CipherMax

SAN*Cruiser*™

Graphical SAN and Security Management System for CipherMax Storage Security Systems

HIGHLIGHTS

Global administration of all CipherMax devices throughout the enterprise storage environment

GUI-enabled navigation of every level of the Fibre Channel fabric topology

Discrete storage and security administrative roles enforces natural separation of duties

Centralized point of management for LTO-4 tape drive encryption policy and key management

Easy-to-use drag-and-drop interfaces for zone, access control and system management

Configuring systems and ensuring consistent policy enforcement across distributed enterprise storage environments can be a huge challenge with first generation point solutions for storage security. SAN*Cruiser* allows SAN and security administrators to easily configure, monitor and maintain storage security services with a Graphical User Interface (GUI)-based, global management system. SAN*Cruiser*'s intuitive dialogs and displays provide a single point of management for all CipherMax systems distributed across an entire enterprise. SAN*Cruiser* is a Java-based client-server application and supports clients running on Linux- and Windows®-based platforms.

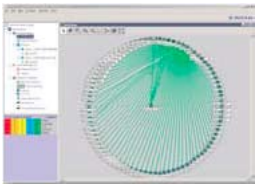
SAN*Cruiser* provides a suite of integrated, flexible tools for managing storage networks and security services supported by CM systems and LTO-4 encrypting tape drives. Real-time displays of SAN fabric topology and zone maps, and auto-discovery views of servers and storage devices, including LUN information, simplify system management and assist the storage administrator in configuring access control mappings. SAN*Cruiser* makes security administration easy by providing a single point of management for validating access control mappings and assigning encryption keys. SAN*Cruiser* also provides complete management of the CM environment from monitoring chassis temperatures to upgrading firmware on all systems, both local and remote.

The user interface for SAN*Cruiser* has been designed to be intuitive and simple to use. Fabric-based intelligence and simplicity of use makes administrative tasks easier and less prone to error. A powerful drag-and-drop interface manages up to thousands of security policies for multiple CipherMax systems in single or clustered configurations.

Product Features

World View Map

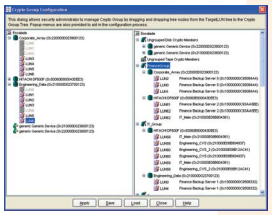
Most SANs consist of a mesh of devices that require multiple management tools. SAN*Cruiser* quickly discovers and navigates the topology of all of the fabrics and devices in the entire storage network. To help SAN and security administrators view and navigate large storage networks, SAN*Cruiser* provides a hierarchy of topology maps that present the administrator with different levels of SAN topology. At the top of the hierarchy is the World View map,



a detailed, color-coded graphical view of the current state and type of all network entities managed by—or visible to—SAN*Cruiser*. An administrator can also drill down to view the topology map for each individual fabric, where failed links and devices are graphically displayed. SAN*Cruiser* also provides a set of convenience tools that allow an administrator to zoom and pan all topology maps. SAN*Cruiser* supports Fibre Channel (FC) in-band discovery of third-party switches and storage devices that conform to the T11 FC-SW and FC-GS set of standards.

Global Security Policy Administration

A discrete security management interface with optional RADIUS user authentication provides a natural separation of duties between SAN and security groups for system configuration and management tasks throughout the entire SAN. Storage administrators define access control mappings between initiator (host) and target (LUN) groups that restrict data access to authorized systems. Security administrator



approval is required to activate the access control mappings. Security administrators can then attach a security policy to the mappings that enforces the application of encryption based on the organization's business-level security policy. This access control visibility enables storage administrators to effectively perform their job duties while providing security administration with control over data viewing.

Key*Cruiser* Integration

To ensure the recoverability of data at all times, SAN*Cruiser* works seamlessly with the Key*Cruiser* key lifecycle management system. Key*Cruiser* maintains a nearline backup of the entire encryption key database, providing fast access to keys and system configurations for recoverability at the media, LUN or device level.

Zone Management

SAN*Cruiser* uses a drag-and-drop interface to configure zone sets and to add or remove a port or node from a zone. Multiple fabrics can be viewed and configured simultaneously, and the switch ports associated with the attached devices are displayed graphically, reducing the need to switch between views. SAN*Cruiser*'s unique ability to filter the topology map based on zone sets dramatically improves a manager's view of SAN fabric configurations. Ports and nodes can be grouped together and associated with user-friendly alias names supported across the entire fabric, including third-party switches. SAN*Cruiser* integration of zone management with security policy management prevents users from making errors in the configuration of their secure SAN fabric.

SAN Fabric Inventory

SAN*Cruiser* automatically captures an inventory of all devices in the SAN fabric under management. Easy-to-use views display the inventory categorically, including CM systems, third party switches, hosts, devices and their LUNs, and the properties of these devices.

Chassis Management

Administrators can see at a glance from the real-time, graphical representation of the chassis, which ports are active and which are not. The properties, status and access to each chassis element, such as cards and ports, can be viewed by selecting the relevant object.

Performance Management

A real-time display shows individual port performances, as well as advanced statistics, error counters, zoning violations, and performance-tuning parameters.

Fault Management

The Network Events View shows a detailed list of the status and source of all storage administrative network events. The Alarm Count View and Alarm Table show a real-time, detailed, color-coded statistical window of each device condition. Severity levels define how alarms are displayed and a remote alert notification system sends alarms via email or pager to administrators based on severity levels.

Firmware Management

SAN*Cruiser* manages firmware upgrades of any CM system throughout an enterprise. Fail-safe remote system upgrades are performed using a three-stage process (download, apply, rollback or commit) which allows users to test-run a new release without losing the ability to revert back to an old release.

Security Configuration Recovery

In the event of an unrecoverable system failure, SAN*Cruiser* allows the recovery of a CipherMax system security configuration using a quorum-based (M of N) authorization model. By querying the Key*Cruiser* database or accessing a CM configuration backup file, Security Administrators are able to quickly and easily duplicate the security access and encryption parameters of the previous system.

CORPORATE HEADQUARTERS
CipherMax, Inc.
1975 Concourse Drive
San Jose, CA 95131 USA
Tel: +1-408-382-6500
Fax: +1-408-382-6599

CIPHERMAX ASIA-PACIFIC
CipherMax, Inc.
Room 1035
Shanghai Central Plaza
381 Huai Hai Zhong Lu
Shanghai, 200020
Tel: +86-13601216832

ADDITIONAL CONTACTS
General: info@ciphermaxinc.com
Partners: partners@ciphermaxinc.com
Sales: sales@ciphermaxinc.com
Technical Support: 1-800-670-4423

WEBSITE
www.ciphermaxinc.com

CipherMax

© 2008 CipherMax Inc. CipherMax, the CipherMax logo, CM140T, CM180D, CM250, CM500, Key*Cruiser*, SAN*Cruiser*, SecureDR, SecureRemote and SecureVTL are registered trademarks or trademarks of CipherMax, Inc. in the United States and other countries. All other company and product names may be trademarks or registered trademarks of the respective organizations. P/N 61-00047-01 F, 0308