APPLICATION READY NETWORK GUIDE

MICROSOFT WINDOWS SERVER 2008

Comprehensive Application Ready infrastructure that enhances the security, availability, and performance of Microsoft Windows Server 2008 deployments

SUMMARY

Microsoft® Windows® Server 2008 is much more than ***just*** a new release from Microsoft. From a next generation TCP/IP stack to new versions of Windows Terminal Services and Internet Information services, as well as new technologies like Windows PowerShell and Secure Socket Tunneling Protocol, Windows Server 2008 helps information technology professionals maximize control over their infrastructure while providing unprecedented availability and management capabilities. F5 has worked with Microsoft during the beta cycle and beyond to ensure a high level of interoperability and optimization with the entire Windows Server 2008 platform. F5's Application Ready Network for Windows Server 2008 not only helps optimize end-to-end performance, availability, and scalability for Windows Server 2008 deployments, but reduces the costs associated with deployment, management, and operation.

Benefits and F5 Value

User Experience and Application Performance

Microsoft Windows Server 2008 gives organizations a powerful new platform that is designed to power the next-generation of networks, applications, and Web services. Windows Server 2008 includes some exciting new components such as Microsoft's new TCP/IP stack, Secure Socket Tunneling Protocol (SSTP), and new versions of industry standard applications like Windows Terminal Services and Internet Information Services. F5 has been working closely with Microsoft to ensure that F5's Application Ready Network for Microsoft Windows Server 2008 provides the highest level of application availability, performance, and end user satisfaction.

One of the highlights of Microsoft Windows Server 2008 is a next generation TCP/IP stack that has been completely redesigned from the ground up. F5 solutions include a host of TCP/IP optimization technologies that are compatible with Microsoft's new stack. These optimizations, which combine session-level application awareness, persistent tunnels, selective acknowledgements, error correction, and optimized TCP windows, enable F5 devices and Microsoft Server 2008 installations to fully utilize available bandwidth. This enables F5 devices to adapt, in real time, to the latency, packet loss, and congestion characteristics of WAN links, and accelerate virtually all application traffic. And F5 isolates, controls, and independently optimizes user and server connections, enabling both the server and end user to maximize productivity.

With the rapid expansion of the Internet and the quickly diminishing number of IPv4 addresses available, organizations are looking to ensure their network infrastructure is adequately prepared for the future. Internet Protocol version 6 (IPv6) support is no longer a luxury, it is a necessity. IPv6, a new suite of standard protocols for the network layer of the Internet, is built into both Windows Server 2008, as well as F5 devices, ensuring that your network and Microsoft applications are ready for this inevitable change. With F5's IPv6 support, organizations have a clear strategy for staging network migration as IPv6 traffic grows, without wholesale network and application upgrades. Additionally, F5 devices can perform IPv6/IPv4 translation, translating traffic for consumption by either IPv4 or IPv6 end points. This allows organizations to stage their migration gradually as demand for IPv6 increases. F5 enables you to freely intermingle IPv4 and IPv6 services on Windows Server 2008; for example, F5 can serve as an IPv4 front end to Windows Server 2008 Web Access servers that only use IPv6. With F5, organizations have a strong solution for today and well into the future.

Windows Server 2008 is extremely effective at what it was designed to do: provide a solid foundation for server workload and application requirements. One of F5's core strengths is the ability to enhance end-user experience while increasing application and server performance. We do this by taking on many of the duties that servers traditionally have to perform. If each server has to carry out processor-intensive tasks such as compression, caching, and SSL processing and certificate management, the amount of processing power these devices have left to perform core tasks is reduced. By offloading these types of tasks onto F5's centralized and high powered network devices, F5 greatly improves Windows Server 2008 server efficiency and enables organizations to reduce the amount of hardware. This applies to all the major components of Windows Server 2008, including Windows Terminal Services, Internet Information Servers, and SSTP.

F5 provides technology that guarantees the most efficient network possible. Because F5's unique TMOS™ operating system is a full proxy, it can optimize any end point that connects through the system. As a full broker of communications, the system optimizes communication for every single end-device communicating through it. This optimization can take place up and down the entire stack — from the transport layer to the protocol and application layer — functions outside the control of Windows Server 2008. This takes the workload off of the Windows Server 2008 devices for increased server efficiency. By reducing unnecessary protocol communication across the network, F5 improves application response times and utilization for Windows Server 2008 deployments and other applications on the network.

Even high-powered and efficient applications and servers, like Windows Server 2008, as well as other devices on the local area network (LAN), are not much help over the wide area network (WAN). Network latency across the WAN is one of the biggest challenges facing IT departments around the world, and is a major concern for organizations deploying applications like Windows Terminal Services where users can access applications from anywhere. Simply increasing bandwidth does nothing to solve the problem. F5 helps drastically reduce the impact of latency in a number of ways. In addition to the benefits from TMOS, F5 solves latency problems with a group of capabilities that eliminates the need for the browser to download repetitive or duplicate data, as well as ensuring the best use of bandwidth by controlling browser behavior. By reducing the extra conditional requests and excess data (re)transmitted between the

"Windows Server is one of the most popular application platforms that we see within our enterprise customer base. As such, F5 has put substantial resources into testing its application delivery portfolio with the Windows Server platform technologies through every step of the beta to maintain a high level of interoperability."

Jim Ritchings, VP of Business Development at F5

Benefits and F5 Value

browser and the web application, F5 mitigates the effects of WAN latency, networking errors, and packet loss.

One of the strengths of the F5's Application Ready Network is the wide variety of materials that ease the burden of configuring and optimizing our devices, freeing valuable IT resources to work on other projects. As part of the Application Ready Network for Microsoft Windows 2008, F5 has configured, tested, and tuned our devices with the major components of Windows Server 2008 and carefully documented the procedures in our Deployment Guide. F5 also provides configuration Profiles and Policies to make configuration incredibly simple yet powerful and flexible, with some policies including prebuilt drop-downs for components like Microsoft Internet Information Services and Windows Terminal Services. And now with our management devices, the deployment guide configuration files are available as a template, which can be easily uploaded and pushed to F5 devices. With the power of Microsoft PowerShell, the command line shell and scripting language included with Windows Server 2008, and F5's iControl PowerShell Cmdlets and scripts, developers have a unique way to control and manage F5 devices in one location[1].

Application Security

While performance and end-user experience are vital to a successful deployment of Windows Server 2008, ensuring application security can be even more crucial. Because of the sensitive nature of data stored in applications and databases, coupled with new compliance initiatives and government regulations on data protection, securing your applications is more important than ever before. F5 security solutions provide comprehensive protection for Windows Server 2008, ensuring your data and applications are secure.

Years ago, merely having network firewalls in front of the LAN was considered an adequate level of security. Next came intrusion protection/detection systems, which added another level of security, albeit one that provided a negative security model. However, IPS/IDS systems could only protect against a known list of attacks and signatures, and soon attacks became more sophisticated, with zero-day attacks that would bypass these systems as their signatures were previously unknown. Recently, hackers are shifting their focus to applications themselves with attacks that look harmless to both network firewalls and intrusion protection/detection systems. More than 50 percent of all new vulnerabilities being identified on a weekly basis are attributed to web applications[2]. Devices relying solely on a known list of signature attacks cannot defend against targeted attacks involving a malicious user seeking vulnerabilities unique to a particular application. F5 detects and mitigates patternless exploits in real time, adding accurate, complementary protection to existing firewalls and IDS devices, which do not efficiently address HTTP and HTTPS-borne threats.

In addition to analyzing and blocking known attack signatures, F5 can strip out identifying operating system and web server information (such as version strings, signatures, and fingerprinting) from message headers, conceal any HTTP error messages from users, and remove application error messages from pages sent to users while checking to ensure no server code or private HTML comments leak onto public web pages.

And attacks do not always come from the outside of the network; internal users can gain sensitive information or sabotage applications with greater ease than external users. Because F5 devices can offload SSL encryption duties, organizations can encrypt traffic for entire transactions, without affecting performance for the end user. This prevents information from being sent in clear text over the internal network, mitigating risks associated with internal users as well as complying with state and federal regulations related to privacy.

F5 devices also protect against attacks that use cookies and other tokens that are transparently distributed for their entry point. F5 devices can be easily configured to encrypt cookies used by Windows Server 2008, preventing cookie tampering and other cookie-based attacks. This gives organizations superior security for all stateful applications and a higher level of user identity trust.

F5 includes extremely granular endpoint security for remote users connecting to the network and to Windows Server 2008 servers and applications. Before a remote user can even log on to the F5 devices to gain access to the network, F5 can determine if an antivirus or personal firewall is running on their PC and if it is up-to-date, or enforce a specific operating system patch level, among a host of other pre-logon checks. F5 can direct the user to a remediation page for further instructions or even turn on antivirus or firewalls for the user. F5 remote access also supports two-factor authentication from leading vendors for those organizations that require more than just a user name and password for access to the network. And F5's remote access solution can be easily integrated with Active Directory, providing centralized authentication.

When the remote user is finished working with their remote access session, F5 includes a cache cleanup control that removes cookies, browser history, auto-complete information, browser cache, temp files, and all ActiveX controls installed during the remote access session from the client PC. This makes ensures that no information is left behind, which is critical for users connecting from public computers, such as a kiosk.

Not only does F5 provide comprehensive application security, but we produce extremely secure devices. We ensure your Windows Server 2008 deployment, and the information it contains, remains completely secure.

Unified Security Enforcement and Access Control

Another integral piece of a complete security platform is security enforcement and access control. The number of employees requiring access to corporate resources from outside the network is growing every year. And it's not only employees who need access to the network. With more business-to-business

[1] For more information on iControl and Microsoft PowerShell integration, see http://devcentral.f5.com/Default.aspx?tabid=71
[2] SANS@RISK, "The Consensus Security Vulnerability Report"

Benefits and F5 Value

transactions, and partners, contractors, and suppliers all clamoring for access to different internal applications, organizations are struggling with access control and enforcement issues. F5 provides a complete approach to security enforcement and providing access control for Windows Server 2008, regardless of end user, client type, application, access network, or network resources.

In the past, remote access was provided by IPsec VPN solutions — a complicated deployment which required software installation and maintenance on every client, and was difficult to enforce and control. IPSec has shown it is unable to keep up with the growing demands of remote access required by today's enterprise organizations. F5's remote access solution enables you to easily grant remote access to anyone from any device, while ensuring this access is carefully controlled and restricted on a granular basis.

With F5, access to Windows Server 2008 resources can be easily controlled on an extremely granular level. For example, employees can be granted full access to internal resources, while a trusted partner group can be restricted to a specific subset of applications, and a contractor group could be locked down to a specific application or port. F5 centralizes this access control, and makes configuring and enforcing this type of control simple. F5 can even gather device information (like IP address or time of day) and determine if a resource should be offered. The F5 solution also includes control for any access network and any device, with no need to deploy multiple access control solutions for remote users, wireless LANs, and the LAN.

F5 supports virtual administration domains, allowing a single F5 device to be managed by multiple application teams without interference. Every user can be assigned to specific administrative domains which define which objects are visible to that user. Multiple levels of access are also definable for each user, with basic read-only users who can log on to the devices to monitor status of specific objects and traffic quantities to full administrative users capable of making configuration changes to every object on the device. This increases productivity by reducing the time spent in meetings, tracking down appropriate administrative personnel, and improves the ability of application administrations to manage applications when it's necessary. F5 helps streamline the business process and improve the productivity and efficiency of operational personnel.

Business Continuity and Disaster Recovery

Disaster recovery and business continuity are vital to the success of an organization. Merely having a solid security platform cannot protect against unexpected events and disasters that create a wide range of obstacles, ranging from knocking out the power to wiping out entire data centers. These disruptive events not only cost organizations thousands or even millions of dollars, but can bring about legal ramifications with industry and government rules concerning data protection and disaster recovery. With the amount of irreplaceable, business critical information stored on the network and in applications like those found in Windows Server 2008, having an effective disaster recovery plan is essential.

F5 products are uniquely positioned to help organizations mitigate disasters and other disruptive events. F5 is the only vendor to virtualize data centers, VPN access, optimization, and traffic in an integrated fashion — ensuring the Windows Server 2008 devices and applications are always available.

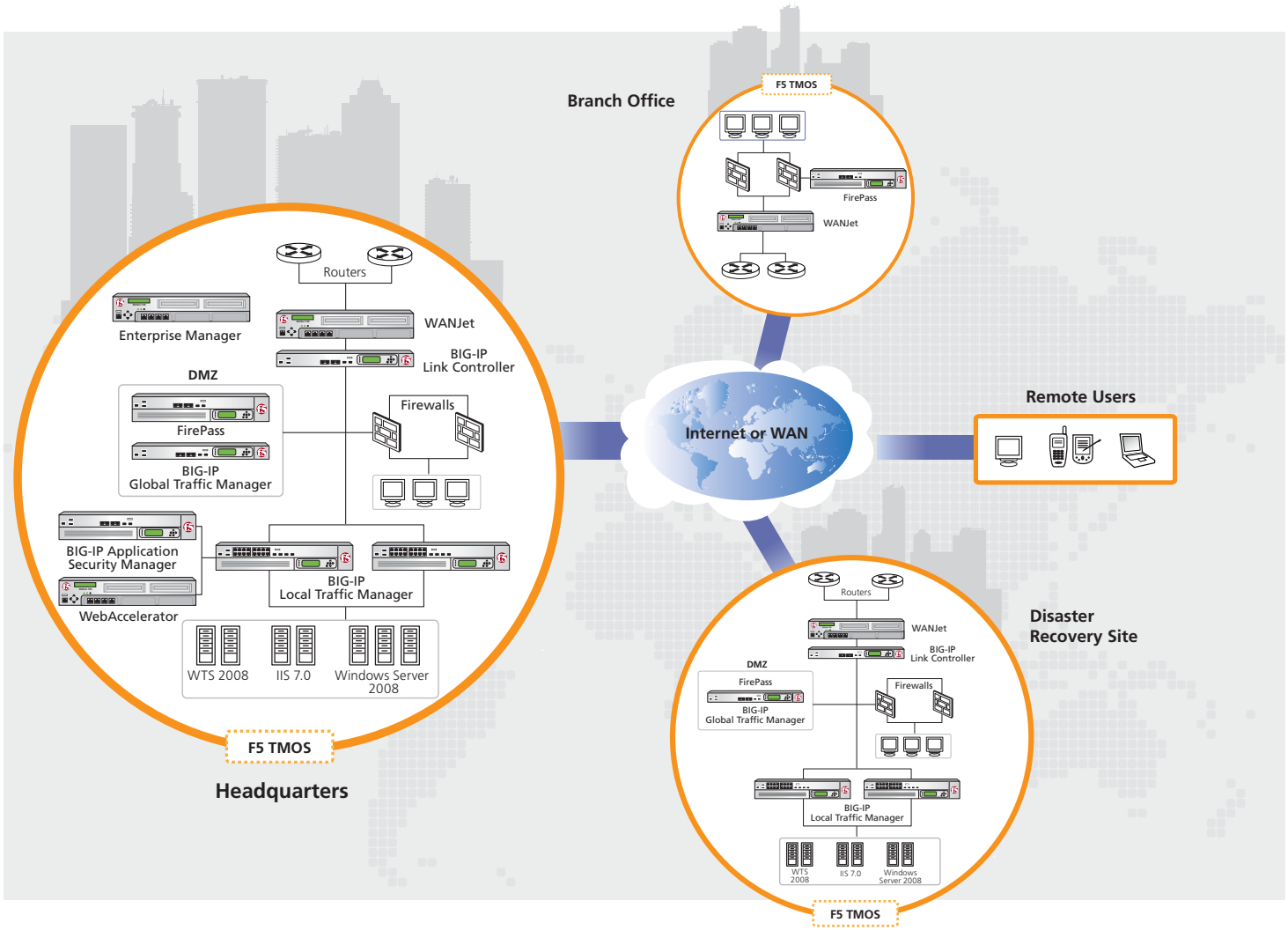
F5 provides the industry's most comprehensive solution for site failover and business continuity. From performing comprehensive site application availability checks, to defining the conditions for dynamically and transparently shifting all traffic to a backup data center, failing over an entire site, or controlling only the affected applications, F5 has the complete solution.

When one of these disruptive events does happen, even something as simple as a snow storm that prevents most employees from making it to the office, F5 provides extremely secure remote access to the network and Windows Server 2008 deployment, ensuring that even though the physical office might be unavailable, as long as a single data center is still up, business can continue. F5 remote access devices support Microsoft Vista and access to Windows Server 2008 devices, and even provide secure application access from Windows Mobile® 5/6 PocketPC and Smartphones.

One scenario often neglected in a disaster recovery plan is when the event doesn't happen to your organization, but to your ISP. While many organizations do have multiple links, they have to contend with complicated BGP configurations. F5 simplifies multi-homed deployments so you no longer need ISP cooperation, designated IP address blocks, ASNs, or reliance on complex BGP configurations to protect your network from ISP failures. With F5 technology, an organization also has the choice of aggregating multiple small connections together rather than having to invest in a single high bandwidth connection. This frees businesses to expand their service as they grow. F5 seamlessly monitors availability and performance of multiple WAN ISP connections to intelligently manage bi-directional traffic flows to a site, providing fault tolerant and optimized Internet access. F5 devices detect errors across an entire link to provide end-to-end, reliable WAN connectivity. F5 monitors the health and availability of each connection, detecting outages to a link or ISP. In the event of a failure, traffic is dynamically directed across other available links so users stay connected.

Global F5 and Windows Server 2008 Deployment

The following example shows a global configuration, using the F5 suite of products to optimize, secure, and deliver Windows Server 2008 installations over the WAN and LAN.



Additional Information

Deployment Guides

Deploying the BIG-IP System with Microsoft Internet Information Services 7.0

Provides detailed procedures on how to configure the BIG-IP® Local Traffic Manager™ (LTM) and WebAccelerator™ with Internet Information Services 7.0.

Deploying the BIG-IP System with Microsoft Windows Server 2008 Terminal Services

Provides detailed procedures on how to configure the BIG-IP LTM with the new version of Windows Terminal Services.

See the Deployment Guide index on the F5 Solution Center for more Microsoft Guides.

For more information about the partnership between F5 and Microsoft, see the Microsoft Partner Showcase on the F5 Solution Center.

F5 Product offerings

BIG-IP Product Family

The BIG-IP products deliver high availability, improved performance, application security, and access control, all in one unit. A single BIG-IP device can do the work of a dozen single-purpose products. More importantly, it can do that work in an efficient, cohesive manner that is easier to manage and adapt as business and technology needs change.

Product Modules (These modules can also be run as standalone appliances)

LTM: The BIG-IP LTM allows organizations to ensure quality of service and manageability, apply business policies and rules to content delivery, support increasing traffic volumes, deliver their applications securely, enjoy operational efficiency and cost control, and remain flexible to future application and infrastructure changes to protect their investments.

GTM: The BIG-IP Global Traffic Manager™ (GTM) Module provides high availability, maximum performance and global management for applications running across multiple and globally dispersed data centers. Seamlessly virtualizes FirePass VPN to automatically provide always-on access control.

ASM: The Application Security Manager™ provides application layer protection from both targeted and generalized application attacks to ensure that applications are always available and performing optimally.

WA: F5 WebAccelerator™ is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms, and WAN latency issues which impact user performance.

LC: The BIG-IP Link Controller™ Module seamlessly monitors availability and performance of multiple WAN connections to intelligently manage bi-directional traffic flows to a site – providing fault tolerant, optimized Internet access.

Feature Modules: These are individual feature packs that can be added to a BIG-IP traffic management platform. The Feature Modules include the Message Security, Intelligent Compression, L7 Rate Shaping, IPv6 Gateway, Advanced Client Authentication, SSL Acceleration, Fast Cache, and Advanced Routing Modules.

FirePass

F5's FirePass® SSL VPN appliance provides secure access to corporate applications and data using a standard web browser. Delivering outstanding performance, scalability, ease-of-use, and end-point security, FirePass helps increase the productivity of those working from home or on the road while keeping corporate data secure.

WANJet

WANJet® is an appliance-based solution that delivers LAN-like application performance over the WAN. WANJet accelerates applications including: file transfer, e-mail, client-server applications, data replication, and others, resulting in predictable, fast performance for all WAN users.

Enterprise Manager

F5's appliance-based Enterprise Manager ™gives you the power to centrally discover and maintain the F5 devices in your network. With Enterprise Manager, you can archive and safeguard device configurations for contingency planning, Configure new devices from a central location without manually working on each device, easily and quickly roll-out software upgrades and security patches and much more.

F5 Acopia ARX

F5 Acopia™ award-winning intelligent file virtualization solutions decouple file access from physical file location. Our ARX® products integrate seamlessly into existing Network Attached Storage (NAS), Windows®, UNIX® and Linux environments. ARX devices provide industry-leading scalability, performance and reliability, and are specifically designed to meet the needs of enterprise storage environments.

iControl API

iControl® is F5's SOAP API exposed on each BIG-IP LTM system. iControl enables automation between the application and the network, and gives organizations the power and flexibility to ensure that applications and the network work together for increased reliability, security, and performance. F5's developer community, DevCentral, has sample iControl applications and code. Visit the Microsoft page on DevCentral for Microsoft-specific forums and other useful information about F5 integration with Microsoft applications.

www.f5.com