

SUNSCREEN™ SECURE NET 3.1 FOR THE SOLARIS™ OPERATING ENVIRONMENT

THE SOLARIS™ OPERATING ENVIRONMENT

The Solaris™ 8 Operating Environment is the established OS leader for availability, scalability, and security in the Internet age. In Solaris 8 software, Sun delivers a trustworthy, universal platform to meet the needs of dot-com businesses — from small startups to large Fortune 1000 enterprises.

It's no surprise that the Solaris Operating Environment is the leading UNIX® environment today. Solaris software was originally designed with the Internet in mind. TCP/IP, the central Internet protocol, has been at the core of Solaris networking for more than 15 years. Through its time-tested design — a small, stable kernel, modular and extensible components, and well-defined interfaces — Solaris software delivers rock-solid stability and predictability for business-critical applications. And the Solaris 8 Operating Environment provides complete compatibility with prior versions, so you can be confident that your current applications will continue to run.

REQUIREMENTS FOR THE SECURE BUSINESS NETWORK

Today, the focus in network security has shifted from preventing attacks from the Internet with a single firewall to providing security throughout the corporate network. The reason for this paradigm shift is simple: network-wide security now allows large organizations to utilize the Internet's full potential, enabling new business models such as secure intranets, secure extranets for partners, and secure remote access for employees.

The secure business network is a comprehensive security system for the entire corporate infrastructure. Although a firewall plays an important part in providing this level of security, a true secure business network is far more extensive than a single firewall.

A secure business network includes:

- Multiple, high-performance screens (firewalls) to support the ever-increasing network demands
- Increased security for screens
- Centralized management of multiple screens
- High availability for screening and encryption

SUNSCREEN™ SECURE NET FOR ENTERPRISE-WIDE SECURITY

SunScreen™ Secure Net is a versatile firewall that 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. It 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 software also reaches out from the enterprise. Corporate partners that have a SunScreen firewall, or use SunScreen™ SKIP (Simple Key-management for Internet Protocols) encryption-based firewalls, can connect into a secure extranet.

- SunScreen Secure Net 3.1 is a bundle consisting of:
 - SunScreen 3.1 firewall
 - SunScreen SKIP 1.5.1 for the Solaris Operating Environment
 - SunScreen SKIP 3.0.7 for Microsoft Windows
- SunScreen™ 3.1 Lite is bundled with Solaris 8 Operating Environment (6/00 update) at no additional charge
- The SunScreen 3.1 firewall is supported on Solaris 8, 7, and 2.6 Operating Environments as well as the Trusted Solaris™ 7 Operating Environment, SPARC™ Edition
- Delivers an enterprise-grade firewall suitable for perimeter, department and individual server protection
- Offers stealth capability for perimeter defense
- Provides routing and proxy support
- Now includes Gigabit Ethernet and ATM CIP support
- Includes improvements to:
 - SNMP status reporting
 - Centralized management
 - Administration Graphical User Interface
 - Documentation

SUNSCREEN PRODUCT FEATURES

CENTRALIZED MANAGEMENT

Large secure business networks can require anywhere from 10 to 100 or more firewalls throughout the world, and ideally, all these firewalls should be managed from a central location. By grouping these firewalls, one screen can act as the primary screen for a group of firewalls with common address groups, service groups, user groups, and rules for defining the network configuration. Each individual screen's configuration inherits these common definitions, however, the configuration can be customized through the implementation of rules and objects unique to the specific firewall.

GUI MANAGEMENT SYSTEM

Java™ technology-based GUIs running on a browser enable an administrator to remotely manage the screens. SunScreen SKIP, managed by the `skiptool` GUI, secures the connection between the system running the browser and the screens. Additionally, an installation wizard GUI assists new installations.

OPERATING MODES

A SunScreen firewall has two distinct operating modes. Customers can designate interfaces in either routing or stealth mode on a screen-by-screen or port-by-port basis.

Routing

In routing mode, the SunScreen product is a firewall with the optional use of proxies for content filtering and user authentication. Fully engineered for multiprocessing, SunScreen is one of the fastest firewalls available. Typically, a routing firewall is used within the enterprise intranet.

Stealth

Because no IP address is used, stealth screens provide a higher level of security. Configurable stealth solves the problem of organizations that need both types of firewalls. When connecting to non-secure networks, stealth capability provides extra security against firewall attack.

HARDENED OPERATING SYSTEM

Stealth mode offers optional hardening of the operating environment on the screen. Hardening removes packages and files from the Solaris Operating Environment that are not used by the SunScreen firewall.

HIGH AVAILABILITY

High availability (HA) is available for both routing and stealth mode installations. The primary HA screen manages secondary HA screens in an HA cluster. Passive HA screens within an HA cluster mirror the state of the active screen, which can be the primary or a secondary HA screen. When the active screen fails, the passive screen that has been running the longest takes over as the active screen within the cluster.

PROXIES

In routing mode, optional proxies provide content filtering and user authentication. A SunScreen firewall provides proxies for:

- **HTTP Proxy:** Allows or denies connections based on source and destination addresses and provides filtering functions such as passing or dropping Java applets, Java applets based on signatures, cookie requests and responses, and Active X content.
- **Telnet Proxy:** Provides a virtual terminal relay, allows or denies connections based on source and destination addresses, and performs user authentication.
- **FTP Proxy:** Functions as a relay for FTP and controls connections based on source and destination addresses and user authentication. The proxy limits access to certain file transfer commands such as `put` or `get` based on these same criteria.
- **SMTP Proxy:** Provides a relay for electronic mail and makes access determinations based on source and destination addresses. Anti-spam filtering is also available.

NETWORK ADDRESS TRANSLATION

Network address translation (NAT) enables a screen to map an internal network address to a different external address, masking the identity of machines within the enterprise. As it passes packets between an internal host and a public network, the addresses in the packet are replaced with new addresses transparently, checksums and sequence numbers are corrected, and the state of the address map is monitored. Administrators can specify when a packet using ordered network address translations is applied based on source or destination addresses.

TIME-OF-DAY RULES

Administrators can define rules that are active only during specified time periods.

LOGGING

Administrators can search and filter log messages to find critical information quickly and easily. They can monitor logs in real time using the browser or export logs for subsequent processing.

CONFIGURATION VERSIONS

Individual versions of a policy are copied or saved into a new policy. Each version of a policy is maintained, and either all or a portion of a policy can be used at a later date.

ADMINISTRATION PRIVILEGES

There are four administrative roles to appropriately separate privileges. The Status Administrator can view the log information and statistics page. The Read-Only Administrator has read access, which permits viewing of firewall configurations such as rules, address groups, etc., as well as allowing backup of configuration and log information. The Write Administrator has all the privileges of both the Read-Only Administrator and the Status Administrator. The Administrator role has the same privileges as the Write Administrator plus the authority to assign administrator roles.

TUNNELING

Encrypted tunnels hide network topology from intruders and enable the setup of secure VPN gateways over insecure public networks.

SUNSCREEN 3.1 LITE

SunScreen 3.1 Lite is bundled with the Solaris 8 Operating Environment (6/00 update) to provide sophisticated protection for every Solaris server, and is easily upgradable to the full version of the SunScreen 3.1 product. SunScreen 3.1 Lite includes the same features of the full version of the SunScreen 3.1 firewall with the following differences:

- No proxy support
- No high availability support
- No stealth support
- SunScreen 3.1 Lite firewalls can be managed by members of a centralized management group, but cannot create one

- Only two network interfaces are permitted
- Only 2 NAT rules and a maximum of 10 source address translations are allowed

SUNSCREEN SKIP

Strong standards-based SKIP encryption provides protection for data whenever critical information is sent over untrusted internal networks or the Internet. For example, user groups within certain functional areas — such as finance — can have e-mail and other communication encrypted over the network. Additional security measures can be invoked for services such as file copying (FTP) and remote login (telnet).

To enable secure remote access from a remote administration station, SunScreen Secure Net includes SunScreen SKIP clients for Solaris and Microsoft Windows 95, 98, 98 Second Edition, and NT 4.0 environments. SunScreen SKIP provides protection for the data being transmitted by ensuring its integrity and enforcing a high level of authentication between two SunScreen SKIP nodes.

SunScreen SKIP features include:

- **Application Independence:** SunScreen SKIP is a software module that lies at the IP layer and is application independent
- **Automatic Certificate Discovery:** Eliminates manual key distribution
- **Optional Certification Authority Infrastructure Support**

SunScreen SKIP is available in two versions: 56-bit and 128-bit. The two versions support self-generated or issued certificates from 1028 bits to 4096 bits. Data encryption varies from 40-bit RC2 and RC4 to 128-bit SAFER CBC and 3-Key Triple-DES.

SUNSCREEN SYSTEM REQUIREMENTS

HARDWARE/SOFTWARE PLATFORMS

- Any system running the Solaris 8, 7, or 2.6 Operating Environment on SPARC or Intel Architecture platforms
- Any system running the Trusted Solaris 7 Operating Environment on SPARC platforms

LINK SUPPORT

- Ethernet, Fast Ethernet, Gigabit Ethernet, ATM (155 and 622 Mbit/sec in LAN emulation mode; CIP mode), Token Ring, and FDDI

BROWSERS

- Browsers supported for administrating SunScreen Secure Net are the HotJava™ (Solaris 7 and 2.6 only) browser, Netscape™ Communicator, and Internet Explorer browsers supporting JDK™ 1.1 software (and later) and running on the Solaris 8, 7, 2.6, and 2.5.1 Operating Environment as well as PCs running Windows 95, 98, 98 Second Edition, and NT 4.0

MEMORY

- For systems running just the screen, 32 Mbytes minimum; for systems running the administration station, 32 Mbytes minimum (64 Mbytes strongly recommended)

DISK SPACE

- A minimum of 1 Gbyte

NOTE: HA in routing mode is supported for Ethernet and Fast Ethernet. In addition, HA requires that the two screens be connected via a non-switched hub or an Ethernet switch that can function as a “dumb” hub.

SUNSCREEN SKIP SYSTEM REQUIREMENTS

HARDWARE/SOFTWARE PLATFORM

- Any system running the Solaris 8, 7, or 2.6 Operating Environment on SPARC or Intel Architecture platforms as well as PCs running Windows 95, 98, 98 Second Edition, and NT 4.0 (up to and including Service Pack 6/6a)

I/O DEVICES

- One or more supported network interfaces, a CD-ROM drive, and a diskette drive if using issued certificates

MEMORY

- A minimum of 16 Mbytes is required; 32 Mbytes is recommended

DISK

- A minimum of 12 Mbytes of disk space is required for installation, 7 Mbytes of which will be permanently used

FOR MORE INFORMATION

To learn more about SunScreen Secure Net, please visit our Web site at www.sun.com/security.