NetCare
The knowledge behind the network
Lucent Technologies
Bell Labs Innovations

Virtual Private Networks: How They Work

By Roger W.Younglove, CISSP
Senior Network Systems Consultant, NetworkCare Security Services, Lucent Technologies

VPNs, IPSec, PKI, and SLA are buzzwords that everyone is using, and lists of these acronyms are a mile long. In fact, an *InternetWeek* survey of 200 IT managers found that 29% of those surveyed were currently using a VPN, while the remaining 71% were 6 months to one year or more away from deployment (*InternetWeek* VPN supplement, September 13, 1999). Those 29% have had to learn how a VPN works either the hard way by building it themselves, or the easier way by contracting a managed service from a service provider (SP).

Cost is usually the determining factor of whether the VPN is built in house or is contracted out. Cost per connection for a service is weighed against the total equipment, training, maintenance, and management costs spread over the number of connections required for a VPN built in house. Another important consideration is who maintains control of the equipment. Some companies do not use contract services, regardless of cost, because they want full control over the VPN.

What is required to construct a basic VPN? A tunneling protocol and a means to authenticate that tunnel origin. This is not always simple, since a choice must be made between one of two tunneling protocols: Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP). The major tunnel protocol used for the enterprise VPN is IPSec, while L2TP is typically utilized by SPs to provide remote dialup VPN access for customers. The benefit of L2TP remote access is that it uses PPP for encapsulation and does not require installation of an extra package on the remote client. This article focuses on enterprise VPNs.

IPSec (RFC 2401) with additional RFCs 2402/2412 for codifying the essential components has become the de facto industry standard for an IP-based VPN infrastructure. Following the successful pattern of other Internet services, IPSec developed organically over time. In March 1993, the swIPe Experimental Protocol was written; in July 1994 IPSec was defined as a mandatory protocol for IPv6; and in August 1995 RFCs 1825-29 were written. The present RFCs superseded the originals in November 1998. IPv6 has IPSec built in, and when it is fully deployed, it will render the current IPSec implementation methods obsolete.

IPSec supports two different topologies in IPv4: client implementation and gateway implementation. The client implementation is referred to as the bump in the stack (BITS) because it is inserted between the IP stack and the local network drivers. Since source code access for the IP stack is not required, this implementation approach is appropriate for use with legacy systems. It can be installed in Windows 95, 98, and NT; Macintosh, and Unix operating systems, depending on the specific vendor implementation. When Windows 2000 is released, it will have Microsoft's implementation of IPSec built in. It will be applicable for remote access or for supplying a secure network within a LAN, such as in a finance department with multiple personnel spread throughout a large enterprise network and a secure communication requirement for a client/server application. In this case, one would implement BITS on every client and server.

The gateway implementation is referred to as the bump in the wire (BITW) because there is a piece of equipment running IPSec on the edge of the network being protected. The gateway implementation may be in software or hardware. An example of a software implementation is IPSec running on a firewall or router. An example of a hardware implementation is an appliance running IPSec in silicon (black box), which is much faster because of the lack of OS overhead. A VPN requires at least one gateway implementation at the central site or the remote LAN, and a client implementation for each remote site (road warrior or single PC site).

Multiple vendors provide gateways and client implementations. In the implementation of an extranet VPN (Automotive Network eXchange®), equipment from multiple vendors is implemented. To ensure interoperability, the ANX® designated ICSA in September 1998 to verify interoperability of IPSec vendor equipment. (Visit www.icsa.net for test configurations used and other information.)

The IPSec protocol provides tunnel authentication and encryption. Since IPSec was designed to be algorithm-independent, several acceptable options of encryption and authentication algorithms are supported, allowing an optimal choice to be made for a specific VPN's required security level. For authentication, the supported algorithms are HMAC MD5 (normal usage) and for a higher level of security authentication, it is HMAC SHA1 (FIPS-180-1). Encryption algorithms are DES, 3DES, RC5, Cast, Idea, and Blowfish, with others being added. DES and 3DES are mandatory, but not all vendors support additional encryption algorithms, so if a higher level of encryption is required the individual vendors' products must be researched.

IPSec was designed so that once an encryption algorithm is chosen, the actual keying material used by the algorithm can be regenerated inside the tunnel in a requested time frame (once every hour, each 10Mbs, etc.) to change the session keys, effectively changing the encryption. Therefore, even though DES has been broken in less than 23 hours, it is still usually acceptable for use if the session key is automatically changed every hour. Even if the tunnel data is intercepted and subjected to a brute force attack, only one hour of data would be compromised.

We have mentioned the various algorithms for authentication and encryption and have stated that IPSec is algorithm independent, which allows IPSec VPNs to have various levels of security. But how do you know what algorithms to use when setting up an IPSec tunnel with a new company? The company may advise you to initiate the connectivity or designate your preferred algorithms in the implementation. Negotiations to find the highest level of encryption algorithms that both endpoints can use take place during the authentication negotiation phase prior to the tunnel setup. If one endpoint does not meet the other's minimum encryption requirements, the tunnel is not set up.

Different implementations of IPSec offer a variety of authentication methods, including shared secret, token cards or digital certificates. Shared secret is fairly easy to utilize for a small number of endpoints (clients and/or gateways). Token cards work very well for large intranet implementations, but for a large extranet implementation the easiest method is to use a digital certificate (Public Key Infrastructure).

A Public Key Infrastructure (PKI)starts with a Certificate Authority (CA), a software package operated in a high security area, that issues digital certificates. It also includes a directory service to make the certificate widely available. When implementing a PKI, you can either contract for the service or implement the operation in house. The decision to contract or purchase must be based not only on cost, but more importantly on security policy and requirements. Do you have full control of the PKI or do you let some one else operate it for you?

Besides a CA, a PKI also includes, at minimum, a X.509v3-compatible database. The CA operator issues the digital certificates to the end entity (EE)—IPSec endpoints in this case—and records the information in the database. When a certificate is either compromised or is no longer correct for some reason, it is listed by the CA operator on a Certificate Revocation List (CRL). Each time an IPSec endpoint checks the validity of a certificate that is presented for authentication, it checks the CRLs to see if that certificate is listed. If the certificate is listed, it is no longer valid and the IPSec endpoint will reject it.

If you implement a PKI, you should write a Certificate Policy (CP) regardless of whether you operate or outsource your CA. The CP delineates the requirements (for example, a certificate must be requested in person and requires two forms of ID, one a picture ID) to receive a certificate from the CA and/or a level of authority (for example, this certificate allows signature authority for one million dollars). For an IPSec endpoint, the CP defines what information must be submitted to the CA for certification. The CP should also specify the requirements that the CA must meet for security reasons.

To successfully implement a CA, the operator of the CA must write a Certificate Practice Statement (CPS), which responds to the CP spelling out how the operation of the CA matches the CP requirements. If you implement your own CA, you should create both the CP and the CPS. Although this might seem unnecessary since you have full control of the implementation, it is important for two reasons. First, it ensures optimal security by requiring written documents for both operational guidance and for audit purposes. Second, if you ever wish to cross-certify (that is, be treated as an equal and able to accept certificates) with a CA operated by someone else, both the CP and CPS are required to ensure that both certificates are considered equal in the required aspects.

We have now covered everything required for a VPN. Operating a VPN over the Internet is not an exact science because the Internet is not a guaranteed transport. If you do not require a guaranteed service, the Internet will provide adequate VPN transport. However, if you require guaranteed service, you can enter into a service level agreement (SLA) with a SP for your VPN transport. An SLA is a money-back guarantee that the SP will provide a specific level of service, such as overall network availability of 99.7%, end-to-end latency not greater than 150 ms round-trip, local loop availability of 99.7%, or a packet loss of less than 1% over all throughput. The agreement will dictate such terms as, for instance, a refund of one month of charges if the SP abrogates any of the agreed upon service levels.

Whether it is an intranet or an extranet, a VPN will reduce the cost of communications by replacing multiple communication links and legacy equipment with a single connection and one piece of equipment for each location.

WP.GN.VPN.1299