

Roaming International Analysts Switch On To AEP Networks For Secure Global Remote Access

SSL VPN provides increased productivity at CRU International

The Challenge

If you are a high profile analyst, stationed in a remote part of South America who is being relied upon for valuable economic and investment advice by financial institutions or national governments, you cannot afford to be late with your reports or suffer security leaks because of ineffective IT links with your office.

This is typical of the challenge faced by the team of consultants employed by CRU, a specialist provider of independent business analysis and consultancy, focused on the mining, metals, power, cables, fertilizer and chemical sectors. Employing over 180 experts in London, Beijing, Santiago, Sydney and key centres within the United States, CRU provides reports, monitors, daily on-line news and consultancy services to customers that can include banks, financial institutions, mining and other private companies, as well as national governments that have an interest in the commodities.

CRU's experts are constantly travelling the globe, anywhere from Australia to South America, visiting mines, steel plants and other sites relevant to the sectors they are advising on. To be productive while on the move, it is essential for them to have round-the-clock, secure remote access to economic modelling and other data intensive applications as well as email and office software which is running on the company's head office network in London.

Since 2001 the CRU had relied on an Internet Protocol Security (IPSec) Virtual Private Network (VPN) which allowed its employees to remotely log on to the office network via secure Internet connections. While this remote working technology did allow the company's experts to work on the move, there was room for improvement as Manvinder Singh, Group IT Director explained:

"We were aware that our staff could be more productive if they had an easier-to-use, more reliable system – and because we are in a people business, enabling them to work faster and more efficiently would have a direct impact on the success of the company. Similarly, as a relatively small IT team, we wanted a remote working system which would be less time intensive for us to manage and support."

To use the IPSec VPN, CRU's experts first had to log on to the Internet, and then to fire up the IPSec tunnel connectivity software to create a link to the office network, entering user IDs and passwords. The connectivity software, did not always work first time and it was not uncommon for users to have to go through the process several times before being able to log on to their applications.

Added to this, the IPSec VPN did not integrate well with the Citrix platform used by CRU to run the data modelling and other software that staff relied on. The integration difficulties meant it was not uncommon for users to experience difficulties working with these applications.

Productivity was further impeded if users were stationed in a location where the Information Communication Technology (ICT) infrastructure was not fully developed, meaning that bandwidth problems could restrict access to the network.

One of the biggest difficulties lay in the fact that in general IP Sec VPNs can only be accessed from PCs which had been pre-loaded with client software for the purpose by the IT department.

"If for any reason there was a problem with a laptop used by one of our consultants from a remote location, then it could seriously affect productivity. They would not have an alternative way of accessing the network until we had managed to fix their laptop or provided them with a replacement," Singh explained. "If they were working to meet a deadline, this could cause serious problems."

Maintaining the system also placed a significant burden on the IT department:

“Every laptop had to have the IPsec VPN software pre-installed. Each time the software was upgraded we had to update each and every laptop. Frequently, to fix a problem, the software had to be re-installed. For a small IT team, which also had to handle day-to-day support calls related to the VPN, this was a significant draw on our time.”

The Solution

Working with Enforce Technology, one of the UK's leading security consultants and integrators, Singh began evaluating Secure Sockets Layer (SSL) VPN solutions. SSL VPNs, which are emerging as an alternative to IPsec VPNs, are well regarded for their flexibility, ease of use and for being simple to manage and support. They rely on the standard SSL web protocol that is designed for server authentication, data encryption and message integrity over Internet links.

SSL VPNs minimize the need to configure and maintain remote devices because they function in a 'clientless' environment, operating through Web browsers that are built into every PC. Because most users are familiar with browsers, little training and support is needed, translating into lower support costs. Moreover it is possible to log on to an SSL VPN from any PC with a browser; users are not restricted to logging on from a specific machine.

“Our main concern was that the solution that we chose would be very simple and easy for people to use - to enhance productivity,” Singh emphasized. “We also wanted to be convinced that it was secure, because our experts are often dealing with commercially sensitive data that needs to be guarded. And because users may be logging on from hardware not supplied by the IT department, we wanted to ensure we were protected from viruses and other malicious software. And of course, cost of ownership is always important.”

CRU looked at demonstrations of three different SSL VPN solutions but was quickly convinced that the Netilla Security Platform (NSP) from AEP Networks was the best option. A four-week trial with a small group of users soon confirmed that users would be happy with the environment.

“People could connect with the network from wherever they are, using a web browser. They are greeted on-screen with a familiar representation of their desktop and the system has strong security features, as well as being very intuitive and easy to use.”

~ Manvinder Singh, Group IT Director

The Result

With no software to install on users' PCs and very little end user training required, deploying the NSP was very straightforward. New users can be added in minutes and upgrades only need to be applied to the NSP appliance, rather than to each and every user PC. Right from the start, CRU was aware of the reduction in time required to manage the system.

Over a period of six months, approximately ninety of CRU's employees who work remotely had transferred to using the new system. The original IPsec VPN has been retained as a backup.

“Since introducing the NSP, ease of use benefits has been very obvious. Users can be up and running and able to access applications much faster than before. They are genuinely comfortable with it and these benefits must be translating into improved productivity,” said Singh. .

“We have also noticed a fall off in the number of calls to the support desk – freeing up time for other activity. Hopefully this is due to the system being more reliable and resilient, as well as users having fewer queries. Of course we have retained the original backup IPsec VPN, so there is also an alternative means of connectivity if they do have any problems,” Singh continued.

Part of the improvement is due to NSP's design which incorporates tight integration with the Citrix platform used by CRU.

Security is another key benefit. The NSP uses an 'application layer proxy', which means that end users never directly connect to the private side network. The NSP appliance intermediates between

the network and the end users, presenting them with a 'proxy' of the application, protecting the application servers from direct exposure to the Internet. NSP is able to apply security policy, functioning as a gatekeeper between network and the Internet. Network resources are further protected by the PKI protection built into the appliance.

Because users now have the flexibility to access applications from anywhere, using any PC with a browser, CRU is reassured by some of the additional security features on the system.

"NSP incorporates specific features which will allow us to configure it to test the integrity of any machine that is trying to access the system. This includes checking that it has a firewall and has up-to-date anti virus software for example."

The system will also provide functionality to perform a cache clean-up after each session so there is 'zero footprint' of information left on the machine for 'prying eyes' who may have access to a machine after the CRU executive.

"Confidentiality is written into our contracts with clients, so we need to be sure that we are doing all we can to protect the information that our executives are working on," said Singh.

"All in all, NSP has provided pretty much everything we were looking for. A flexible, user-friendly system that increases productivity, has strong security

features and requires minimal support. It is also very good value for the money," concluded Singh.

Looking to the future, CRU is looking at using the NSP for supplying users with a Voice over IP system allowing them to make Internet phone calls.

About AEP Networks

AEP Networks offers a comprehensive Policy Networking solution that provides complete security starting at the endpoints and working throughout a network—from the edge to the core. AEP's integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, high assurance IPsec-based VPN encryptors, and hardware security modules for key management.

Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company is headquartered in Somerset, New Jersey, with offices worldwide

Contact AEP Networks

info@aepnetworks.com, www.aepnetworks.com

U.S: 877-652-5200 x5207 • EMEA: +44 (0) 1442 458 640 •
Japan: +81-3-3432-3336 • China: +86-571-8702-2892