

## Remote Access System Helps 'Fast Track' Railway Engineering Projects

*AEP Netilla Security Platform provides secure remote access to critical design and planning systems at First Engineering*

### The Challenge

First Engineering is one of the UK's largest rail engineering organisations. It offers total solutions for the rail industry, including installing, managing and maintaining systems and assets. Its multi-disciplinary services include communications, power systems, signaling, track renewals and specialist construction work. The company's strengths lie in its ability to manage assets that are spread over a wide geographical area within a safety critical environment.

Much of First Engineering's work involves managing engineering projects for the rail industry, working with a variety of



partner companies. The projects can be located anywhere in the UK and one of the challenges has been finding ways to give the organisation's engineers and project managers the required remote access to company IT applications to enable them to work effectively.

"We had tried a variety of approaches, including cumbersome dial up systems and software based VPNs which we found time consuming to manage and support. On a basic level some of our staff were relying on web mail to keep in touch from home, or hotel rooms and wireless access while travelling - but they needed a lot more than this," explained Alan Robertson, IT Manager at First Engineering.

The lack of a satisfactory remote access technology often led to lengthy delays at the start of projects while managers collated all the documentation and

information they might need. It also meant staff did not have an effective way of collaborating and staying in touch during the course of projects.

The company needed a reliable, easy to use, remote access system that would allow secure access to Windows Terminal Server (WTS) based applications.

"Our main Enterprise Resource Planning system, IFS, uses Terminal Server and it was vital that any remote access system could work with this effectively," explained Robertson. "It also had to be scalable, allowing us to add new applications easily as well as being easy to support and simple to use. Security was a key requirement for protecting the confidential information on our network."

### The Solution

Working with systems integrator, Enforce Technology, First Engineering began evaluating potential applications, which included GoToMyPC and SonicWALL. The AEP Netilla Security Platform (NSP) was considered to be the strongest product they had tested.

---

"We found that NSP was by far the most powerful and reliable solution for working with Terminal Server. And we could see right away that it would be very easy to support and use."

Alan Robertson – IT Manager, First Engineering

---

NSP is a Secure Sockets Layer (SSL) Virtual Private Network (VPN) solution which relies on the standard SSL web protocol designed for server authentication, data encryption and message integrity over internet links. It is specifically targeted at providing easy access to WTS applications via the Internet through an embedded thin client technology.

The system's thin client proxy model means remote users interact with virtual representations – or screen scrapes – of applications, not directly with the applications themselves. The applications reside on WTS MetaFrame Servers on the main corporate network, rather than the remote PC and application processing is performed on the

corporate server. The remote machines handle only the input and output data, such as key strokes, mouse clicks and graphical display. In this way, NSP protects application servers from direct exposure to the Internet, applying security policy and functioning as a gatekeeper. Network resources are further protected by the PKI protection built into the appliance.

First Engineering worked with Enforce to conduct a four-week pilot trial of NSP with approximately 50 end users. The resulting user feedback survey was very positive and there was unanimous approval from the board to go ahead with rolling out the technology.

The system was implemented within a four week period with the NSP appliance installed at First Engineering's Glasgow head office sitting on top of the local area network (LAN) which covers 40 sites. To boost security the installation includes the VASCO two-factor authentication system, natively integrated into the NSP platform. VASCO key fobs, which must be used by all authorised remote workers, generate a security code which has to be entered as part of logging on to the system.

The organisation has installed two NSP systems, with one acting as a failover in the event of a disaster.

## Results

A quarter of First Engineering's workforce, 500 staff, have been authorised to use NSP. The applications they can access include the IFS ERP system, Primavera P3 project management and AutoCad design systems as well as email and Microsoft Office applications.

The system rollout and support has been very smooth according to Robertson: "We were really impressed with how easy NSP has been to install and use. We had to do very little end user training. We nominated regional coordinators throughout the country to agree which employees should use the system depending on job requirement. Each user was given a VASCO key fob and an eight page instruction guide to the system. Most people have found it very easy to get to grips with - working with

Terminal Server the users see exactly what they would on their desktop.

"It's becoming increasingly important for us to work closely together in client and partner offices and the NSP allows us to access all of our core systems rapidly. It often means we can mobilize our project teams up to 100 times faster when preparing for a project."

In one recent example, the NSP's remote access facilities enabled First Engineering to set up a project team in Lichfield within hours, instead of what could have been weeks, when the company was engaged by Network Rail to work on the high profile project to widen the existing railway between Armitage with Handsacre and Tamworth as part of the West Coast Mainline upgrade.

"The NSP was chosen due to the seamless integration with Windows Terminal Server and the ability to use two-factor authentication out of the box. Remote access is now simple for the end user, through Web-based access to the NSP menu system; no messing about with dial-up settings, VPN clients or modem cables."

Alan Robertson – IT Manager, First Engineering

## About AEP Networks

AEP Networks ([www.aepnetworks.com](http://www.aepnetworks.com)) 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 access control enforcement points, identity-based application security gateways, SSL VPNs, 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 worldwide. The company is headquartered in Somerset, New Jersey, with offices worldwide.

## Contact AEP Networks

[info@aepnetworks.com](mailto:info@aepnetworks.com)  
[www.aepnetworks.com](http://www.aepnetworks.com)

U.S: +1 877-638-4552 • EMEA: +44 1442 458 600 •  
Japan: +81 3-3432-3336 • China: +86 136-4626-0288