

## Secure Information-Sharing Architecture, Part 2: What Communities of Interest Need to Confidently Share Storage

*By Chris Shenefiel, Federal Government Industry Solutions Manager, Cisco*

*In the previous issue of this newsletter, we introduced the [Cisco Secure Information-Sharing Architecture \(SISA\)](#) and discussed one of its four layers: [access control services](#). This article discusses another of the four layers: [data protection services](#).*

The Secure Information-Sharing Architecture (SISA) facilitates collaboration within a community of interest. It does this by enabling members to dynamically share information when the need arises, with the assurance that their information is protected and is only made available on a need-to-know-basis. The basic approach is to consolidate previously separate networks into a common, cost-effective infrastructure that maintains the security of independent networks.

Special precautions are needed for communities of interest to securely share the same storage. Specifically, members need assurance that:

- Each partner's information remains secure as it travels over the storage area network (SAN)
- Each partner's data remains separate from other partners' data, even on shared storage media
- Unauthorized users cannot view or copy files stored on shared workstations

One of the four layers of SISA (the other three are access control, content protection, and watchdog services), [data protection services](#) addresses all three requirements.

### **Protecting Data in Transit To and From Shared Storage**

When communities of interest share a physical SAN infrastructure, they can nevertheless keep their own traffic separate as it travels in and out of storage. Cisco MDS 9000 Series director switches support multiple virtual SANs (VSANs) on the same physical SAN fabric. Each agency or major application, for example, can have its own private VSAN, with its own encryption key, quality of service, security policies, and management functions. Employees can only connect to their own agency's VSAN, even though other agencies share the same physical SAN.

### **Protecting Data at Rest on Shared Storage**

Within the SISA, data is protected in shared storage with Decru DataFort storage security appliances, which compartmentalize stored data in cryptographic vaults on EMC storage arrays. The cryptographic vaults protect data from unauthorized users and administrators and also prevent stored data from accidental or intentional alteration.

## Protecting Data on Workstations

Agencies that share workstations can keep files on the hard disk private in two ways. One is using Cisco Security Agent to disallow actions such as saving files on removable media or copying them across the network. Another is using third-party digital rights management solutions to control file access (number of views, length of views), altering, sharing, copying, printing, and saving. SISA integrates Microsoft's Digital Rights Management Services and, when combined with partner rights management tools from Titus Labs and Liquid Machines, files are "watermarked" with classification and rights access information that follow and control file access no matter where the file goes.

## Security Certifications

SISA components meet federal security requirements:

- Cisco MDS 9000 Series director switches are undergoing NIST evaluation ([http://niap.nist.gov/cc-scheme/in\\_evaluation.html#c](http://niap.nist.gov/cc-scheme/in_evaluation.html#c)) for EAL 3.
- Decru DataFort has received FIPS 140-2 Level 3 certification, NIST certification for AES and Secure Hash Algorithm (SHA) encryption, and DoD 5015.2 certification, and is currently underway with National Information Assurance Partnership (NIAP)/Common Criteria EAL-4+ certification.

For more information on the Cisco SISA, visit: <http://www.cisco.com/go/sisa>.



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)