



Sun Fire™ B10p SSL Proxy Blade Version 1.1 Administration Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 817-7321-10
September 2004, Revision A

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

Copyright 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in the Sun Microsystems, Inc. license agreements and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct. 1998), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, AnswerBook2, docs.sun.com, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISÉE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



Please
Recycle



Adobe PostScript

Contents

- 1. Product Overview 1**
 - Hardware and Software Overview 1
 - Software Architecture 2
 - Command Line and Console Interfaces 3
 - Application Software 4
 - BSC Firmware 5
 - Hardware and Software Requirements 6
 - Product Features 6
 - Key Features 6
 - Supported Protocols 7
 - The Role of the SSL Proxy Blade 7
 - Topology Fundamentals 11
 - The Role of the B10p SSL Proxy Blade 13
 - Failover Alternatives 14
 - The Role of VLANs 15
 - System Integration 17
 - User Access 17
- 2. Installing the Blade and Setting Up the System 19**
 - Installing the Blade 19

- ▼ To Install the Blade 19
- LED Displays 23
- Location of Ports 24
 - Connecting to the 10/100/1000BASE-T Data Network Ports 26
- Serial Port Pin Numbers 26
- Powering On the SSL Proxy Blade 27
- Powering Off the SSL Proxy Blade 29
 - Powering Off With an Orderly Shut Down of the SSL Software 29
 - ▼ Forcing the Power Off 30
 - ▼ Powering Off an SSL Proxy Blade Without Requiring the Confirmation Prompt 30
 - ▼ Powering an SSL Proxy Blade Down to Standby Mode to Save Power 30
 - ▼ Powering Off an SSL Proxy Blade Before Removal 31
- Upgrading the Sun Fire B10p SSL Proxy Blade Software 31
- 3. Initial Configuration 33**
 - Initializing the SSL Proxy Blade 33
 - ▼ To Initialize the SSL Proxy Blade 34
 - ▼ To Create Keys and Certificates 37
 - ▼ To Create Services for the Servers 38
 - ▼ To Verify and Save the Configuration 39
- 4. Setting Up Sun Fire Blades for Load Balancing SSL Traffic 43**
 - Setting Up for Load Balancing SSL Traffic 43
 - Setting Up the Sun Fire B10n Content Load Balancing Blade 44
 - ▼ To Configure the Network Interface and VLAN 44
 - ▼ To Configure the SSL Proxy Blade 45
 - ▼ To Verify the SSL Proxy Blade Configuration on the B10n Content Load Balancing Blade 46

- ▼ To Configure a Layer 7 SSL Service on a B10n Content Load Balancing Blade 46

Setting Up the SSL Proxy Blade 48

- ▼ To Access the SSL Proxy Blade Console 48
- ▼ To Set Up the SSL Proxy Blade 49

Setting Up the Router 53

Setting Up the Sun Fire B1600 Switch 54

- ▼ To Get to the Sun Fire B1600 Switch Console 54
- ▼ To Set Up the Sun Fire B1600 Switch 54
- ▼ To Create VLANs 55

Setting Up Sun Fire B100s Solaris Server Blades 57

Setting Up Clients/External Routers 58

5. **Command-Line Interface** 59

Command-Line Interface Basics 59

User Access 60

User Access Commands 62

Concurrent User Commands 62

Global Commands 63

Global Command Examples 64

System State Commands 68

Commands and Processing States 69

Fault State 70

SSL Traffic Commands 70

TCP Port Numbers 71

- ▼ To Display the Current TCP Port Settings 72
- ▼ To Set the TCP Port Numbers 72
- ▼ To Show HTTPS Forwarding 73
- ▼ To Set HTTPS Forwarding 73

Traffic Port Network Settings	74
▼ To Display the Current Link Settings	74
▼ To Set the Link Availability for Ports	74
Network Interfaces	75
▼ To Display the Current Interface Settings	75
▼ To Display the Current Router Information	76
Configuration Storage	76
Configuration Management Commands	77
▼ To Display Differences Between Configurations	77
▼ To Reset the Default Configuration Settings	78
▼ To Reset the Configuration	78
▼ To Save the Configuration	78
Backups	79
Import and Export	79
▼ To Export the Active Configuration Using FTP or TFTP	79
Import	80
▼ To Import the Active Configuration Using FTP	80
Keys and Certificates	81
▼ To Create a Self-Signed Certificate.	82
▼ To Create a CA-Signed Certificate.	82
▼ To Import a Certificate From a Server	84
Certificate Formats	85
Certificate Management Commands	86
▼ To Display Information About Keys	86
▼ To Create a Key	86
▼ To Delete a Key	86
▼ To Import a Key Using FTP	87
▼ To Import a Key Using TFTP	87

- ▼ To Import a Key 88
- ▼ To Export a Key Using FTP 88
- ▼ To Export a Key Using TFTP 89
- ▼ To Export a Key 89
- ▼ To Create a Certificate 90
- ▼ To Import a Certificate Using FTP 91
- ▼ To Import a Certificate Using TFTP 91
- ▼ To Import a Certificate 92
- ▼ To Export a Certificate Using FTP 92
- ▼ To Export a Certificate Using TFTP 93
- ▼ To Export a Certificate 93

Setting Default Information for Certificates 93

- ▼ To Display the Default Settings for Creating Certificates 93
- ▼ To Set the Default Certificate Parameters 94

Creating a Certificate Signing Request (CSR) 94

- ▼ To Create A Certificate Signing Request 94
- ▼ To Export a Certificate Signing Request Using FTP 95
- ▼ To Export a Certificate Signing Request Using TFTP 95
- ▼ To Export a Certificate Signing Request 96

Services 96

Service Commands 97

- ▼ To Create a Service 97
- ▼ To Delete a Service 98
- ▼ To Display Current Services 99
- ▼ To Display Available Ciphers 99

DNS Name for a Service 99

- ▼ To Create a New Service With a DNS Name (IP=0.0.0.0) 99
- ▼ To Display DNS Server Settings 100

▼ To Set the DNS Server Settings	100
Diagnostics	100
▼ To Send a ping Request	101
▼ To Set the Number of Lines for a Telnet Session	101
Statistics	101
▼ To View the Global Accumulated Statistics	102
▼ To View the Global Detailed Statistics	103
▼ To View the Service Statistics	104
▼ To Reset the Statistics	104
Event Logging Commands	104
Log Levels	105
Info Events	105
Log Destination	105
Log Commands	107
SNMP Commands	110
▼ To Enable the SSL Proxy Blade for SNMP Support	110
▼ To Disable SNMP	112
▼ To Check the SNMP State	112
6. Upgrading the Application Software and the BSC Firmware	113
Software Architecture	113
Setting Up a TFTP Server	114
▼ To Set Up a TFTP Server	114
Upgrading the Application Software From a VLAN-Capable Server	116
Executing Boot Upload Commands	116
▼ To Execute Boot Upload Commands Using an FTP Server	117
▼ To Execute Boot Upload Commands Using a TFTP Server	119
Verifying the Upgrade	120
Reverting to a Previous Software Version	120

Factory Image	121
Image Commands	121
show version	121
reboot	121
show boot	122
boot activate	122
boot revert	123
boot upload	123
boot upload-tftp	123
Upgrading the Application Software From a non-VLAN-Capable Server	124
▼ To Update the Image From a Non-VLAN-Capable Server	124
Upgrading the BSC Firmware	126
A. Security Primer	129
Encryption	129
Symmetric Key Encryption	129
Public Key Encryption	130
Authentication	130
Secure Socket Layer	130
SSL Accelerators	131
Sessions Per Second	131
Concurrent Sessions	132
Bulk Encryption Data Rate	132
Authenticated Software Upgrades	132
Export	132
SSL Proxy Blade Security Features	133
User Access	133
Tamper Protection	133
Configuration Back Up	133

Supported Ciphers	134
Key Lengths	137
B. Application Notes	139
Web Server Configuration	139
Redundant Systems	140
Fail Over Unit Setup	140
C. Requesting a Certificate	141
Managing Keys and Certificates	141
Key Management Features	142
D. Boot Information	143
E. SSL Statistics	145
Persistence of Statistics Counters	145
Statistics Counters Important to SSL Proxy Blade	146
Performance	146
SSL Connection vs. SSL Session	146
Session ID Reuse	146
Variable Descriptions	147
Up Time	147
Transactions Per Second (TPS)	147
Concurrent Connections	148
Throughput	149
SSL Handshakes	149
SSL Handshakes With Reused Session IDs	150
Number of Dropped Reuse ID Requests (Persistent)	150
F. Troubleshooting	153
Sanity Check	153

SSL Proxy Blade Troubleshooting Information Sources	153
Basic Troubleshooting Principles	154
Most Common Problems for the SSL Proxy Blade	154

G. Alphabetical Command Reference 155

A	155
B	155
C	155
D	156
E	156
H	157
I	157
L	158
P	158
R	158
S	158
T	161
W	161

Glossary 163

Index 165

Declaration of Conformity

Compliance Model Number: BP-5
Product Family Name: Sun Fire B10p SSL proxy blade

EMC

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022:1998 / CISPR22:1997 Class A

EN55024:1998 Required Limits (as applicable):

EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass

EN61000-3-2:1995 + A1, A2, A14 Pass

EN61000-3-3:1995 Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN60950:1992, 2nd Edition, Amendments 1, 2, 3, 4, 11 TÜV Rheinland Certificate No. Not Required

IEC 950:1991, 2nd Edition, Amendments 1, 2, 3, 4 CB Scheme Certificate No. US/6982/UL

Evaluated to all CB Countries

FDA DHHS Accession Number (Monitors Only)

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
901 San Antonio Road, MPK15-102
Palo Alto, CA 94303-4900 U.S.A.
Tel: 650-786-3255
Fax: 650-786-3723

DATE

/S/

Peter Arkless
Quality Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: 0506-670000 Fax: 0506-760011

DATE

Regulatory Compliance Statements

Your Sun product is marked to indicate its compliance class:

- Federal Communications Commission (FCC) — USA
- Industry Canada Equipment Standard for Digital Equipment (ICES-003) — Canada
- Voluntary Control Council for Interference (VCCI) — Japan
- Bureau of Standards Metrology and Inspection (BSMI) — Taiwan

Please read the appropriate section that corresponds to the marking on your Sun product before attempting to install the product.

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables to comply with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted-pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables in order to maintain compliance with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

ICES-003 Class A Notice - Avis NMB-003, Classe A

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ICES-003 Class B Notice - Avis NMB-003, Classe B

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.


VCCI 基準について

クラス A VCCI 基準について

クラス A VCCI の表示があるワークステーションおよびオプション製品は、クラス A 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

クラス B VCCI 基準について

クラス B VCCI の表示  があるワークステーションおよびオプション製品は、クラス B 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

BSMI Class A Notice

The following statement is applicable to products shipped to Taiwan and marked as Class A on the product compliance label.

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。



Safety Agency Compliance Statements

Read this section before beginning any procedure. The following text provides safety precautions to follow when installing a Sun Microsystems product.

Safety Precautions

For your protection, observe the following safety precautions when setting up your equipment:

- Follow all cautions and instructions marked on the equipment.
- Ensure that the voltage and frequency of your power source match the voltage and frequency inscribed on the equipment's electrical rating label.
- Never push objects of any kind through openings in the equipment. Dangerous voltages may be present. Conductive foreign objects could produce a short circuit that could cause fire, electric shock, or damage to your equipment.

Symbols

The following symbols may appear in this book:



Caution – There is a risk of personal injury and equipment damage. Follow the instructions.



Caution – Hot surface. Avoid contact. Surfaces are hot and may cause personal injury if touched.



Caution – Hazardous voltages are present. To reduce the risk of electric shock and danger to personal health, follow the instructions.



On – Applies AC power to the system.

Depending on the type of power switch your device has, one of the following symbols may be used:



Off – Removes AC power from the system.



Standby – The On/Standby switch is in the standby position.

Modifications to Equipment

Do not make mechanical or electrical modifications to the equipment. Sun Microsystems is not responsible for regulatory compliance of a modified Sun product.

Placement of a Sun Product



Caution – Do not block or cover the openings of your Sun product. Never place a Sun product near a radiator or heat register. Failure to follow these guidelines can cause overheating and affect the reliability of your Sun product.



Caution – The workplace-dependent noise level defined in DIN 45 635 Part 1000 must be 70Db(A) or less.

SELV Compliance

Safety status of I/O connections comply to SELV requirements.

Power Cord Connection



Caution – Sun products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electric shock, do not plug Sun products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.



Caution – Not all power cords have the same current ratings. Household extension cords do not have overload protection and are not meant for use with computer systems. Do not use household extension cords with your Sun product.



Caution – Your Sun product is shipped with a grounding type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

The following caution applies only to devices with a Standby power switch:



Caution – The power switch of this product functions as a standby type device only. The power cord serves as the primary disconnect device for the system. Be sure to plug the power cord into a grounded power outlet that is nearby the system and is readily accessible. Do not connect the power cord when the power supply has been removed from the Sun Fire B1600 blade chassis.

Lithium Battery



Caution – On Sun CPU boards, there is a lithium battery molded into the real-time clock, SGS No. MK48T59Y, MK48TXXB-XX, MK48T18-XXXPCZ, M48T59W-XXXPCZ, or MK48T08. Batteries are not customer replaceable parts. They may explode if mishandled. Do not dispose of the battery in fire. Do not disassemble it or attempt to recharge it.

Battery Pack



Caution – There is a sealed lead acid battery in Sun Fire B10p SSL proxy blade units. Portable Energy Products No. TLC02V50. There is danger of explosion if the battery pack is mishandled or incorrectly replaced. Replace only with the same type of Sun Microsystems battery pack. Do not disassemble it or attempt to recharge it outside the system. Do not dispose of the battery in fire. Dispose of the battery properly in accordance with local regulations.

System Unit Cover

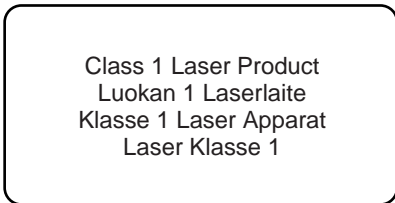
You must remove the cover of your Sun computer system unit to add cards, memory, or internal storage devices. Be sure to replace the top cover before powering on your computer system.



Caution – Do not operate Sun products without the top cover in place. Failure to take this precaution may result in personal injury and system damage.

Laser Compliance Notice

Sun products that use laser technology comply with Class 1 laser requirements.

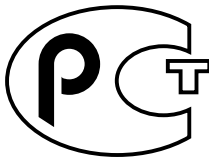


CD-ROM



Caution – Use of controls, adjustments, or the performance of procedures other than those specified herein may result in hazardous radiation exposure.

GOST-R Certification Mark



Conformité aux normes de sécurité

Lisez attentivement la section suivante avant de commencer la procédure. Le document ci-dessous présente les consignes de sécurité à respecter au cours de l'installation d'un produit Sun Microsystems.

Mesures de sécurité

Pour votre protection, observez les mesures de sécurité suivantes lors de l'installation de l'équipement:

- Observez tous les avertissements et consignes indiqués sur l'équipement.
- Assurez-vous que la tension et la fréquence de votre source d'alimentation électrique correspondent à la tension et à la fréquence indiquées sur l'étiquette de la tension électrique nominale du matériel.

- N'insérez en aucun cas un objet quelconque dans les orifices de l'équipement. Des tensions potentiellement dangereuses risquent d'être présentes dans l'équipement. Tout objet étranger conducteur risque de produire un court-circuit pouvant présenter un risque d'incendie ou de décharge électrique, ou susceptible d'endommager le matériel.

Symboles

Les symboles suivants peuvent figurer dans cet ouvrage :



Attention – Vous risquez d'endommager le matériel ou de vous blesser. Observez les consignes indiquées.



Attention – Surface brûlante. Evitez tout contact. Ces surfaces sont brûlantes. Vous risquez de vous blesser si vous les touchez.



Attention – Tensions dangereuses. Pour réduire les risques de décharge électrique et de danger physique, observez les consignes indiquées.



MARCHE – Met le système sous tension alternative.

Selon le type d'interrupteur marche/arrêt dont votre appareil est équipé, l'un des symboles suivants sera utilisé :



ARRÊT – Met le système hors tension alternative.



VEILLEUSE – L'interrupteur Marche/Veille est sur la position de veille.

Modifications de l'équipement

N'apportez aucune modification mécanique ou électrique à l'équipement. Sun Microsystems décline toute responsabilité quant à la non-conformité éventuelle d'un produit Sun modifié.

Positionnement d'un produit Sun



Attention – N'obstruez ni ne recouvrez les orifices de votre produit Sun. N'installez jamais un produit Sun près d'un radiateur ou d'une source de chaleur. Si vous ne respectez pas ces consignes, votre produit Sun risque de surchauffer et son fonctionnement en sera altéré.



Attention – Le niveau de bruit inhérent à l'environnement de travail, tel qu'il est défini par la norme DIN 45 635 - section 1000, doit être inférieur ou égal à 70Db(A).

Conformité aux normes SELV

Le niveau de sécurité des connexions E/S est conforme aux normes SELV.

Raccordement à la source d'alimentation électrique



Attention – Les produits Sun sont conçus pour fonctionner avec des systèmes d'alimentation électrique monophasés avec prise de terre. Pour réduire les risques de décharge électrique, ne branchez jamais les produits Sun sur une source d'alimentation d'un autre type. Contactez le gérant de votre bâtiment ou un électricien agréé si vous avez le moindre doute quant au type d'alimentation fourni dans votre bâtiment.



Attention – Tous les cordons d'alimentation n'ont pas la même intensité nominale. Les cordons d'alimentation à usage domestique ne sont pas protégés contre les surtensions et ne sont pas conçus pour être utilisés avec des ordinateurs. N'utilisez jamais de cordon d'alimentation à usage domestique avec les produits Sun.



Attention – Votre produit Sun est livré avec un cordon d'alimentation avec raccord à la terre (triphase). Pour réduire les risques de décharge électrique, branchez toujours ce cordon sur une source d'alimentation mise à la terre.

L'avertissement suivant s'applique uniquement aux systèmes équipés d'un interrupteur Veille :



Attention – L'interrupteur d'alimentation de ce produit fonctionne uniquement comme un dispositif de mise en veille. Le cordon d'alimentation constitue le moyen principal de déconnexion de l'alimentation pour le système. Assurez-vous de le brancher dans une prise d'alimentation mise à la terre près du système et facile d'accès. Ne le branchez pas lorsque l'alimentation électrique ne se trouve pas dans le châssis du système.

Pile au lithium



Attention – Sur les cartes UC Sun, une batterie au lithium a été moulée dans l'horloge temps réel, de type SGS n° MK48T59Y, MK48TXXB-XX, MK48T18-XXXPCZ, M48T59W-XXXPCZ ou MK48T08. Cette batterie ne doit pas être remplacée par le client. Elle risque d'exploser en cas de mauvaise manipulation. Ne la jetez pas au feu. Ne la démontez pas et ne tentez pas de la recharger.

Bloc-batterie



Attention – Les unités Sun Fire B10p SSL proxy blade contiennent une batterie étanche au plomb. Produits énergétiques portatifs n° TLC02V50. Il existe un risque d'explosion si ce bloc batterie est manipulé ou installé de façon incorrecte. Ne le remplacez que par un bloc batterie Sun Microsystems du même type. Ne le démontez pas et n'essayez pas de le recharger hors du système. Ne le jetez pas au feu. Mettez-le au rebut conformément aux réglementations locales en vigueur.

Couvercle du système

Pour ajouter des cartes, de la mémoire ou des unités de stockage internes, vous devez démonter le couvercle de votre système Sun. N'oubliez pas de le remettre en place avant de mettre le système sous tension.



Attention – Ne travaillez jamais avec un produit Sun dont le couvercle n'est pas installé. Si vous ne respectez pas cette consigne, vous risquez de vous blesser ou d'endommager le système.

Avis de conformité des appareils laser

Les produits Sun faisant appel à la technologie laser sont conformes aux normes de sécurité des appareils laser de classe 1.

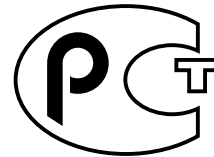
Class 1 Laser Product
Luokan 1 Laserlaite
Klasse 1 Laser Apparat
Laser Klasse 1

CD-ROM



Attention – L'utilisation de contrôles et de réglages ou l'application de procédures autres que ceux spécifiés dans le présent document peuvent entraîner une exposition à des radiations dangereuses.

Notice de qualité GOST-R



Einhaltung sicherheitsbehördlicher Vorschriften

Lesen Sie diesen Abschnitt sorgfältig durch, bevor Sie mit dem Arbeitsablauf beginnen. Der folgende Text beschreibt Sicherheitsmaßnahmen, die bei der Installation von Sun-Produkten zu beachten sind.

Sicherheitsmaßnahmen

Zu Ihrem eigenen Schutz sollten Sie die folgenden Sicherheitsmaßnahmen bei der Installation befolgen :

- Befolgen Sie alle auf die Geräte aufgedruckten Anweisungen und Warnhinweise.
- Beachten Sie die Geräteaufschrift, um sicherzustellen, daß Netzspannung und -frequenz mit der Gerätespannung und -frequenz übereinstimmen.
- Führen Sie niemals Gegenstände in die Geräteöffnungen ein. Es könnten elektrische Spannungsfelder vorhanden sein. Leitende Fremdkörper können Kurzschlüsse, Feuer und elektrische Schläge verursachen oder Ihr Gerät beschädigen.

Symbole

Die folgenden Symbole werden in diesem Handbuch verwendet:



Achtung – Es besteht die Gefahr der Verletzung und der Beschädigung des Geräts. Befolgen Sie die Anweisungen.



Achtung – Heiße Oberfläche. Vermeiden Sie jede Berührung. Diese Oberflächen sind sehr heiß und können Verbrennungen verursachen.



Achtung – Elektrisches Spannungsfeld vorhanden. Befolgen Sie die Anweisungen, um elektrische Schläge und Verletzungen zu vermeiden.



Ein – Das System wird mit Wechselstrom versorgt.

Abhängig von der Art des Stromschalters Ihres Gerätes wird eventuell eines der folgenden Symbole verwendet:



Aus – Das System wird nicht mehr mit Wechselstrom versorgt.



Wartezustand – (Der Ein-/Standby-Schalter befindet sich in der Standby-Position).

Modifikationen des Geräts

Nehmen Sie keine elektrischen oder mechanischen Gerätemodifikationen vor. Sun Microsystems ist für die Einhaltung der Sicherheitsvorschriften von modifizierten Sun-Produkten nicht haftbar.

Aufstellung von Sun-Geräten



Achtung – Geräteöffnungen Ihres Sun-Produkts dürfen nicht blockiert oder abgedeckt werden. Sun-Geräte sollten niemals in der Nähe von Heizkörpern oder Heißluftklappen aufgestellt werden. Nichtbeachtung dieser Richtlinien können Überhitzung verursachen und die Zuverlässigkeit Ihres Sun-Geräts beeinträchtigen.



Achtung – Der Geräuschpegel, definiert nach DIN 45 635 Part 1000, darf am Arbeitsplatz 70dB(A) nicht überschreiten.

SELV-Richtlinien

Alle Ein-/Ausgänge erfüllen die SELV-Anforderungen.

Netzanschlußkabel



Achtung – Sun-Geräte benötigen ein einphasiges Stromversorgungssystem mit eingebautem Erdleiter. Schließen Sie Sun-Geräte nie an ein anderes Stromversorgungssystem an, um elektrische Schläge zu vermeiden. Falls Sie die Spezifikationen der Gebäudestromversorgung nicht kennen, sollten Sie den Gebäudeverwalter oder einen qualifizierten Elektriker konsultieren.



Achtung – Nicht alle Netzanschlußkabel besitzen die gleiche Stromleitung. Normale Verlängerungskabel besitzen keinen Überspannungsschutz und sind nicht für den Gebrauch mit Computersystemen geeignet. Benutzen Sie keine Haushaltverlängerungskabel für Sun-Geräte.



Achtung – Ihr Sun-Gerät wurde mit einem geerdeten (dreiadrigen) Netzanschlußkabel geliefert. Stecken Sie dieses Kabel immer nur in eine geerdete Netzsteckdose, um Kurzschlüsse zu vermeiden.

Der folgende Hinweis bezieht sich nur auf Geräte mit Standby-Stromschalter:



Achtung – Der Stromschalter dieses Produkts funktioniert nur als Standby-Gerät. Das Netzanschlußkabel dient als Hauptabschaltgerät für das System. Stellen Sie sicher, daß Sie das Netzanschlußkabel in den geerdeten Stromausgang in der Nähe des Systems einstecken. Schließen Sie das Netzanschlußkabel nicht an, wenn die Stromzufuhr vom Systemgehäuse entfernt wurde.

Lithium-Batterie



Achtung – CPU-Karten von Sun verfügen über eine Echtzeituhr mit integrierter Lithiumbatterie, Teile-Nr. MK48T59Y, MK48TXXB-XX, MK48T18-XXXPCZ, M48T59W-XXXPCZ oder MK48T08. Batterien sollten nicht vom Kunden ausgetauscht werden. Sie können bei falscher Handhabung explodieren. Entsorgen Sie die Batterien nicht im Feuer. Entfernen Sie sie nicht und versuchen Sie auch nicht, sie wiederaufzuladen.

Batterien



Achtung – Die Geräte Sun Fire B10p SSL proxy blade enthalten auslaufsichere Bleiakumulatoren, Produkt-Nr. TLC02V50 für portable Stromversorgung. Wenn die Batterien nicht richtig gehandhabt oder ausgetauscht werden, besteht Explosionsgefahr. Tauschen Sie Batterien nur gegen Batterien gleichen Typs von Sun Microsystems aus. Versuchen Sie nicht, die Batterien zu entfernen oder außerhalb des Geräts wiederaufzuladen. Entsorgen Sie die Batterien nicht im Feuer. Entsorgen Sie die Batterien ordnungsgemäß entsprechend den vor Ort geltenden Vorschriften.

Abdeckung des Systems

Sie müssen die Abdeckung des Sun-Computersystems entfernen, um Karten, Speicher oder interne Speichergeräte hinzuzufügen. Stellen Sie sicher, daß Sie die Abdeckung wieder einsetzen, bevor Sie den Computer einschalten.



Achtung – Sun-Geräte dürfen nicht ohne Abdeckung in Gebrauch genommen werden. Nichtbeachtung dieses Warnhinweises kann Verletzungen oder Systembeschädigungen zur Folge haben.

Laserrichtlinien

Alle Sun-Produkte, die Lasertechnologie nutzen, erfüllen die Laserrichtlinien der Klasse 1.

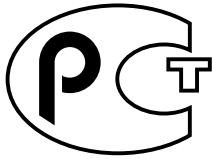
Class 1 Laser Product
Luokan 1 Laserlaite
Klasse 1 Laser Apparät
Laser Klasse 1

CD-ROM



Achtung – Die Verwendung von anderen Steuerungen und Einstellungen oder die Durchführung von Arbeitsabläufen, die von den hier beschriebenen abweichen, können gefährliche Strahlungen zur Folge haben.

Verbandsmarke GOST-R



Normativas de seguridad

Lea esta sección antes de llevar a cabo cualquier procedimiento. El texto que aparece a continuación explica las medidas de seguridad que deben tomarse durante la instalación de un producto Sun Microsystems.

Medidas de seguridad

Por su propia seguridad, tome las medidas de seguridad siguientes al instalar el equipo:

- Siga todas los avisos y las instrucciones que aparecen impresas en el equipo.
- Cerciórese de que el voltaje y la frecuencia de la fuente de alimentación coinciden con el voltaje y frecuencia indicados en la etiqueta de clasificación eléctrica del equipo.
- No introduzca objetos de ningún tipo a través de las aberturas del equipo. Dentro pueden darse voltajes peligrosos. Los objetos conductores extraños podrían producir un cortocircuito y, en consecuencia, fuego, descargas eléctricas o daños en el equipo.

Símbolos

Los símbolos siguientes pueden aparecer en este manual:



Precaución – Existe el riesgo de que se produzcan lesiones personales y daños en el equipo. Siga las instrucciones.



Precaución – Superficie caliente. Evite todo contacto. Las superficies están calientes y pueden causar lesiones personales si se tocan.



Precaución – Riesgo de voltajes peligrosos. Para reducir el riesgo de descargas eléctricas y de daños en la salud de las personas, siga las instrucciones.



Encendido – Proporciona alimentación de CA al sistema.

Según el tipo de interruptor de alimentación del que disponga el dispositivo, se utilizará uno de los símbolos siguientes:



Apagado – Corta la alimentación de CA del sistema.



Espera – El interruptor de encendido/espera está en la posición de espera.

Modificaciones en el equipo

No realice modificaciones mecánicas ni eléctricas en el equipo. Sun Microsystems no se hará responsable del cumplimiento de las normas en el caso de un producto Sun que ha sido modificado.

Lugar y colocación de un producto Sun



Precaución – No obstruya ni tape las rejillas del producto Sun. Nunca coloque un producto Sun cerca de radiadores o fuentes de calor. El incumplimiento de estas directrices puede causar un recalentamiento y repercutir en la fiabilidad del producto Sun.



Precaución – El nivel de ruido en el lugar de trabajo, definido en el apartado 1000 de DIN 45 635, debe ser 70 Db (A) o inferior.

Cumplimiento de las normas SELV

Las condiciones de seguridad de las conexiones de E/S cumplen las normas SELV.

Conexión del cable de alimentación



Precaución – Los productos Sun han sido diseñados para funcionar con sistemas de alimentación monofásicos que tengan un conductor neutral a tierra. Para reducir el riesgo de descargas eléctricas, no enchufe ningún producto Sun a otro tipo de sistema de alimentación. Si no está seguro del tipo de alimentación del que se dispone en el edificio, póngase en contacto con el encargado de las instalaciones o con un electricista cualificado.



Precaución – No todos los cables de alimentación tienen la misma clasificación de corriente. Los cables de prolongación domésticos no ofrecen protección frente a sobrecargas y no están diseñados para ser utilizados con sistemas informáticos. No utilice cables de prolongación domésticos con el producto Sun.



Precaución – El producto Sun se suministra con un cable de alimentación (de tres hilos) con conexión a tierra. Para reducir el riesgo de descargas eléctricas, enchufe siempre el cable a una toma de corriente con conexión a tierra.

La precaución siguiente sólo se aplica a aquellos dispositivos que posean un interruptor de alimentación de espera:



Precaución – El interruptor de alimentación del producto funciona como dispositivo de espera solamente. El cable de alimentación actúa como el dispositivo de desconexión primario del sistema. Cerciérese de enchufar el cable de alimentación a una toma de corriente con conexión a tierra situada cerca del sistema y a la que se pueda acceder con facilidad. No conecte el cable de alimentación cuando se haya quitado la fuente de alimentación del bastidor del sistema.

Batería de litio



Precaución – En la placa CPU de los productos Sun, hay una batería de litio incorporada en el reloj en tiempo real, SGS núm. MK48T59Y, MK48TXXB-XX, MK48T18-XXXPCZ, M48T59W-XXXPCZ o MK48T08. Los usuarios no deben cambiar las baterías. Podrían estallar si no se utilizan adecuadamente. No arroje la batería al fuego. No la desmonte ni intente recargarla.

Paquete de baterías



Precaución – Las unidades Sun Fire B10p SSL proxy blade contienen una batería de plomo sellada, Productos eléctricos portátiles núm. TLC02V50. Existe el riesgo de explosión si el paquete de baterías no se utiliza correctamente o se sustituye de forma incorrecta. Sustitúyalo sólo por el mismo tipo de paquete de baterías de Sun Microsystems. No lo desmote o intente recargarlo fuera del sistema. No arroje la batería al fuego. Deshágase de las baterías correctamente siguiendo las normas locales vigentes.

Cubierta de la unidad del sistema

Debe retirar la cubierta de la unidad del sistema informático Sun para añadir tarjetas, memoria o dispositivos de almacenamiento internos. Asegúrese de volver a colocar la cubierta superior antes de encender el equipo.



Precaución – No ponga en funcionamiento los productos Sun sin que la cubierta superior se encuentre instalada. De lo contrario, podrían producirse lesiones personales o daños en el sistema.

Aviso de cumplimiento de las normas para láser

Los productos Sun que utilizan tecnología láser cumplen los requisitos para láser de Clase 1.

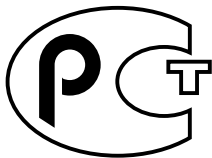
Class 1 Laser Product
Luokan 1 Laserlaite
Klasse 1 Laser Apparat
Laser Klasse 1

CD-ROM



Precaución – La utilización de controles, ajustes o la realización de los procedimientos distintos a los especificados en el presente documento podrían provocar la exposición a radiaciones peligrosas.

Certificación GOST-R



Nordic Lithium Battery Cautions

Norge



ADVARSEL – Litiumbatteri —
Eksplosjonsfare. Ved utskifting benyttes kun
batteri som anbefalt av apparatfabrikanten.
Brukt batteri returneres apparatleverandøren.

Sverige



VARNING – Explosionsfara vid felaktigt
batteribyte. Använd samma batterityp eller en
ekvivalent typ som rekommenderas av
apparatillverkaren. Kassera använt batteri
enligt fabrikantens instruktion.

Danmark



ADVARSEL! – Litiumbatteri —
Eksplosionsfare ved fejlagtig håndtering.
Udskiftning må kun ske med batteri af samme
fabrikat og type. Levér det brugte batteri
tilbage til leverandøren.

Suomi



VAROITUS – Paristo voi räjähtää, jos se on
virheellisesti asennettu. Vaihda paristo
ainoastaan laitevalmistajan suosittelemaan
tyyppiin. Hävitä käytetty paristo valmistajan
ohjeiden mukaisesti.

Tables

TABLE 1-1	Hardware and Software Requirements	6
TABLE 1-2	VLAN Based Security	16
TABLE 1-3	User Privileges	18
TABLE 2-1	Blade and Power Supply Status Codes	24
TABLE 2-2	10/100/1000BASE-T Data Network Port Pinouts	26
TABLE 2-3	Serial Port Pinouts	27
TABLE 3-1	Worksheet of Values for the SSL Proxy Blade Initialization	34
TABLE 3-2	Commands to Display Configuration Information	41
TABLE 5-1	User Privileges	61
TABLE 5-2	User Access Commands	62
TABLE 5-3	Concurrent User Commands	62
TABLE 5-4	Global Commands	63
TABLE 5-5	Show State Commands	69
TABLE 5-6	Commands That Require the SSL Proxy Blade to be Stopped or Rebooted	70
TABLE 5-7	TCP Port Numbers	71
TABLE 5-8	Traffic Network Settings Worksheet	74
TABLE 5-9	Available Cipher Suites	98
TABLE 5-10	Progressive Levels of Log Detail	105
TABLE A-1	Supported Ciphers	134
TABLE A-2	Security Levels for Ciphers	135

Figures

FIGURE 1-1	SSL Proxy Blade Images and CLI Commands	5
FIGURE 1-2	Ethernet Ports and Interfaces on the Sun Fire B1600 Blade Chassis and Their Default VLAN Numbers	9
FIGURE 1-3	A Dedicated Management Network and Web Server Network Isolated from the Backend Network	10
FIGURE 1-4	Dual Tree Using External and Internal Switches	13
FIGURE 2-1	The Filler Panel Locking Mechanism	20
FIGURE 2-2	Disengaging the Blade-Locking Mechanism	20
FIGURE 2-3	Removing the Filler Panel	21
FIGURE 2-4	Blade Locking Mechanism	21
FIGURE 2-5	Aligning and Inserting the Blade	22
FIGURE 2-6	Closing the Blade Lever Mechanism	23
FIGURE 2-7	External Cable Connections	25
FIGURE 2-8	10/100/1000BASE-T Data Network Ports	26
FIGURE 2-9	Serial Port Pin Numbers	27
FIGURE 5-1	Configuration State	77

Preface

The *Sun Fire B10p SSL Proxy Blade Administration Guide* provides installation and configuration instructions for the Sun Fire™ B10p SSL proxy blade. These instructions are designed for an experienced system administrator with networking knowledge.

How This Book Is Organized

Chapter 1 describes the product hardware and software and lists hardware and software requirements and features. It includes a summary of the basic operation of the blade.

Chapter 2 describes how to install the hardware and software.

Chapter 3 describes the steps required to initialize and configure the SSL proxy blade for use in a network environment.

Chapter 4 describes the steps required to configure the SSL proxy blade for load balancing SSL traffic.

Chapter 5 describes the command-line interface (CLI) for the SSL proxy blade used for viewing and configuring information and statistics.

Chapter 6 describes how to upgrade the firmware and software.

Appendix A provides a quick overview of the basic security concepts that are useful to the SSL proxy blade administrator, especially those new to the area of SSL security.

Appendix B includes application notes on various aspects of including the SSL proxy blade in new and existing network infrastructures.

Appendix C discusses requesting and managing certificates.

Appendix D shows a sample display of the information to the serial console during boot.

Appendix E lists and describes the key SSL statistics.

Appendix F outlines some common troubleshooting issues.

Appendix G provides an alphabetical listing of all the commands.

Glossary is a list of words and phrases and their definitions.

Using UNIX Commands

This document might not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices.

See one or more of the following for this information:

- *Solaris Handbook for Sun Peripherals*
- Other software documentation that you received with your system

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	% su Password:
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. To delete a file, type rm <i>filename</i> .

* The settings on your browser might differ from these settings.

Shell Prompts

Shell	Prompt
C shell	<i>machine-name%</i>
C shell superuser	<i>machine-name#</i>
Bourne shell and Korn shell	\$
Bourne shell and Korn shell superuser	#

Related Documentation

Application	Title	Part Number
Installation	<i>Sun Fire B1600 Blade System Chassis Hardware Installation Guide</i>	816-7614-10
	<i>Sun Content Load Balancing Blade Installation and User's Guide</i>	817-0677-10
Software setup	<i>Sun Fire B1600 Blade System Chassis Software Setup Guide</i>	816-3361-10
Safety and compliance	<i>Sun Fire B1600 Blade System Chassis Safety and Compliance Manual</i>	816-3364-10

Accessing Sun Documentation

You can view, print, or purchase a broad selection of Sun documentation, including localized versions, at:

<http://www.sun.com/products-n-solutions/hardware/docs/>

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

<http://www.sun.com/hwdocs/feedback>

Please include the title and part number of your document with your feedback:

Sun Fire B10p SSL Proxy Blade Version 1.1 Administration Guide, part number 817-7321-10

Product Overview

This chapter describes the Sun Fire™ B10p SSL proxy blade hardware and software, and lists both their features and the requirements for using them.

This chapter contains the following sections:

- “Hardware and Software Overview” on page 1
- “Software Architecture” on page 2
- “Hardware and Software Requirements” on page 6
- “Product Features” on page 6
- “The Role of the SSL Proxy Blade” on page 7
- “The Role of VLANs” on page 15
- “System Integration” on page 17
- “User Access” on page 17

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

Hardware and Software Overview

The Sun Fire B10p SSL proxy blade provides SSL handshake and encryption/decryption capabilities for the Sun Fire™ B1600 blade chassis. Designed specifically to optimize SSL processing, the custom hardware specialty blade can process SSL transactions many times faster than CPU-based SSL processing. The SSL proxy blade increases platform utilization by freeing system processors to complete other tasks, which enables maximum resource use, increased platform performance and availability of secure applications at lower costs.

The SSL proxy blade support for direct Proxy-to-Client response virtually eliminates the signal response back through the Sun Fire™ B10n content load balancing blade, which further speeds up response times and increases total capacity. Tamper-proof and centralized storage features as well as management capability of security keys and certificates also deliver higher levels of security and ease of management.

The primary performance parameter for SSL is the rate in which SSL sessions are established and the first file returned. This parameter is referred to as SSL sessions per second or transactions per second (TPS). The Sun Fire B10p SSL proxy blade has a maximum SSL sessions per second of 4000.

This product enables you to select the performance level that best fits your application. Up to four SSL proxy blade can be used in the same Sun Fire B1600 blade chassis. In the future, this maximum number may be increased. Check with your local Sun representative or the Sun.com web site for the latest configuration information.

Software Architecture

The Sun Fire B10p SSL proxy blade deliver their 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 SSL proxy blade software components are as follows:

- Application software
- BSC firmware

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

<http://www.sun.com/software/download/network.html>

The following three files are related to SNMP and are available at the download site (<http://www.sun.com/software/download/network.html>).

- SUN-B10P-SSL-ACCELERATOR-MIB
- SUN-B10P-SSL-ACCELERATOR-MIB.dat
- v2ConfTrap.sun_B10p

The first two files describe the SNMP MIB structure for the SSL proxy blade and are used to enable SNMP manager software for communicating with the SNMP agent on the blade.

For example, if you use the SNMP manager software from SNMP Research International on a UNIX system, you can rename the `SUN-B10P-SSL-ACCELERATOR-MIB.dat` file to `snmpinfo.dat` and save it in `/etc/srconf/mgr`, which is the default configuration directory used by SNMP Research.

`v2ConfTrap.sun_B10p` is a configuration file that should be imported to the SSL proxy blade for its SNMP agent to run. For more information on enabling the Sun Fire SSL Proxy Blade for SNMP, see “SNMP Commands” on page 110.

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 service 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.

```
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 this case 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 if a problem occurs when updating the software.

- Active image – Primary image stored in Flash and loaded into RAM on bootup
- Backup image – Secondary image stored in Flash which can be moved to the active image. This image is overwritten when new image is uploaded
- Factory image – Loaded into Flash at time of manufacture. Used when 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 a configuration file that holds the configuration data (see “Configuration Storage” on page 76). 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 1-1 shows the various images and how various CLI commands alter or copy them.

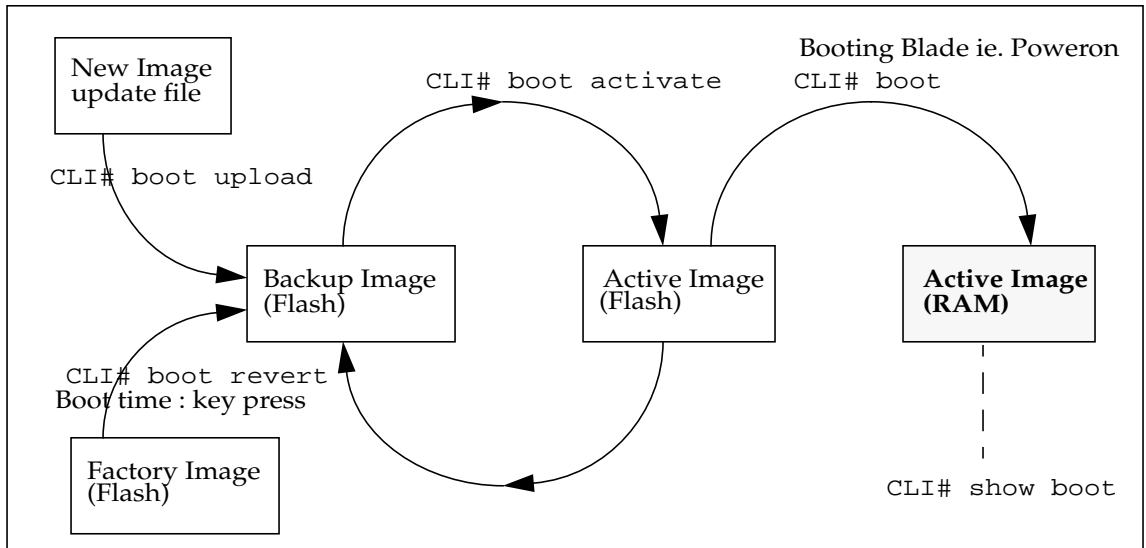


FIGURE 1-1 SSL Proxy Blade Images and CLI Commands

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 service controller software is managing the process.

Hardware and Software Requirements

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

TABLE 1-1 Hardware and Software Requirements

Hardware and Software	Requirements
Hardware	<ul style="list-style-type: none">• Sun Fire B10n content load balancing blade (at least one Sun Fire B10n content load balancing blade for up to four Sun Fire B10p SSL proxy blades)• Sun Fire B1600 blade chassis and other horizontally scaled Sun platforms• Sun Fire B100s blade server
Software	<ul style="list-style-type: none">• Sun Fire B10n content load balancing blade application software version 1.2 or subsequent compatible version• Sun Fire B10n content load balancing blade BSC firmware version v5.1.3* or subsequent compatible version• Sun Fire B10p SSL proxy blade application software version BSSL_1872.pkcs or subsequent compatible version• Sun Fire B10p SSL proxy blade BSC firmware version v5.1.0* or subsequent compatible version• Sun Fire B100s blade server Solaris 8 HW 3/03, Solaris 8 HW 7/03, or Solaris 9 8/03 operating system or subsequent compatible version• Sun Fire B1600 SC 1.2 or subsequent compatible system controller firmware

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

Product Features

Key Features

- Two full-duplex Gigabit Ethernet interfaces
- 4000 SSL connections per second
- Over 300Mb/s bulk throughput

- Proxy to client direct response
- 64k concurrent connections
- RSA key strengths: 512, 1024, 2048 bits
- Keys erased upon tamper detection
- Maximum allowed: 1024 keys, 1024 certificates, 1024 VIPs
- Path and blade failover
- Integrated management with the Sun Fire B1600 blade chassis, the Sun blade servers, and content load balancing blades

Supported Protocols

The following protocols are used for services or management functions:

- SSL 3.0/TLS 1.0
- TCP
- UDP
- HTTPS
- FTP
- TFTP
- ICMP
- ARP
- Telnet

The Role of the SSL Proxy Blade

The Sun Fire B10p SSL proxy blades are components within a larger system ultimately delivering highly available web services to a client population over an IP-based network. This section describes the role of such a highly integrated SSL proxy blade within the larger system.

The minimal set of components comprising the system encompasses:

- One or more Sun Fire B1600 blade chassis
- One or more Sun Fire B10n content load balancing blades
- One or more Sun Fire B10p SSL proxy blades
- One or two Switch and System Controller (SSC) units per Sun Fire B1600 blade chassis
- One or more servers which can be any mix of blade servers housed in the Sun Fire B1600 blade chassis and stand-alone Sun servers external to the Sun Fire B1600 blade chassis but connected to the same Ethernet broadcast domain (Layer 2 network)

Additionally, the system may have:

- External distribution switches extending one or more of the networks.
- Additional servers providing content, local name, and configuration services, and aggregate management for one or multiple shelves. These servers may participate in the overall system by supporting various TFTP, NFS, DHCP, DNS, and N1 deployment related functions.

In general terms, the intra-shelf network topology formed by connecting the Sun Fire B1600 system components is either a single or a dual redundant Layer 2 topology with blades “one-arm” connected to each of the switch fabrics. The switch fabric is VLAN partitionable for strict traffic isolation. SSC switches and uplinks can be used for a simple inter-shelf network, or connected to external distribution switches for larger configurations.

Note – This section defines the generic features and functions of the Sun Fire B10p SSL proxy blades. For more information about a specific software release, refer to the *Sun Fire B10p SSL Proxy Blade Product Notes*.

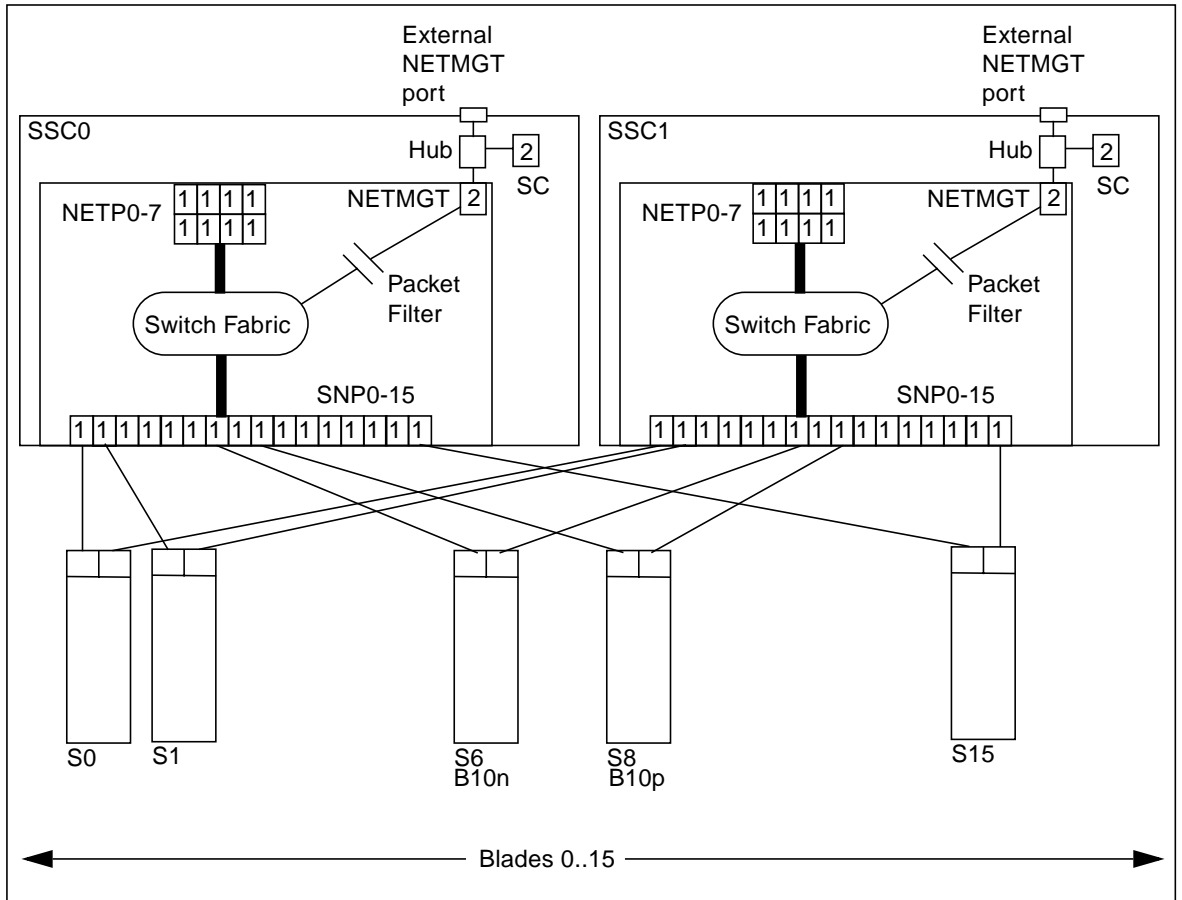


FIGURE 1-2 Ethernet Ports and Interfaces on the Sun Fire B1600 Blade Chassis and Their Default VLAN Numbers

FIGURE 1-2 shows the intra-shelf network, where an SSL proxy blade (shown in slot S8) can reside in any slot (S0 through S15) and connect to both SSC0 and SSC1 switch fabrics. The uplinks are labeled NETP0 through NETP7. The corresponding B10n content load balancing blade in slot S6 is shown for completeness.

The numerals associated with each port (either 1 or 2), represent the VLAN numbers programmed into the system by default. These numbers indicate that there is one data VLAN (1), and one management VLAN (2). Further VLAN partitioning might be desirable as shown in FIGURE 1-3. The actual VLAN-ID assignment can be coordinated with the VLANs used in the external switches, or its scope can be limited to the internal switches, by keeping the uplinks as untagged VLANs.

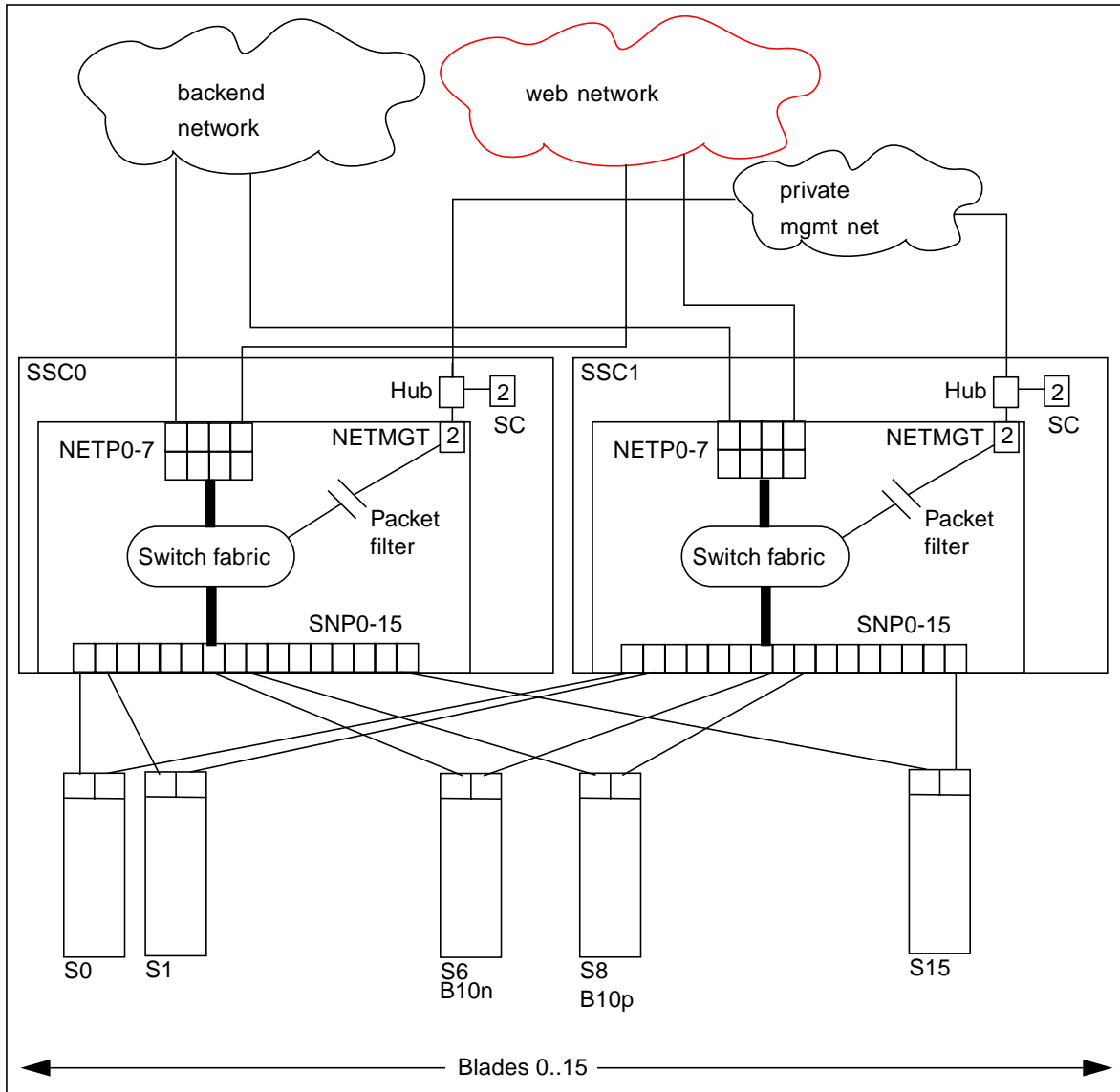


FIGURE 1-3 A Dedicated Management Network and Web Server Network Isolated from the Backend Network

The role of the B10n content load balancing blade is to present a set of highly available network services. These services can be transported over HTTP, HTTPS, TCP, or UDP, and are addressable through one or more virtual IP addresses (VIPs) that the content load balancing blade is responsible for:

- Providing one level of address indirection so that the number and nature of actual servers can transparently evolve over time
- Dividing requests among servers grouped in load balancing groups so that the total service demand can be satisfied through horizontal scaling
- Maintaining persistence for clients or groups of clients requesting services that require affinity, that is, services where multiple consecutive requests must be satisfied by the same server
- Delivering highly available services by taking responsibility for the failover functions that alter network paths, servers, and load balancer pairs upon service failure detection
- Associating VIPs to VLAN-based partitions are based on meaningful criteria (such as service owner and back-end network)
- Participating one or more SSL proxy blade in the request packet flow whenever SSL decryption is necessary

VIPs are the routable IP addresses that clients obtain for the service through DNS lookups. A VIP address is *owned* by one content load balancer at a given time. VIPs are preserved through the content load balancer all the way to servers. Requests are directed to servers by re-writing their MAC addresses and their VLAN tags (and optionally the TCP/UDP port values).

A service is identified by a 3-tuple comprising the VIP, the Layer 4 protocol value (TCP or UDP), and the TCP/UDP destination port. A multi-homed service can be associated with more than one 3-tuple.

Whenever any of the services involve HTTPS, the Sun Fire B10n content load balancing blade content is responsible for involving the Sun Fire B10p SSL proxy blade as described later in this chapter.

Topology Fundamentals

To match the ample switching capacity of the SSC units in the Sun Fire B1600 blade chassis, the content load balancer solution is designed to direct server responses toward clients without passing through the content load balancer. This enables the outbound capacity of the system to scale in proportion to the number of servers deployed, and to exploit the natural web traffic asymmetry where most of the traffic is server outbound. Equivalently, HTTPS responses are passed through a direct flow from servers to the SSL proxy and on to clients, without involving the content load balancer.

To combine the uncompromised Layer 7 service performance with the direct server response, the content load balancer and SSL proxy blades rely on a software module in each server. This server module contributes to the solution's high degree of integration by providing key attributes, for example, path failover functionality.

The Sun Fire B1600 blade system switches are separate networks, leaving the system designer the option to connect them externally and create a symmetrically configured redundant system where every blade is dual-homed, or to leave the switches segregated for a system where full redundancy is either not necessary (or achieved elsewhere in the system hierarchy), and blades are single-homed to separate networks. You can also create intermediate configurations where critical blades (content load balancers, proxies, and so on) reside on shelves with dual switches, but blade servers do not.

When you connect SSC switches to create redundant paths, it is best if:

- The interconnection occurs at the highest point in the network hierarchy.
- The internal fabric of one shelf is connected directly to the corresponding fabric of another shelf (that is, daisy chain SSC0 with SSC0 and SSC1 with SSC1, and connect these uplinks at an external distribution switch, if any).

The above connections help ensure that the SSC switches are indeed leaf switches within the network infrastructure, and enable the content load balancer to use the shortest path within the redundant fabric (that is, the path that involves only one fabric).

Additionally, given the ingress request interactions between content load balancing and their corresponding SSL proxy blade or blades, it is beneficial to place them in the same shelf to minimize switching hops.

FIGURE 1-4 illustrates nine shelves connected using a combination of distribution switches and internal SSC switches. Note that the SSC0 versus SSC1 fabric correspondence is preserved throughout the Layer 2 network, and that the fabrics are interconnected at the distribution switch level. In asymmetrical (capacity and hops) topologies like the one shown in FIGURE 1-4, it is also appropriate to house the content load balancing blades in shelves directly connected to the distribution switches.

Routers are shown for completeness as they represent the boundary of the Layer 2 network on the path towards the service clients.

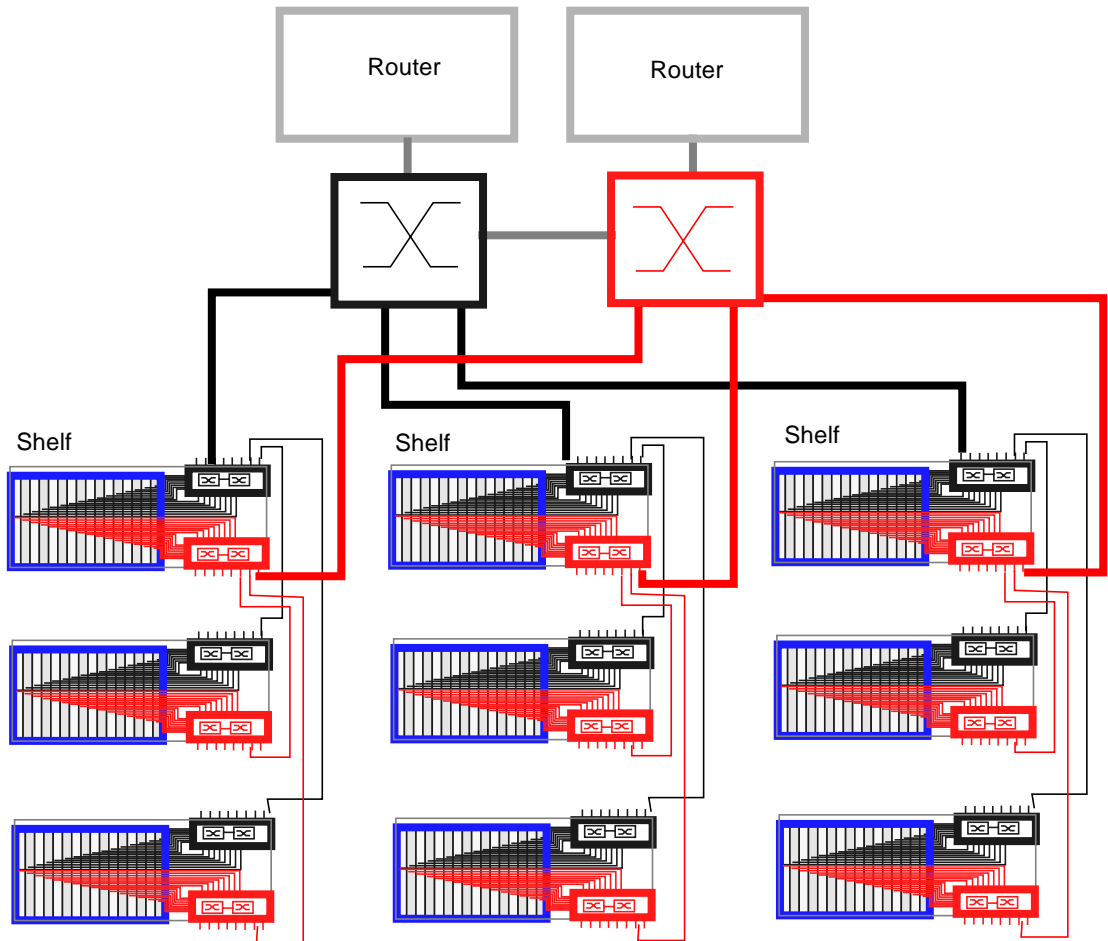


FIGURE 1-4 Dual Tree Using External and Internal Switches

The Role of the B10p SSL Proxy Blade

The Sun Fire B10p SSL proxy blade is a companion product to the Sun Fire B10n content load balancing blade, and the role of this blade is briefly described in this section. The SSL proxy blade performs the following:

- Consolidates and secures storage of server side certificates (servers remain stateless in terms of long-term secrets, and can be dynamically repurposed or replaced).
- Accelerates RSA transactions and bulk encryption and decryption.
- Enables the content load balancer to perform Layer 7 load balancing on cleartext (decrypted) cookies and URLs.

For every service, the content load balancer can be configured with one or more SSL proxy blades supporting the SSL sessions of the given service. SSL requests are delegated by the content load balancer and processed after decryption. Outbound data from servers are sent to the SSL proxy without going through the content load balancing blade.

The content load balancing blade, along with its server-side module, are responsible for the appropriate path selection, failover, and VLAN tag selection for SSL traffic. The following functions are provided:

- Secure traffic in cleartext form (after decryption or before encryption) is contained to a VLAN (if VLANs are enabled)
- Secure traffic in cleartext form (after decryption or before encryption) is contained to a single fabric (and to a single shelf if all participating blades are in the same shelf)

Failover Alternatives

The service availability obtainable from a given system is a function of the intrinsic failure rates of its components and the automatic failover capabilities of the system itself. A system designed around Sun Fire B1600 blade system product family has the following service failover aspects:

1. Server failover – The ability of any load balancer to remove non-responsive servers from service groups so that new requests go to functional servers. This capability is based on the server-monitoring function.
2. Path failover – The ability of the system to use an alternate network path whenever the current path does not appear to work, because of cable, switch, link, or end-point faults. This type of failover tends to be transparent, in the sense that session state at all endpoints is still valid and usable.
3. Blade failover – This is the ability to deploy content load balancing blades in high availability (HA) pairs that monitor each other. For a given service one of the load balancing blades is a standby blade, identically configured to the active blade, and responsible for taking over if the active blade fails. SSL blades do not monitor each other, and their failover is rather controlled by the load balancing blade monitoring them as if they were servers.

The system designer can decide which level of failover to design into the system:

- Server failover – always provided
- Path failover – possible whenever dual redundant switches are used; this failover is controlled by the content load balancing blade, by its server module, and by configuring Solaris IPMP on each server for server outbound path failover (towards the router)
- Blade failover – possible whenever content load balancing blades are deployed in pairs.

The Role of VLANs

The use of VLANs within the Sun Fire B1600 blade platform provides the ability to separate traffic into logical groups on the same Ethernet switch fabric. The use of VLANs is preferred for separation between data and management traffic and when using the Sun Fire B10p SSL proxy blade to create logical separation of client side traffic (between the specialty network blades and the switch uplinks) from the server side traffic (between the specialty network blades and the servers).

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 and they may either not be configured or they may be disabled. For the SSL proxy blades, VLANs are set to on by default, but they can be disabled with the `set vlan filter disable` command from the CLI interface. Refer to the *Sun Fire B10p SSL Proxy Blade Administration Guide*.

SSL proxy blades are configured to enforce the separation and direction of client side versus server side VLANs. The content load balancer and the SSL proxy blade cooperate to enforce the association between the operation performed (encryption versus decryption) with the allowed direction to and from the client VLAN.

Switches are responsible for VLAN separation enforcement, based on the VLAN identifiers present on Ethernet packets (explicitly or implicitly), as well as the physical ingress and egress switch ports involved.

The scope of the VLANs may be confined to the Sun Fire B1600 shelves while keeping all the uplinks VLAN untagged, or alternatively tagging may be enabled in the SSC uplinks to extend VLANs through the external switch infrastructure; in this case the VLAN ID assignment must be consistent with the external switch/router infrastructure VLAN assignments.

The minimal set of VLANs recommended for a proxy blade system are:

- Client side VLAN
- Server side VLAN

■ Management VLAN

TABLE 1-2 presents how the different VLAN assignments and the Sun Fire content load balancer and proxy blade duties accomplish the desired security outcome.

TABLE 1-2 VLAN Based Security

VLAN Involved	Requirement	Action
Management VLAN	<ul style="list-style-type: none"> • Confine the Sun Fire™ SSL proxy management to a management VLAN 	<ul style="list-style-type: none"> • Sun Fire SSL proxy only accepts management traffic on its management VLAN
Server side VLAN for secure traffic in its cleartext form	<ul style="list-style-type: none"> • Confine SSL traffic before encryption and after decryption to a VLAN 	<ul style="list-style-type: none"> • Server side VLANs configured at SSC for secure traffic includes just the relevant server(s), content load balancing blades, and SSL proxy blades. • Content load balancing blade responsible for transferring from client side VLAN to server side VLAN on ingress. • SSL proxy blade responsible for transferring from server side VLAN to client side VLAN on egress at encryption time. • Content load balancing module uses client side VLAN for cleartext egress traffic vs. server side VLAN for secure traffic in cleartext form.
Client side VLAN	<ul style="list-style-type: none"> • Prevent spoofing of traffic to be encrypted/decrypted 	<ul style="list-style-type: none"> • SSL proxy blade never encrypts/decrypts traffic arriving on client side VLAN.

The above actions, assigned to the different system components, must be complemented with the appropriate VLAN configuration at the SSC's and possibly other switches involved. The exact configuration scheme for the switches depends on how the uplinks are used and whether physical or VLAN separation is used.

VLANs can be extended to separate traffic for different user groups or tenants within the same Sun Fire B1600 blade platform.

In a multi-tenant environment it is appropriate to separate traffic based on the service 3-tuple. A VLAN identifier can be assigned by the SSL proxy blade to identify the tenant (that is, the service owner), and thus ensure that its requests can only go to the specified tenant servers. In combination with the server side VLAN configuration, you can use VLANs to separate:

- Blade servers of different tenants
- Different tiers of a tenant (web tier, application server, NFS, and management)
- Pre- and post-encryption traffic of an SSL service

System Integration

Although this book describes the administration of the Sun Fire B10p SSL proxy blades at the lowest possible level, you may want to approach system integration (that is, through CLI and scripting). It is certainly possible and desirable to achieve higher levels of integration abstraction with other Sun software products such as N1 deployment, and Sun ONE Web and Portal Servers.

User Access

Users must first log on to the command interface before access to any commands is allowed.

The SSL proxy blades support three access levels for initialization and configuration purposes. The three levels are: User, Administrator, and Security Officer (so), each with its own password. The privileges for each access level are described in the table below.

TABLE 1-3 User Privileges

Access Level	Command	Privileges
User	user	<ul style="list-style-type: none"> • Can only display certain system information. • Cannot change any system information or state of the SSL proxy blade
Administrator	admin	<ul style="list-style-type: none"> • All User privileges • Perform network administration • Manage services • Cannot manage keys or certificates. • Cannot backup and restore device configuration
Security Officer	so	<ul style="list-style-type: none"> • All User privileges • All Administrator privileges • Can perform initial setup. • Manage (add, delete) keys or certificates. • Can backup and restore device configuration.

The command descriptions (shown below) include the required access levels User, Administrator, or Security Officer for each command. Commands are not accessible if the access level of the command is higher than the access level of the logged in user.

Concurrent access to the SSL proxy blade is supported. Multiple users of any type can access the SSL proxy blade at a given time. This includes any combination of Telnet or console. The `who` and `write` commands, described below, can be used to arrange single so or admin access during delicate configuration tasks.

Installing the Blade and Setting Up the System

This chapter describes how to install the Sun Fire B10p SSL proxy blade hardware.

This chapter contains the following sections:

- “Installing the Blade” on page 19
- “Location of Ports” on page 24
- “Serial Port Pin Numbers” on page 26
- “Powering On the SSL Proxy Blade” on page 27
- “Powering Off the SSL Proxy Blade” on page 29
- “Upgrading the Sun Fire B10p SSL Proxy Blade Software” on page 31

Installing the Blade

The instructions in this section are specific to installing the Sun Fire B10p SSL proxy blades into the Sun Fire B1600 blade chassis. However, these instructions are general, so be sure to refer to the documentation that came with your Sun Fire B1600 blade chassis.

▼ To Install the Blade

Note – You must populate all 16 blade slots with either blades or filler panels before you apply power to the Sun Fire B1600 blade chassis. Do not leave any slots empty.

1. Remove the filler panel from an unpopulated slot in a Sun Fire B1600 blade chassis or other supported system.

Insert your finger in the pull recess located in lower portion of the filler panel lever and pull gently to disengage the locking mechanism (FIGURE 2-1).

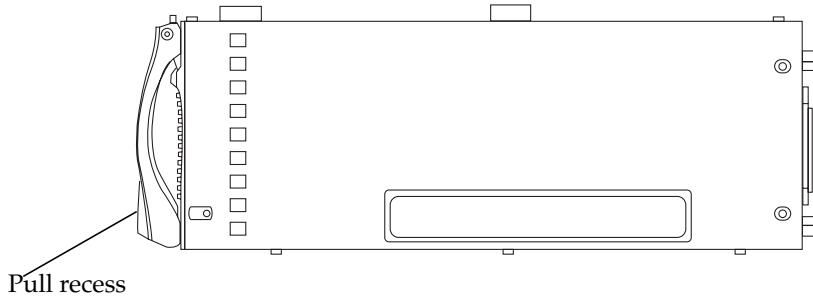


FIGURE 2-1 The Filler Panel Locking Mechanism

2. Pull the lever mechanism in a forward and upward motion, causing the filler panel lever to unlatch and eject the filler panel partially from the Sun Fire B1600 blade chassis (FIGURE 2-2).

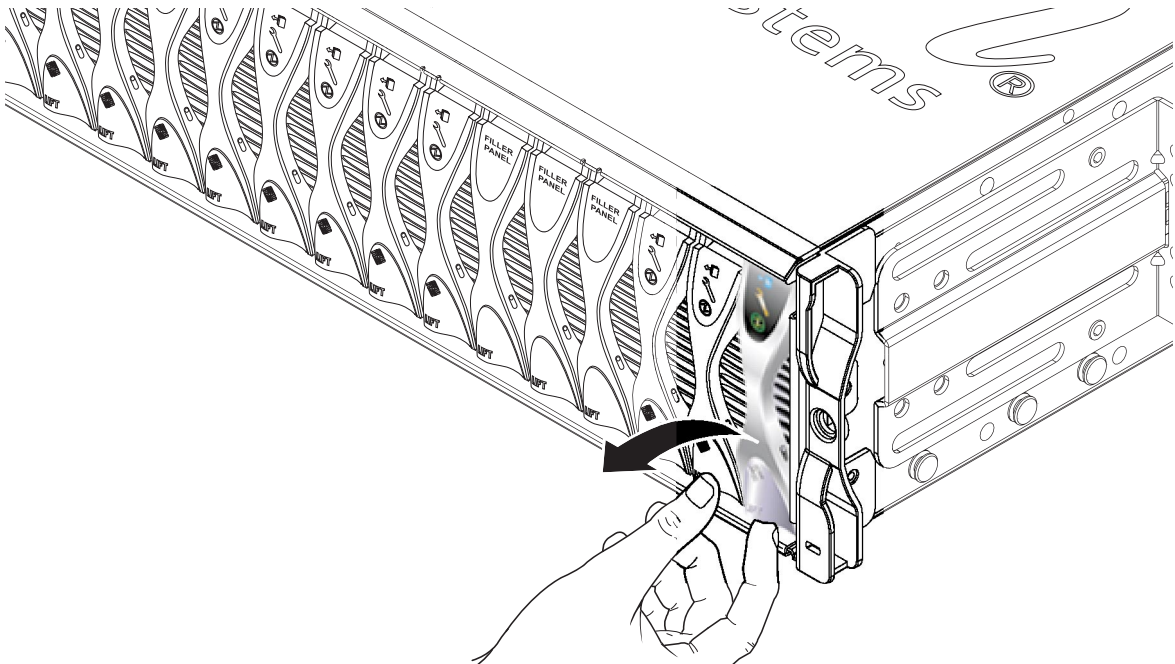


FIGURE 2-2 Disengaging the Blade-Locking Mechanism

3. Pull the lever to remove the filler panel from the Sun Fire B1600 blade chassis (FIGURE 2-3).

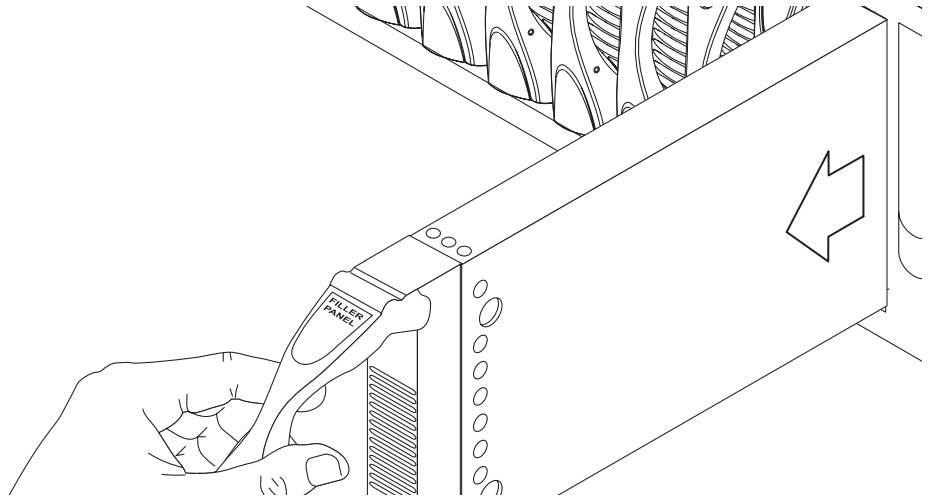


FIGURE 2-3 Removing the Filler Panel

4. If required, open the blade lever by inserting a finger in the pull recess located in lower portion of the blade lever and pull the lever mechanism in a forward and upward motion, causing the lever to unlatch (FIGURE 2-4).

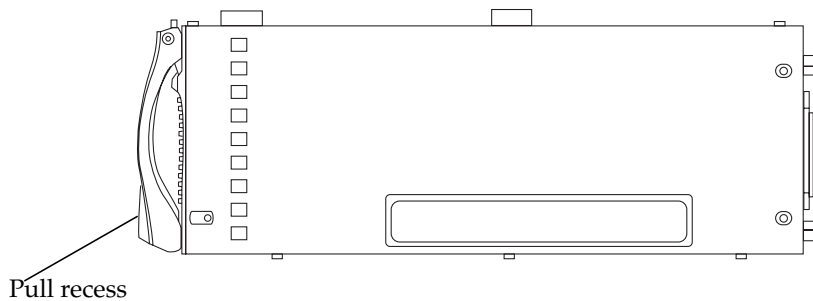


FIGURE 2-4 Blade Locking Mechanism

5. Align the Sun Fire B10p SSL proxy blade with an empty slot in the Sun Fire B1600 blade chassis.

Ensure that the blade connector is facing towards the Sun Fire B1600 blade chassis, with the hinge point of the lever mechanism uppermost. Support the bottom of the blade with your free hand while lifting the blade up to the Sun Fire B1600 blade chassis (FIGURE 2-5).

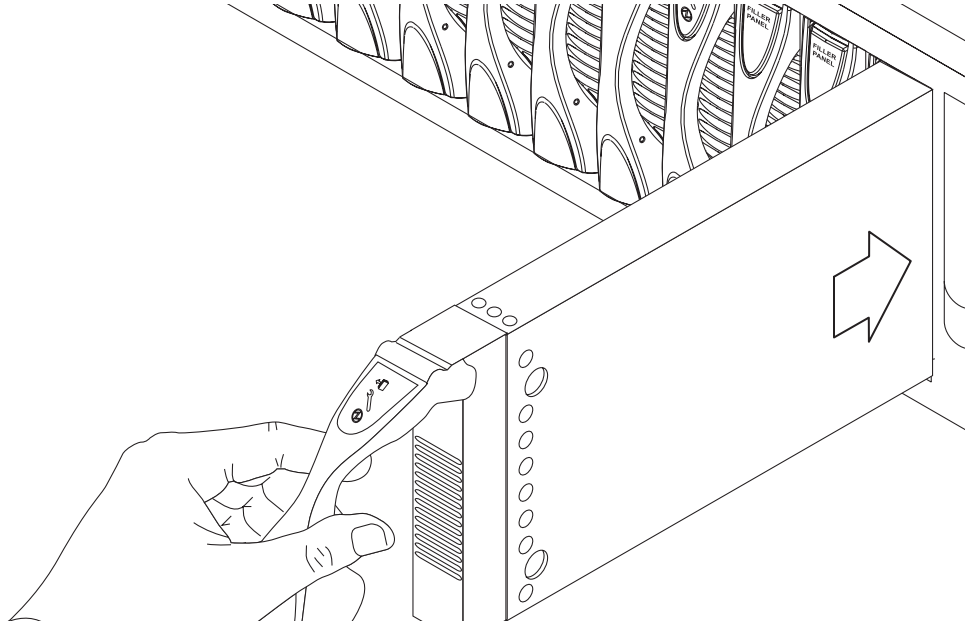


FIGURE 2-5 Aligning and Inserting the Blade

6. Insert the SSL proxy blade into the system.

Caution – Ensure that the blade engages with the Sun Fire B1600 blade chassis guidance system. Failure to align the blade correctly can result in damage to the Sun Fire B1600 blade chassis midplane or the blade connection.

7. Gently push the blade into the slot until the blade latch ears, on top of the lever, are positioned in the Sun Fire B1600 blade chassis (FIGURE 2-6).

8. Complete the blade installation by closing the blade lever fully, which engages the blade into the Sun Fire B1600 blade chassis slot (FIGURE 2-6).

The green LED flashes as the blade powers up, and glows steadily when the blade is up and running.

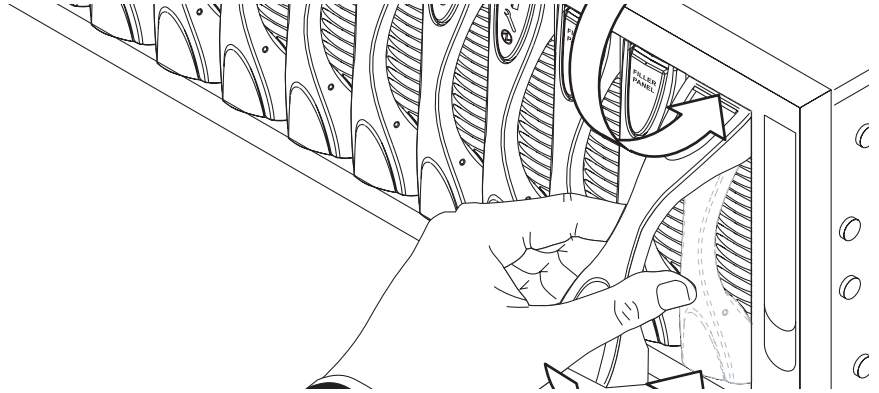


FIGURE 2-6 Closing the Blade Lever Mechanism

LED Displays

Use the LEDs on the individual system components to determine if the system is operating normally. Monitor LEDs routinely on the:




- Power supplies
- Server blades

The LEDs can be off, on, or flashing. When the fault LED is on (lit), this indicates that a fault has occurred in the component. A fault is any condition that is considered to be unacceptable for normal operation. When the fault LED is lit, you must take immediate action to clear the fault. You can only remove a hot-swappable component when the blue Removal OK LED is lit.

TABLE 2-1 lists the LED status codes for the following hot-swappable components:

- Blade
- Power supply

TABLE 2-1 Blade and Power Supply Status Codes

Power (Green)	Fault (Amber)	OK to Remove (Blue)	Indication	Corrective Action
				
Off	Off	Off	Component not operating. Fault condition unknown.	You can remove a component from the system.
Off	On	Off	Component not operating. Fault condition present.	You cannot remove a component from the system.
Off	Off	On	Component not operating. No fault condition present.	You can remove a component from the system.
Off	On	On	Component not operating. Fault condition unknown.	You can remove a component from the system.
On	Off	Off	Normal component operation.	N/A
On	Off	On	Component not operating. No fault condition present.	You can remove a component from the system.
On	On	Off	Component operating. Fault condition present.	You cannot remove a component from the system.
On	On	On	Component operating. Fault condition present.	You can remove a component from the system.
Flashing	Off	Off	Component is powering up.	N/A

Location of Ports

All ports are located at the back of the Sun Fire B1600 blade chassis. These connections are shown in FIGURE 2-7.

Note the location of the following ports:

- 10/100BASE-T network management ports
- 10/100/1000BASE-T data network ports
- RS232 serial ports

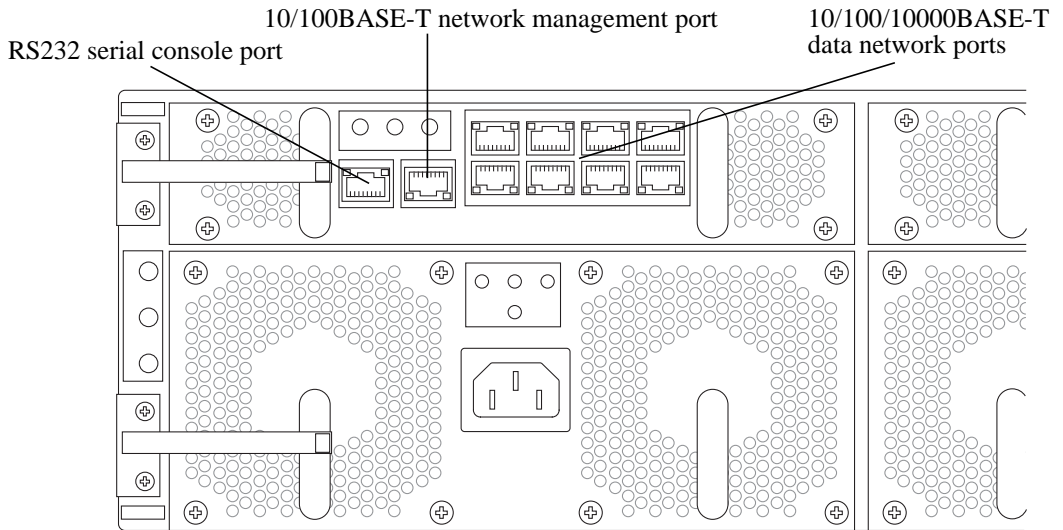


FIGURE 2-7 External Cable Connections



Caution – Do not connect a telephone jack connector to any RJ-45 port. This can damage the switch. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards, or local national wiring or electrical regulations.

Note – Twisted-pair cables must not exceed 328 feet (100 meters).

Connecting to the 10/100/1000BASE-T Data Network Ports

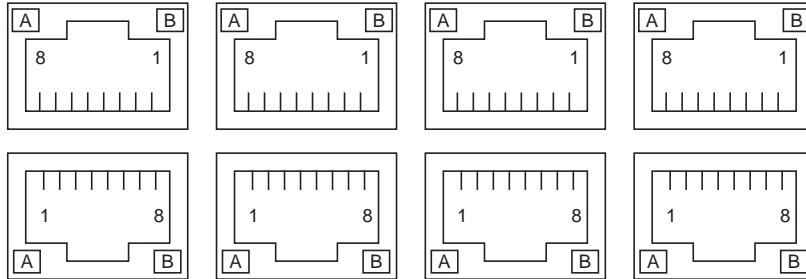


FIGURE 2-8 10/100/1000BASE-T Data Network Ports

Arranged as a 4x2 array, these RJ-45 ports provide the connection to the Combined Switch and Service Processor (CSSP). Each port has integral green Link Present and Link Active LED indicators.

Note – The Link Present indicator is always on the left, regardless of the orientation of the RJ-45 port.

TABLE 2-2 10/100/1000BASE-T Data Network Port Pinouts

Pin 1	Pin 2	TRD0-
Pin 3	Pin 4	TRD2+
Pin 5	Pin 6	TRD1-
Pin 7	Pin 8	TRD3-
LED A	LED B	Link Active

Serial Port Pin Numbers

Viewing the Sun Fire B1600 blade chassis from the back, pin 1 of the RJ-45 serial port is on the left, and pin 8 is on the right.

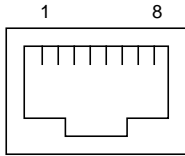


FIGURE 2-9 Serial Port Pin Numbers

TABLE 2-3 Serial Port Pinouts

Pin Number on Sun Fire B1600 Blade Chassis	Signal
Pin 1	RTS
Pin 2	DTR
Pin 3	TXD
Pin 4	Signal Ground
Pin 5	Signal Ground
Pin 6	RXD
Pin 7	DSR
Pin 8	CTS

Powering On the SSL Proxy Blade

Note – To power on any server blade, you must have access to the system controller and r-level user permission. Refer to the *Sun Fire B1600 Blade System Chassis Administration Guide* for information on system controller user permissions.

- To power on a single blade, type:

```
sc> poweron Sn
```

Where S indicates the slot and *n* is the number of the slot containing the blade you want to power on. Valid slot numbers range from 0 to 15.

- To power on more than one blade, specify each blade in a space-separated list as in the following example:

```
sc> poweron S6 S11
```

- Use the `showplatform` command to verify the status of the SSL blade:

```
sc> showplatform

FRU           Status           Type
-----
S0            OK               SF B100s
S1            OK               SF B100s
S2            OK               SF B100s
S3            OK               SF B100s
S4            Not Present     ***
S5            Not Present     ***
S6            Not Present     ***
S7            Not Present     ***
S8            Not Present     ***
S9            Not Present     ***
S10           Not Present     ***
S11           Not Present     ***
S12           Not Present     ***
S13           Not Present     ***
S14           OK               SF B10p
S15           OK               SF B10p
SSC0          OK               SF B1600 SSC
SSC0/SC
SSC0/SWT
SSC1          Not Present     ***
SSC1/SC
SSC1/SWT
PS0           OK               SF B1600 PSU
PS1           OK               SF B1600 PSU
CH            OK               SF B1600

Domain        Status
-----
S0            OS Running
S1            OS Running
S2            OS Running
S3            OS Running
S14           OS Running
S15           OS Running
SSC0/SWT     OS Running
SSC0/SC      OS Running (Active)
```

Note – Slots 14 and 15 show that the B10p SSL proxy blade is OK.

Powering Off the SSL Proxy Blade

Note – To power off any server blade, you must have r-level user permission. Refer to the *Sun Fire B1600 Blade System Chassis Administration Guide* for information on system controller user permissions.

Note – The various options referred to in this section for use with the `poweroff` command can all be used on the same command-line except for the `-r` and `-s` commands. These two commands are alternatives to each other.

Powering Off With an Orderly Shut Down of the SSL Software

The `poweroff` command attempts to shut down the operating system on a blade or blades in an orderly fashion. The command also prompts you to confirm that you intend to shut down the blade or blades you have specified.

- To `poweroff` a single blade, type:

```
sc> poweroff $n
```

Where *n* is the number of the slot containing the blade you want to power off.

- To `poweroff` more than one blade, specify each blade in a space-separated list, as in the following example:

```
sc> poweroff $6 $11
```

▼ Forcing the Power Off

The `poweroff` command attempts to shut down the SSL software on a SSL proxy blade in an orderly fashion. If this orderly shut down fails on a particular server blade, the `poweroff` command will not continue to power off the server blade.

- To force the SSL proxy blade to power off even if an orderly shut down has failed, include the `-f` option on the command-line, as in the following example:

```
sc> poweroff -f S6
```

▼ Powering Off an SSL Proxy Blade Without Requiring the Confirmation Prompt

When you run the `poweroff` command to power off a blade, you are prompted to confirm that you intend to power off the blade you have specified.

- To avoid receiving the confirmation prompt when you use the `poweroff` command, include the `-y` option on the command-line.

For example:

```
sc> poweroff -y S6 S11
```

▼ Powering an SSL Proxy Blade Down to Standby Mode to Save Power

There are two ways to power a blade down to standby mode. You can use either the `standbyfru` command or the `poweroff` command.

- To power down a blade or blades to standby mode using the `poweroff` command, type:

```
sc> poweroff -s Sn
```

Where *n* is the number of the slot containing the blade you want to power down. When a blade is in standby mode, the system service processor continues to monitor its operational state.

▼ Powering Off an SSL Proxy Blade Before Removal

- To power down a blade for removal, type:

```
sc> poweroff -r Sn
```

Where *n* is the number of the slot containing the blade you want to power down. When a server blade is powered off for removal, the OK to Remove LED is lit.

Note – You cannot use the `-s` option on the same command line as the `-r` option.

Upgrading the Sun Fire B10p SSL Proxy Blade Software

If upgrading your software, please export any configurations, keys, and certificates first or you may lose this information after the software upgrade. See Chapter 6 for details on how to upgrade the software.

Initial Configuration

This chapter describes the steps required to initialize and configure an SSL proxy blade for use in a network environment. This setup procedure assumes that the SSL proxy blade has already been installed according to the previous installation instructions and all relevant network cables are connected.

This chapter contains the following sections:

- “Initializing the SSL Proxy Blade” on page 33
- “To Initialize the SSL Proxy Blade” on page 34
- “To Create Keys and Certificates” on page 37
- “To Create Services for the Servers” on page 38
- “To Verify and Save the Configuration” on page 39

Initializing the SSL Proxy Blade

To use the SSL proxy blade, it must be initialized with required information using the blade console, which is accessible through the Sun Fire B1600 system controller. Once the SSL proxy blade has been initially configured, it can be managed through Telnet.

▼ To Initialize the SSL Proxy Blade

1. Gather the required information.

When the SSL proxy blade is powered on for the first time, you must set the values for the parameters listed in TABLE 3-1 before the device can operate correctly. Use the empty value column as a worksheet.

TABLE 3-1 Worksheet of Values for the SSL Proxy Blade Initialization

Parameter Name	Default	Value	Description
Name	SSL proxy blade		Name for the SSL proxy blade for administration purposes.
Management (admin) IP address	0.0.0.0		IP address for administration by means of Telnet.
Administration port netmask	255.255.255.0		Netmask for the local administration subnet.
Default gateway	0.0.0.0		IP address of the gateway in the local subnet.
Security officer password	so		Initial security officer password. Should be changed by the security officer.
Management VLAN	0		This parameter must be set based on your network setup.
Traffic ports			
Secure/clear portpair	443/880		TCP port numbers for secure/clear client traffic.
Certificates	none		If you have no certificates, then you can create a key and generate a signing request. For simplicity, in this setup we will create a self-signed certificate.
Keys	none		RSA private key that can be used to generate a certificate request or a self-signed certificate.
Services IP addresses	none		Each service supports a server. To set up the services, you need the IP address of each HTTP server for which the SSL proxy blade should process SSL traffic.

2. Set up the SSL proxy blade.

a. Log on to the SSL proxy blade.

When the SSL Proxy blade console is accessed, the `Login:` prompt displays after the boot process completes.

```
# telnet B1600_sc_ip-addr
sc> console sn
Login: so
Password:
```

Where n is the slot number for the SSL proxy blade.

Note – For initial setup you must be logged in as the security officer (so).

After validating the user and password the command prompt should now be displayed: `CLI#`

b. Change the security officer password with the command:

```
CLI# set password
```

For more information about user access and privileges see the “User Access” on page 60.

c. Run the setup command.

After logging in for the first time you need to run the `setup` command before setting any configuration information. The `setup` command prompts you for the required information listed above.

```
CLI# setup
Enter secure port (https) (443):
Enter clear port (http) (880):

Change the password:
Enter login password:
Enter new password:
Re-enter new password:
Password changed.
    Setup has completed successfully.
    You should add keys and services to complete the configuration.
    To save the configuration enter: config save
CLI#
```

The `setup` command configures the blade for the first time. You can use specific commands to change the initial parameters later.

3. Verify that the blade is connected.

a. To verify connectivity, ping any host on the same subnet from the SSL proxy blade. The ping should report the host to be alive.

```
CLI# ping ip-addr
PING 192.50.50.11 from 192.100.100.205: 56 data bytes
64 bytes from 192.50.50.11: icmp_seq=0 ttl=255 time=0 ms

--- ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
    host is alive.
CLI#
```

Note – In the previous command the IP address (*ip-addr*) must be entered as a numeric IP address and not a hostname.

b. To verify Telnet, use Telnet to connect to the SSL proxy blade.

This option allows you to continue the setup process from a local area network

▼ To Create Keys and Certificates

Before the SSL proxy blade can process SSL traffic, the keys and certificates must be installed.

See “Keys and Certificates” on page 81 for more information on the `import` and `create` commands.

1. Create a key.

```
CLI# create key keyname
Enter key strength (1024): 512|1024|2048
Key keyname generated.
```

2. Create a certificate.

You may create a self-signed certificate for a temporary certificate used for testing purposes.

```
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.
```

Or, you may create a certificate signed by a certificate authority.

```
CLI# create certrequest
Enter key name: previously_created_keyname
Enter country (US):
Enter state or province (CA):
Enter locality (Company Town):
Enter common name (www.companyname.com):
Enter organization (Company Name):
Enter organization unit (Company Unit):
Enter email address (support@company-name.com):
Certificate signing request previously_created_keyname generated.
```

3. Hand off this certificate request to a certificate authority. Use this certificate authority to generate the certificate. After receiving the signed certificate from the certificate authority, use the following `import certificate` command or `import ftp|tftp certificate` commands to import the certificate into the system.

```
CLI# import certificate
```

▼ To Create Services for the Servers

After the certificates have been installed, you can create services for each server. The services enable the SSL proxy blade to process SSL traffic.

- Create a service:

```
CLI# create service
Enter service name: new_servicename
Enter key name: keyname
Enter server IP Address: (0.0.0.0): server_ip-addr
Enter cipher (export/best/optional/high/medium/low) (best): cipher
Enter portpair number (1..4) (1): 1
Service new_servicename created.
```

See “Services” on page 96 for a full explanation of service settings.

▼ To Verify and Save the Configuration

1. Use the `show config` or `show all` commands to display the current SSL proxy blade configuration.

```
CLI# show all
  port 1:
    management (admin) IP:      192.50.50.205
    management (admin) netmask: 255.255.255.0
    management (admin) gateway: 0.0.0.0
  port 2:
    management (admin) IP:      0.0.0.0
    management (admin) netmask: 255.255.255.0
    management (admin) gateway: 0.0.0.0
  ... ..
portpair 1:
  secure port:      443
  clear port:       880
portpair 2:
  secure port:      0
  clear port:       0
portpair 3:
  secure port:      0
  clear port:       0
portpair 4:
  secure port:      0
  clear port:       0
  ... ..
CLI#
```

Other configuration information can be displayed using the commands described in TABLE 3-2.

2. Save the configuration as permanent.

```
CLI# config save
```

When you log out you will be reminded if the configuration has not been saved and given an option to cancel the logout. Configuration changes that are not saved will be lost if the SSL proxy blade is rebooted. The command `config compare` can determine if the configuration in memory is different than the permanent configuration stored in flash.

3. Verify and start processing.

Note – Browsers have preloaded recognized CA certificates. Thus, with self-signed certificates as used in this example, a browser will not recognize the CA and issues a warning.

a. Perform diagnostics (if required).

- The `show version` and `show features` commands display information about the SSL proxy blade version and enabled capabilities, respectively. This information identifies the exact SSL proxy blade version and model. The `show boot` command displays the version of internal hardware/software components and is provided for diagnostic purposes.
- Use the `show log` command and the associated `set log` command to generate run time logs that monitor system operations. The log output can be directed to internal or external destinations. The log contains information about administration and other system events. Use the `show log` command to see the current log configuration and `export log` to view the contents of the logs.

See “Event Logging Commands” on page 104 for more details.

- The `show stats` command displays various system statistics. This is useful to determine the patterns of client traffic for your SSL proxy blade. This information helps you fine tune the configuration or to plan for timely upgrades. See “Statistics” on page 101 for details.

b. Use the following CLI# commands to display important information about the SSL proxy blade configuration.

TABLE 3-2 Commands to Display Configuration Information

Command	Description
<code>show portpair</code>	Shows all TCP port settings
<code>show all</code>	Shows all system information
<code>show config</code>	Shows all system information
<code>show snmp</code>	Shows the SNMP agent
<code>show service</code>	Shows all current services
<code>show log</code>	Shows logging config. information
<code>show stats</code>	Shows statistics
<code>show features</code>	Shows software license information
<code>show version</code>	Shows software version
<code>show boot</code>	Shows release version information
<code>show state</code>	Shows various system settings
<code>show link</code>	Shows inband port link settings
<code>show interface</code>	Shows inband interface settings

These and other show commands are described in detail in Appendix G.

c. Start processing.

After adding certificates, services, and configuring the Sun Fire B10n content load balancing blade, you can start the SSL proxy blade using the **start** command. The `start` command is used to start the SSL proxy blade processing SSL traffic.

```
CLI# start
```

4. Exit the CLI interface.

After the setup process is finished, and the SSL proxy blade is successfully processing traffic, use the `logout` command to exit the command-line interface.

Setting Up Sun Fire Blades for Load Balancing SSL Traffic

This chapter 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.

This chapter includes the following sections:

- “Setting Up for Load Balancing SSL Traffic” on page 43
- “Setting Up the Sun Fire B10n Content Load Balancing Blade” on page 44
- “Setting Up the SSL Proxy Blade” on page 48
- “Setting Up the Router” on page 53
- “Setting Up the Sun Fire B1600 Switch” on page 54
- “Setting Up Sun Fire B100s Solaris Server Blades” on page 57
- “Setting Up Clients/External Routers” on page 58

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
- Sun Fire B1600 blade chassis
- Server blades
- Clients/External routers

In addition to modifying these components, you must set up three VLANs:

- Data/client VLAN for security.

- Management VLAN for separation of management traffic. Heartbeat messages between the load balancing blade, the server blades and the SSL proxy blade are on this VLAN.
- Service VLAN for tenant separation. Service related traffic between the load balancing blade and the server blades is on this VLAN.

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 and VLAN

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
```

2. Set the data/client VLAN:

```
puma{admin}# config data vlan N
```

Where *N* is the number of the data/client VLAN.

Example:

```
puma{admin}# config data vlan 10
```


3. Enable the data/client VLAN:

```
puma{admin}# config enable vlan data
```

4. Set the management VLAN:

```
puma{admin}# config management vlan N
```

Example:

```
puma{admin}# config management vlan 3
```

5. Enable the management VLAN:

```
puma{admin}# config enable vlan management
```

▼ 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. Set the service VLAN

```
puma{admin}# config service vlan svc1 vlan N
```

Where *N* is the VLAN ID number.

The B10n content load balancing blade will tag all traffic from this service, destined to the server blades with the VLAN ID number specified here when VLAN is enabled on the service.

Example:

```
puma{admin}# config service vlan svc1 vlan 5
```

5. Enable VLAN tagging for the service.

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

6. Enable the service `svcl` on the B10n content load balancing blade:

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

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

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

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.

7. Set the client VLAN:

```
CLI# set vlan client #
```

Note – This is the VLAN on which all SSL encrypted traffic (to be load balanced) from the client is sent. The value must also correspond to that set on the B10n content load balancing blade with the `config data vlan` command.

Example:

```
CLI# set vlan client 10
```

8. Set the management VLAN on port 1:

```
CLI# set vlan management

Enter port number (1..2) (1): 1
Enter management vlan tag (admin) (0..4095): 3
```

Note – This is the VLAN (3 in this example) on which all the management traffic from the SSL proxy blade is sent (that is, for FTP, export, health checks towards the inbound router, and such). The value must correspond to that set on the B10n content load balancing blade with the `config management vlan` command.

9. Set the inband (data) VLAN on port 1:

```
CLI# set vlan inband

Enter port number (1..2) (1): 1
Enter management vlan tag (0..4095): 10
```

Note – This is the VLAN (10 in this example) on which all health check traffic towards the outbound router is sent out. Its value should correspond to that used in the `set vlan client` command on the SSL proxy blade.

10. Enable the VLAN filtering on the SSL proxy blade:

```
CLI# set vlan filter enable
```

For a B10n content load balancing blade with an SSL proxy blade, the VLAN filter must be enabled. This means that the SSL proxy blade will not process any incoming traffic on the client VLAN (10 in this example). This filtering is a security measure on the SSL proxy blade.

11. 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.

12. Create a service svcl on the SSL proxy with the key key1 associated with it:

```
CLI# create service

Enter service name: svcl
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 svcl 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.

13. 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. **On the client/data VLAN, 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 an interface on a client VLAN of 10.

```
# ifconfig ce10000 addif 192.100.100.254 netmask 255.255.255.0 broadcast +up
```

2. **On the client/data VLAN, 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 on a client VLAN of 10.

```
# ifconfig ce10000 addif 110.10.10.254 netmask 255.255.255.0 broadcast +up
```

3. **On the client/data VLAN, 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 on a client VLAN of 10, for clients/external routers in the 199.99.9.0 subnet.

```
# ifconfig ce10000 addif 199.99.9.254 netmask 255.255.255.0 broadcast +up
```

Setting Up the Sun Fire B1600 Switch

▼ To Get to the Sun Fire B1600 Switch Console

1. If you are not already logged into the switch, 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 switch console:

```
sc0> console ssc0/swt
```

▼ To Set Up the Sun Fire B1600 Switch

1. Configure the VLAN database:

```
Console# configure vlan database  
Console(config-vlan)#
```

2. Create the management VLAN (3 in this example):

```
Console(config-vlan)# vlan 3 name mgmt-vlan media ethernet
```

3. Create the client/data on VLAN (10 in this example):

```
Console(config-vlan)# vlan 10 name client-vlan media ethernet
```

4. Create the service VLAN (5 in this example):

```
Console(config-vlan)# vlan 5 name service-vlan media ethernet
```

5. Exit to the console prompt:

```
Console(config-vlan)# exit
Console#
```

▼ To Create VLANs

1. Configure a slot for the B10n content load balancing blade to allow the management, client, and service VLANs:

```
Console# configure
Console(config)# interface ethernet SNP13
Console(config-if)#
Console(config-if)# switchport allowed vlan add 3 tagged
Console(config-if)# switchport allowed vlan add 10 tagged
Console(config-if)# switchport allowed vlan add 5 tagged
```

Where SNP is the internal port and 13 is the slot number in which the B10n content load balancing blade is located.

2. Configure a slot for the SSL proxy blade to allow the management, client and service VLAN.:

```
Console# configure
Console(config)# interface ethernet SNP15
Console(config-if)#
Console(config-if)# switchport allowed vlan add 3 tagged
Console(config-if)# switchport allowed vlan add 10 tagged
Console(config-if)# switchport allowed vlan add 5 tagged
```

Where SNP is the internal port and 15 is the slot number in which the SSL proxy blade is located.

3. Configure slots for server blades to allow the management, client, and service VLANs:

```
Console# configure
Console(config)# interface ethernet SNP10
Console(config-if)#
Console(config-if)# switchport allowed vlan add 3 tagged
Console(config-if)# switchport allowed vlan add 10 tagged
Console(config-if)# switchport allowed vlan add 5 tagged
```

Where SNP is the internal port and 10 is the slot number in which the server blade is located.

4. Configure uplink slot with Router to allow the management and client VLANs.

```
Console# configure
Console(config)# interface ethernet NETP7
Console(config-if)#
Console(config-if)# switchport allowed vlan add 3 tagged
Console(config-if)# switchport allowed vlan add 10 tagged
```

Where NETP is the uplink port and 7 is the uplink port number to which the router is connected.

5. Configure uplink slots with clients/external routers to allow the management and client VLANs.

```
Console# configure
Console(config)# interface ethernet NETP5
Console(config-if)#
Console(config-if)# switchport allowed vlan add 3 tagged
Console(config-if)# switchport allowed vlan add 10 tagged
```

Where NETP is the uplink port and 5 is the uplink port number to which a client/external router is connected.

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 on the management VLAN (3 in this example):

```
# ifconfig ce3000 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 any (unique) IP on the service VLAN (5 in this example):

```
# ifconfig ce5000 plumb 0.0.0.0 netmask 255.255.255.0 up
```

4. Configure IP on the client/data VLAN (10 in this example) to reach the clients through the router:

```
# ifconfig ce10000 plumb 192.100.100.10 netmask 255.255.255.0 up
```

5. Configure the VIPs on the loopback interface, for example:

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

6. Add the interfaces to the `clbmod`:

```
# /opt/SUNWclb/bin/clbconfig add ce3000
# /opt/SUNWclb/bin/clbconfig add ce5000
# /opt/SUNWclb/bin/clbconfig add ce10000
```

Add `ce3000`, `ce5000`, `ce10000` to `/etc/opt/SUNWclb/clb.conf`, one on each line, to automatically add the interfaces to `clbmod` across reboots.

7. Check the interfaces on which the module is plumbed:

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

8. Make sure the Sun Fire B100s solaris server blade is not routing, that is, `/etc/notrouter` file should be present.
9. Configure your web server to listen on the decrypted port, that is, 880 in this example.
10. 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 VLAN (10 in this example) with the target address specified as the client side interface on the router as specified in section “Setting Up the Router” on page 53.

Example:

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

```
# ifconfig ce10000 plumb 199.99.9.101 netmask 255.255.255.0 broadcast + up
```

This command configures a `ce0` interface on VLAN 10 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 53.

```
# 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 53.

Command-Line Interface

The command-line interface (CLI) for the Sun Fire B10p SSL proxy blade is used for viewing and configuring information and statistics. The interface is accessible by using the `console` command from the Sun Fire B1600 service controller command-line (`sc>`). See the *Sun Fire B1600 Blade System Chassis Software Setup Guide* section 1.5 for details on connecting to the service controller. This provides a good framework to present all commands and their relationship to each other. In Appendix G, the commands are listed alphabetically.

This chapter contains the following sections:

- “Command-Line Interface Basics” on page 59
- “User Access” on page 60
- “SSL Traffic Commands” on page 70
- “Network Interfaces” on page 75
- “Configuration Storage” on page 76
- “Keys and Certificates” on page 81
- “Certificate Management Commands” on page 86
- “Services” on page 96
- “Diagnostics” on page 100
- “Statistics” on page 101
- “Event Logging Commands” on page 104
- “SNMP Commands” on page 110

Command-Line Interface Basics

Commands are organized by function using a hierarchy of menus. Each menu supports its own set of commands, prompt, and help messages. The main (`root`) menu is the first menu accessible to the operator. Depending on the operator’s access level different menus and commands are available and displayed.

Parameters to commands can be entered directly on the command line or be entered by the operator when prompted for the input. Some commands do not accept command-line parameters and will prompt for all input (for example, `set management`). Default values for prompts are set whenever possible and can be entered by hitting the Return or Enter key. The "." character can be used to cancel the current command.

Operator-specified names must be 32 characters or less, alphanumeric, and may contain spaces.

The command-line interface supports features such as automatic command completion, history, context-sensitive help, and other editing commands and shortcuts. For example, the command to create a key can be entered as either `create key` or `cr k` (or by as few characters as necessary to avoid conflict). The `logout` command must be entered in full to avoid conflict with the `log` command.

The following two command sequences are equivalent.

```
CLI# create key keyname 1024
```

or

```
CLI# create  
CLI(create)# key  
Enter key name: keyname  
Enter key strength(1024): 1024
```

Note – Enter `?` or `help` to see a list of available commands and context-sensitive help.

User Access

Users must first log on to the command interface before access to any commands is allowed.

The SSL proxy blade supports three access levels for initialization and configuration purposes. The three levels are: User, Administrator, and Security Officer, each with its own password. The privileges for each access level are described in the table below.

TABLE 5-1 User Privileges

Access Level	Command	Privileges
User	user	Can only display certain system information. Cannot change any system information or state of the SSL proxy blade.
Administrator	admin	All User privileges. Perform network administration. Manage services. Cannot manage keys or certificates. Cannot backup and restore device configuration.
Security Officer	so	All User privileges. All Administrator privileges. Can perform initial setup. Manage (add, delete) keys or certificates. Can backup and restore device configuration.

The following command descriptions include the required access levels (User, Administrator, or Security Officer) for each command. Commands are not accessible if the access level of the command is higher than the access level of the logged in user.

Concurrent access to the SSL proxy blade is supported. Multiple users of any type can access the SSL proxy blade at a given time. This includes any combination of Telnet or console. The `who` and `write` commands arrange single Security Officer or Administrator access during delicate configuration tasks.

User Access Commands

The CLI enables operators to log on, log off, change operator password, and write to other users who are currently logged on.

TABLE 5-2 User Access Commands

Syntax	Access Level	Description
login	User Administrator Security Officer	Initiates access to the CLI.
logout	User Administrator Security Officer	Issues the following reminders: 1. Reminder to save the configuration. 2. Reminder to set auto-run to true, if false. 3. Reminder to issue <code>start</code> command, if the SSL proxy blade is stopped. The normal SSL proxy blade state during operation should be: Configuration saved, SSL processing ON, and Watchdog fully enabled by <code>autorun=enable</code> .
set password	User Administrator Security Officer	Enables current users to change their password.

Concurrent User Commands

TABLE 5-3 Concurrent User Commands

Syntax	Access Level	Description
who	User Administrator Security Officer	Displays all users currently logged in for administration.
<i>write user message</i>	User Administrator Security Officer	Inter-user communication. A message sent to multiple users with the same login is delivered to only one of them.

Concurrent User Examples

All commands are typed at the CLI# prompt.

For example, for the who command:

```
CLI# who
so console
user 254.163.1.9
user 254.163.1.11
```

Following is an example using the write command:

```
CLI# write user "Please log out now."
```

Global Commands

The following commands can be entered from within any menu.

TABLE 5-4 Global Commands

Syntax	Access Level	Description
start	User Administrator Security Officer	Start SSL processing.
stop	User Administrator Security Officer	Stop SSL processing.
reboot	User Administrator Security Officer	Reboot the system.
alias <i>token message</i>	User Administrator Security Officer	Provides command-line text substitution for the current user session. Aliases are only valid for full commands and are not valid for use as input when the operator is prompted for input. Up to 32 aliases can be defined. Aliases are not saved across reboots. Note: Use quotes for aliases that contain spaces.
clear	User Administrator Security Officer	Clear the screen.

TABLE 5-4 Global Commands (Continued)

Syntax	Access Level	Description
exit	User Administrator Security Officer	Go up one menu level (or to root menu).
history	User Administrator Security Officer	Provides a numbered list of the last 10 commands. To recall a command, use exclamation mark and the command number in the list, for example, CLI# !3.
date	User Administrator Security Officer	Displays the current time. Note that 'show date' is not a command.
show ntp	Administrator Security Officer	Shows NTP settings
set ntp	Administrator Security Officer	Sets NTP settings.* Port 123 is standard for NTP.
show config	Administrator Security Officer	Displays the system configuration information.
logout	User Administrator Security Officer	Log off this system
who	Administrator Security Officer	Display users currently logged in
write	Administrator Security Officer	Write text to another user
? or help	User Administrator Security Officer	Provides context-sensitive help about the commands and parameters in the current menu.

* When NTP is enabled, the SSL proxy blade synchronizes the time at the time of enabling NTP, every 12 hours, and at boot time. To force an immediate synchronization, disable and enable NTP. By enabling NTP, the UTC or Universal Time Code is used. Previous local time setting based on local time and local time zone are reset by enabling NTP.

Global Command Examples

Following are examples of the global commands listed in TABLE 5-4.

```
show ntp
```

The `show ntp` command returns output similar to the following:

```
CLI# show ntp
NTP server IP address: 192.168.1.5
NTP server IP port: 123
NTP service : enable
```

```
set ntp
```

- As so or admin, type the `set ntp` command.:

```
CLI# set ntp
Enter NTP server IP address (192.168.1.5):
Enter NTP port (123):
Enter NTP enable/disable (enable):
    NTP synchronization enabled.
    2002-04-02 23:22:01 UTC
```

```
show config
```

The `show config` command provides a great deal of system information. It returns output similar to the following:

```
CLI# show config
name: Sun_Fire_Blxp
state: Started
date: 2003-10-09 22:28:03 UTC
version: 1.872
secure port: 443
clear port: 880
https forward: disabled
mode: routed
trace state: stopped
serial rate: 9600
web access enabled: disabled
connection timeout (seconds): 120
mode: routed

routed settings:
port 1:
    router inbound IP : 0.0.0.0
```

```
router outbound IP (primary) : 192.100.104.254
router outbound IP (secondary) : 0.0.0.0
port 2:
  router inbound IP : 0.0.0.0
  router outbound IP (primary) : 192.100.104.254
  router outbound IP (secondary) : 0.0.0.0

inband settings:
port 1:
  inband IP: 192.100.104.235
  inband netmask: 255.255.255.0
port 2:
  inband IP: 192.100.104.236
  inband netmask: 255.255.255.0
port 1:
  vlan: 1234
port 2:
  vlan: 1234

client vlan: 1234

server vlan: 0

vlan filter enabled: enabled

management settings:
port 1:
  management (admin) IP: 192.50.54.235
  management (admin) netmask: 255.255.255.0
  management (admin) gateway: 0.0.0.0
port 2:
  management (admin) IP: 192.50.54.236
  management (admin) netmask: 255.255.255.0
  management (admin) gateway: 0.0.0.0

port 1:
  vlan: 1234
port 2:
  vlan: 1234

link settings:
link pairs: disabled
port 1: enabled
port 2: enabled

ethernet interface settings:
port 1: link: up: ( auto, speed: - , duplex: - , flow control: - )
        actual: speed: 1000, duplex: full, flow control: on
port 2: link: up: ( auto, speed: - , duplex: - , flow control: - )
```

```
actual: speed: 1000, duplex: full, flow control: on

features settings:
UnitID: 1100001EAF01
TPS [SSL/sec]: 4000 [options: 2500, 5000]
BULK [Mbps]: 300 [options: 300, 400]
SESSIONS: 64000 [options: 32000, 64000]

log settings:
file: off
mem: off
serial: off
snmp: off
syslog: off
ntp settings:
NTP server IP address: 0.0.0.0
NTP server IP port: 123
NTP service: disabled

dns settings:
DNS IP address (primary): 0.0.0.0
DNS IP address (secondary): 0.0.0.0
Domain name:
DNS service: disabled

ciphers:
EXP-RC4-MD5:EXP1024-RC4-MD5:EXP1024-RC4-SHA:RC4-MD5:RC4-SHA:
EXP-DES-CBC-SHA:DES-CBC-SHA:DES-CBC3-SHA

keys:
Key Name Cert Use Count
=====
1024 cert 2

port pairs:
portpair 1:
secure port: 443
clear port: 880
portpair 2:
secure port: 0
clear port: 0
portpair 3:
secure port: 0
clear port: 0
portpair 4:
secure port: 0
clear port: 0
```

```

services:
Service      IP Address      Key      Cipher      PortPair
=====
svcl         110.10.14.1    1024     best        443|880
CLI#

```

System State Commands

The SSL proxy blade can be in one of several different operating states: Uninitialized, Stopped, Started, and Fault. During normal operating conditions the SSL proxy blade will be in one of two main states:

State	Description
Start	SSL processing on
Stop	SSL processing off

During error or fault conditions, the SSL proxy blade will be in one of two secondary states:

State	Description
Uninitialized	No secure content (for example, no keys), state after tamper detection.
Fault	An unrecoverable error has occurred.

TABLE 5-5 describes the system state commands:

TABLE 5-5 Show State Commands

Syntax	Access Level	Description
<code>show state</code>	all	Displays the current state of the system. The state is one of un-initialized, started, stopped, or fault.
<code>set autorun</code> <i>[enable disable]</i>	all	If autorun is enabled then upon reboot the SSL proxy blade will start processing traffic. This is the mode for benefiting from automatic reboot (watchdog) protection. If the SSL proxy blade is set to reboot to the stop state, SSL processing will not resume until the operator enters the <code>start</code> command. A warning is given when logging out if autorun is disabled.
<code>set password</code>	User Administrator Security Officer	Enables current users to change their password.
<code>start</code>	Administrator Security Officer	Enables SSL processing. Otherwise <i>NO</i> SSL sessions will be accepted.
<code>stop</code>	Administrator Security Officer	Disables SSL processing. No new SSL sessions are accepted. Existing connections are closed.

Commands and Processing States

Most commands can be used while the SSL proxy blade is processing traffic. Some commands require the system to be stopped before they can be performed. Configuration changes, like software upgrades and feature installation, cannot be made while the SSL proxy blade is processing SSL traffic and require reboot after completion.

TABLE 5-6 lists the commands that require the SSL proxy blade to be stopped or rebooted or both. If the command cannot be executed in the current SSL proxy blade state, the CLI will display a message and tell you to reboot when completed.

TABLE 5-6 Commands That Require the SSL Proxy Blade to be Stopped or Rebooted

Command	SSL Off Required	Reboot Required
import config	yes	yes
config default	yes	no
config reset	yes	no
Software upgrade (boot upload, boot activate)	yes	yes
import feature	yes	yes
set link pair	yes	yes
set dns	no	yes

Fault State

When the SSL proxy blade detects an unrecoverable problem, it goes to a limited functionality fault state. The fault state allows some commands for diagnostics purposes.

SSL Traffic Commands

The SSL proxy blade has two traffic ports dedicated to processing SSL traffic for the servers. Both ports use the same TCP port number for encrypted traffic, typically 443, and the same TCP port number for clear text, for example, 880.

There are commands available for port numbers, enabling traffic ports, and setting network interface parameters for duplex, speed, and flow control.

TCP Port Numbers

In the context of TCP/IP protocol specifications, the TCP port numbers below 1024 are reserved for TCP services. Some numbers in this range are reserved for specific protocols, such as FTP (20,21), HTTP (80), HTTPS (443), while other numbers are available for new services (see TABLE 5-7). The port numbers 1024 and above are used by clients, which typically assign them sequentially to new TCP connections.

TABLE 5-7 TCP Port Numbers

TCP Services	Port Number	Protocol	Service Description
FTP data	20	TCP	File Transfer Protocol, data
FTP control	21	TCP	File Transfer Protocol, control
Telnet	23	TCP	Telnet
SMTP	25	TCP	Simple Mail Transfer
TFTP	69	UDP	Trivial File Transfer Protocol
HTTP	80	TCP	World Wide Web HTTP
pop-3	110	TCP	Post Office Protocol - Version 3
SNMP	161	UDP	Simple Network Management Protocol
IMAP3	143	(TCP, UDP)	Interactive Message Access Protocol v3
HTTPS	443	TCP	HTTP protocol over TLS/SSL
imaps	993	(TCP, UDP)	imap4 protocol over TLS/SSL
POP3S	995	TCP	pop3 protocol over TLS/SSL
Available	880		

Currently, the SSL proxy blade supports the HTTPS/HTTP protocol. In addition, the SSL proxy blade has been successfully used in lab settings with POP3S and IMAPS protocols.

The SSL proxy blade requires a secure TCP port number to listen to traffic from the clients, and a clear TCP port number to send traffic to the server. The secure port number is usually 443, the standard port number for HTTPS clients. The clear port must be an available TCP number below 1024.

In the SSL proxy blade, the secure and clear port numbers apply to all services.

External access, for example, from remote browsers or even local machines, can be prevented by combining one or more of the following techniques:

- Contain the clear port traffic within a VLAN that has no local machines other than the web servers. The SSL proxy replaces the VLAN as it encrypts; therefore the router does not need to be in the same VLAN.

- Use local IP addresses for the web servers. Only the service VIP addresses are routable addresses accessible by remote browsers. VIPs are claimed (that is, ARP replied) by the content load balancer, not by servers.
- Block the secure port (for example, 880) at the appropriate firewalls.

▼ To Display the Current TCP Port Settings

- As any user, type the `show portpair` command:

```
CLI# show portpair
portpair 1:
  secure port:    443
  clear port:     880
portpair 2:
  secure port:    0
  clear port:     0
portpair 3:
  secure port:    0
  clear port:     0
portpair 4:
  secure port:    0
  clear port:     0
```

▼ To Set the TCP Port Numbers

Use the `set portpair` command to set the TCP port numbers used for processing secure and clear traffic.

Typical standard settings are:

- Secure port: 443 (secure HTTPS traffic)
- Clear port: 880 (clear HTTP traffic)

These port numbers are used for all services.

- As so or admin, type the `set portpair` command:

```
CLI# set portpair
Enter portpair number (1..4) (1):
Enter secure port (https) (443):
Enter clear port (http) (880):
    config save & reboot to use activate portpair(s).
CLI#
```

▼ To Show HTTPS Forwarding

Use the `show httpsforward` command to learn whether HTTPS forwarding is enabled or disabled.

- As any user type the `show httpsforward` command:

```
CLI# show httpsforward
httpsforward: disabled
```

▼ To Set HTTPS Forwarding

Use the `set httpsforward` command to set the HTTPS forward function.

- As so or admin, type `set httpsforward` command:

```
CLI# set httpsforward
```

Traffic Port Network Settings

You can enable and configure each of the SSL proxy blade's two traffic ports with IP address and netmask. This allows the port to respond to ARP and ping requests and to be used for health check purposes. In addition, you can specify each port's network link and interface settings.

TABLE 5-8 Traffic Network Settings Worksheet

Parameter Name	Value	Description
Port 1		
Link		Enables/disable the port for all traffic
Management (admin) IP		IP address for the port
Netmask		Netmask for the port
Port 2		
Link		Enables/disable the port for all traffic
Management (admin) IP		IP address for the port
Netmask		Netmask for the port

▼ To Display the Current Link Settings

Use the `show link` command to display the current link settings for all traffic ports.

- As any user, type the `show link` command:

```
CLI# show link
Link pairs: disabled
port 1: enabled
port 2: enabled
```

▼ To Set the Link Availability for Ports

Use the `set link` command to set the link availability for a specified port or for all ports. You can save the configuration to make it permanent to exist after power off. You can also disable the link, which turns off the interface until the link is enabled again.

Use the `set link restart` command to apply the link settings instead of rebooting the SSL proxy blade. If the blade is not stopped you will be prompted to stop it when you try to change the link settings.

- **As so or admin, type the `set link` command and the desired variable:**

```
CLI# set link [port|all] [enable|disable|restart]
```

The following example enables all ports.

```
CLI# set link all enable
```

Network Interfaces

The SSL proxy blade has two network interfaces for traffic running at 1000 Mbps full duplex.

▼ To Display the Current Interface Settings

Use the `show interface` command to display the current interface settings for the two traffic ports. The configuration appears in parenthesis, the non-parenthesis is the negotiated setting. The port LEDs reflect the negotiated setting.

- **As any user, type the `show interface` command:**

```
CLI# show interface
ethernet interface settings:
port 1: link: up: ( auto, speed: - , duplex: - , flow control: - )
          actual: speed: 1000, duplex: full, flow control: on
port 2: link: ( auto, speed: - , duplex: - , flow control: - )
```

▼ To Display the Current Router Information

- As any user, type the `show routed` command:

```
CLI# show routed
port 1:
  router inbound IP           : 192.50.50.132
  router outbound IP (primary) : 192.100.100.254
  router outbound IP (secondary) : 0.0.0.0
port 2:
  router inbound IP           : 0.0.0.0
  router outbound IP (primary) : 0.0.0.0
  router outbound IP (secondary) : 0.0.0.0
```

Configuration Storage

The SSL proxy blade stores all configuration information in encrypted form with a device-unique key. The SSL proxy blade stores a permanent configuration, which is read and decrypted when the device is powered on or rebooted with an operator command. All changes to the active configuration must be saved for the change to be made permanent.

The configuration can be exported and saved as a backup. The `import` command allows a configuration to be set from a backup. All backups are encrypted using a pass-phrase.

Note – Save changes often, using the `config save` command.

Except for the commands that only display information, most `CLI#` commands change the active configuration immediately. Be sure to save the configuration after changes are made. In addition, when logging out or performing a shut down you are prompted to save the configuration.

The `config compare` command displays any difference between the RAM configuration and the Active Configuration file. The `config default` command overwrites the permanent configuration stored in flash.

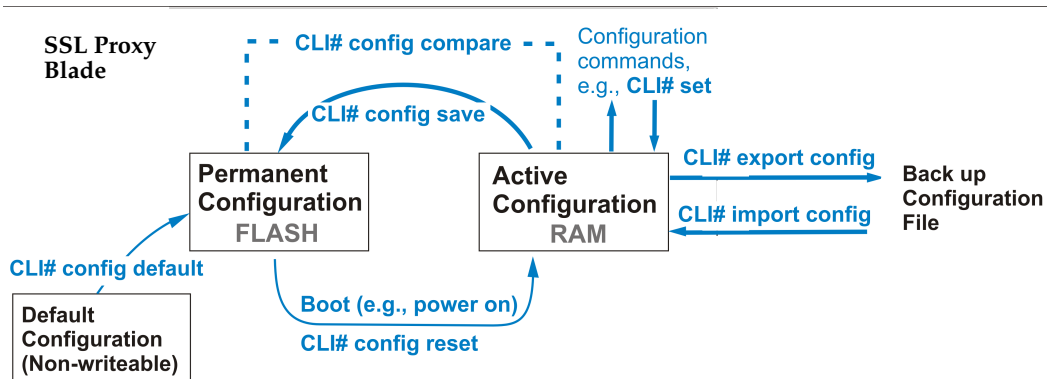


FIGURE 5-1 Configuration State

Configuration Management Commands

Following are descriptions of the configuration management commands.

▼ To Display Differences Between Configurations

Use the `config compare` command to display the differences between the current running configuration and the configuration saved as permanent in the flash memory.

- As `so` or `admin`, type the `config compare` command.

If the configuration matches, you see the following output:

```
CLI# config compare
Configuration matches.
```

If the configuration does not match, you see the following output:

```
CLI# config compare
Configuration is different.
```

▼ To Reset the Default Configuration Settings

Use the `config default` command to reset the permanent configuration information to its initial default settings. All values are set to defaults. The resulting state is called uninitialized because there is no secure content.

- As so or admin, type the `config default` command:

```
CLI# config default
This will clear all configuration settings in flash. Continue (Yes/No)?
```

▼ To Reset the Configuration

Use the `config reset` command to reset the active configuration with the permanent configuration.

Note – The `config reset` command overwrites any changes to the active configuration. You must stop all SSL processing before performing this command.

- As so or admin, type the `config reset` command:

```
CLI# config reset
This will erase current configuration in memory
Are you sure you want to do this (Yes/No)?
```

▼ To Save the Configuration

Use the `config save` command to save the active configuration to flash. This overwrites the permanent configuration in flash. Use this command after you make changes to the active configuration.

- As so or admin, type the `config save` command:

```
CLI# config save
permanent configuration updated.
```

Backups

The SSL proxy blade allows the security officer to create encrypted backups of configurations. The import and export commands are used for this purpose. During the export command, the operator is prompted to enter a user defined pass-phrase that is used to encrypt the configuration. The pass-phrase must be re-entered when the configuration is imported. Configurations are encrypted and then imported or exported using PEM format.

Configurations may be imported from another SSL proxy blade. There are some restrictions regarding licenses for software features that are imposed when importing configurations from another SSL proxy blade. See the section on licensing for more information.

Import and Export

Only the security officer (so) can export and import configurations because the user pass -phrase must be entered to decrypt the configuration. The configuration is exported using TFTP or FTP. Copy and paste functions are not provided because the configuration can span many pages.

▼ To Export the Active Configuration Using FTP or TFTP

Note – This example uses FTP; however, to use TFTP, simply replace `ftp` with `tftp` in the following commands.

Use the `export ftp config` command to export the active configuration using FTP to copy the configuration to a remote computer.

- As so, type the command `export ftp config`:

```

CLI# export ftp config
Enter remote file name (flash.cfg): remote_filename
Enter remote path (configurations): remote_directory
Enter remote IP Address: (192.168.0.11): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_user_password
Enter pass phrase: pass_phrase
Re-enter pass phrase: pass_phrase
    connecting and writing configurations/flash.cfg to 192.168.0.11.
    config exported.

```

Import

The operator can import a configuration using FTP, TFTP, or by pasting the configuration into the CLI when prompted. It is also possible to perform a partial import, where only a specified section of a configuration is imported. The SSL proxy blade must be stopped before an import can be performed.

The import command will prompt the operator for the specific section to import. The choices are:

<i>all</i>	Import a complete configuration
<i>password</i>	Import password information only
<i>system</i>	Import system configuration: Includes networks, logging, and settings
<i>services</i>	Import SSL configuration: Includes certificates and services settings

▼ To Import the Active Configuration Using FTP

Use the `import ftp config` command to import a configuration using FTP and set it to the active configuration.

Note – The SSL proxy blade must be stopped before importing a configuration.

- As so, type the command `import ftp config`:

```
CLI# import ftp config
Enter import options (all/password/system/services) (all): import_option
Enter remote file name (flash.cfg): remote_filename
Enter remote path (configurations): remote_directory
Enter remote IP Address: (192.168.0.11): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_user_password
Enter pass phrase: pass_phrase
    connecting and reading configurations/flash.cfg to 192.168.0.11
    configuration imported.
    To save the configuration enter: config save
```

Keys and Certificates

The SSL proxy blade requires that keys and certificates be installed before SSL traffic can be processed. The SSL handshake requires a private key and signed certificate to be associated with each server. The certificate contains the public key and key issuer information, and is digitally signed by a recognized Certificate Authority (CA).

To create a valid certificate, a key and certificate signing request are created. The certificate request contains the public key, key issuer information, and other information. The key is then submitted to a certificate authority (such as Verisign) for signing. The signed certificate is then imported into the SSL proxy blade using the original key.

The SSL proxy blade can hold up to 1024 keys, which are identified by a key name. For each key, information including private keys and certificates are stored. The `show keys` command lists the available keys and their signing status. Other CLI commands are used to generate private/public key pairs, create signing requests for the CA, and import and export certificates and keys. See the “Certificate Formats” on page 85 for information on certificate format compatibility.

Self-signing is used for testing or for intranet use. There are three basic operations associated with keys and certificates:

- Create a self-signed certificate.
- Create a CA signed certificate.
- Import a key or certificate from a server.

▼ To Create a Self-Signed Certificate.

1. Create a private-public key pair.

```
CLI# create key
      Enter key name: keyname
      Enter key strength (1024): 512/1024/2048
      Key keyname generated.
```

2. Create a self-signed certificate from the new key pair.

```
# create certificate
Enter key name: keyname
Enter country (US):
Enter state or province (CA):
Enter locality (US):
Enter common name (US):
Enter organization (www.company.com):
Enter organization unit ():
Enter email():
Certificate generated.
```

3. Use show keys, or export certificate commands to see the resulting key and certificate.

Note – When a server or SSL proxy blade uses a certificate that is not signed by a certificate authority recognized by the browser, as is the case for self-signed certificates, the browser displays a warning to the user indicating that this server may not be trusted. The self-signed certificate authority could be installed in all relevant browsers of an intranet to avoid this message.

▼ To Create a CA-Signed Certificate.

This is the standard way to create a certificate that most browsers recognizes as valid. This method does not generate any errors or warnings for the user.

1. Create a private-public key pair.

```
CLI# create key
      Enter key name: keyname
      Enter key strength (1024): 512/1024/2048
      Key keyname generated.
```

2. Create a certificate signing request using the new key pair.

```
CLI# create certrequest
      Enter key name: previously_created_keyname
      Enter country (US):
      Enter state or province (CA):
      Enter locality (Company Town):
      Enter common name (www.company.com):
      Enter organization (Company Name):
      Enter organization unit (Company Unit):
      Enter email(support@companyname.com):
      Certificate request generated.
```

● Observe the following restrictions when creating a certificate.

- a. Enter the two-letter ISO code for the country.
 - b. To avoid client browser warnings the common name should be the same as the domain name for the web site that is requesting the certificate.
 - c. Do not use any of these characters: `!, @, #, $, %, ^, *, (,), \, /, ?, ~`
 - d. Make sure the email address contains an at sign (`@`)
3. Use `show keys`, or `export certrequest` commands to see the resulting key and certificate.
 4. Copy and paste the certificate request into a file.

You can also export the certificate request using `ftp` or `tftp`.

```
CLI# export tftp certrequest
      Enter key name: previously_created_keyname
      Enter remote file name (certificate-request.txt): filename_with_certrequest
      Enter remote IP Address: (192.168.1.28): tftp_server_ip-addr
      certrequest exported.
```

5. Send the certificate request file to the CA and receive a signed certificate.

See Appendix C for details.

6. Import the certificate received from the CA into the SSL proxy blade by using either `import certificate` command and cut and paste the certificate, or by using the `import ftp/tftp certificate` command.

```
CLI# import tftp certificate
Enter key name: previously_created_keyname
Enter remote file name (certificate.txt): filename_with_certificate
Enter remote IP Address: (192.168.1.28): tftp_server_ip-addr
Enter format: 1 - PEM,
              2 - DER,
              3 - PKCS12 (.p12 or .pfx),
              4 - Netscape (.net),
              5 - PKCS7 (.p7b)
              6 - PKCS7 (.pem) certificate_format
certificate imported
```

▼ To Import a Certificate From a Server

When you install the SSL proxy blade, you might have an existing certificate in the server that you may want to load into the SSL proxy blade. Following are instructions to load an existing key and associated certificate from a server. The SSL proxy blade supports copy and paste as well as FTP and TFTP methods for import.

1. Import the private key (from a server, for example).

```
CLI# import ftp key
Enter key name: keyname
Enter remote file name (key.pem): remote_filename
Enter remote path (keys): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_password
Enter pass phrase (or enter): pass_phrase
key imported.
```


2. Import the certificate.

```
CLI# import ftp certificate
Enter key name: keyname
Enter remote file name (certificate.txt): remote_filename
Enter remote path (/tmp): remote_directory
Enter remote IP Address: (192.168.101.128): remote_ip-addr
Enter remote user name (root): remote_username
Enter remote user password: remote_password

Enter format: 1 - PEM,
              2 - DER,
              3 - PKCS12 (.p12 or .pfx),
              4 - Netscape (.net),
              5 - PKCS7 (.p7b)
              6 - PKCS7 (.pem)
: 1

connecting and reading [/tmp/cert.txt] from 192.168.101.128
```

Certificate Formats

The SSL proxy blade supports the X.509 V3 standard certificate format used by most servers, and issued by recognized certificate authorities (for example, Verisign, Thawte, and others).

The X.509 format defines the data fields in the certificate. The PEM standard is commonly used to encode x.509 certificates for storage and transfer. PEM uses a character representation of text and binary data that is easy to handle for email, copy and paste, and other data transfer mechanisms. The SSL proxy blade supports importing and exporting of keys and certificates in PEM format.

Most Certificate Authorities provide PEM encoded certificates. Most servers provide facilities to export certificates and keys in PEM format. Private keys are often encrypted such that user must enter a pass-phase during export and import operations.

Note – You can set the default values for a certificate (country, state, and so on) by using the `set defcert` command.

Certificate Management Commands

▼ To Display Information About Keys

Use the `show keys` command to display the keys, the status (if a certificate or certificate signing request exists) and the number of services that are actively using the key.

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

```
CLI# show keys
  Key Name          Cert          Use Count
  =====
  key1024           cert | csr    1
  key512            0
```

▼ To Create a Key

Use the `create key` command to create a new key with the specified name. A key is generated using the specified strength. The default strength is 1024 bits.

- As `so` or `admin`, enter the `create key` command:

```
CLI# create key
Enter key name: keyname
Enter key strength (1024): 512/1024/2048
Key keyname generated.
```

▼ To Delete a Key

Use the `delete key` command delete the specified key and any certificates or certificate requests associated with the key.

Note – The key will not be deleted if it is currently in use by a service.

1. As so, enter the `delete key` command:

```
CLI# delete key keyname
Key keyname deleted.
```

2. Use the `show keys` command to see if the key has been deleted:

```
CLI# show keys
Key Name          Cert          Use Count
=====
key1024          cert|csr      1
key512           0
```

▼ To Import a Key Using FTP

Use the `import ftp key` command to import a key using FTP.

- As so, enter the `import ftp key` command:

```
CLI# import ftp key
Enter key name: keyname
Enter remote file name (key.pem): remote_filename
Enter remote path (keys): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_password
Enter pass phrase (or enter): pass_phrase
key imported.
```

▼ To Import a Key Using TFTP

Use the `import tftp key` command to import a key using TFTP.

- As so, enter the `import tftp key` command:

```
CLI# import tftp key
Enter key name: keyname
Enter remote file name (key.pem): remote_filename
Enter pass phrase (or enter): pass_phrase
    key imported.
```

▼ To Import a Key

Use the `import key` command to import a key. Paste the key into the CLI and type a period (.).

1. As so, enter the `import key` command:

```
CLI# import key
Enter pass phrase (or return):
Enter key, '.' to stop:
```

2. Paste the key into the CLI, then type a period.

```
>-----BEGIN RSA PRIVATE KEY-----
>MIICXAIBAABgQC2r5i9vb5+XLzjGozxF/lq9VATOLQr1NqnnQ
>iEMzqvKuPhB0etZ6iWi6+B/ed/HSNny2j9o6UJGzRB+xPA5g1YH6n
>HFwSPxzam+VahsreE6ECQAsHQf/N3faVtrsLPzStqUJysAW+M8z
>tI8FwwGXf+zfNnSTs7EpzqgcFeopa86ZuFrmeCgwwSg=
>-----END RSA PRIVATE KEY-----
> .
    key imported.
```

▼ To Export a Key Using FTP

Use the `export ftp key` command to export a key.

- As so, enter the `export ftp key` command:

```
CLI# export ftp key
Enter key name: keyname
Enter remote file name (key.pem): remote_filename
Enter remote path (keys): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_password
Enter pass phrase: pass_phrase
Re-enter pass phrase: pass_phrase
Key exported.
```

▼ To Export a Key Using TFTP

Use the `export tftp key` command to export a key using tftp.

- As so, enter the `export tftp key` command:

```
CLI# export tftp key
Enter key name: keyname
Enter remote file name (key.pem): remote_filename
Enter pass phrase: pass_phrase
Re-enter pass phrase: pass_phrase
Key exported.
```

▼ To Export a Key

Use the `export key` command to export a key. The key is displayed in PEM format.

- As so, enter the export key command:

```
CLI# export key keyname
Enter pass-phrase <or return>: pass_phrase
key:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, Encrypted
DEK-Info: DES-EDE3-CBC, 365E321C0C05C656
MIICXQIBAAKBgQDNLk7/ADQQV22yi3u77vUKhWA/R99NfvVzjtVypCHN7I12MCuq
wesgJYfNSqNrfSLOdk4aWWHJOx7luXLD69t7YPNJAMhi4E2pbzAvWvnzz/G9+B4z
e3wzNHXMuAVwjMVCtLk5tVR0/OkCEbei/ZN+wBxzUECP2DuZyq6FXdIiHQIDAQAB
AoGAFqdMwXNmrDc7AW+tJb7oh1UIjfQdj6zo501sW9ALe3UW2WnQKHZow4/hQqVv
DbtdPvaJARfFWDaS3sJvDXrJLM9vgw+DkxVpDMkCl6m2R8pdKJHcx4ZyXx1kKVr
C5lwAxpNbAmiHTSHXCWfeLGBRB0Lg+7FPqHNhyr16U/mj3ECQQD37Wdn01fokrFL
XTUT3Qfwo5jV+hlxTpe2M9uTi6BNrYfQyF1We6TgZBVuIZTi6Jbx38eJ/x71YeVv
9roOzwIXAKEA09rp+zd2e+Z6ZuyRZ5ez84IeYBPBwVpZ+6M/HAnZwNVGXQah2Kw
dcuEKprI3nRddstIfeZlvXwhBcVfRNPh6wJAPiLQvLO6H37MUnAMwmt98B4qIAi
6kN4/cAncuYwigFIxC3tPqSEYPyUZmKiNvBGDF6iWtKGxsb/Qr1aSiXVhwJBAKR9
s/CnRqq68Ezb36YkZsdqPzVwAU8enLHiybrzRdS5BKknubVmzgYYB72gwtfeV/d1
rQp8CoDOUUG01wK01RMCQQC9zYJ+uYYdkYAchPzKmoqu+ZVZh5B8Wt1UhMws0L4L
fKq7RHoI2quyAAEZxQ7z0ON6LVM5cLYeEb44149QaLRH
-----END RSA PRIVATE KEY-----
```

▼ To Create a Certificate

Use the `create certificate` command to create a certificate for a specified key. The security officer is prompted for the information required to create a self-signed certificate. A self-signed certificate can be used for testing purposes.

Be sure to observe the following restrictions when creating a certificate:

- The key, common name, and email address are required fields.
- Enter the two-letter ISO code for the country.
- Do not use any of these characters: !, @, #, \$, %, ^, *, (,), \, /, ?, ~
- Make sure the email address contains an at sign (@).
- To avoid client browser warnings the common name should be the same as the domain name for the web site that is requesting the certificate.

- As so, type the create certificate command:

```
CLI# create certificate
Enter key name: keyname
Enter country (US):
Enter state or province (CA):
Enter locality (Company Town):
Enter common name (www.company.com):
Enter organization (Company Name):
Enter organization unit (Company Unit):
Enter email(support@companyname.com):
Certificate generated.
```

▼ To Import a Certificate Using FTP

Use the `import ftp certificate` command to set the certificate for an existing key.

- As so, enter the import ftp certificate command:

```
CLI# import ftp certificate
Enter key name: keyname
Enter remote file name (key.pem): remote_file_name
Enter remote path (keys): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_password
Enter pass phrase (or enter): pass_phrase
key imported.
```

▼ To Import a Certificate Using TFTP

Use the `import tftp certificate` command to set the certificate for an existing key.

- As so, enter the `import tftp certificate` command:

```
CLI# import tftp certificate
Enter key name: previously_created_keyname
Enter remote file name (certificate.txt): filename_with_certificate
Enter remote IP Address: (192.168.1.28): tftp_server_ip-addr
Enter format: 1 - PEM,
              2 - DER,
              3 - PKCS12 (.p12 or .pfx),
              4 - Netscape (.net),
              5 - PKCS7 (.p7b)
              6 - PKCS7 (.pem) certificate_format
certificate imported
```

▼ To Import a Certificate

Use the `import certificate` command to import a certificate for an existing key.

- As so, enter the `import certificate` command:

```
CLI# import certificate
Enter pass phrase (or return):
Enter key, '.' to stop:
```

▼ To Export a Certificate Using FTP

Use the `export ftp certificate` command to export a certificate.

- As so, enter the `export ftp certificate` command:

```
CLI# export ftp certificate
Enter key name: keyname
Enter remote file name (key.pem): remote_filename
Enter remote path (keys): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_password
certrequest exported.
```


▼ To Export a Certificate Using TFTP

Use the `export tftp certificate` command to export a certificate.

- As so, enter the `export tftp certificate` command:

```
CLI# export tftp certificate  
Enter key name: keyname  
Enter remote file name (cert.pem): remote_filename  
certificate exported.
```

▼ To Export a Certificate

Use the `export certificate` command to export a certificate.

- As so, enter the `export certificate` command:

```
CLI# export certificate keyname  
Enter pass-phrase <or return>: pass_phrase  
key:
```

Setting Default Information for Certificates

▼ To Display the Default Settings for Creating Certificates

Use the `show defcert` command to display the default settings used for creating certificates and signing requests.

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

```
CLI# show defcert
country: US
state/province: CA
locality: Company Town
common name: www.companyname.com
organization: Company Name
organization unit: Company Unit
email address: email@companyname.com
```

▼ To Set the Default Certificate Parameters

Use the `set defcert` command to set the default certificate parameters used when creating certificates or signing requests.

- **As so, enter the `set defcert` command:**

```
CLI# set defcert
Enter country (US):
Enter state or province (CA):
Enter locality (Company Town):
Enter common name (www.company.com):
Enter organization (Company Name):
Enter organization unit (Company Unit):
Enter email(support@companyname.com):
```

Creating a Certificate Signing Request (CSR)

The security officer can create, export, or import a certificate signing request. The security officer is prompted for the information required to create the request. A signing request can be exported and sent to a recognized signing authority (CA) and then be imported back into the system.

▼ To Create A Certificate Signing Request

Use the `create certrequest` command to create a certificate signing request (CSR).

- As so, enter the `create certrequest` command:

```
CLI# create certrequest
Enter key name: previously_created_keyname
Enter country (US):
Enter state or province (CA):
Enter locality (Company Town):
Enter common name (www.company.com):
Enter organization (Company Name):
Enter organization unit (Company Unit):
Enter email(support@companyname.com):
Certificate request generated.
```

▼ To Export a Certificate Signing Request Using FTP

Use the `export ftp certrequest` command to export a CSR using FTP.

- As so, enter the `export ftp certrequest` command:

```
CLI# export ftp certrequest
Enter key name: keyname
Enter remote file name (csr.pem): remote_filename
Enter remote path (keys): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_password
    connecting & writing ... 192.168.0.28 keys/csr.pem
Certificate request exported.
```

▼ To Export a Certificate Signing Request Using TFTP

Use the `export tftp certrequest` command to export a CSR using TFTP.

- As so, enter the `export tftp certrequest` command:

```
CLI# export tftp certrequest
Enter key name: previously_created_keyname
Enter remote file name (certificate-request.txt): filename_with_certrequest
Enter remote IP Address: (192.168.1.28): tftp_server_ip-addr
certrequest exported.
```

▼ To Export a Certificate Signing Request

Use the `export certrequest` command to export a CSR using TFTP.

- As so, enter the `export certrequest` command:

```
CLI# export certrequest
Enter key name: keyname
certificate request:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwwYoxCzAJBgNVBAYTA1VMTQswCQYDVQ
QIEwJDQTEVMBMGAlUE
BxMMQ29tcGFueSBUb3duMRUwEwYDVQQKEwxDb2HDAaBgNVBAMT
E3d3dy5jb21wYW55bmFtZS5jb20xIjAgBgkE3d3d0Bjb21wYW55
bmFtZS5jb20wgZ8wDQYJKoZIhvcNAQMIgJAoGBAOADtplrUv/gwoDt
9FNzkQ7GP5WAmZaAXR4IgJB06v/vXEN8ntU/NodTKukwqH97k77
fw0XgIWmMEuCXZ1/byrgsYq1mdiUrsl5vyOBiH7zysfRoA+e9ugr1BuJS/
Qq8ZxwW6k3bQ4kyEZuQxOApz9SeND4a4XcsuKPTtgQ==
-----END CERTIFICATE REQUEST-----
```

Services

Services are used to represent each virtual IP (VIP) server and its associated IP address. The server IP should be a virtual IP with many load balanced servers. The SSL proxy blade can support up to 1024 services and services are stored in the configuration.

A service is associated with an existing certificate. Many services may be associated with the same certificate. The service also defines the level of cipher strength supported for secure connections.

When the SSL proxy blade receives encrypted data for an IP address, the associated service will be identified. The service determines the certificate and cipher strength to be used for SSL processing. If the service is not found, the SSL connection will not be accepted. No unassigned SSL traffic is allowed through the SSL proxy blade.

If DNS is enabled, the service name will be used as a DNS name. See “DNS Name for a Service” on page 99 for details on DNS.

Service Commands

The Security Officer (so) or Administrator (admin) can create, delete, or show services.

▼ To Create a Service

Use the `create service` command to specify the servers that will have SSL processing. The service must specify a valid IP address and a valid key.

TABLE 5-9 describes the six available cipher suites.

- As so or admin **type the `create service` command:**

```
CLI# create service
Enter service name: servicename
Enter key name: keyname
Enter server IP Address: (0.0.0.0): server_ip-addr
Enter cipher (export/best/optimal/high/medium/low) (best)
Service created.
```

TABLE 5-9 Available Cipher Suites.

Cipher Suite	Ciphers
export	XP-RC4-MD5 EXP1024-RC4-MD5 EXP1024-RC4-SHA EXP1024-DES-CBC-SHA
best	EXP-RC4-MD5 EXP1024-RC4-MD5 EXP1024-RC4-SHA RC4-MD5 RC4-SHA EXP-DES-CBC-SHA DES-CBC-SHA EXP1024-DES-CBC-SHA
optimal	RC4-MD5 RC4-SHA
high	DES-CBC3-SHA
medium	RC4-MD5 RC4-SHA DES-CBC3-SHA
low	EXP-RC4-MD5 EXP1024-RC4-MD5 EXP1024-RC4-SHA RC4-MD5 RC4-SHA EXP-DES-CBC-SHA DES-CBC-SHA DES-CBC3-SHA EXP1024-DES-CBC-SHA

▼ To Delete a Service

Use the `delete service` command to delete the specified service.

Use the `show service` command to see if it is active or pending deletion.

- **As so or admin type the delete service command:**

```
CLI# delete service servicename  
Service deleted.
```

Note – The service will not be deleted immediately if it is currently servicing a client browser connection. In this case, the service is marked “pending deletion” and is finally deleted in a few seconds.

▼ To Display Current Services

Use the `show services` command to display current services.

- **As so or admin type the `show services` command:**

```
CLI# show services
Service      IP Address      Key      Cipher      PortPair
=====
svc1         110.10.14.1     1024     best        443|880
```

▼ To Display Available Ciphers

Use the `show config` command to display the available ciphers.

- **As so or admin type the `show config` command.**

DNS Name for a Service

If DNS is properly setup (`set dns`) and enabled, the service name is used as a DNS name to obtain the service IP address.

The service IP address has priority over DNS lookup. Thus, service IP must be 0.0.0.0 for DNS IP lookup to occur.

▼ To Create a New Service With a DNS Name (IP=0.0.0.0)

1. **At the CLI# prompt, set DNS or make sure DNS is already enabled.**

2. Create a new service:

```
CLI# create service
Enter service name: test-service
Enter key name: 1024
Enter server IP Address (0.0.0.0): server_ip-addr
Enter cipher (export/best/optimal/high/medium/low) (best):
Enter portpair number (1..4) (1):
    Service test-service created.
```

▼ To Display DNS Server Settings

Use the `show dns` command to display the DNS server settings.

- As so or admin type the `show dns` command:

```
CLI# show dns
DNS IP address (primary):   DNS_ip-addr
DNS IP address (secondary): 0.0.0.0
Domain name:                foo.com
DNS service:                 enabled
```

▼ To Set the DNS Server Settings

Use the `set dns` command to set the DNS server settings.

- As any user, type the `set dns` command:

```
CLI# set dns
Enter DNS IP address (primary) (192.168.101.1):
Enter DNS IP address (secondary) (0.0.0.0):
Enter domain name (foo.com):
Enter DNS enable/disable (enabled):
    DNS enabled.
```

Diagnostics

The following commands are typically used for diagnostics. Additional informational commands, such as `show boot`, are described in TABLE 3-2.

▼ To Send a ping Request

- As any user, enter the ping command:

```
CLI# ping 192.50.54.7
PING 192.50.54.7 from 192.50.54.235: 56 data bytes
64 bytes from 192.50.54.7: icmp_seq=0 ttl=255 time=0 ms

--- ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
    host is alive.
CLI#
```

▼ To Set the Number of Lines for a Telnet Session

Use the `set lines` command set the number of lines for the Telnet session.

Note – The typical number of lines on a Telnet terminal is 24. On terminals with small windows, or after windows resize, the display might request: Press any key to continue, to continue the output.

Using a value of 0 sets an infinite number of lines.

With some indirect connections such as Expect scripts, the negotiation that tells the server how many lines is turned off. This command can be helpful in these cases.

- As any user, enter the `set lines` command plus the number of lines:

```
CLI# set lines
Enter lines: 24
```

Statistics

The SSL proxy blade maintains global statistics that can accumulate for long periods. The `reset stats` commands clears the statistics. The per-service statistics are cleared every time the SSL proxy blade is rebooted.

Statistics provide information regarding system load, traffic mix, and some types of network errors.

The SSL proxy blade statistics are focused on SSL proxy blade performance and SSL related statistics. You can obtain additional statistics from the servers (for service related statistics) and from supporting network equipment, such as load balancers and switches, for network related statistics.

The following commands support the statistics functionality.

▼ To View the Global Accumulated Statistics

- As so or admin, type the command `show stats glob accum`.

```
CLI# show stats glob accum
Statistics:
=====

System Up time           0 dys 19 hrs 32 min 41 sec
Acc. Up time             21 hrs 11 min 21 sec
Acc. SSL time            19 hrs 21 min 44 sec
Start stat. date        2003-07-24 02:00:01 UTC

Connection rate ave. (1min)           0 [SSL/sec]
Connection rate max.                  1062 [SSL/sec]

Concurrent connections (now)          0
Concurrent connections max.           8642
Concurrent SSL handshakes             0

Clear data in                2,821,849,429
Clear data out                292,978,491,579
Connections Succeeded         44,248,523

SSL requests                   44,265,606
  Reuse                        24,529,732
SSL handshakes                 44,265,116

SSL requests rejected (forces client to retry)
  Max TPS reached              21,786,664
  Max concurrent TPS reached   0
  Max SSL handshakes reached   0
```

▼ To View the Global Detailed Statistics

- As so or admin, type the command `show stats glob detail`.

```
CLI# show stats glob detail
Statistics:
=====
System Up time          0 dys  0 hrs  7 min 17 sec
Acc. Up time           0 hrs 12 min 33 sec
Acc. SSL time          0 hrs 10 min  9 sec
Start stat. date       2003-07-16 08:42:19 UTC

Connection rate ave. (1min)          1449 [SSL/sec]
Connection rate max.                 1556 [SSL/sec]
Concurrent connections (now)         11517
Concurrent connections max.          13195
Concurrent SSL handshakes            496
Clear data in                        35,919,814
Clear data out                       3,695,152,580
Connections Succeeded                 559,357
Connections Succeeded                 559,357

SSL requests                         571,605
  Reuse                               251,706
SSL handshakes                        571,003
SSL requests rejected (forces client to retry)
  Max TPS reached                     0
  Max concurrent TPS reached           0
  Max SSL handshakes reached           0

Detail statistics:
=====
SSL Reuse
  Reuse hits                          251,706
  Reuse drops
    Look-up miss                      393
    Timeout                           0
    Session Cache full                 56,866
Concurrent Handshakes                  496
Corrected ECC Errors                   0
Connections Terminated
  Total                               563,776
  Bad Crypto Recv                      0
  Bad Crypto Sent                      0
  Connection Reset                      9
  Connection Timeout                   4,117
  Handshake Fail                       0
  Protocol Violation                   0
  Bad Decryption                       0
```

Bad Signature	0
SSL Data after Closure	0
Data After FIN or RST	0
Others	0

▼ To View the Service Statistics

- As `so` or `admin`, type the command `show stats serv servicename`.

```
CLI# show stats serv servicename
```

▼ To Reset the Statistics

- As `so` or `admin`, type the command `reset stats`.

```
CLI# reset stats
statistics reset.
```

Note – Run the `config save` command after `reset stats` to save the changes.

Event Logging Commands

The SSL proxy blade logs messages (events) associated with various system and user activity. For diagnostic purposes it can also monitor traffic activity and exceptions. Each tracked event generates a log entry consisting of time stamp, category, and event description. There are many levels of logging, and the log destination(s) can be external or internal.

Log Levels

The SSL proxy blade provides five progressive levels of detail that determine the amount of information and quantity of events sent to each log destination. The `set log` command is used to set one of the following levels: `off`, `alert`, `error`, `info`, `debug`, from low to high amount of detail.

TABLE 5-10 Progressive Levels of Log Detail

Log Level	Description
alert	Displays only most important events (least amount of information).
error	Displays alerts and error events.
info	Displays alerts, error, and informational events.
debug	Shows all events including debug-level events.

Each log level will log all events for the specified level and all lower log levels. Each log destination may have a different level.

Info Events

Info level events track various management events such as login, logout, reboot, back up configuration and can be categorized as State, Access, and Config.

The following is an example of a log output:

```
2003-07-24 02:19:08 UTC SSL proxy blade tBeeapp : software version: 1.872
2003-07-24 02:19:09 UTC SSL proxy blade tBeeapp : configuration version: 1.872
2003-07-24 02:19:10 UTC SSL proxy blade tBeeapp : State, SYSTEM start
2003-07-24 02:19:12 UTC SSL proxy blade tCONSOLE : Access, login so [ok]
2003-07-24 02:21:16 UTC SSL proxy blade tCONSOLE : State, SYSTEM stop
```

Debug level events is reserved for diagnostic purposes. The debug level can effect performance and should be off during normal operation. At logout or reboot, you will be prompted if the log is set to debug.

Log Destination

The SSL proxy blade can log messages to any of four destinations at the same time:

- SSL proxy blade console
- syslog server
- SSL proxy blade permanent storage

- SSL proxy blade internal memory

Each destination method is described below.

Serial Port

Serial port logging displays messages on the blade console of the Sun Fire B1600 Blade.

syslog Server File

syslog logging sends UDP-based messages to remote UNIX-based syslogd servers. Both the log level and log facility can be used to direct the log events to a unique file on the UNIX-based host.

On a UNIX host, add the following line in `/etc/syslog.conf`:

```
local6.*    /var/log/sslp.log
```

Note – On a UNIX host, syslogd must be restarted to read changes in `/etc/syslog.conf`.

SSL Proxy Blade Permanent Storage Logging

The permanent log is intended to keep limited information about important system events. It is limited to a circular file of 64KB and is permanent across reboots. The internal log can be retrieved with the `export log` command.

SSL proxy blade internal memory logging.

The internal memory log is intended to keep information about important system events. It is limited to a circular file of 1MB. The log is not preserved across reboots. The internal memory log can be retrieved with the `export mem` command.

Log Commands

```
set log serial
```

The `set log serial` command sets serial port logging to the SSL proxy blade console.

The initial default and preferred setting is off. The serial off setting does not turn-off boot messages to the serial port.

- **As so or admin, set the serial port logging to the serial port:**

```
CLI# set log serial level
Enter log level (off, alert, error, info, debug):
```

```
set log syslog
```

The `set log syslog` command sets the remote UNIX syslog logging. The default and recommended setting is off.

- **As so or admin, set the remote UNIX syslog logging:**

```
CLI# set log syslog level ip-addr facility
Enter log level (off, alert, error, info, debug):
Input syslog server IP Address (0.0.0.0):
Enter facility (auth, user, local1,.. local6):
```

```
set log file
```

The `set log file` command sets permanent logging to an internal file in flash memory. The initial default and recommended setting is off.

- **As so or admin, set the remote UNIX syslog logging:**

```
CLI# set log file level
Enter log level (off, alert, error, info, debug):
```

```
set log mem
```

The `set log mem` command sets permanent logging to an internal memory. The current release does not allow you to set `mem` and `serial log` at the same time.

The initial default and recommended setting is off.

- **As so or admin, set the permanent logging to an internal memory:**

```
CLI# set log mem level  
Enter log level (off, alert, error, info, debug):
```

```
show log
```

The `show log` command displays the current log settings.

- **As so or admin, display the current log settings:**

```
CLI# show log  
serial:      info  
syslog:      error  
file:        off  
Note: "file" refers to an internal file in flash memory.
```

```
export ftp log
```

The `export ftp log` command exports the permanent log to a remote computer using FTP.

- **As so or admin, export the permanent log to a remote computer:**

```
CLI# export ftp log  
Enter remote file name (file): remote_filename  
Enter remote path (keys): remote_directory  
Enter remote IP Address: (192.168.0.28): remote_ip-addr  
Enter remote user name (labuser): remote_username  
Enter remote user password: remote_password  
log exported.
```



```
export tftp log
```

The `export tftp log` command exports the permanent log to a remote computer using TFTP.

Use this command when the permanent log in flash is one of the log targets. To set this up, use the `set log file info` command.

Commands such as `start` and `stop` create log entries.

When you have some entries, `export tftp log` will export the entries to an external file.

- **As so or admin, export the permanent log to a remote computer:**

```
CLI# export tftp log
Enter remote file name (file): remote_filename
Enter remote IP Address: remote_ip-addr
log exported.
```

```
export ftp mem
```

The `export ftp mem` command exports the permanent log to a remote computer using FTP.

- **As so or admin, export the internal memory log to a remote computer:**

```
CLI# export ftp mem
Enter remote file name (file): remote_filename
Enter remote path (keys): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password: remote_password
log exported.
```

```
export log
```

The `export log` command exports the permanent log kept to the serial port.

- **As so or admin, export the permanent log to the serial port:**

```
CLI# export log
```

SNMP Commands

The following three files are related to SNMP and are available at the download site (<http://www.sun.com/software/download/network.html>).

- SUN-B10P-SSL-ACCELERATOR-MIB
- SUN-B10P-SSL-ACCELERATOR-MIB.dat
- v2ConfTrap.sun_B10p

The first two files describe the SNMP MIB structure for the SSL proxy blade and are used to enable SNMP manager software for communicating with the SNMP agent on the blade.

For example, if you use the SNMP manager software from SNMP Research International on a UNIX system, you can rename the `SUN-B10P-SSL-ACCELERATOR-MIB.dat` file to `snmpinfo.dat` and save it in `/etc/srconf/mgr`, which is the default configuration directory used by SNMP Research.

`v2ConfTrap.sun_B10p` is a configuration file that should be imported to the SSL proxy blade for its SNMP agent to run.

▼ To Enable the SSL Proxy Blade for SNMP Support

1. Enable SNMP.

```
CLI# set snmp enable
SNMP agent enabled.
```

2. Import the v2ConfTrap.sun_B10p configuration file.

```
CLI# import ftp snmp
Enter remote file name (configuration.txt): v2ConfTrap.sun_B10p
Enter remote path (releases): /tmp
Enter remote IP Address: (192.168.1.28): 192.168.1.28
Enter remote user name (labuser): username
Enter remote user password: password

      connecting and reading [/tmp/v2ConfTrap.sun_B10p] from 192.168.1.28
Command TYPE I.(2) done!
Command CWD /tmp.(2) done!
Command PORT 192,168,1,125,4,1.(2) done!
Command RETR v2ConfTrap.sun_B10p.(1) done!
      Received: [5476] bytes

SNMP Configuration imported.
```

Note – There are several SNMP manager software packages. This example uses the SNMP Research SNMP manager.

3. Use the following SNMP Research commands to start the SNMP manager from the platform to exchange SNMP messages with the SSL proxy blade.

```
# getone -v2c -retries 0 192.168.1.125 pt2cPssl maxConnRate.0
```

Or..

```
# getmany -v2c -retries 0 192.168.1.125 pt2cPssl sslAcceleratorStats
```

In these examples, pt2cPssl is the password specified in the v2ConfTrap.sun_B10p configuration file.

▼ To Disable SNMP

- Use the following command to disable SNMP:

```
CLI# set snmp disable
SNMP agent disabled.
CLI#
```

▼ To Check the SNMP State

- Use the following command to check the SNMP status:

```
CLI# show snmp
      snmp:      disabled
CLI#
```

Upgrading the Application Software and the BSC Firmware

This chapter describes how to upgrade the software and firmware on one or more Sun Fire B10p SSL proxy blades. It also describes how to set up a TFTP (Trivial File Transfer Protocol) server if you do not already have one set up on your network. The software upgrade procedures require you to use TFTP.

- “Software Architecture” on page 113
- “Setting Up a TFTP Server” on page 114
- “Upgrading the Application Software From a VLAN-Capable Server” on page 116
- “Upgrading the Application Software From a non-VLAN-Capable Server” on page 124
- “Upgrading the BSC Firmware” on page 126

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 SSL proxy blade software components are as follows:

- Application software
- BSC firmware

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

<http://www.sun.com/software/download/network.html>

To update the firmware and application software, there must be network connectivity between the B10p SSL proxy blade and the TFTP or FTP server. The B10p SSL proxy blade requires that all management traffic (including updates) must always be VLAN tagged.

A TFTP and FTP server can be made available as a:

- Server blade in the chassis
- Server connected to one of the SSC's uplinks

If a server is used that has a management VLAN interface configured, the management VLAN must be added to the respective port on the switch. If a server is used that does not have the VLAN configuration, refer to "Upgrading the Application Software From a non-VLAN-Capable Server" on page 124 for instructions how to create network connectivity between the server and the B10p SSL proxy blade.

Setting Up a TFTP Server

The procedures for upgrading software for the Sun Fire B10p SSL proxy blade involve using TFTP. Hence to use the blade, you need to have a TFTP server available on your network.

Note – If you are using separated data and management networks, set up a TFTP server available on both networks.

▼ To Set Up a TFTP Server

1. On the system that you intend to set up as the TFTP server, log in as root.
2. Use a text editor to un-comment the following line in the file `/etc/inetd.conf`:

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

3. On the same system create a TFTP home directory by typing the following at the Solaris prompt:

```
# mkdir /tftpboot
# chown root /tftpboot
# chmod 755 /tftpboot
```

4. Restart `inetd` by typing:

```
# /etc/init.d/inetd stop
# /etc/init.d/inetd start
```

5. Verify that TFTP is working.

To do this, use TFTP to get a file from the `/tftpboot` directory. Follow the instructions below:

- a. On the system that you are using as the TFTP server, copy any file (for example, the Solaris `/etc/release` file) to the `/tftpboot` directory.

Type the following command at the Solaris prompt:

```
# cp /etc/release /tftpboot/filename
```

Where *filename* is the name of the file you intend to make available on the TFTP server.

- b. Make the file you have just copied read-only:

```
# chmod 444 /tftpboot/filename
```

Where *filename* is the name of the file you intend to make available on the TFTP server.

Note – Note that TFTP is not the same as FTP. It does not display the same error messages as FTP, and you cannot use the `cd` or `ls` commands (or indeed most other commands) that FTP allows you to use.

Upgrading the Application Software From a VLAN-Capable Server

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 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.

Check <http://www.sun.com/supporttraining/> for information on upgrade packages. Copy the upgrade package 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 log in as `so` (security officer) to perform upgrades.

Executing Boot Upload Commands

This section describes how to use the `boot upload` commands for network-based software upgrades.

Note – If you enter `boot upload` before the management port(s) are configured correctly, the B10p blade prints a misleading message: `Admin IP or inband admin IP not set`. It is confusing because the B10p does not support the `set admin` command. The following is an example of the message.:

```
CLI# boot upload
Admin IP or inband admin IP not set. Set admin IP first.
CLI# set admin
Feature not supported with this platform.
```


A workaround to this message is to enter the following commands:

```
CLI# set manage
Enter port number (1..2) (1):
Enter inband (admin) IP Address (0.0.0.0): 192.168.1.115
Enter inband (admin) netmask (255.255.255.0):
CLI# set vlan filter
Enter enable/disable (enabled): disable
CLI# config save
```

Once the above commands are entered, you can successfully enter `boot upload`.

- **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 B10p SSL proxy blade.

▼ To Execute Boot Upload Commands Using an FTP Server

1. Stop the B10p SSL proxy blade if it is currently running.

```
CLI# stop
Stopped
```

2. Get the new image from the FTP server.

```
CLI# boot upload
Enter remote file name (update.pkcs): PSSL_1872.pkcs
Enter remote path (releases): /tftpboot/
Enter remote IP Address: (192.168.1.28): 192.50.50.10
Enter remote user name (labuser): root
Enter remote user password:

    connecting to 192.50.50.10
    starting to load image.
    Verification Successful.
    image loaded.
    Type boot activate to install.
```

3. Install the new image to take effect after the reboot.

```
CLI# boot activate
*** Warning. Do not turn off power! ***
    activating boot.

Updating boot image with BOOT1872.GZS
Update boot image complete.
    image updated.
    reboot to run new image.
CLI# 2003-08-07 22:02:37 UTC Sun_Fire_Blxp tCONSOLE : Config,
Updated image
```

4. Reboot the B10p SSL proxy blade to run the new image.

```
CLI# reboot

    Preboot Version [ 1872 ] Oct  1 2003
        Serial port [ OK ]
            System ID [ 1100001FEF09 ]
Preboot Checksum [ OK ]
        Data Bus [ OK ]
            Memory Chips [ 256 Mbit ]
                Address Bus [ OK ]
                    L3 Cache [ none ]
                        Tamper [ OK ]

=====
                Start Cause [ Hardware Reset ]
                    Start Type [ 00000000 ]
                        Loading Boot [ OK ]
```

```
Boot Version [ 1872 ]
    Created [ Oct  1 2003, 19:34:53 ]
Board Version [ 66 ]
Spartan Version [ 65 ]
    Revision [ 22 ]
    Cpu Speed [ 600 MHz ]
    Memory Size [ 400 MB ]
PCI Boot Configuration [ OK ]
    RTC [ OK ]
    Date [ OK ]
14423556
    Loading Application [ OK ]
        Test Memory [ OK ]
            RTC [ OK ]
            Date [ OK ]
    Flash File System [ OK ]
        Product ID [ SF B10p ]
        Load Mash [ OK ]
            Version [ MASH1005.GZ ]
        Load Buff [ OK ]
            Version [ BUFF3108.GZ ]
    Resetting Pci Bus [ OK ]
    PCI Configuration [ OK ]
        ISC Driver [ OK ]
            BootLine [ default ]
            Test Mash [ OK ]
            Test Buff [ OK ]
            Test Zoo [ OK ]
            Mash Date [ 2002/06/03 ]
            Buff Date [ 2003/07/22 ]
                Date [ 2003/10/11 ]
                Time [ 16:16:24 UTC ]
            DIMM Size [ 512 MB ]
```

▼ To Execute Boot Upload Commands Using a TFTP Server

1. Stop the B10p SSL proxy blade if it is currently running.

```
CLI# stop
      Stopped
```

2. Get the new image from the server.

```
CLI# boot upload-tftp
Enter remote file name (PSSL_1601.pkcs ): remote_package_filename
Enter remote IP Address: (192.168.0.28): remote_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.

3. 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.
```

4. 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 a Previous Software Version

If the upgrade has unwanted side effects, you can always revert to the previous version of software. The `boot activate` command swaps the current and backup versions, but does not swap the boot images. If the upgrade documentation indicates that a new version of the boot image is part of the upgrade, do not use the `boot activate` command 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 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 Factory Image, power on the SSL proxy blade, and press and hold the Esc key down until you are 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 factory image.

If the SSL proxy blade loses power during the upgrade process, the backup image may 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 are 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: 66 CPLD version: 65
  preboot 1872 Oct  1 2003
  boot 1872 Oct  1 2003
  app 1872 Oct  1 2003
  Buff: BUFF3108.GZ
  Mash: MASH1005.GZ

  Active:  BAPP: 1872, BOOT: 1872, MASH: 1005, BUFF: 3108
  Backup:  Not installed
  Required: BAPP: 1872, MASH: 1005, BUFF: 3108, CPLD: 65.22D

CLI#
```

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 (PSSL_1601.pkcs ): remote_image_filename
Enter remote path (releases): remote_directory
Enter remote IP Address: (192.168.0.28): remote_ip-addr
Enter remote user name (labuser): remote_username
Enter remote user password (): remote_user_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 (PSSL_1601.pkcs ): remote_image_filename
Enter remote IP Address: (192.168.0.28): remote_ip_addr
Connecting to 192.168.0.28
starting to load image
Verification Successful.
image loaded.
Type boot activate to install.
```

Upgrading the Application Software From a non-VLAN-Capable Server

You can configure the Sun Fire B1600 blade chassis to update the Sun Fire B10p SSL proxy blade image from a server that is not VLAN capable.

▼ To Update the Image From a Non-VLAN-Capable Server

1. Connect the network with this server to one of the eight uplinks of the chassis. In this example, the server is connected to port 0.
2. Insert the B10p SSL proxy blade into the chassis. In this example, slot 0 is used.
 - a. Choose a VLAN tag to be used for the management VLAN configured on the B10p SSL proxy blade. In this example, VLAN tag 3 is used.
 - b. Configure the B10p SSL proxy blade's networking with this VLAN and an appropriate IP address on the server's subnet.
3. From the SSC console, connect to the switch console.

```
sc> console SSC0/SWT
```

4. Log in to the switch console as the `admin` user; the default password is `admin`.

5. Add the VLAN to the database.

```
Console# config
Console(config)# vlan database
Console(config-vlan)# vlan 3 name SSL-mgmt media ethernet
Console(config-vlan)# end
```

6. Verify that the output of the `show VLAN` command contains the following line:

```
Console# show VLAN
3  Static          SSL-mgmt      Active
```

7. Add the VLAN to the B10p SSL proxy blade port.

```
Console# configure
Console(config)# interface ethernet SNP0
Console(config-if)# switchport allowed vlan add 3 tagged
Console(config-if)# end
```

8. Add the VLAN as the native VLAN to the uplink port.

```
Console# configure
Console(config)# interface ethernet NETP0
Console(config-if)# switchport allowed vlan add 3 untagged
Console(config-if)# switchport native vlan 3
Console(config-if)# end
```

9. Verify that the output of the `show VLAN` command contains the following line:

```
Console# show VLAN
3  Static          SSL-mgmt      Active      SNP0      NETP0
```

10. Verify that the output of the `show interfaces` command is similar to the following:

```
Console# show interfaces
VLAN membership mode: Hybrid
  Ingress rule: Disabled
  Acceptable frame type: All frames
  Native VLAN: 3
  Priority for untagged traffic: 0
  Allowed Vlan:    1(u),    3(u),
```

11. For the B10p SSL proxy blade slot, verify that the output of the `show interfaces switchport ethernet SNP0` command is similar to the following:

```
Console# show interfaces switchport ethernet SNP0
VLAN membership mode: Hybrid
  Ingress rule: Disabled
  Acceptable frame type: All frames
  Native VLAN: 1
  Priority for untagged traffic: 0
  Allowed Vlan:    1(u),    3(t),
```

There should now be network connectivity between the server and the B10p SSL proxy blade.

Upgrading the BSC Firmware

Note – To perform the update procedures in this chapter, you need to log into one of the system controllers using Telnet. This is because you need to transfer the new firmware from a location on your network.

The BSC on each blade server is a management agent for the system controller. It communicates information about the blade server it resides in to the system controller. It also receives and processes any commands that you type into the system controller's command-line interface.

Follow the instructions in this chapter if you have been advised by a Sun support engineer to download new firmware onto a System Controller, blade server, or integrated switch.

- Using the TFTP server from the server controller enter the following command:

```
sc> flashupdate -s tftp_ip -f filename sn
```

Where *S* indicates the slot and *n* is the number of the slot containing the blade you want to update. Valid slot numbers range from 0 to 15.

The following example shows the TFTP IP address as 10.4.128.103 and the file as /tftpboot/FRU/bsc-rel/scg-nrst-03.flash, updating the blade in slot 4. It also shows the messages that are returned and prompts:

```
sc> flashupdate -s 10.4.128.103 -f /tftpboot/FRU/bsc-rel/scg-nrst-03.flash S4
```

```
Warning: Are you sure you want to flashupdate the S4 bsc image;  
all console connections to S4 will be lost (y/n)? y
```

```
S4: Preparing to flashupdate.
```

```
Warning: Cannot determine supported blade type.
```

```
Do you want to continue (y/n)? y
```

```
Apr 10 19:22:46: MINOR: S4: Environmental monitoring disabled.
```

```
flashupdate: update 131072 bytes of 131072 completed on S4
```

```
S4: flashupdate complete.
```

```
Apr 10 19:23:55: MINOR: S4: OS Running.
```

```
Apr 10 19:23:56: MINOR: S4: Active LED state changed to ON.
```

```
Apr 10 19:23:56: MINOR: S4: Environmental monitoring enabled.
```


Security Primer

This appendix provides a quick overview of the basic security concepts that are useful to the SSL proxy blade administrator, especially those new to the area of SSL security. We provide selected references at the end of the section for those who become more interested in the field of security.

The following topics are addressed:

- “Encryption” on page 129
- “Authentication” on page 130
- “Secure Socket Layer” on page 130
- “SSL Accelerators” on page 131
- “Export” on page 132
- “SSL Proxy Blade Security Features” on page 133
- “Supported Ciphers” on page 134
- “Key Lengths” on page 137

Encryption

A key component of secure communications is that of hiding the message using encryption. Only the intended recipient should be able to read the message. The two types of common encryption algorithms are symmetric encryption and public key encryption.

Symmetric Key Encryption

In symmetric encryption, the sender and the receiver share a binary or text key. The key is used together with an algorithm to encrypt and decrypt the messages. The size of the key in bits determines the strength of the security provided.

Popular symmetric encryption algorithms are DES (56 bit), triple DES (168 bit) and RC4 (64 and 128 bit). The numbers in parenthesis are the typical key sizes. The larger the key size in bits, the stronger the security against an attacker.

Public Key Encryption

Public key encryption is an efficient way to exchange keys based on today's technology. In public key encryption, a key generation algorithm is used to generate a key pair, a public and private key. The public key can be made available freely to allow sender to encrypt messages intended for the owner of the private key. Only the private key can decrypt a message. The private key cannot be derived from the public key. In SSL, public key encryption is used only to exchange a randomly generated symmetric key. The reason is that using public key for the whole communication would be slower due to excessive computation.

Authentication

Authentication verifies that the message has not been altered, and verifies the identity of the receiver or sender.

In SSL, an authentication mechanism is used to verify the identity of the server or client who provide a certificate that is digitally signed by a recognized certificate authority (CA). The integrity of the data is verified by signing each SSL bulk message.

Secure Socket Layer

The Secure Sockets Layer (SSL) is a protocol to exchange data securely. SSL uses the Internet (that is, TCP/IP), as its communication mechanism. Commonly used browsers like Netscape™, are equipped with SSL clients. Thus, the most popular version of SSL (SSL 3.0) is available on most PCs. SSL 3.0 is believed to be secure and commonly used for eCommerce. The latest version of SSL (SSL 3.1) also called TLS 1.0, is not widely deployed yet. The SSL proxy blade supports SSL 3.0 and TLS 1.0. Commonly used web servers like Sun™ ONE Web Servers and Apache Web Servers with mod-SSL, support SSL and are compatible with the SSL proxy blade.

When a Browser connects to a server securely, for applications such as sending a credit card number or viewing bank account or stock trade information, the HTTPS protocol is used to establish an SSL session with the server. This session establishment is called an SSL handshake and it is very computation intensive due to the use of public key encryption to exchange the symmetric keys that will be used to encrypt the data. The public key algorithms used in the handshake are RSA or Diffie-Hellman, among others.

Following the SSL handshake, there is encrypted data transfer. The SSL client in the browser encrypts the data and the SSL server on the Web server decrypts the data. The server response is encrypted by the server and decrypted by the browser. The data is not only encrypted, but also digitally signed. The most common symmetric encryption algorithms used by SSL are DES, triple DES (3DES), and RC4. The hash algorithms used for the signature are MD5 and SHA-1.

Some of the items that make SSL secure for communications are: (1) the keys are never sent unencrypted, (2) the identities of the sender and receiver can be verified, and (3) the integrity of each message is authenticated.

SSL Accelerators

SSL accelerators come in two types: server side interface cards, and edge offload appliance systems. Both offload the SSL processing function from the server—the server side solution partially, and the offload appliance totally. The SSL proxy blade is a third-generation SSL acceleration system that provides performance in the thousands of handshakes per second. First and second generation devices operate from 200 to 600 SSL handshakes per second.

The figures of merit of SSL acceleration systems are listed below. Measuring these figures of merit might require a large number of clients and servers to provide sufficient load, and some figures lend themselves to interpretations depending on how the measurement is done and with what type of traffic. The following sections provide information about how to evaluate an SSL accelerator.

Sessions Per Second

The number of sessions per second is the number of handshakes per second that the accelerator can process. It is somewhat connected with the number of encryption operations that the internal engine or chip can perform.

In most systems, the net handshakes per second is much lower than what the engine can provide because there is much more to an SSL handshake than a decryption operation. Thus, information about internal speed of encryption/decryption chips does not carry a direct connection to system performance.

SSL provides a method to resume a session that enables you to omit calculations already expected the first time. When the performance measurement includes a typical number of sessions, the result is a more favorable performance rating.

Concurrent Sessions

The SSL proxy blade supports an unusually high number of concurrent sessions, compared to other products in the market, due to its Packetized SSL technology, which enables optimized handling of SSL connection and session state. The net result is that the SSL proxy blade can support up to 64K concurrent sessions for each SSL proxy blade.

Bulk Encryption Data Rate

The SSL proxy blade performs especially well at bulk encryption. The Packetized SSL technology uses a low overhead TCP/IP non-proxy stack, and the SSL proxy blade handles bulk traffic in hardware, which avoids overloading of data busses. Bulk encryption in the SSL proxy blade is handled at near line speeds and the architecture is designed to scale to multigigabit speeds.

Authenticated Software Upgrades

Software upgrades are a convenient feature of the SSL proxy blade that allows for secure updates and available feature upgrades. Because an SSL accelerator is a security product, an authenticated upgrade mechanism is used.

Export

The Sun Fire B10p SSL proxy blade is classified as retail status.

SSL Proxy Blade Security Features

Security is enforced by having sound security policies and best practices that are supported by the security features of the SSL proxy blade. The security features of the SSL proxy blade are described below.

User Access

User access control by means of a password ensures that unauthorized personnel will not affect the operation of the box.

Note – Passwords are alpha numeric, can include (-) and spaces, are case sensitive, and can be up to 15 characters long. The initial password is the same as the user type: User, Administrator, or Security Officer.

The first action to make the SSL proxy blade more secure is to change all the passwords, for User, Administrator, and Security Officer. The User has only view privileges, security officer the password for it can be blank.

Tamper Protection

The configuration of the SSL proxy blade, including the services private keys, is securely stored in encrypted form inside the SSL proxy blade persistent memory. The key to decrypt the configuration, called the Configuration Key, is randomly generated by the SSL proxy blade; thus, this key is never accessible to any user, so, or any external entity. The configuration key is stored in a special memory area, which is cleared if the blade enclosure is tampered with. After tampering, the system loses all custom configuration such as keys, certificates, and services. This is one of the reasons that configuration backups are recommended. If tampering occurs, please contact your Sun services representative.

Configuration Back Up

The configuration file of the SSL proxy blade contains all the information that can be configured in the unit. This includes certificates and associated private keys, service information, and network configuration parameters, among others.

The configuration should be backed up using the `export config` command. The `export config` command is only available to the `so`, and uses FTP to create an encrypted configuration file.

The `so` provides a Configuration Storage pass phrase every time the configuration is exported or imported. This Configuration Storage pass phrase determines the encryption key of the Configuration file. Thus, losing this pass phrase will render the backups unusable. Also, knowledge of this pass phrase might enable a security expert to decrypt the configuration file, thus exposing the private keys.

The SSL proxy blade provides a high degree of system security, yet overall security still depends on secure management of relevant keys, in this case, the Configuration Storage pass-phrase.

Exporting the configuration from one SSL proxy blade unit allows its configuration to be copied by importing the configuration to another SSL proxy blade.

Supported Ciphers

This section explains the ciphers supported by the SSL proxy blade.

TABLE A-1 Supported Ciphers

SSL ID	Name
0,3	RSA_EXPORT_WITH_RC4_40_MD5
0,4	RSA_WITH_RC4_128_MD5
0,5	RSA_WITH_RC4_128_SHA
1,8	RSA_EXPORT_WITH_DES40_CBC_SHA
1,9	RSA_WITH_DES_CBC_SHA
1,10	RSA_WITH_3DES_EDE_CBC_SHA
0,96	RSA_EXPORT1024_WITH_RC4_56_SHA
0,100	RSA_EXPORT1024_WITH_RC4_56_MD5

The first number of the SSL ID corresponds to the protocol number, 0 for SSL3 and 1 for TLS1. The second number corresponds to the cipher indicated in the name column. The name of the cipher can be broken in sub fields as indicated below.

- Protocol – SSL or TLS

- Public Key Algorithm – RSA, RSA_EXPORT
- Bulk Encryption Algorithm – RC4_40, RC4_128
- Bulk Signature Algorithm – MD5, SHA

The level of cipher security for a service can be set through the CLI to high, medium, or low. These settings correspond to a specific list of ciphers that guarantee a minimum security level for the server.

TABLE A-2 Security Levels for Ciphers

Cipher Level	Cipher List on This Level
High security	Cipher suites with key lengths larger than 128 bits: RSA_WITH_3DES_EDE_CBC_SHA
Medium Security	Cipher suites with key lengths equal to 128 bits or higher: RSA_WITH_3DES_EDE_CBC_SHA RSA_WITH_RC4_128_MDA RSA_WITH_RC4_128_SHA
Optimal (Medium security with high performance)	Includes all Medium security ciphers, except DES ciphers. RSA_WITH_RC4_128_MD5 RSA_WITH_RC4_128_SHA

TABLE A-2 Security Levels for Ciphers (*Continued*)

Cipher Level	Cipher List on This Level
Best (High compatibility with high performance)	Includes all Low security ciphers, except DES ciphers. RSA_WITH_RC4_128_MD5 RSA_WITH_RC4_128_SHA RSA_EXPORT_WITH_RC4_40_MD5 RSA_EXPORT_WITH_DES40_CBC_SHA RSA_EXPORT1024_WITH_RC4_56_SHA RSA_EXPORT1024_WITH_RC4_56_MD5
Low security (Highest browser compatibility)	Includes everything: RSA_WITH_3DES_EDE_CBC_SHA RSA_WITH_RC4_128_MD5 RSA_WITH_RC4_128_SHA RSA_WITH_3DES_CBC_SHA RSA_EXPORT_WITH_RC4_40_MD5 RSA_EXPORT_WITH_DES40_CBC_SHA SSL_RSA_EXPORT1024_WITH_RC4_56_SHA SSL_RSA_EXPORT1024_WITH_RC4_56_MD5
Export security (Mainly for export use)	RSA_EXPORT_WITH_RC4_40_MD5 RSA_EXPORT_WITH_DES40_CBC_SHA RSA_EXPORT1024_WITH_RC4_56_SHA RSA_EXPORT1024_WITH_RC4_56_MD5

The cipher is negotiated by the SSL endpoints. A configured service will only accept the particular cipher or accept negotiation to something equal or stronger.

The Export cipher enforces a maximum limit for the level of security in order to meet export laws.

If your intent is to set up security such that the connection is done with the highest security that the browser can support, then the cipher level that has this behavior is **low**.

Key Lengths

The SSL proxy blade supports the following RSA key sizes in bits: 512, 1024, and 2048. The SSL proxy blade can generate and import keys and certificates that use these sizes. Currently, 1024 bit is the recommended level of security for commercial applications.

Application Notes

A typical application of the SSL proxy blade is to offload SSL processing from servers. The network configurations vary depending on the application (eCommerce and Financial services), the total supported bandwidth, and level of fault tolerance. The advantage of the SSL proxy blade platform is that it scales from low-end to very high-end applications, as it provides the fastest transaction throughput, the largest number of concurrent sessions, and the fastest data transfer in the market by a large factor. This chapter includes application notes on various aspects of including the SSL proxy blade in new and existing network infrastructures.

The SSL proxy blade platform and associated models are many times superior than any other SSL accelerators in the market in all the three key figures of merit: SSL transactions per second, Bulk bandwidth, and concurrent sessions.

Web Server Configuration

In a typical eCommerce or Financial Services application, the user enters a non-secured home page using HTTP. The application switches to Secure HTTP (HTTPS) only when entering the check-out/purchase page where credit card information is requested, or after login into the member services. The switch to HTTPS can be implemented with HTTPS links or by forcing the plain text server to redirect the client to a different secure web server in the same or different system. The client uses HTTPS until the application switches back to the plain text server.

When the SSL proxy blade is introduced, the secure pages need to be served in clear text. Thus, the secure server is set up to listen in port 880, for example. If the SSL proxy blade clear port is set to 880, the secure server is set up to serve clear pages on port 880. The plain server does not require configuration change.

Redundant Systems

The SSL proxy blade often needs to be installed in fault tolerant networks. A true fault tolerant setup requires the main SSL proxy blade to fail over to another SSL proxy blade that has the same configuration. The fail over is done by the switch upstream of the two SSL proxy blade units.

Fail Over Unit Setup

The configuration of the main SSL proxy blade can be exported to a file and imported into the fail over unit. Depending on the network, the fail over unit may need a different network configuration, to be applied after the configuration transfer from the main unit.

Requesting a Certificate

Once you have generated a certificate request using the SSL proxy blade and also have exported the request to a file, it needs to be sent to a Certificate Authority (CA) so that a certificate will be issued. The process of obtaining a certificate is referred to as a certificate enrollment. Certificate enrollment procedures vary from CA to CA but in most cases, you either email the request or enter the information on the CA's web site. The CA ensures that the information you provided is accurate. Once the CA completes the issuance process, the certificate will be delivered to you by email.

Getting your certificate issued by a recognized CA is a guarantee that your server certificate will interoperate (be recognized and accepted) by well-known browsers such as Netscape.

Once the CA signed-certificate is available, it can be loaded into the SSL proxy blade. For SSL proxy blade commands on keys and certificates see Appendix A.

The following are well known certificate authorities:

- Verisign (<http://www.verisign.com>)
- Digital Signature Trust Company (<http://www.digsigtrust.com/>)
- GlobalSign (<http://www.globalsign.com/>)
- GTE Cybertrust (<http://www.cybertrust.gte.com/>)
- Entrust (<http://www.entrust.net>)
- Thawte (<http://www.thawte.com/>)

Managing Keys and Certificates

There are two main reasons why certificates require some management time.

- Expiration date – Certificates have an expiration date, thus you need to remember to renew them.

- Security issues – Certificates must correspond with their corresponding private key. Private keys are difficult to handle (transferred or backed-up) in a secure manner.

These issues become compounded with multiple certificates on multiple systems.

Key Management Features

Like for every other information system task, good organizational skills are the best recommendation to minimize certificate management time. Commercial key management systems are a good solution where tight security controls are required.

The SSL proxy blade supports key management in the following manners.

- The high performance and capacity of the SSL proxy blade supports centralized management of many certificates in a single SSL proxy blade.
- The export certificate command can be used to verify the expiration date of a certificate.
- The SSL proxy blade is compatible with key management systems.

Boot Information

This appendix shows a display of the information to the serial console during boot. This information may vary among different SSL proxy blade versions or upgrades, but the information will be similar to that shown in CODE EXAMPLE D-1.

CODE EXAMPLE D-1 Boot Information

```
Preboot Version [ 1872 ] Oct 1 2003
  Serial port [ OK ]
    System ID [ 1100001FEF09 ]
Preboot Checksum [ OK ]
  Data Bus [ OK ]
    Memory Chips [ 256 Mbit ]
    Address Bus [ OK ]
      L3 Cache [ none ]
      Tamper [ OK ]
=====
  Start Cause [ Hardware Reset ]
  Start Type [ 00000000 ]
  Loading Boot [ OK ]
  Boot Version [ 1872 ]
    Created [ Oct 1 2003, 19:34:53 ]
  Board Version [ 66 ]
  Spartan Version [ 65 ]
    Revision [ 22 ]
    Cpu Speed [ 600 MHz ]
    Memory Size [ 400 MB ]
  PCI Boot Configuration [ OK ]
    RTC [ OK ]
    Date [ OK ]
423556
  Loading Application [ OK ]
```

CODE EXAMPLE D-1 Boot Information

```
Test Memory [ OK ]
    RTC [ OK ]
    Date [ OK ]
Flash File System [ OK ]
    Product ID [ SF B10p ]
    Load Mash [ OK ]
    Version [ MASH1005.GZ ]
    Load Buff [ OK ]
    Version [ BUFF3108.GZ ]
Resetting Pci Bus [ OK ]
PCI Configuration [ OK ]
    ISC Driver [ OK ]
    BootLine [ default ]

Test Mash [ OK ]
Test Buff [ OK ]
    Test Zoo [ OK ]
Mash Date [ 2002/06/03 ]
Buff Date [ 2003/07/22 ]
    Date [ 2003/10/11 ]
    Time [ 16:16:24 UTC ]
DIMM Size [ 512 MB ]
```

SSL Statistics

This appendix lists and describes the key SSL statistics. The following topics are addressed:

- “Persistence of Statistics Counters” on page 145
- “Statistics Counters Important to SSL Proxy Blade” on page 146
- “Variable Descriptions” on page 147

Persistence of Statistics Counters

The statistics counter on the SSL proxy blade system are persistent. Thus, the statistics counters are not cleared on power-off or reboot. All statistics are accumulated since the last statistics reset. The `reset stats` command resets all statistics counters to zero.

Persistent statistics have better diagnostics value and provide better tracking and auditing because valuable information is not lost with power-off or reboot. To fully update counters on power-down, use the `shutdown` command. However, the counters are also updated every time the `config save` command is used.

Statistics Counters Important to SSL Proxy Blade

Performance

The SSL proxy blade exhibits very high performance in SSL handshakes per second, number of concurrent connections, and encrypted data throughput. To provide the best value, the SSL proxy blade comes in various models that exhibit different performance. These models can be upgraded by means of software. Thus, SSL proxy blade statistics counters include measures of the above performance figures. This is useful, both to display the value provided by the SSL proxy blade, and to determine when to upgrade to a higher performance model. Some counters are provided both as an *average* and as a *maximum value reached*, to facilitate decisions about model capacity required in installations with variable load. Variable loads can occur during the day, as a result of promotions, or seasonally.

SSL Connection vs. SSL Session

An SSL connection is the same as a TCP connection that uses SSL. An SSL session can include many connections if the SSL session ID is reused. When this happens, it is said that the SSL session was resumed. For example, the counter for concurrent SSL connections refers to the SSL connection and session concepts.

Session ID Reuse

Some statistics are associated with SSL session ID reuse. SSL can reuse an SSL session ID that was negotiated through a previous full handshake. When a session ID is reused, the handshake can be processed more quickly. Reuse of sessions ID is commonly used by the browser to retrieve objects on a given web page. Reuse is typically not extended to other pages because too much reuse can weaken the security associated with encryption.

To support reuse, the reuse IDs must be cached in the Reuse ID Cache. a cache miss is a rejection of a session that was not found in the cache. Rejections can also occur when the cache is full. In some types of traffic, reuse rejections can occur; for example, if more than 32,000 sessions are pending reuse. In most cases, reuse rejections due to cache full are not an indication of a problem, because those sessions

are negotiated as new, which actually increases the security. The SSL proxy blade can process a new session almost as fast as a reuse session, unlike most other implementations of SSL acceleration.

Variable Descriptions

Up Time

- Statistics begin date
 - Statistics display: Start stat. date 01/02/2001 05:04:32
 - Description: Date when statistics started. This is the same as the date of last statistics reset. This records the date from when statistics have been accumulated.
- Power-on time (persistent)
 - Statistics display: On time 14 hrs 33 min 30 sec
 - Description: Accumulated time ON since last statistics reset. This is not time since last reboot, but since last statistics reset. This tracks use or effective hours of service of the SSL proxy blade.
- SSL up time (persistent)
 - Statistics display: Up (traffic) time 10 hrs 06 min 02 sec
 - Description: Accumulated time is Start or SSL mode since last statistics reset. This is not time since last reboot, but since last statistics reset. This tracks effective hours on the network ready to pass SSL traffic.

Transactions Per Second (TPS)

- SSL Connection rate average
 - Statistics display: Connection rate ave.(1min) 830 [SSL/sec]
 - Description: Average number of successfully completed SSL connections in one second. The average is over one minute, with one second sampling rate. The SSL connection rate is also called SSL TPS (SSL Transactions Per Second). The TPS will normally not exceed the TPS limit of the SSL proxy blade model. Use `show features` to see the TPS limit. The TPS information is useful to determine the TPS load that the SSL proxy blade is processing. The TPS number should match that reported by external test tools that may be used for evaluation in a test environment, such as WebBench, or by sniffer equipment. When the TPS load varies within a second or a minute, and the sampling rate or the average time of the tool is different than that of the SSL proxy blade, some minor differences may be observed due to averaging.

- Maximum SSL connection rate (persistent)
 - Statistics display: Connection rate max. 1200 [SSL/sec]
 - Description: Maximum value of the connection rate average (or TPS, see “Transactions Per Second (TPS)” on page 147) that occurred since the last time the statistics counters were reset to zero. Connections that are “Reusing” the SSL session ID are also counted. The maximum TPS will normally not exceed the TPS limit of the SSL proxy blade model. Use `show features` to see the TPS limit. The Max. TPS information is useful to determine if the TPS limit is being reached, in which case, a TPS feature upgrade or an additional SSL proxy blade system should be obtained.
- TPS Limit Counter (persistent)
 - Statistics display: TPS requests 3,200,000
 - Description: Number of SSL requests rejected (forces client to retry) due to TPS limit reached. The TPS average went above the TPS feature limit, and this caused a rejection of a connection. SSL rejections due to other causes are not included here. Any number larger than zero means that traffic reached the SSL proxy blade TPS capacity after statistics were reset.

Concurrent Connections

- Concurrent SSL connections
 - Statistics display: Concurrent connections (now) 5,000
 - Description: Number of concurrent connections open at the current time. Connections that are “Reusing” the SSL session id are also counted. The number of concurrent connections will normally not exceed the concurrent connection limit of the SSL proxy blade model. Use `show features` to see the concurrent connection limit. The concurrent connection information is useful to determine if the concurrent connection limit is being reached, in which case, a performance/feature upgrade or an additional SSL proxy blade system should be obtained. A single SSL proxy blade can handle at least 16000 concurrent sessions.
- Maximum concurrent SSL connections (persistent)
 - Statistics display: Concurrent connections max. 16,000
 - Description: Maximum number of concurrent connections that were reached since last statistics reset. Connections that are “Reusing” the SSL session ID are also counted. The maximum number of concurrent connections will normally not exceed the concurrent connection limit of the SSL proxy blade model. Use `show features` to see the concurrent connection limit. The concurrent connection information is useful to determine if the concurrent connection limit is being reached, in which case, a performance/feature upgrade or an additional SSL proxy blade system should be obtained. A single proxy blade can handle at least 16000 concurrent sessions.
- Concurrent SSL Connections Limit Counter (persistent)
 - Statistics display: Concurrent limit 20,000

- Description: Number of SSL requests rejected (forces client to retry) due to concurrent connections limit being reached. The concurrent connections went above the concurrent connection feature limit, and this caused a rejection of a connection. SSL rejections due to other causes are not included here. Any number larger than zero means that traffic reached the SSL proxy blade concurrent connection capacity after statistics were reset.

Throughput

- SSL data throughput delivered to the server (persistent)
 - Statistics display: Clear data in [KB]: 350,009
 - Description: Accumulated bytes of data delivered to the server using SSL. Thus, it is the SSL data throughput of the incoming (inbound) traffic channel, that is, from client to server. This counter is persistent since last statistics reset. This measure is about payload delivered to the servers. This counter includes all SSL proxy blade ports with traffic to the servers. Thus, this measure includes all effective data (by SSL only) that goes from client to server. Network overhead (retries) and encryption overhead (handshake, signatures) are not included. The counter relies on the TCP sequence numbers to track the data payload byte count.
- SSL data throughput returned by the server (persistent)
 - Statistics display: Clear data out [KB]: 4,350,002
 - Description: Accumulated bytes of data returned by the server using SSL. Thus, it is the SSL data throughput of the outgoing (outbound) traffic channel, that is, from client to server. This counter is persistent since last statistics reset. This measure is about payload delivered to the clients. This counter includes all SSL proxy blade ports with traffic from the servers to the clients. Thus, this measure includes all effective data (via SSL only) that goes from Server to Client. Network overhead (retries, etc.) and encryption overhead (handshake, signatures) are not included. The counter relies on the TCP sequence numbers to track the data payload byte count.
- Number of TCP requests (persistent)
 - Statistics display: TCP requests 3,200,000
 - Description: Number of accumulated TCP requests. Any type, clear and secure, broadcast or not.

SSL Handshakes

- Number of SSL requests (persistent)
 - Statistics display: SSL requests 3,000,000

- Description: Number of SSL handshake requests accumulated since last statistics reset. SSL handshakes completed, and also those not completed, are counted. Handshakes with a reused SSL session ID are also counted. This counter captures all SSL requests.
- Number of completed SSL handshakes (persistent)
 - Statistics display: SSL handshakes 2,900,000
 - Description: Number of successfully completed SSL Handshakes, accumulated since last statistics reset. Handshakes with reused SSL session ID are also counted. A difference between handshake requests and completed handshakes is the number of failed handshakes. Handshakes can fail for a variety of reasons, from bad certificates to performance limitations. The statistics counters provide a quick way to analyze the SSL traffic behavior.

SSL Handshakes With Reused Session IDs

- Number of SSL requests with reused SSL session IDs (persistent)

Statistics display: SSL requests/ Reuse 2,500,000

Description:

Number of SSL Handshake requests with a reused ID, accumulated since last statistics reset. This counter includes only reused handshakes. Reuse SSL handshakes completed, and also those not completed, are counted.
- Number of Reuse ID requests found in cache (persistent)
 - Statistics display: SSL Reuse/ Reuse hit 1,056
 - Description: Number of reuse SSL requests found in the reuse ID cache. This count is accumulated since last statistics reset.

Number of Dropped Reuse ID Requests (Persistent)

- Reuse request drops due to ID not in cache.
 - Statistics display: SSL Reuse/ Reuse drop/ Look-up miss 56
 - Description: Number of reuse SSL requests dropped because of a session ID look-up miss; that is, the SSL session ID not found in the cache. This does not include cache full or timeout. This is not common.
- Reuse request drops due to reuse cache full.
 - Statistics display: SSL Reuse/ Reuse drop/ Cache full 23
 - Description: Number of reuse SSL requests dropped because of a session ID look-up miss; that is, the SSL session ID is not found in the cache. This is most likely due to timeout or full reuse cache.
- Reuse request drops due to timeout.

- Statistics display: SSL Reuse/ Reuse drop/ Timeout 85
- Description: Number of reuse SSL requests dropped because of a session ID look-up miss; that is, the SSL session ID is not found in the cache. This is most likely due to timeout or full reuse cache.

Troubleshooting

This appendix outlines some common troubleshooting issues associated with identifying and fixing a problem initially associated with the SSL proxy blade.

This appendix contains the following sections:

- “Sanity Check” on page 153
- “SSL Proxy Blade Troubleshooting Information Sources” on page 153
- “Basic Troubleshooting Principles” on page 154
- “Most Common Problems for the SSL Proxy Blade” on page 154

Sanity Check

Very often a small problem can cause downtime and escalate into a big problem, or confuse the troubleshooting process.

These are the first steps that Sun Support will ask you to do, so please check all of the following prior to contacting Sun Microsystems technical support:

- Verify that the SSL proxy blade is powered on.
- Verify that you can ping the Admin port of the SSL proxy blade.
- Browse a server web page and verify the browser indicates encrypted traffic.

SSL Proxy Blade Troubleshooting Information Sources

Gather information provided by the SSL proxy blade.

- Check the Boot messages. Use serial terminal during boot up.
 - Check SSL proxy blade statistics (`show stats`).
 - Check the log (`export log`).
 - Check module version information (`show boot`).
-

Basic Troubleshooting Principles

The basic troubleshooting principles are listed below:

- Analyze the symptoms
 - Gather relevant data (from logs, diagnostics, configuration, and versions)
 - Work from a known state
 - Eliminate as many variables as possible. Simplify the problem.
 - Change one variable at a time
 - Try to make the problem reproducible
 - Consider effects of recent changes in the system.
-

Most Common Problems for the SSL Proxy Blade

The most common reported problems occur in the following categories.

- Configuration errors
 - Incomplete or wrong SSL proxy blade configurations that can be traced with the sanity checks indicated in “Sanity Check” on page 153.
- Network environment setup
 - Assumptions about equipment other than the SSL proxy blade that are not correct for the environment. This is especially true in terms of performance expectations of other devices when configured with particular functions.

Alphabetical Command Reference

This appendix provides an alphabetical listing of all the SSL proxy blade commands.

A

alias Text substitution

B

boot Manage field upgrades of software versions
boot activate Activate backup image
boot revert Restore factory installed software
boot upload Upload new system image using FTP.

C

clear Clear the screen
config Manage system configuration
config compare Compare configuration and flash
config default Set configuration to factory defaults

config read	Read configuration from flash
config reset	Reset configuration from flash
config save	Save configuration to flash
create	Create a key, certificate, signature, or service
create certificate	Generate a certificate
create key	Create a key
create service	Create a service
create certrequest	Generate a signing request

D

delete	Delete a key or service
delete all keys	Delete all keys
delete all services	Delete all services
delete features	Delete features
delete key	Delete key
delete service	Delete service

E

exit	Exit intermediate mode
export	Export a key, certificate, signature or configuration
export certificate	Export a certificate
export ftp certificate	Export a certificate via FTP
export ftp certrequest	Export a signing request via FTP
export features	Export feature coupon
export ftp config	Export current configuration

export ftp features	FTP export feature coupon
export ftp key	Export a key via FTP
export ftp log	Export the log file via FTP
export ftp mem	FTP export memory log
export key	Export a key
export log	Export the log file
export mem	Export the log memory
export tftp certrequest	Export a signing request via TFTP
export tftp certificate	Export a certificate via TFTP
export tftp config	Export current configuration
export tftp features	TFTP export feature coupon
export tftp key	Export a key via TFTP
export tftp log	Export the log file via TFTP
export tftp trace	TFTP export trace

H

help	Show command help
history	Show command history

I

import	Import a key, certificate, signature or configuration
import certificate	Import a certificate via copy/paste
import key	Import a key pair via copy/paste
import ftp certificate	Import a certificate via FTP
import config	Import configuration

import ftp config Import and set current configuration via FTP
import ftp key Import a key pair via FTP
import tftp certificate Import a certificate via TFTP
import tftp config Import and set current configuration via TFTP
import tftp key Import a key pair via TFTP
import features Import feature license (for performance upgrade)

L

logout Log off this system

P

ping Ping a remote IP address form the admin. port.

R

reboot Reboot system
reset stat Reset statistics counters
start Start SSL processing

S

set Set information
set attrib ssl cipher Set cipher strength
set attrib tcp idletime Set connection idle time

set autorun	Set autorun
set clsralrt-chk	Set ClosureAlert check for SSL session end
set console	Set console-display
set defcert	Set default certificate parameters
set defservice	Set default service parameters
set gateway	Set gateway
set lines	Set number of lines for the display
set log	Set logging destinations: serial, file, syslog
set ntp	Set NTP server IP address and TCP port
set password	Set a new password
set port	Set secure and clear ports
set portpair	Set secure and clear portpair(s)
set routed	Set routed info (port no., router IP addresses)
set trace	Set trace state
setup	First time system initialization
show	Show commands
show all	Display system information
show attrib ssl	Display a service's SSL attributes
show attrib tcp	Display a service's TCP attributes
show autorun	Display autorun (starts on reboot)
show boot	Display available software versions
show ca	Display the list of all known certificate authorities (CAs)
show clsralrt-chk	Display ClosureAlert check for SSL session end
show config	Display system information
show console	Display the console-display settings
show date	Display the date
show defcert	Display default certificate parameters
show defservice	Display default service parameters

show failover-opt	Display failover options (health check interval, MAC address swapping)
show features	Display the features
show gateway	Display the gateway
show inband	Display inband data info (port, IP address, netmask)
show interface	display the Ethernet interface settings
show lines	Display number of lines per screen
show log	Display log settings
show mac	Display the administration and inband MAC address
show management	Display inband admin info (port, IP address, netmask)
show ntp	Display NTP server IP address and TCP port
show port	Display secure/clear TCP ports
show portpair	Display secure/clear TCP portpair(s)
show routed	Display routed information (port, router IP addresses)
show router	Show router IP addresses
show serial	Display serial settings
show snmp	Display whether snmp support is enabled or disabled.
show state	Display system state
show stats	Display session statistics
show trace	Display trace state
show version	Display software version
show vlan client	Display global client VLAN tag
show vlan filter	Display VLAN filter state
show vlan inband	Display inband VLAN tags (one per port)
show vlan management	Display management VLAN tags (one per port)
shutdown	Shut down
start	Start SSL connection(s) processing
stop	Stop SSL processing

T

traceroute Trace route to a remote IP address

W

who Display users currently logged in

write Write text to another user

Glossary

This glossary contains definition of terms that appear throughout the user's guide.

- admin port** Dedicated Ethernet port for administration use.
- clear** Clear text, clear port, and similar terms refer to non-encrypted data
- in-band traffic** A network traffic that reaches the in-band ports, as opposed to the administration port. The in-band ports are usually connected to switches or other production network devices, while the administration traffic is sometimes confined to an administration private LAN.
- incoming traffic** Traffic that goes from the client to the server.
- inline** A mode of operation in which the client traffic and server traffic each use a separate physical port on the SSL proxy blade.
- outgoing traffic** Traffic that goes from the server to the client.
- secure** Secure port and similar terms refer to encrypted data.
- traffic ports** Ethernet ports used for traffic. There are two traffic ports, also called in-band ports.
- watchdog** The SSL proxy blade has a watchdog device that checks for an electronic heart beat of a supervisory process. This process checks all other supervised processes. If the watchdog misses a heart beat, it will reboot the SSL proxy blade, which allows recovery in case of unexpected failure or loss of control.

Index

NUMERICS

10/100/1000BASE-T Data Network Port
Pinouts, 26

A

Authenticated software, 132
Authentication, 130

B

boot
 activate, 122
 revert, 123
 show, 122
 upload, 123
Bulk encryption data rate, 132

C

Certificate
 CA signed, 81, 82
 create, 90, 94
 Default information, 93
 export, 93
 export certrequest, 96
 export certrequest(ftp), 95
 export certrequest(tftp), 95
 export(ftp), 92
 export(tftp), 93

formats, 85
import, 92
Import from a server, 84
import(ftp), 91
import(tftp), 91
Request, 94
self signed, 81, 82
set defcert, 94
show defcert, 93

Concurrent sessions, 132

config
 compare, 77
 default, 78
 save, 78

Configuration
 compare, 77
 default, 78
 export(ftp), 79, 80
 import(ftp), 81
 reset, 78
 save, 78

Configuration Storage, 76

create
 certificate, 90, 94
 key, 86
 service, 97

D

delete
 key, 98
Diagnostics, 100

E

Encryption, 129

Event Logging, 104

export

- certificate, 93
- certificate(ftp), 92
- certificate(tftp), 93
- certrequest, 96
- certrequest(ftp), 95
- certrequest(tftp), 95
- config(ftp), 79, 80
- key, 89
- key(ftp), 89
- key(tftp), 89
- log, 108, 109

H

hardware installation, 19

I

import

- certificate, 92
- certificate(ftp), 91
- certificate(tftp), 91
- config(ftp), 81
- key, 88
- key(ftp), 87
- key(tftp), 87

K

Keys and Certificates, 81

L

LED status codes, 23

Log commands, 107

P

ping, 101

ports

location of, 24

power off a blade, 29

power on a blade, 27

Private key

- create, 86
- delete, 86, 98
- export, 89
- export(ftp), 89
- export(tftp), 89
- import, 88
- import(ftp), 87
- import(tftp), 87

Private keys

show, 86

R

reboot, 121

Redundant systems, 140

S

Secure Socket Layer, 130

Security Primer, 129

serial port

pin numbers, 27

Service

create, 97

Services

show, 99

Set

ports, 72, 73

set

- defcert, 94
- lines, 101
- link, 74
- log file, 107
- log mem, 108
- log serial, 107
- log syslog, 107

show

- ciphers, 100
- defcert, 93
- interface, 75

- keys, 86
- link, 74
- log, 108
- ports, 72
- services, 99
- stats, 102
- version, 121

shutdown

- forcing, 30
- orderly, 29

SSL Accelerators, 131

standby mode, 30

Statistics, 101

System Images, 4

system state, 68

T

- TCP ports, 71
- TFTP
 - setting up a TFTP server, 114
- TPS, 131

V

- VLANs, 9

W

- Web Server Configuration, 139

