

## LOCK YOUR WINDOWS! USING SSL VPNs TO SECURE MICROSOFT TERMINAL SERVICES AND CITRIX METAFRAME ENVIRONMENTS

*An AEP Networks White Paper*

### Executive Summary

---

*The majority of business applications in use today run on Windows platforms—either as native Microsoft® Windows® Terminal Services (WTS) or in conjunction with Citrix® MetaFrame Presentation Server™. There are clear business benefits to the server-based/thin-client computing environments that these technologies enable. Employees in remote offices or on the road can easily access Windows applications and files via the Internet as if they were working in the main office.*

*From an IT cost and resources standpoint, installing, managing and maintaining applications from centrally located servers offers huge advantages over deploying applications on hundreds and in some cases thousands of individual remote devices. Organizations can reduce IT support costs while providing business-critical applications and information to a wide array of users. This server-based, thin-client environment can deliver a fast return on investment and reduce ongoing IT costs significantly.*

*Yet providing effective security for Windows and Citrix applications – particularly when opening such resources for remote access over the Web – remains a central challenge. As threats to security grow and more mobile users need access to data and applications from remote locations, the need to protect IT resources only increases. In addition to protecting valuable information resources, organizations must comply with new government regulations that include far-reaching security and privacy requirements. In fact, many of the advantages inherent in server-based computing may be mitigated by threats to data privacy and integrity, particularly when access occurs over the public Internet.*

*This white paper will describe the challenges and explain why the AEP Netilla Security Platform (NSP), an SSL VPN from AEP Networks, delivers the most effective solution for secure access to WTS and Citrix MetaFrame environments.*

## The Challenge: Security Concerns

Server-based computing is well suited for onsite access to applications and data. But organizations today often provide access to these resources for users over the public Internet. These users encompass employees in remote offices, telecommuters, business partners and consultants, extranet partners and many others. Maintaining security over these resources – particularly when access occurs from locations outside of the IT department's control - is critical. Companies must find ways to provide secure access to server-based data and applications, even while making these resources more easily available. That includes ensuring that only authorized users can gain access to specific applications and information, and that they are using these resources in appropriate ways.

Unfortunately, neither native Windows Terminal Services nor Citrix MetaFrame applications are by design secure for access over the Internet. As a result, protecting these computing environments is expensive, complex and difficult to manage.

Both WTS and Citrix MetaFrame servers reside on the Windows operating system, and one of the big security challenges in recent years has been how to harden the Windows platform so that it's not so vulnerable to security breaches—particularly for servers in the Demilitarized Zone (DMZ) or other security zone for public access via the Internet.

The solution to Windows security weaknesses frequently is to employ careful application of patches, leading to management issues and costs that can easily get out of control for large organizations with extensive network requirements. For many companies, providing security in this environment is risky and a high-cost, high-maintenance undertaking.

The solution to Citrix security has historically required the complex, resource- and server-intensive Citrix Secure Gateway for MetaFrame (Secure Gateway) software, requiring multiple servers and a battery of costly implementation services. Recently, Citrix has attempted to collapse the assorted elements of Secure Gateway into an appliance called Citrix Access Gateway (CAG). Yet the CAG appliance is lacking in security and expandability features – it was eliminated from the Network World's December 2005 SSL VPN testing for its lack of proxy technology, for instance - and lacks third party validation and security accreditations such as ICSA and VPNS. Citrix themselves have indicated that CAG is not recommended for enterprise deployment.

Native WTS and Citrix also lack the cryptographic protection needed to counter the growing technical sophistication of intruders. Such environments are not easily set up to employ PKI solutions such as server-side certificates, and as a result they are subject to man-in-the-middle attacks, in which an intruder is able to access and modify messages between two parties without either party knowing that the link has been compromised. These attacks rely on convincing two hosts that the computer in the middle is the other host, which can be accomplished through techniques such as domain name spoofing.

## The SSL VPN Solution

Fortunately, the emergence of SSL VPNs offers a simpler, safer, and less costly alternative. SSL VPNs such as the AEP Netilla Security Platform (NSP) provide the protection organizations need when creating server-based access environments for WTS and Citrix applications, while adding a wide range of deployment features that allow companies to extend their application infrastructure with a surprising level of ease. SSL VPNs overcome many of the drawbacks of remote access IPsec VPNs and provide additional benefits to organizations, delivering an application-layer approach to securing WTS/Citrix in distributed environments.

SSL is a standard Web protocol that provides server authentication, data encryption and message integrity over TCP/IP links. It has become the de facto standard for supporting transactions such as online credit card purchases and banking. These VPNs minimize the need to configure and maintain remote devices because they function in a "clientless" environment, operating through the Web browsers that are built into every PC. Because of users' familiarity with browsers, little training and support is needed, which also translates to lower operational costs.

Taking this clientless approach one step further, the NSP distinguishes itself from other SSL VPNs by providing easy access to WTS/Citrix and other applications via the Internet through an embedded thin-client technology. In this model, the applications that users access reside on WTS or Citrix MetaFrame servers located in the main corporate network, rather than on the remote PC itself.

With this thin-client proxy model, application processing is performed on the server in a corporate data center, while the user's machine handles only the input and output data such as keystrokes, mouse clicks, and graphical display. Users interface with virtual representations of applications through screens, not directly with the applications themselves. But the application works just as well as it would if it were installed directly on the user's PC.

**AEP Thin-Client Proxy: The Highest Security for Extranet, Home, and Kiosk Access**

When integrated into an SSL VPN appliance like the NSP, this thin-client computing model represents the most secure methodology for accessing WTS and Citrix applications over the Internet. It is a far simpler and more complete solution than Citrix Secure Gateway or Citrix Access Gateway, and it adds critical layers of security that are not available with native Terminal Services.

In this arrangement, the NSP uses an “application-layer proxy” (the appliance generates a proxy or representation of the application), so remote users can access different applications through native protocols such as Remote Desktop Protocol (RDP) data for Windows-based applications. One advantage is that the user only has to launch a Web browser to access any applications he is authorized to use, regardless of their location or platform.

Security is another benefit. As shown in Figure 1, the NSP intermediates the connection between remote-client requests and the network-based application server, terminating incoming SSL connections at the application layer in the NSP appliance, located in the DMZ. Once the incoming request is terminated, the NSP translates the data to the appropriate application protocol, such as RDP for the terminal server/Citrix server. During this termination period the NSP is able to apply security policy, functioning as a gatekeeper between the Internet and the private network.

It is this crucial security benefit – unavailable with native WTS or Citrix deployments – that distinguishes the NSP from competitors. In this application-layer proxy model, the end user never directly connects to a “private side” network resource; instead, the NSP functions as a proxy, protecting application servers from direct Internet exposure.

In a WTS/Citrix remote access environment, this approach affords a number of benefits:

- For Citrix, secure workstation-to-MetaFrame communication is made possible without using Citrix Secure Gateway and Web Interface (NFuse). Instead, MetaFrame servers remain shielded behind the NSP which proxies the traffic on behalf of the user
- Windows Terminal Servers can be pulled back from the DMZ into the private network, eliminating patch management concerns
- Network resources are further secured by the PKI protection built into the SSL VPN appliance.
- Users gain secure access to specific applications based on policy, and are unable to access or even view the wider network
- Eliminates the risk of viruses, worms and other exploits from passing from the end user to the network
- The NSP streamlines deployment to remote endpoints. The only requirement on the workstation is a Web browser, plus the associated, downloadable Java applet
- End point integrity concerns are also addressed, providing the crucial elements of a secure desktop environment, Client Machine ID authentication and session trace removal (cache cleaning)
- The NSP’s Universal Printing eliminates the headaches typical to a WTS/Citrix environment with a low bandwidth / high compatibility solution
- The NSP adds key productivity features, such as client drive-mapping, single-application publication, and server load balancing, along with session timeouts, reporting and logging, and session monitoring.

*Capping Citrix with the NSP*

Another benefit accrues from simplifying the deployment. For example, even if an organization relies on Citrix MetaFrame applications, users can still “talk” RDP to the Citrix server, because Citrix is a service that runs on a Terminal Server. In this way, the NSP enables an organization to “cap” its Citrix deployment and instead deploy AEP thin-client technology to provide access for new remote users to the same applications that they use in the office, rather than having to expand Citrix further.

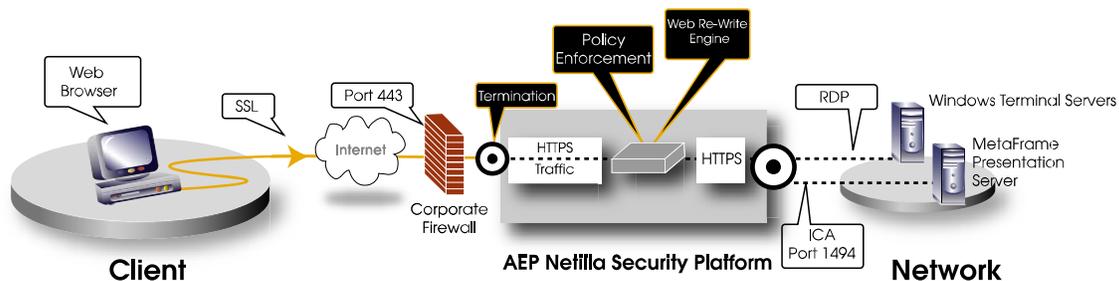


Figure 1: Thin Client Proxy for Windows and Citrix Applications

### AEP Intelligent Port Forwarding: Access for Native Clients and Corporate-issued PCs

Organizations that prefer to use the Microsoft native RDP client or native Citrix ICA client, and whose user base typically accesses the network via corporate-issued machines and are employees of the company – can use AEP Intelligent Port Forwarding. This technique, shown in Figure 2, involves automatically delivering a Java client that sits on a remote Windows machine and looks for the TCP port or ports that a particular application uses. As soon as data starts to flow, the client encapsulates and encrypts all the traffic in SSL and forwards it to the NSP gateway at the enterprise side of the network, where it can be deciphered and delivered to a terminal server.

The NSP provides access to such environments with a clever automatic “client push.” When a user connects to the network for the first time, the NSP can package a Java applet that contains everything that particular client needs in order to connect to the network applications, whether they are running via Citrix (Java, ActiveX or Native clients) or via a RDP client. Administrators therefore do not have to send each user disks to install a driver onto the machine, and end users are not required to do anything other than click an icon; the NSP provides the appropriate client seamlessly and without administrative hassles.

The NSP appliance supports the full Win32 Citrix ICA client via application-layer intelligent port forwarding technology, so users who already have the Citrix ICA client resident on their machines can access MetaFrame resources from any location. The NSP can provide access directly to the MetaFrame servers themselves (without requiring Citrix Web Interface), further cutting costs and management. The AEP appliance also enables organizations to avoid using Citrix Access Gateway, the Citrix VPN appliance that is severely lacking in security features and capabilities.

Port forwarding often meets the security needs of many organizations. Note, however, that many SSL VPN competitors must rely on 100% port forwarding to access remote applications, rather than offering the NSP’s application-layer Thin proxy model for the highest level of security. Port forwarding translates from one incoming TCP port to another, providing no opportunity to segregate public- and private-side data streams. This means that data passes through the SSL VPN appliance with limited policy enforcement opportunities, creating a point-to-point connection from end user to application server, a potential security liability.

The NSP addresses this situation by offering administrators the flexibility to choose when to use port forwarding on an “as needed” basis. This “intelligent” port forwarding solution means that only those components that cannot be re-written are port forwarded – such as ActiveX and other dynamic HTML elements, often as a part of a Web application – while everything else can be secured via Web Reverse Proxy or AEP’s unique Thin Client technology.

### Web Portal Security: Defining Policy and Access Rights

SSL VPNs like the NSP allow network administrations to create custom access portals to specific applications as defined by policy. This means that different users gain access to key application depending on their role, or requirement. Network resources are not exposed to the entire user base: Administrators can set user permissions and policies to limit access to specific applications for specified users as needed. For example, some employees who work directly with billing applications will be presented with just those applications upon sign-in. Others, who may be affiliated only with the engineering department, will be limited to “seeing” only their necessary applications. The NSP provides this functionality through seamless interaction with policy servers located in the network infrastructure. These include LDAP, Microsoft ActiveDirectory, and others. Likewise, a wide range of authentication options are

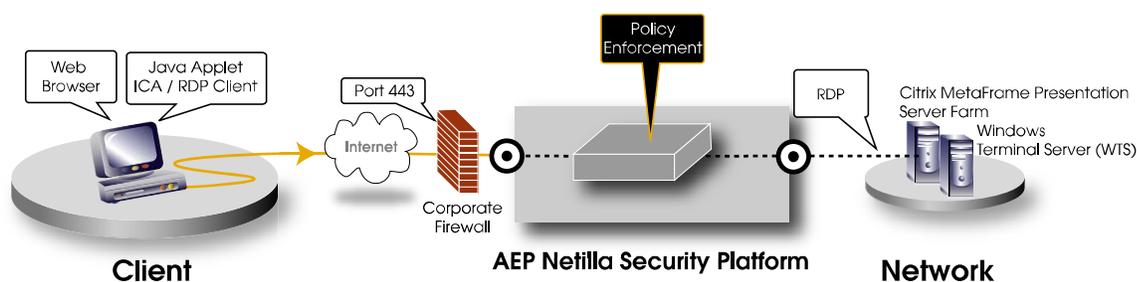


Figure 2: Port Forwarding for Citrix and Terminal Services

also supported, including integrated support for RSA, VASCO, RADIUS, Novell Directory Services (NDS) and more.

Another major advantage of the NSP is that it gives organizations the flexibility to custom-tailor access environments based on users' needs. Some users require access to Citrix applications while others need to gain access to WTS natively. Some need Outlook Web Access and others the full Outlook client. The NSP supports all these various access requirements with a seamless access environment that suits the various needs of an enterprise.

### The NSP in Action: Customer Case Study

The Abilene Independent School District (ISD) in Abilene, Texas, is using the AEP SSL VPN to provide secure access to Windows applications for thousands of students. The school district deployed the gateway in 2004 and is seeing significant benefits, says Martin Yarborough, chief technology officer for Abilene ISD.

Students using desktop and portable PCs in classrooms, libraries and their homes can access a variety of applications including Microsoft Office, Adobe and school-specific multimedia applications such as standardized testing and textbook software. The applications are accessible from 40 Windows 2003 Terminal Servers located within the district.

One of the biggest benefits of the system is that it enables Abilene ISD to give students access to the applications they need without having to install the software on each device, Yarborough says. "We're not putting software on PCs anymore," he says. "We're buying thin clients and converting existing PCs to thin clients. And we know students are getting the same version of the software at home that they get at school."

The result has been less need for IT support, resulting in savings of thousands of dollars per year, Yarborough says. "The technical support savings is phenomenal in terms of time and people costs," he says. "We don't need to hire additional staff to maintain the growing number of PCs" or to install new software.

Ease of use is another benefit of the NSP. Because the SSL VPN is browser-based, students "never even know they're using it," Yarborough says.

The Abilene ISD had considered using Citrix to provide secure access to Windows applications, but opted for the AEP approach. "We felt that the NSP gave us the same or better performance at a much reduced cost," Yarborough says. "If this was a Citrix installation we'd need to have a person dedicated to Citrix. And the fact that NSP is clientless makes a significant difference."

### NSP: The Secure Solution

SSL VPNs – and the NSP in particular – represents an outstanding choice to secure server-based computing environments. The technology supports endpoint security, adaptive policies, client machine identification, and client integrity scans. It offers a FIPS-validated solution and is an ICSA Labs certified appliance. Application auto-launch, an automatic "client-push" technology, a single-click, icon-driven access portal, and reporting and logging features round out the robust solution. And by offering additional application access modes, including a secure Web Reverse Proxy for web applications and network-layer connectivity over an SSL Tunnel, the NSP offers a solution that can grow with needs.

Leading industry publications have recognized the NSP's performance and capabilities. The product received the "Best VPN Solution Award" at the SC Magazine 2005 Product of the Year Awards. And the NSP received top scores for application redirection in the interoperability section of the NetworkWorld SSL VPN Test conducted late in 2005. NetworkWorld tested the NSP and products from other vendors against four of the most common client/server applications used as part of SSL VPN deployments: WTS, Citrix Presentation Server, Telnet and SSH.

"The clear winner in this space is AEP's Netilla Security Platform," NetworkWorld reported. "In this particular case, our choice of applications was particularly fortuitous because it showcased AEP's thin-client technology, arguably the strongest part of its product."

In the final analysis, SSL VPNs offer tremendous value as secure application gateways, offering a far simpler, safer, and less costly approach than traditional access alternatives. The result is a powerful tool - one that delivers a high level of flexibility for network administrators, who can arm their remote users with a wide range of applications based on changing conditions and needs, while protecting the company's critical business assets.

## Contact AEP Networks

[info@aepnetworks.com](mailto:info@aepnetworks.com)

[www.aepnetworks.com](http://www.aepnetworks.com)

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	
European Headquarters	Asia-Pacific	Japan
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	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](http://www.aepnetworks.com) [info@aepnetworks.com](mailto:info@aepnetworks.com)