

Security in the Solaris™ 9 Operating System

Enabling communications and privacy while limiting exposure to risks.



Key feature highlights

- SunScreen™ versatile, integrated enterprise firewall
- IPSec suite of communication channel security protocols
- IKE key management facility
- Secure LDAP naming service
- Solaris Secure Shell secure and easy-to-use network administration
- TCP Wrappers monitoring and filtering
- Kerberos support for single sign-on
- Thread Safe BSM audit trails
- Role-based access control with access control lists
- Pluggable authentication modules
- Pluggable password encryption
- Smart card support

Today, businesses are rethinking how they create, manage, extend, and ultimately deliver information technology (IT) services with greater functionality and reduced cost and complexity. Managing data center complexity from a services perspective lets businesses focus on choosing the right solution for the job at hand, rather than managing individual systems.

Since its inception in 1982, Sun's vision and strategy has been the same: connect everything through network computing. Sun continues to leverage open standards and technologies, innovate on top of them, and create the types of systems customers demand. The foundations for this revolution are Sun's Java™ Enterprise System software, Java technology, N1™ software, and the Solaris™ Operating System. Providing the most scalable product line packed with features, tighter integration, more complete testing, and the highest security levels for general purpose servers, Sun gives companies the freedom to choose the systems and software that best meet their business needs.

For more than ten years, the Solaris Operating System (OS) has delivered the power, massive scalability, high levels of security, and mainframe-class functionality that companies demand. It's the leading UNIX® environment — and the choice for powering enterprise networks that need to deliver information to networked users at any time, any place, on any platform.

Integrated, End-to-End Security

In today's Internet age, "anytime, anywhere" access to information, electronic commerce, Web-based applications, and other mission-critical solutions creates new challenges for the data center when it comes to ensuring privacy and limiting the enterprise's exposure to business risks. The Solaris 9 Operating System provides integrated features that deliver the end-to-end security you need in order to safely deploy these powerful new solutions in your complex, enterprise computing environment.

Security in the Solaris Operating System

The Solaris 9 Operating System introduces a variety of new security features, while at the same time setting new standards for operating system security. From integrated security services and applications to enhanced encryption algorithms all the way to an enterprise firewall for network protection, the Solaris 9 OS addresses security needs at every layer.

The Solaris 9 Operating System provides integrated features that deliver the end-to-end security you need in order to safely deploy these powerful new solutions in your complex enterprise computing environment.

SunScreen™ 3.2 Software

Designed for access control, authentication, and network data encryption, SunScreen™ 3.2 software is a versatile enterprise firewall — integrated into the Solaris 9 Operating System — that provides both host-based and network-based access control capabilities. It consists of a rules-based, stateful packet-filtering engine for network access control as well as an encryption and authentication engine that enables customers to create secure virtual private network (VPN) gateways by integrating public-key encryption technology. SunScreen 3.2 software delivers secure administration through an easy-to-use graphical user interface (GUI) using a Web browser.

The SunScreen firewall product is one of the first firewall solutions to address high availability (HA) for standards-based encryption. By deploying it throughout the enterprise, corporate security policy is expanded beyond Internet firewall containment and is integrated right into the enterprise infrastructure.

SunScreen 3.2 software is a highly scalable and feature-rich enterprise-class firewall that offers a variety of features:

- Stateful packet filtering
- Configurable as a stealth and routing mode firewall
- Standalone IPSec/IKE
- Centralized management facility
- Failover functionality (HA)

- Proxy services for Telnet, FTP, HTTP, and SMTP with Trend Micro Antivirus scan
- Network address translation

IPSec/IKE

IPSec is a key feature of Solaris 9 security. IPSec is a suite of security protocols that secures communication channels and ensures that only authorized parties can communicate on them.

The industry de facto standard for encryption and tunneling over network connections, IPSec is now equipped with its own key management facility — Internet Key Exchange (IKE). IPSec/IKE enables users to establish transparent and encrypted network connections and tunnels over any given TCP/IP network infrastructure. It fully complies with the IETF specifications.

With these powerful capabilities, users can implement a wide array of security approaches in the Solaris 9 OS, such as:

- Restricting ISPs' services so that only specific services are accessible to users
- Securing communications between the tiers of multitier enterprise applications, so even those with physical network access cannot view data they are not authorized to see
- Establishing (VPNs to enable remote offices and users to communicate securely over the Internet to the home office

Secure Lightweight Directory Access Protocol (LDAP)

The Solaris Operating System enables secure authentication for applications that use LDAP-compliant data stores. In addition to IPSec, the Solaris 9 OS has SASL/DIGEST-MD5 and SSL/TLS 1.0 algorithms that allow password or complete session encryption. SSL/TLS 1.0 and IPSec support 128-bit encryption while authenticating against any LDAP-compliant data store. This allows a high degree of assurance in using LDAP as a naming service.

Solaris Secure Shell

Now integrated into the Solaris 9 OS, Solaris Secure Shell enables secure and easy-to-use network administration. Based on the established OpenSSH, Solaris Secure Shell provides more secure versions of well-known administration commands (e.g., Telnet, rlogin, etc.), all with similar interfaces. This provides experienced systems administrators with a simple transition to use Solaris Secure Shell. Organizations with a need for higher security and encryption “over the wire” can now use Solaris Secure Shell capabilities for managing their remote administration and file transfer needs.

System Minimization

The new system packaging architecture of the Solaris 9 Operating Environment enables organizations to custom build a Solaris 9 system based on a higher granularity of available install packages. In short, fewer unnecessary packages installed on a system means fewer opportunities for system attack.

For example, Telnet is a standalone package as opposed to being a part of the core package. This allows for a system configuration where only service-specific features and systems applications are installed, and mitigates the risk of introducing a potential security hole.

TCP Wrappers

TCP Wrappers capitalizes on the client-server relationship necessary for most TCP/IP applications by inserting itself into the middle of the relationship. Using its access control feature to authenticate hosts, it acts as the server until it authenticates the client/host.

The well-known TCP Wrapper application is fully integrated into the Solaris 9 OS. It provides an extremely effective method for monitoring and filtering incoming network requests for network services such as systat, finger, FTP, Telnet, rlogin, rsh, and more.

Kerberos v5

Kerberos enables communication between different systems based on the Kerberos standard for authentication. It provides a distributed, enterprise-wide authentication mechanism for single sign-on that reduces the number of times each user must go through a login sequence, thereby increasing user productivity.

The KDC server is integrated into the core Solaris 9 Operating System and allows for incremental DB propagation. It also has password interoperability with the MIT and Microsoft Windows 2000 versions of Kerberos.

Disable Stack Execution

The Solaris 9 OS reduces system vulnerabilities by preventing malicious code from running and accessing other information on the stack. It provides the ability to prevent code from being written onto the stack and executed, typically using the return address that is also on the stack. It is much less likely to use a stack-based buffer overflow to run code on the stack and gain root access.

Thread Safe BSM

The Base Security Module (BSM) supports the creation of audit trails for kernel events in the Solaris 9 Operating System. Previously a single-threaded application, the Solaris 9 platform now provides a multithreaded version of the audit daemon.

The audit files can be used for billing, intrusion detection, or system usage reports. The Solaris OS auditing is fully supported in both the C and Java programming languages. Performance improvements versus previous versions of Solaris software are expected to be significant depending on exactly what is being audited. Solaris audit tools also export data into the XML format. This standards-based format enables easier parsing, reduction, and analysis of the data.

Security in the Solaris™ 9 Operating System

Role-Based Access Control

Role-based access control (RBAC) is an alternative to the traditional superuser model of root access to UNIX systems. RBAC lets administrators assign rights to individual trusted users as well as perform specific operations, including access to such resources as serial port, file, log, printer management, user login control, and system shutdown. Users are authenticated before any role is assumed so that all privileged activities can be logged and associated with a person. Access control lists (ACLs) let you control file access rights on a per-user basis.

Pluggable Authentication Modules

Pluggable Authentication Modules (PAMs) provide a uniform means for third-party applications, as well as the Solaris Operating System itself, to access user authentication facilities. PAM modules can be easily constructed to support site-specific authentication requirements, for example, an interface with a biometric scanning device such as a palm scanner for user identification.

Pluggable Password Encryption

Passwords in the Solaris 9 OS can be encrypted using standard crypt, MD5, or Blowfish algorithms. The MD5 and Blowfish algorithms provide better protection of the passwords and are compatible with Linux and BSD-based operating systems.

Solaris 9 software also features a pluggable interface for password encryption, so customers or ISVs can extend encryption to use their own algorithms, a key requirement for some government and high security environments. Pluggable password encryption technology is compatible with passwords stored in files, NIS, NIS+ and LDAP naming services, provided all clients and servers are using the Solaris 9 OS.

Smart Card Support

Smart cards can offer a tremendous boost to an enterprise's security architecture. The Solaris 9 Operating system supports functions — including smart card authentication, storing of personal information, Java applet management, and support for the Smart Card Framework (SCF) — to enable organizations to implement smart card solutions.

About Sun

For years, customers have turned to Sun Microsystems to help them expand their business, lower their costs, and gain competitive advantage. Sun is a leading provider of industrial-strength hardware, software, services, and technologies that make the Net work.

For more information on Sun, please visit sun.com.

System Requirements

Security is a feature of the Solaris Operating System

Learn More

Get the inside story on the trends and technologies shaping the future of computing by signing up for the Sun Inner Circle program. You'll receive a monthly newsletter packed with information on the latest innovations, plus access to a wealth of resources. Register today to join the Sun Inner Circle Program at sun.com/joinic.

To receive additional information on Sun software, products, programs, and solutions, visit sun.com/software.

For More Information

To learn more about security in the Solaris 9 Operating System, visit sun.com/security. For more information on the Solaris 9 Operating System, visit sun.com/solaris.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 800 786-7638 or +1 512 434-1577 Web sun.com



Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, 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 +603-21161888, 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, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-596-9900, 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

SUN™ © 2003 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, Solaris, and SunScreen 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. Information subject to change without notice. v3.0 9/03 R1.0