Securing Sun Enterprise™ 10000 System Service Processors

By Alex Noordergraaf - Enterprise Engineering

Sun BluePrints™ OnLine - March, 2002

http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 816-4458-10
Revision 01, 03/18/02
Edition: March 2002

Please
Recycle

Securing Ultra Enterprise 10000 System Service Processors

This Sun BluePrints OnLine™ article describes a secure Sun Enterprise™ 10000 (Enterprise 10000) configuration that is fully Sun supported. It provides tips, instructions, and guidance for creating a more secure Enterprise 10000 system.

This article contains the following topics:

The Enterprise 10000 System Service Processor (SSP) controls the hardware components that comprise an Enterprise 10000 server. Because the SSP is a central control point for the entire frame, it represents an excellent attack point for intruders. To improve reliability, availability, and serviceability (RAS), secure the SSP against malicious misuse and attack.

The Enterprise 10000 SSP runs the Solaris 8 OE; many of the recommendations made in other Sun BluePrints OnLine articles about hardening the Solaris OE apply to the Enterprise 10000 SSP. This article uses these recommendations and offers SSP-specific recommendations to improve the overall security of the Enterprise 10000 SSP.

This article and other security articles are available electronically from Sun BluePrints OnLine at:

```
http://www.sun.com/security/blueprints
```

Background Information

This section contains the following topics:

Assumptions and Limitations

In this article, our recommendations are based on several assumptions and limitations as to what can be done to secure an Ultra Enterprise 10000 using a Sun supported configuration.

Our recommendations assume a platform based on Solaris 8 Operating Environment 10/01, the SUNWCall Solaris OE installation cluster, and System Service Processor (SSP) software versions 3.3, 3.4, and 3.5.

The hardening configuration in this document is also supported with SSP software version 3.5 running Solaris 9 OE.

Solaris Operating Environment (Solaris OE) hardening can be interpreted in many ways. For purposes of developing a hardened SSP configuration, we address hardening all possible Solaris OE options. That is, anything that can be hardened, is hardened. When there are good reasons for leaving services and daemons as they are, we do not harden or modify them.

Note – Be aware that hardening Solaris OE configurations to the level described in this article may not be appropriate for your environment. For some environments, you may want to perform fewer hardening operations than recommended. The configuration remains supported in these cases; however, additional hardening beyond what is recommended in this article is not supported.

Minimizing the Solaris OE or removing Solaris OE packages to minimize security exposure is not a supported option on the Enterprise 10000 SSP. Only Solaris OE hardening tasks described in this article are supported configurations for the SSP.

Note – Standard security rules apply to hardening Enterprise 10000 SSPs: *that which is not specifically permitted is denied*.

When addressing security of the SSPs, we focus on SSP functionality inherent in or required by SSP servers. We do not address security for non-SSP servers running Solaris 8 OE. For recommendations on generic Solaris OE security configuration, refer to other sources such as the security-related Sun BluePrints OnLine articles.

In this article, we omit additional software that you can install on the SSP, such as Sun Remote Services Event Monitoring, Sun Remote Services Net Connect, and Sun Management Center software.

Note – The SSP code uses gethostbyname() to retrieve the IP address of the domains. To ensure proper function of this routine it is critical that the SSP name resolution be configured properly. Each SSP must have the domains' private network addresses and their corresponding IP addresses listed in the `/etc/hosts file`. In addition, the SSPs must be using files for name resolution.

We do not use InterDomain Networking (IDN) in the reference architecture. IDN uses the backplane of an Enterprise 10000 system to route network traffic between domains. This routing might introduce security vulnerabilities. Before using IDN in a secured Enterprise 10000 environment, carefully review the security implications.

Qualified Software Versions

The Solaris OE security hardening recommendations in this article are based on Solaris 8 Operating Environment 10/01 (Update 6).

The SSP software versions qualified to run in the secured environment are SSP versions 3.3, 3.4, and 3.5. Note that Solaris 9 OE is qualified with SSP version 3.5 too.

Note – For the SSP software to function properly, SSP version 3.5 must have patch 112248-01 or newer installed. Also, SSP version 3.4 must have patch 111174-02 or newer installed.

The Solaris Security Toolkit (Toolkit) version used is 0.3.5.

Obtaining Support

The Enterprise 10000 SSP configuration implemented by the Solaris Security Toolkit (Toolkit) SSP module (`starfire_ssp-secure.driver`) is a Sun supported configuration. A hardened SSP is *only* supported by Enterprise Services if the security modifications are performed using the Toolkit. Support calls to Sun Enterprise Services are handled the same as other service orders.

Note – The Toolkit itself is not a supported Sun product. Only configurations created with the Toolkit are supported.

To obtain Toolkit support, use the Solaris Security Forum link at the following web site:

```
http://www.sun.com/security/jass
```

Sun Enterprise™ 10000 System Features and Security

The following paragraphs describe features and security issues of the Sun Enterprise 10000 (Enterprise 10000) system.

Enterprise 10000 System Features

The Enterprise 10000 server is the largest in the Sun Enterprise server line. With 64 processors, domain capabilities, and other features this server is frequently used in server consolidation projects and multitiered architectures.

One of the most unique features of the Enterprise 10000 system is its management. The resources of the frame—such as processors and I/O resources—can be virtually assigned to any domain within the frame. The management of these resources is controlled by one or two servers external to the frame. These servers are sun4u based servers such as the Sun Enterprise™ 250 server.

Enterprise 10000 System Security Issues

Over IP, the SSPs have management connections to the control boards of the frame, in addition to connections to each domain. The standard configuration for these network connections is to have one network, or IP range, interconnecting the domains, control boards, and SSPs. This configuration poses a significant security risk because this network could be used to access one domain from another domain. This risk may exist even when the action is specifically prohibited by firewalls or other access control technologies on the other networks connected to the domains.

For example, in the default configuration, a malicious user on `domain_a` might directly access `domain_b` over the control board/SSP network despite firewalls that separate these domains on the public or production networks.

In addition to this security issue, a malicious user might use the SSPs to access other domains. For example, a malicious user on `domain_a` could gain access to the SSP, then use the SSP to gain access to `domain_b`.

To enforce domain separation, the SSP management network connection to the domains and the SSP itself must be secured. Domain separation enforces privacy of information and resources between domains or systems.

SSPs and the management networks on which they depend can pose a serious threat to overall domain security on an Enterprise 10000 system. To mitigate this risk, configure the SSPs and management network to protect themselves and the domains inside the frame against potential misuse.

System Service Processor (SSP)

The *Sun Enterprise 10000 SSP 3.4 Users Guide* describes the SSP as follows:

> The System Service Processor (SSP) is a SPARC™ workstation or SPARC server that enables you to control and monitor the Sun Enterprise 10000 system. You can use a Netra T1, Ultra™ 5, or Sun Enterprise 250 workstation server as an SSP. In this book, the SSP workstation or server is simply called the SSP. The SSP software packages must be installed on the SSP. In addition, the SSP must be able to communicate with the Sun Enterprise 10000 system over an Ethernet connection.
>
> The Sun Enterprise 10000 system is often referred to as the platform. System boards within the platform may be logically grouped together into separately bootable systems called Dynamic System Domains, or simply domains. Up to 16 domains may exist simultaneously on a single platform...The SSP lets you control and monitor domains, as well as the platform itself.

Clearly, the SSP provides many critical functions for an Enterprise 10000 system. The domains do not operate properly if a controlling SSP is absent. Preserving the security of the SSP is very important.

SSP Redundancy

You can use up to two SSPs to manage the Enterprise 10000 frame. Each SSP is one of the sun4u based servers on which the SSP software is supported, such as the Sun Enterprise 250 server.

The two SSPs should have the same configuration. This duplication should include the Solaris OE installation, security modifications, network configurations, patch installations, and all other system configuration aspects. This statement is less a recommendation for security than it is a reminder that configuration and change management of the SSP is critical to its ongoing maintainability.

SSP Features

Systems running SSP enable system administrators to perform the following tasks, which is a partial list:

- Create domains by logically grouping system boards together. Domains are able to run their own operating system and handle their own workload.
- Boot the domains.
- Dynamically reconfigure a domain so that currently installed system boards can be logically attached to or detached from the operating system while the domain continues running in multiuser mode. This feature is known as Enterprise 10000 system dynamic reconfiguration and is described in the *Sun Enterprise 10000 Dynamic Reconfiguration User Guide*. (A system board can easily be physically swapped in and out when it is not attached to a domain, even while the system continues running in multiuser mode.)
- Perform automated dynamic reconfiguration of domains.
- Assign paths to different controllers for I/O devices, which enables the system to continue running in the event of certain types of failures. This feature is known as Alternate Pathing (AP) and is described in the *Sun Enterprise Server Alternate Pathing 2.3 User Guide*.
- Monitor and display temperatures, currents, and voltage levels of one or more system boards or domains.
- Monitor and control power to components within a platform.
- Execute diagnostic programs such as power-on self-test (POST).

More information about the capabilities of the SSP software is available in the *Sun Enterprise 10000 SSP 3.5 User Guide*.

SSP Default Configurations

This section provides an overview of the default configurations of SSP software applicable when you install the required software to secure an Enterprise 10000 system.

SSP Packages

The SSP software bundle is comprised of the following packages, which are specific to the Enterprise 10000 system:

```
application SUNWsspdf      System Service Processor Data Files
application SUNWsspdo      System Service Processor Domain Utilities
application SUNWsspdr     System Service Processor Dynamic Reconfiguration Utilities
application SUNWsspfp      System Service Processor Flash Prom Image
application SUNWsspid      System Service Processor Inter-Domain Networking
application SUNWsspmn      System Service Processor On-Line Manual Pages
application SUNWsspob      System Service Processor Open Boot Prom Utilities
application SUNWsspop      System Service Processor Core Utilities
application SUNWssppo      System Service Processor POST Utilities
application SUNWsspr       System Service Processor (Root)
application SUNWsspst      System Service Processor Scan Tests
application SUNWsspue      System Service Processor User Environment
```

SSP Accounts and Security

The SSP automatically adds the following users to the `/etc/passwd` file:

```
ssp:x:12:10:SSP User:/export/home/ssp:/bin/csh
```

Additionally, the following are new SSP `/etc/shadow` contents:

```
ssp:NP:11603::::::
```

When the SSP adds the preceding accounts, including the `ssp` account, they are initially locked with “NP” as the encrypted password.

Note – A system administrator should set the password for the `ssp` user, on both SSPs, immediately after installing the SSP software or upon first powering up the Enterprise 10000 system.

The SSP does not add any entries to the `/etc/group` file.

SSP Daemons

The SSP daemons are organized into two separate types, which are each listed below with sample output.

The platform or core daemons that run on both the main and spare SSP are as follows:

```
ssp  1367     1  0 15:42:59 ?        0:22 fad
ssp  1383     1  0 15:43:00 ?        0:01 machine_server -m
ssp   784     1  0 15:36:12 ?        0:10 fod
```

The daemons that run only on the main SSP are as follows:

```
root 467  1 1 15:33:50 ? 2:31 scotty -f /etc/opt/SUNWssp/ssp_startup.tcl 15
ssp  1496 1 0 15:45:15 ? 0:00 edd
ssp  1446 1 0 15:45:03 ? 0:00 datasyncd
ssp  1452 1 0 15:45:06 ? 0:07 cbs
root 3712 1 0 12:08:36 ? 0:00 snmpd
ssp  1477 1 0 15:45:09 ? 0:00 straps
```

Note – This listing of daemons is a sample of the services that may be encountered. Depending on how many domains are in use, more daemons are running for each domain.

The SSP daemons are started by `/etc/rc2.d/S99ssp`, which calls the startup script `/etc/opt/SUNWssp/ssp_startup.sh`.

The following table provides a brief description of each daemon. For additional information on these daemons, refer to the *Sun Enterprise 10000 SSP 3.5 User Guide* and the *Sun Enterprise 10000 SSP 3.5 Reference Manual*.

Daemon	Description
`cbs`	Provides the SSP communication interface to the Enterprise 10000 system. This server daemon communicates directly with the control board executive (CBE) on the active control board via TCP/IP. (The communication protocol between `cbs` and CBE is called control board management protocol (CBMP). Other SSP daemons communicate with `cbs` via RPC.
`datasyncd`	Synchronizes SSP configuration files between the main and spare SSP. Copies files from the main to the spare SSP through a TCP/IP connection over the private SSP data network. Traffic from datasyncd is routed through the private connection that is not used for control board management. This daemon relies on other SSP daemons, including `fod` and `fad`. The datasyncd daemon runs only on the main SSP. Note: this daemon is not present in SSP version 3.3.
`edd`	Uploads event detection scripts to the control board executive (CBE) through `cbs`. The event detection scripts run within the event monitoring task of CBE and poll various conditions with the platform such as environmental conditions, signature blocks, and voltages. Changes monitored by the scripts are transmitted as SNMP event traps to `edd`. These traps are processed by response action scripts invoked through `edd` when traps are received.
`fad`	Provides distributed file access services to SSP clients that need to monitor, read, and write changes to SSP configuration files. Only readable files listed in `fad_files` can be monitored. This daemon relies on other SSP server daemons, including `machine_server`. Each SSP can run only one instance of `fad` at a time.
`fod`	Monitors the health of dual SSPs and control boards. One control board serves as the primary control board, while another control board serves as a backup. Run only one copy of `fod` on both the main and spare SSP at all times. Note: this daemon is not present in SSP 3.3.
`machine_server`	Performs several functions, including: servicing TCP and UDP port registration requests, processing `netcon_server` and `snmpd` port lookup requests from SSP client programs, and ensuring that error messages are routed to the proper messages file. Each SSP can run only one instance of `machine_server` at a time.

Daemon	Description
scotty	Extends Tcl, an interpretive language much like shell or perl. The scotty extensions handle TCP/IP sockets and SNMP. The SSP further extends scotty with SSP-specific commands. Note: the scotty interface is not available to SSP users.
snmpd	Propagates traps to other SSP daemons such as edd.
straps	Listens to the SNMP trap port for incoming trap messages and forwards received messages to all connected clients. Each SSP can run only one instance of straps at a time.

Solaris OE Defaults and Modifications

The Solaris OE configuration of an SSP has many of the same issues as other default Solaris OE configurations. For example, too many daemons are used and other insecure daemons are enabled by default. Some insecure daemons include: in.telnetd, in.ftpd, fingered, and sadmind. For a complete list of default Solaris OE daemons and security issues associated with them, refer to the *Solaris Operating Environment Security: Updated for Solaris 8 OE* Sun BluePrints OnLine article.

Based on the Solaris OE installation cluster (SUNWCall) typically used for an SSP, almost 100 Solaris OE configuration modifications are recommended to improve the security configuration of the Solaris OE image running on each SSP.

Implementing these modifications is automated when you use the driver script starfire_ssp-secure.driver available in the Solaris Security Toolkit. This new driver is available in version 0.3.5 of the Toolkit.

Disabling Unused Services

We recommend that you disable all unused services. Reducing services offered by an SSP to the network decreases the access points available to an intruder. The modifications to secure an SSP Solaris OE configuration result in reducing the number of TCP, UDP, and RPC services available from an SSP.

The typical hardening of a Solaris OE system involves commenting out all of the services in /etc/inetd.conf and disabling the inetd daemon from starting. All interactive services normally started from inetd are then replaced by secure shell (ssh). Unfortunately, the SSP does not permit you to comment out the entire contents of the /etc/inetd.conf.

Note – A secured configuration must be considered in the context of the application and services provided. The secured configuration implemented in this article is a *high-water mark* for system security; every service not required by the SSP is disabled. Using the information in this article, you can determine clearly what can be disabled without adversely affecting the behavior of the SSP in your environment.

Recommendations and Exceptions

Our recommendations for securing the SSP follow closely with the hardening described in the *Solaris Operating Environment Security - Updated for Solaris 8 Operating Environment* Sun BluePrints OnLine article.

We made the following exceptions to these recommendations, due to functionality that is required by the SSP and due to support constraints:

- Remote procedure call (RPC) system startup script is *not disabled*, because RPC is used by the failover daemon (`fod`).
- Daemon entries `in.rshd`, `in.rlogind`, and `in.rexecd` in the `/etc/inetd.conf` file are *not disabled*, because the failover daemon (`fod`) requires them.
- Solaris Basic Security Module (BSM) is *not enabled*. The BSM subsystem is difficult to optimize for appropriate logging levels and produces log files that are difficult to interpret. This subsystem should only be enabled at sites where you have the expertise and resources to manage the generation and data reconciliation tasks required to use BSM effectively.
- Solaris OE minimization (removing unnecessary Solaris OE packages from the system) is not supported for the SSP.

Mitigating Security Risks of Solaris OE Services

Detailed descriptions of Solaris OE services and recommendations on how to mitigate their security implications are available in the following BluePrint OnLine articles:

- *Solaris Operating Environment Security - Updated for the Solaris 8 Operating Environment*
- *Solaris Operating Environment Network Settings for Security - Updated for Solaris 8*

The recommendations are implemented by the Toolkit in either its standalone or JumpStart modes.

Using Toolkit Scripts to Perform Modifications

Each of the modifications performed by the Toolkit `starfire_ssp-secure`.driver are organized into one of the following categories:

- `Disable`
- `Enable`
- `Install`
- `Remove`
- `Set`
- `Update`

The following paragraphs briefly describe these categories and the modifications the scripts within the driver perform to harden the SSP. For a complete list of the scripts in the `starfire_ssp-secure`.driver, refer to the Toolkit `Drivers` directory.

For more detailed information about what each of the scripts do, refer to the Sun BluePrints OnLine article titled *The Solaris Security Toolkit - Internals - Updated for Version 0.3*.

In addition to these modifications, the Toolkit copies files from the Toolkit distribution to increase the security of the system. These files are system configuration files that change the default behavior of `syslogd`, system network parameters, and other Solaris OE options.

Disable

These scripts disable services on the system. Disabled services include network file system client and server, the automounter, DHCP server, printing services, window manager, and a variety of others. The goal is to disable all services not absolutely required by the system.

A total of 31 disable scripts are in the `starfire_ssp-secure`.driver. These scripts perform modifications to either disable all or some aspect of the following services and configuration files:

`apache`	`ldap_cachemgr`	sendmail
`aspppd`	`lpsched`	slp
`automountd`	`mipagent`	snmpdx
`core generation`	`mountd`	printd
`dhcp`	`nfsd`	syslogd
`snmpXdmid`	`nscd`	smcboot
`dtlogin`	`picld`	
`IPv6`	`pmconfig`	
`keyservd`	`pam.conf`	

Enable

These scripts enable security features that are by default disabled on Solaris OE. These modifications include:

- enable optional logging for `syslogd` and `inetd`
- require any NFS client to use a port below 1024
- enable process accounting
- enable improved sequence number generation [RFC 1948]
- enable optional stack protection and logging

Even though some of these services remain disabled after the modifications, their optional security features are enabled so that if they are used in the future, they are used securely.

Install

The install scripts create new files and install security software. The driver scripts create the following Solaris OE files to enhance the security of the system:

- new `/etc/cron.d/at.allow` file to restrict access to `at` commands
- updates `/etc/ftpusers` file to include all system accounts
- new `/var/adm/loginlog` file to log unsuccessful login attempts
- updates `/etc/shells` file to include all available system shells
- new `/var/adm/sulog` file to log su attempts

In addition to creating files, some install scripts install software on the system. For the SSP, the following software can be installed by the scripts:

- Recommended and Security Patch Cluster software
- FixModes software
- OpenSSH software
- MD5 software

Remove

Only one remove script is in the driver; it removes unused Solaris OE system accounts. The removed accounts are no longer used by the Solaris OE and can safely be removed. The removed accounts are the following:

- `smtp`
- `nuucp`
- `listen`
- `nobody4`

Set

The set scripts configure security features of the Solaris OE that are not enabled by default. There are thirteen of these scripts in the SSP driver and they can configure the following:

- root password
- ftpd banner
- telnetd banner
- ftpd UMASK
- login RETRIES
- power restrictions
- use of SUID on removable media
- system suspend options
- TMPFS size
- user password requirements
- user UMASK

Update

The update scripts update configuration files shipped with the Solaris OE but that do not have all of their security settings properly set. Modifications are made to the following configuration files:

- `at.deny`
- `cron.allow`
- `cron.deny`
- `logchecker`
- `inetd.conf`

Building a Secure Enterprise 10000 System

Building a secure system requires that entry points onto the system be limited and restricted, in addition to limiting how authorized users obtain privileges.

To effectively secure an SSP, changes are required to the Solaris OE software running on the SSP and, to a lesser degree, the Enterprise 10000 system domains.

Properly securing the primary and backup SSP on an Enterprise 10000 system requires the following:

- “Modifying Network Topology” on page 16
- “Installing Main SSP Detection Script” on page 20
- “Adding Security Software” on page 21
- “Creating Domain Administrator Accounts” on page 28

Although *optional*, for those who are administrating sites requiring the most secure configurations, we recommend that you add a host-based firewall on both SSPs. Refer to “Adding Host-Based Firewalls” on page 30.

By performing these procedures there is considerable improvement in the security and domain separation of the Solaris OE images running on SSPs and domains.

Caution – In a dual-SSP environment, do not harden the spare SSP until you have hardened the main SSP and tested it to ensure that it functions properly in your environment.

Modifying Network Topology

Modify the network topology of the SSP management network (recommended and documented in the Enterprise 10000 documentation) to provide separation of each domain to SSP connection.

Note – We recommend that you disable the failover mechanism before hardening the SSPs. Re-enable automated failover only after you harden and test both SSPs.

---

1. **Isolate domains by implementing a separate and private network connection between the SSP and each domain.**

   By providing separate networks for each domain, you make it impossible for a rouge domain user to use the SSP management network to attack other domains.

Note – If some of the domains are in the same security zone and connected on the public-side network already, then you might not need to separate those domains. For example, if two of six domains in an Enterprise 10000 system are application servers providing the same services on the same network and managed by the same organization, then these systems have the same security exposures and are in the same security zone. You could place these two domains on the same private SSP management network—in a secured configuration—without compromising the security of the environment.

---

2. **Repeat Step 1 for all domains that are present in the Enterprise 10000 system.**

   By implementing these recommendations there is no network connection between multiple domains. Correspondingly, the weakest link is now the SSP and its Solaris OE configuration. (Recommendations on how to mitigate these risks are described later in this article.)

Note – Consolidating many domains into a few security zones and assigning private SSP management networks—based on these security domains—limits the number of separate networks required between the domains and SSPs.

The number of security zones and separate SSP management networks required can impact the hardware used for the SSPs. For example, an Ultra 5 system has three PCI slots: one slot is typically used for a monitor and two slots are available for Sun Quad FastEthernet™ cards, which amounts to nine network ports. These ports can be configured as follows:

- two ports for control boards
- one port for a production network connection
- six ports for private SSP management networks

A Sun Enterprise 250 system has an additional PCI slot, supporting four more private SSP management networks than the Ultra 5 system.

The following sample configuration isolates each domain onto a separate network. This configuration has: two domains, `domain_a` and `domain_b`; two SSPs, ssp_a and ssp_b, and two control boards, `control_board_0` and `control_board_1`. Each domain and SSP has one Sun Quad FastEthernet card. The networks connected to the Sun Quad FastEthernet ports are listed next to each component.

Components	Networks
domain_a	qfe0 - domain_a ssp mngt network - IP Address 192.168.153.115
	qfe1 - production network
	qfe2 - not used
	qfe3 - not used
domain_b	qfe0 - domain_b ssp mngt network IP Address 192.168.154.115
	qfe1 - production network
	qfe2 - not used
	qfe3 - not used
ssp_a	hme0 - control board 0 mngt network - IP Address 192.168.151.113
	qfe0 - control board 1 mngt network - IP Address 192.168.152.113
	qfe1 - domain_a ssp mngt network - IP Address 192.168.153.113
	qfe2 - domain_b ssp mngt network - IP Address 192.168.154.113
	qfe3 - external management network
ssp_b	hme0 - control board 0 mngt network - IP Address 192.168.151.114
	qfe1 - control board 1 mngt network - IP Address 192.168.152.114
	qfe0 - domain_a ssp mngt network - IP Address 192.168.153.114
	qfe2 - domain_b ssp mngt network - IP Address 192.168.154.114

Components	Networks
	qfe3 - external management network
control_board_0	192.168.151.123
control_board_1	192.168.152.123

The following are the network segments for our sample configuration:

- control board 0 mngt network - 192.168.151.0
- control board 1 mngt network - 192.168.152.0
- domain_a ssp mngt network - 192.168.153.0
- domain_b ssp mngt network - 192.168.154.0

These four network segments all use a 24-bit netmask that has an entire Class C IP address space in it. You can subnet the SSP-domain management networks into parts of Class C networks. You must not subnet the SSP domain on the control board networks; subnetting to control board networks is not supported

The following figure illustrates our configuration.

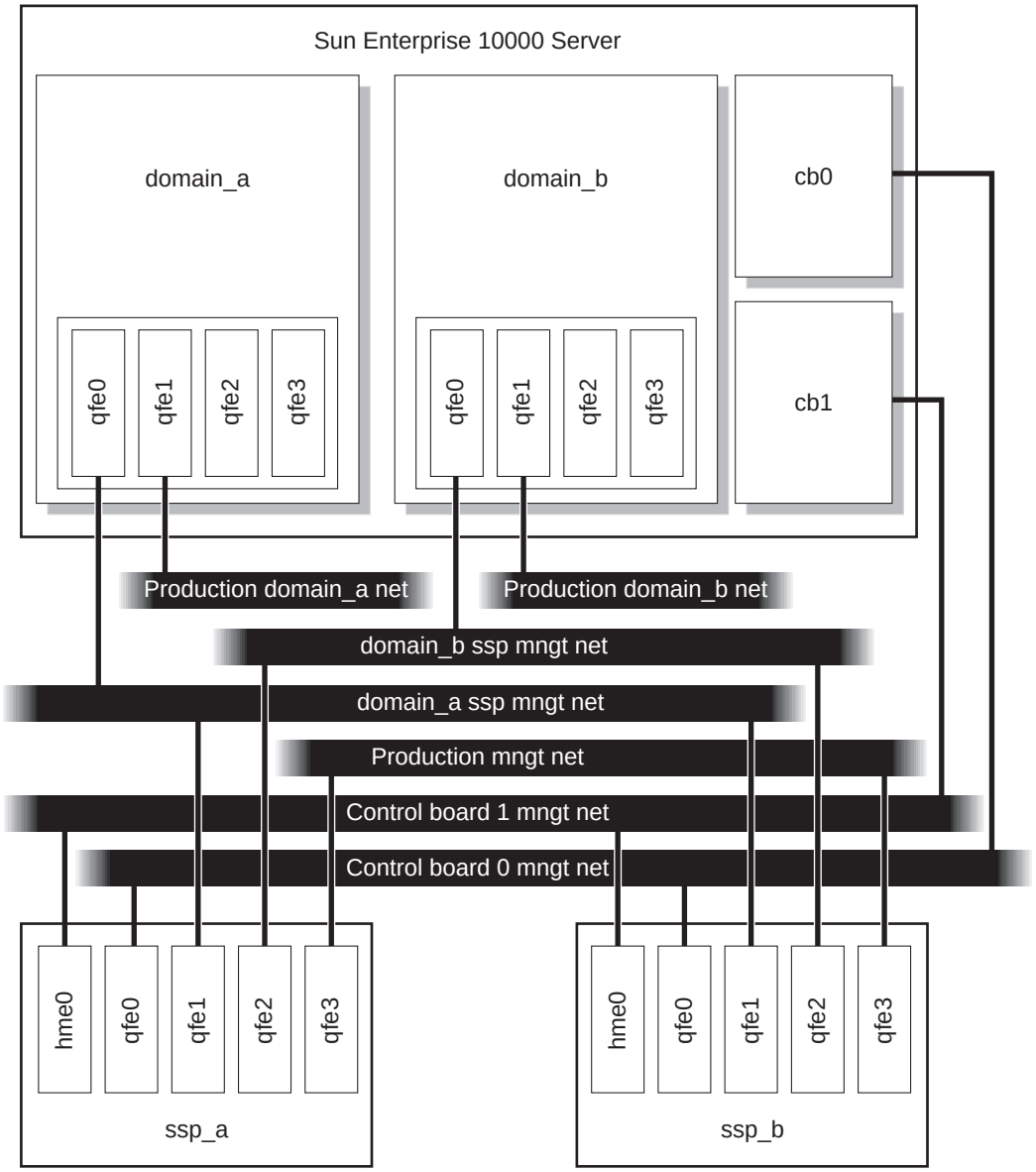

FIGURE 1 Modified Network Topology Sample

Installing Main SSP Detection Script

This script detects the main SSP in a redundant SSP environment. Use it for configurations where a floating SSP name and IP are either not valid or not supported.

The script is required for SSP failover to function properly on SSP versions 3.4 and 3.5. It is not required on SSP version 3.3. Before running the script, some simple preparation work needs to be done on the domains; see the comment section of the script for details.

Caution – Install this script only on a hardened Enterprise 10000 system.

---

1. **Download the script from the Sun BluePrints Tools web site at:**

   `http://www.sun.com/blueprints/tools`

2. **Install the script on each domain of a hardened Enterprise 10000 system.**

Note – This script poses negligible impact on the domain running it.

---

3. **Before running the script, manually edit the file, `/etc/ssphostname`, to contain the resolvable uname of the main SSP.**

4. **Set up a cron job to run the script periodically.**

   We recommend running this script every 3 minutes.

5. **Refer to the `crontab(1)` manual page for additional information on how to create `crontab` entries.**

   The script runs as a `cron` job. No argument is needed. The following is a portion of a sample root `crontab` setting:

```
0 * * * * /find_main_ssp.ksh > /dev/null 2>&1
3 * * * * /find_main_ssp.ksh > /dev/null 2>&1
6 * * * * /find_main_ssp.ksh > /dev/null 2>&1
```

When using this script with host-based firewalls, the SSPs may generate error messages to SYSLOG. We encountered these error messages when testing SunScreen 3.1 software rulesets as the SSP firewall. The SYSLOG errors generated are similar to the following:

```
Jan 7 14:22:34 xf4-ssp2 SSP Startup : [ID 702911 local0.info]
Error: Failed to receive acknowledgement from cb xf4-cb0
Jan 7 14:22:34 xf4-ssp2 SSP Startup : [ID 702911 local0.info]
Error: Failed to receive acknowledgement from cb xf4-cb1
```

If you encounter these error messages, they can be ignored. The root cause of the errors is the SunScreen 3.1 software; there is no apparent failure of the SSP or control board network.

Adding Security Software

The next stage in hardening an SSP requires downloading and installing additional software security packages. This section covers the following tasks:

- "Install Toolkit Software" on page 22
- "Download Recommended Patch Software" on page 22
- "Download FixModes Software" on page 24
- "Download OpenSSH Software" on page 24
- "Download MD5 Software" on page 25

Note – Of the software described in this section, the Solaris Security Toolkit, Recommended and Security Patch Cluster, FixModes, and MD5 software are required. Instead of OpenSSH, you can substitute a commercial version of SSH, available from a variety of vendors. You must install an SSH product on the SSP.

Install Toolkit Software

The Toolkit version 0.3.5 software must be downloaded first, then installed on the SSP. Later, you'll use the Toolkit to automate installing other security software and implementing the Solaris OE modifications for hardening an Enterprise 10000 system.

The primary function of the Toolkit is to automate and simplify building secured Solaris OE systems based on the recommendations contained in this and other security-related Sun BluePrints OnLine articles.

Note – The following instructions use filenames that are correct only for version 0.3.5 of the Toolkit.

---

1. **Download the source file (**`SUNWjass-0.3.5.pkg.Z`**) from the following web site**:

   `http://www.sun.com/security/jass`

2. **Extract the source file into a directory on the server using the** `uncompress` **command**:

```
# uncompress SUNWjass-0.3.5.pkg.Z
```

3. **Install the Toolkit onto the server using the** `pkgadd` **command**:

```
# pkgadd -d SUNWjass-0.3.5.pkg SUNWjass
```

Executing this command creates the `SUNWjass` subdirectory in `/opt`. This subdirectory contains all Toolkit directories and associated files. The script `make-pkg`—included in Toolkit releases since version 0.3—allows administrators to create custom packages using a different installation directory.

Download Recommended Patch Software

Patches are regularly released by Sun to provide Solaris OE fixes for performance, stability, functionality, and security. It is critical to the security of a system that the most up-to-date patch is installed. To ensure that the latest Solaris OE Recommended and Security Patch is installed on the SSP, this section describes how to download the latest patch cluster.

Downloading the latest patch cluster does not require a SunSolve^{SM} program support contract.

Note – Apply standard best practices to all patch installations. Before installing any patches, evaluate and test them on non-production systems or during scheduled maintenance windows.

1. **Download the latest patch from the SunSolve Online™ web site at:**

   `http://sunsolve.sun.com`

2. **Click on the "Patches" link, at the top of the left navigation bar.**

3. **Select the appropriate Solaris OE version in the "Recommended Solaris Patch Clusters" box.**

   In our example, we select Solaris 8 OE.

4. **Select the best download option, either HTTP or FTP, with the associated radio button, then click "Go."**

   A "Save As" dialog box is displayed in your browser window.

5. **Save the file locally.**

6. **Move the file securely to the SSP with the `ftp` command.**

7. **Move the file to the `/opt/SUNWjass/Patches` directory and uncompress it as follows:**

```
# cd /opt/SUNWjass/Patches
# mv /var/tmp/8_Recommended.zip .
# unzip 8_Recommended.zip
Archive:  8_Recommended.zip
   creating: 8_Recommended/
  inflating: 8_Recommended/CLUSTER_README
  inflating: 8_Recommended/copyright
  inflating: 8_Recommended/install_cluster
[. . .]
```

Later, using the Toolkit, you'll install the patch after downloading all the other security packages.

Note – If you do not place the *Recommended and Security Patches* software into the `/opt/SUNWjass/Patches` directory, a warning message displays when you execute the Toolkit.

Download FixModes Software

FixModes is a software package that tightens the default Solaris OE directory and file permissions. Tightening these permissions can significantly improve overall security of the SSP. More restrictive permissions make it even more difficult for malicious users to gain privileges on a system.

1. **Download the FixModes pre-compiled binaries from:**

   `http://www.Sun.COM/blueprints/tools/FixModes_license.html`

   The FixModes software is distributed as a precompiled and compressed `tar` file formatted for SPARC-based systems. The file name is `FixModes.tar.Z`.

2. **Save the file, `FixModes.tar.Z`, in the Solaris Security Toolkit `Packages` directory in `/opt/SUNWjass/Packages`.**

Caution – Leave the file in its compressed state.

Later, using the Toolkit, you'll install the FixModes software after downloading all the other security packages.

Download OpenSSH Software

In any secured environment, the use of encryption in combination with strong authentication is required to protect user-interactive sessions. At a minimum, user interactive sessions must be encrypted.

The tool most commonly used to implement encryption Secure Shell (SSH) software, whether a commercial or open source (freeware) version. To implement all the security modifications performed by the Toolkit and recommended in this article, you must implement a SSH software product.

Note – When hardening an SSP running Solaris 9 OE, do not download or install OpenSSH. The SSH functionality is included with the OS; use it instead of OpenSSH.

The Toolkit disables all non-encrypted user-interactive services and daemons on the system, in particular daemons such as `in.rshd`, `in.telnetd`, and `in.ftpd`. Access to the system can be gained with SSH similarly to what is provided by RSH, TELNET, and FTP.

Note – If you choose to use an SSH product other than OpenSSH, install and configure it before or during a Toolkit run.

- **Obtain the following online article and use the instructions in the article for downloading the software.**

  A Sun BluePrints OnLine article about how to compile and deploy OpenSSH titled: *Building and Deploying OpenSSH on the Solaris Operating Environment* is available at:

  ```
  http://www.sun.com/blueprints/0701/openSSH.pdf
  ```

  Later, using the Toolkit, you'll install the OpenSSH software after downloading all the other security packages.

Caution – Do not compile OpenSSH on the SSP and do not install the compilers on the SSP. Use a separate Solaris OE system—running the same Solaris OE version, architecture, and mode (i.e., Solaris 8 OE, sun4u, and 64 bit)—to compile OpenSSH. If you implement a commercial version of SSH, then no compiling is required.

Download `MD5` Software

The MD5 software validates MD5 digital fingerprints on the SSP. Validating the integrity of Solaris OE binaries provides a robust mechanism to detect system binaries that are altered or *trojaned* (hidden inside something that appears safe) by unauthorized users. By modifying system binaries, attackers provide themselves with back-door access onto a system; they hide their presence and cause systems to operate in unstable manners.

To install the MD5 program (Intel and SPARC Architectures), follow these steps:

1. **Download the MD5 binaries from** `http://www.sun.com/blueprints/tools/md5_license.html`

   The MD5 programs are distributed as a compressed tar file.

2. **Save the downloaded file,** `md5.tar.Z`**, to the Solaris Security Toolkit** `Packages` **directory in** `/opt/SUNWjass/Packages`

Note – Do not uncompress the tar archive.

Later, when you execute the Solaris Security Toolkit software, the MD5 software is installed.

After the MD5 binaries are installed, you can use them to verify the integrity of executables on the system through the Solaris Fingerprint Database. More information on the Solaris Fingerprint Database is available in the Sun BluePrints OnLine article titled *The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files*:

```
http://www.sun.com/blueprints/0501/Fingerprint.pdf
```

3. **(Optional) Download and install Solaris Fingerprint Database Companion and Solaris Fingerprint Database Sidekick software from the SunSolve Online web site at:**

   ```
   http://sunsolve.sun.com
   ```

   We strongly recommend that you install these optional tools, and use them with the MD5 software. These tools simplify the process of validating system binaries against the database of MD5 checksums. Use these tools frequently to validate the integrity of the Solaris OE binaries and files on the main and spare SSPs.

   These tools are described in the same *The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files* article mentioned previously.

Install Downloaded Software and Implement Modifications

The Solaris Security Toolkit version 0.3.5 provides a driver (`starfire_ssp-secure.driver`) for automating the installation of security software and Solaris OE modifications. The driver for the Enterprise 10000 SSPs performs the following tasks:

- installs and executes the FixModes software to tighten filesystem permission
- installs the `MD5` software
- installs the Recommended and Security Patch software
- implements almost 100 Solaris OE security modifications for the Enterprise 10000 system

The Toolkit focuses on Solaris OE security modifications to harden and minimize a system. *Hardening* means modifying Solaris OE configurations to improve the security of the system. *Minimization* means removing unnecessary Solaris OE packages from the system, thus reducing the components that must be patched and made secure. Reducing components potentially reduces entry points to an intruder. However, minimization is not addressed, recommended, or supported on Enterprise 10000 SSPs at this time.

Note – During the installation and modifications implemented in this section, all non-encrypted access mechanisms to the SSP —such as TELNET, RSH, and FTP—are disabled. The hardening steps do not disable console serial access over SSP serial ports.

- **Execute the** `starfire_ssp-secure.driver` **script as follows:**

```
# cd /opt/SUNWjass
# ./jass-execute -d starfire_ssp-secure.driver
./jass-execute: NOTICE: Executing driver,
starfire_ssp-secure.driver

============================================================
starfire_ssp-secure.driver: Driver started.
============================================================
[...]
```

To view the contents of the driver file and obtain information about the Solaris OE modifications, refer to the Solaris Security Toolkit documentation available either in the `/opt/SUNWjass/Documentation` directory or through the web at:

`http:/www.sun.com/security/jass`

For information about other scripts in the Toolkit, refer to the Sun BluePrints OnLine article titled *Solaris Security Toolkit Internals: Updated for Version 0.3*.

Each Solaris Security Toolkit run creates a run directory in `/var/opt/SUNWjass/run`. The names of these directories are based on the date and time the run is initiated. In addition to displaying the output to the console, the Toolkit creates a log file in the `/var/opt/SUNWjass/run` directory.

Note – Do not modify the contents of the `/var/opt/SUNWjass/run` directories under any circumstances. Modifying the files can corrupt the contents and cause unexpected errors when you use Solaris Security Toolkit features such as `undo`.

The files stored in the `/var/opt/SUNWjass/run` directory track modifications performed on the system and enable the `jass-execute` undo feature. You can undo arun, or series of runs, with the jass-execute -u command. For example, on a system where two separate Toolkit runs are performed, you could undo them by using the following command:

```
# pwd
/opt/SUNWjass
# ./jass-execute -u
Please select from one of these backups to restore to
1. September 25, 2001 at 06:28:12 (/var/opt/SUNWjass/run/
20010925062812)
2. April 10, 2001 at 19:04:36 (/var/opt/SUNWjass/run/
20010410190436)
3. Restore from all of them
Choice? 3
./jass-execute: NOTICE: Restoring to previous run
//var/opt/SUNWjass/run/20010410190436

============================================================
undo.driver: Driver started.
============================================================
[...]
```

Refer to the Toolkit documentation for details on the capabilities and options available in the `jass-execute` command.

Now that all the software is installed—including an alternative administrator access mechanism with either OpenSSH or SSH—the Solaris OE image running on the Enterprise 10000 SSP can be secured.

Creating Domain Administrator Accounts

The default SSP configuration provides SSP administrators with root privileges to all Enterprise 10000 domains through the SSP administration role. In secured environments, and particularly in those organizations where different administrators are responsible for different domains, it is beneficial to have a separate and more restrictive account. This account is referred to as the domain administrator. Create domain administrator accounts to establish restricted domain administrator accounts on each SSP.

Domain administrators use these accounts to access the console and any other SSP domain-specific functionality for a domain by logging into the appropriate account as a domain administrator.

1. **For each domain, create a shell script called** `domain_console` **in the directory**:

   `/var/opt/SUNWssp/adm/<`*`domain_a`*`>`

   where *`domain_a`* is the name of domain running on the Enterprise 10000 system.

2. **Create a shell script for each domain that supports the restricted shells.**

   a. **Assign permission mode 0555.**

   b. **Designate ownership as root of group root.**

   c. **Include the following in the script**:

```
#!/bin/sh

setenv SUNW_HOSTNAME <domain_a>
source /export/home/ssp/.cshrc
/opt/SUNWssp/bin/netcon_wrapper
```

3. **Set the permissions and user/group ownerships with the following command**:

```
# chown root:root /var/opt/SUNWssp/adm/<domain_a>
# chmod 0555 /var/opt/SUNWssp/adm/<domain_a>
```

4. **For each domain, create a domain administrator account with the following command**:

```
# useradd -m <domadma> -u 12 -g 10 -s /var/opt/SUNWssp/adm/
<domain_a>
```

   where *`domadma`* is the account name.

5. **For each account, first set, then expire, the password using the following commands**:

```
# passwd <domain_a>
New password:
Re-enter new password:
passwd (SYSTEM): passwd successfully changed for root
# passwd -f <domadma>
```

   This step ensures that the administrator has to enter a new password immediately after logging into the account for the first time.

Note – The examples use *domain_a* as the domain name and *domadma* as the account name. Use unique user ids (uid) for each account as well.

6. **Repeat Step 1 through Step 5 for each domain on the Enterprise 10000 system.**

Adding Host-Based Firewalls

For some environments, you might want to implement host-based firewalls on the Enterprise 10000 SSPs. Host-based firewalls control a systems network access to protect against malicious misuse. These firewalls provide another layer of protection for the SSP against network-based attacks.

Based on the recommendations made up to this point—network separation, addition of security tools, and hardening of the SSP—the SSP management environment is now considerably more secure than the default configuration and any previously available and supported configuration.

For customers requiring the most-secure and best-instrumented configuration, we recommend installing and implementing host-based firewall software on the SSPs. The goal of this recommendation is to provide additional controls to the services that must be run on the SSPs.

The following information provides an example of how to install a host-based firewall on the SSP. Choose a firewall software product that best fits your environment. Additionally, adapt the rule sets to fit the firewall product you choose.

Note – When using the Automated Main SSP Detection script with host-based firewalls, the SSPs may generate false error messages to SYSLOG. We encountered these error messages when testing SunScreen 3.1 software rulesets and determined that the messages can be ignored.

Using SunScreen Software Version 3.1

For example purposes, we test a SunScreen 3.1 software configuration and recommend rulesets. For more information about SunScreen 3.1 software—including debugging tips and how to manage a firewall from its command line interface—refer to the Sun BluePrints *Securing Systems with Host-Based Firewalls - Implemented With SunScreen Lite 3.1 Software* at:

```
http://sun.com/blueprints/0901/sunscreenlite.pdf
```

Our configuration is based on a two-domain Enterprise 10000 system. The firewall software allows traffic to flow freely between the SSPs and the domains on any management segment.

Only certain traffic is allowed to originate from the domain destined for the SSPs. This traffic is SYSLOG and the failover check traffic. All other traffic from the domain to the SSP is not permitted—including administrative access to SSH on the SSP.

The only access to the Secure Shell daemons running on the SSPs is over the production network segments connected to the SSPs. Secure Shell is the only one permitted to access the SSP over these production network segments. No other protocols may access the SSPs. Of course, the SSPs can request information as appropriate.

Establishing Rulesets

In our sample configuration, we propose rulesets that are point-to-point for all authorized systems. Because the rulesets explicitly define the source and destination of each permitted data stream, unauthorized IP addresses are not able to communicate with any of the authorized devices.

The following table lists rulesets that correspond to `ssp_a` (shown in FIGURE 1 on page 19). Modifications are required before deploying them on `ssp_b`.

TABLE 1 Rulesets for `ssp_a` Domain

Action	Source	Destination
`deny`	`all from *`	`to *`
`allow all IP`	`from ssp_a cb0_mngt_network IP addresses`	`to ssp_b cb0_mngt_network IP addresses`
`allow all IP`	`from ssp_b cb0_mngt_network IP addresses`	`to ssp_a cb0_mngt_network IP addresses`
`allow all IP`	`from ssp_b cb1_mngt_network IP addresses`	`to ssp_a cb1_mngt_network IP addresses`
`allow all IP`	`from ssp_a and ssp_b IP addresses`	`on cb_0_mngt_net to cb0 IP address`
`allow all IP`	`from ssp_a and ssp_b IP addresses`	`on cb_1_mngt_net to cb1 IP address`

TABLE 1 Rulesets for ssp_a Domain *(Continued)*

Action	Source	Destination
allow all IP	from cb_0 IP address on cb_0_mngt_net on cb1_mngt_network	to ssp_a and ssp_b IP addresses
allow all IP	from cb_0 IP address on cb_1_mngt_net	to ssp_a and ssp_b IP addresses
allow TCP port 442	from ssp_a and ssp_b IP addresses on domain_a_ssp_mngt_network	to domain_a IP address
allow TCP port 442	from ssp_a and ssp_b IP addresses	on domain_b_ssp_mngt_network to domain_b IP address
allow all RCP/ Portmapper	from domain_a IP address	on cb0_mngt_network to ssp_a and ssp_b IP addresses
allow all RCP/ Portmapper	from domain_b IP address	on cb0_mngt_network to ssp_a and ssp_b IP addresses
allow all RCP/ Portmapper	from domain_a IP address	on cb1_mngt_network to ssp_a and ssp_b IP addresses
allow all RCP/ Portmapper	from domain_b IP address	to ssp_a and ssp_b IP addresses
allow all RCP/ Portmapper	from ssp_a and ssp_b IP addresses on cb0_mngt_network	to domain_a IP address
allow all RCP/ Portmapper	from ssp_a and ssp_b IP addresses on cb0_mngt_network	to domain_b IP address
allow all RCP/ Portmapper	from ssp_a and ssp_b IP addresses on cb1_mngt_network	to domain_a IP address
allow all RCP/ Portmapper	from ssp_a and ssp_b IP addresses on cb1_mngt_network	to domain_b IP address
allow SYSLOG	from domain_a IP address on domain_a_mngt_network	to ssp_a and ssp_b IP addresses
allow SYSLOG	from domain_b IP address on domain_a_mngt_network	to ssp_a and ssp_b IP addresses

TABLE 1 Rulesets for ssp_a Domain *(Continued)*

Action	Source	Destination
allow SYSLOG	from domain_a IP address on domain_b_mngt_network	to ssp_a and ssp_b IP addresses
allow SYSLOG	from domain_b IP address on domain_b_mngt_network	to ssp_a and ssp_b IP addresses
allow SSH	from *	to production_mngt_network IP addresses of SSPs
allow TCP port 111	from ssp_a and ssp_b IP addresses on domain_a_ssp_mngt_network	to domain_a IP addresses
allow TCP port 111	from ssp_a and ssp_b IP addresses on domain_b_ssp_mngt_network	to domain_b IP addresses
allow TCP port 111	from domain_a IP addresses	to ssp_a and ssp_b IP addresses on domain_a_ssp_mngt_network
allow TCP port 111	from domain_b IP addresses	to ssp_a and ssp_b IP addresses on domain_b_ssp_mngt_netw
allow TCP port 665	from ssp_a and ssp_b IP addresses on domain_a_ssp_mngt_network	to domain_a IP addresses
allow TCP port 665	from ssp_a and ssp_b IP addresses on domain_b_ssp_mngt_network	to domain_b IP addresses

Denying Protocols and Services on Management Networks

The proposed firewall rulesets deny many of the protocols that may have been used to manage SSPs, including some domain installation capabilities from the SSPs.

The following services are denied: TELNET, FTP, remote X display, R* services, and all user-interactive administrative type access over the SSP management networks.

Denying these services enforces domain separation in the architecture. The only user-interactive protocol permitted to access the SSPs is Secure Shell, from the production network connected to the SSPs.

Although the SSPs are permitted to send any protocol to the domains, some services require an additional firewall rule such as FTP. For FTP to function properly, the domains must be allowed to open a high-port connection back to the SSPs. This connection represents a serious risk to the security of the SSP management network and is strongly discouraged. We recommend using alternatives such as Secure Shells version 2, FTP mode, or FTP in PASV mode.

We disable the use of JumpStart™ software from the SSPs to install an OS on a domain.

Internet Control Message Protocols (ICMP) messages are not permitted within the management network, which means that commands such as `ping` would not be allowed. If you need `ping` functionality within the environment, enable it by adding the following rules:

Action	Source	Destination
`allow icmp echo-request / echo-reply`	`from domain_a IP address`	`to SSPs IP addresses`
`allow icmp echo-request / echo-reply`	`from domain_b IP address`	`to SSPs IP addresses`
`allow icmp echo-request / echo-reply`	`from SSPs IP address`	`to domain_a IP addresses`
`allow icmp echo-request / echo-reply`	`from SSPs IP address`	`to domain_b IP addresses`

Simple Mail Transport Protocol (SMTP) on the management network, including the SSPs ability to receive SMTP messages, is disabled.

The use of `traceroute` on the SSP management network is disabled. Normally it would not be expected that this protocol would be used on the SSP management network. Traceroute still works when directed against the production networks attached to the SSPs and domains.

The use of Network Time Protocol (NTP) over the SSP management networks is disabled. Instead of using the SSP as the NTP master for the domains, we recommend that the domains and the SSP function as an NTP client of a separate NTP time server—with the appropriate stratum classification. Additional information on NTP and how it can be securely configured is available in Sun BluePrints OnLine articles (refer to “Bibliography and Recommended Reading” on page 40).

The use of X-based window managers on the SSPs is disabled. When X-based applications must be run on the SSPs, we strongly recommend that you use the Secure Shell to tunnel the X traffic back to the local desktop. The capability to tunnel is available in UNIX® platform based SSH clients.

The use of Sun Management Center (Sun MC) was also disabled. If Sun MC software is to be used add the following rules functionality within the environment, enable it by allowing UDP traffic to ports 166 on the SSPs and 1161 on the domains from the Sun MC server. Port 1161 is used on the domains as the default port, 161, is already in use.

Verifying SSP Hardening

After performing the procedures in this article to harden an Enterprise 10000 SSP, test the configuration and hardening.

For the example configuration, our testing resulted in the following:

- TCP IPv4 services listed by `netstat` went from 31 to 6
- UDP IPv4 services listed by `netstat` went from 57 to 5

By reducing the number of services available, we reduced exposure points significantly.

Note – We recommend that you disable the failover mechanism before hardening the SSPs. Re-enable failover only after you harden and test both SSPs.

Testing the Main SSP

To implement the hardening procedures you completed for the main SSP, do the following.

1. **Disable the failover mechanism.**
2. **Reboot the SSP.**
3. **Place the hardened SSP in the main SSP role.**
4. **Verify that the SSP takes control of the frame.**
5. **Verify that the SSP controls the platform and functions properly.**
6. **Validate that the number of daemons and services running on the SSP are significantly lower than before hardening.**
7. **After verifying that the main SSP is hardened and functioning properly, perform all of the same procedures in this article (all software installation and hardening processes) on the spare SSP.**
8. **Manually define the newly hardened and tested main SSP as the default main SSP.**

Testing the Spare SSP

After hardening the main SSP, testing it, and manually defining it as the main, harden and test the spare SSP.

Caution – Do not harden the spare SSP until you verify that the hardened main SSP functions properly in your environment.

---

1. **Disable the failover mechanism.**
2. **Reboot the SSP.**
3. **Place the hardened SSP in the spare SSP role.**
4. **Verify that the spare SSP takes control of the frame by becoming the main SSP, and that the spare SSP controls the platform and functions properly.**
5. **Validate that the number of daemons and services running on the SSP are significantly lower than before hardening.**
6. **Enable failover.**

   Enable failover only after you harden and test both SSPs.

Acknowledgements

Many thanks to everyone who help develop and test the configurations documented in this article. Without the help of Jason Beloro, Dina Kurktchi, Ray Ng, Ken Yan, and Meng Zhang this could never have been published as a Sun supported configuration.

About the Author

Alex Noordergraaf has over 10 years experience in the area of Computer and Network Security. As a Senior Staff Engineer in the Enterprise Engineering group of Sun Microsystems, he is developing, documenting, and publishing security Best Practices through the Sun BluePrints OnLine program. Published article topics include: Sun Fire Midframe System Controller security, secure N-Tier environments, Solaris OE Minimization, Solaris OE Network Settings, and Solaris OE Security. In addition he co-authored the recently published book *Jumpstart Technology- Effective Use in the Solaris Operating Environment*. Alex is one of the authors of the very popular freeware *Solaris Security Toolkit* (JASS).

Prior to his role in Enterprise Engineering he was a Senior Security Architect with Sun Professional Services where he worked with many Fortune 500 companies on projects that included Security Assessments, Architecture Development, Architectural Reviews, and Policy / Procedure review and development. In addition to providing billable services to customers, he developed and delivered an Enterprise Security Assessment methodology and training curriculum to be used worldwide by SunPS. His customers have included major telecommunication firms, financial institutions, ISPs, and ASPs.

Sample SunScreen Software Configuration File

The following sample illustrates the SunScreen 3.1 software configuration we used to test the recommendations and processes covered in this article.

CODE EXAMPLE 1 Master SunScreen Software Configuration File

```
# Master SunScreen configuration file (used on ssp_a only)
# SSP host network interface definitions
add address "ssp_a-hme0" HOST 192.168.151.113
add address "ssp_a-qfe0" HOST 192.168.152.113
add address "ssp_a-qfe1" HOST 192.168.153.113
add address "ssp_a-qfe2" HOST 192.168.154.113
add address "ssp_a-qfe3" HOST 192.168.96.121
add address "ssp_b-hme0" HOST 192.168.151.114
add address "ssp_b-qfe0" HOST 192.168.152.114
add address "ssp_b-qfe1" HOST 192.168.153.114
add address "ssp_b-qfe2" HOST 192.168.154.114
add address "ssp_b-qfe3" HOST 192.168.96.115
add address "cb0" HOST 192.168.151.123
add address "cb1" HOST 192.168.152.123
# UE10000 domain host definitions
add address "domain_a" HOST 192.168.153.115
add address "domain_b" HOST 192.168.154.115
# group definitions
add address "all-domains" GROUP { "domain_a" "domain_b" }
add address "all-cbs" GROUP { "cb0" "cb1" }
add address "all-ssp_a-cbs" GROUP { "ssp_a-hme0" "ssp_a-qfe0" }
add address "all-ssp_a-domains" GROUP { "ssp_a-qfe1" "ssp_a-qfe2"
}
add address “all_ssp_b-cbs” GROUP { "ssp_b-hme0" "ssp_b-qfe0" }
# Service definition
add service "cmd-term" GROUP "ssh" COMMENT "Command Terminal
Services"
add service "cb-ssp" GROUP "tcp all" "udp all" COMMENT "service
for tcp/udp traffic between SSP and CB"
add service "netcon" SINGLE FORWARD "tcp" PORT 442 COMMENT "service
for tcp port 442: cvc_hostd"
add service “rpc-ssp” GROUP “pmap tcp all” “pmap udp all” “rpc all”
“rpc tcp all” COMMENT “RPC calls between SSP and domain for AP and
DR”
#-- Rule 1-2 allows all traffic between SSPs and CBs
```

CODE EXAMPLE 1 Master SunScreen Software Configuration File *(Continued)*

```
# Master SunScreen configuration file (used on ssp_a only)
add rule “ip all” "all-ssp_a-cbs" "all-cbs" ALLOW
add rule “ip all” "all-cbs" "all-ssp_a-cbs" ALLOW
#-- Rule 3-4 allows all traffic between SSPs over two CB networks
add rule ip all "all-ssp_a-cbs" "ssp_b-cbs" ALLOW
add rule ip all "all-ssp_b-cbs" "ssp_a-cbs" ALLOW
# -- Rule 5-6 allows rpc and portmapper traffic from domains to/
from ssp_a
add rule “rpc-ssp” “all-domains” “all-ssp_a-domains” ALLOW
add rule “rpc-ssp” “all-ssp_a-domains” “all-domains” ALLOW
#-- Rule 7
add rule "netcon" "all-ssp_a-domains" "all-domains" ALLOW
#-- Rule 8
add rule "syslog" "all-domains" "all-ssp_a-domains" ALLOW
#-- Rule 9
add rule "cmd-term" * "ssp_a-qfe3" ALLOW
#-- Rule 10-11(allow ssp_a to ping any system and for ssp_a to be
pinged from domains)
add rule "ping" "ssp_a" * ALLOW
add rule "ping" "all-domains" "ssp_a" ALLOW
```

Bibliography and Recommended Reading

- Deeths, David and Glenn Brunette, *Using NTP to Control and Synchronize System Clocks - Part I: Introduction to NTP*, July 2001
- Deeths, David and Glenn Brunette, *Using NTP to Control and Synchronize System Clocks - Part II: Basic NTP Administration and Architecture*, August 2001
- Deeths, David and Glenn Brunette, *Using NTP to Control and Synchronize System Clocks - Part III: NTP Monitoring and Troubleshooting*, September 2001
- Englund, Martin, *Securing Systems with Host-Based Firewalls - Implemented With SunScreen Lite 3.1 Software*, Sun BluePrints OnLine, September 2001, http://sun.com/blueprints/0901/sunscreenlite.pdf
- Noordergraaf, Alex, *Building Secure N-Tier Environments*, Sun BluePrints OnLine, October 2000, `http://sun.com/blueprints/1000/ntier-security.pdf`
- Noordergraaf, Alex and Brunette, Glenn, *The Solaris Security Toolkit - Quick Start: Updated for version 0.3*, Sun BluePrints OnLine, June 2001, http://sun.com/blueprints/0601/jass_quick_start-v03.pdf
- Noordergraaf, Alex and Watson, Keith, *Solaris Operating Environment Security: Updated for the Solaris 8 Operating Environment*, Sun BluePrints OnLine, April 2001, http://sun.com/blueprints/0401/security-updt1.pdf
- Reid, Jason M and Watson, Keith *Building and Deploying OpenSSH in the Solaris Operating Environment*, Sun BluePrints OnLine, July 2001, http://sun.com/blueprints/0701/openSSH.pdf
- *Sun Enterprise 10000 SSP 3.5 Installation Guide and Release Notes* (806-7615-10) http://docs.sun.com
- *Sun Enterprise 10000 SSP 3.5 User Guide* (806-7613-10) http://docs.sun.com/
- *Sun Enterprise 10000 SSP 3.5 Reference Manual* (806-7614-10) http://docs.sun.com/
- *SunScreen 3.1 Reference Manual* (806-4128) http://docs.sun.com/
- Watson, Keith and Noordergraaf, Alex, *Solaris Operating Environment Network Settings for Security: Updated for the Solaris 8 Operating Environment*, Sun BluePrints OnLine, December 2000, http://sun.com/blueprints/0401/network-updt1.pdf