An overview of VPN technology

A number of diverse computing topics contribute to the subject of VPNs and this can make the subject appear daunting to a newcomer. This section seeks to provide a roadmap for readers interested in implementing a straightforward IPSec or SLL VPN with minimal background reading. A discussion of the practicalities of implementing an IPSec VPN using Windows® and Cisco® routers is provided in Section 7 along with some examples. SSL VPNs are covered in more detail in Section 8 followed by a configuration guide in Section 9. The guide finishes with Section 10 covering the configuration of Linksys Routers as IPSec wireless VPN endpoints.

Motivation

There are two general networking scenarios for which a secure VPN solution is appropriate. Both concern the extension of a LAN over existing links to the Internet.

Remote Site VPN

In this scenario, a college wishes to connect a small remote office to the main campus without investing in a dedicated leased line to link the two. Both the main campus and the satellite are connected to the Internet, for example by means of a high-bandwidth leased line at the main campus and an ADSL connection at the satellite. Inter-campus network traffic can flow between the two sites with data encryption ensuring that confidentiality is maintained.

Remote User VPN

A college may wish to offer its staff the facility to log on to the local network from their houses without incurring the expense and support burden of operating a private dial-up service. These remote users would have access using normal domestic ISP connections to the local file servers and databases that would ordinarily not be reachable from the Internet for obvious security reasons. Certificate-based authentication ensures that only approved remote computers are able to negotiate a connection.

These two scenarios have been identified in order to illustrate the main uses of the technology. The processes involved in realising either of the above two scenarios are very similar, if not identical.

Elements

A secure VPN consists of two Internet-connected devices that, after having authenticated one another, exchange data over the Internet in a secure fashion. The four processes that comprise a secure VPN are **tunnelling**, **confidentiality**, **integrity** and **authentication**.

Tunnelling

This is the defining characteristic of a VPN as it allows packets to travel to destinations that would not ordinarily be reachable over the Internet. This allows existing Internetinfrastructure to replace a dedicated intersite leased line or dial-up service. A VPN tunnel consists of two Internet-connected devices, one at either end. These tunnel endpoints both dispatch packets to the other endpoint and receive packets, sent by the peer, that are emerging from the tunnel.

In order to send a packet down the tunnel it is first placed within another packet. This has the effect of creating a new outermost IP header whose source and destination fields are filled with the addresses of the sending and receiving tunnel endpoints. When this packet is received at the far end of the tunnel, the additional headers concerned with delivery via the tunnel are stripped away and the original packet is regenerated. This mechanism can be used to dispatch two types of packet over the Internet that would, by their very nature, ordinarily be undeliverable.

Invalid Protocols

Some sites may employ network-level protocols, such as AppleTalk® or Novell's IPX (Internet Packet Exchange), on disparate LANs. The Internet, by definition, only routes IP packets and so other Layer III protocols cannot be carried in their native form. Encapsulating an IPX packet within an IP 'envelope' would permit the two campuses to use the Internet rather than private leased lines to exchange Netware traffic.

Invalid Addresses

Many sites employ IP addresses from the designated private ranges on their local networks. A college with several campuses, each using private IP numbers, could use tunnelling to allow the campuses to exchange these packets via the Internet.

There are two broad classes of tunnelling methods that work by either encapsulating Layer II frames (usually PPP (Point-to-Point Protocol) or Layer III packets).

Confidentiality

A VPN causes traffic local to an organisation to be transmitted over infrastructure that carries general Internet traffic. It is essential to guard against the remote possibility that these packets could be intercepted and examined by some third party. Data confidentiality may be achieved by encrypting the payload of any packets that are destined for the remote end of a VPN tunnel (a separation of confidential traffic from public Internet traffic by carrying it along dedicated MPLS circuits is another way of achieving that). The encryption process is a compromise between the inevitable increase in transmission delays and the strength of the cryptographic cipher employed. There are two categories of encryption algorithm and both are used to secure packets that travel over a VPN.

Symmetric

These algorithms rely upon the two security endpoints agreeing upon a secret phrase that is used for all subsequent encryptions and decryptions. Although they operate quickly, the great drawback of these encryption algorithms is that the shared key must be agreed in advance over the insecure medium. If this initial exchange were conducted in plaintext, any third party that managed to intercept it would be able to decode all the subsequent encrypted data.

Asymmetric

These algorithms do not require a secret phrase to be shared between the security peers. Each peer generates two keys, one of which (the *Public Key*) is published while the other (the *Private Key*) is kept secret. A message that has been encrypted with a peer's Public Key can only be decrypted by means of the partnering Private Key. Despite their great security, these algorithms are slow and therefore unsuitable for ongoing encryption of a stream of data such as IP packets.

A useful compromise between the speed of the symmetric algorithms and the security of the asymmetric type is readily achieved. A fast symmetric algorithm is used for securing the data stream with the shared secret (the *Session Key*) being encrypted using an asymmetric cipher. This means that transmission times for packets traversing the VPN are kept to a minimum without compromising security by exchanging the Session Key in plaintext. It is normal practice for the Session Key to be assigned a limited lifetime so that it must be periodically renewed. This further increases security, as an attacker would have insufficient time to discover the Session Key by means of some brute force attack before it expires and is replaced with a completely new key.

Integrity

It is vital that any data arriving at one of the endpoints of a VPN is guaranteed to have originated from the recognised security peer and not to have been modified en-route. Both of these assurances can be provided by use of digital signatures.

Passing a message through a mathematical function called a hash function produces a short, fixed-length digest. If even one bit of the original message is changed then a different digest will be produced. Data integrity can be assured by attaching a digest to an outgoing message. When a message that has been transmitted via a VPN is received, the recipient applies the hash function to the data that was sent and compares the resulting digest to one that was

generated by the sender and attached to the message. If the two digests differ, the recipient endpoint will know the message has been modified.

The problem with this scheme is that the sender's digest that accompanies the message could easily be replaced with one that had been calculated from the modified data. The recipient would then be unaware that the sender's message had been changed. The digest can be guaranteed to have originated from the sender by instead using a keyed hash function that uses the message and a key as the input. A symmetric hash function is one where the key is a secret phrase that the two security peers have previously agreed upon. A slower, but more secure, asymmetric hash function employs the sender's Private Key. An on-going stream of data will be authenticated using the fast symmetric variant and the key will be the same one used for the symmetric encryption. Because only the two security peers know the key, third parties will not be able change the digest and the recipient can be confident that the message has not been changed en-route from the sender.

Authentication

By introducing VPN technology into the network, servers that would otherwise be shielded from the dangers of exposure to the Internet can be rendered vulnerable. It is absolutely essential therefore that measures be taken to ensure that only approved remote stations are able to inject packets via a tunnel into the local network. Two different techniques can be used to identify approved stations.2.2.4.1 Shared Secret

A password is configured on both of the stations that are acting as the tunnel endpoints. The authentication process requires each endpoint to check that the peer's copy of the secret matches its own.

Certificate Authentication

A digital certificate is installed on each of the tunnel endpoints. Providing the two stations have been configured so as to 'trust' the issuer of the peer's certificate then authentication will occur. These certificates can either be purchased from a commercial Certification Authority (CA), or the college can configure a server to generate its own local certificates.

The scenario, as described in Section 2.1, will probably be a factor when selecting an authentication method. If a number of remote users require access to the college LAN then issuing certificates (which can later be revoked if a staff member leaves the college's employment) allows the network manager more control over who has access to the VPN facilities. For a single remote site, a shared secret is simpler as it does not require any supporting infrastructure and can be quite secure as the two tunnel endpoints can also be statically configured with the other's IP address as an additional identity check.
