a mechanism could be provided by RADIUS (Remote Access Dial-In User Service). RADIUS has been evolved from the remote access community's need to VPNs over the Internet. RADIUS provides mechanisms for the following requirements:

- Authenticate the user's ability to identify himself through an id and password match
- Authorization assignment of data access parameters based on pre-defined user profiles and security clearances
- Accounting management of a continuous audit-trail, tracking RADIUS-based transactions for accurate billing

4.7 Directory Server

One other major component, which must be added to tomorrow's VPN will be a directory server, a repository loaded with end-user profiles and network configuration data. This will be a separate platform deployed on the corporate network and on the part of the public network controlled by a VPN provider. Although this looks like a simple collocation but this is not the case. In the "old" days, a service provider simply stashed a CSU/DSU and a router in a customer's equipment closet. Directory servers represent physical and logical collocation. Both the equipment and the content are replicated on the private and the public network. These changes will directly affect VPN design. This has an impact on the VPN design. Network architects could decide to create a single physical and logical instance of their directory server, located either at a corporate site or at a carrier NOC. This would keep the costs down and, if the server is located behind a carrier firewall, thus avoiding security halls. This is accomplished by risking the recovery from disaster when failure for some reason occurs. Another alternative would be to deploy directory servers to several sites and make sure that they are logically mirrored to one at a NOC. Although this approach is security vulnerable, it offers both physical and logical redundancy.

5. USER REQUIREMENTS

These requirements are according to VPN uses as presented in section 2:

5.1 Remote users/ Telecommuters requirements

The telecommuter users entering to the headquarters enterprise usually perform the following tasks:

- Email activities
- Company-provided Web access
- Intranet Web Service
- Ftp access to companies' documentation

Dial-up access through the PSTN is not even adequate enough for Web access. As more and more new applications are emerged, there is a trend in the market to use access technologies such as ISDN. However, it is expected that xDSL will be a good alternative solution to alleviate the bandwidth's problem. This technology offers high bandwidth capabilities over current twisted pair copper lines. It is a technology offering up to 8Mbps downstream and up to 800 Kbps upstream.

Regarding the service-dependent versus the service-independent model, the telecommuters usually choose a fixed place to access remotely the corporate site. Therefore, large companies which employ a large number of telecommuters. The advantage is that the network provider provides a number of functionalities allowing the remote users to access the corporate site. However, this model is not suitable for the mobile travelers. In this case appropriate VPN software must be installed at the computer equipment. Therefore, for mobile travelers, the service independent model is more suitable for them.

Robust VPN solutions allow the network provider to control the authentication of users. This can be accomplished by solution such as RADIUS, appropriate use of tunneling protocols up to the corporate site. The IT manager of the corporate site may impose the remote user to further authentication process such as Intranet Service provisioning.

5.2 Branch Offices

This type of VPN is offered for companies with remote branches and possible remote users. Potential applications which may be used by this type of VPN, may include the following:

- Common Voice and Data Integration

- Internal Database Access
- Electronic messaging
- File Access
- Cooperative Work
- Transactions
- Design Information

For small to mid-sized companies, with multiple branch locations, Internet access can be provided through T1/E1 (maximum number of remote users 250), using the service dependent model. If the network provisioning is based on Internet technology, IPsec security with DES encryption could be deployed by the network provider. Password authentication is used in order to manage remote access to email and internal databases and files.

A different engineering approach for medium companies with up to 500 remote users and 10 corporate sites, such as engineering firms, marketing agencies which may have high-value intellectual property. Higher must be provided using 3DES encryption and strong user authentication using a method such as software tokens. Scalability can be enhanced by employing RADIUS servers to manage user names, passwords and policies. These types of VPNs can coexist with firewalls and offer network address translation to allow privately addressed sites to be linked together without requiring changes to the existing LAN addressing schemes. The benefits of the VPNs include higher security, manageable cost and provision for site-to-site communications as well as remote access.

Finally there is where a VPN may support medium to large companies with thousands of remote users and hundreds of sites, including those of business partners and customers, to send and receive customer account status, supply chain transactions and e-commerce activities. Such VPN users may be medical providers, insurance companies, manufacturers or companies that are part of an extended supply chain. Branch office connections are accomplished using fractional, full or multiple T1 lines. Main-site connections could be over multiple T1, fractional T3 or full T3 links. This type of VPN employ a service provider offering QoS and service level agreements to support guaranteed response times for critical applications running between company sites connected to the provider's backbone. The use of certified interoperable IPsec devices enables extranets with users on diverse networks with different equipment. The addition of user-level authentication capabilities such as two-factor authentication tokens or smart cards, supports secure mode remote access and enables user-level usage reporting and billing. For scalable administration, the VPN must employ directory services for storing and retrieving policies as well as for storing certification used

for authentication. Correspondingly, an in-house certificate authority, outsourced certificate service or some method of managing a public key infrastructure is required. This requires sophisticated design skills and ongoing management of sophisticated policies for employee and partner access necessitates the development, implementation and management of a comprehensive corporate security policy.

They support secure transactions for large, multi-national enterprises with more than 10,000 users and thousands of sites that have extended chains of business partners and needs for a high-degree of outsourcing, such as government agencies and financial institutions. The branch sites are connected using fraction, full or multiple T1/E1 links and the main sites can be linked over fractional or full T3/E3 links. A full range of remote access options should be available from dial to xDSL to cable modems. The use of a service provider network that offers real-time QoS and SLAs in conjunction with bandwidth management supporting convergence of applications such as voice and video conferencing over IP. These types of VPNS make extensive use of directory services and PKI technologies to manage policy and verification of user identity and role. These VPNs support sophisticated extranet relationships involving multiple partners and multiple independent PKI systems.