Secure Virtual Private Networks

Universities or colleges consisting of multiple campuses, each with a LAN, traditionally connect geographically diverse ‘islands’ by means of private leased lines. If the connected site is small and consumes little bandwidth, the costs of such WAN links do not necessarily represent value for money. Many organisations also wish to offer their staff the facility to connect to their central network remotely, either from their houses or when travelling on business. Operating a corporate dial-up service is unattractive due to the capital equipment costs and the burden of supporting the service on home computers of unknown provenance.

For both requirements there is now an alternative to the expensive dedicated services of a true private network: a collection of technologies that can be used to construct a Virtual Private Network (VPN). A VPN carries an organisation’s private network traffic securely over networks such as JANET and the Internet. Instead of using a dedicated, real-world connection such as a leased line, a VPN uses virtual connections routed through the Internet from the organisation’s private network to the remote site or employee. This guide discusses techniques for securely extending the reach of an organisation’s network beyond the boundaries of a single physical campus by utilising existing JANET connectivity. Two examples illustrate the need for this wide area connectivity.

The technologies required to support a secure VPN exist as approved standards, and as manufacturers are now implementing these standards in commonly available products, the prospects for implementing stable VPN solutions without purchasing expensive items of equipment or additional software have never been better. However designing, implementing and running a VPN still requires an understanding of those fundamental technologies. Just as a network manager needs to understand addressing, routing and TCP/IP, a VPN manager needs to understand what makes the network tick.

A secure VPN involves:

- encryption, to ensure that private traffic sent over shared networks cannot be read by other users of those networks
- authentication, so that the systems at the two ends of the VPN can be confident of each other’s identity
- tunnelling, so that packets that would normally be contained within a single physical LAN can be carried over a WAN to reach remote segments of that LAN.

This guide brings together these diverse subject areas required to implement secure VPNs into a coherent account of the subject. The general principles of each topic are described along with the implementation of each used by IPSec and SSL, which are the most widely used international standards. Finally two practical examples illustrate the need for wide area connectivity and how VPNs can be created to provide it.

Two different sets of protocols are described in this guide. In addition to traditional IPSec-

based VPNs, SSL VPN technology has grown in popularity in recent years, largely due to the perceived ease of use and accessibility. Wherever one can gain access to an SSL website over port 443, one can gain access to an SSL VPN. There are three main types of SSL VPN:

- The **web-based portal** is accessed using any web browser and provides access through a proxied arrangement. No traffic passes directly onto the organisation's network; it is all terminated on the VPN concentrator. The portal may give access to filestore, on-campus resources, web pages and SSH/RDP, all through web-based links.
- A **Network Connection SSL VPN** provides a full network tunnel back to the home organisation over TCP port 443. This is more closely aligned with what many will immediately think of as a VPN when compared with traditional IPSec. The same concepts like split tunnel apply and policy options can define the access provided to the home organisation's network.
- Finally a **Virtual Desktop** can be provided through an SSL VPN connection: all the remote user has access to is a virtual desktop which resides in their browser window in a similar way to a kiosk configuration. This solution brings many security advantages for the session as well as the clean-up of the remote PC at the end of the session.

Secure VPNs are mostly user provisioned services according to the classification given in [2] [1] .

Links
[1] http://community.ja.net/library/advisory-services/references-0