

As a greater number of organizations implement larger Storage Area Networks (SANs), they are facing new challenges in regard to data and system security.

SECURE FABRIC OS

Highlights

- Significant improvement in SAN security
- Additional management controls
- Flexible security and policy administration
- Complementary function for Brocade advanced zoning capabilities

A comprehensive security architecture for SAN fabrics

A COMPREHENSIVE SAN SECURITY SOLUTION

Especially as organizations interconnect SANs over longer distances through existing networks, they have an even greater need to effectively manage their 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 in conjunction with an industry-leading security practice already deployed in many SAN environments: advanced Brocade Zoning™.

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

- Fabric Configuration Servers
- Management Access Controls

- Device Connection Controls
- Switch Connection Controls
- Secure Management Communications

FABRIC CONFIGURATION SERVERS

Fabric Configuration Servers enable the use of “trusted” Brocade SilkWorm® Fibre Channel fabric switches that are responsible for managing the configuration and security parameters 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 identified to ensure fabric security.

This capability helps eliminate unidentified local management requests initiated from “untrusted” 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, 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.

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 before the new switch can join

the fabric. As a result, each switch must have a digital certificate and a unique private key to enable truly secure 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 certificate and key information 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. Any new switch must have a valid certificate and also appear in the fabric ACL. Digital certificates ensure that the switch name (WWN) is authentic and has not been modified.

SECURE MANAGEMENT COMMUNICATIONS

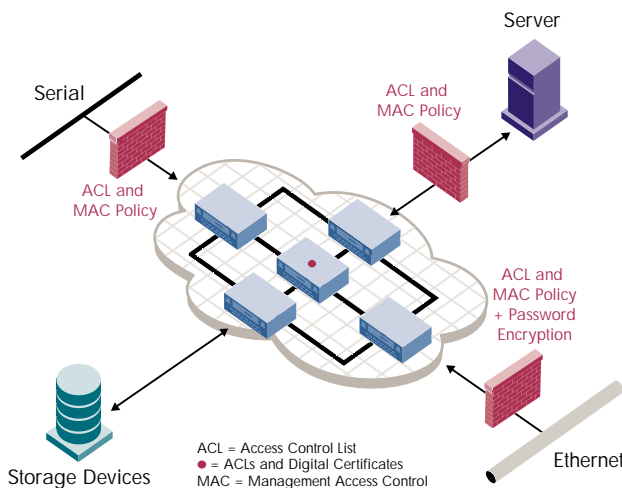
Brocade switches enable secure IP-based management communications between a switch and a manager. Certain elements of the manager-to-switch communications process—such as passwords—are encrypted to increase security.

COMPREHENSIVE FABRIC SECURITY

Because a network is only as secure as its weakest link, either the entire fabric is secure or none of the fabric is secure. As a result, all switches in the fabric must support Secure Fabric OS in order to achieve the highest level of security fabric-wide.

Secure Fabric OS is the initial component of a comprehensive security architecture designed to ensure a secure fabric-wide enterprise without requiring redundant dual fabrics. This approach supports the need to centralize management tasks while helping to accelerate SAN growth and reduce the total cost of ownership. By implementing Brocade Secure Fabric OS throughout their SAN fabric infrastructures, organizations can achieve the high levels of data and system security that today's business requirements demand.

For more information, visit www.brocade.com.



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



Corporate Headquarters

1745 Technology Drive
San Jose, CA 95110
T: (408) 487-8000
F: (408) 487-8101
info@brocade.com

European Headquarters

29, route de l'Aéroport
Case Postale 105
1211 Geneva 15, Switzerland
T: +41 22 799 56 40
F: +41 22 799 56 41
europe-info@brocade.com

Asia Pacific Headquarters

Brocade Communications Systems, Inc.
The Imperial Tower 15th Fl.
1-1-1 Uchisaiwaicho
Chiyoda-ku, Tokyo 100-0011, Japan
T: +81 35219 1510
F: +81 33507 5900
apac-info@brocade.com