APPLICATION READY NETWORK GUIDE

ORACLE'S SIEBEL BUSINESS APPLICATIONS 8.0

Comprehensive Application Ready infrastructure that enhances the security, availability, and performance of Oracle's Siebel deployments

INTEGRATED WITH

ORACLE®

SIEBEL CUSTOMER
RELATIONSHIP MANAGEMENT

SUMMARY

Oracle® Corporation is the world's leading supplier of software for information management, and the first software company to develop and deploy 100% internet-enabled enterprise software across its entire product line. Oracle's Siebel Business Applications help provide insight to the right person at the right time, leading to faster, better informed decisions. Siebel CRM 8.0 leverages the entire Oracle technology stack to bring value to your critical end-to-end business processes.

F5 Application Delivery Networking Solutions are the networking foundation for this market leading CRM and Analytics application. Oracle and F5 have validated and jointly documented the interoperability of F5's BIG-IP LTM and WebAccelerator (the BIG-IP module and standalone appliance) solutions with Siebel working in hundreds of customers worldwide. And Siebel has validated BIG-IP system for interoperability with Siebel Business Applications version 7 through 8. F5 ensures your organization achieves maximum ROI with the minimum amount of work by providing an Application Ready Network to help you optimize, secure, and deliver Siebel applications across the LAN and WAN.

Benefits and F5 value

User Experience and Application Performance

Oracle's Siebel Release 8 has been called the most complete, easy-to-use, and technologically advanced CRM suite ever shipped. Organizations using this Siebel application suite rely on these applications on a daily basis for mission-critical tasks. F5's Application Ready Network for Siebel Business Applications ensures application availability, optimizes performance, and helps dramatically increase user productivity, helping your business, and the Siebel applications it relies on, succeed.

Too often, IT departments embark on expensive application deployments, and when the new application is rolled out, despite being perfectly configured, users are unsatisfied with performance. This typically has nothing to do with the application itself, but often is a result of network conditions, IT infrastructure challenges, or latency across the WAN. These issues can adversely affect adoption rates, causing business productivity to plummet. F5 can quickly and easily solve man of these network infrastructure challenges by optimizing the network for Siebel applications, ensuring the best possible user experience.

When application delays are discovered, frequently an organization's solution is to buy more bandwidth or increase server capacity. Unfortunately, this does nothing to address the one of the fundamental causes of application delays: latency. 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 browser and the web application, F5 mitigates the effects of WAN latency, networking errors, and packet loss. This improves the response times of the Siebel applications for end users, allowing them to be more productive. For example, F5 improves the transaction time of first time visits to Siebel applications by 68% (see Figure 1).

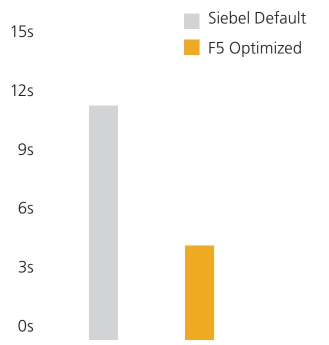


Figure 1: *First time visits to Siebel Call Center in seconds with and without F5.*

Because F5's unique operating system is a full proxy, F5 provides the most efficient network possible. F5 devices 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 - tasks that are outside the control of Siebel Business applications. This relieves the servers, and provides increased efficiency. By reducing unnecessary protocol communication across the network, F5 improves application response times and utilization for Siebel and other applications on the network.

Another way F5 improves the efficiency of Siebel applications is by offloading processor-intensive tasks that aren't vital to application processing. F5 devices include custom hardware and software that alleviate duties such as compression, caching, SSL processing and certificate management from the Siebel devices. By offloading these types of tasks onto F5's centralized and high powered network devices, F5 greatly improves server productivity and allows organizations to reduce the amount of necessary hardware by 20-40%

F5's TCP optimizations increase end user performance, whether the user is on a LAN or 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 has worked closely with Siebel to validate our solution for Siebel Business Applications 8.0. As part of the joint configuration, Siebel and F5 have created a script that automatically generates the F5 configuration, which greatly reduces deployment time and complexity, and frees valuable IT resources to work on other projects. As part of the Application Ready Network, F5 has configured, tested, and tuned our devices with a number of Siebel Business Applications and carefully documented the procedures in our Deployment Guides for Siebel and other Oracle applications. F5 also provides configuration Profiles and Policies to make configuration incredibly simple yet powerful and flexible, with some policies including prebuilt drop-downs for Siebel applications.

F5 helps protect the investment in the application, minimizing the initial negative impact on the ROI of a new application deployment due to lost productivity, increased helpdesk call volume, and adverse network conditions.

Application Security

While application performance is an important part of any Siebel implementation, if the application is not secure, the deployment will not be successful. Most network security measures, such as firewalls and intrusion detection/protection systems simply cannot adequately protect applications. New application-specific attacks appear harmless to network security measures, and can wreck havoc on applications. According to a 2006 CSI/FBI study[1], 68% of respondents reported 100% of security-related losses came from company system penetration from the outside, despite the fact that 98% of the respondents had firewalls in place and 69% implement IPS technologies. Firewalls have to leave application ports open for services, such

[1] CSI/FBI Computer Crime and Security Survey: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Benefits and F5 value

as HTTP, in order for requests to make it on the network. These types of general protection devices aren't nearly enough to protect Siebel Business applications and the information they contain.

The good news is that F5 provides extremely granular, application-specific security for Siebel applications. Along with blocking known attacks, F5 goes much further by also using a positive security model, allowing only approved, acceptable traffic to pass to the applications. 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 cannot efficiently address HTTP and HTTPS-borne threats.

In addition to analyzing and blocking known attack signatures, F5 security solutions can strip out identifying OS 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 out 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 Oracle applications, 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 the Siebel 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 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 third-party authentication 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 Siebel Business applications, and the information they contain, remain completely secure.

Unified Security Enforcement and Access Control

After ensuring application security, the focus shifts to enforcing security policies and access control. Because today's workforce is increasingly mobile, and more business-to-business transactions are taking place, organizations need to extend the reach of their internal applications to mobile employees, and

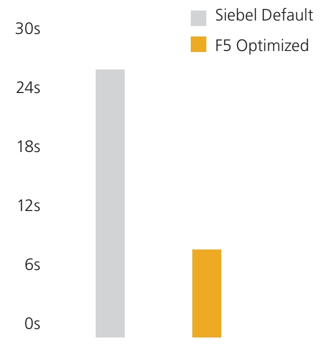


Figure 2: *F5 speeds document retrieval on first visits by 72%.*

partners, contractors, and suppliers. Additionally, these users are going to require different levels of access, and are likely going to be attempting access from widely different devices.

F5 easily handles these challenges and more with a complete approach to security enforcement and access control regardless of end user, client type, application, access network, or network resources.

In the past, remote access was typically 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.

To handle different access types, F5 allows you to easily configure different groups of users (such as an "employee" group, a "partner" group, and a "contractor" group) and provide different levels of access based on these groups. This is extremely useful for organizations who need to provide remote access to the network and Siebel applications to their employees, but also allow contractors or partners access to a specific portion of the application. F5 centralizes access control, and makes configuring and enforcing

Benefits and F5 value

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 also gives users the ability to allow or restrict configuration objects on our devices with virtual administration domains, so a single device to be managed by multiple application teams without interference. Every user can be assigned to specific administrative domains that 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

Creating a comprehensive and effective disaster recovery and business continuity plan is a major concern for today's IT professionals. Organizations must be prepared for unexpected events and outages that can interrupt service, or even bring down entire data centers. Not only do organizations have to ensure business continuity in wake of these events, but they must comply with industry and government regulations concerning data protection and disaster recovery. F5 products are uniquely positioned to help organizations mitigate these types of disasters. F5 virtualizes data centers, VPN access, optimization and traffic in an integrated fashion – ensuring that business-critical Siebel Business 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 an event occurs that prevents most employees from reaching the office, F5 ensures that employees can still be productive. Our remote access solution easily provides extremely secure remote access to the network, or even direct access to the appropriate Siebel application. This means that even though the physical office might be unavailable, as long as a single datacenter is still up, business can continue.

F5's remote access solution much easier to deploy and use than IPsec technology. It can be configured to allow access to Siebel applications with the click of a button, without requiring the user to pre-install or configure any software. And to provide the best possible remote user experience, F5 also provides TCP compression and additional caching to enhance performance for the remote users accessing the network.

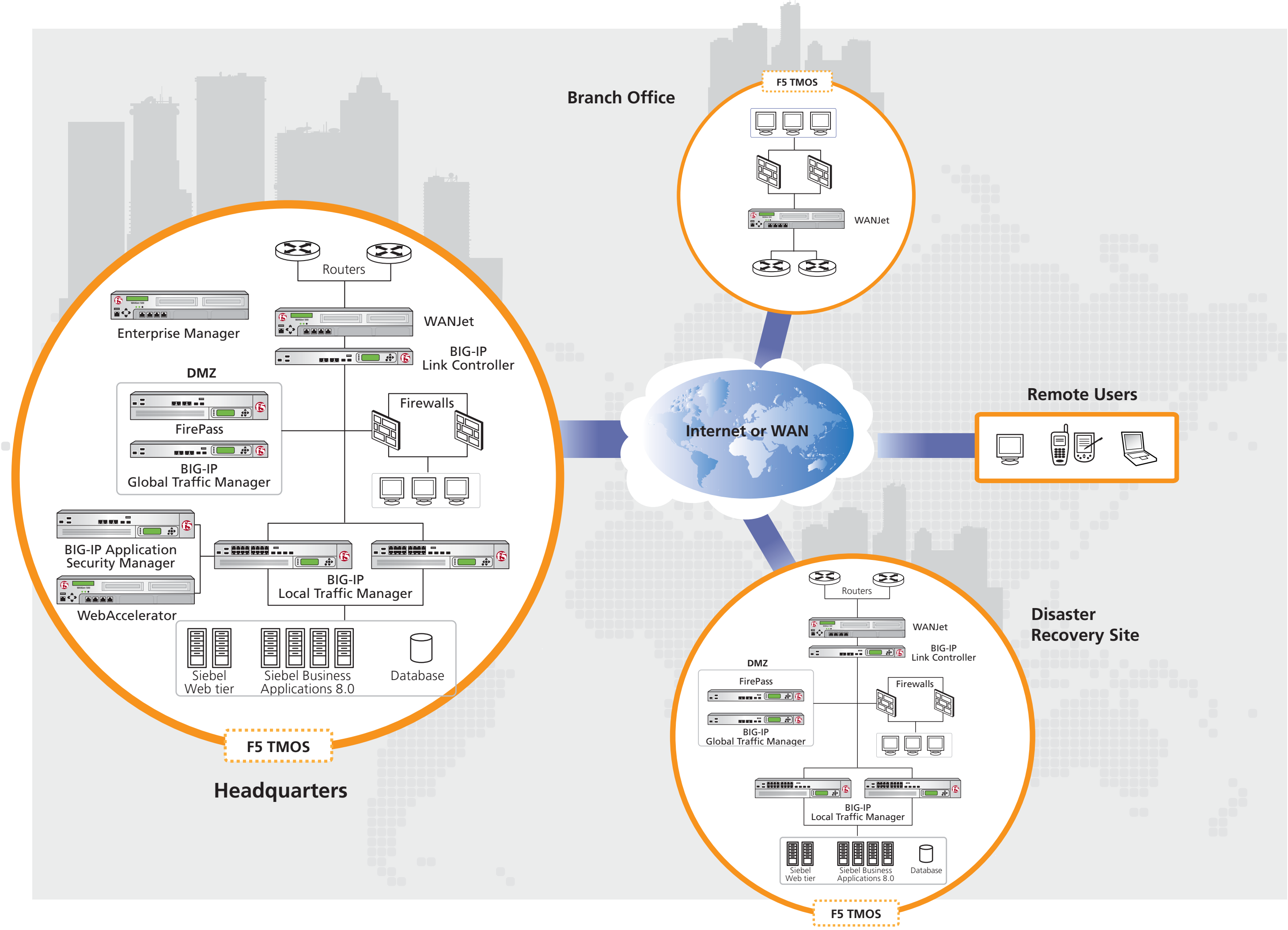
F5 can help even if the disaster doesn't happen to your organization, but to your ISP. F5 simplifies multi-homed deployments so you no longer need ISP cooperation, designated IP address blocks, ASNs, or reliance on complex BGP configurations to protect your network from ISP failures. With F5 technology, 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.

Minor disasters, such as failed hardware, are not even noticed, as F5 devices automatically detect a failure, and direct traffic away from the problematic device. Once the problem as been solved, F5 devices automatically detect the device is once again available and begin sending traffic there. This is also useful for patch management or maintenance windows. Administrators can easily mark down groups of devices from the F5 device, perform patching or other maintenance while other devices remain in service. Once the maintenance is complete, those servers go back in the pool, and the remaining servers are taken down for maintenance, all with zero downtime.

F5's Application Ready Network provides a secure and optimized platform to deliver Siebel Business applications, ensuring availability and maximum return on investment.

Global F5 and Siebel Deployment

The following example shows a global configuration, using the F5 suite of products to optimize, secure and deliver Siebel Business application deployments over the WAN and LAN.



Additional Information

Deployment Guides

Siebel Business Applications 8.0

Deploying F5 with Siebel Business Applications 8.0. Comprehensive deployment guide that includes the configuration for the BIG-IP LTM and the WebAccelerator for the Siebel 8.0 web and applications tiers.

For more information about the partnership between F5 and Oracle|Siebel, including more deployment guides and other solution documents, see the *Siebel and Oracle Application Pages* on the F5.com.

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.

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.

www.f5.com