Technical Case Study: Sun Java Enterprise System SunWeb 4.0

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–7154–10
March 2007

070227@16599

Contents

Tables

Figures

Preface

This technical case study describes the implementation of a Sun Java™ Enterprise System (Java ES) architecture for the deployment of SunWeb™ 4.0, the web-based internal portal for Sun Microsystems employees.

This document describes the requirements for the deployed solution, the architecture developed to meet those requirements, and the deployment specifications. It does not provide detailed information about the installation and configuration of Java ES software. The intent of this document is to describe Sun's deployment of a Java ES infrastructure in such a way that the information can be adapted for a variety of business problems and environments, keeping in mind that the planning, design, and implementation of any Java ES solution is driven primarily by the needs of the specific enterprise.

Who Should Use This Case Study

This case study is intended for system architects who are developing architectures similar to the one described in this document. Architects with similar requirements can use this architecture as the basis for their own.

This case study assumes familiarity with the following:

- The UNIX® operating system
- Internet protocol (IP) computer networks
- Enterprise-level software products
- Java ES and its components

Before You Read This Case Study

Familiarize yourself with the basics of Java ES before reading this case study. See “Java ES Documentation” on page 10 for more information about documentation resources.

How This Case Study Is Organized

This case study describes Sun's deployment of a Java ES infrastructure for its SunWeb internal portal and is organized in the following chapters:

- Chapter 1 introduces the SunWeb internal portal and the SunWeb 4.0 portal deployment.
- Chapter 2 describes the business and technical requirements for the deployment.
- Chapter 3 describes the Java ES architecture developed to meet the requirements.
- Chapter 4 describes the detailed technical specifications developed from the deployment architecture.

Java ES Documentation

This case study does not provide detailed procedures for installing and configuring the Java ES software used in the architecture. For specific procedures, see Java ES documentation at `http://docs.sun.com/app/docs/prod/entsys`. The documentation provides extensive information about Java ES, its components, and its implementation. Additional Java ES resources are also available at `http://www.sun.com/bigadmin/hubs/javaes/`.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is the 7- or 9-digit number found on the book's title page or in the document's URL. For example, the part number for this document is 819–7154–10.

CHAPTER 1

Introducing the SunWeb Deployment

This technical case study describes the implementation of a Sun Java™ Enterprise System (Java ES) architecture for the deployment of SunWeb™ 4.0, the web-based internal portal for Sun Microsystems employees. This document describes the business and technical requirements for the deployed solution, the Java ES architecture developed to meet those requirements, and the deployment specifications developed from the architecture.

The intent of this document is to describe the SunWeb portal deployment so that you can adapt the information for your own deployment. While every deployment is different, the SunWeb 4.0 portal is a good example of how Java ES can be deployed in a complex enterprise environment.

This chapter introduces the SunWeb portal and provides an overview of the SunWeb 4.0 deployment. Subsequent chapters provide technical details for the deployment.

This chapter contains the following sections:

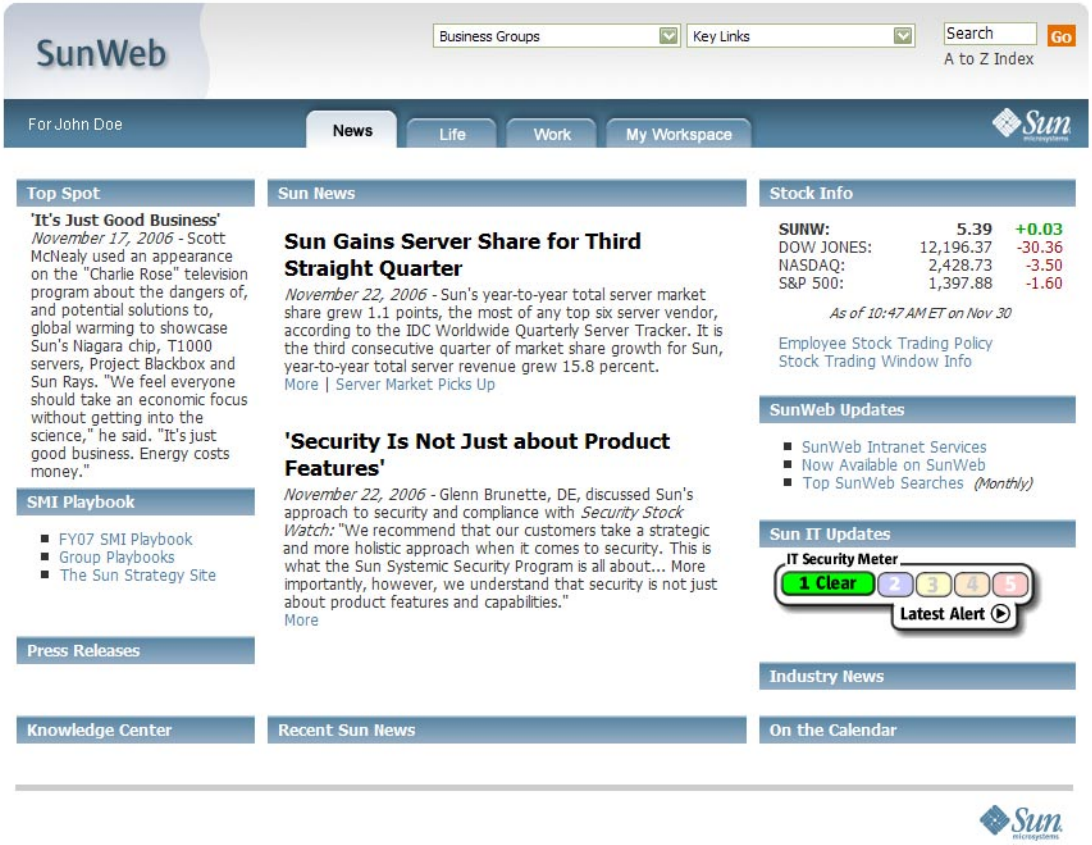
- "About the SunWeb Portal" on page 11
- "Business Case for SunWeb 4.0" on page 13
- "Deployment Planning" on page 13
- "Deployment Overview" on page 15
- "Software in SunWeb 4.0" on page 18
- "Hardware in SunWeb 4.0" on page 20

About the SunWeb Portal

The SunWeb portal is the primary means through which business information and services are delivered to Sun employees and is the standard way the Sun workforce collaborates and shares knowledge. The primary goal of the SunWeb portal is to provide content and services to a global workforce anywhere, anytime, and on any device. SunWeb is continuously evaluated and enhanced to meet that goal.

The SunWeb portal provides services to internal users around the world, which includes employees, contractors, interns, and anyone with a valid Sun ID. Users access email, calendars, applications, collaboration tools, and a wide variety of content sources such as news and blogs.

The following image shows the main page users might see when they log in.



Top Spot

'It's Just Good Business'
November 17, 2006 - Scott McNealy used an appearance on the "Charlie Rose" television program about the dangers of, and potential solutions to, global warming to showcase Sun's Niagara chip, T1000 servers, Project Blackbox and Sun Rays. "We feel everyone should take an economic focus without getting into the science," he said. "It's just good business. Energy costs money."

SMI Playbook

- FY07 SMI Playbook
- Group Playbooks
- The Sun Strategy Site

Press Releases

Knowledge Center

Sun News

Sun Gains Server Share for Third Straight Quarter
November 22, 2006 - Sun's year-to-year total server market share grew 1.1 points, the most of any top six server vendor, according to the IDC Worldwide Quarterly Server Tracker. It is the third consecutive quarter of market share growth for Sun, year-to-year total server revenue grew 15.8 percent.
More | Server Market Picks Up

'Security Is Not Just about Product Features'
November 22, 2006 - Glenn Brunette, DE, discussed Sun's approach to security and compliance with *Security Stock Watch:* "We recommend that our customers take a strategic and more holistic approach when it comes to security. This is what the Sun Systemic Security Program is all about... More importantly, however, we understand that security is not just about product features and capabilities."
More

Recent Sun News

Stock Info

SUNW:	5.39	+0.03
DOW JONES:	12,196.37	-30.36
NASDAQ:	2,428.73	-3.50
S&P 500:	1,397.88	-1.60

As of 10:47 AM ET on Nov 30

Employee Stock Trading Policy
Stock Trading Window Info

SunWeb Updates

- SunWeb Intranet Services
- Now Available on SunWeb
- Top SunWeb Searches *(Monthly)*

Sun IT Updates

Industry News

On the Calendar

FIGURE 1–1 Main SunWeb Page

Some features are standard for all users, while others vary depending on the user's role at Sun and how SunWeb was accessed. SunWeb can be accessed from a computer or device connected to Sun's corporate network (SWAN) or from a computer or device not connected to SWAN using the public Internet and secure remote access.

Business Case for SunWeb 4.0

The SunWeb portal is driven by the current realities of work. The workforce is global and knowledge based, the work location is anywhere with a high-speed Internet connection, and the work schedule is whatever is needed to get the job done across multiple time zones.

The SunWeb portal is driven by these work realities and the continuous challenges that come with them, such as access anywhere, anytime, and on any device, while meeting security, availability, response time, and redundancy requirements and fulfilling corporate compliance and reporting responsibilities. The complexities posed by Sun's work realities are considerable and underscore the critical nature of SunWeb:

- Approximately 40,000 employees in 170 countries
- 18 major business divisions
- 18,000 internal web sites
- 4 million internal web pages
- 5 million emails per day
- More than 900 internal applications

The SunWeb 4.0 portal deployment addressed these complexities by consolidating content, services, and applications on a single platform built on Java ES. The Java ES solution helped Sun achieve many key business objectives, including the following:

- **Improved employee productivity.** Sun's workforce is connected to whom and what they need when and where they need it based on user roles and entitlements.
- **Reduced operational costs and complexity.** Sun's business groups use a single platform for all phases of the information management and distribution life cycle.
- **Demonstration of Sun's use of Sun technology.** Sun's customers see a real-world implementation of a Java ES architecture and gain a better understanding of how a Java ES solution might be designed and deployed in their own environment to address similar business problems and requirements.

Deployment Planning

The SunWeb portal deployment began with deployment planning, a critical piece of any successful deployment. The following table briefly describes the high-level tasks involved with planning the SunWeb deployment and points to specific information in this case study. Consider using a similar approach when planning your own deployment.

This case study is specific to the SunWeb portal deployment. For general information about deployment planning, see the *Sun Java Enterprise System Deployment Planning Guide* in the Java ES documentation set.

TABLE 1–1 SunWeb Deployment Planning Task Map

Task	SunWeb Information
1. Analyze business goals and develop business requirements. Business requirements are used to determine the technical requirements for the deployment.	See Chapter 2, which describes SunWeb requirements.
2. Convert the business requirements into technical requirements. Technical requirements are used to design the deployment architecture and specify quality of service (QoS) features such as performance, availability, and scalability.	See Chapter 2, which describes SunWeb requirements.
3. Develop the deployment scenario. The deployment scenario is used to design the deployment architecture. The scenario consists of a logical architecture, which identifies the Java ES components and other software needed to provide the services, and the requirements defined in the previous step.	See Chapter 3, which describes designing the SunWeb architecture.
4. Develop the deployment architecture. The deployment architecture is based on the deployment scenario and is used to define the specifics of the deployment, mapping the components specified in the logical architecture to a physical environment. While the logical architecture deals with components in a general sense, the deployment architecture specifies details such as the number of computers, how they are connected, how many instances of each component are needed, and so on.	See Chapter 3, which describes designing the SunWeb architecture.
5. Develop the deployment specifications. Deployment specifications are used to implement the solution. The specifications are based on the deployment architecture, but add the detailed information needed to install and configure the set of components identified in the architecture.	See Chapter 4, which describes preparing the deployment specifications.
6. Implement the deployment architecture. Implementation typically involves installing and configuring the hardware infrastructure, installing and configuring the software, modeling users and resources within an LDAP directory design, and so on. The detailed installation and configuration plans are developed from the deployment specifications.	Specific installation and configuration procedures are not provided in this case study. For detailed information about installing and configuring Java ES software, see the Java ES documentation resources at `http://docs.sun.com/app/docs/prod/entsys`. Additional Java ES resources are also available at `http://www.sun.com/bigadmin/hubs/javaes/`.

Deployment Overview

The core SunWeb portal platform is a suite of applications built primarily on Java ES, complemented by content management, document management, search, and collaboration applications. All services are available from a single, distributed Java ES deployment.

As with other such production deployments, the SunWeb 4.0 portal uses an arrangement of portal and Java ES components distributed among several computers behind a load balancer. The deployment encompasses configuration information, a variety of data and data sources, custom code that defines the user interface, security mechanisms, content sources and access, and integration with other in-house and third-party products and services.

Non-Java ES software is included in the deployment, as are services and applications already running on SWAN. For more information about non-Java ES software used in the deployment architecture, see “Preparing the Logical Architecture” on page 30.

SunWeb content is aggregated from a number of different sources, including a content management system and other content providers that are integrated with the SunWeb infrastructure. Content providers include the following:

- MySales and MyMarketing portals, which provide extensive sales and marketing tools and resources
- SunWeb Collaboration, an online knowledge management service that enables virtual teams to develop, share, and retain information
- An executive management portal, available only to executives
- The search engine

More information about the mechanics of content delivery is provided in Chapter 3, including “Analyzing User Interactions with the SunWeb Components” on page 32.

The Sun IT team designed SunWeb 4.0 to meet several key objectives and provide several key services. An overview of those objectives and services is provided in the following sections.

Key Objectives of SunWeb 4.0

The following table lists the key objectives of the SunWeb 4.0 deployment. These objectives might be similar to your own.

TABLE 1–2 Key Objectives of SunWeb 4.0

Objective	Description
Integration and consolidation	SunWeb resources were split across many systems and the integration and consolidation of services was a key driver for the SunWeb 4.0 deployment. The SunWeb 4.0 portal integrated Portal Server Secure Remote Access, mobile access, communication channels (mail and calendar), a blogs channel, and the SunWeb portal desktop into one common platform. This integration of services onto one platform required substantial modification to the existing architecture. Single sign-on functionality was also implemented to provide single sign-on between Portal Server with Access Manager to other applications.
Multitier architecture implementation	A key objective of the deployment was to implement a multitier reference architecture to meet new scalability needs and to decouple the Portal Server, Access Manager, and Directory Server deployment for the multitier architecture.
Software upgrade	A software upgrade was necessary to leverage the latest functionality in Java ES components and the Solaris™ Operating System (Solaris OS). The SunWeb 4.0 framework implemented Sun Java Enterprise System 2005Q1 and Solaris 10 OS with zones (see "Software in SunWeb 4.0" on page 18).
Hardware upgrade	A hardware upgrade was long overdue. The SunWeb 4.0 deployment moved from shared hardware to dedicated Sun Fire™ x64 servers running Solaris 10 OS, demonstrating a reference architecture with zones on AMD Opteron™ processors (see "Hardware in SunWeb 4.0" on page 20).

Key Services Provided by SunWeb 4.0

The SunWeb 4.0 deployment provided enhanced capabilities in many areas, including personalization, remote access, and search. Many of the enhancements were made in response to user input and feature requests.

The following table provides an overview of some of the key services delivered with the deployed solution. Your enterprise might require similar services. Technical details for these and other services are provided in "Detailed Service Requirements" on page 22.

Note – Mail and calendar services are provided by instances of Sun Java System Messaging Server and Sun Java System Calendar Server that are already deployed and running on the main corporate network. The SunWeb portal deployment uses Portal Server channels to provide SunWeb users with access to these services on their portal desktops (to enable this feature, users must add the channels to their portal view).

TABLE 1–3 Key Services Provided by SunWeb 4.0

Service	Description
Portal Server Secure Remote Access (SRA)	■ Provides secure remote access from outside of Sun's corporate network (SWAN). ■ Replaces an older application used for remote access, providing enhanced, updated, and integrated services that are more comprehensive and reliable. ■ Provides device independence that enables users to connect to SunWeb securely from any Java enabled, web-connected computer or mobile device. Remote users launch a browser, enter the URL for the SRA service, authenticate using token-based authentication, and are logged directly into SunWeb with secure access to a customized portal desktop, applications, and content. ■ Enables users to access SunWeb from most customer sites, providing an advantage over virtual private network (VPN), which is often blocked. ■ Provides enhanced security in certain situations when compared with VPN. ■ Enables users to send and receive mail, update their calendars, access their home directories, surf sites within SWAN, and open telnet sessions. ■ Provides a remote access channel to users who log in using SRA. This channel provides various tools such as FTP.

TABLE 1–3 Key Services Provided by SunWeb 4.0 *(Continued)*

Service	Description
Mail channel	■ Enables remote users to add the mail channel to their SunWeb view and to read, write, and reply to messages using the mail channel when connecting to SunWeb through a remote access gateway. ■ Brings the most recent mail messages to the SunWeb view. ■ Enables users to choose how many messages to display and to launch messages directly from SunWeb. ■ Is highly customizable and enables users to perform a high degree of personalization.
Calendar channel	■ Complements the mail channel (requires a Calendar Server account). ■ Enables remote users to add the calendar channel to their SunWeb view and to manage their calendar when accessing SunWeb through a remote access gateway. ■ Is highly customizable and enables users to perform a high degree of personalization.
Blogs@Sun channel	■ Enables users to subscribe to specific blogs and authors. ■ Enables the personalized SunWeb view to be updated as new postings become available.
SunWeb (Java ES) search	■ Integrates the Portal Server search engine with the portal desktop and the SRA service to provide a single entry point. ■ Gives users a more robust search engine for searching within SWAN.

Software in SunWeb 4.0

SunWeb was one of the first implementations of Sun's suite of middleware products known as Sun Java Enterprise System (Java ES). Java ES is a software infrastructure that provides a complete set of middleware services to support enterprise applications distributed across a network or Internet environment. The Java ES components that provide the services are installed using a common installer, synchronized on a common set of shared libraries, and share an integrated user identity and security management system. The SunWeb 4.0 portal is built on Sun Java Enterprise System 2005Q1 and demonstrates a comprehensive implementation of the Java ES platform.

The following table lists the key Sun software components used in SunWeb 4.0 and the functionality each component provides. Your enterprise might require similar functionality.

Note – All software used in the deployment is not listed in the table, just the key Java ES components. For more information about other components and applications used in the deployment, see "Preparing the Logical Architecture" on page 30.

TABLE 1–4 Key Sun Software Used in SunWeb 4.0

Product	Functionality
Sun Java System Portal Server 6.1	Portal Server is the integration framework for the presentation of content and services and performs display-specific tasks such as desktop and channel presentations. Portal Server provides the following SunWeb functionality: ■ Mobile access desktop for internal users ■ SRA ■ End-to-end secure SSL using the Rewriter and Netlet proxies
Sun Java System Access Manager 6.3	Access Manager performs tasks related to authentication, roles, and policies and provides the following SunWeb functionality: ■ Enforces authorized access to network services and resources through the SunWeb portal and Access Manager infrastructure. ■ Manages Sun employee user identity and tightly integrates with policy, identity management, service management, and SAML (Security Assertion Markup Language) to simplify and provide a single point of administration of users. ■ Provides a single identity (single sign-on) across web and application servers and services, such as the MySales and MyMarketing SunWeb portals and also mail and calendar applications. ■ Provides users filtered roles.
Sun Java System Application Server 8.1	Provides the Java 2 Platform, Enterprise Edition (J2EE™) container.
Sun Java System Directory Server 5.2	Directory Server stores the user profile information used by Portal Server and Access Manager. Portal Server and Access Manager read and write to Directory Server, and several other critical operations also occur on the directory servers to perform the following tasks: ■ Update user profiles based on Human Resources records. ■ Implement multimaster replication, which enables data to be replicated between directory servers in real time to keep the data synchronized.

TABLE 1–4 Key Sun Software Used in SunWeb 4.0 *(Continued)*

Product	Functionality
Solaris 10 OS	Provides the operating system (secure build, x86, zones).

Hardware in SunWeb 4.0

A key piece of the SunWeb 4.0 deployment was hardware. SunWeb had quickly outgrown the systems on which it was originally deployed. SunWeb moved to a stack of Sun Fire x64 servers running Solaris 10 OS, which provided greater performance, stability, and scalability.

The hardware used in SunWeb 4.0 includes the following:

- Nine V20z Opteron servers (dual 1.8 GHz CPUs, 16 Gbyte RAM, 2x 72 Gbyte SAS)
- One Sun Fire x4100 (Galaxy, dual 2.2 GHz CPUs, 16 Gbyte RAM, 2x 73 Gbyte SAS)
- Load balancer

For more information about hardware, see "Preparing the Computer Hardware and Operating System Specification" on page 43. For more information about load balancing and redundancy strategies, see "Choosing Redundancy Strategies for the SunWeb Architecture" on page 39.

CHAPTER 2

SunWeb Requirements

This chapter describes the business and technical requirements for the SunWeb 4.0 deployment. The requirements listed in this chapter are one possible set of requirements for an enterprise such as Sun. These requirements might be similar to the requirements needed by your enterprise as you plan to deploy and use Java ES services. Compare the requirements in this chapter with your own business requirements to determine what aspects of the SunWeb 4.0 deployment are applicable for your specific needs.

The requirements described in this chapter specify quality of service (QoS) features such as performance, availability, and scalability. The deployment architecture developed to meet these requirements is described in detail in Chapter 3.

This chapter contains the following sections:

Capacity Requirements

SunWeb provides services to two primary classes of internal users: those accessing SunWeb when connected to the corporate network (SWAN) and those accessing SunWeb using the public Internet and secure remote access gateways (SRA). SWAN users connect directly to the portal server through a load balancer. Internet users (SRA) access load-balanced gateways that connect to the portal servers for serving content and other applications.

Each class of user has access to the same set of services, which includes e-mail, blogs, search, file access, content, tools, applications, and a personalized desktop. Access to specific services, tools, and content is based on an employee's role at Sun (executive, people manager, individual contributor, and so on). The following table lists the approximate number of users in each class.

TABLE 2–1 Number of Users of SunWeb Services

Service Class	Number of Users
Local users logging in to SunWeb from a computer connected to SWAN (includes access via VPN)	Approximately 19,000–21,000 unique users per day
Remote users logging in to SunWeb from a computer or mobile device not connected to SWAN (SRA)	Approximately 1,700–2,100 unique users per day

The SunWeb user base is expected to grow as more applications are integrated into the portal. For the initial deployment of SunWeb 4.0, the requirement was that the system be scalable to support 6,000 concurrent users. To meet future needs, the deployed system must be scalable to accommodate an increasing number of users, with the growth rate for users expected to be 10-15% per year.

Detailed Service Requirements

As highlighted in “Deployment Overview” on page 15, the SunWeb portal provides a wide variety of services to internal users. The following table lists the detailed service requirements that must be met by the deployment.

TABLE 2–2 Detailed Service Requirements

Service	Requirement
SunWeb Portal Desktop	■ Provide role-based desktop access that enables access to applications and services based on a user's role. ■ Integrate with content management systems to dynamically serve content. ■ Provide single sign-on (SSO) with the MySales and MyMarketing portals and with other applications. ■ Integrate with corporate LDAP for authentication and personalization of services. ■ Provide secure login to Access Manager through SSL. ■ Provide dynamic web services and RSS content through blogs and web services. ■ Provide Ajax-based portlets to dynamically refresh and display data. ■ Provide reporting and auditing to generate reports for compliance. ■ Integrate with applications such as employee lookup, the Support ticketing system, the bug reporting system, and so on. ■ Enable and present Human Resources services through a single desktop access. ■ Provide a tab-based desktop to group and present similar applications and services. ■ Ensure that the desktop is highly customizable and user friendly to meet corporate usability requirements and standards.
Access Manager	■ Provide SSO capability to several applications. ■ Use agents and the service infrastructure to enable simplified development and deployment of an SSO infrastructure. ■ Provide advanced policy and user management. ■ Implement a role-based infrastructure to integrate into the corporate LDAP framework. ■ Provide chained authentication and enable higher authentication levels to access secure and sensitive business applications.

TABLE 2–2 Detailed Service Requirements *(Continued)*

Service	Requirement
Remote access	■ Provide secure remote access to the SunWeb portal from anywhere, anytime, and on any device to enable users to access intranet applications, the network, and services in a secure way. ■ Provide token-based authentication to enable users to authenticate in a secure way. ■ Provide a URL-based access control list through the remote access services. ■ Provide SSO for applications using HTTP basic authentication. ■ Provide SSL tunneling end-to-end from the browser to the end application infrastructure. ■ Use Rewriter and Netlet proxies to prevent several ports and access points from being opened in the firewall (restrict the firewall to have only one open port). ■ Enable users to personalize and customize remote infrastructure applications such as telnet and FTP.
Mobile access	■ Build upon the Secure Remote Access Pack (SRAP) and Mobile Access Pack (MAP) of Portal Server. ■ Enable Sun internal users to access Sun's internal mobile content, business applications, and tools anywhere and anytime through SunWeb using a web-enabled mobile device with micro browser and SSL support. Mobile users access the internal portal by accessing the remote gateway for their region on their mobile device. ■ Enable mobile access to the SunWeb portal and its mobile content, applications, and tools channels from the Internet using secure remote access. ■ Provide mobile services for web-enabled cell phones and PDA devices, including support for mobile access of mail and calendar services, employee lookup, and a small set of SunWeb channels.
File access	■ Support the NFS, Window File Services, and FTP protocols. ■ Provide NetFile through the SRA service, and FTP through netlets. NetFile is a Portal Server SRA component that enables users to access and operate on remote file systems and directories.

TABLE 2–2 Detailed Service Requirements *(Continued)*

Service	Requirement
Communications channels (mail and calendar)[1]	The following requirements are common to the mail and calendar channels. Unique requirements for these channels are listed in the channel-specific sections later in this table. The common requirements are as follows: ■ Deploy the mail and calendar channels on SunWeb with SSO based on a SunWeb authenticated session. To provide SSO to mail and calendar, the portal server stores user names and passwords in the directory server. ■ Require authentication before the channels are displayed. ■ Populate channel properties with information drawn from corporate LDAP wherever possible. User preferences data (the user profile) should be retrieved automatically from LDAP without user interaction. ■ Must not impact portal performance. ■ Must be highly customizable.
Mail	■ Enable mobile users to access their email account through the portal anywhere, anytime, using any device and to view, read, and reply to messages. ■ Provide a comprehensive webmail client that allows message forwarding, vacation messages, server-side mail filters, and a server-side address book. ■ Provide SSO with the webmail client. ■ Prepopulate IMAP server and port, user name, password, SMTP server and port, and any other settings required to connect the channel to the user's mail account. ■ Customize the user interface to meet corporate standards. ■ Provide spam and antivirus protection through plug-ins. ■ Provide portal-based mail access through JavaServer Pages™ (JSP™) mail portlets and native client support through SRA. ■ Mailbox size (maximum): 2 GB. ■ Attachment size (maximum): 20 MB.
Calendar	■ Enable mobile users to access and manage their Java ES calendar account through the portal anywhere, anytime, and using any device. ■ Provide SSO with the calendar client. ■ Prepopulate calendar server and port, user name, password, and any other settings required to connect the channel to the user's calendar account. ■ Customize the user interface to meet corporate standards.

[1] Mail and calendar services are provided by instances of Sun Java System Messaging Server and Sun Java System Calendar Server that are already deployed and running on the main corporate network. The SunWeb deployment uses Portal Server channels to provide SunWeb users with access to these services on their portal desktops.

TABLE 2–2 Detailed Service Requirements *(Continued)*

Service	Requirement
Blogs	■ Introduce a custom RSS provider to the SunWeb channel catalog to be developed by the internal product team. ■ Enable authenticated users to add the blogs channel to their tabs in SunWeb and to choose up to seven RSS and blog feeds to personalize the channel's contents. ■ Must be highly customizable. ■ Must not impact portal performance.
SunWeb (Java ES) search	■ Integrate search with the portal desktop and the SRA service to provide a single entry point. ■ Provide advanced search capabilities based on several possible combinations. ■ Implement a paragraph-based search that provides highly intelligent search results. ■ Deploy the multitier architecture to segregate crawling from presentation.

Employee Usage Patterns

SunWeb users are expected to be most active during the 8:00 a.m. to 5:00 p.m. working hours in their respective geographical areas. Employee usage is significant outside of those hours to facilitate communication with colleagues in other time zones.

Availability Requirements

All production instances of the internal portal worldwide must be available 24x7x 365 with 98% uptime. To meet this requirement, the SunWeb 4.0 architecture defines multiple redundant portal servers and gateways. Operationally, each server is online and load balanced. If one server fails, all requests are redirected to the remaining servers.

The long-term goal is 99.99% uptime worldwide, as SunWeb and SRA are an integral part of Sun's business continuity and disaster-recovery strategy. One way to meet this goal is to have three global instances, each at 99.9% availability.

Performance Requirements

All production instances of the internal portal worldwide must support 6,000 concurrent users and have a response time of four seconds or less. To meet this requirement, the SunWeb 4.0 architecture defines multiple load-balanced portal servers and gateways, so each server can handle concurrent requests from users simultaneously. These servers are tuned for optimum performance.

Scalability Requirements

As mentioned in "Capacity Requirements" on page 21, the SunWeb user base is expected to grow. The architecture for SunWeb's Java ES deployment must allow for horizontal scalability (adding more computers to the system as user activity increases). To meet this requirement, the SunWeb 4.0 architecture allows for more portal servers or gateways to be added at a later time to handle the extra load. For more information about scalability strategies, see "Planning for Scalability in the SunWeb Architecture" on page 41.

Security Requirements

Security is a vital consideration for any system accessed by a large number of users over the public Internet. The general security requirements for SunWeb include the following:

- Secure access to confidential data
- Authentication over SSL
- Confidential data captured on SSL
- Remote and mobile client access through token-based and mobile access authentication
- Enforced role-based access control
- Use of appropriate security features in the Access Manager and load balancer

Token-based authentication is used for remote and mobile users accessing SunWeb through the public Internet and the remote access gateways. Corporate LDAP is used for internal users accessing the portal from a computer connected to SWAN. Remote users accessing SunWeb over the public Internet (SRA) first get a login screen in their browser. After authenticating, a customizable desktop is displayed through which they gain access to various back-end applications and services. The specific mechanisms are described in greater detail in Chapter 3, including "Analyzing User Interactions with the SunWeb Components" on page 32.

The following table provides more specific information about security requirements.

TABLE 2–3 SunWeb Security Requirements

Security Category	Requirement
Physical	■ Housed within a secure data center to which only authorized personnel have access
Firewall	■ Redundant firewall protection ■ Secure transfer and storage of data ■ Administrative options provided to customize security settings (explicit policy control)
Transport	■ Compatible with SSL-enabled web browsers and Transport Layer Security (TLS) ■ 128-bit encryption for mail transfer between client and server
Backup and recovery	■ All software and configurations backed up (weekly or nightly incremental backups) ■ Operating system backed up weekly ■ Backups stored for 2 weeks ■ Maximum 24 hours of data loss
Disaster recovery	■ Distributed architecture in multiple data centers with failover capability ■ Disaster recovery to be completed within 24 hours
Privacy	■ Data storage that follows applicable regulations, corporate security policies, and corporate privacy policies

For more information about security strategies, see “Choosing Security Strategies for the SunWeb Architecture” on page 39.

CHAPTER 3

Designing the SunWeb Architecture

A Java ES architecture is a high-level technical description of a Java ES solution. You design an architecture to identify the combination of Java ES components and other technologies that will deliver the services described in your requirements. This chapter describes the architecture that the SunWeb team developed to satisfy the requirements described in Chapter 2.

A Java ES architecture is developed in two stages:

1. **The deployment scenario.** The deployment scenario identifies the Java ES components and other software that provide the services named in the requirements and, separately, lists the quality of service requirements.
2. **The deployment architecture.** The deployment architecture merges the two types of information that appear in the deployment scenario. Where the deployment scenario simply identifies the components that are needed to provide the services identified in the requirements, the deployment architecture describes how to provide the services at the specified quality of service, by using multiple component instances distributed across the network, implementing one or more redundancy strategies, and choosing the appropriate hardware.

This chapter describes the architecture for the SunWeb 4.0 deployment in the following sections:

- "Preparing the Deployment Scenario" on page 29
- "Designing the Deployment Architecture" on page 32

Preparing the Deployment Scenario

The deployment scenario for the SunWeb 4.0 deployment is a combination of the following:

- The logical architecture, which identifies the Java ES components and other software needed to provide the services described in "Detailed Service Requirements" on page 22.

- The quality of service requirements, which specify the performance required from the Java ES components and other software named in the logical architecture.

Preparing the Logical Architecture

The Java ES components needed to provide the services listed in "Detailed Service Requirements" on page 22 are diagrammed in the following figure. This set of components is prepared by examining the list of services required in the SunWeb 4.0 deployment and determining which Java ES component will be used to provide the services.

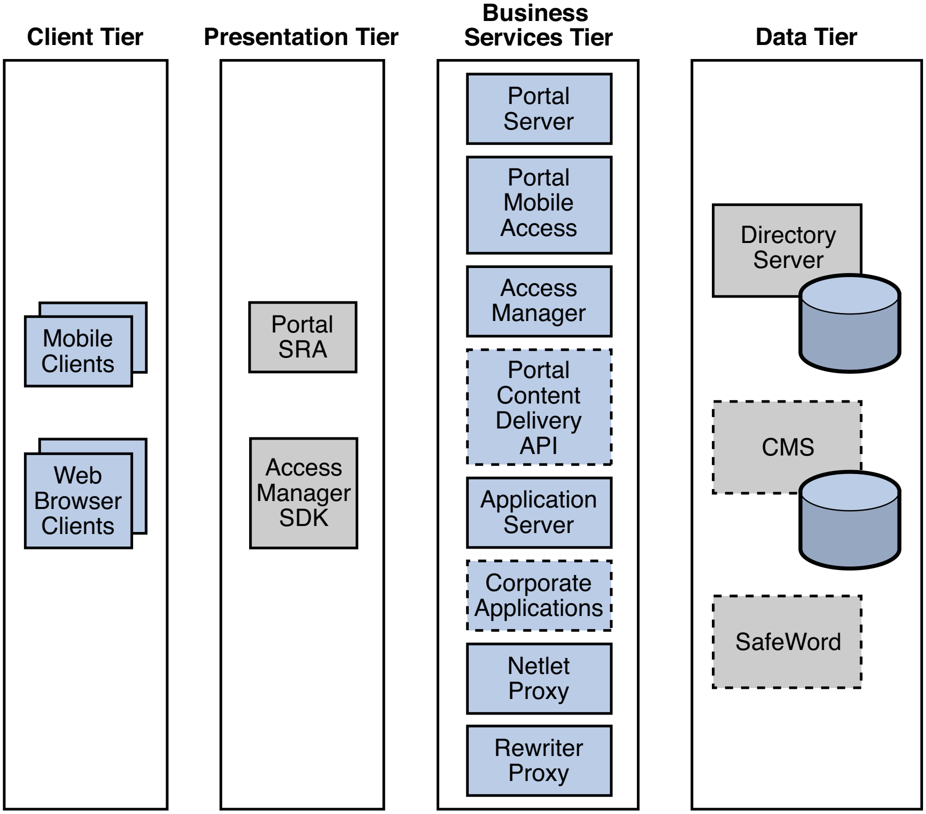


FIGURE 3–1 SunWeb Deployment Logical Architecture

Notice that the logical architecture includes Java ES components, represented as boxes with solid outlines, and non-Java ES software, represented as boxes with dashed outlines. Non-Java ES software is used as follows:

- The Portal Content Delivery API is installed as part of the SunWeb deployment, and supports interaction between the SunWeb deployment and the content management system (CMS).
- The CMS is already running on the main corporate network. The SunWeb components are configured to interact with the CMS. The CMS appears in the logical architecture's data tier, but the CMS is more a service used by the SunWeb components than a part of the actual SunWeb deployment.
- The logical architecture also includes existing corporate applications and web sites. These existing applications and web sites, including the corporate messaging and calendar services also running already on the main corporate network. These applications and web sites are represented in the logical architecture's business services tier, but they play a role similar to the CMS. The corporate applications and web sites are more accurately regarded as services used by the SunWeb components than as part of the actual SunWeb deployment.
- The logical architectures shows SafeWord, which is already running on the main corporate network. Access Manager is configured to interact with SafeWord in order to authenticate login requests from remote users. (Access Manager ships with a module for this purpose.) SafeWord, too, is more accurately regarded as a service used by the SunWeb components than as a part of the SunWeb deployment.

Reviewing the Quality of Service Requirements

The logical architecture identifies the Java ES components that provide the services named in the requirements, but does not tell you how you should install the components on your network. In a typical production deployment you satisfy quality of service requirements such as response time, service availability, and service reliability by installing and configuring multiple instances of the components and distributing the components among several computers. For example, you could provide failover capability for your portal service by configuring multiple instances of Portal Server on multiple computers behind a load balancer.

To review the quality of service requirements for the SunWeb deployment, see the following sections in Chapter 2:

- "Availability Requirements" on page 26
- "Performance Requirements" on page 27
- "Scalability Requirements" on page 27
- "Security Requirements" on page 27

Designing the Deployment Architecture

The deployment architecture merges the two types of information found in the logical architecture and the quality of service requirements. To design your deployment architecture you must consider such questions as the following:

- Which redundancy strategies are you using to meet your availability and reliability requirements? The main redundancy strategies available to you with Java ES are the following:
  - Installing and configuring multiple instances of a component and load balancing the instances
  - Installing and configuring multiple instances of a component on Sun Cluster nodes
  - Using multiple instances of Directory Server that are synchronized through the multimastering and replication features
- How many instances of each component must be installed and configured in order to implement the redundancy strategies you are using in the solution? How many instances must be installed and configured to satisfy your performance requirements?
- How are your component instances combined on your computers? For example, in a medium-sized solution, you could install and configure instances of both Portal Server and Access Manager on a single computer. In a larger solution with more user activity, you might install Portal Server and Access Manager on separate, dedicated computers to meet your performance requirements.
- How many CPUs are needed on each computer to achieve the performance specified in your quality of service requirements?

In addition to answering these questions, you analyze use cases and usage information and determine how the Java ES components and other software can be deployed on your network to provide access and security.

This section describes how the SunWeb team analyzed the SunWeb use cases and developed a deployment architecture.

Analyzing User Interactions with the SunWeb Components

The main user interactions with the set of components used for the SunWeb deployment are illustrated in Figure 3–2 and Figure 3–3. These figures show how users interact with the Java ES components in the proposed logical architecture to obtain the specified services. As you continue the design process, you analyze the component interactions represented in these figures, factor in the user base and usage patterns, and begin to make decisions about a deployment architecture that supports these interactions with the specified quality of service.

Notice that the security requirements are being considered at this stage of the analysis. The figures include proposed access zones for the SunWeb deployment.

The following figure illustrates the interactions between a user who is logged in to the corporate network and the Java ES components in the proposed logical architecture for the SunWeb deployment.

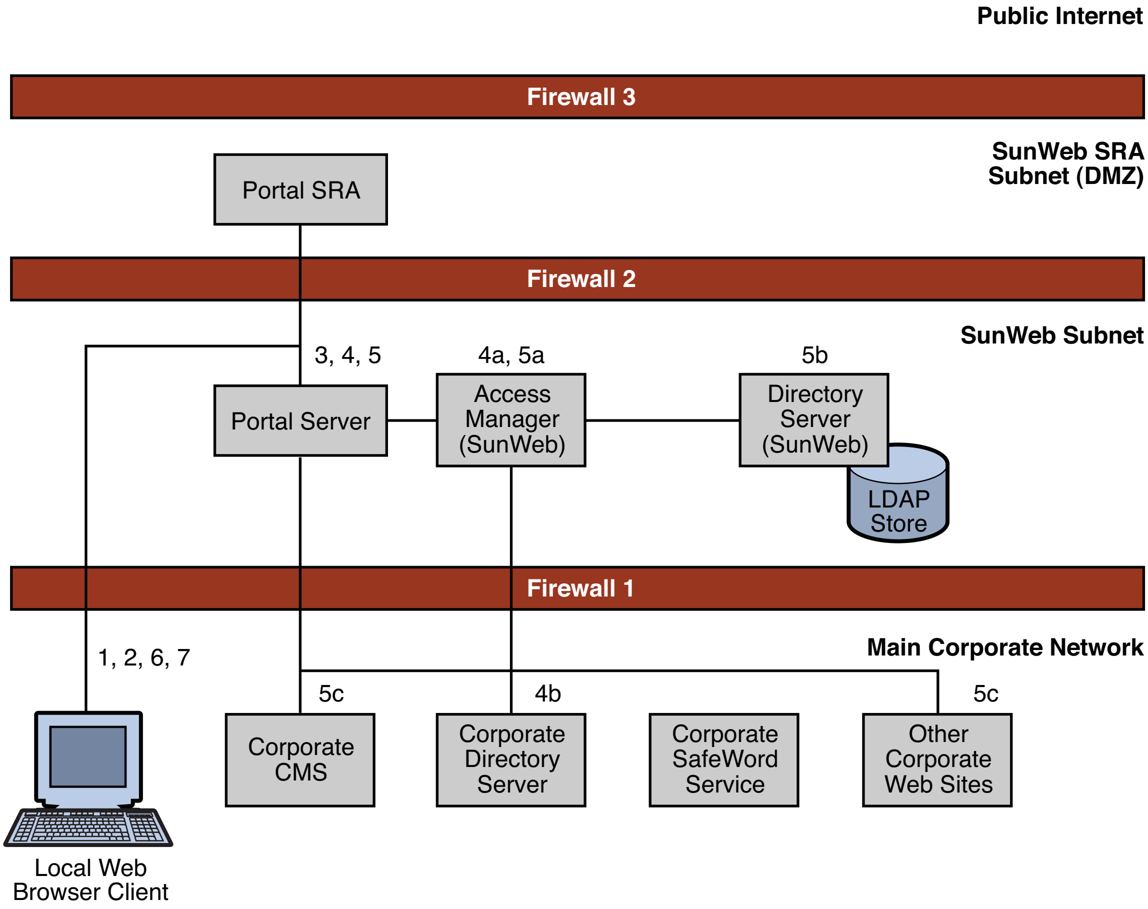


FIGURE 3–2 Local User Interactions

The interactions shown in the preceding figure are described in the following table.

TABLE 3–1 Interacting With SunWeb Components Over the Corporate Network

Step	Description
1	A user logs in to a computer connected to the corporate network. The computer can be physically connected to the corporate network or connected to the corporate network over the public Internet with a virtual private network (VPN) session.
2	The user starts a web browser and opens the SunWeb URL. This request is directed to a custom wrapper for the Portal Server desktop servlet.
3	The Portal Server desktop servlet wrapper checks for a SunWeb session cookie: ■ If the cookie exists (meaning that the user is already authenticated for SunWeb), the Portal Server formats the user's personalized desktop as described in step 5. ■ If the cookie does not exist (meaning that the user has explicitly logged out of his or her previous session), the desktop servlet displays an anonymous view of the SunWeb desktop. The anonymous view includes fields for user ID and password. The user can work with the anonymous view or log in, as described in step 4.
4	If the user supplies a user ID and a password in the desktop login fields, SunWeb's Access Manager (4a) uses a custom authorization module to authenticate the user's ID and password against the corporate LDAP directory (4b). When the user is authenticated, Portal Server displays the user's personalized desktop view, as described in step 5.
5	To display the user's SunWeb desktop, Portal Server aggregates content from a variety of sources. The specific content that appears on each user's personalized desktop is determined by a portal profile that is managed by the SunWeb Access Manager (5a) and stored in the SunWeb Directory Server (5b). The Portal Server mechanisms for aggregating content are described in the following list: ■ Static content: The Portal Server's URLScraper feature pulls static content that is stored in the local file system as HTML files. These local files are updated every ten minutes by the Portal Content Deliverer (PCD). The PCD scans source material on the corporate content management system (CMS) and updates the local content as necessary. ■ Dynamic content, including the portal mail, calendar, and blog channels: The Portal Server's URLScraper feature dynamically pulls content from URL addresses on the main corporate network (5c) and presents it on the user's desktop.
6	The user reviews his or her portal desktop and chooses to review details of one or more channels.

TABLE 3–1 Interacting With SunWeb Components Over the Corporate Network *(Continued)*

Step	Description
7	The user can end his or her desktop session by closing the web browser window or by explicitly logging out of the SunWeb portal. If the user closes the web browser window, the SunWeb cookie persists. If the user explicitly logs out, the SunWeb cookie is deleted, and the user must log in to the SunWeb portal again at the beginning of his or her next session.

The following figure illustrates the interactions between an employee who accesses SunWeb services over the public Internet and the Java ES components in the proposed logical architecture.

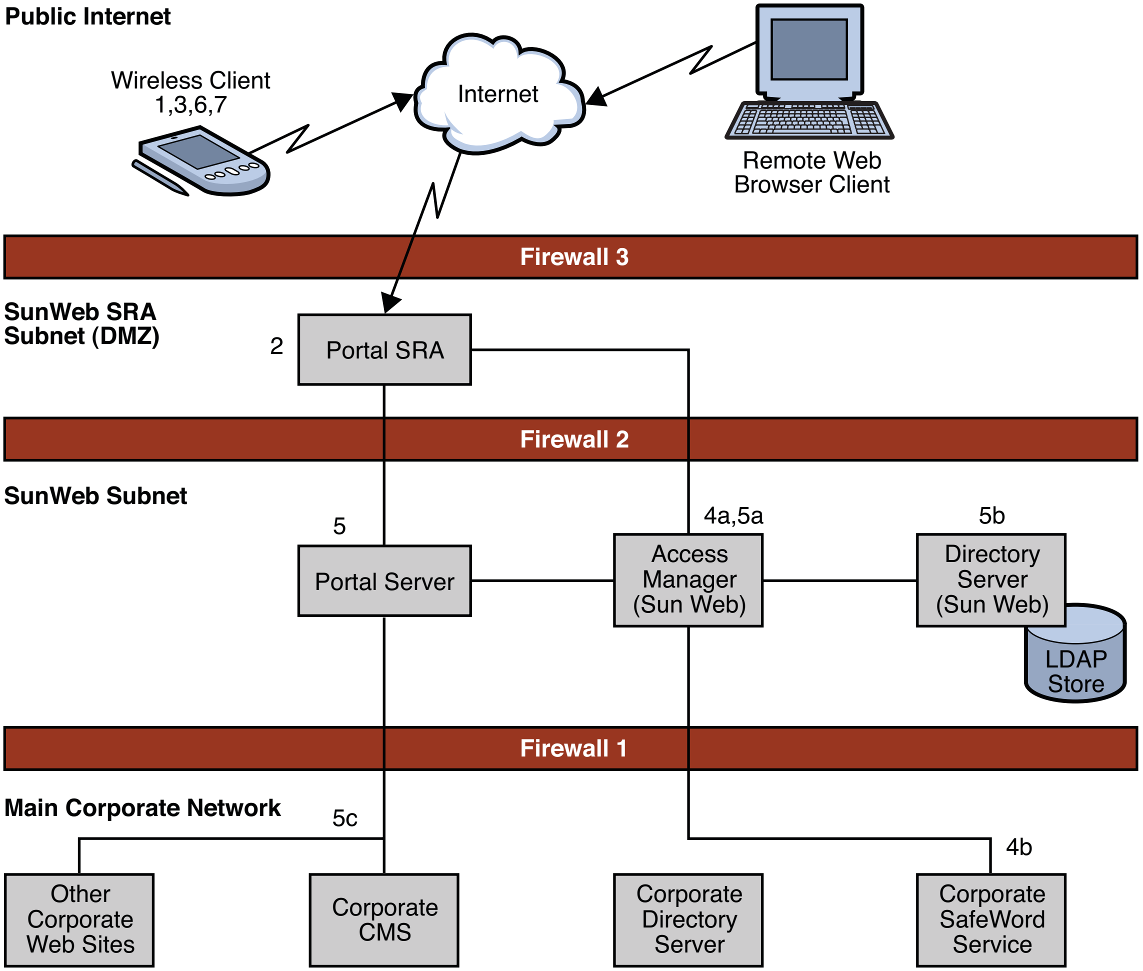


FIGURE 3–3 Remote User Interactions

The interactions shown in the preceding figure are described in the following table.

TABLE 3–2 Interacting With SunWeb Components Over the Internet

Step	Description
1	From a computer not connected to SWAN or a mobile device, the user starts a web browser and opens the URL for SunWeb remote access. This request is routed to the SunWeb gateway service, provided by Portal Server Secure Remote Access.
2	The gateway service displays a login window to the user.

TABLE 3–2 Interacting With SunWeb Components Over the Internet *(Continued)*

Step	Description
3	The user enters both an ID and a dynamically generated token card code.
4	SunWeb components authenticate the user as follows: The gateway passes this information to Access Manager (4a). Access Manager uses its SafeWord Module, a standard Access Manager feature, to authenticate the information with the corporate SafeWord service (4b). ■ If the user is authenticated, the SunWeb portal service displays the user's personalized desktop, as described in step 5. ■ If the user is not authenticated, the user is prompted again for password and token card code.
5	To display the user's SunWeb portal desktop, Portal Server aggregates content from a variety of sources. The specific content that appears on each user's personalized desktop is determined by a portal profile that is managed by the SunWeb Access Manager (5a) and stored in the SunWeb Directory Server (5b). The Portal Server mechanisms for aggregating content are described in the following list: ■ Static content: The Portal Server's URLScraper feature pulls static content that is stored in the local file system as HTML files. These local files are updated every ten minutes by the Portal Content Deliverer (PCD). The PCD scans source material on the corporate content management system (CMS) and updates the local content as necessary. ■ Dynamic content, including the mail, calendar, and blog channels: The Portal Server's URLScraper feature dynamically pulls content from URL addresses on the main corporate network (5c) and presents it on the user's desktop.
6	The user reviews his or her portal desktop and chooses to review details of one or more channels.
7	The user closes the web browser and ends the SunWeb session.

Representing the Deployment Architecture Graphically

As you analyze your requirements and user interactions, you develop a graphical representation of your proposed deployment architecture. The graphical representation uses a set of boxes that represent the computers in the deployment. Each box in the figure is labeled with the name of the computer and the components that are installed on the computer. The deployment architecture for the SunWeb deployment is illustrated in the following figure.

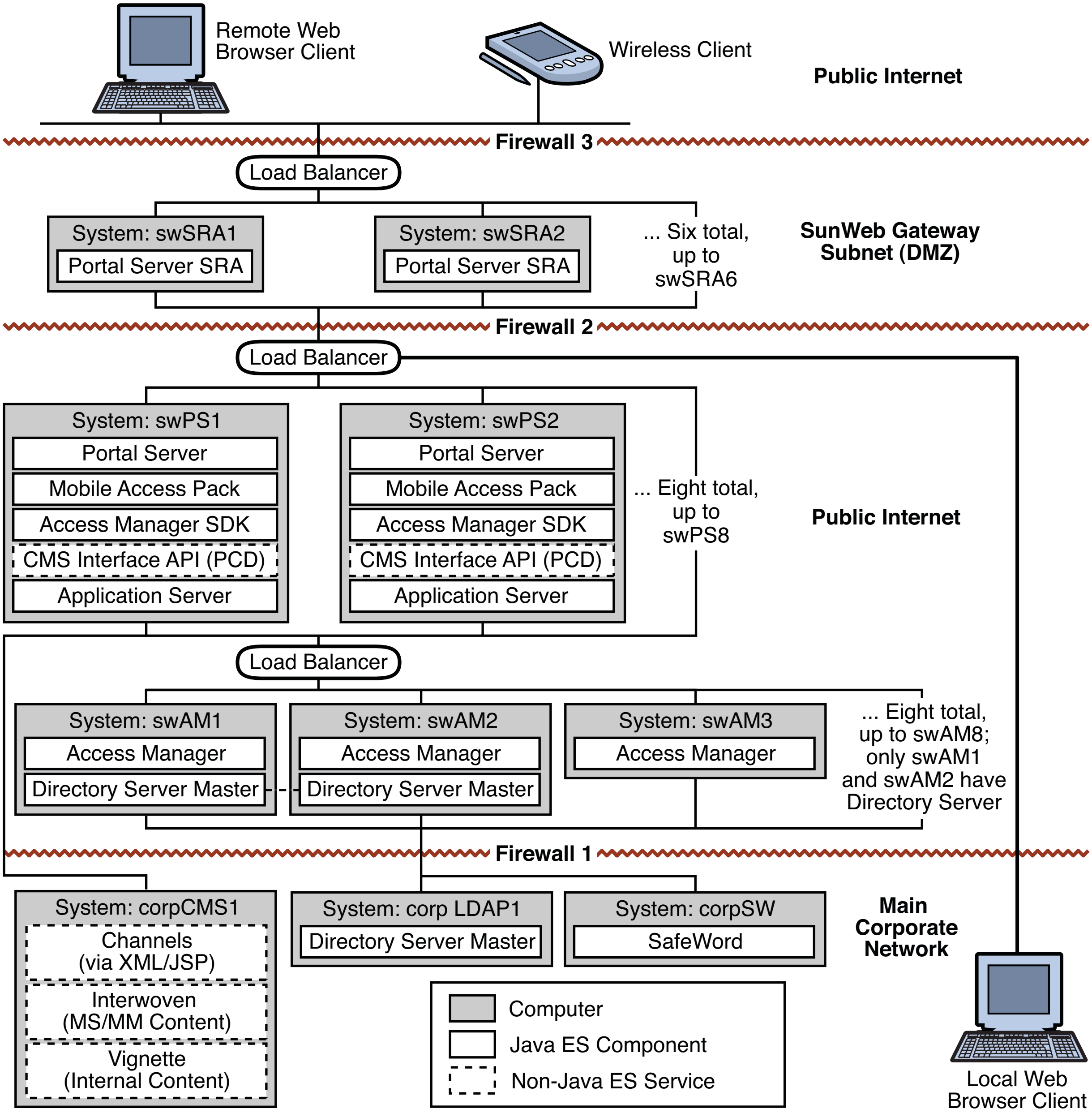


FIGURE 3–4 SunWeb Deployment Architecture

Note – The system names that appear in the preceding figure are not the names used in the actual SunWeb deployment. The system names in the figure are used only to illustrate the architecture.

Choosing Redundancy Strategies for the SunWeb Architecture

The architecture represented in the preceding figure uses two redundancy strategies to meet the quality of service specified for the SunWeb deployment. The two redundancy strategies, load balancing and Directory Server multimaster replication are chosen for the following reasons:

- Load balancing. This solution is preferred for components that do not need to synchronize database updates. Load balancing uses redundant hardware and software components to distribute requests for a service among multiple components instances that provide the service so that no single instance is overloaded. This redundancy also means that if any one instance of a components fails, other instances are available to assume a heavier load. Depending on the latent capacity built into the deployment, a failure might not result in significant degradation of performance. Load balancing is used for several components in the SunWeb architecture, for example, the Portal Server and Access Manager components on `sunwebPS1` and `sunwebPS2`.
- Directory Server multimaster replication. This solution is preferred for Directory Server, which provides data that is crucial to the operation of the entire deployment. Multimaster replication is specifically designed for Directory Server and is therefore relatively easy to implement. The SunWeb architecture uses Directory Server multimaster replication for all the Directory Server instances included in the SunWeb deployment. The SunWeb architecture uses two instances of Directory Server. All eight instances of Access Manager normally connect to the primary Directory Server instance. If the primary Directory Server fails, all eight instances of Access Manager fail over to the secondary Directory Server.

Choosing Security Strategies for the SunWeb Architecture

The requirements for the SunWeb portal service posed the following security challenges:

- First, each employee's access must be limited to the services and data channels that he or she is authorized to view.
- Second, the SunWeb portal service must allow Sun employees secure remote access to SunWeb services and data channels over the public Internet while preventing unauthorized people from accessing the portal.

For more information on the security requirements, see “Security Requirements” on page 27.

The SunWeb architects met the first challenge by including Access Manager and Directory Server in the deployment to control employee access to portal content. These Access Manager and Directory Server instances are separate from the main corporate LDAP service. The SunWeb directory service is dedicated to maintaining each employee's portal desktop profile. The desktop profile includes any desktop customization performed by the employee, as well as LDAP attributes and object classes that determine what content an employee is authorized to view. For more information on this aspect of the deployment, see "The LDAP Schema" on page 46.

The SunWeb architects met the second challenge by including the Portal Server Secure Remote Access component and its gateway service in the deployment and by designing network access zones that take maximum advantage of the gateway service. The access zones are demarcated by firewalls. The access zones and the firewalls are represented in Figure 3–4.

The outermost zone in Figure 3–4 is the demilitarized zone (DMZ), which contains the portal gateway. The DMZ is reasonably secure. The portal gateway service behind the firewall can be accessed at one specific URL only. Employees who connect to the SunWeb portal with remote web browser clients or mobile clients access the gateway service at the specified URL. The firewall blocks all other ports and addresses.

In addition to deploying the gateway service behind Firewall 3 in the DMZ, the SunWeb architecture protects the gateway service in the following ways:

- The gateway service requires users to authenticate themselves. Employees who open the URL for the gateway service in their web browsers are presented with a login page. Employees must enter a user ID and a dynamically generated password to gain access to any content.
- The computers that provide the gateway service are behind a hardware load balancer. The load balancer provides a single point of contact for the gateway service, even though multiple component instances are running on multiple computers. As a result, there is only one opening in the firewall for the gateway service, and all of the traffic for the gateway service is routed through the load balancer.
- Not shown in Figure 3–4, but implied in the deployment architecture, is a network topology that creates separate subnets for each of the access zones. The IP addresses used in the subnets are private IP addresses, making the subnets invisible to the public Internet. These subnets are connected only through the load balancers, further impeding the ability of intruders to see the actual computers behind the public URL. For more information on the network topology, see "Preparing the Network and Connectivity Specification" on page 44.

The next zone, behind Firewall 2, is the SunWeb subnet. This zone contains the actual SunWeb portal service, which is provided by eight instances of Portal Server, supported by eight instances of Access Manager and two instances of Directory Server. This zone is defined by an additional firewall (Firewall 2).

In addition to deploying the portal service on its own subnet behind Firewall 2, the SunWeb architecture protects the portal service in the following ways:

- Remote access to the portal service from the public Internet is controlled by the Portal Server SRA gateway service in the DMZ. All remote access to the portal service is through the gateway service. This aspect of the architecture allows the portal service to reside behind an additional firewall and an additional layer of hardware load balancing.
- The load balancer behind Firewall 2 provides a single point of contact for the portal service, even though the service consists of eight Portal Server instances that are running on eight computers. The load balancer is the only opening in the firewall for the portal service, and all of the traffic for the portal service is routed through the load balancer. Employees connected to the main corporate network also access the SunWeb portal through this load balancer.
- Local access to the portal service is only from trusted computers on the main corporate network after users have authenticated themselves to the corporate LDAP directory service.
- The computers running Portal Server and Access Manager are on a different subnet from the computers in the DMZ, and this subnet is defined by private IP addresses. The only bridge between the subnets is the hardware load balancer.

The main corporate network contains various corporate information services that are accessed by the SunWeb portal service. These services are protected by Firewall 1. In addition to Firewall 1, the main corporate network is protected by the following measures:

- There is no direct remote access to these corporate services. All remote access is indirect, through the Portal Server instances.
- The CMS only allows traffic from the PCD instances that are colocated with the Portal Server instances. All other traffic is blocked.

Not shown in Figure 3–4 is the fact that the individual computers running the Java ES services are hardened.

Planning for Scalability in the SunWeb Architecture

The Java ES services used in the SunWeb portal architecture are provided by multiple component instances running on multiple computers behind a load balancer. For example, the portal service is provided by eight Portal Server instances running on computers `sunwebPS2` through `sunwebPS9`.

This architecture could be scaled either horizontally or vertically to handle more incoming connections in the following ways:

- To scale horizontally, the number of computers running Portal Server SRA instances could be increased, up to the capacity of the load balancing hardware. The architecture would remain essentially the same, but the load balancer would be distributing a greater number of incoming connections among a greater number of Portal Server SRA instances. The load on each component instance would remain constant. Similarly, the number of computers running Portal Server, Access Manager, and Directory Server could also be increased, as needed.

The Access Manager and Directory Server instances could be installed on separate computers, giving each instance more computing resources.

- To scale vertically, additional Solaris 10 zones can be created, if the computers have sufficient memory and disk storage. You can install and run additional component instances in the new zones to increase the capacity of the Java ES services on a single computer hardware system.

CHAPTER 4

Preparing the SunWeb Deployment Specifications

The deployment specifications are a technical description of SunWeb that is more detailed than the deployment architecture. You derive the deployment specifications from the architecture by adding detailed information that is needed to install and configure the set of components identified in the architecture.

This chapter describes the deployment specifications for the SunWeb deployment in the following sections:

Preparing the Computer Hardware and Operating System Specification

The computer hardware and operating system specification describes the hardware and operating system configuration for each computer in the deployment. Your choice of hardware primarily depends on the level of performance you require from the components running on the computer.

The following table lists the computer hardware chosen for the SunWeb deployment. All of these computers run the Solaris 10 (x86) operating system with zones.

TABLE 4–1 Computer Hardware and Operating System Specification

Computers	Installed Components	Service Description	Hardware Model
swSRA1 through swSRA6	Portal Server SRA	Gateway service for remote portal access	Sun Fire V20z, 2 x Opteron

TABLE 4–1 Computer Hardware and Operating System Specification (Continued)

Computers	Installed Components	Service Description	Hardware Model
swPS1 through swPS8	Portal Server, Portal Server Mobile Access Pack, Access Manager SDK, Application Server, CMS Interface API	SunWeb portal service	Sun Fire V20z, 2 x Opteron
swAM1, swAM2	Access Manager, Directory Server	SunWeb Access Manager service, SunWeb directory service	Sun Fire V20z, 2 x Opteron
swAM3 through swAM8	Access Manager	SunWeb Access Manager service	Sun Fire V20z, 2 x Opteron

Preparing the Network and Connectivity Specification

Before you install and configure the Java ES components that appear in your deployment architecture, the computers must be attached to the network and assigned IP addresses. Preparing the network for a Java ES deployment can be a complex task that requires you to create several subnets to implement the security zones described in the architecture. Before you begin to set up the network, prepare a network and connectivity specification that maps all of the network connections needed to implement the deployment architecture.

A network and connectivity specification is typically a graphical representation of the required network configuration. The following figure is a graphical representation of the network configuration required to implement the SunWeb architecture.

Note – The IP addresses that appear in the following figure are not the addresses used in the actual SunWeb deployment. The IP addresses in the figure are used only to illustrate the concept of subnet configuration.

The network topology illustrated in the following figure implements the security strategies described in "Choosing Security Strategies for the SunWeb Architecture" on page 39. In particular, the following figure shows how the network and connectivity specification assigns private IP addresses to establish the secure network topology.

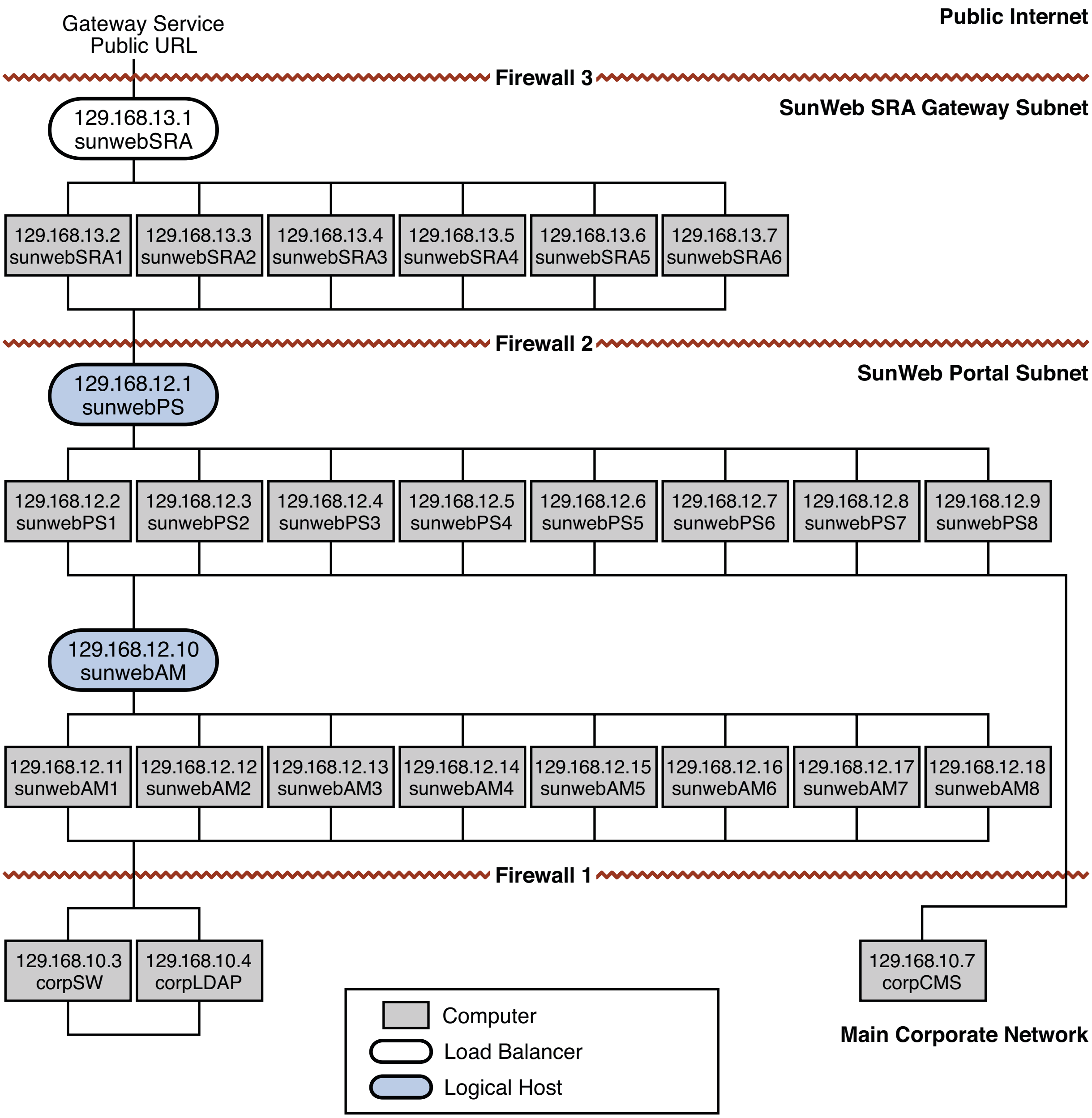


FIGURE 4–1 Network and Connectivity Specification

The computers running the gateway service and the computers running the portal service are on separate subnets. The existing corporate services are already deployed on the main corporate network, and appropriate security measures that allow the SunWeb portal controlled access to the information on the main corporate network are in place.

Access from the public Internet is restricted to HTTPS (SSL) access to the load balancer for the gateway service. Certificates are used.

For employees accessing the portal service over the public Internet only the load balancer in the DMZ (subnet 129.168.13.*x*) is actually exposed as shown in Figure 4–1. Everything else, according to the philosophy of minimizing the surface of attack, is hidden through use of private IP addresses.

Since the DMZ contains the SRA service that is accessed by Sun employees over the public internet, the IP address for the load balancer `sunwebSRA` is a normal IP address, which is accessible from the Internet. The IP address shown for this load balancer in Figure 4–1 is 129.168.13.1. When this load balancer is configured, however, this address is replaced with the real, publicly accessible address for the gateway service.

All of the other hardware in this zone is assigned 129.168.13.*xx* IP addresses, which are private addresses. These private addresses are not recognized by the Internet and are not routed outside the corporate network.

The only bridge between the DMZ and the portal service subnet is the load balancer, which controls the traffic between the subnets. Therefore, if the DMZ is compromised there is no direct route to the portal service subnet.

Preparing the User Management Specification

The process of installing and configuring a Java ES deployment establishes both the LDAP schema and the basic tree structure of the LDAP directory. Before beginning the installation and configuration process, you must analyze your directory needs and develop specifications for a schema and a directory tree structure that support your Java ES deployment. At installation and configuration time, the specification ensures that the correct values are input.

This section specifies the LDAP schema and the directory tree specifications for the SunWeb deployment. It also describes how the installation and configuration process establishes the directory schema and the directory tree structure for the deployment.

The LDAP Schema

The Java ES installation and configuration process establishes an LDAP schema for the deployment. The LDAP schema is constructed in stages. Depending on the components in the deployment, the schema can be constructed by the Java ES installer, several of the configuration tools, and the LDAP commands.

With Java ES deployments in general, you need to specify the LDAP schema before you install and configure so that you can select the correct installation and configuration parameters. This section describes the LDAP schema for the SunWeb deployment and the installation parameters that you input to construct the schema.

The first step in specifying the schema for a deployment is to identify the services that the directory service must support. For the SunWeb deployment, the directory service must support the following basic services:

- Access Manager authentication and single sign-on for SunWeb portal users
- Proxy authentication for Sun employees who access the corporate mail and calendar services through their portal desktops
- Control of employee access to portal content

These requirements lead to a relatively simple schema for the SunWeb LDAP directory. To support Access Manager, the schema must be brought up to Schema 2.

Note – Java ES solutions that use Directory Server can use either of two versions of a Sun standard LDAP schema for messaging and calendaring, which are known as Schema 1 and Schema 2. Schema 2 natively supports Access Manager and Access Manager's single sign-on feature.

To support control of employee access to portal content, a number of object classes and attributes that correspond to the different types of portal content must be added to the schema. Access Manager uses these object classes and attributes to determine which types of content each user is allowed to view.

The installation and configuration process constructs the schema for the SunWeb deployment as follows:

1. Installing Directory Server creates the basic schema.
2. Installing Access Manager applies Schema 2 to the directory.

   Directory Server must be installed before Access Manager, and the Directory Server instances must be running while the Access Manager instances are installed.
3. Adding the object classes and attributes that identify portal services and portal desktop configuration prepares the directory for use in the SunWeb deployment.

   Some of the attributes used in the SunWeb schema make use of Directory Server's filtered role feature. The roles are associated with portal display profiles that specify the personalized content for a portal user based on several attributes.

The Directory Tree Structure

The LDAP directory for a Java ES deployment can be simple or complex, depending on the organization's needs for organizing user data. The LDAP directory for the SunWeb deployment is primarily used to support employees who use the portal service. The SunWeb directory does not need a complex tree structure to classify employee records. That type of classification is maintained in the main corporate LDAP directory.

The directory structure developed to support the SunWeb requirements is illustrated in the following figure.

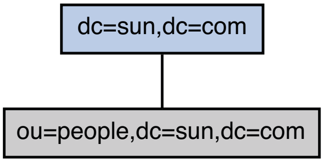


FIGURE 4–2 LDAP Directory Tree for the SunWeb Deployment

The root of the SunWeb directory tree is `dc=sun,dc=com`. The data for SunWeb portal users is stored in `ou=people,dc=sun,dc=com`.

Index