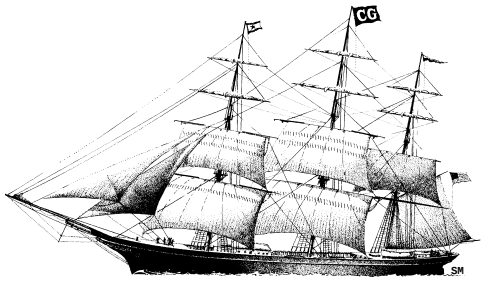
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006082 September 25, 2006

Community of Interest Provides Military-Grade Security for All

Analyst: Dianne McAdam

Management Summary

For many years, we have talked about the importance of information to an organization. We have said things like *Information is one of the enterprise's most critical assets*. Organizations need to use information strategically to maintain their competitive advantage. We protect this information so that our competitors cannot get it. We put locks on computer room doors. We put firewalls around our networks. We encrypt data over the wire. We do lots of things to prevent the *bad guys* from accessing our data.

But what if we need to share some of that information with our business partners? Our business partners can sometimes be our partners and other times they are our competitors. We would like to share some, but not all, information with them and be able to do it quickly, easily and most importantly, selectively. That is a challenge for network administrators today.

That can be a very big headache for those responsible for creating and maintaining the networks that support the United States military. The United States military needs to share information with its business partners – in this case, those partners are allies of the US government. Setting up a new coalition network using old methods could take many months. In his fast-paced world, changes that would require months to implement are changes that take too long. Information needs to be shared quickly when world events threaten the safety of civilians and military personnel.

Cisco and Decru worked together with Microsoft to provide an architecture for the military to consolidate networks and storage and provide limited, secure access, all while simplifying management. This initiative, called the *Community of Interest (COI)* now allows organizations to set up new community of interest networks in a fraction of the time with minimal to no additional cost. That's good news for the United States military and its other allies. It is also good news for civilian organizations since this same initiative is now available for them. Read on to find out more about the infrastructure components of the COI.

Today's Network Challenges

Large enterprises have several distinct networks that allow them to physically separate data. There may be one highly-secured network dedicated to the research department. This contains sensitive data that the company does not want available to other employees. A second network may support normal email traffic, while a third network might support content distribution to remote offices. Separate networks require employees to log on to two or more networks (each with different passwords for each network) to accomplish their job. Information is not easily shared; in fact, it must be duplicated to make it available on another network. Sharing data may require copying the information to a tape, CD, or memory stick and

IN THIS ISSUE

physically *carrying* it to the other network. This is time consuming and a serious security concern if the media gets into the wrong hands. Separate security policies must be maintained across each network. Separate networks add complexity (and cost) to the management and monitoring processes. Duplicating data requires additional storage capacity and presents a third management challenge – how to keep track of all these additional copies of data.

When this large enterprise enters into a business partnership with a second company, a new disparate network must be created and maintained to share some of the information with the business partner. Each new partnership adds a new network and more cost and complexity.

Enter Communities of Interest (COI)

Corporations excel at generating information, but have struggled with sharing it. Cisco, Decru and Microsoft have developed an architecture called the *Communities of Interest* that uses commercially-available products to make sharing information easy. The premise is simple. Each partner, or ally, operates on its own virtual network in a shared infrastructure. Individuals, when needed, can access and share information with other employees or partners, if both individuals have the proper security authorization.

COI – What's Needed

Creating this collaborative network requires several key features. It must:

- Restrict access at the edge of the network;
- Keep data separate as it travels across the shared network;
- Protect data from unauthorized viewing through encryption; and
- Create and maintain security policies in a centralized location.

How it all Fits Together

First, we need to protect the edges of the network. Several commercially-available Cisco products are used to restrict access to the network.

- *Cisco Security Agent (CSA)* protects against host intrusions, intrusions from spyware, malicious code from mobile devices, and provides distributed firewalls.
- *Cisco Secure Access Control Server (ACS)* controls authentication and authorization for end users that attempt to access the network.
- *Lightweight Directory Access Protocol (LDAP)* directories or *Microsoft Active Directory for Windows* can be used to manage all user accounts centrally. These directories support the authentication mechanisms used within the COI network.
- *Cisco Network Admission Control (NAC)* uses CSA agents that are embedded at the network endpoints to determine if devices that ask to connect to the network are compliant with established policies and should be allowed to connect. Devices that are out of compliance are denied access or quarantined.

Path Isolation

Next, we need to keep data separate as it travels through the network. Here, the Cisco *MDS 9000* switches and directors work closely with Decru's *DataFort* security appliance. The combination of these two devices can connect multiple SANS while keeping data flows separate and secure. DataFort encrypts data in flight and at rest, while Cisco switches and directors enforce authentication between themselves and the endpoints of the network. VSANs[1] allow storage traffic to be segregated without requiring separate physical networks.

Data Protection

The third component requires that data be protected and secure in flight and at rest. *DataFort FC-Series* appliances are installed within a SAN and encrypt data at wire speed. Data can be segregated into compartments called *Cryptainer Vaults*, which allow COI data to share the same storage devices as other non-COI data, yet provide needed security and separation. Decru also provides security for Network-attached Storage (NAS) with the *DataFort E-Series* appliances. DataFort E-Series supports numerous file protocols such as *CIFS*, *NFS*, and FTP, as well as hardware-based IPsec and SSL.

Policy Enforcement

Lastly, we need to centralize the monitoring and management of the security policies to simplify management. *Cisco Security Monitoring, Analysis and Response System (CS-MARS)* is an appliance that allows administrators to monitor network attacks and can issue commands to eliminate those attacks. Decru *Life-*

[1] Virtual SANs.

time Key Management provides the infrastructure to centrally manage the keys across the heterogeneous storage devices. Keys are encrypted at all times and sharing of the keys requires a quorum of *Recovery Smart Cards*. Decru's *CryptoShred* ensures that all copies of data that have been distributed are deleted by shredding the keys.

How It Works

How do these products work together? Let's follow the steps as an employee logs on to his network to retrieve some information from a business partner.

1. The user logs on to a workstation attached to the network.
2. The user's profile is accessed on a LDAP or Microsoft Active Directory server. If the authentication is successful, then traffic is allowed to pass through the server port.
3. The workstation's configuration is scanned for software such as personal firewalls or antivirus programs. This information is forwarded to Cisco's ACS, which determines if this configuration matches current security policies. If it does not, the ACS prevents the workstation from connecting to the network.
4. Once the user is logged on, CSA monitors the activity of the workstation and blocks it from attempting to access unauthorized paths.
5. When the user accesses data that he is authorized to view, the Cisco switches and Decru DataFort appliances allow access to the data while ensuring that the data remains encrypted while in transit.

Conclusion

Cisco, Decru and Microsoft have provided a way for enterprises to connect disparate networks and share information without exposing data to unauthorized access. While the military and others could accomplish this in the past, it was very costly, very complex, and very time consuming.

Community of Interest provides a centralized way to manage and secure combined networks without using new special-purpose equipment. In fact, Cisco, Decru, and Microsoft have developed this architecture using products that have been commercially available for years in most cases. This initiative allows datacenters that already own Cisco and Decru products to protect their current investment, while expanding their services to other groups within their organization or partners outside their enterprise. No additional training is required, which keeps costs low.

The Cisco and Decru products are investing in numerous Department of Defense and National Security Agency (NSA) evaluations and certifications. These include NSA/NIAP Common Criteria validation, National Institute of Standards (NIST) FIPS 140-2 certification which includes AES and SHA encryption, and Department of Defense 5015.2 certification.

Community of Interest is not new. What is new is that Cisco, Decru, and Microsoft are now bringing this project to commercial data centers. We expect that it will receive a great deal of attention from large enterprises that need to share information dynamically without breaking the bank. In today's environment, an increasing number of enterprises are realizing that military-grade security is a good business idea.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Dianne McAdam **is Director of Enterprise Information Assurance for the Clipper Group**. She brings over three decades of experience as a data center director, educator, technical programmer, systems engineer, and manager for industry-leading vendors. Dianne has held the position of senior analyst at Data Mobility Group and at Illuminata. Before that, she was a technical presentation specialist at EMC's Executive Briefing Center. At Hitachi Data Systems, she served as performance and capacity planning systems engineer and as a systems engineering manager. She also worked at StorageTek as a virtual tape and disk specialist; at Sun Microsystems, as an enterprise storage specialist; and at several large corporations as technical services directors. Dianne earned a Bachelor's and Master's degree in mathematics from Hofstra University in New York.

- ***Reach Dianne McAdam via e-mail at dianne.mcadam@clipper.com or at 781-235-0085 Ext. 212. (Please dial "212" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group *Captain's Log***, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, "*Navigating Information Technology Horizons*", and "*teraproductivity*" are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.