Sun Fire™ B10p SSL Proxy Blade Version 1.1 Product Notes

Sun Microsystems, Inc.
www.sun.com

Part No. 817-7322-10
September 2004, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Please
Recycle

Contents

Sun Fire B10p SSL Proxy Blade Version 1.1 Product Notes

This document contains important information about the Sun Fire™ B10p software. This document also covers the Sun Fire™ B10n content load balancing blade application software update P1.2, and supplements the *Sun Fire B10p SSL Proxy Blade Administration Guide* (Part Number 817-0826-11).

Note – The current Sun Fire B10p SSL proxy blades are shipped with the Version 1.0 software. This document explains how to upgrade your software to the latest version.

Refer to the latest issues of the Sun Fire™ Blade Application Journals for further configuration and architectural overiew information. The Application Journal is available at: `http://www.sun.com/blades/`

Viewing the Latest Product Notes

Additional issues may arise after the publication of this version of the product notes. For the latest information, refer to the latest version of this document available at:

`http://wwws.sun.com/products-n-solutions/hardware/docs/Servers/Workgroup_Servers/Sun_Fire_Blade_Platform/Sun_Fire_b100s/index.html`

Software Release Features

New Features Supported in Version 1.1

The Sun Fire B10p SSL proxy blade does not have operating system dependencies. However, other devices required by the SSL proxy blade do have operating system requirements. VLANs are supported and optional on all operating systems supported by the required devices except for Red Hat Enterprise Linux AS 2.1. TABLE 1 lists the VLAN support and the supported operating systems for the required Sun Fire B100s and B100x server blades.

TABLE 1 Supported Operating Systems

Operating System	Version	Hardware	VLAN Support
Solaris	8 HW 12/02	SF B100s /SPARC	VLANs supported and optional
Solaris	8 HW 5/03	SF B100s /SPARC	VLANs supported and optional
Solaris	8 HW 7/03	SF B100s /SPARC	VLANs supported and optional
Solaris	9 8/03	SF B100s /SPARC	VLANs supported and optional
Solaris	9 12/03	SF B100s /SPARC	VLANs supported and optional
Red Hat Enterprise Linux	AS 2.1	SF B100x /x86	No VLAN support

Features Introduced in Version 1.0.2

The Sun Fire B10p SSL proxy blade application software release 1.0.2 adds support for no VLAN mode for sites that choose not to use VLANs within the Sun Fire B1600 blade platform.

VLAN Operation

The use of VLANs within the Sun Fire B1600 blade system is preferred when using the Sun Fire B10p SSL proxy blade. VLANs are configured at the SSC switches to create logical groups of endpoints that can communicate as if they were on the same LAN. VLANs also prevent or restrict traffic between endpoints on separate VLANs. However, some environments might not support VLANs. To disable VLAN operation for the Sun Fire B10p SSL proxy blade, use the `set vlan filter disable` command from the CLI interface.

Note – Disabling the VLAN filter clears all of the VLAN tags that are currently set. You must reset all VLAN tags if you decide to enable the VLAN filter after it was disabled. This will change in a future release.

```
CLI# set vlan filter disable
```

You cannot set a non-zero VLAN tag for client, inband, or management if the VLAN filter is disabled.

```
CLI# set vlan client 10
Can't set vlan tag while vlan filter is disabled.
CLI# set vlan inband 1 10
Can't set vlan tag while vlan filter is disabled.
CLI# set vlan management 1 3
Can't set vlan tag while vlan filter is disabled.
```

Enabling the VLAN filter allows you to set nonzero VLAN tags.

```
CLI# set vlan filter enable
CLI# set vlan client 10
CLI# set vlan inband 1 10
CLI# set vlan management 1 3
CLI# show vlan filter
    vlan filter enabled: enabled
CLI# show vlan client
    client vlan:      10
```

Operation in a Sun Fire B10n Content Load Balancing Blade Failover Environment

If the Sun Fire B10p SSL proxy blade is being used in a Sun Fire B10n content load balancing setup with failover, then the following configuration on the Sun Fire B10p SSL proxy blade is required for `router inbound IP address`. This configuration enables the Sun Fire B10p SSL proxy blade to continue processing SSL requests when one Sun Fire B10n content load balancing blade fails over to another.

Note – The Sun Fire B10n content load balancing blades must be set up correctly for failover operation. Refer to the *Sun Fire B10n Content Load Balancing Administration Guide* for detailed information.

```
CLI# set routed
Enter port number (1..2) (1):
Enter router inbound IP address (0.0.0.0): 0.0.0.0
Enter primary router outbound IP address (0.0.0.0): router's-IP-address
Enter secondary router outbound IP address (0.0.0.0):
CLI#
```

Updating the Software and Firmware

Before you setup and configure the Sun Fire B10p SSL proxy blade you need to ensure you have the latest software and firmware for the SSL proxy blade, the B10n content load balancing blade, and the Sun Fire™ B1600 blade system chassis. The minimum versions are listed in TABLE 2.

The latest software and firmware versions can be downloaded from:

`http://wwws.sun.com/software/download/network.html`

Hardware and Software Requirements

Before using the Sun Fire B10p blade, make sure your system meets the following hardware and software requirements.

TABLE 2 Hardware and Software Requirements

Hardware and Software	Requirements
Hardware	• Sun Fire B10p SSL proxy blade • Sun Fire B10n content load balancing blade (at least one Sun Fire B10n blade for every four SSL proxy blades) • Sun Fire B1600 blade system chassis and other horizontally scaled Sun platforms • Sun Fire B100s blade server for SPARC or Sun Fire B100x blade server for x86
Software	• Sun Fire B10p application software 1.0.2 (1.872) or subsequent compatible version • Sun Fire B10p BSC firmware v5.1.0-SUNW* or subsequent compatible version • Sun Fire B10n application software 1.1.3 or subsequent compatible version • Sun Fire B10n BSC firmware v5.1.4 or subsequent compatible version • Sun Fire B100s blade server Solaris Operating System versions: Solaris 8 HW 12/02 Solaris 8 HW 5/03 Solaris 8 HW 7/03 Solaris 9 8/03 Solaris 9 12/03 • Sun Fire B100x blade server Linux operating system version: Red Hat Enterprise Linux AS 2.1 • Sun Fire B1600 SC (system controller) 1.2 or subsequent compatible system controller firmware • B10n Solaris server blade module version 1.55 or B10n Linux server blade module version 1.36 (or subsequent compatible versions) for Red Hat Enterprise Linux AS 2.1 • Sun GigaSwift Ethernet Adapter Patch 111883-18 or subsequent compatible patch for supported versions of Solaris 8. Sun GigaSwift Ethernet Adapter Patch 112817-10 or subsequent compatible patch for supported versions of Solaris 9.** • Sun Ethernet VLAN Patch 112119-04 or subsequent compatible patch for supported versions of Solaris 8. Sun Ethernet VLAN Patch 114600-02 or subsequent compatible patch for supported versions of Solaris 9.**

* The version number displayed from the `showsc -v` command from the Sun Fire B1600 SC CLI printout refers to the BSC firmware version. The application software version is observed using the console `show version` command.

** The patch currently installed can be displayed by entering `showrev -p | grep <patch-id without the rev>` for example: `showrev -p | grep 111883`. You can download patches from `http://sunsolve.sun.com`

Checking the Software Versions

▼ To Check the Sun Fire B1600 Software Version

- **Type the `showsc -v` command:**

```
sc> showsc -v
Sun Advanced Lights Out Manager for Blade Servers 1.2
Copyright 2003 Sun Microsystems, Inc. All Rights Reserved.
ALOM-B 1.2

Release: 1.2.6
```

▼ To Check the Sun Fire B10n Content Load Balancing Blade Application Software

- **Type the `console s1` and `show system` commands:**

```
sc> console s1
puma{admin}# show system
Boot Options:
================================================================================
Config Type   Config File   Boot Image         Diag Level   Verbose Mode
--------------------------------------------------------------------------------
running                1   1 (1.2)                  0              0
next                   1   1 (1.2)                  0              0
================================================================================


Image Information Table:
================================================================================
Image   Blade   Image Type      Version      Build Date:Time      Size
--------------------------------------------------------------------------------
1       B10n    Load Balancer   1.2        10/14/03 : 23:16     4035122
2       B10n    Load Balancer   1.1.8        09/29/03 : 14:30     4022705
diag    B10n    Diagnostics     1.2        10/20/03 : 16:55     2410797
================================================================================

Flash FS /RFA0 free space = 17,600,512 bytes
```

▼ To Check the Sun Fire B10p SSL Proxy Blade Application Software Version

- **Type the** `console s2` **and** `show version` **commands:**

```
sc> console s2
CLI# show version
    software version: 1.872
```

▼ To Check any Sun Fire Blade BSC Firmware Version

- **Type the** `showsc -v` **command:**

```
sc> showsc -v
FRU   Software Version                Software Release Date
-------------------------------------------------------------
S0    v5.1.0-SUNW,B10p,SecureBlade1   Jun 16 2003 16:41:38
S6    v5.1.3-SUNW,B10n,NetBlade1      Aug  6 2003 15:43:56
```

Software Architecture

The Sun Fire B10p SSL proxy blade delivers high performance by utilizing optimized hardware engines and a tightly coupled embedded processor running a real time operating system. The code that runs on this processor is called the application software and can be updated using an FTP process.

In addition to the embedded processor, there is a micro controller called the blade support controller (BSC). The BSC is the primary interface to the Sun Fire B1600 service controllers (SCs) and performs the advanced lights out management (ALOM) functions for a given blade. These functions include powering on and off, and the resetting and monitoring functions. The code that runs on this device is called the BSC firmware and can be updated using the `flashupdate` command which involves using TFTP.

The Sun Fire B10p software components are as follows:

- Application software
- BSC firmware

Check the following web site to ensure you have the latest software:

`http://wwws.sun.com/software/download/network.html`

Command-Line and Console Interfaces

There are two types of command-line interfaces when working with blades in a Sun Fire B1600 system. The first type is the system controller or `sc>` interface. The commands for this interface are detailed in the *Sun Fire B1600 Blade System Chassis Software Setup Guide*. You will recognize this interface by the `sc>` prompt.

The second type is the switch interface and is accessed with the `console` command. The individual blades in the chassis are accessed through the `console` command that is entered at the `sc>` prompt, for example:

```
sc> console sn
```

Where *n* is the blade slot you wish to access, for example:

```
sc> console s0
```

Once the blade has been powered on and you are at the blade `console` prompt and have logged into the desired blade, you can administer the commands as outlined, in the *Sun Fire B10p SSL Proxy Blade Administration Guide*. You will recognize this interface by the `CLI#` prompt.

You can return to the `sc>` interface by using the `#.` key sequence. (that is, the hash (#) character followed by the dot (.) character.

Application Software

The Sun Fire B10p SSL proxy blade has the ability to hold three versions of the application software: an active image, a backup image, and a factory image. This capability ensures that you can revert to a safe image of the application software if a problem occurs with the current version or a problem occurs when updating the software. The software images are stored and loaded as follows:

- Active image – Primary image stored in Flash and loaded into RAM on bootup
- Backup image – Secondary image stored in Flash and can be moved to the Active image. This image is over written when a new image is uploaded
- Factory image – Loaded into Flash at time of manufacture. Used in case both Active and Backup images are corrupted.

The typical operations associated with images are:

- Booting – loading the permanent active image into RAM and starting the system (automatic on power up)

- Upgrading – loading a new image as permanent. The backup image and the factory image are protection mechanisms to ensure recovery from failed or undesired upgrades.

There is also a configuration file that holds the configuration data (see the "Configuration Storage" section of the *Sun Fire B10p SSL Proxy Blade Administration Guide*). The operator will be prompted to overwrite the permanent configuration. It is important to backup the configuration of the system prior to the time when new software is uploaded.

FIGURE 1 shows the various images and how various CLI commands alter or copy them.

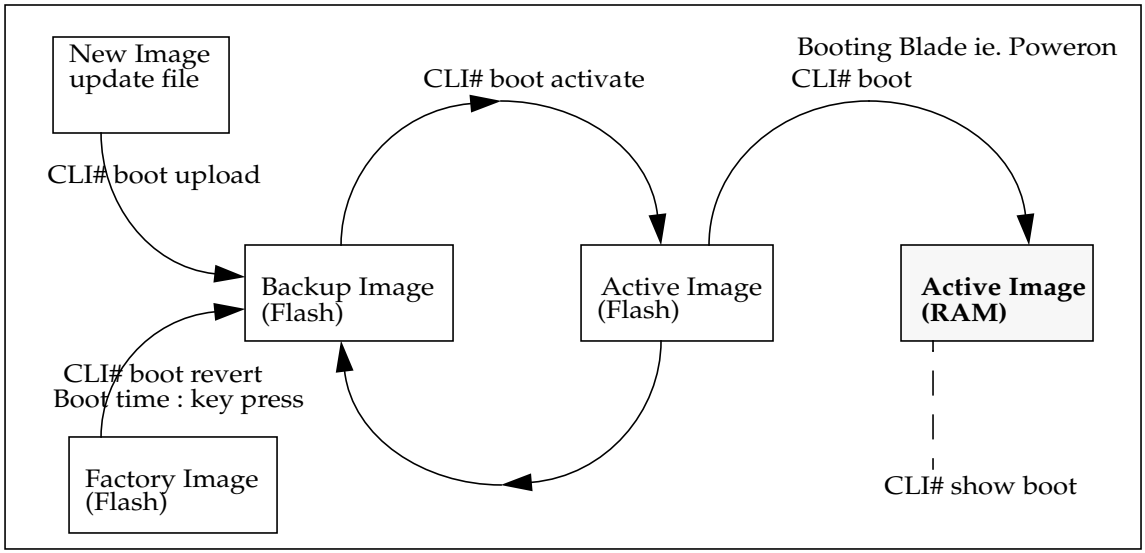

FIGURE 1 SSL Proxy Blade Images and CLI Commands

BSC Firmware

The BSC is the primary interface to the Sun Fire B1600 SCs. There is a single image stored in the micro controller that can be overwritten through the `flashupdate` process. If there is a problem during the BSC `flashupdate` process the recovery is just a matter of repeating the update as the SC software is managing the process.

Updating the Sun Fire B1600 System Controller

Before you install the Sun Fire B10p SSL proxy blade in your Sun Fire B1600 chassis, you must first update the system controller (`sc`) firmware version `SC1.2`. You can download the latest version of the `sc` firmware from Sun's download site:

`http://wwws.sun.com/software/download/network.html`

You need to set up a TFTP boot server to update the `sc` firmware. See the "Setting Up a TFTP Server" section of the *Sun Fire B10p SSL Proxy Blade Administration Guide.*

You can access all the Sun Fire B1600 documentation from the following web site:

`http://www.sun.com/products-n-solutions/hardware/docs/Servers/Workgroup_Servers/Sun_Fire_b100s/index.html`

▼ To Update the System Controller Firmware

1. **At the `sc>` prompt, type the following command:**

```
sc> flashupdate -s install server -f path SSCn/SC.
```

In the following example, 10.4.128.25 is the IP address for your TFTP boot server and `stiletto.1.1/c8/SunFireB1600-sc-v1.1.6.flash` is the path to the file:

```
sc> flashupdate -s 10.4.128.25 -f stiletto.1.1/c8/SunFireB1600-sc-v1.1.6.flash
SSC0/SC
Warning: Are you sure you want to flashupdate the SSC0/SC flash image (y/n)? y
SSC0/SC: Preparing to flashupdate.
flashupdate: erasing segment 36 programming address ffedfffd
SSC0/SC: flashupdate complete.
```

2. **Reset the system using `resetsc` to load the new image.**

Updating the Sun Fire B10n Application Software and BSC Firmware

It is important to verify that you have the latest software for the Sun Fire B10n content load balancing blade. Check the following web site for the latest software and documentation:

```
http://wwws.sun.com/software/download/network.html
```

You need to set up a TFTP boot server to update the BSC firmware. See the "Setting Up a TFTP Server" section of the *Sun Fire B10p SSL Proxy Blade Administration Guide.*

You also need to configure the management IP address and default gateway address. Refer to the "Configuring the Networking" section of the *Sun Fire B10n Content Load Balancing Blade Administration Guide.*

Note – If you are updating both the B10n application software and BSC firmware, be sure to update the B10n application software *first*.

▼ To Update the Sun Fire B10p Application Software

The SSL proxy blade supports the ability to perform network based software upgrades to the device. The software upgrades to the SSL proxy blade are encrypted and authenticated in order to preserve their security. Normal operation of the SSL proxy blade must be stopped during the upgrade process because a reboot is required after activating an upgrade.

Note – Read this section completely before proceeding to perform a software upgrade.

Download the application software to a local FTP/TFTP server before performing the upgrade.

Upgrades are a two step process. First, verify and copy the upgrade package as the backup image of the software. Then activate the new software using the `boot activate` command. This command swaps the active software with the backup, thus making the upgrade active on the next boot.

The upgrade sequence is as follows. You need to login as `so` (security officer) to perform upgrades.

▼ Executing Boot Upload Commands

1. **Use FTP or TFTP to copy the package from the specified FTP or TFTP server.**

   The upgrade package is automatically decrypted and verified for authenticity. The successfully verified package is placed in the backup image location within the SSL proxy blade. An upgrade package can be up to three Megabytes in size and may take up to one minute to copy from a local FTP server. A spinning cursor shows activity during the process.

Note – The FTP/TFTP server IP address must be on the same subnet as the management (admin) IP address of the SSL proxy blade.

- Executing `boot upload` commands using an FTP server:

```
CLI# boot upload
Enter remote file name (520-3440-02.pkcs ): package_name
Enter remote path (releases): directory
Enter remote IP Address: (192.168.0.28): ip-addr
Enter remote user name (labuser): username
Enter remote user password (): password
 starting to load image
 Verification Successful.
 image loaded.
 Type boot activate to install.
```

- Executing `boot upload` commands using a TFTP server:

```
CLI# boot upload-tftp
Enter remote file name (520-3440-02.pkcs ): package_name
Enter remote IP Address: (192.168.0.28): ip-addr
 starting to load image
 Verification Successful.
 image loaded.
 Type boot activate to install.
```

If the upgrade package is not successfully verified, then contact the Sun Microsystems support service to report the problem.

Note – A particular upgrade package may require some additional installation steps. For example, you may need to import a new key. Please read the release notes carefully before performing any upgrade.

2. **Once the upgrade is in the backup location, activate it:**

```
CLI# boot activate
Do you want to overwrite your existing flash.cfg file (Yes/No)? No
*** Warning. Do not turn off the power! ***
activating boot.
image updated.
reboot to run new image.
```

3. **After the upgrade is activated, reboot the SSL proxy blade:**

```
CLI# reboot
```

Verifying the Upgrade

As soon as the upgrade is finished:

- Verify that the SSL proxy blade boots properly
- Perform some basic tests to make sure the SSL proxy blade operates correctly

Reverting to Previous Versions of Software

You can always revert to the previous version of software by upgrading to a previous version. Also, the `boot activate` command will swap the current and backup versions, but this does not swap the boot images. If the upgrade documentation indicates that a new version of the boot image is part of the upgrade, then do not use `boot activate` to revert to the previous version.

Factory Image

The SSL proxy blade has a built in Factory image that guarantees the SSL proxy blade platform is recoverable even if an unbootable image is loaded on it. Because SSL proxy blade software is authenticated, image corruption is extremely unlikely.

Although the Factory image can be used to process SSL traffic, it is intended to provide a safe mode to load the latest available software version for the SSL proxy blade.

The Factory image should be used only if the SSL proxy blade is not booting to a point where new software can be loaded. Before booting from the factory image, connect a serial terminal and reboot to inspect the boot up messages. The boot problem could be associated with some internal hardware malfunction. If this is the case, call support.

To boot from the Factory image, power on the SSL proxy blade and hold the `Esc` key down until prompted for input. When the boot menu is displayed, press `r` to revert to the Factory image. Under normal system operation, the command `boot revert` also reboots from the Factory image.

If the SSL proxy blade loses power during the upgrade process, the Backup image might be corrupted. In this case, it is best to ignore the Backup image and perform the upgrade process again.

Image Commands

The description of each CLI command relevant to software image and booting is given below.

`show version`

Use the `show version` command to display the current version of the software.

- **As any user, enter the `show version` command:**

```
CLI# show version
    software version: 1.872
```

`reboot`

Use the `reboot` command to restart the blade. You will be prompted to save the configuration, if needed. This command resets all connections and reboots the system.

- **As `so`, reboot the device:**

```
CLI# reboot
```

show boot

Use the `show boot` command to display version information for all system software components.

- **As `so` or `admin`, enter the `show boot` command:**

```
CLI# show boot
     versions:
     BBID: 67 CPLD version: 65
     preboot 1863 Oct  1 2003
     boot 1867 Dec  8 2003
     app  1867 Dec  8 2003
     Buff: BUFF3108.GZ
     Mash: MASH1005.GZ

     Active:   BAPP: 1867, BOOT: 1867, MASH: 1005, BUFF: 3108
     Backup:   BAPP: 1866, BOOT: 1866, MASH: 1005, BUFF: 3108
     Required: BAPP: 1867, MASH: 1005, BUFF: 3108, CPLD: 65.22D
```

boot activate

Use the `boot activate` command to activate the backup software version. The current active version is saved as the backup. This command is used after uploading a new software version. There may be a prompt to confirm overwriting the flash configuration (which should have been previously exported). You can also use this command to revert to a backup version.

- **As `so`, enter the `boot activate` command:**

```
CLI# boot activate
Do you want to overwrite your existing flash.cfg file (Yes/No)? Yes
*** Warning. Do not turn off power! ***
activating boot.
image updated.
reboot to run new image.
```

boot revert

Use the `boot revert` command to restore the factory installed software version. This command also clears the flash memory, removing *all* information including configuration, log files, and other information. This command reboots the SSL proxy blade and performs the operation.

- **As** so**, enter the** `boot revert` **command:**

```
CLI# boot revert
This will reformat the system and erase all system files
Are you sure you want to do this (Yes/No)?
```

boot upload

Use the `boot upload` command to load new images of the software using FTP.

- **As** so**, enter the** `boot upload` **command:**

```
CLI# boot upload
Enter remote file name (520-3440-02.pkcs ): filename
Enter remote path (releases):  directory
Enter remote IP Address: (192.168.0.28): ip-addr
Enter remote user name (labuser): username
Enter remote user password (): password
Connecting to 192.168.0.28
starting to load image
Verification Successful.
image loaded.
Type boot activate to install.
```

boot upload-tftp

Use the `boot upload-tftp` command to load new images of the software using TFTP.

- **As** so**, enter the** `boot upload-tftp` **command:**

```
CLI# boot upload-tftp
Enter remote file name (520-3440-02.pkcs ): image_filename
Enter remote IP Address: (192.168.0.28): ip-addr
Connecting to 192.168.0.28
starting to load image
Verification Successful.
image loaded.
Type boot activate to install.
```

▼ To Update the BSC Firmware

1. **Escape to the system controller console:**

```
puma{admin}# #.
```

2. **At the `sc` prompt, check the current version of the BSC firmware:**

```
sc> showsc -v
FRU   Software Version            Software Release Date
-------------------------------------------------------
S0    v5.1.4-SUNW,B10n,NetBlade1  Aug 12 2003 15:31:48
```

3. **At the `sc` prompt, enter the following command:**

```
sc> flashupdate -s TFTP_ip-addr -f filename Sn
```

Updates to the Sun Fire B10p SSL Proxy Blade Administration Guide

Chapter 1, "Product Overview"

In section "Why VLANs are Required for the Sun Fire B10p SSL Proxy Blade" on page 14, replace the first paragraph with the "VLAN Operation" section on page 2 of this document.

Chapter 4, "Setting Up Sun Fire Blades for Load Balancing SSL Traffic"

Add the following section:

Setting Up Sun Fire Blades for Load Balancing SSL Traffic in non-VLAN Mode

This section describes how to set up a Sun Fire B1600 for load balancing SSL traffic with the Sun Fire B10n content load balancing blade and the Sun Fire B10p SSL proxy blades while in non-VLAN mode.

This section includes the following topics:

Setting Up for Load Balancing SSL Traffic

You must configure the following components to load balance SSL traffic:

- Sun Fire B10n content load balancing blade
- Sun Fire B10p SSL proxy blade
- Router
- Server blades
- Clients/External routers

Setting Up the Sun Fire B10n Content Load Balancing Blade

The following limitations apply:

- A maximum of 16 SSL blades can be added for each service.
- A maximum of 128 SSL blade entries can be created on a B10n content load balancing blade.

▼ To Configure the Network Interface on the B10n Content Load Balancing Blade

1. **Set the IP address on interface 0:**

```
puma{admin}# config ip interface 0 ip-addr mask subnet_mask
```

Example:

```
puma{admin}# config ip interface 0 192.50.50.132 mask 255.255.255.0
```

▼ To Configure the SSL Proxy Blade

Note – Refer to Chapter 4, "Command-Line Options" and "Configuring SSL Blade Entries" of the *Sun Fire B10n Content Load Balancing Blade Administration Guide* for detailed descriptions of the commands.

---

1. **Create an SSL blade entry on the B10n content load balancing blade with the following command.**

```
puma{admin}# config ssl name ssl_device_name ip-addr
```

Example:

```
puma{admin}# config ssl name ssl1 192.50.50.205
```

This command creates an SSL blade device name `ssl1`.

Note – The interface IP address must correspond to the one configured on the SSL proxy blade with the `set management` command.

---

2. **Add a port pair to the entry with the `secureport` specified at 443 and the `clearport` specified at 880.**

```
puma{admin}# config ssl port-pair ssl1 secureport 443 clearport 880
```

Note – These values must correspond to the same values specified on the SSL proxy blade with the `set portpair` command.

▼ To Verify the SSL Proxy Blade Configuration on the B10n Content Load Balancing Blade

1. **Display the basic information about all the SSL blades configured on the B10n content load balancing blade:**

```
puma{admin}# show ssl
```

2. **Display detailed information about the SSL proxy blade entry `ssl1`:**

```
puma{admin}# show ssl ssl1
```

▼ To Configure a Layer 7 SSL Service on a B10n Content Load Balancing Blade

1. **Create an SSL service on the B10n content load balancing blade that is load balanced on Layer 7 for the HTTP protocol.**

```
puma{admin}# config service name svc1 vip 110.10.10.1:443:tcp ssl
880 interface 0 lb-layer 7 l7-proto http
```

The previous example shows the service `svc1` is bound to interface 0 and is offered at the VIP 110.10.10.1, port 443 and the TCP protocol. The port specified after the SSL keyword, that is, 880, is the decrypted port.

Note – The VIP specified for the service (110.10.10.1 in this example) must be configured as the server address in the `create service` command on all the SSL proxy blades added to the service. The service port (443 in this example) must correspond to the secure port of the port pair associated to the service on the SSL proxy blade and the decrypted port (880 in this example) must correspond to the clear port of the port pair on the SSL proxy blade.

2. **Configure the default load balancing group of the service with two servers (192.50.50.10, and 192.50.50.11 in this example) and the load balancing scheme specified as weighted round robin.**

```
puma{admin}# config service lb-group default svc1 server 192.50.50.10:0:tcp:2:1
192.50.50.11:0:tcp:3:1 scheme wt-round-robin
```

3. **Add the SSL proxy blade entry `ssl1` to the service in an active mode.**

```
puma{admin}# config service ssl svc1 ssl ssl1:active
```

An SSL service cannot be enabled until one or more SSL entries are added to it using the `config service ssl` command.

4. **Enable the service `svc1` on the B10n content load balancing blade:**

```
puma{admin}# config enable service name svc1
```

5. **Check the service configuration on the B10n content load balancing blade:**

```
puma{admin}# show service svc1
```

Setting Up the SSL Proxy Blade

▼ To Access the SSL Proxy Blade Console

1. **Telnet to the Sun Fire B1600 console.**

```
% telnet sc_ip-addr
```

Where *sc_ip-addr* is the IP address of the Sun Fire B1600.

2. **Get to the SSL proxy blade console:**

```
sc0> console Sn
Login:so
Password:
CLI#
```

Where *n* is the slot number of the SSL proxy blade.

▼ To Set Up the SSL Proxy Blade

1. **Create the key on the SSL proxy blade:**

```
CLI# create key

Enter key name: key1
Enter key strength (1024): 1024
    Key key1 generated.
```

This example creates the key `key1` on the SSL proxy blade.

2. **Use the `show key` command to display all the keys configured on the SSL proxy blade.**

3. **Create a self-signed certificate:**

```
CLI# create certificate

CLI#  create certificate
Enter key name: keyname
Enter country (US): abbreviated_country
Enter state or province (CA): abbreviated_state
Enter locality (Company Town): town_name
Enter common name (www.company-name.com): www1.my-company.com
Enter organization (Company Name): my_company_name
Enter organization unit (Company Unit): department
Enter email address (support@company-name.com): email@company_name.domain
Certificate generated.
```

The previous example creates a certificate using the key `key1`. Use the `show key` command to display the certificate along with the key.

4. **Set the parameters on port 1 for operation of the SSL proxy blade in the `routed` mode .**

```
CLI# set routed

Enter port number (1..2) (1): 1
Enter router inbound IP address (0.0.0.0): 192.50.50.132
Enter primary router outbound IP address (0.0.0.0): 192.100.100.254
Enter secondary router outbound IP address (0.0.0.0): 0.0.0.0
```

The router inbound IP address corresponds to the management IP address configured on the B10n content load balancing blade with the `config ip` command.

5. **Set the inband (data) IP address on port 1 (192.100.100.205 in this example) and the subnet mask (255.255.255.0 in this example):**

```
CLI# set inband

Enter port number (1..2) (1): 1
Enter inband (data) IP Address (0.0.0.0): 192.100.100.205
Enter inband (data) netmask (255.255.255.0): 255.255.255.0
```

Note – This address has to be on the same subnet as the outbound router IP address as configured by the `set routed` command.

---

6. **Set the management parameters on port 1.**

```
CLI# set management

Enter port number (1..2) (1): 1
Enter inband (admin) IP Address (0.0.0.0): 192.50.50.205
Enter inband (admin) netmask (255.255.255.0): 255.255.255.0
```

In this example, the management IP is set to 192.50.50.205 with a subnet mask of 255.255.255.0.

Note – This is the IP address used for health checks towards the inbound router; that is, the B10n content load balancing blade and also the IP address configured on the B10n content load balancing blade to perform health checks on the SSL proxy blade.

For a B10n content load balancing blade with an SSL proxy blade in non-VLAN mode, the VLAN filter must be disabled. This means that the SSL proxy blade will not expect a VLAN tag for any incoming or outgoing traffic and no filtering will be done based on the VLAN ID.

7. **Disable the VLAN filtering on the SSL proxy blade:**

```
CLI# set vlan filter disable
```

8. **Configure port pair 1 on the SSL proxy with the secure port specified as 443 and the clear port specified as 880:**

```
CLI# set portpair

Enter portpair number (1..4) (1): 1
Enter secure port (https) (443): 443
Enter clear port (http) (880): 880
```

Note – Up to four such port pairs can be configured on the SSL proxy blade. The maximum value of each port cannot exceed 1023. Each of the eight ports in the four port pairs must be unique.

---

9. **Create a service `svc1` on the SSL proxy with the key `key1` associated with it:**

```
CLI# create service

Enter service name: svc1
Enter key name: key1
Enter server IP Address (0.0.0.0): 110.10.10.1
Enter cipher (export/best/optimal/high/medium/low) (best): best
Enter portpair number (1..4) (1): 1
    Service svc1 created.
```

In this example, the service is offered at the IP address 110.10.10.1. The *best* cipher is chosen for this service and port pair 1 (with secure port 443 and clear port 880) is configured for the service.

10. **Use `show service` to display all the services configured on the SSL proxy blade.**

Note – Unique keys and certificates must be used for each service configured on an SSL proxy blade. The same key and certificate must be used for the same service configured on multiple SSL proxy blades.

Setting Up the Router

Configure the following interfaces on the router.

1. **Configure one or more interfaces for the SSL proxy blades and the Sun Fire B100s Solaris server blades to reach the clients.**

Note – The address of this interface will be the one configured as the outbound router on the SSL proxy blade, that is, 192.100.100.254 in this example.

Example:

If the router was a Solaris system, the following command would configure the interface.

```
# ifconfig ce0 plumb 192.100.100.254 netmask 255.255.255.0 broadcast + up
```

2. **Configure one interface on each subnet on which services are provided. This provides routes from the clients/external routers to the VIPs (on the VIP side).**

   In this example, one interface has to be configured on the 110.10.10.0 subnet.

   Example:

   If the router was a Solaris system, the following command would configure an interface for the VIP subnet.

```
# ifconfig ce0 addif 110.10.10.254 netmask 255.255.255.0 broadcast + up
```

3. **Configure one interface on each subnet on which clients are configured. This provides routes from the clients/external routers to the services (on the client side).**

   Example:

   If the router was a Solaris system, the following command would configure an interface for clients/external routers in the 199.99.9.0 subnet.

```
# ifconfig ce0 addif 199.99.9.254 netmask 255.255.255.0 broadcast + up
```

Setting Up Sun Fire B100s Solaris Server Blades

1. **Return to the Solaris prompt and download and install the `clbmod` packages:**

```
# cd location_of_the_clbmod_packages
pkgadd -d
```

2. **Configure the real IP address for the management subnet:**

```
# ifconfig ce0 plumb 192.50.50.10 netmask 255.255.255.0 up
```

   This example shows switch 0 as active, so interface `ce0` is being configured.

3. **Configure the VIPs on the loopback interface, for example:**

```
# ifconfig lo0:1 plumb 110.10.10.1 netmask 255.255.255.0 up
```

4. **Add the interfaces to the `clbmod`:**

```
# /opt/SUNWclb/bin/clbconfig add ce0
```

   Add `ce0` to `/etc/opt/SUNWclb/clb.conf`, to automatically add the interfaces to `clbmod` across reboots.

5. **Check the interfaces on which the module is plumbed:**

```
# /opt/SUNWclb/bin/clbconfig list
```

6. **Make sure the Sun Fire B100s Solaris server blade is not routing, that is, the `/etc/notrouter` file should be present.**

```
# /opt/SUNWclb/bin/clbconfig add ce0
```

7. **Configure your web server to listen on the decrypted port, that is, 880 in this example.**

8. **Repeat the above steps for each server blade you want to configure.**

Setting Up Clients/External Routers

On the clients/external routers add routes to the VIPs to use interfaces on the client subnet with the target address specified as the client side interface on the router as specified in section "Setting Up the Router" on page 25.

Example:

On a Solaris client directly connected to one of the uplink ports of the B1600 system chassis, the following commands can be used:

```
# ifconfig ce0 plumb 199.99.9.101 netmask 255.255.255.0 broadcast + up
```

This command configures the `ce0` interface with an IP address of 199.99.9.101 which is on the same subnet as the client side interface (199.99.9.254) on the router as specified in section "Setting Up the Router" on page 25.

```
# route add -net 110.10.10.0 199.99.9.254 static
```

This adds a static route to the VIPs in the 110.10.10.0 subnet through the client side interface (199.99.9.254) on the router as specified in section "Setting Up the Router" on page 25.

Known Issues

Crashes Might Occur in Large Configurations Due to Memory Loss (Bug ID 4955398)

When a large configuration is used (512 1K keys and 255 services), and the system has been running with 64K open connections, the Sun Fire B10p SSL proxy blade might not have enough memory for an additional operation and could crash. This issue is seen in rare cases and is not likely to happen under normal usage.

Using the `boot upload` Command Without IP Addresses

If you execute the `boot upload` command when the management ports and the inband ports have zero IP addresses, the B10p blade displays `Admin IP or inband admin IP not set. Set admin IP first`. However, there is no `set admin` command. Use the `set management` command instead.