



What's inside:

- 2 Improving application performance and user experience
- 3 Enhancing application security
- 4 Providing unified security enforcement and access control
- 5 Enabling seamless business continuity and disaster recovery

F5 and WebLogic help align your IT agility with the demands of your business

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. With the addition of BEA WebLogic Server to Oracle's already impressive Middleware portfolio, enterprise organizations have a platform that spans Java Application Servers, transaction processing monitors, SOA and business process management, user interaction and Web 2.0, identity management, business intelligence, enterprise content management and vertical-specific technologies.

F5 and Oracle have collaborated on delivering market-leading application delivery solutions for WebLogic Server 10. F5 has designed an integrated, agile and adaptable network platform for delivering WebLogic applications across the LAN and WAN. The result is an intelligent and powerful solution that secures and speeds your WebLogic deployment today, while providing an optimized architecture for the future. F5 enables IT agility, your way.

Key benefits

Increase WebLogic Portal performance over the WAN

F5 WAN optimization technologies can dramatically increase WebLogic Portal performance by more than 5x across the WAN.

Enhance Security

F5 gives peace of mind with comprehensive application-level security.

Gain WebLogic server capacity

Extend server capacity by offloading tasks like compression and SSL processing onto F5's unified, simple to manage platform.

Reduce bandwidth usage

Achieve 20 to 30 times bandwidth reduction for remote office users.

Increase administrator efficiency

F5's application templates, WebLogic policies, and step-by-step configuration guidance help reduce deployment cycles by 1/3rd.

Benefits and F5 value

F5's application ready solution for Oracle BEA WebLogic ensures a secure, fast and available deployment, providing the following benefits to organizations, and their end users.

Improving application performance and user experience

The Oracle|BEA WebLogic suite of products, including WebLogic Server® and WebLogic Portal®, are mission-critical applications that businesses rely on for day-to-day operations. Users demand a smooth and speedy application experience, and don't really care if the network or other factors are at fault for slowing the application; they just care whether it's responsive. F5 gives organizations the flexibility to deploy WebLogic solutions that scale and adapt on demand. We ensure your customers, employees, and partners have the best possible experience by delivering WebLogic applications that are fast, secure and available.

According to a recent Forrester study, respondents indicated that 75-94% of their IT priorities are tied to an application rollout or upgrade, and 71% experienced some sort of deployment issue, such as unacceptable performance, in their production environment¹. These issues typically have nothing to do with the applications themselves, and are a often result of network infrastructure problems or latency over the WAN. And the IP network is commonly a shared resource, with a variety of other services, including email, VOIP, and general Internet access, consuming network resources which can negatively impact the performance of WebLogic applications. F5's Application Ready Solution for WebLogic solves many of these issues by optimizing the network for BEA WebLogic and other applications, ensuring the best possible user experience.

With F5, IT departments do not have to spend hours or even days tuning the applications and tweaking the network parameters to improve performance. F5 ensures the successful implementation of WebLogic applications by integrating our intelligent application delivery with advanced WAN optimization technologies. This enables traditional acceleration technologies like SSL offloading, compression, caching, and traffic prioritizing to combine with optimization technologies like symmetric adaptive compression and application quality of service, reducing complexity in your data center and increasing performance for your end users. F5 devices adapt, in real time, to the latency, packet loss, and congestion characteristics of WAN links, to fully utilize available bandwidth and accelerate application traffic. These optimizations are particularly effective when delivering services over congested links, and are typically many times greater than the gains made by tuning the WebLogic applications.

F5 can further improve the performance of WebLogic WAN traffic by optimizing application protocols, prioritizing traffic, optimizing TCP from clients to servers, and reducing the amount of data sent over the WAN, helping to prevent costly bandwidth upgrades. These technologies ensure that critical or time-sensitive applications receive priority over others to maximize performance over the WAN. They provide granular control of traffic based on need, enabling you to manage and prioritize bandwidth per application and improve quality of service for WebLogic users over the WAN.

F5 can even help application speed for global users connecting to the WebLogic applications on the network. It doesn't matter that these users are often using a number of different types of connections that have widely varying speeds. F5 devices efficiently control the traffic flows for WebLogic deployments by optimizing client side delivery while maintaining server-optimized connections on the inside of the network. And now, F5 devices can be deployed symmetrically to create a site-to-site secure connection to further improve transfer rates, reduce bandwidth, and offload applications for more efficient WAN communication.

Green Infrastructure

F5 can accelerate and secure applications while enhancing performance and availability, all on the same device. This reduces energy consumption with no additional hardware or rack space needed.

To further reduce the burden on the servers and increase productivity, 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, performance, and helps IT departments become a little more “green”. We also make security compliance even easier and save valuable IT time by enabling the exporting of policies for use by offsite auditors. Auditors working remotely can view, select, review, and test policies, without requiring critical time and support from the web application security administrator.

And F5 makes it easy to optimally configure our devices while maintaining flexibility and control of your infrastructure. Our devices contain acceleration policies specifically designed for WebLogic, enabling administrators to simply choose the policy from a list for out of the box optimization. And F5 deployment guides give step-by-step instructions on how to configure our devices with WebLogic. While deployment guides save a significant amount of time and effort, they still require manual input of each configuration procedure. Now, F5 has rolled our deployment guides into a wizard-like template, so optimally configuring F5 devices for WebLogic requires only minimal information and takes just minutes. Satisfying both end users and IT administrators has never been easier.

Enhancing application security

Most organizations have network security covered; firewalls, intrusion detection/protection systems, and other devices do an adequate job of protecting the network from attack. So it's no surprise that malicious users turned their attention to a target that typically does not have specific protection: applications. Most attacks targeting applications look completely harmless to firewalls and other network protection devices. And over 50% of all new vulnerabilities being identified on a weekly basis are attributed to web applications (SANS @RISK, “The Consensus Security Vulnerability Alert”).

Some level of application-specific security is imperative. Failure to keep data secure can be extremely costly, not only because of the value of the data itself, but the stiff penalties imposed for failing to meet compliance initiatives such as PCI, HIPAA, SOX, BASEL II, and other regulations.

F5 enables advanced, built-in security protection and remote auditing to help your organization comply with industry security standards, including PCI DSS, HIPAA, Basel II, and SOX, in a cost effective way—without requiring multiple appliances, application changes, or rewrites. F5 provides advanced reporting on new attacks such as layer 7 denial-of-service (DoS), brute force, SQL injection and more. With PCI reporting, F5 lists security measures required by PCI DSS 1.2, determines if compliance is being met, and details steps required to become compliant if not. In addition, F5 integrates with leading security vendors for vulnerability assessment, auditing, and real-time and database reporting to provide security breach reviews, attack prevention, and compliance.

Most of today's Intrusion Detection and Protection Systems, and even many application firewalls, are limited to guarding against a limited list of known attacks. But with the influx of new attacks targeting applications, this type of negative security protection isn't nearly enough. Unlike signature inspection methods, F5 also provides a positive security model, permitting only valid and authorized application transactions, while automatically protecting critical web applications from entire classes of HTTP and HTTPS-based threats (both known and unknown) such as Google hacking, cross-site scripting, and parameter tampering.

Scaling Access Control

By driving application and user identity into the network, organizations have a more centralized, repeatable and cost effective way to scale access control services.

F5 helps you protect your brand by shielding your websites from web scraping attacks that copy and reuse valuable intellectual property and information. By differentiating between a human and a bot behind a browser, F5 protects against automated requests to obtain data.

F5 can secure and accelerate applications while also enhancing performance and availability, on the same device. And now, all data can be symmetrically encrypted between local and remote F5 devices, providing a new way to ensure site-to-site data security. This secure connection, or tunnel, not only secures the data, but also improves transfer rates, reduces bandwidth, and offloads applications for more efficient WAN communication. This provides an efficient multi-solution platform for WebLogic deployments, adding security without performance reduction. Attacks are now filtered immediately and web applications are accelerated for improved user experience and application performance. Because there is no need to introduce new appliances to the network, overall energy consumption is reduced and no additional hardware or rack space is needed. F5 enables an all-in-one appliance solution for maximum cost effectiveness, and a cleaner, greener IT department.

With today's global, partnership-driven business landscape, protecting applications becomes even more important. F5's comprehensive Endpoint Security for remote access gives your WebLogic deployment the best possible protection for (and from) remote users. F5 technology prevents infected PCs, hosts, or users from connecting to your network and the applications inside, and delivers a Secure Virtual Workspace, pre-login endpoint integrity checks, and endpoint trust management.

And because malicious users can use any small piece of information as a clue to unlocking your network and applications, F5 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.

F5 products allow organizations to implement comprehensive application security, providing a centralized point of enforcement, and a coordinated and unified line of defense that lowers TCO and improves ROI.

Providing unified security enforcement and access control

As organizations expand into new markets and grow through mergers and acquisitions, more and more organizations outsourcing development, services or applications, and are trying to cope with the need to extend the reach of their internal applications to partners, contractors and suppliers. This means that companies are faced with more users and devices attempting to access protected resources. F5 provides a complete approach to providing access control regardless of end user, client type, application, access network or network resources.

F5 allows administrators to grant certain users – for example, business partners using equipment not maintained by the company – access to WebLogic applications and other extranet applications and sites. F5 provides centralized access and application availability services to users based on the context of the user and the application they are accessing. By driving application and user identity into the network, organizations have a more centralized, repeatable and cost effective way to scale access control services. This new simplified access management system allows users to easily access approved web applications and networks without multiple authentications for greater worker productivity.

Network administrators scale efficiently, simplify enforcement and reduce costs with F5 by removing a specialized proxy with one integrated high performance solution dramatically reducing CAPEX and OPEX. As users roam from office to remote locations, the F5 client accesses corporate networks and applications dynamically enabling mobile users to stay connected without business productivity declining. Application acceleration and security are designed together with access to scale supporting application growth and performance.

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 the origin or destination VLANs, IP addresses, and protocols. You can refine this security with stricter access rules based on authentication results or application responses. With F5, you can easily define custom security policies. All of these capabilities can be used to implement LAN segmentation, different zones, such as trusted, public, private, protected, and so on.

With F5, you can even partition our devices themselves, enabling organizational efficiency and an easy way to scale management. Every user can be assigned to specific administrative domains, that define which objects are visible to that user. For example, the application owner for WebLogic Portal can be given permission to only view or modify objects that reside in the Portal domain, while not being able to modify the configuration for additional WebLogic Server applications or other objects on the F5 device.

Enabling seamless business continuity and disaster recovery

Hurricanes, earthquakes, and other natural and man-made disasters have put business continuity and disaster recovery at the top of IT department priority lists. Because every minute an application is down or not responding properly can cost an organization thousands of dollars, deploying F5 devices with BEA WebLogic is essential for providing organizations with business-critical availability. Whether planning for a natural disaster, a pandemic like swine flu, trying to achieve regulatory compliance, or just carefully planning a new application deployment, F5 can help. F5 easily and effectively virtualizes data centers, VPN access, optimization and traffic in an integrated fashion.

F5 provides the industry's most comprehensive solution for site failover and business continuity. In addition to performing comprehensive site application availability checks, you can define 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.

In a situation where employees cannot reach the office to work, but at least one data center is still functioning, F5 provides secure remote access to the network and applications like BEA WebLogic that is much easier to use and scale than other solutions like IPsec – and much quicker to deploy and maintain in a disaster situation.

A disruptive event does not always have to be a disaster - even a hardware failure of a single server can cause expensive downtime. F5 makes hardware, software, and service failures inconsequential by automatically detecting failures and directing traffic away from the troubled server. Once the problem has been solved, F5 devices automatically detect the server and begin sending traffic there. This can also be useful for patch management or maintenance windows. Administrators can easily remove groups of devices from the F5 pool, 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.

For organizations with multiple ISP links, F5 simplifies multi-homed deployments so you no longer need ISP cooperation, large bandwidth connections, designated IP address blocks, ASNs, or high-end routers to protect your network from ISP failures. Using DNS-based technology that removes the dependency on BGP to provide failover capabilities, the F5 eliminates multi-homed problems such as latency, high update overhead, and inferior traffic management, ensuring that users can always get to the WebLogic applications. Organizations can benefit from guaranteed availability without delays or costly misrouting. It also gives you the ability to aggregate inexpensive links, with more granular control over which link to use based on performance, costs, and business policies.

And business continuity doesn't always have to do with a disruptive event. 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 WebLogic, as well as F5 devices, ensuring that your network and WebLogic 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 WebLogic devices. With F5, organizations have a strong solution for today and well into the future.

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

More Information

To learn more about F5 and WebLogic, use the search function on F5.com to find these and other resources.

Application Page

[BEA WebLogic Server](#)

Deployment Guides

[BEA WebLogic 10](#)

[BEA WebLogic 8.1 and BIG-IP v10.x](#)

[BEA WebLogic 8.1 and BIG-IP v9.x](#)

Oracle Solution Page on DevCentral

<http://devcentral.f5.com/Default.aspx?tabid=147>

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

