



By implementing Brocade Secure Fabric OS, organizations can achieve the high levels of data and system security as well as improved change management controls that today's business requirements demand.

SECURE FABRIC OS

Highlights

- Significant improvement in SAN security
- Centralized security management
- Flexible security and policy administration
- Complementary function for Brocade Advanced Zoning capabilities
- Simplified management with the optional Brocade Fabric Manager

A comprehensive security architecture for SAN fabrics

As organizations grow their Storage Area Networks (SANs) and interconnect them over longer distances through existing networks, they have an even greater need to effectively manage SAN security and policy requirements.

To help these organizations improve security, Brocade® has developed Secure Fabric OS®, a comprehensive security solution for Brocade-based SAN fabrics. With its flexible design, Secure Fabric OS enables organizations to customize SAN security in order to meet specific policy requirements. In addition, Secure Fabric OS works with a security practice already deployed in many SAN environments: Brocade Advanced Zoning.

The most complete solution for securing SAN infrastructures, Secure Fabric OS includes the following features:

- Fabric Configuration Servers (“trusted” switches)
- Management Access Controls
- Device Connection Controls

- Switch Connection Controls
- Secure Management Communications

FABRIC CONFIGURATION SERVERS

Fabric Configuration Servers are trusted Brocade SilkWorm® fabric switches responsible for managing the configuration and security parameters (including zoning) of all other switches in the fabric. Any number of switches within a fabric can be designated as Fabric Configuration Servers as specified by World-Wide Name (WWN), and the list of designated switches is known fabric-wide.

As part of the security policy configuration process, organizations select a primary Fabric Configuration Server and potential backup servers. Only the primary Fabric Configuration Server can initiate fabric-wide management changes, and all initiation requests must be authenticated to ensure fabric security—a capability that helps eliminate unidentified local management requests initiated from subordinate switches.

MANAGEMENT ACCESS CONTROLS

Management Access Controls enable organizations to restrict management service access to a specific set of end points—either IP addresses (for SNMP, Telnet, HTTP, or API access), device ports (for in-band methods such as SES or Management Server), or switch WWNs (for serial port and front-panel access). Disabling front-panel access to switches prevents unauthorized users from manually changing fabric settings.

Device ports are specified by WWN and typically represent Host Bus Adapters (HBAs).

DEVICE CONNECTION CONTROLS

Device Connection Controls—also known as WWN Access Control Lists (ACLs) or Port ACLs—enable organizations to bind an individual device port to a set of one or more switch ports. Device ports are specified by WWN and typically represent HBAs (servers).

These controls secure the server-to-fabric connection for both normal operations and management functions. By binding a specific WWN to a specific switch port or set of ports, Device Connection Controls can prevent a port in another physical location from assuming the identity of a real WWN. This capability enables better control over shared switch environments by allowing only a set of predefined WWNs to access particular ports in the fabric. This also helps prevent accidental attachment of devices to a specific port.

SWITCH CONNECTION CONTROLS

Switch Connection Controls enable organizations to restrict fabric connections to a designated set of switches, as identified by WWN. When a new switch is connected

to a switch that is already part of the fabric, the two switches must be mutually authenticated. As a result, each switch must have a digital certificate and a unique public/private key pair to enable truly authenticated switch-to-switch connectivity.

New switches receive digital certificates at the time of manufacture. However, organizations with existing switches will need to upgrade them with a certificate at the installed location.

Switch-to-switch operations are managed in-band, so no IP communications are required. This capability prevents users from arbitrarily adding switches to a fabric, which helps improve change management. Any new switch must have a valid certificate and also appear in the fabric-authorized switch ACL. Digital certificates ensure that the switch name (WWN) is authentic and has not been modified.

SECURE MANAGEMENT COMMUNICATIONS

Brocade switches enable secure IP-based management communications between a

switch and a management console or the fabric manager. Certain elements of the manager-to-switch communications process—such as passwords—are encrypted to increase security (see Figure 1). Secure Shell (SSH v2) support is available on certain switch models.

COMPREHENSIVE FABRIC SECURITY

Because a network is only as secure as its weakest link, all switches in the fabric must support Secure Fabric OS in order to achieve the highest level of security fabric-wide.

MAXIMIZING SAN INVESTMENTS

Brocade and its partners offer complete SAN solutions to meet a wide range of technology and business requirements. These solutions include education and training, support, service, and professional services to help optimize SAN investments. For more information, contact an authorized Brocade sales partner or visit www.brocade.com.

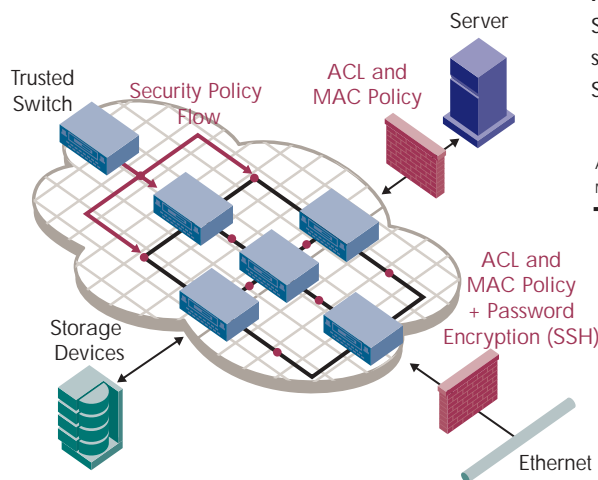


Figure 1. Secure Fabric OS provides security for heterogeneous SANs or SAN fabrics.

ACL = Access Control List
MAC = Management Access Control
— Certificate-based authentication and ACLs between all switches



Corporate Headquarters

San Jose, CA USA
T: (408) 333-8000
info@brocade.com

Asia Pacific Headquarters

Tokyo, Japan
T: +81-3-5402-5300
apac-info@brocade.com

European Headquarters

Geneva, Switzerland
T: +41 22 799 56 40
emea-info@brocade.com

Latin America Headquarters

Miami, FL USA
T: (305) 716-4165
latinam-sales@brocade.com

© 2004 Brocade Communications Systems, Inc. All Rights Reserved. 01/04 GA-DS-105-04

Brocade, the Brocade B weave logo, Secure Fabric OS, and SilkWorm are registered trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON is a registered trademark of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States Government.