



MICROSOFT INTERNET INFORMATION SERVICES

F5 Helps Optimize, Secure, and Deliver Microsoft Internet Information Services (IIS)

Executive Summary

Organizations integrating F5's BIG-IP system with Microsoft Internet Information Services (IIS) 6.0 experience not only optimal availability and security but also increased performance and reliability for enterprise deployments of the Microsoft® Application Server platform, including Internet Information Services and ASP.NET. With its comprehensive feature set, including Fast Cache, TCP Express, and intelligent compression, the BIG-IP system can offload a number of different services from the IIS servers. This offloading functionality improves performance for the end user by more than 70% and frees the servers to operate as they were designed: serving content. And with F5's FirePass controller, remote users can reach IIS servers on the corporate network easily and securely from any device, in any location.

F5 provides the industry's leading set of integrated products and services to manage, control, secure, accelerate and optimize Internet traffic and content. F5 solutions automatically and intelligently deliver the best possible Internet performance, availability and content distribution.

F5's application delivery networking products increase the existing benefits of deploying Microsoft's IIS servers to provide enterprises, managed service providers, and e-businesses an easy-to-use solution for deploying, managing and securing global and local area traffic.

With its unique iControl® SOAP/XML API (Application Programming Interface), F5 is the only application delivery networking solution provider offering the ability to programmatically control BIG-IP and IIS 6.0 deployments to provide an adaptable, extremely reliable and secure delivery of Web services and applications.

Challenges

Applications and services that run on IIS 6.0 servers have been playing an increasingly critical role in the network. Whether e-commerce, intranet, or enterprise applications, these services are expected to be highly available and are expected to respond quickly to user requests, while remaining secure to protect the often sensitive nature of the content. Failure to meet any one of these requirements can result in severe and costly consequences.

To effectively provide for these types of demanding requirements, administrators need solutions that allow them to provide high availability, scalability, increased security, flexible administration, increased application performance, and dynamic control.

In the past, administrators had to deploy and separately manage multiple point solutions to achieve these requirements, and then struggle with integration, interoperability and latency issues. The IIS 6.0 server's role in an organization has evolved from a simple web site to an essential element of the enterprise application infrastructure supporting a variety of commercial and internally developed IP applications. Meanwhile, increasing pressure to deploy voice, video and data services over the same common network is presenting many administrators with a difficult task: they must design a network flexible enough deliver high performance while they also offer and support various levels of security for all present and future traffic types.

Organizations with rigid solutions in place face delaying deployment of future applications and services, losing company revenue and increasing costs as applications must be re-engineered and additional traffic management solutions have to be acquired.

With early web-enabled application solutions, performance is very difficult to guarantee or even control. In the data center, web servers are performing tasks that are not related to delivering content to their users. As a result, corporate server farms spend up to thirty percent of their processing power on work that is not related to serving content and maximizing user experience. Tasks such as SSL encryption, authorization, and logging can not only contribute to application performance problems, but raise the cost of server infrastructure, maintenance and management.

With hundreds of applications sharing the same network, each application group is creating its own top-level authentication mechanism and spending server resources on performing initial user authorization. This strategy makes it extremely difficult to manage and enforce authentication and authorization across different groups, requires additional code modifications on the application, and consumes server resources that could otherwise be spent on serving users. These challenges are further complicated by the need to allow remote users an easy-to-use, extremely secure means of accessing internal resources from a variety of different operating systems and from a variety of different locations.

Key Benefits of F5

- F5 provides 80% bandwidth reduction for Microsoft IIS Deployments
- Fast Cache offloads 98% of server connections
- TCP Express provides a 135% improvement in connection reliability for dial-up users
- TMOS features improve performance for end users by more than 70%



MICROSOFT INTERNET INFORMATION SERVICES

Solution

By deploying F5 application delivery networking solutions with Microsoft Internet Information Services, enterprises benefit from an optimally performing, highly available, and secure solution. This best of breed solution allows administrators to consolidate their network resources into one device, reducing the burden and other negative effects of point solutions.

Because of its location at a centralized point in the network, the F5 can offload the overhead on IIS 6.0 servers associated with functions that are not related to the server, such as SSL termination, HTTP compression, authorization and authentication. And because of the power and flexibility of TMOS, F5 devices are able to optimize and accelerate IIS deployments with features like selective HTTP compression, Fast Cache, and TCP Express. These features improved performance for the end user by more than 70% in testing with the Gomez® Performance Network on average web sites using the BIG-IP LTM system with IIS web servers (Figure 1). The Gomez Testing service uses real clients from all corners of the globe, providing a true representation of Internet conditions, WAN issues, and other inefficiencies seen in full application transactions (in contrast to LAN-based testing and best case claims).

The BIG-IP system provides the industry’s most intelligent HTTP compression capabilities, giving organizations using Microsoft IIS the ability to selectively compress traffic. This compression feature helps organizations realize large performance gains along with bandwidth reduction. Because compressing all types of traffic does not necessarily yield a reduction in bandwidth usage, the BIG-IP device, using the Universal Inspection Engine for deep packet inspection and the iRules policy-based engine, looks deep inside a payload and can make a decision to compress certain application types based on access method, application type, or parameters like latency, round trip times, and others. In the Gomez Performance Network tests, the BIG-IP device’s compression feature gave impressive results. Configuring the BIG-IP device to use its intelligent compression not only freed processing cycles on the IIS servers but also resulted in over 80% bandwidth savings, leading to significantly faster download speeds for clients.

The BIG-IP system now has an intelligent memory-based caching module called Fast Cache. Fast Cache provides the flexibility and control needed to extend caching on a per application basis, adapting to an organization’s specialized caching needs. In the Gomez tests, the Fast Cache feature offloaded over 95% of the requests from the servers, further reducing the burden on the IIS servers. With Fast Cache enabled, organizations integrating the BIG-IP solution with Microsoft IIS servers can achieve significant server connection offload while increasing end user performance for their frequently accessed pages.

The TCP Express feature set allows the BIG-IP to enhance and optimize TCP handling. Utilizing independent client and server side TCP stacks, the TCP Express features bridge the gap between client and backend servers, optimizing each connection independently. This functionality also enables the BIG-IP device to shield and transparently optimize non-compliant TCP stacks running across servers within the corporate data center, providing dramatic performance improvements across IIS deployments.

Utilizing this TCP/IP proxy architecture, TCP Express also ensures both client and server are transmitting data at the optimal rate, reducing the overhead and increasing the capacity of the IIS servers by streamlining communication to the client, which improves bandwidth link utilization for a site and minimizes errors associated with lost and reordered packets. TCP Express features accept and buffer the complete server response, allowing the server to send data at its optimum rate while the client receives the data at the appropriate rate for the connection. This optimization is particularly effective when the client is on a slow dial-up connection. Using TCP Express, the BIG-IP system provides a 135% reduction in the number of timeout errors, vastly improving reliability for WAN communications.

F5 can also protect the applications running on IIS servers from application-specific attacks. The ICSA-certified BIG-IP Application Security Module identifies, isolates, and blocks sophisticated attacks without impacting legitimate application transactions. ASM utilizes a highly efficient positive security model to validate each user transaction at the application level based on user session context, authorization privileges, user input, and application response time. Unlike signature inspection methods, the ASM also uses a positive security model to protect against entire classes of HTTP and HTTPS-based threats. New attacks that can defeat signature inspection because they have no known signature are easily blocked by this positive security model.

Application Response Times

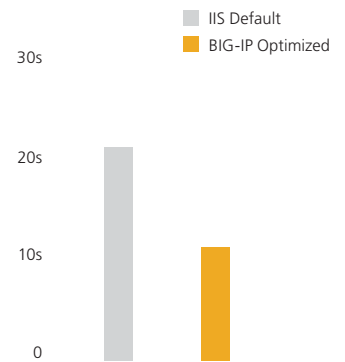


Figure 1: Application response time in seconds with and without the BIG-IP system

RAM Cache Hit Count

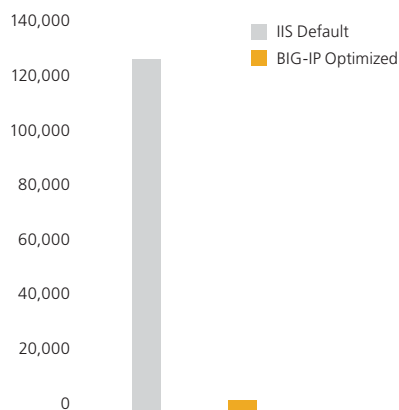


Figure 2: Fast Cache offloads 98% of the connections from IIS Servers



MICROSOFT INTERNET INFORMATION SERVICES

Solution - Continued

When application performance suffers, IT managers often assume that adding bandwidth will solve the problem. Unfortunately, because of the way the TCP protocol works, adding bandwidth is often ineffective. TCP throughput degrades significantly on the WAN, particularly on high-latency, intercontinental links. To overcome these inherent protocol limitations, F5's WANJet device employs adaptive TCP optimization (which combines session-level application awareness, persistent tunnels, selective acknowledgements, error correction, and optimized TCP windows) to fully utilize available bandwidth. This enables WANJet to adapt, in real time, to the latency, packet loss, and congestion characteristics of WAN links, and accelerate virtually all application traffic.

And for organizations with multiple data centers, the BIG-IP Global Traffic Manager (GTM) is the only solution that tracks application state and provides the intelligence to deliver a superior client experience. End user connections can now persist across applications and data centers and be automatically routed to the appropriate data center or server based on application state. Session integrity is always maintained, with no more broken sessions, lost or corrupted data. Organizations gain improved infrastructure scalability, lower TCO, and fewer support calls.

Using the FirePass controller, organizations can simply and securely extend access to IIS server resources to remote users as easily as from inside the corporate LAN. Once users are authenticated by the FirePass controller they are able to access internal resources from any device, in any location without having to re-authenticate when accessing multiple resources. The FirePass controller not only delivers and secures access to content and applications running on IIS servers, but also allows for granular control of access to intranet resources on a group basis.

The overall deployment is further enhanced by using the BIG-IP system with iControl®, F5's open API/SDK. With iControl, applications and services using Microsoft IIS 6.0 can communicate with and influence the behavior of the underlying network in a variety of functions, from a load balancing and traffic management perspective, to a content delivery and fulfillment infrastructure, or both. The result is an integrated Web application, service, and network environment that is highly available, scalable, performs optimally, and is secure. This integrated architecture allows the network to be dynamically tuned based upon IIS 6.0 applications, services, and customer needs.

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability—all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.

About Microsoft Internet Information Services

Microsoft Internet Information Services (IIS) turns a computer into a Web Application Server that can provide web applications based on ASP, .NET, .NET web services, Wide Web publishing services, File Transfer Protocol (FTP) services, Simple Mail Transport Protocol (SMTP) services, and Network News Transfer Protocol (NNTP) services. You can use IIS to host and manage Web sites and other Internet content once you obtain an IP address, register your domain on a DNS server, and configure your network appropriately. IIS is a component of the Microsoft® Windows® operating system.