

Securing Microsoft Terminal Services

AEP White Paper for Series A



Securing Access to Microsoft Terminal Services

An AEP Series A® Solution Summary

As threats to security grow and more mobile users need access to data and applications from remote locations, the need to protect IT resources increases. 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. It's no surprise that SSL VPNs continue to be the favored method of minimizing these threats by providing policy driven secure remote access to application servers.



Windows Remote Desktop Services (RDS) reside on the Windows operating system, and one of the greatest 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.

And, with employees in remote offices, telecommuters, business partners and consultants, extranet partners and many others requiring network access, maintaining security over these resources – particularly when access occurs from locations outside of the IT department's control - is critical.

“Windows may be safer, but cyber-criminals still have plenty of other places to attack. And when you can hit hundreds of millions of users with a single attack, why change the game plan? So most of the worst attacks today still target PCs running Windows, whether the OS itself is secure or not.”¹

Windows RDS provides several security features. Unfortunately, these features are not robust enough for today's enterprise environments. As a result, protecting these computing environments is expensive, complex and difficult to manage. 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.

¹ McMillan, Robert IDG News Service (November 10, 2009). PCWorld. *Windows 7 May Be More Secure, But Are Windows Users Safer?* <http://www.pcworld.com/businesscenter/article/181894>



Why AEP Series A? More Than an SSL VPN

A pioneer of SSL VPN technology, Series A[®] has continued to make strides in the evolution of secure, remote application access. Series A provides the protection organizations need when creating server-based secure access environments for Windows RDS applications as well as other application types (e.g., OWA, XenApp, SSL Tunnel) with a surprising level of ease.

RemoteApp Support

Continue to use the RDS features you're accustomed to with the added security and flexibility of Series A. Series A includes support for RemoteApp programs where programs accessed remotely via RDS in Windows Server 2008, appear as if running locally.

Enhanced Universal Printing

Series A offers a universal printing option to enable clients to print documents located on a remote Windows RDS Server 2008 or 2003 to their local printers without having to install local printer drivers on the remote servers. And, without having to install Microsoft .NET Framework 3.0 SP1 as is the case with Terminal Services Easy Print. In fact, there are no client requirements at all. Not even Adobe Acrobat is needed.

Client Machine “Fingerprinting”

While nearly all SSL VPNs offer client security features such as anti-virus checks and cache cleaner capability, Series A also provides client machine “fingerprinting” to guarantee only approved computers are granted access. Combine Series A's client machine identification feature with verification of the health of the client device, and strong user authentication and you have a high degree of device and user verification prior to granting access to remote Windows servers.



Securing VDI & Other Desktop Types

The migration toward virtualization and virtual corporate data centers has increased the importance of securing this Virtual Desktop Infrastructure (VDI). Although Microsoft has added support for VDI with the latest Windows Server 2008 R2, allowing access to VDI desktops from outside the corporate network poses a security challenge. AEP Series A provides that remote access to corporate VDI desktops securely. And, Series A's native support for Windows 7, Remote Apps and Remote Desktop Connection Broker ensures that the investment made into Windows RDS technologies is leveraged outside the network in a secure manner.

AEP Series A provides the most versatile access to user desktops by delivering comprehensive access support in a single appliance. Whether you need access to a physical desktop, virtual desktop or remote desktop services-driven desktops, Series A delivers seamless, custom-tailored access to virtual and physical desktops and specific terminal services-based applications. All you need is a web browser and an Internet connection.

With Series A's MyDesktop feature, IT staff can quickly set up direct, secure access to many user desktops. Initial configuration and ongoing management via Active Directory and Series A eliminates the need to perform redundant, time consuming administration. And, users connect to their desktops securely with just one click.



Segment User Authentication and Authorization via Security Zones

Series A's security features go beyond the offerings of most SSL VPNs. With Series A's V-Realms framework, you can create security zones on a user-by user or group basis to segment user access and vary the authentication methods and access privileges by zone. This powerful framework integrates external authentication and policy structures, providing the flexibility for a variety of user situations, including extranet partners, work-at-home employees, mobile field staff, MSP customers or even internal employees located within the boundaries of the LAN. Policy is enforced before the user's traffic reaches the application server in the data center.



Figure 1: Series A's V-Realms Layered Authentication Framework

AEP's V-Realm Framework works with numerous authentication and authorization protocols, including 2-factor solutions RSA SecurID®, VASCO, and ActivIdentity, along with Windows® 2000, Active Directory, LDAP, RADIUS, and Kerberos.

Secure Access to Other Application Types: Citrix, UNIX, Mainframe

Need to provide secure access to other application host types such as UNIX or mainframe? Historically, the answer to handling a heterogeneous environment has been the implementation of multiple access methods each requiring its own client software resulting in time consuming and expensive tasks for IT staffs and usability challenges for users.

With Series A, you can secure access to all of your business applications in a single appliance (virtual or hardware). Series A is the ideal solution for efficient, all-inclusive access to mixed application server environments including Microsoft, Citrix, UNIX, Web-based and mainframe where users enjoy access to all of their applications via a single web page completely unaware of the multiple paths occurring behind the scenes.

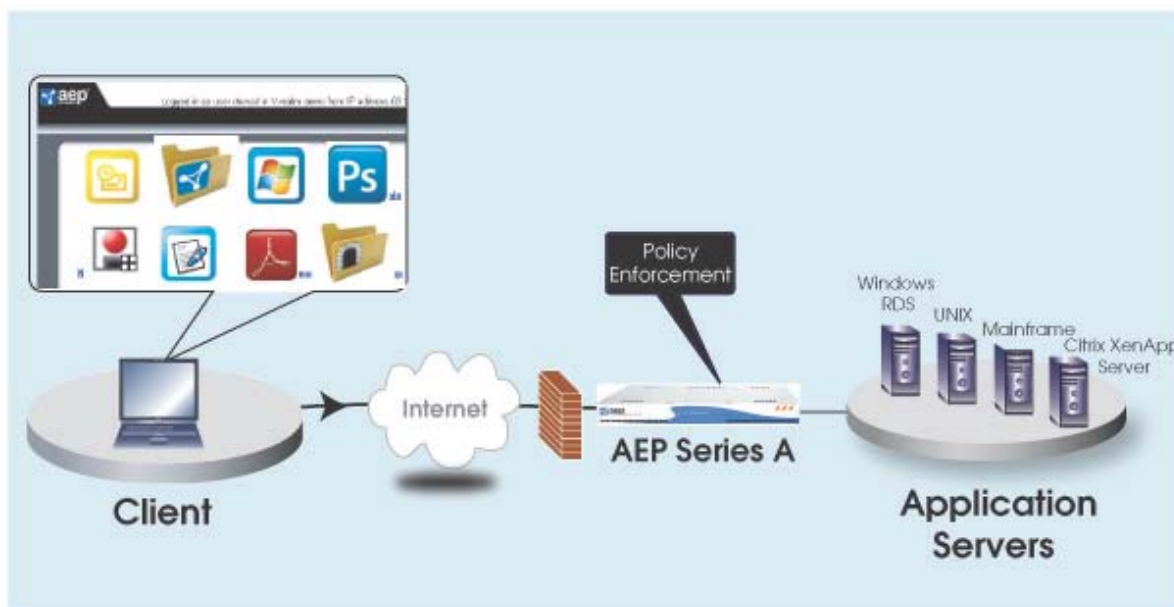


Figure 2: Series A's Universal Application Access



Comparing the Approaches

Although Microsoft offers its IAG appliance for secure remote access, is this the right solution for you? Is it highly secure? Does it provide flexible application access? Can it accommodate any type of application that may be required?

Compared to IAG, Series A offers more security, functionality and flexibility.

Microsoft IAG Product Gaps vs. AEP Series A		
Feature/Option	AEP Series A	MS IAG
Virtualized (VMware based) appliance choice	✓	✗
Series A Load Balancer option (hardware and virtualized versions)	✓	✗
Windows RDS server Load Balancing	✓	✗
Built-in support for Citrix XenApp (No additional client or server components required.)	✓	✗
Integrated VASCO server (Built in 2-factor authentication. Just add tokens)	✓	✗
Device “fingerprinting” (client machine authorization)	✓	✗
Integrated dynamic, stateful firewall	✓	✗
Highest level FIPS 140-2 option (level 4)	✓	✗
Concurrent user license model	✓	✗

Conclusion: The Most Secure, Cost Effective, Versatile Remote Access Gateway Available

Series A offers 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.