

Extended Security for SAP Enterprise Portal



Sun Infrastructure Solution — Network Services for SAP Enterprise Portal

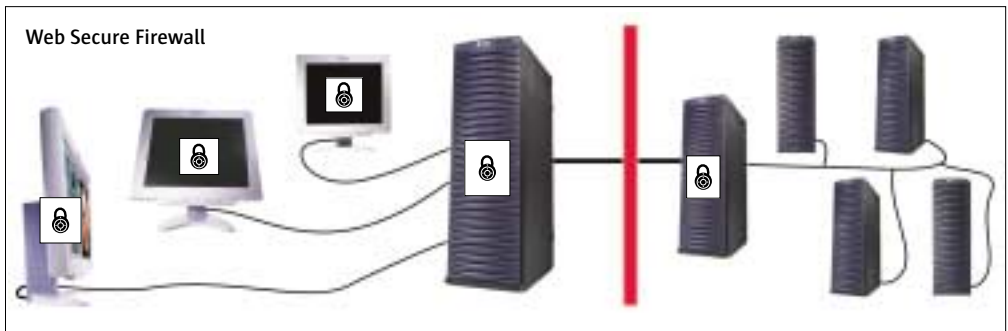
Highlights

- Enables customers to manage secure remote access to Web and non-Web-based applications.
- Allows authorization based secure access to all relevant resources behind the corporate firewall.
- Enables an enterprise or service provider to rapidly and inexpensively deploy and manage a remote access solution.
- Extends the value of internal resources through remote connectivity and through the centralization of user and access management.

Sun Network Services for SAP Enterprise Portal adds functionality to manage and secure remote access to internal resources like:

- A highly scalable LDAP-based user repository
- Single-sign-on to SAP and non-SAP systems
- Single point of entry through firewall
- Enhanced security through encryption, authentication, authorization, and architecture
- VPN-on-demand functionality
- Single point of administration for remote access rights and user data
- Role-based access to internal resources like mail server, ftp-server, file server, Web server, or applications
- Session validity is checked in the DMZ
- Policy based authentication and authorization

Sun Infrastructure Solution — Network Services for SAP Enterprise Portal (EP) is a standards-based solution set designed for SAP Enterprise Portal customers to help manage secure remote access to Web and non-Web-based applications — both on the intranet and extranet. The SAP Enterprise Portal is a key component of SAP NetWeaver, SAP's open integration and application platform. SAP EP also enables an enterprise or service provider to rapidly and inexpensively deploy and manage a remote access solution. The Solution can increase return on investment by extending the value of internal resources through remote connectivity and through the centralization of user and access management.



The Solution consists of three major components: the Sun Java System Secure Remote Access Portal, the Sun Java System Identity Server and the Sun Java System Directory Server. These components will be installed next to the SAP Enterprise Portal, adding functionality to manage and secure remote access to internal resources like:

- A highly scalable LDAP-based user repository
- Single-sign-on to SAP and non-SAP systems
- Access to internal resources through firewalls without opening up the firewall (Netlet, URL-Rewriting)
- Enhanced security through encryption, authentication, authorization and architecture
- VPN-on-demand functionality
- Single point of administration for remote access rights and user data
- Role-based access to internal resources like mail servers, ftp-server, file server, Web server or applications
- Authentication takes place in the DMZ
- Session validity is checked in the DMZ

- Policy based authentication and authorization
- Policy based access control to Portal URLs for all users
- Single point of entry through the firewall

Sun Network Services for SAP Enterprise Portal allows users to access all relevant resources, Web or non-Web, in a highly secure and managed way. Sun Network Services for SAP Enterprise Portal simplify IT administration and maintenance overhead while dramatically reducing the time and cost of deployment. It provides extensive scalability, high availability, reliability, and performance for enterprises and service providers.

Enhanced Security—Single Point of Contact

The Sun Secure Remote Access Gateway is installed in the DMZ. All access to internal resources will be handled by the Gateway as a single point of contact. All other internal resources will be inside the company's intranet, protected against unauthorized external access. Users connecting to the gateway will be authenticated using the Sun Java System Identity Server. The Identity Server authenticates the user against the relevant authentication mechanism, either the central LDAP Directory or other external authorization mechanisms like Radius, SafeWord or other authentication services. The Identity Server offers open APIs to easily build customized authentication modules. The SAP Enterprise Portal Users will be stored in the Directory Server, therefore authentication for SAP Enterprise Portal users is built into the solution.

Single Sign On

Once authenticated, the user has access to all authorized resources. Single Sign On with the SAP Enterprise Portal is provided as part of the solution set. Since all access has to run through the Gateway sitting in the DMZ, the Gateway has complete control over any access. The Gateway can be configured to

define which resources can and cannot be accessed externally. In addition, each user, once authenticated, is granted access rights depending on the information stored in the Sun Java System Directory Server. The Sun Java System Identity Server uses role-based access control mechanisms to centrally create and manage users, delegate user administration, and define the access policies for users on intranets and extranets. By leveraging the Sun Java System Directory Server as a central policy and identity data store, the Sun Java System Identity Server can support very large-scale deployment topologies with sustained availability and performance. The Identity Server delivers a set of policy agents that can be installed in front of Web servers and application servers, adding single-sign-on functionality to Web resources without having to change the code.

Single Point of Administration

The Sun Java System Identity Server provides a single point of administration for user and access management. Using a common identity infrastructure, administration that normally occurs across many applications by multiple administrators can be consolidated into a single management console. This single point of administration makes it possible to consistently delegate management tasks to partners, customers, and internal company departments based on business requirements. The result is an environment that is integrated, flexible, easy to manage, and secure. Security implementations and access control rules that are typically contained within each application can be consolidated to provide centralized authentication and authorization to resources. The SAP Enterprise Portal can store all user information in a corporate LDAP, the Sun Java System Directory Server.

Enhanced Security—VPN on demand

The Secure Access Gateway provides a Netlet architecture, which dynamically downloads an applet to the browser. In turn the Netlet architecture opens up a secure IP-Tunnel to the Intranet, allows secure access to mail and calendar servers, MS Exchange, ftp-servers, file-servers, etc., without having to install anything on the client. Sun Network Services for SAP Enterprise Portal helps lower remote access costs as well as minimize investments in dedicated modems, remote access appliances, WATS (800 toll-free numbers) calls, and related management and user support costs by providing a solution built on an Internet-based connection, as opposed to costly virtual private networks (VPN) or private dial-up line solutions. In addition, patented Java technology allows existing applications, content, files, and services to go online without the need to rewrite or modify the code. With a minimal client and connectivity investment (a Web browser and Internet connection), an enterprise or service provider can easily and rapidly extend resources to employees, business partners, and suppliers to create low-cost extranets "on the fly" as needed.

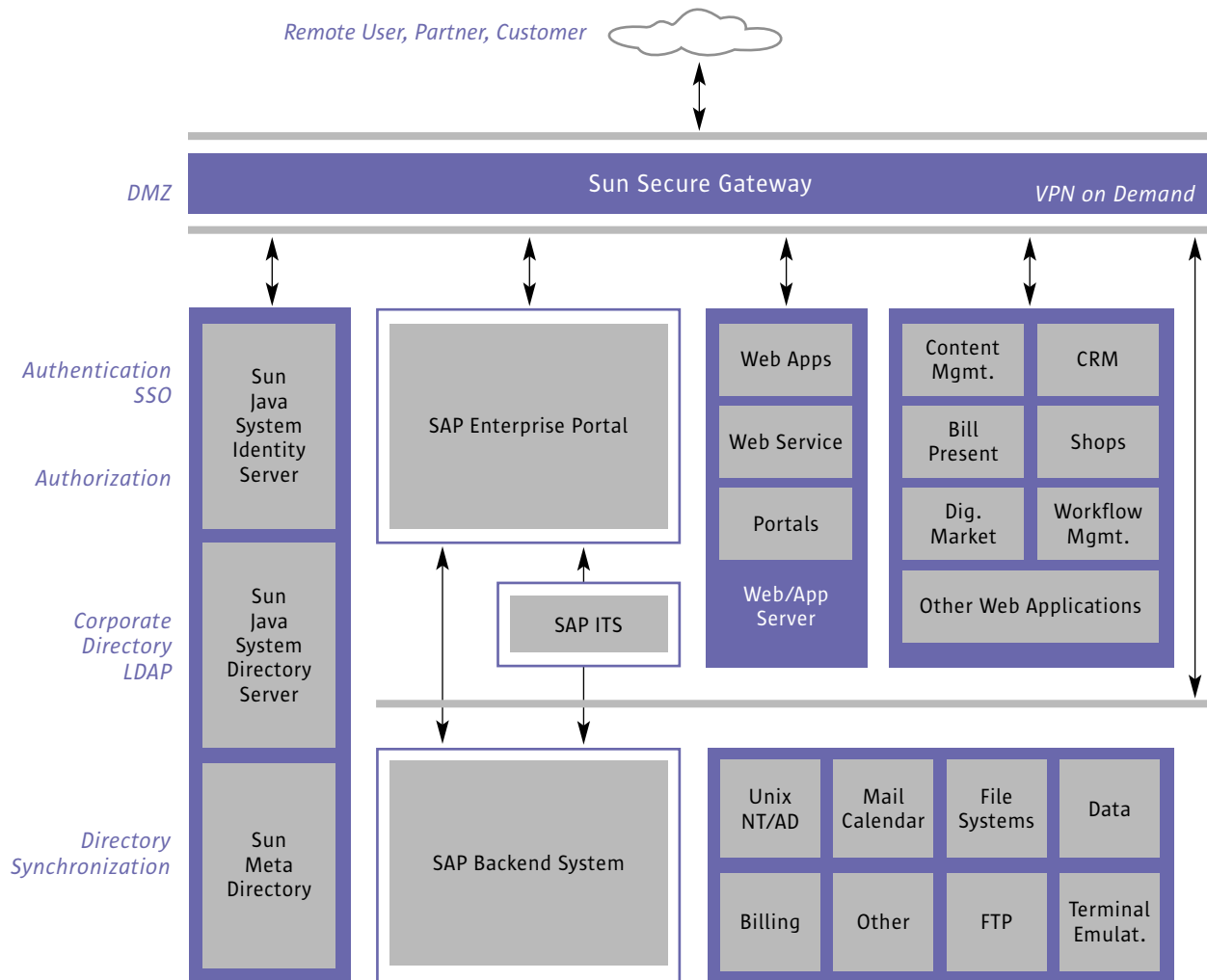
Enhanced Security—Encryption

Network security concerns continue to grow with the expanding need to deliver remote access to portal information, applications, files, content, and services situated behind corporate firewalls for anytime, anywhere access. Built on open, Internet standards, the solution addresses these security concerns. To maximize security and privacy, Sun Network Services for SAP Enterprise Portal delivers encryption through Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for any system or application. Users log on from any available browser, enter their Web URL address, and then enter their user identification. User authentication is handled over an encrypted SSL or TLS channel between the Web browser and the Secure Access Gateway.

Sun Java System provides the key security components to operate homogenous and heterogenous SAP NetWeaver landscapes.

Enhanced Security—URL-Rewriting

In a secure environment, when a user is trying to access intranet pages from outside, direct access may not be possible. The Rewriter component enables end-users to browse the intranet by making links and other URL references on those pages operate correctly. The basic premise of URL rewriting is that browser requests for internal content will always come back to a single location, the secure remote access gateway. The request will go directly to the publicly available content server if the request is for external content. This flexibility does not place unnecessary stress on the network, but provides much needed security when accessing potentially sensitive internal Web sites or downloading sensitive information. The Rewriter is an independent component that translates all the URLs (in both HTML and JavaScript™ languages) to ensure that the intranet content is always fetched through the Gateway. The administrator defines a ruleset (a collection of rules) to identify all the URLs that need to be rewritten in a page. With the Generic Ruleset that is shipped with the Rewriter, it is possible to rewrite most of the URLs without any additional rules. It is also possible to associate rulesets with domains for domain-based rewriting. The URL-Rewriter is configured to rewrite the SAP Enterprise Portal content to be delivered through the gateway.



Solution and Benefits to Business

- Customers, employees, suppliers and partners get secure remote access to sensitive data, information, Web services and applications in a strongly managed, authorized and authenticated way.
- IT management requires a low cost, ease of administration VPN solution, which has no remote client overhead. Simply put, the Secure Remote Access solution makes no demands of the remote user, other than an Internet connected browser on any device.
- It provides a cost-efficient method for providing secure remote access. This creates a lower total cost of ownership due to ease of maintenance, administration, accessibility and scalability of remote access.
- It provides increased revenues through the ability to focus on rapid deployment of existing Web, application and portal services to remote clients. This increases the return on investment of existing Web-based assets.

To learn more
visit <http://www.sun.com/sap>

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA 1-650-960-1300 or 1-800-555-9sun www.sun.com



Sun Worldwide Sales Offices: Argentina: +5411-4317-5600, Australia: +61-2-9844-5000, Austria: +43-1-60563-0, Belgium: +32-2-704-8000, Brazil: +55-11-5187-2100, Canada: +905-477-6745, Chile: +56-2-3724500, Colombia: +571-629-2323, Commonwealth Of Independent States: +7-502-935-8411, Czech Republic: +420-2-3300-9311, Denmark: +45 4556 5000, Egypt: +202-570-9442, Estonia: +372-6-308-900, Finland: +358-9-525-561, France: +33 134-03-00-00, Germany: +49-89-46008-0, Greece: +30-1-618-8111, Hungary: +36-1-489-8900, Iceland: +354-563-3010, India: Bangalore: +91-80-2298989/2295454; New Delhi: +91-11-6106000; Mumbai: +91-22-697-8111, Ireland: +353-1-8055-666, Israel: +972-9-9710500, Italy: +39-02-641511, Japan: +81-3-5717-5000, Kazakhstan: +7-3272-466774, Korea: +822-2193-5114, Latvia: +371-750-3700, Lithuania: +370-729-8468, Luxembourg: +352-49 11 33, 1, Malaysia: +603-21151888, Mexico: +52-5-258-6100, The Netherlands: +00-31-33-45-15-000, New Zealand: Auckland: +64-9-976-6800, Wellington: +64-4-462-0780, Norway: +47 23 36 96 00, People's Republic Of China: Beijing: +86-10-6803-5588; Chengdu: +86-28-619-9333; Guangzhou: +86-20-8755-5900; Shanghai: +86-21-6466-1228; Hong Kong: +852-2202-6688, Poland: +48-22-8747800, Portugal: +351-21-4134000, Russia: +7-502-935-8411, Saudi Arabia: +9661 273 4567, Singapore: +65-6438-1888, Slovak Republic: +421-2-4342-94-85, South Africa: +27 11 256-6300, Spain: +34-91-767-6000, Sweden: +46-8-631-10-00, Switzerland: German: 41-1-908-90-00; French: 41-22-999-0444, Taiwan: +886-2-8732-9933, Thailand: +662-344-6888, Turkey: +90-212-335-22-00, United Arab Emirates: +9714-3366333, United Kingdom: +44-1-276-20444, United States: +1-800-555-9SUN OR +1-650-960-1300, Venezuela: +58-2-905-3800, Or Online at sun.com/store

SUN™ THE NETWORK IS THE COMPUTER ©2004 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, and JavaScript are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. All other trademarks are trademarks of their respective owners. Printed in USA 04/04 Data Sheet DE1923-1