



Key Benefits of F5

- Speeds document downloads by 4.5x for DSL users, and 40x or more for high bandwidth connections
- Reduces SAP server CPU utilization by 44%
- Provides a 20x reduction in the number of SAP server-side connections
- Cuts SAP Enterprise Portal login time by 2x for WAN users
- Reduces bandwidth costs associated with delivering SAP applications over the WAN

F5's Application Ready Solution delivers a powerful, flexible, and forward-looking infrastructure for SAP deployments

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, organizations can achieve a secure, fast and available network infrastructure that reduces the total cost of operation and increases ROI.

F5 technology provides an adaptable and agile network framework for SAP deployments. This 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. 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. IT agility, your way.

Benefits and F5 value

Improving 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 shared by a variety of other services including email, VOIP and general internet access, and these services, by consuming network resources, can negatively impact SAP applications.

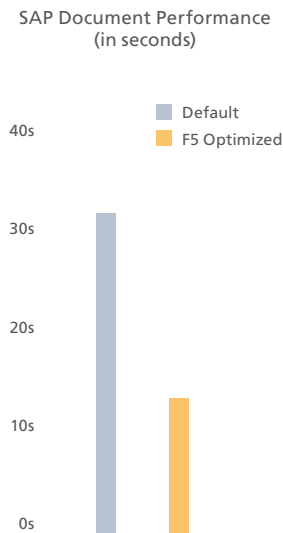
Poor performance of applications, due to network conditions, IT infrastructure challenges, or other factors, can be problematic by impeding adoption rates and introducing unnecessary delay into business processes. Users faced with a new application are may be resistant to change. If the performance of 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 solution can solve many of these network infrastructure challenges by optimizing the network for SAP and applications, ensuring the best possible user experience.

F5 offers a unique platform for unified application delivery services that understands the context of the user, network conditions, and resources available at the time the request is made. It brings the end-to-end intelligence necessary to extend the data center out into the cloud and the branches, enabling secure, accelerated delivery of SAP applications with regard to the specific context in which the application must be delivered.

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.

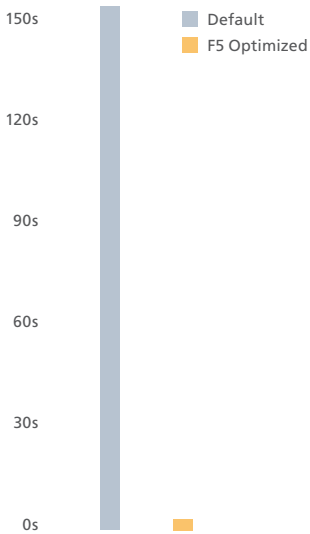
SAP deployments contain multiple application components that provide a variety of business critical services. F5 ensures that these vital applications aren't bogged down with processor-intensive tasks that are not relevant to the core application. F5 provides a comprehensive solution to offload many of these types of burdensome or repetitious functions (such as compression, caching, and SSL processing) 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



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

SAP Document Performance
(in seconds)



F5 WAN optimizations drastically reduced the document download times for clients using a high bandwidth connection with 1% packet loss over the WAN (for example, between a city in the United States and an office in Asia Pacific)

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 ensures applications are always available with advanced monitoring capabilities that help reduce the volume of traffic on the network and the burden on servers imposed by using valuable resources to respond to health checks. By passively monitoring application exchanges (such as data flows) through F5 devices to determine status, capacity, and data pertinent to load balancing decisions on performance and availability, F5 improves server efficiency, capacity, and performance. And for F5 devices, there is a graphical reporting engine to display real-time historical statistics by the hour, day, week, or month. The dashboard reports statistics on CPU and memory usage, connections, and throughput with an easy-to-read graphical view.

While all of these optimizations might sound complicated, F5 provides advanced tools that make it easy to manage our devices while maintaining flexibility and control of your infrastructure. Our deployment guides help administrators quickly optimize and accurately configure F5 devices for their SAP deployments. Even with this guidance, administrators have to their spend valuable and expensive time on manual configuration procedures. This is no longer necessary with our Application Ready Templates for SAP. We've rolled our deployment guides into a wizard-like template, so optimally configuring F5 devices requires only minimal information and takes just minutes. F5 helps simplify system management by consolidating security, acceleration, and availability in one easy to manage platform.

Enhancing 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, and the stiff penalties imposed for failing to meet compliance initiatives such as PCI, HIPAA, SOX, BASEL II, and other regulations. 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.

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. F5 security devices report previously unknown threats, such as brute force attacks, and mitigate web application threats, shielding the organization from data

breaches. Our full inspection and event-based policies deliver a greatly enhanced ability to search for, detect, and apply numerous rules to block known OSI L7 attacks.

F5 also applies secure application templates to block unknown attacks and attacks targeted at the business logic of applications. F5 can secure any parameter from client-side manipulation and validate log-on parameters and application flow to prevent forceful browsing and logical flaws.

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 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.

Providing 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.

One important aspect of F5's universal access approach is the ability to partition the network into various segments to protect and monitor access from one segment to the other. At the network level, you can use IP addresses, VLANs, MAC addresses, and packet filtering mechanisms to define practically any combination of network security policy based on any network parameter such as originating or destination VLANs, IP addresses, and protocols. You can refine this security with stricter access rules based on authentication results or application responses.

And not only can you partition the network, but F5 provides organizational efficiency and an easy way to scale management by allowing our devices themselves to be managed by multiple application teams without interference. These administrative partitions enable organizations to assign varying degrees of administrative rights and views to each F5 device. For example, the application owner for SAP Enterprise Portal can be given permission to only view or modify objects that reside in the Enterprise Portal domain, while not being able to modify the configuration for the ERP Central Component or other objects 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.

Enabling Seamless Business Continuity and Disaster Recovery

In addition to ensuring the performance and security of SAP deployments, IT managers 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 solution 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

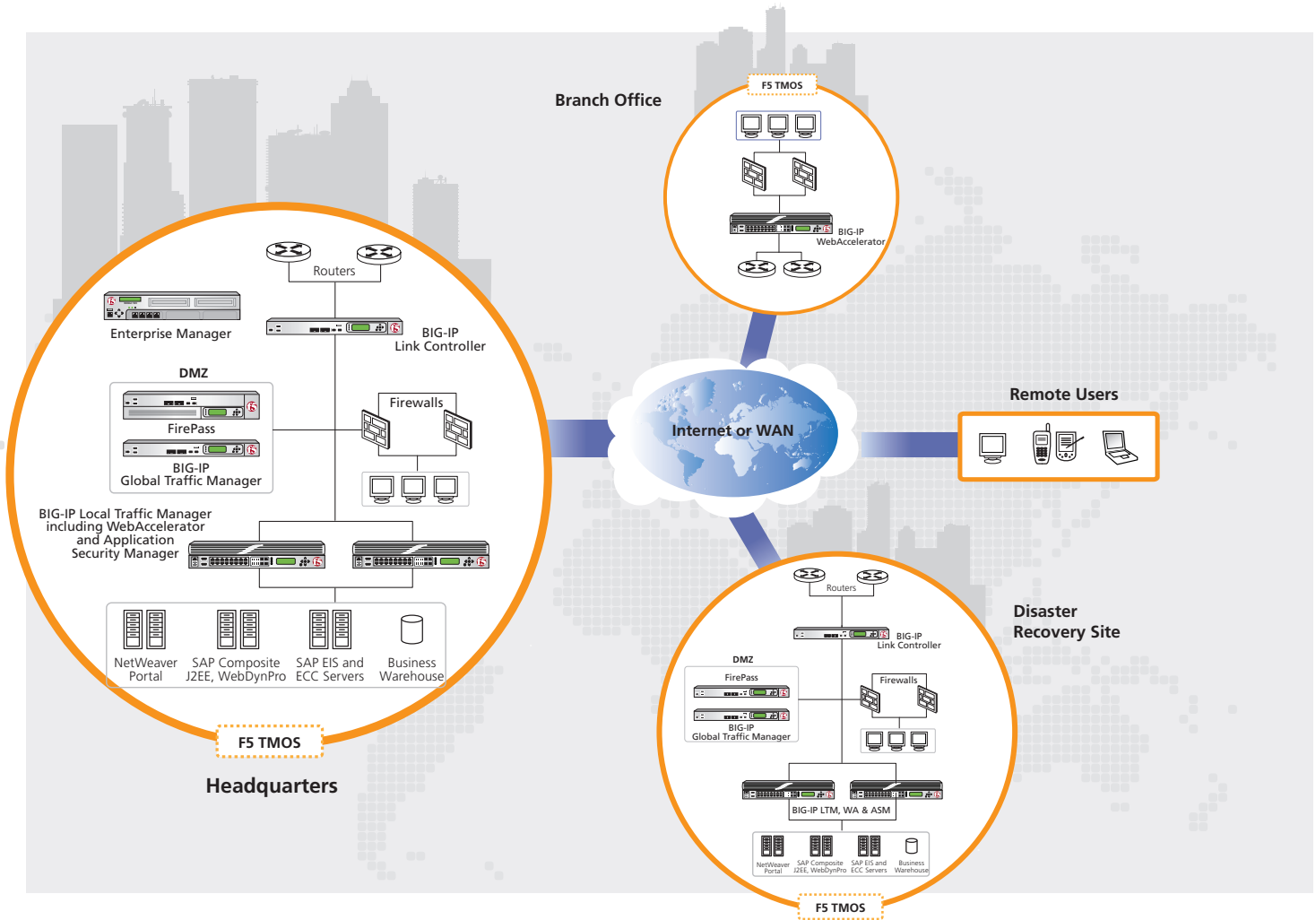
affect the users of SAP applications, resulting in lost productivity when users must wait for responses from the application. For example, call center efficiency is often measured by metrics such as volume and customer wait times, both of which are adversely affected by slow network connections because 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 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.

F5's Application Ready Solution for SAP: Explore it. Deploy it. And run your business with it.

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.



Additional Information

SAP and F5 Solution Documents

[Deploying the BIG-IP System v10 with SAP NetWeaver and Enterprise SOA: Enterprise Portal](#)
Includes the configuration for the Application Ready Template, as well as manual configuration procedures for the BIG-IP LTM with the WebAccelerator module, version 10.

[Deploying the BIG-IP System v10 with SAP NetWeaver and Enterprise SOA: ERP Central Component](#)

Includes the configuration for the Application Ready Template, as well as manual configuration procedures for the BIG-IP LTM with the WebAccelerator module, version 10.

[Deploying F5 with SAP NetWeaver and Enterprise SOA](#)

Includes the configuration procedures for the BIG-IP LTM system with the WebAccelerator module version 9.x, the FirePass controller, and WANJet appliance.

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

For more information about F5's Application Ready Solution Portfolio, visit <http://www.f5.com/products>.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

