

Secure Remote Working

Are We Virtually There Yet? An AEP Networks White Paper

Introduction	1
The State of Remote Working Today.....	2
SSL VPNs as a Primary Tool for Remote working	3
<i>“Thin Client” Access to Server-based Applications</i>	4
<i>Web Reverse Proxy for Web Applications</i>	4
<i>Network Layer Access to Client/Server Applications (Layer 3)</i>	5
Section 3: Remote Working In Action: U.K. District Councils.....	6
Contact AEP Networks	7

Introduction

Has remote working's golden moment finally arrived?

Remote working – also known as teleworking, telecommuting or flexible working – is an elegantly simple idea that has taken a surprisingly long time to germinate. Remote working's promise is that it can save an enterprise (be it commercial or government) significant time, money and resources for an employee to work regularly from home rather than travel to an (often distant) office. Remote working can also contribute directly to greater employee productivity and satisfaction by letting home-based workers accommodate domestic needs such as caring for a sick child, attending to home repairs or juggling school appointments.

But for many years, the concept of remote working has had to confront some ingrained (and increasingly inaccurate, thanks to advances in technology) prejudices that have slowed its acceptance. One is the idea that employees, once outside the office, cannot be counted on to have the focused approach to work that occurs naturally within the workplace. Another is the idea that remote working deprives home workers of the face-to-face interaction and problem-solving that takes place at work. But perhaps the biggest perceived stumbling block to remote working is the idea that the technology does not yet exist to provide a worker with access to the full resources they have at the office – the computer-based applications, files and data that today are at the heart of many work environments.

This white paper will deal largely with this third assumption – and will attempt to demonstrate decisively that the technological tools *do* exist that can give a home-based worker secure access to all of the critical files and applications they enjoy at the office. Some statistics: more than 91 percent of UK households have access to broadband Internet connections; and there are now more than 6 million broadband users in the UK, with over 60 thousand new subscribers per week.

Today's SSL VPN (Secure Sockets Layer Virtual Private Network) technology from AEP Networks and other vendors leverages that installed base of infrastructure. By deploying an SSL VPN appliance, enterprises can enable their remote or mobile workers to securely access all of the applications and files they use in the office. Work in progress can be completed, new jobs begun, new applications started – regardless of the employee's location.

One of the greatest benefits of SSL VPN technology is that because it is user-based, not device-based, an authorised user can login from any Web-enabled PC. No longer is it necessary to carry a laptop from office to home or on the road; the necessary authorisation is obtained through a Web portal accessible from anywhere. And today's SSL VPNs incorporate powerful "end point integrity" subsystems to ensure that the enterprise network is protected from viruses and other threats that may reside on home PCs outside the company's control.

Simply put, SSL VPNs have quickly become the technology of choice that is enabling many companies to provision their workers with the ability to work from anywhere, without any compromise in functionality, accessibility or performance. And because they rely on already-deployed Web technology such as browsers and SSL encryption, the cost of these systems is far less than older, non-Web-based VPNs such as IPSec-based systems.

While remote working remains attractive for all the reasons outlined above, it should also be recognised that Web-based systems for working remotely can be of strategic importance when unforeseen events arise. Recent news headlines are impossible to ignore:

**HUNDREDS OF THOUSANDS HOMELESS IN HURRICANE KATRINA'S WAKE;
BUSINESSES FORCED TO RELOCATE**

**U.S. GASOLINE PRICES SOAR TO MORE THAN \$3.50 PER GALLON: DRIVERS
LOOK FOR ALTERNATIVES TO LONG DAILY COMMUTES**

**LONDON SUBWAY BOMBINGS LEAD TO RANDOM SEARCHES OF COMMUTERS
IN LONDON, NEW YORK, ADDING TO TRAVEL DELAYS**

These news stories bring a sharp new focus to one incontrovertible fact: Emergencies, whether natural or manmade, cause disruption to our social fabric and can inflict huge economic losses as governments, businesses and individuals struggle to adjust and recover. During such times, the fact that some or all of an enterprise's employees are equipped to work from home – with no special requirements other than a username and password to access the SSL VPN – can be a small yet significant factor that helps economic and business activity continue or reassume, even when it may be impractical to get to the office.

The State of Remote Working Today

Remote working is clearly on the rise – although precise statistics can be difficult to come by. Organisations such as the Telework Coalition (www.telcoa.org) and Innovations Canada (www.ivc.ca) are useful sources of information on remote working.

Consider these facts:

United Kingdom:

A British government employment survey, sponsored by Department for Trade and Industry, reveals working from home has risen to over 28% of workplaces since 1998.

Key findings of the 2005 RAC Foundation study in the U.K.:

- Over 70% of working mothers in the UK would like to work flexibly or from home at least some of the week
- Women now work half a day longer than five years ago - an average of almost 34 hours a week.
- Asked what they would like for Mother's Day more than six out of ten asked for more time to spend with families.
- The number of remote workers in the U.K. grew to 2.2 million in 2001, or about 7.4 percent of the total workforce. Of these, 1.8 million could not do their jobs without a computer and phone. That number reflects rapid growth: the total number of remote workers in the U.K. grew by 65 to 70 percent between 1997 to 2001. (U.K. Department of Trade and Industry)

U.S.

The International Telework Association and Council (ITAC) estimates 23.5 million employed Americans worked from home during business hours at least one day per month in 2003. JALA International, in association with ITAC, forecasts over 40 million teleworkers in the US by 2010.

CNN Report (January 2005): The results of a survey of 1,286 technology experts found that 56% believe telecommuting and home-schooling will expand, blurring boundaries between work and leisure, and affecting family dynamics.

The U.S. Census Bureau reports that nearly 4.2 million people worked at home in 2000, up from 3.4 million in 1990. This 23 percent increase in home-based workers age 16 and older was double the growth in the overall workforce during the decade.

In fact, this increased acceptance of remote working was also one of the clear findings of a survey of remote workers conducted by AEP Networks in April, 2004. The AEP Networks Flexible Working Survey 2004 canvassed commuters at two teeming transportation hubs – New York City's Penn Station and London's Liverpool Street Station. The survey found that 77% of the 165 people surveyed would jump at the opportunity to work from home if their employers offered it to them and that 86 percent felt that having the choice to work either at home or in the office was the ideal setup.

Stress, quality of life and enhancing relationships with their partners were the key factors for most workers keen for the chance to work remotely, with 80% claiming that it would

make their job less stressful and 74% convinced that it would enhance their relationship with their partner.

One woman respondent said she was certain that it would perk up her love life as she'd at least have the energy to spend quality time with her husband if she didn't have to endure such long hours and her daily commute. Over half of the commuters admitted that they felt long hours affected their relationship adversely, with one man saying his long hours at work is the reason he's getting a divorce.

While the survey found that commuters on both sides of the Atlantic are strongly in favor of the option to work from home some interesting differences also emerged:

- Only 67 percent of U.S. commuters felt that the remote working option would make their jobs less stressful, compared to 84 percent of the British commuters surveyed. Several American respondents noted that since they were managers, they felt they needed to be in the office to supervise employees.
- 81 percent of U.K. commuters surveyed said that flexible working would enhance their significant-other relationship, while 52 percent of U.S. commuters did.
- 87 percent of American commuters said they would miss the office social life if they worked from home all the time, while only 80 percent of British workers said they would. One U.S. commuter said he would miss the "intellectual capital" gained from interactions in the office.

SSL VPNs as a Primary Tool for Remote working

It's clear from the above discussion that remote working is on the rise, with no signs of slowing down. But before teleworking can realise its full potential, technologies that are instrumental – such as SSL VPNs – need to be widely deployed by organisations and made available to those employees who need to access their applications and data from outside the office.

For example, AEP Networks' AEP Netilla Security Platform (NSP) is an SSL VPN that provides remote access to the widest range of corporate applications, using a Web browser as a ready-made access client. As a dedicated network appliance, the NSP integrates into existing network and security designs seamlessly by offering rapid deployment, easy installation, minimal maintenance, and high security. With the NSP, remote users need only a computer and a Web browser to access virtually any business application on the corporate network. This approach leverages the global reach of the Internet for streamlined delivery of business-critical information to partners, suppliers, and employees, with strong security, privacy, and network protection. Such a system is tailor-made to meet the needs of teleworking employees and the organisations they work for.

The NSP differs from other SSL VPN solutions by providing the choice of three application-access technologies in a single gateway device:

- | | |
|---------------|--|
| <i>Thin</i> | ❑ Layer 7, application gateway access to applications residing on Windows Terminal Servers, Unix/Linux servers, and mainframe or AS/400 machines |
| <i>Web</i> | ❑ Web Reverse Proxy access to web-based applications and intranet portals |
| <i>Tunnel</i> | ❑ Layer 3 (network-layer) access for any TCP/UDP-based applications via SSL tunnelling |

AEP's ability to elegantly integrate such a broad level of application flexibility into single security appliance architecture greatly distinguishes the NSP from competitors. Because many organisations have a broad range of applications that need to be remotely accessible to remote workers, this versatility and broad application support becomes a key benefit.

“Thin Client” Access to Server-based Applications

Applications residing on centralised Windows, UNIX/Linux, mainframes and AS/400 machines form a vital core of the business applications used today. The challenge facing enterprises is to leverage these crucial applications in way that allows remote users to safely and simply access these resources over the Internet.

The NSP solves this dilemma, providing remote access to remote applications by incorporating Web-enabling technology directly within the platform. This integrated approach, unique to AEP among SSL VPN vendors, eliminates the need for enterprises to deploy and maintain server-based “middleware” — such as Citrix Secure Gateway — or remote-access clients, such as those required by IPsec approaches.

In the NSP’s thin access model, the NSP initiates a session to the application server on behalf of the user, and presents a rendering of the session to the user’s web browser. This allows the user to interact with the application as if it were installed locally.

An example using Microsoft Outlook is shown below.

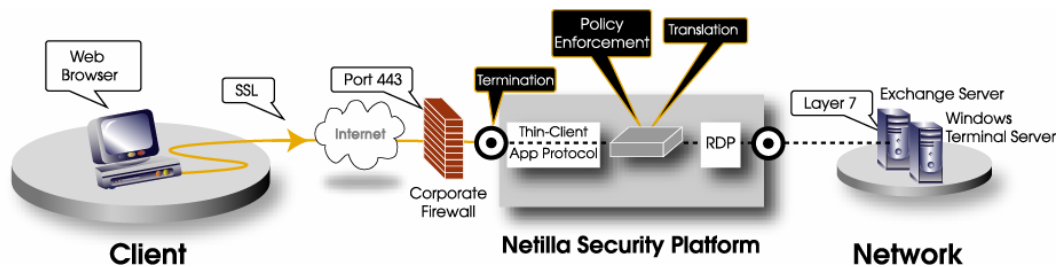


Figure 1: Thin Access to Outlook

As Figure 1 shows, the NSP “intermediates” the connection between remote-client requests and the network server, terminating incoming connections at the application layer. Once the incoming request is terminated, the NSP processes and translates the data to the appropriate backend application protocol – in this case, RDP for the terminal server, which presents the Outlook application to the user.

AEP’s thin access mode supports applications residing on Windows, UNIX, Linux, mainframe and AS/400 servers. By incorporating remote printing, client drive mapping, and file access, this approach effectively recreates the main office environment from any authorised computer.

Web Reverse Proxy for Web Applications

In addition to thin application access, the NSP also provides browser-based access to Web-based resources using Web reverse proxy technology. With this approach, a single point of entry over the Internet – the NSP itself – lets remote users access back-end, intranet Web servers securely through a Web browser.

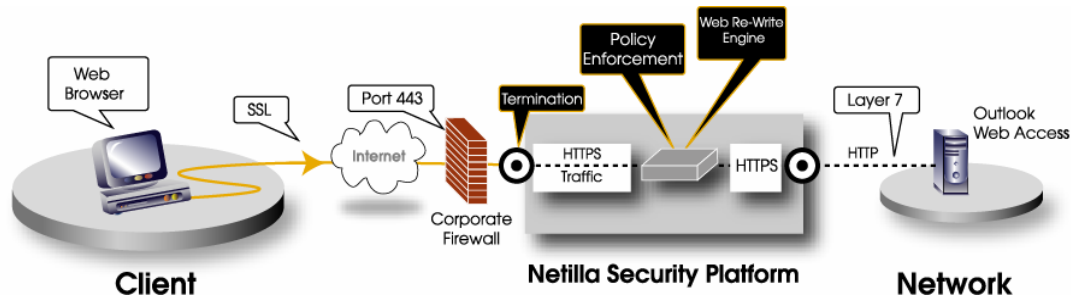


Figure 2: Outlook Web Access Through Reverse Proxy

As shown in Figure 2, a similar proxy approach used for Thin sessions is also well suited for Web-based intranet applications and portals. In this case, the NSP terminates, examines, and rewrites HTTP requests. Remote users are then presented with Web-application resources as allowed by corporate-defined security policy. For more complex web applications, such as Citrix Web Interface (formerly NFUSE), the NSP employs a sophisticated Java applet re-write module, allowing smooth presentation of these applications.

Authorised remote users thus gain instant, clientless access to a wide range of internal Web applications from any location, allowing internal DNS addresses that do not resolve publicly to be accessed securely over the Internet. This approach is ideal for enterprises that need to make their growing list of Web-enabled applications remotely accessible to telecommuting employees.

Network Layer Access to Client/Server Applications (Layer 3)

The third access mode option supported by the NSP allows access to client-server applications that require synchronization directly with the corporate server. The NSP provides this data transfer over a Layer 3 SSL tunnel, which is accomplished by using the browser as a conduit to install a virtual adapter. The virtual adapter negotiates the secure SSL tunnel via the user's Web browser to the NSP, where each of these SSL tunnels is terminated as a PPP interface. Policy may be applied to these interfaces using the NSP's integrated stateful packet inspection (SPI) firewall, facilitating a policy enforcement point similar to the NSP's other access modes. In a teleworking environment, this option is best suited for teleworking employees with the necessary applications already installed on their computer; network-layer tunnelling allows the local application to exchange data with the enterprise's central servers.

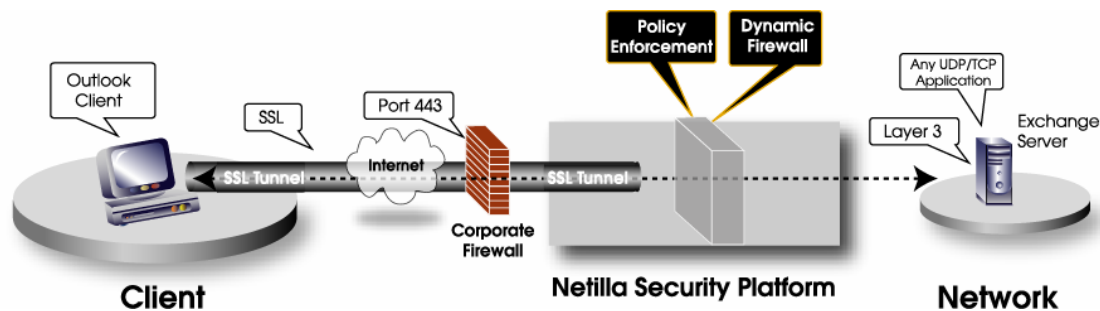


Figure 3: Client/Server Access Over Network Layer Tunnel

As shown in Figure 3, the NSP allows for applying dynamic policy over the layer 3 SSL tunnel. In this mode, the NSP's dynamic firewall is used to open and close specific ports. For the duration of each session, the administrator is able to grant access only to the Exchange server if required.

Endpoint Integrity: Ensuring Corporate Security Compliance

Protecting your network from outside threats is always a concern; such dangers grow larger when opening up your network for access from various locations outside of your IT department's control. Before you allow road warriors, partners and telecommuters to connect to your corporate network you must ensure against digital leakage and other

threats. That's why some SSL VPNs such as the AEP Netilla Security Platform offer an integrated endpoint security solution, with the flexibility to assign client integrity features for just those users who require it. The NSP, for example, offers Host Integrity, Adaptive Policies, a Secure Desktop and cache cleaner, session timeouts, and other crucial security solutions to protect your network.

Section 3: Remote Working In Action: U.K. District Councils

We have seen the growing awareness of, and demand for, flexible working solutions that enable workers to accomplish much of their work from their home PC or laptop. And we have seen how SSL VPN systems such as those offered by AEP Networks can provide the secure technological foundation for providing access to all key network-based resources via the Web – not simply email. Now, it will be helpful to review the rapid adoption of SSL VPN technology to enable flexible working in one industry segment: municipal district councils within the U.K.

First, the big picture: A government requirement for ambitious efficiency gain savings of £6.45bn by 2007/08 (as set out in the 2004 Spending Review) is one of the main factors driving the boom in local authority investment for secure remote application access technology and North Norfolk District Council is just the latest of a growing band of councils ready to go live with their SSL VPN-based flexible working solution.

According to the Society of IT Management (Socitm), since 2000, councils have spent some £2.5 billion on eGovernment projects, supported in England by £675m of ODPM central funding, and the government is now demanding that councils generate significant ROI on that investment.

Shipments of SSL VPN products have experienced a rapid increase, particularly in the U.K. Behind this surge is the fact that more local authorities are coming to realise that the UK legislative requirements to consider requests from parents to work flexibly from home, or on the move, actually provide a better fit with their future service delivery strategies of delivering services 24/7, anywhere within a Council's boundaries (even a client's home), rather than the traditional framework of centralised office based staff. Easy-to-use Web-based SSL VPN technology that is fast and secure -- and facilitates both mobile and tele-working – can enable councils to meet those savings targets.

"Demand is red hot in the local government sector as word has got around that there are real benefits to offering flexible working to staff, Members and external service providers. Within a very short time councils are seeing a return on investment as well as a great boost in staff morale," explains David Riley Director of Marketing for AEP Networks.

A survey of European public sector managers says the average public sector IT budget in 2004 increased by 6%, three times the growth rate in the private sector. Forrester Research identified one of the key areas the money is being spent on is virtual private networks, with 30% of public sector organisations considering introducing such networks, while 18% are already using them.

These figures have been backed up by the large number of local authorities who have taken on secure remote application access from AEP Networks. A partial customer list includes: Wigan Metropolitan Council, North Wiltshire District Council, Mole Valley District Council, Hambleton District Council, Staffordshire Borough Council, Wigan Metropolitan Borough Council, Newcastle City Council, Cherwell District Council, Dorset City Council, Lancaster City Council, Dundee City Council, South Lanarkshire Council, Ipswich Council, Limavady Borough Council and Rochdale Metropolitan Council.

Traditionally remote working has been sold on the benefits of reduction in office space requirements and saving of travelling time, however the recent launch of the national Project Nomad on 10th February 2005 gave a hint of some of the real benefits to come from the technology, as one case study on integrated assessment for residential and non-residential care where clients needs are assessed and records updated electronically in their homes reported:

- Process time savings of 29%
- Average office based time reduced by 47%
- Phone calls querying assessments have dropped from around 80% to around 1% of cases
- Payment process and collection enhanced – client acceptance of charge during visit avoids large retrospective bills

An early adopter of the technology was North Wiltshire District Council, which uses a Netilla Security Platform from AEP Networks to support home-working for key staff. The Council was keen to provide flexible working for staff in the benefits assessment office, following an alarming increase in staff turnover.

"The network allows home-workers to access the full range of council applications, together with email, the intranet and the Council's computerised telephone network. In some cases, productivity has risen by more than 20%," said Dave Lovelock, the Council's ICT Strategy and e-government officer. "It also requires no IT support and you can add new users in minutes."

North Wiltshire is also extending the network to allow key suppliers access for remote diagnostics and troubleshooting.

The IT director of another U.K. district council commented: "The main reason for choosing the AEP Netilla Security Platform is that it is an ideal secure black box solution, you configure it and away you go – it's simple for the users to use, and if there are any problems they get resolved quickly."

This district council initially ran their pilot with 60 early-adopter employees and are now commencing the general roll out to a broader base of users. Out of 3,500 LAN-connected users, it is anticipated that the SSL VPN will be used by up to 1,100 users. The only prerequisites for the service are a key fob for security and a broadband connection.

Towards the end of the pilot period, this council carried out a questionnaire with 60 of the early adopters to find out whether they wanted to continue with the remote access system. There was an overwhelming hands-up. The council's IT director noted, "It is rare to introduce a new solution that doesn't draw some kind of criticism from some of the staff. "

"Netilla is fab!" "Savings on phone bills and IT costs." These were just a few comments made by the district council's staffers once they'd experienced remote working enabled by Netilla Security Platform from AEP Networks.

Contact AEP Networks

Corporate Headquarters	Government Solutions Group
AEP Networks 347 Elizabeth Ave., Suite 100 Somerset NJ 08873 Toll-Free: 1-877-638-4552 Tel: +1 732-652-5200	AEP Networks 40 West Gude Drive, Suite 200 Rockville, MD 20850 Toll-Free: 1-800-495-8663 Tel: +1 240-399-1200
Europe	Asia-Pacific
AEP Networks Focus 31, West Wing, Cleveland Road Hemel Hempstead Herts HP2 7BW U.K. Tel: +44 1442 458 600	AEP Networks 2107 Tower 2 Lippo Centre 89 Queensway Hong Kong Tel: +852 2845 1118
Japan	
JOYO Bldg 6-22-6 Shimbashi Minato-ku Tokyo 105-0004 Japan Tel: 81-3-3432-3336	

© AEP Networks, Inc. All rights reserved. The AEP Networks Logo is a trademark of AEP Networks, Inc., with registration pending in the U.S. All trademarks or registered trademarks mentioned in these documents are property of their respective owners. www.aepnetworks.com
info@aepnetworks.com