



# APPLICATION READY NETWORK GUIDE

## SAP

Comprehensive Application Ready infrastructure that enhances the security, availability and performance of SAP deployments

## SUMMARY

SAP®, the world's largest business software company, provides a comprehensive range of enterprise software applications and business solutions to empower every aspect of business. Organizations deploying SAP have invested a significant amount of time and money in these powerful applications. By taking advantage of F5's Application Ready infrastructure for SAP, tested and validated at SAP, organizations can achieve a secure, fast and available network infrastructure that reduces the total cost of operation and increases ROI. And F5's FirePass SSL VPN, BIG-IP Local Traffic Manager and WANJet appliance have been certified by SAP for integration with SAP ERP 6.0 based on NetWeaver 7.0.

F5 technology provides an adaptable network framework for SAP deployments that allows organizations to ensure quality of service and manageability, apply business policies and rules to content delivery, support increasing traffic volumes, deliver applications securely, enjoy operational efficiency and cost control, and remain flexible to future application and infrastructure changes to protect their investments. The result is elegant and powerful solutions to protect you from security threats, network failures and traffic congestion, while providing an optimized architecture for the future.

## Benefits and F5 value

### User Experience and Application Performance

Deploying a core suite of applications like SAP involves careful planning and execution. In many cases, only after the application is put into production, organizations realize that although the application is configured optimally, the network infrastructure ends up slowing the performance of the application for the end users. An organization's IP network is commonly a shared resource by a variety of other services including email, VOIP and general internet access. These services, by consuming network resources, can negatively impact SAP applications.

Poor performance of applications, due to network conditions, IT infrastructure challenges, or other factors, can be problematic by impeding adoption rates and introducing unnecessary delay into business processes. Users faced with a new application are already resistant to change. If the performance of that application is less than ideal, even if it's not the fault of the application itself, adoption rates and attitudes can plummet, both of which negatively impact business productivity. These types of performance issues impede not only user productivity by introducing unnecessary delay into the process, but can also frustrate and potentially drive away customers who interact either directly or indirectly with the application over consumer-grade Internet connections. F5's Application Ready network can solve many of these network infrastructure challenges by optimizing the network for SAP and applications, ensuring the best possible user experience.

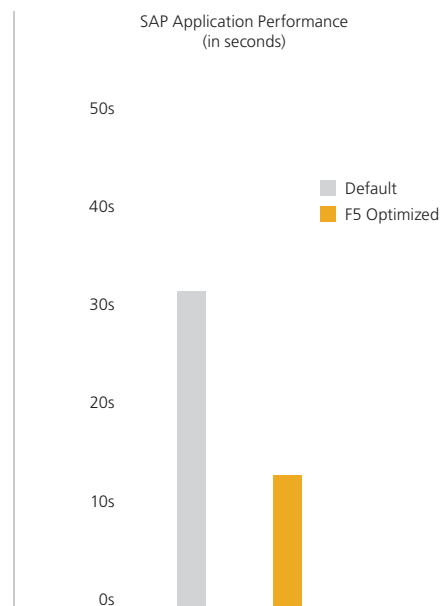
Often, an organization's first response to Web application delays is to increase bandwidth or increase server capacity, but this does not address one of the fundamental issues: latency. F5's solves this problem with a group of capabilities that eliminates the need for the browser to download repetitive 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 browser and the web application, F5 mitigates the effects of WAN latency, networking errors, and packet loss. This functionality also significantly reduces the amount of data downloaded without requiring the users to download special software or making changes to the browser.

SAP deployments contain multiple application components that provide a variety of business critical services. F5 ensures that these vital applications aren't bogged down with processor-intensive tasks that are not relevant to the core application. F5 provides a comprehensive solution to offload many of these types of burdensome or repetitious functions (such as compression, caching, and SSL offload) onto centralized and high powered network devices, which greatly improves server efficiency. In recent testing, one scenario involved simulating 500 users connecting and interacting with the SAP application over the WAN. The result? Using F5 technology reduced CPU utilization of the SAP servers from 68% to 38%.

To further enhance end user performance, F5 provides extensive connection management and TCP optimization capabilities that increase server performance and dramatically speed page load times. For example, F5 can greatly increase SAP server capacity by aggregating thousands of user requests down to a much smaller number of server-side connections, ensuring requests are handled efficiently by the backend system. In the same 500 user test mentioned previously, 1,000 client-side connections were combined into 50 connections to the application servers.

F5's TCP optimizations increase end user performance, whether the user is on a local area network (LAN) or a wide area network (WAN). For high-speed LANs, F5's TCP stack quickly expands buffer sizes and detects low-latency to manage congestion. For low-speed WANs, F5's detects client speed and estimates bandwidth to limit packet loss and recovery in the case of dropped packets.



*F5 Optimizations provide a significant decrease in page download times for clients using a small link (for example a remote office or home users)*

F5 isolates, controls, and independently optimizes user and SAP server connections to provide the best performance for every device connecting to the network and the SAP applications running on it. F5 eliminates the need for clients and servers to negotiate the lowest common denominator for communications. We intermedate on behalf of the client and use TCP enhancements to optimize client-side delivery while maintaining server-optimized connections on the inside of the network. For example, with F5, WAN users experienced a 2x performance improvement logging into the Enterprise Portal and Knowledge Management systems.

And to make enhancing application performance and end user experience for SAP deployments as easy as possible, F5 provides a specific acceleration policy for SAP. Instead of struggling with multiple configuration options, merely choose the custom policy for SAP for quick, simple acceleration.

# Benefits and F5 value

## Application Security

Much like end user experience, providing specific, application-level security is often left to the end of application deployment scenarios, or even neglected altogether, as organizations rely on existing network security measures to provide application security. This can often be a costly mistake, especially with a business-critical application like SAP. More and more malicious users are targeting applications, with attacks that look harmless to normal network security measures. F5 has a number of ways to protect SAP deployments and other applications on the network.

F5's application security goes far beyond what most firewalls or intrusion detection/protection systems and other signature inspection methods can provide. F5 utilizes a positive security model; allowing only known, acceptable traffic through rather than simply analyzing and blocking known attack signatures. Devices relying on a known list of signature attacks cannot defend against targeted attacks involving a malicious user seeking vulnerabilities unique to a particular application.

### Key Benefits of F5

- F5 can cut SAP Enterprise Portal login time by more than half for WAN users
- F5 can speed document downloads by 4.5x for DSL users, and 40x or more for high bandwidth connections
- F5 can reduce SAP server CPU utilization by 44%
- F5 can provide a 20x reduction in the number of SAP server-side connections
- F5 significantly reduces bandwidth costs associated with delivering SAP applications over the WAN

F5 can detect and mitigate patternless exploits in real time, adding accurate, complementary protection to existing firewalls and IDS devices, which cannot efficiently address HTTP and HTTPS-borne threats.

As attacks get more and more sophisticated, hackers are using objects like cookies and other tokens that are transparently distributed to legitimate users for their entry point. In the default SAP configuration, the application uses cookies stored on the user's hard drive. While uncommon, a malicious user could modify this cookie to gain unauthorized access. F5 devices can be easily configured to encrypt these cookies, preventing cookie tampering and other cookie attacks.

F5 also virtualizes and hides all application and server error codes, as well as real URL references that may provide hackers with clues about infrastructure, services and their associated vulnerabilities. Further, F5 can strip out identifying OS and web server information (such as version strings, messages, signatures, and fingerprinting) from message headers, conceals 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 out onto public web pages.

F5 includes extremely granular endpoint security for remote users connecting to the network and the SAP applications running there. 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 who require more than just a user name and password for access to the network.

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, to make sure that no information is left behind, which is critical for users connecting from public computers, such as a kiosk.

F5 prides itself on creating exceptionally secure devices that provide comprehensive network and application security. We ensure your SAP applications, and the information they contain, remain completely secure.

## Unified Security Enforcement and Access Control

With a strong security infrastructure in place, attention now turns to enforcing these security policies and controlling access to the applications on the network. Organizations deploying SAP applications often have partners, vendors, and contractors who need some level of access SAP and the network, but this access needs to be restricted and carefully controlled. Providing access can be complicated not only by the different users requiring different access levels, but also by the types of devices that need access. F5 provides a complete approach to providing access control regardless of end user, client type, application, access network or network resources.

With F5, you can easily add groups of users, and restrict access based on these groups. For example, one group may consist of business partners who need access to portions of the SAP applications; another group may contain contractors only allowed to access one specific SAP application. F5 centralizes access control, and makes configuring and enforcing this type of control extremely 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 device to be managed by multiple application teams without interference.

## Benefits and F5 value

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 reduces the time spent in meetings, tracking down appropriate administrative personnel, and improves the ability of application administrations to manage applications when it's necessary. This streamlines the business process and improves the efficiency of operational personnel.

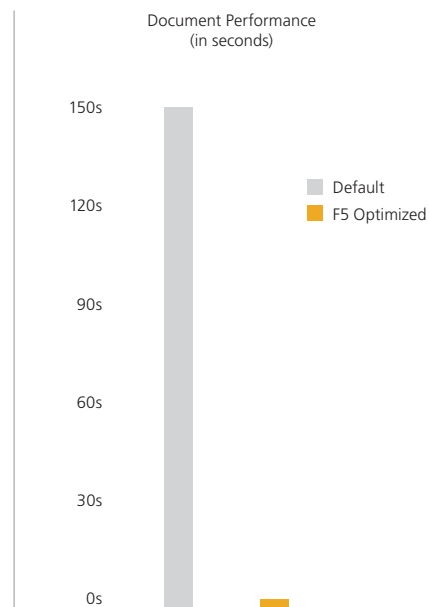
### Business Continuity and Disaster Recovery

Not only do IT managers have to ensure the performance and security of SAP deployments, but they must also be prepared for unexpected disruptions and even catastrophic events that can bring down entire data centers. This is especially important considering new industry and government rules concerning data protection and disaster recovery. F5 products are uniquely positioned to ensure your business-critical SAP applications are always available.

When a disruptive event does happen, even something as minor as a snowstorm where the majority of employees can't make it to the office, F5 provides extremely secure remote access to the network, SAP, and other applications. Not only is F5's remote access solution much easier to deploy and use than IPSEC technology, it can be configured to allow access to SAP applications with the click of a button, without requiring the user to pre-install or configure any software. And to ensure the best possible remote user experience, F5 also provides TCP compression and additional caching to enhance performance for the remote users accessing the enterprise network. Need proof? SAP uses F5's remote access solution; nearly 7,000 SAP employees access applications through the F5 SSL VPN every day.

F5 can even help in the event that the disaster doesn't happen to your business or SAP deployment directly, but to your ISP. F5 simplifies multi-homed deployments so you no longer need ISP cooperation, designated IP address blocks, ASNs, high-end routers, 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.

SAP applications generally only make up a small percentage of an organization's network traffic. However, this traffic is crucial to the continuity of the business. The applications often have 7x24 availability requirements and when their performance is compromised, it affects many areas of the business. Even minor degradations in the performance of the network can affect the users of SAP applications, resulting in lost productivity when users must wait for responses from the application. For example, call center efficiency is often measured by metrics such as volume and customer wait times, both of which are adversely affected by slow network connections because they can cause users of SAP applications to wait for responses, slowing their processing time per caller and decreasing total volume over the course of a day. This also has an adverse affect on the cost to service customers, which can result in diminishing margins.

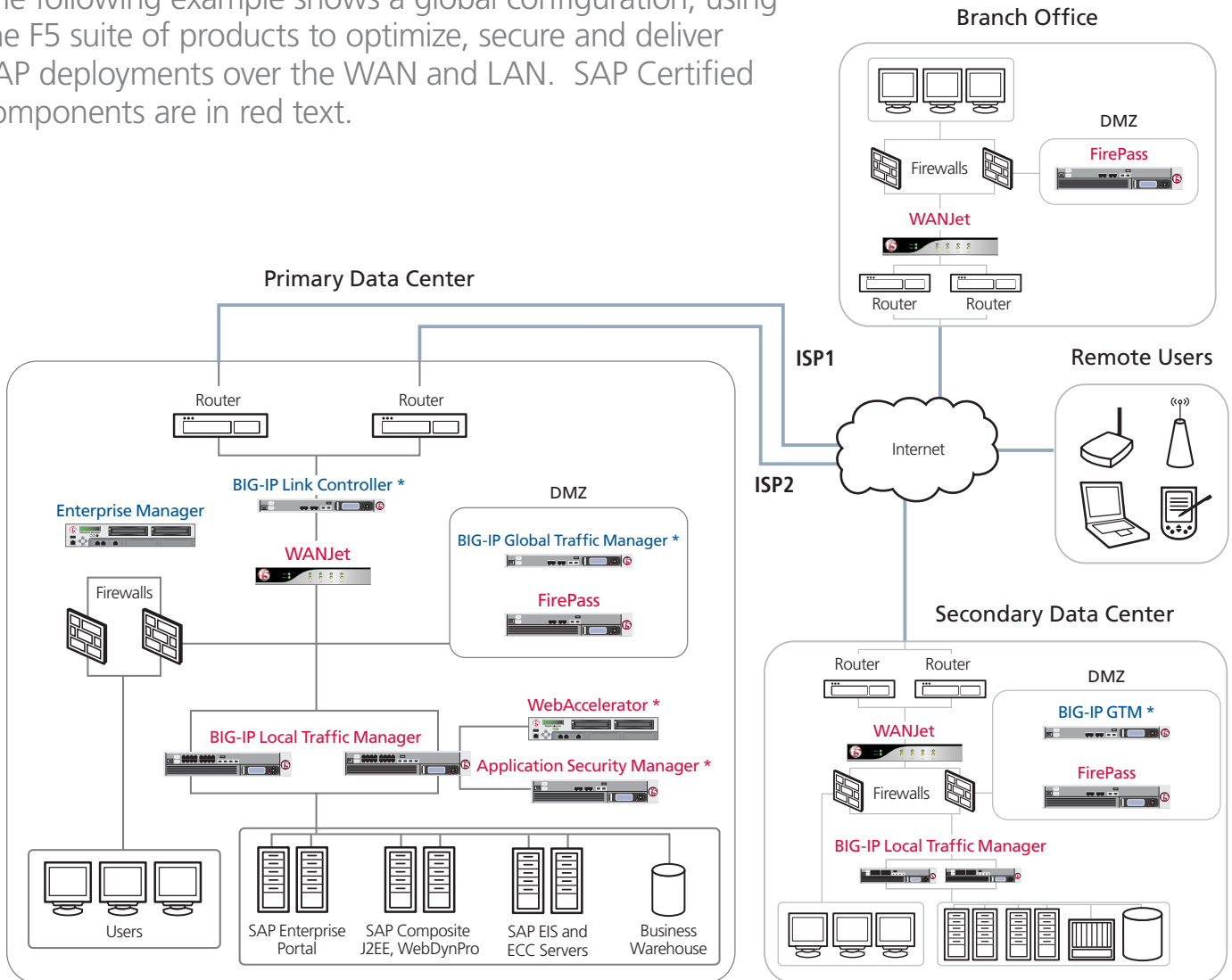


*F5 WAN optimizations drastically reduced the document download times for clients using a high bandwidth connection with 1% packet loss over the WAN (i.e. between a US city and an office in Asia Pacific)*

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.

# Global F5 and SAP Deployment

The following example shows a global configuration, using the F5 suite of products to optimize, secure and deliver SAP deployments over the WAN and LAN. SAP Certified components are in red text.



\* Available as a module on the BIG-IP LTM system

# Additional Information

## SAP and F5 Solution Documents

### SAP Deployment Guide

This guide provides detailed, step-by-step procedures on how to configure the BIG-IP LTM, WebAccelerator, FirePass, and WANJet with SAP NetWeaver and Enterprise SOA

### SAP Case Study

This F5 Case Study describes how SAP replaced their previous VPN technology with F5's FirePass SSL VPN solution

### SAP Certification Datasheet

This certification data describes the F5 products that have achieved SAP certification.

For more information about the partnership between F5 and SAP, see the [SAP Partner Showcase](#) on the F5 Solution Center.

## F5 Product offerings

### BIG-IP 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.

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

**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 Module 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.

### 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.

### 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.

## SAP Certifications

### BIG-IP LTM v9 with WA

- Network Performance Optimization for Enterprise SOA-Based Solutions
- SOA Landscapes Access Reliability and Availability Through Networks
- Network Security for Enterprise SOA-Based Solutions

### BIG-IP LTM v9 with ASM

- Network Security for Enterprise SOA-Based Solutions

### FirePass controller v6

- Network Security for Enterprise SOA-Based Solutions

### WANJet v5

- Network Performance Optimization for Enterprise SOA-Based Solutions



[www.f5.com](http://www.f5.com)