SunScreen 3.2 Release Notes

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

Part No: 806–6350
January 2002

020529@3984

Contents

SunScreen 3.2 Release Notes

This document contains information that was not available when the SunScreen 3.2 documents were printed.

This document is the companion to the following:

- *SunScreen 3.2 Installation Guide* (PN 806-6345)
- *SunScreen 3.2 Administration Guide* (PN 806-6346)
- *SunScreen 3.2 Administrator's Overview* (PN 806-6347)
- *SunScreen 3.2 Configuration Examples* (PN 806-6348)
- *SunScreen SKIP User's Guide, Release 1.5.1*, (PN 806-5397)
- *SunScreen SKIP, Release 1.5.1, Release Notes*

Documentation Errata

The following documentation errors could not be corrected before FCS.

SunScreen 3.2 Administrators Guide

In this manual, Appendix A lists the differences between the Full and Lite versions of SunScreen 3.2. However, there is no Lite version of SunScreen 3.2.

SunScreen 3.2 Administrators Overview

- The supported hardware and software requirements in Chapter 1 are incorrect. Please refer to the *SunScreen 3.2 Installation Guide* for the correct requirements
- Chapter 9 describes VirusWall content scanning. This feature is not available in SunScreen 3.2.

What is New in This Release

SunScreen 3.2 offers the following enhancements:

- Support for the Trusted Solaris 8 and Solaris 9 operating environments.
- Support for IPsec, the IETF standard security protocols for data privacy and authentication. Cryptographic keys can be configured manually or configured using IKE (Internet Key Exchange).
- IKE includes the following capabilities:
  - Support for SunScreen IKE protocol for automatic algorithm and key exchange.

    If you are using Trusted Solaris 8, IKE and IPsec require the Solaris `SUNWcryr` and `SUNWcryrx` packages that contain encryption modules. You must download these packages from: `www.sun.com/software/solaris/encryption/download.html`.

    If you are using Solaris 9, DES and 3DES cryptographic support is bundled with the operating environment. However, if you need more support (for AES for example), you also have to install the cryptography packages.
  - Support for IKE with the centralized management group feature.
  - Support for IKE between a Windows 2000 system and a Screen using pre-shared keys or CA-signed certificates.
  - Support for IKE between a Screen and a Windows 2000 system acting as a remote Administration Station using CA-issued certificates.

Note – For background information on IKE, see the *SunScreen 3.2 Administrators Overview*. For step-by-step instructions on performing IKE related tasks, see the *SunScreen 3.2 Administrators Guide*. For network examples using IKE, see the *SunScreen 3.2 Configuration Examples* manual.

- SunScreen SKIP 128-bit encryption as the default (SunScreen SKIP, release 1.5.1)
- An updated installer developed to meet Solaris software requirements
- Updated packaging that makes graphical user interface (GUI) and encryption software installations optional.
- Spoof detection is more robust and configurable.
- Enhanced performance for transmission control protocol (TCP), user datagram protocol (UDP), and network address translation (NAT).
- Supports Destination Address Checking used to detect certain kinds of routing misconfigurations and misbehaving applications.
- Blocks IPv6 interfaces.

SunScreen identifies IPv6 interfaces when they are plumbed and blocks those interfaces configured for use by SunScreen from passing IPv6 packets through the firewall.

- Support for `tcp_keepalive` state engine.
- Supports overlap of interface address groups (used for IPMP, and so forth).
- Support for up to 15 stealth interfaces and virtually unlimited routing interfaces.
- Support for SNMP alerts and logging of HA events; specifically HA failover.
- Support for fault tolerant `pnet` interfaces.

  This interface is used with the Netra ft1800. Modifications were made to the startup scripts to successfully and securely plumb the interface of the Netra ft1800.
- Support for generating WebTrends Enhanced Log Format (WELF) format log files using the SunScreen `welfmt` utility.

  The SunScreen `welfmt` program reads a SunScreen binary log file and generates an ASCII log file to WELF standards. WebTrends Firewall Suite (WFS) produces various reports from the SunScreen WELF log files on such topics as bandwidth usage, protocol distribution, email and Web activity, FTP transfers, and Telnet sessions.

Note – WFS is a third-party product from WebTrends. If it is already loaded on your system, ensure you are using version 3.0 or later.

SunScreen 3.2 Limitations

- SunScreen SKIP does not work in a Trusted Solaris 8 Update 4 operating environment when using the TSOL protocol.
- On Trusted Solaris 8, Update 4, there is a problem with `dac_write` privileges when using the GUI installer as admin. To install on this release, run

  ```
  # chmod u+w /var/sadm/install
  ```

  in a privileged role like `secadmin` and then run the installer as `admin`.
- SKIP Version 1 is not supported on SunScreen 3.2.
- RSA-ENCRYPTION-REVISED is not supported on SunScreen 3.2.
- Because Windows 2000 does not support RSA-ENCRYPTION for authentication, use RSA-SIGNATURES instead.
- Within IKE, support for the RSA-ENCRYPTION authentication method does not work.
- Centralized management groups cannot use IKE and SKIP simultaneously.

- You cannot select IKE as a Remote Administration encryption option from the Solaris Web Start Wizards™ installer program (command line or GUI).
- If you encounter a Java memory exception error during installation: `java.lang.OutOfMemoryError`, exit the installation, remove `/var/sadm/install/prod*`, and restart the installation.

SunScreen 3.2 Known Problems

The following known problems exist in the SunScreen 3.2 product.

- BugID #4548783

  In a Trusted Solaris 8 Update 4 environment, IKE does not work with the TSOL protocol.

- BugID #4554498

  In an HA configuration with IKE, if the secondary HA system becomes active, existing IKE connections do not fail over and no new IKE connections can be initiated.

- BugID #4531858

  The IKE daemon may sporadically and on infrequent occasions, get in a state where it will not successfully negotiate new connections. The workaround is to kill the daemon and reactivate the policy.

- BugID #4502706

  Running SunScreen on the Trusted Solaris 8 operating environment when using the TSOL networking protocol, packets labeled CDP or IKE do not leave the system and `iked` eventually exits.

  Two problems exist: One is the insufficient `priv` on `ss_iked_restart`; the second is that TSOL needs an explicit `isakmp` rule that unlabeled packets or the regular Solaris software do not need.

  Perform the following steps:

  Note – The first two steps are always required. The third step is required for `TSOL` traffic, but *not* for unlabeled traffic.

  ---

  1. Type the following command:

     ```
     # setfpriv -s -a ALL /usr/lib/sunscreen/lib/ss_iked
     ```

  2. Change the `tsol ss_iked_restart exec_attr` line to include `35,61,68`

     ```
     SunScreen:tsol:cmd:::
     /usr/lib/sunscreen/lib/ss_iked_restart:privs=35,61,68;uid=0
     ;gid=3;euid=0
     ```

Note – Do this on the line that begins with `SunScreen:tsol` and *not* on the line that begins with `SunScreen:suser`.

3. For IKE with TSOL labeled traffic, you must add a rule to allow UDP port 500 traffic by typing:

```
edit> add rule isakmp ALLOW
```

- BugID #4495529

  IKE does not work with the Commercial Internet Protocol Security Option (CIPSO) networking protocol.

  IKE packets with CIPSO labels are dropped by `screen_ipsec`. `"screen_ipsec predecrypt: not ipv4 or packet has options"` IKE packets with options should be allowed by a Screen because they are valid in this situation.

- BugID #4504676

  Due to a packaging problem with `SUNWsfwi`, the `ss_iked` binary does not have all allowed privileges.

  Perform the following steps:

  1. Run the following as the `secadmin` role by typing:

```
# setfpriv -s -a all /usr/lib/sunscreen/lib/ss_iked
```

     Without allowed privileges, IKE cannot get the inherited privileges defined in `exec_attr`.

  2. Create the file `pkgs/SUNWsfwi/tsolinfo` with the following contents:

```
default        allowed_privs     all
```

     This ensures that all executables delivered with this package have all allowed privileges (and, thus, can inherit them).

- BugID #4491808

  IKE fails in tunnel mode on SunScreen to a Windows 2000 system.

  The same systems can connect in *transport* mode with a connection initiated from either side. Initiating a connection from a Windows 2000 system to the Screen in tunnel mode does work. Also, once an SA is negotiated, encrypted connections work from any direction. The `oakley.log` file on the Windows 2000 system says: "Tunnel mode is transport mode," which is an undocumented error message.

- BugID #4500831

  When installing SunScreen 3.2 on a Trusted Solaris 8 system and choosing to use SunScreen SKIP encryption on the remote Administration Station, a Java™ error causes the installer to exit when configuring and activating.

  Do a default installation, then manually configure the remote Administration Station at a later time.

- BugID #4496677

  Using `ssadm ha status -Z` on a Non-high availability (HA) system returns the message: `cannot open`.

- BugID #4497611

  When multiple certificates have the same subject alternative name, the following error message is returned: "bad remote certificate, rejected!"

  Windows 2000 IKE ignores CA preferential ordering and agrees on the first match it finds in its database, regardless of the ruleset. To fix this problem, limit the list of possible CA-issued certificates in the rule to one CA-issued certificate on Windows 2000 systems.

- BugID #4330437

  Removing an interface from the host causes the Screen to not come up.

  The Screen does not work when you physically remove an interface from the host or change the Solaris network configuration and reboot without first removing the SunScreen Interface object definition for that interface. This happens when the interface that was removed has already been defined in the Screen.

  You must add the interface back onto the host and reboot to fix this problem. Or, if the interface no longer exists, remove the interface object from the Screen.

Note – You can no longer activate a policy through the command line user interface because the Screen cannot contact its secondary.

Perform the following steps:

1. Find the current policy by typing:

   ```
   # ssadm active
   ```

   For example, the output could be `Initial.n`, where `n` is the policy version number.

2. Activate the policy by typing:

   ```
   # ssadm activate -1 Initial.m
   ```

   Where m=n-1.

   Now, you can login to the `ssadm` server.

   Note – Rebooting, also brings up the Screen.

Use the following steps to remove the SunScreen `interface` object definition:

1. Log onto the console of the Screen as root, if not already.

2. Remove the offending Interface object from your SunScreen policy by typing:

```
# ssadm edit Initial
edit> delete interface qfe2
edit> save
edit> quit
```

Note – See "Interfaces" in the *SunScreen 3.2 Administration Guide* for more information on removing an interface.

3. Activate the policy by typing:

```
# ssadm activate Initial
```

4. Reboot the system.

A Word of Caution

If you are using SKIP, IPsec, or IKE cryptography on your Screen, you should secure any core files and private keys. A savecore file (kernel core dump) contains your local cryptographic secret or secrets. It would be difficult for someone to discern or discover the secret, but it is possible. You should, therefore, protect a core file as carefully as any of your other local secrets.

Remember, if you send your core file out-of-house for analysis, you are giving your local secret to the analyst.

Because all regular system backups made while a core file exists contain the files in which your local secret or secrets are stored, any system backups must be considered a possible means of discovering your local secret or secrets.

Note – Keep all of your regular system backups in a secure location.