TERMINAL SERVICES

Description of the Application

Terminal Services allow organizations to expand access to application deployments while reducing costs associated with high-powered computers, bandwidth needs and administration. In a Terminal Services deployment, enterprise applications are centrally installed on high-powered Terminal Servers and accessed remotely using inexpensive thin-clients.

Because the application processing takes place on the server, and only keyboard, video and mouse signals are transmitted across the network, organizations can benefit from using lower-power, inexpensive devices, including Pocket PCs and other remote devices, while taking advantage of greatly reduced bandwidth requirements.

Challenges to the Application Type

Deployment of server-based applications and services requires significant attention to network architecture to ensure security, access and availability. There are several challenges that need to be met to smoothly deploy and maintain Terminal Services:

Enhancing security - Terminal Servers supply access to services for use outside the boundaries of an enterprise, so securing those services is crucial. Most Terminal Services provide for some level of authentication, but that authentication takes place after the firewall has already allowed access to the network. In order to maintain the security of the entire network, terminal services deployments require solutions that can handle authentication and ensure that the terminals themselves are not compromised.

Ensuring and controlling access - In order to achieve the greatest return on investment for enterprise organizations, Terminal Services should provide secure and efficient clientless access for a variety of platforms. Terminal users need access to all types of applications and data, including web applications, email, and legacy systems. Meanwhile, system administrators need the ability to configure access to applications and data on an individual and group basis.

Providing high availability and scalability - With the possibility of an entire organization relying on a server-based application and contending for CPU time, disk access, and RAM, the ability to load balance and scale those systems is crucial to a successful deployment. Most Terminal Servers have no features to help with either high availability or scalability, and persistence is not commonly available on Terminal Servers. While some Terminal Servers have recently employed a form of persistence, it is less than ideal because of the way the session directory maps clients to the appropriate servers. If a client connects to the wrong server in the cluster, the target server checks its client-server mapping and attempts to perform a redirection to the correct server, which is often unreliable.

F5 Solution Overview

F5 Networks' products include a number of recent features that solve the challenges of using Terminal Services within the enterprise. The FirePass SSL VPN provides remote users with full access to enterprise Terminal Services from any device, on any platform, including Microsoft® Windows®, Apple® Macintosh®, Linux®, Sun® Solaris® and PocketPC®. By leveraging the browser as a standard thin client, the FirePass controller enables the organization to extend secure remote access easily and cost-effectively to anyone connected to the Internet, with no special software or configuration on the remote device. The client is not even required to be running Windows in order to access Windows-based applications. The FirePass device also enables administrators to configure group access policies and provides authentication support, including single sign-on for Windows Terminal Services and Citrix® MetaFrame® servers.

In order to ensure the highest standards of security for devices accessing the LAN, the FirePass Endpoint inspection engine provides capabilities to detect personal firewall software, anti-virus software, operating system and browser patch levels, and the absence or presence of specified processes before allowing users to authenticate to the network. The FirePass device also prevents back door attacks and accidental leakage of information through the use of unique, built-in features such as Safe Split-Tunneling, which prevents the malicious or accidental misrouting of the public network to the protected network and vice versa, and Protected Workspace, which ensures that no cached or downloaded data is left behind on the client system.

Increasing performance and ROI, the FirePass controller can provide SSL offload using proven hardware-based SSL key exchange and data encryption technology. Data compression is also available for all forms of access, including network (any IP based), portal (HTTP), and application (TCP) traffic, providing better end user performance and bandwidth savings.

Integrating F5's BIG-IP product within an enterprise solution ensures the deployment of Terminal Servers according to industry Best Practices. Enterprises benefit from the persistence and scalable capabilities of the BIG-IP product in a number of ways. The BIG-IP product functions as a virtual server (VIP), receiving and forwarding all requests to the appropriate Terminal Server. Scalability is also enhanced through the ability to add new pools or individual servers, and quickly redirect and load balance traffic to these new resources.

TERMINAL SERVICES

F5 Solution Overview - continued

When Terminal Servers include a form of persistence, it is generally only available on those specific servers. Using this form of persistence requires that every server in the pool must be of a specific type. But many enterprises also need an alternative persistence option. The BIG-IP product provides this persistence, and even allows the use of a mixed solution by creating pools for different types of servers. For example, BIG-IP provides out-of-the-box Session Directory Integration for Windows Terminal Server.

Version 9 of the BIG-IP controller also provides a suite of WAN optimization and acceleration features that enhance Terminal Services deployments. TMOS utilizes independent client and server side TCP stacks to ensure that data transmission is optimized for both the remote client and the Terminal Server. These TCP Express optimizations reduce application response time and minimize errors associated with lost and re-ordered packets, thus significantly improving end-user experience.

Benefits

Application acceleration and compression improve end user performance - The FirePass VPN controller provides data compression for all forms of network traffic, including IP-based, HTTP, and TCP traffic, improving performance for all remote users. In addition, integrating the BIG-IP solution with Terminal Servers provides a specialized Layer 4-7 architecture with superior processing power, optimizing application speed and network Quality of Service levels. The BIG-IP version 9 TCP Express features ensure that both client and server are transmitting data at the optimal rate and thus simultaneously reduce server download times and improve bandwidth link utilization for a site. These dramatic WAN optimization and client performance improvements can not be found in other networking devices.

Hardware and administration expenditure reductions result in increased ROI - For encrypted traffic, F5 Networks products provide integrated SSL encryption and decryption capabilities. Offloading processor-intensive SSL transactions from Terminal Servers greatly improves the performance of the server cluster, freeing it to fill more user requests. This solution maximizes application availability, allows for trouble-free maintenance and reduces administration overhead. By offloading SSL and persistence functions (processor and server intensive operations) customers do not have to buy expensive hardware to support their applications. The results are savings on hardware costs and increased application performance.

Simple scalability maximizes efficient network expansion - F5 products provide a highly scalable solution that allows enterprises to meet growing organizational demands on web and application resources. If one service is nearing capacity, scaling it is as simple as adding another instance of the service to your network and then to the BIG-IP load balancing pool. The FirePass controller also provides a scalable access policy management system that allows for grouping of resources. With this feature, access control policies can be defined for a group, and resources can then be added to or removed from a resource group without changing the access control policy. This approach greatly simplifies access control policy management, lowering TCO for the organization.

F5 solutions ensure high availability for Terminal Services - Through the use of its advanced health checking capabilities, the BIG-IP product can recognize when a resource is unavailable or under-performing and direct traffic to another resource. The BIG-IP product recognizes when the node is once again available, and resumes sending traffic. With the BIG-IP product, your terminal services can achieve mission-critical availability (99.999% uptime) while reducing operational complexity and costs.

Centralized security reduces management costs - In addition to best-of-breed Endpoint inspection, Protected Workspace, and Safe Split-Tunneling features, the FirePass VPN provides application layer and user level protection against malicious attacks, while email attachments and file uploads are verified by a transparent anti-virus scanner. VLAN support allows for improved logical and physical segmentation of the network based on the trust level of users, further ensuring the security of the remote-user network. The BIG-IP product comes standard with numerous security features that provide an extremely scalable, highly available, and secure solution for both internal and external applications. F5 Networks' products enable stringent access control, secure administration, and help resist common attacks. They are also the first application traffic management solution with a FIPS (Federal Information Processing Standard) 140-2 Level 2 certified cryptographic/SSL accelerator.