



MICROSOFT WINDOWS TERMINAL SERVICES

Integrating F5's Application Delivery Network with Microsoft Windows Terminal Services

Executive Summary

Microsoft® and F5 Networks offer a solution that helps enterprises maximize the efficiency of their networks. This joint solution provides security, high availability, scalability, and integrated management for enterprises running Microsoft Terminal Services. This solution takes advantage of the BIG-IP® product's unique Windows Terminal Service persistence feature, which provides an efficient way of load balancing traffic and maintaining persistent connections between Windows® clients and servers that are running Microsoft's Terminal Services.

The BIG-IP product's Windows Terminal Server (WTS) persistence feature provides an efficient way of load balancing traffic and maintaining persistent connections between Windows clients and servers that are running Microsoft's Terminal Services service.

The WTS persistence feature strengthens the integration of the BIG-IP solution with Windows Server platforms. Not only does the BIG-IP efficiently load balance and maintain persistent connections between Windows clients and servers, it also performs health monitoring for Windows servers that are running various services. For example, the BIG-IP health monitoring feature provides useful data on CPU, memory, and disk utilization of Windows Management Interface (WMI) servers, to ensure the most efficient load balancing of traffic to those servers. Also, the BIG-IP product provides service checking for servers running Microsoft SQL Server (versions 6.5 and 7.0).

The F5 FirePass SSL VPN extends secure access to this highly available, optimally performing network to remote users. With the FirePass controller, employees or partners can access resources from any device in any location as easily and securely as from within the corporate LAN. The FirePass provides secure Web-based access to Microsoft Terminal Servers and supports automatic downloading and installation of the correct Terminal Services remote-platform client component, if it is not currently installed on the remote device.

Challenges

Without the WTS persistence feature on the BIG-IP product, when a Windows Server 2003 (running the Terminal Services service) is participating in a session directory, it maps clients to their appropriate servers, using redirection when necessary. If a client connects to the wrong server in the cluster, the targeted server must check its client-server mapping and perform a redirection to the correct server.

Allowing the increasing number of remote users access to internal resources introduces a host of new challenges. Legacy solutions such as IPSec VPNs are costly and extremely difficult to maintain. Most internal resources are often highly sensitive and confidential, so providing security is a critical component. There are requirements for allowing access to any user regardless of location, platform or operating system.

Solution

When the BIG-IP product's WTS persistence is enabled, a Windows Server 2003 device participating in a session directory always redirects the connection to the same BIG-IP virtual server, instead of directly to another server. The BIG-IP system then sends the connection to the correct Windows Server.

When WTS persistence is enabled on a BIG-IP product, and the servers in the pool participate in a session directory, the BIG-IP product load balances a Terminal Services connection according to the way that the user has configured the BIG-IP for load balancing. Thus, the use of Windows Server 2003 and Session Directory, combined with the BIG-IP product's WTS persistence feature, provides more sophisticated load balancing and more reliable reconnection when servers become disconnected.

With F5's FirePass controller, organizations are able to extend access to Microsoft Windows Terminal Services resources to their remote workforce, partners, or customers. The FirePass SSL VPN provides secured, clientless access to off-site users as easily as if they were in the corporate LAN. Once authenticated by the FirePass controller, users pass through the corporate firewall and are able to access Microsoft WTS resources without having to re-authenticate for multiple resources.

The necessary Windows Terminal Services client remote software is integrated into the FirePass device and is downloaded on demand, eliminating the need for any pre-installed Terminal Services software on the client device. This allows a wide variety of users to gain remote access to applications running on Windows Terminal Services, while lowering the management cost and complexity.

About Microsoft WTS

Microsoft Windows Terminal Services provide access to the latest Windows-based applications for client computers. IT managers and system administrators use WTS to increase flexibility in application deployment, control computer management costs, and remotely administer network resources. They use it to also provide desktop and installed application access for end-users anywhere, from any supported client.