

REMOTE CASE STUDY

The Challenge

A global organisation had basic remote access capabilities in the UK, which had not progressed from direct analogue dial-up, and Exchange Outlook Web Access only. This was causing issues and high costs for home workers and travellers, especially when overseas or in hotel rooms. The project was initiated to provide various remote access methods, allowing employees to access the IT systems of the organisation from anywhere, either via direct dial-up or preferably over the Internet. The business requirements were as follows:

- All access methods must be protected by strong security
- Connectivity must be achievable through both dial-up and across the Internet
- IT systems must be accessible from corporate devices, i.e. laptops and devices in overseas offices, and external machines such as home PCs and devices in Internet cafés

The Solution

On receipt of the business requirements, a number of remote access options from various suppliers were considered. The options were collated and a report generated detailing the solutions recommended along with purchase and ongoing costs. The solutions offered were as follows:

Security

To ensure strong protection against unauthorised access, the RSA SecurID product was recommended. This provides two-factor authentication, with something-you-know and something-you-have, the something-you-know being a four digit pin which must be remembered and the something-you-have being a tag containing a six digit number which is constantly changed on a sixty second cycle. This is recognised as one of the most secure access methods currently available and was recommended to cover all remote access methods.

Dial-Up

The previous dial-up solution utilised within the organisation comprised of a Microsoft Windows server with the in-built Routing and Remote Access service. Eight analogue lines were available through this service but this proved to be unreliable and slow.

A Cisco router with ISDN PRI capability along with the Cisco Access Control Server product was recommended. This would be capable of providing thirty concurrent digital or analogue connections with secure authentication and logging when integrated with the SecurID service.

E-Mail Synchronisation

Possibly the most important requirement was that of e-mail synchronisation for company laptops. This would be achievable through the dial-up method but access across the Internet would considerably reduce the cost and increase the speed of this facility. An Avantail SSL VPN appliance was recommended to provide simple and secure access to synchronise e-mail and to provide access to internal systems such as the Intranet and files held on company servers.

Internal System Access

The organisation already had a considerable investment in the Citrix MetaFrame product to centralise its internal systems and provide access from remote offices across the UK. It was recommended that the Citrix Secure Gateway and NFuse product be implemented to provide access to internal systems from any device with Internet connectivity. This would also be integrated with SecurID authentication, and 128-bit SSL encryption would be used to secure the traffic between the client and the Citrix Gateway.

The Result

On receipt of the formal recommendations, agreement to proceed was obtained and a project plan generated for the implementation. Hardware and software were purchased and each solution implemented with sign off and security testing at key stages. It is now possible for employees of the company to access almost any system that they require from anywhere and at a much-reduced cost. With the increasing popularity of broadband Internet connectivity at home, employees can work remotely at a fixed low cost and utilising whichever method they prefer.

To complement the companies disaster recovery plan, a backup SecurID, dial-up, and Citrix Secure Gateway solution has also been implemented into their disaster recovery site, which is a mirror of the live systems. This provides both an always-on backup to cover failure of the live system and a method for employees to work from home if a disaster was to be declared and the disaster recovery plans activated.

