APPLICATION READY NETWORK GUIDE

PEOPLESOFT ENTERPRISE APPLICATIONS

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

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 PeopleSoft Enterprise applications are leaders in ERP and the leader in Human Resource Management Systems (HRMS) and Education/Campus Solutions. F5 has designed and painstakingly tested a comprehensive Application Ready Network infrastructure for PeopleSoft Enterprise applications, ensuring your organization achieves maximum ROI with the minimum amount of work. F5 provides all of the tools to help organizations optimize, secure, and deliver PeopleSoft Enterprise applications across the LAN and WAN.

Benefits and F5 value

User Experience and Application Performance

Oracle's PeopleSoft Enterprise applications are designed to address the most complex business requirements, providing comprehensive business and industry solutions. Organizations using PeopleSoft rely on these applications every day for business critical functions. If applications are not performing optimally because of configuration or infrastructure problems, user productivity drastically decreases. F5's Application Ready Network for PeopleSoft Enterprise applications ensures application availability, optimizes performance, and helps dramatically increase user productivity.

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 PeopleSoft Enterprise applications. This takes the workload off of the servers for increased server efficiency. By reducing unnecessary
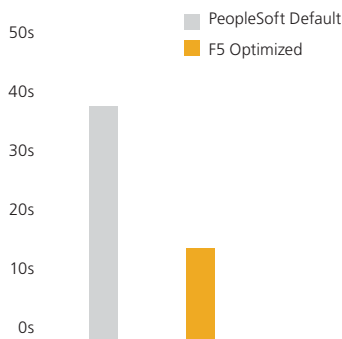

Figure 1: *Transactional user test results for a first visit timesheet update, using PeopleSoft HRM over the WAN.*

protocol communication across the network, F5 improves application response times and utilization for PeopleSoft and other applications on the network.

Because more and more users are requiring access to PeopleSoft applications from locations outside the corporate network, application performance over the WAN is quickly becoming a big concern for IT departments. WAN latency, adverse network conditions, infrastructure challenges, and other issues prevent web applications from being delivered quickly.

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

To further increase application performance and productivity for PeopleSoft Enterprise applications and other applications on the network, F5 provides a number of TCP optimizations. These optimizations, which combine session-level application awareness, persistent tunnels, selective acknowledgements, error correction, and optimized TCP windows, allow F5 devices 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.

Because PeopleSoft applications are constantly performing large numbers of transactions (such as timesheet entries, payroll processing, and General Ledger transactions) it is imperative that these devices are not bogged down with duties that are not vital to the application. Functions such as compression, caching, and

SSL processing take a significant amount of processing power from the servers. F5 devices include custom hardware and software that take on these processor-intensive tasks. 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%.

And not only does F5 make PeopleSoft Enterprise applications more productive, but F5 also provides a variety of options 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, F5 has configured, tested, and tuned our devices with a number of PeopleSoft Enterprise applications and carefully documented the procedures in our Deployment Guides for PeopleSoft 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 PeopleSoft Enterprise applications. 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.

F5 ensures responsive applications, which leads to increased adoption rates and more satisfied and productive users. This provides added benefit of reducing the load on call centers and help desks, as users are less likely to call the IT department complaining about speed issues that are often unrelated to the application itself. 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 call volume, and adverse network conditions.

Application Security

Because of the sensitive nature of the information contained in PeopleSoft Enterprise applications (and the stiff penalties imposed for failing to meet compliance initiatives), organizations need to have a robust security

Benefits and F5 value

infrastructure in place. Security to most organizations means having network firewalls and possibly an intrusion protection system in place. 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 as HTTP, in order for requests to make it on the network. These types of general protection devices aren't nearly enough to protect PeopleSoft Enterprise applications and the information they contain.

F5 provides organizations using PeopleSoft Enterprise applications with extremely granular, application-specific security. More than half of all new vulnerabilities being identified on a weekly basis are attributed to web applications[2]. PeopleSoft Enterprise applications include financial and payroll information that would be disastrous in the wrong hands. Network firewalls and intrusion protection/detection systems provide a level of protection against certain types of known attacks. F5 goes much further by also using a positive security model, allowing only known, 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 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 Oracle 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 PeopleSoft Enterprise applications, and the information they contain, remain completely secure.

Unified Security Enforcement and Access Control

While network and application security are important aspects of overall security for PeopleSoft deployments, they are not the only security concerns. With an increasingly mobile work force and more business-to-business transactions, organizations need to extend the reach of their internal applications to partners, contractors, and suppliers. These users are going to require access to protected resources from a variety of different devices. F5 provides a complete approach to security enforcement and providing access control 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.

Organizations using PeopleSoft Enterprise applications often need to allow third-party vendors access to a specific portion of an application. F5 enables you to easily configure different groups of users, such as an "employee" group, and a "payroll partner" group, and restrict access based on these groups. This is extremely useful for organizations who need to provide remote access to the network and PeopleSoft Enterprise applications to their employees, but also allow contractors or partners access to a specific application. F5 centralizes access control, and makes configuring and enforcing this type of control extremely simple.

[1] CSI/FBI Computer Crime and Security Survey: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml
[2] SANS@RISK, "The Consensus Security Vulnerability Report"

Benefits and F5 value

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. 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

Performance and security are not the only concerns facing today's IT professionals. They must also 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 is the only vendor to virtualize data centers, VPN access, optimization and traffic in an integrated fashion – ensuring that business-critical PeopleSoft Enterprise 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, F5 provides extremely secure remote access to the network (including PeopleSoft Enterprise applications), ensuring 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 PeopleSoft Enterprise 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.
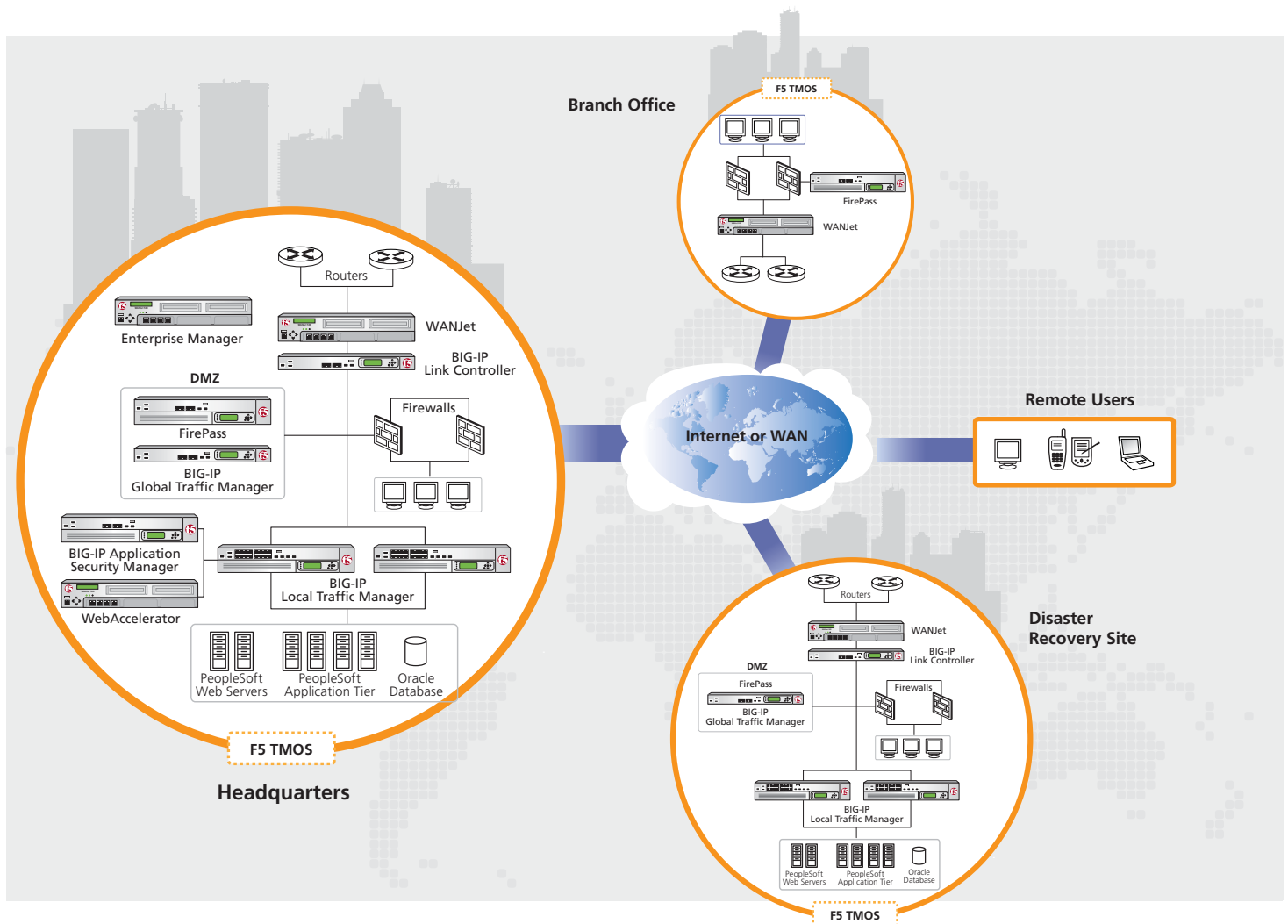
Even a hardware failure of a single server can cause expensive downtime, until a administrator can remove the device from service. F5 makes

hardware failures a complete non-issue by automatically detecting a failure, and directing traffic away from the problematic server. Once the problem as been solved, F5 devices automatically detect the server and begin sending traffic there. This is also useful for patch management or maintenance windows. Administrators can easily remove groups of devices from the F5 load balancing 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.

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

Global F5 and PeopleSoft Deployment

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

Additional Information

Deployment Guides

Deploying F5 with PeopleSoft Enterprise Applications

Provides detailed, step-by-step procedures on how to configure the BIG-IP LTM system, WebAccelerator, and FirePass controller with the PeopleSoft Enterprise Applications.

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

For more information about the partnership between F5 and Oracle|PeopleSoft, see the Oracle 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 Oracle page on DevCentral for Oracle-specific forums and other useful information about F5 integration with Oracle applications.

www.f5.com