

Cost-Effective VPN-Based Remote Network Connectivity Over the Internet

Alwin Thomas and George Kelley*

Department of Computer Science
University of Massachusetts
100 Morrissey Boulevard
Boston, MA 02125-3393
gkelley@cs.umb.edu
thomas4116@aol.com
+1-309-210-1666 fax/messages

Abstract

This paper presents an overview of VPNs (Virtual Private Network) security issues from the perspective of a company that sought to reduce the costs associated with dial-up remote network connectivity and at the same time increase the level of satisfaction of its end-user employees and customers with secure remote connectivity solutions. The capabilities and limitations of various VPN configuration options are outlined, and an example implementation detailed.

1. Introduction

Network security is increasing in importance for companies of all sizes. The types of connections that must be secured are increasingly more varied and complex. The increase in telecommuting, corporate branch offices, and a mobile work force, and the global use and availability of the internet is transforming business-to-business communications very rapidly and dramatically. The need to securely and inexpensively share information with employees, partners and customers worldwide is driving many organizations to deploy Virtual Private Networks (VPNs) to afford convenience and to save considerably in communications costs. VPNs have been reviewed (King 2000; Tiller, 2001;) and popularized in the trade literature (Thyfault, 1999; Fratto, 1999, Seltzer 2000; Wirbel 2000). The total market for IP-based VPN services in the United States is projected to triple from just more than \$5.4 billion in 2001 to nearly \$14.7 billion in 2006, at an annual growth rate of 22 percent (Malik, 2002).

In general, security is not a single product or technology but an integration of several technologies combined with a management policy that provides protection balanced against acceptable risks. Security services include the primary services of confidentiality, integrity, and assurance (Poore, 1999). These primary security services can be further subdivided as shown in

Figure 1. The overall purpose of security is to minimize disclosure, adulteration, and breakdown risks associated with transmitting sensitive information over public and privately managed networks.

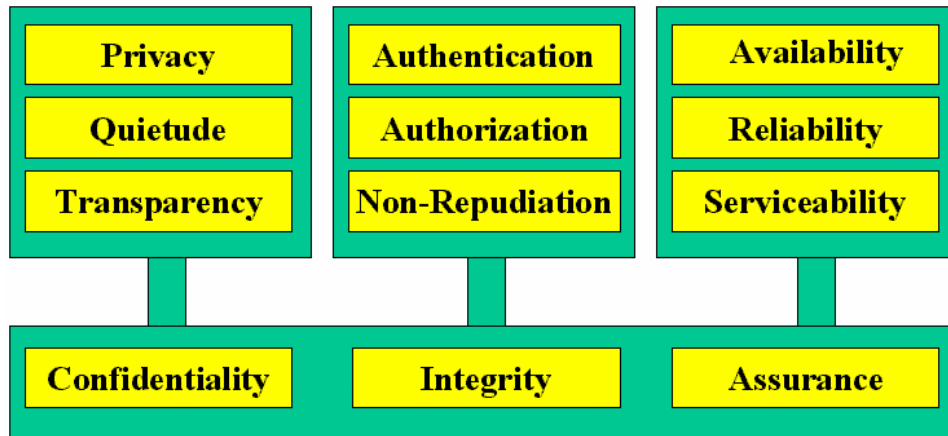


Figure 1. Systems Security Needs. Based on the GASSP Pervasive Principles given in (Poore, 1999) and the formulations adopted in (ISO/IEC 17799:2000), (ISO/IEC 15408-1,2,3:1999), and (NIST Handbook 800-12).

2. Virtual Private Networks

A virtual private network (VPN) is a type of network that combines the use of both private and public networks segments with the use of security software that compresses, encrypts, and then masks the flow of the digital packets the network is transmitting. Telecommunications carriers typically configure VPNs so that appear to be private national or international networks to their customers when they are, in fact, sharing backbone trunks with other customers. To the customer, a VPN like that of Figure 2 offers the security of a private network via access control and encryption, while at the same time affording the comfort and the economies of scale of the substantive nature of the administrative network facilities of large public networks. A private network segment could be for example a channelized T1 link between company branch locations, or a modem-initiated telephone switched-circuit link to a corporate modem bank connected to a Remote Access Server (RAS). The Internet backbone, essentially a mesh of interconnected OC-3 optical fiber links, is an example of a public network segment. A private segment shields the network user from the network traffic from the outside world, and as such tends to keeps the information on the network relatively private and protected from prying eyes and nefarious souls. On a public network segment, there is a much greater risk that the information on the network will be intercepted or altered by the much larger community of outsiders. A point-to-point protocol (PPP) can use a VPN to establish a secure communication link between one source and one destination of a network comprised of both private and public segments. For example, with the Point-to-Point Tunneling protocol (PPTP) or Layer Two Tunneling Protocol (L2TP), it is possible to securely access resources on a network by connecting to a remote access server (RAS) freely through the Internet without incurring per-

minute long distance telephone charges, and without the need to maintain a bank of inbound telephone lines to support in-house modem banks. This is the setup shown in Figure 3.

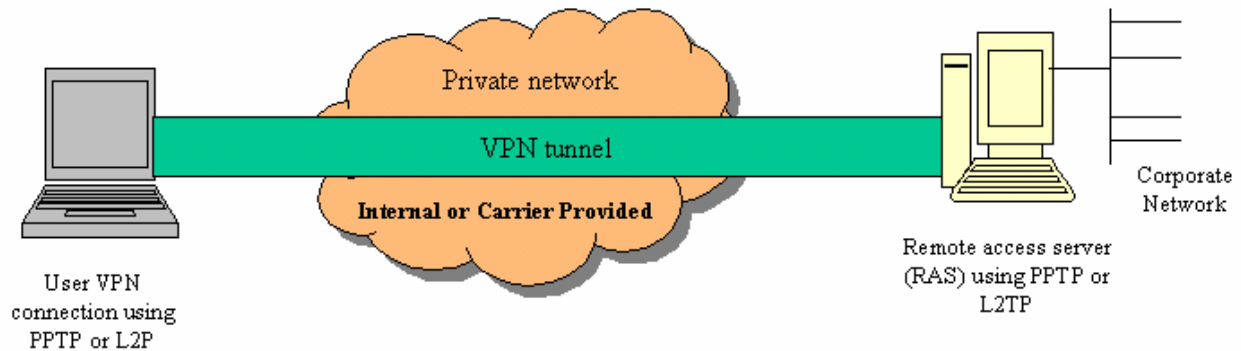


Figure 2. VPN tunnel established over a private carrier network

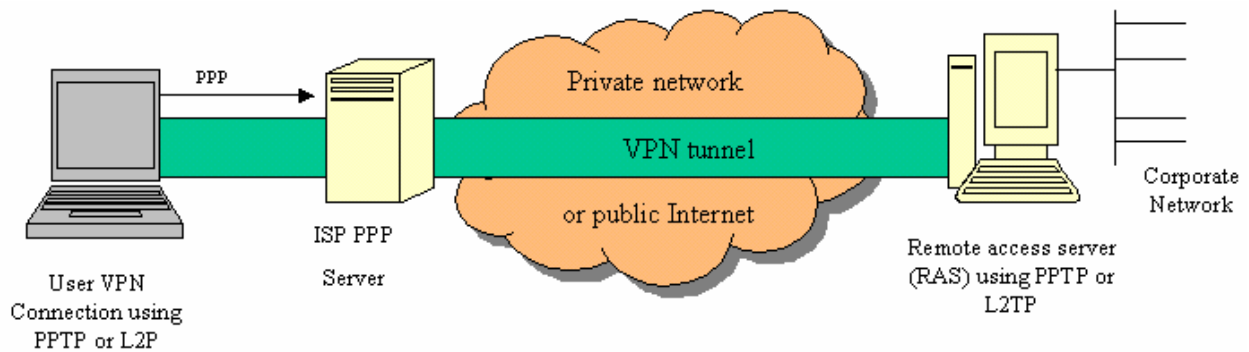


Figure 3. VPN tunnel connection using an ISP (Internet Service Provider)

3. VPNs and the 7 Layers of the OSI Model

VPN security must include tools to provide security services across all 7 layers of the OSI model. The OSI Physical Layer 1 security functions must safeguard against the adulteration of information via injected bit flips. The Link Layer 2 security must ensure that data frame labeling, fragmentation and assembly and hardware-based compression and encryption are not compromised. The Network Layer 3 must securely assemble frames into packets with source and destination information that must not be altered. Transport Layer 4 security, needed when setting up transfer processes of packets across different network segments, must be able to notice when transmission errors are maliciously induced, and correct and report them. This layer must also be able to act on congestion caused by denial of service (DoS) attacks by throttling data packet flow rates data, compensate for losses from black hole attacks, and protect the inter-segment processes from being led astray by impersonation attacks (man in the middle identity spoofing), and duplication and sequencing attacks. The Session Layer 5 security must protect the dialog messages that initiate, respond to, negotiate, setup, maintain, arbitrate error checking and

correction, and otherwise track end-to-end dialog network message exchanges to completion. Session Layer 6 security must protect at least three types of information. One is the message translation and sentinel functions related to software-level encryption mechanisms, for example protect PKI (public key infrastructure) public and private encryption and decryption keys and the related authenticity and integrity of certificates issued by Certificate Authorities (CAs). The second and the third are to protect software-level compression and decompression mechanisms and the end-user login IDs and passwords used to arm a VPN. Finally, Application Layer 7 security provisions must ensure the security of the PPP (point-to-point protocol) that will function as the wrapper protocol that will provide the overall end-to-end secure network functionality across all seven layers of the OSI model.

4. TLS, LLS, and ENLS Based VPN Security Frameworks

The need to provide security at all seven layers of the OSI model has led to roughly three major ways to secure a VPN: frameworks based on Transport Layer Security (TLS), Link layer security (LLS), and End-To-End Network Layer Security (ENLS).

1. *Transport Layer Security (TLS)* permits protection of TCP-based protocols, including World Wide Web sessions. Today, many applications are hosted for access across public and privately managed networks, secured through transport layer security technologies such as HTTPS, SOCKS, or SSL. Transport layer security as provided by SSL/TLS means that TCP-based applications are written specifically to use these security services. However, SSL/TLS applications are not well suited to centralized management because these services are frequently applied on a webpage-by-webpage basis. SOCKS is an authenticated firewall traversal protocol that provides for extensible authentication, as well as granular authorization for both incoming and outgoing sessions. SOCKS V applies both to TCP and UDP-based protocols, and is amenable to centralized management. As a result, SSL/TLS, and SOCKS technologies are complementary and can be used together to provide transport layer security within VPNs and extranets both.

2. *Link Layer Security (LLS)* encrypts data in transit within remote access sessions as well as within branch network connections. Many companies use private or trusted network infrastructures including internal and outsourced cable-plants and wide area networks, which offer a level of privacy by virtue of physical security. Alone, these networks do not protect against inadvertent or intentional viewing of information as it passes over a network. Because most security breaches occurring within a company network, additional technologies are required to protect information from theft and attack.

3. *End-to-end Network Layer Security (ENLS)* services, converged through Internet Protocol (IP) Security, or IPSec permits security services to be applied on internal networks. End-to-end network security consists of security techniques and protocols that transparently secure communications requiring application awareness. Careful network design and configuration is required to achieve this security. These tools are generally managed through administrative policy so that communications are safely protected as they travel across a network, without the knowledge or involvement of applications or end users.

All three approaches have been discussed in the industry under the broad category of Virtual Private Networking (VPN). Whereas it is true that each model provides some level of private networking, this broad definition is not always very helpful. This paper focuses on link layer and end-to-end security. It demonstrates how Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IPsec protocol can be used to address diverse corporate VPN security requirements. In this paper, "VPN" refers more narrowly to providing security across a public or untrusted network infrastructure. This means primarily: 1. How to secure remote access from client-to-gateway, either through Internet connections or within private or outsourced networks; and 2. How to secure gateway-to-gateway connections, across the Internet or across private or outsourced networks.

5. VPN Protocols

Over the past several years, a number of protocols have emerged that are categorized as VPN protocols and that secure communications through encrypted communications. These include:

1. *IPSec - Internet Protocol Security*: An OSI Layer 3 Network architecture, protocol, and related Internet Key Exchange (IKE) protocol, which are described by IETF RFCs 3168 and 2401-2409 (see <http://www.rfc-editor.org/>). IPSec provides network data packet integrity protection, authentication, and can be configured to offer privacy and replay protection services. IPSec relies on a complex security Internet Key Exchange (IKE) handshake validated by PKI (Private Key Infrastructure) mutual-authentication certificates issued by a trusted third-party Certificate Authority (CA) entity. IPSec packets are of two types: Encapsulating Security Payload (ESP) format, which see to privacy, authenticity, and integrity, and Authentication Header (AH) format, which provide for authenticity and integrity but not privacy. IPSec Transport is used to provide security for end-to-end IP communications traffic. It takes existing packets and protects them from spoof and tampering while in transit. IPSec Tunnel is used primarily by network midpoints, routers, or gateways to secure connections between networks mediated by a third, usually public, and as such untrusted network, for example the Internet. The IETF IPSec Tunnel specification (IETF RFC 2709) did not specify mechanisms for user authentication and client IP address configuration (at the behest of interested vendors). As a result, IPSec Tunnel is not intrinsically well suited for use by end-point remote access VPN clients.

2. *L2F - OSI Layer 2 Forwarding*: A proprietary protocol (Cisco) that is similar to PPTP. Unlike PPTP, it can encapsulate IP as well as other OSI Layer 4 Transport protocol formats. It can work with the authentication methods used by PPP, but requires special hardware on the host system.

3. *L2TP - OSI Layer 2 Tunneling Protocol*: A combination and enhancement of PPTP and L2F, described in RFC 2661. It evolved through the IETF standards process and the hands of a number of industry consortia. It was designed to specifically support authenticated and encrypted gateway-to-gateway as well as end-point client to network access server. It uses a simple user ID/password and does not require the administrative, performance, and added traffic overhead of PKI based certificates. L2TP encapsulates PPP frames to tunnel them through IP, X.25, frame relay, AppleTalk, IPX (Internetwork Packet eXchange), or ATM (Asynchronous Transfer Mode) networks, usually with compression and encryption enabled. Like L2F, L2TP

supports more than just the IP protocol, yet does not require costly hardware upgrades to implement. L2TP is optimized to work with both IPv6 (RFC 2460), the next generation of IPv4, with added multimedia QoS (Quality of Service) capabilities) and IPSec. The IPSec Internet Key Exchange (IKE) protocol negotiates security for the L2TP tunnel. The IKE security authentication process uses a Public Key Infrastructure (PKI) to issue third-party certificates to establish that the source and destination computers should trust each other. If IPSec Transport security is successfully established, L2TP negotiates the tunnel (including compression and user authentication options) and performs access control that is based on the user identity (for example CHAP passwords and EAP tokens and smart cards). The multi-protocol and IPSec support makes L2TP/IPSec interoperable and as such attractive for remote VPN user connections. L2TP/IPSec has been widely implemented as a result. The L2TP/IPSec packet structure looks like the example in Figure 4. The PPP payload portion contains the original IP datagram. A signature derived from the information in the IPSec ESP header and the IPSec encrypted portion of the packet is stored in the IPSec Authentication Trailer.

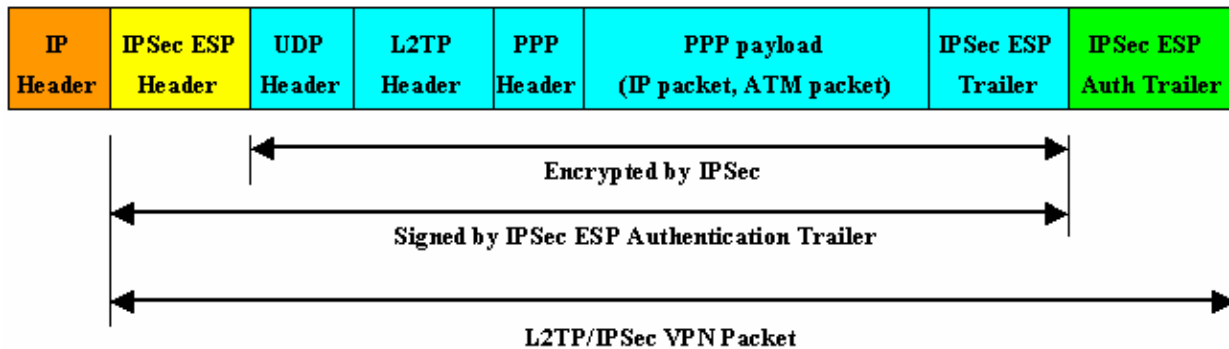


Figure 4. L2TP/IPSec VPN packet

4. *PPTP - Point-to-Point Tunneling Protocol:* An OSI Layer 2 protocol created by the PPTP Industry Forum (US Robotics--now 3Com, 3Com/Primary Access, Ascend, Microsoft, and ECI Telematics). It encapsulates PPP so that any data can traverse the Internet masked as an ordinary IP transmission. PPTP supports the encryption, authentication, and network directory access provided by RAS. Instead of users having to connect directly by phone from their present remote location through a dial-up Remote Authentication Service (RAS) access server box located at a central destination (typically over a phone line at 33.6 Kbps uplink/ 56Kbps downlink speeds), they can connect indirectly through their ISP (Internet Service Provider) using a phone dial-up, internet enabled cableTV link, or xDSL hookup account, and so gain access to their corporate network files and email the same as if they were sitting at work in their offices. The connection runs through the pipe established by their ISP (typically 33.6/56Kbps uplink/downlink speeds for modem dial up, 128/384+Kbps for cable or xDSL), their ISP's and their company's ISP's high-speed connection to the internet (usually at least an OC-3 155Mbps connection), and their company's connection to their ISP (usually a T1 1.544 Mbps connection).

5. *PPP - Point to Point Protocol*: A serial communications protocol that enables a workstation to connect to a server. PPP can support multiple OSI Layer 3 Network Protocols. It requires little configuration of the client workstation and can use both synchronous and asynchronous communication protocols. Synchronous protocols validate transmitted information with check sequences, asynchronous protocols validate transmitted information one character at a time using start and stop bits. PPP is inherently slow, particularly when used in combination with PPTP and L2TP, because to PPP (like SLIP) is a “serial line encapsulation protocols” that encodes packets for transmission on a slow (and often unreliable) serial line [Nemeth 2000].

Although IPsec, L2TP, and PPTP are viewed by many as competing technologies, these protocols offer different capabilities that are appropriate for different complementary uses. For example, PPTP/PPP and L2TP/PPP can pass through NATs (Network Address Translators) used by some network border devices, but L2TP/IPsec, IPsec Transport, and IPsec Tunnel often cannot. NATs are commonly used to present one IP address to the outside world, mask internal IP addresses that are not globally assigned by IANA (the Internet Assigned Names Authority, <http://www.iana.org/>), and at the same time shield the internal IP address identity of an internal link participant. Conversely, the verification of network packet authenticity and integrity is available when using L2TP/IPsec, IPsec Transport, and IPsec Tunnel, but not with PPTP/PPP or L2TP/PPP.

6. Example VPN Implementation

As an example VPN implementation, the sections that follow one company's implementation efforts is shown in Figure 5.

The company's goal was to implement a faster, secure, cost effective means for remote connectivity when away from the office for its own employees to gain access to email and file servers located at the company headquarters. The company implemented an L2TP/IPsec based secure VPN over the Internet as a solution. The use of L2TP required a public key infrastructure (PKI) to issue computer certificates to the VPN server and to clients so that the Internet Key Exchange (IKE) authentication process could take place.

7. Solution Design and Implementation

The solution design and implementation followed a 6-step Systems Planning & Implementation methodology consisting of Opportunity, Feasibility, Sponsorship, Logistics, Acceptance, and Assessment phases. This model provides added responsibilities and extends the role of Systems Planning & Implementation, which has traditionally (and demonstrably and tragically rather ineffectively) been largely limited to Logistics. The methodology seeks to enable IT systems implementations that are simple and deliver good results on time and within budget. The 6-phase cycle is detailed next.

8. Step 1: Opportunity

The company used in this VPN example creates and hosts web-based software that provides affordable online, after-sales support capabilities to medium-sized businesses and divisions within large corporations. It has about 80 employees and has been in business for more than three years. As a software development company, the company saw it was mission critical that there be security in and outside of its physical structure. Threats were seen as cumulative, and present in and outside of the organizations' physical domain. The company writes and maintains its own software, and must maintain the code under version control while making it available to several software programmers. The company like any other also hosts sensitive data of its on the network, for example software release schedules, bug reports, their customer lists and their sales leads, competitive analyses, and financial cash flow information. By nature of its business contracts, the company also hosts several of their customer's customer lists, contract schedules, geographic coverage, and help desk volume and issue tracking information. Security is zealously safeguarded. For example, the central server room housing the firewall, servers, routers and switches is temperature controlled and is kept cool by secured sensors. Closed circuit TV monitors log personnel access to the room and all activities within the room. Access to the various company departments is restricted by area. Access is negotiated via security cards. The cards are programmable and provide access based on company policy and the Principle of Least Privileges (Anderson, 2001). Security and activity reports are generated and reviewed to identify usage patterns and unauthorized or malicious activities. Desktops and laptops use a combination of Windows NT and Window 2K as the base operating system. User authentication and access to corporate network resources is based on a login and password that grants permissions based on a written company policy based on the Principle of Least Privileges.

The network supports a total of about seventy users at any given time. Fifteen to twenty users can be remotely connected simultaneously. The network is monitored and supported by a help desk team of six individuals who field trouble tickets. The team rotates in and out field service call and telephone bank service calls. A Cisco 2600 router with extended ACL (Access Control List) filtering provides access to the Internet over a 24-channel T1. An ISO Layer 3 switch is located between the Cisco 2600 series router and the firewall to direct traffic to the company's web page. On the internal network is 10/100Mbit switch connecting the NT4.0 Random Remote Access Server (RRAS) to the network. The RRAS was reaching the end of its hardware and software life cycle, and was expensive and troublesome to maintain. The company was making corporate-grade monthly payments and often per-minute long distance connect fees to the local telephone company for more than a dozen dedicated telephone lines committed exclusively to the RRAS modem bank for employee dial-up access when at home or on the road.

Between the external and internal switch the company had an underutilized ISA (Integrated Services Architecture) firewall running on a dual-homed Windows 2K operating system. Internet Security and Acceleration (ISA) in its integrated mode provides secure, fast, and manageable Internet connectivity. ISA Server includes an extensible, multilayer enterprise firewall featuring security with packet-, circuit-, and application-level traffic screening, stateful inspection, integrated virtual private networking (VPN), smart application filters, transparency, and secure server publishing. ISA Server also monitors access and usage and can alert the network administrators to attacks.

The company's Information Systems Manager realized that the company would benefit from considerable savings, higher end-user satisfaction, and added functionality by migrating its dial-up modem bank to the available ISA server. The Information Systems Manager then undertook the feasibility phase of the project to address issues related to the technological, economic, and organizational capabilities and limitations of the systems migration she envisaged.

9. Step 2: Feasibility

1. Technological Feasibility: The Manager of Information Systems and an assistant researched the ISA software vendor's internet website. They reviewed and discussed the benefits and disadvantages of various available VPN connection and configuration options, as detailed above. For example, they soon realized PPTP offered no encryption (RC4 and 128 bit DES not being supported by their vendor), whereas IPSec offered the encryption but at the expense of added administrative and configuration burdens.

To ensure successful and secure VPN communication the best solution would be to configure the ISA Server and clients to use L2TP and the IPSec/ IKE protocol in combination with ISAKMP / Oakley Key Determination protocol to perform a two-phase negotiation. IPSec peers perform certificate-based digital signature authentication during Main Mode negotiation. IKE module uses CryptoAPI to retrieve the certificate chain that will be sent, verify peer certificates and certificate chains, check certificate revocation, and create and verify digital signatures. All certificate, certificate chain, and digital signature information is exchanged in a so-called Main Mode. Main Mode messages use the following authentication method:

Main Mode Message	Sender	Payloads
1	Initiator	Security Association (contains proposals), Vendor ID
2	Responder	Security Association (contains a selected proposal), Vendor ID
3	Initiator	Key Exchange (contains Diffie-Hellman key), Nonce
4	Responder	Key Exchange (contains Diffie-Hellman key), Nonce, Certificate Request
5 (encrypted)	Initiator	Identification, Certificate, Certificate Request, Signature
6 (encrypted)	Responder	Identification, Certificate, Signature

By sending the Certificate Request payload, each IPSec peer is specifying to the other IPSec peer that, for authentication, it will accept only a certificate from an issuing CA that can follow a chain back to a CA in the list of trusted root CAs. When submitting a certificate, each IPSec peer uses the CryptoAPI to retrieve a certificate chain from its local certificate store. Each

IPSec peer must have the private key for the certificate and the certificate must follow a chain back to one of the listed trusted root CAs that are sent by the other IPSec peer in the received Certificate Request payload. The certificate chain (without the root certificate) is inserted into a Certificate payload and sent to the other IPSec peer. Each IPSec peer also includes a digital signature in the ISAKMP Signature payload, providing proof that the submitting IPSec peer has access to the private signing key of the submitted certificate.

Certificate authentication is successful when each peer verifies the other peer's certificate and digital signature. The list of trusted root CAs is not configurable for L2TP over IPSec connections. Instead, the trusted root CA list sent in the Certificate Request payload of Main Mode messages 4 and 5 contains the trusted root CAs for which a corresponding computer certificate is installed. For L2TP over IPSec connections, the IPSec peers must have computer certificates issued through a common trusted root CA, or by using cross-certificates that allow the client and server certificates to be trusted by each other. Each peer must be able to build the trust chain using the other peer's certificate to its own machine certificate root CA.

2. Economic Feasibility: Because the ISA server was already installed and available, no investment in new hardware was needed. The existing 24-channel T1 providing the company's connection to the internet also would not have to be upgraded. No other hardware or software licensing fee expenses were identified. The labor investment for the implementation and deployment of the VPN was estimated at about 80 man-hours. Some of these hours were seen as providing the added benefit of training. The savings from the disconnected phone lines and associated long distance charges would pay for the labor cost within a month. The increase in user satisfaction from the added reliability and convenience of the VPN approach was recognized but not quantified. Because the company was already reimbursing remote employees for their home ISP costs, the VPN, no additional end-user costs would be incurred.

3. Organizational Feasibility: Budgeting and the help desk phone staff played a critical role in defining the issues. In reviewing call logs the help desk observed an ongoing sizable trouble ticket history, and of late a noticeable increase in RRAS related calls. This was brought to the attention of the Information Systems manager. The budgeting department also reviewed phone service cost cutting measures to determine if any additional saving were available.

10. Step 3: Sponsorship

The IT manager outlined the issues and presented the proposed solution to the company president. In reviewing the cost associated with the project the return on invest (ROI) far outweighed the implementation cost. The president sent out a company wide email announcing the project and his support for of it.

11. Step 4: Logistics

The project was also used as a training opportunity for one of the company's employees. The logistical phase of the project was completed in one week. The only resource expenses consisted of the man-hours invested by the project lead and an assistant. No added hardware or software purchases were needed. The company took advantage of its previously underutilized infrastructure. The IT manager and the project lead had the authority and responsibility to

implemented the various stages of the VPN solution. The actual VPN implementation work was completed according to the following work schedule:

- ? 1 day of implementation research
- ? 1 day for project implementation
- ? 1 day to build the test environment
- ? 1 day of testing
- ? 1 day for deployment

The configuration of the VPN ISA server was presented earlier.

A connectoid was used to configure the remote end-user stations. A connectoid is a dial-up connection profile. The connection profiles allow a user to dial out (or really have the computer dial out) to a number of local Internet connection points (ISP's) such as Earthlink or a local Internet service provider (ISP). The connectoid is small enough to fit on a floppy disk the user can carry around with when out of town, and then quickly add to any available computer. By setting up a new connection in each location on the go, the user can roam to over 1300 locations nationwide (in the case of Earthlink) and connect to the functionality of the corporate network at headquarters with no extra connection or roaming charges.

The connectoid automatically creates a Dial Up Networking connection with all the settings necessary to get online. End-users do not have to worry about DNS Settings, gateways or other complicated network settings. It even sets up the mail software such as Outlook, Outlook Express, Netscape Messenger and some versions of Eudora with the proper mail settings so that all the user needs do is click send and receive over a secure internet transmission, without long distance toll costs or the need to support a dial-up modem bank and associated phone lines and telephone company charges. Users that connect to an Internet service provider (ISP) decrease connectoid logon time by specifying only those services and protocol that are necessary.

12. Step 5: Acceptance

The company employees were already functioning within an organization wherein technological change is constant, and the breath of technology changes every nine to eighteen months.

The remote configuration of the end-user connection was distributed to employees on the day of deployment by using floppy disks containing a small file (the connectoid) that automatically configured the end user's workstation to support a remote VPN connection. No employee training was needed beyond telling the user not to use the inbound dial-up phone lines anymore, and instead supply a login name and password when prompted by the connectoid.

The project was welcomed and well-received by the remote end-user community, most of whom were technically sophisticated. Remote users with prior experience with using connectoids were reconfigured. New users were configured for remote access and given a

demonstration using the connectoid. A set of additional internal network traffic reports were generated to monitor any changes in network traffic patterns and server loads arising from the new VPN implementation.

The project was well received by the end-user community primarily for two reasons.

- ? The overall technical knowledge of the end user was already moderate to high, and so required negligible downtime and training. In a larger organization with remote users not technically knowledgeable, more training would have been required.
- ? A faster and more reliable and trouble-free connection was obtained from a local connectoid thus increasing network speed and end-use satisfaction with the setup.

13. Step 6: Assessment

The original objectives of the VPN initiative were to implement a faster, more reliable, and more cost effective means for remote employees to have easy and convenient access around the clock and from around the world to email and file servers located at the companies headquarters. These employees included those who were traveling on behalf of the company and who had to connect from a hotel room or from the customer's premises, or yet those who sought to work from home offices on weekends to meet project deadlines, perform maintenance chores, as a personal accommodation, or under flextime arrangements. The biggest concern was not to sacrifice the security of the corporate network in the process.

In the end the company improved employee productivity and personnel morale, and also realized a considerable savings in recurring monthly phone line and timed per-minute connect charges. Help desk trouble-ticket maintenance headaches associated with dial-up connections were also eliminated.

Even in the face of the added VPN network traffic and associated security traffic encryption and decryption and key exchange cycles, the company did not have to increase its bandwidth from its existing 24 channel T-1. Network performance as measured by the connection of the company to its ISP via its T1, and on the internal network was not degraded by the VPN key validation and encryption traffic or added network load from remotely connected users. The VPN implementation was completely transparent to users on the network.

The company did experience considerable savings in its telephone long distance charges. It disconnected several internal dedicated and 800-numbered telephone lines that had been incurring sizable monthly telco service charges and premium per-minute connect charges. No having had to make any investment in hardware or software, the company recouped its project investment in the way of employee implementation and training man-hours from the difference in the payment due amount of the next telephone bill from the telephone company compared to the previous month's bill. The need to support expensive dedicated and 800-number international, national, and regional numbers to its own employees virtually disappeared.

Network speed and the user's sense of satisfaction with the VPN setup was improved for several reasons. The user's added sense of ownership of the process was enhanced by connecting

through their own ISP, the physical and mental isolation and separation of user connectivity problems from corporate network access problems, and the increase in reliability and performance of the connection because dial-up connections were made locally and not long-distance. For example, the same PC with the same modem often connects to the same corporate telephone number at different rates, not just from different locations, but from the same location. This is particularly important when phone connections had to be made from overseas, and from international hotels, where international communications costs are typically prohibitively expensive and subject to house surcharges. This variation typically left the end-user with the impression that the corporate network had problems and was at fault. In reality, telephone line quality (cross-talk and attenuation) and the physical distance to and from the telephone company central office, measured by physical distance and the total number of telephone switches traversed to close a phone circuit are factors that critically affect how fast and reliable a dial-up connection to corporate will be. Once the phone circuit is established and the long-distance call armed, the quality of the transmission however good or poor is set for the duration of the call. With a VPN solution on the contrary, the quality and performance of the connection is determined by the number of individually dropped packets on the network and the latency, jitter, throughput, and available bandwidth of the network infrastructure, all elements which change on the timescale of milliseconds. The exposure and dependence on the quality of the telephone connection circuitry is limited to only from the user's dial-up workstation at home or in a hotel room (invariably through a PBX) to their local telephone company. The overall network performance would be determined by slowest point in the network, typically the end-user's asymmetric connection via a 56kbps downstream (33.6kbps upstream) for connections through an ISP that supports digital downstream traffic, and a symmetric 28kbps (typical) for users in hotel rooms who have to traverse an internal hotel PBX with an analog phone cross-over card bank (the typical setup).

Importantly, end-users with xDSL or internet-enabled cableTV hookups, and those connecting through their customer's corporate internet link (typically a T1 or even a T3) would not be limited to the availability of an analog phone line at the customer's premises (one typically supporting one of the customer's fax machines), and much less to the limited 56kbps downstream, 33.6kbps upstream dial-up phone connection. For them the dial-up 56kbps/33.6kbps bottleneck was replaced by the much faster connection (for example 384kbps downlink speeds for xDSL, fast enough to support quality audio and compressed video transmissions).

Implementing VPN/L2TP allowed for greater security connecting remotely through the Internet. The enhanced security of a VPN connection hides sensitive data from Internet users, but makes the data securely accessible to appropriate users through the VPN connection. Because TCP/IP is the backbone networking protocol for the Internet, the corporate software applications application supporting TCP/IP could be accessed remotely and securely via a VPN connection the same as at the office.

The VPN is encrypted so the address used for connection is protected. Internet users can only see the external IP address. This is helpful for organizations with nonconforming internal IP addresses, requiring no administrative overhead associated with change IP addresses for remote access via the Internet.

14. Conclusions

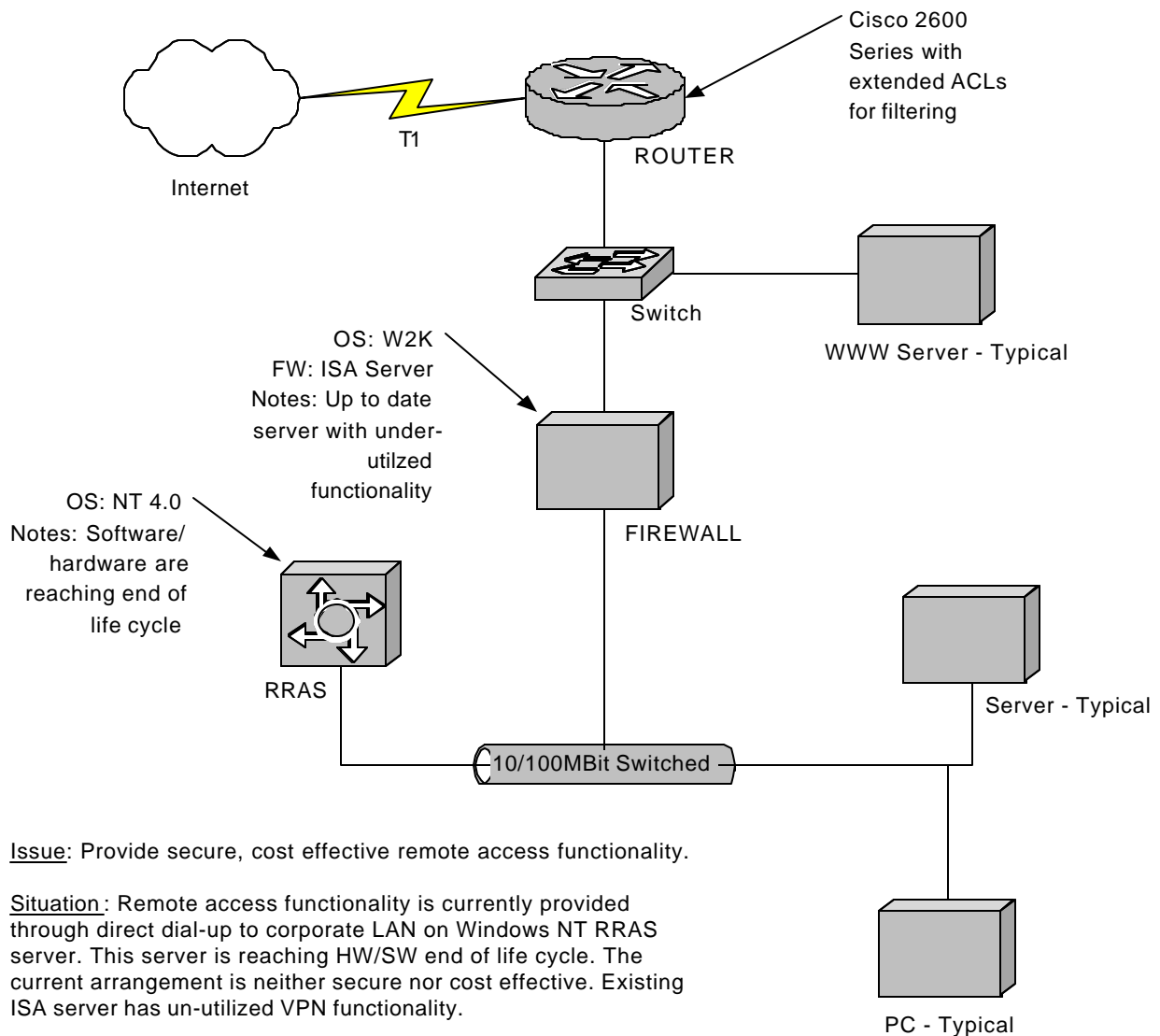
The VPN described in this should be of service to any organization seeking a solution to security related issues when connecting remote end-users to sensitive company data over the Internet securely and inexpensively. The VPN solution provided an internet-based secure connection at a fraction of the cost of the dial-up system it had been using, and with a great measure of added reliability, performance, and end-user satisfaction.

From a project standpoint, the VPN implementation detailed in this study was a success for the following reasons:

1. The opportunity to serve a need was from the outset clearly identified, quantified, and validated;
2. The economic, technological, and organizational feasibility of the project was carefully considered before project initiation;
4. Sponsorship from management in the way of a mandate (balancing authority and responsibility) and a sentient allocation of resources (budget, staff, and timeframe) was obtained before project initiation.
5. The logistical implementation followed an action plan that included modular testing.
6. The acceptance of the solution was obtained by participatory buy-in.
7. A quantitative assessment of the gap between the outcome and the initial objectives was conducted.

15. Acknowledgements

The authors would like to thank the company that recently implemented the VPN described in this paper for generous access to their senior and operations staff, their VPN, and their VPN project documentation, as well as the reviewers for helpful comments.



Issue: Provide secure, cost effective remote access functionality.

Situation: Remote access functionality is currently provided through direct dial-up to corporate LAN on Windows NT RRAS server. This server is reaching HW/SW end of life cycle. The current arrangement is neither secure nor cost effective. Existing ISA server has un-utilized VPN functionality.

Solution: Retire outdated NT RRAS server and implement VPN server functionality on existing ISA server.

Challenges/Strategy: Need buy-in from mgmt. Show significant hard cost savings that are returned immediately, and implementation costs are low.

Costs: Planning and configuration time estimated at 5 days.

ROI: Soft costs - reduced administration of resources. Hard costs - long distance telephony costs, hardware and licensing costs not required to update existing system.

Result: Costs associated with deploying new hardware and modems for RRAS server, as well as new licensing costs for OS are avoided. Long distance costs are eliminated. Secure remote connectivity to multiple concurrent users is provided.

LAN Info

Users total: 70
 Simultaneous remote users: 15-20
 OS: Mix of NT and W2K

Figure 5. Layout of security access L2TP/IPSec VPN solution as implemented.

16. References

- Anderson, R., Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2001.
- Fratto, M., VPNs. Network Computing, 10/04/99, Vol. 10 Issue 20, p 60.
- International Standard ISO/IEC 17799:2000, Information Security Management, Code of Practice for Information Security Management. Available at <http://www.iso.org/>. See also "International Standard ISO/IEC 17799:2000 Information Security Management, Code of Practice for Information Security Management Frequently Asked Questions, December 2001" available at <http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf>. Last viewed October 20, 2002.
- International Standard ISO/IEC 15408-1,2,3:1999, the Common Criteria for IT Security Evaluation. Part 1: Introduction and general model; Part 2: Security functional requirements; Part 3: Security assurance requirements. Available from <http://www.iso.org/>
- King, C. M., Remote Access VPNs: Selection And Deployment Issues. New England Review, Summer 2000, Vol. 21 Issue 3, p. 52.
- Malik, O., "Sargasso Sea: The telecommunications industry won't recover before 2004." Red Herring, August 13, 2002. Available at <http://www.redherring.com/insider/2002/0813/briefing-broadband081302.html>. Last viewed October 20, 2002.
- NIST Handbook 800-12. An Introduction to Computer Security: The NIST Handbook Special Publication 800-12. National Institute of Standards and Technology Administration, U.S. Department of Commerce. Available at <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>. Last viewed October 20, 2002.
- Poore, R.S., "GASSP - Generally Accepted System Security Principles." © Copyright 1996, 1997, 1998, 1999 by the International Information Security Foundation (I2SF). Available at http://www.auerbach-publications.com/dynamic_data/2334_1221_gassp.pdf. Last viewed Oct 20, 2002.
- Seltzer, L., VPNs Come Of Age. Internet World, 08/15/2000, Vol. 6 Issue 16, p 34.
- Nemeth, E., Snyder, G., Seebass, S., and Hein, T.. UNIX System Administration Handbook, Third Edition. © 2000 Prentice Hall PTR
- Thyfault, M. E.; Larsen, A. K., Global Push For VPNs. InformationWeek, 05/17/99 Issue 734, p 26.
- Tiller, J. S., Security of Virtual Private Networks. Information Systems Security, Mar/Apr2001, Vol. 10 Issue 1, p18.
- Wirbel, L., Carriers step forward as VPN service providers. Electronic Engineering Times, 09/18/2000 Issue 1131, p 24.