



Introduction to

Secure Connection Manager 2.0

“The question is not why can’t we stop E-Crime acts from happening, but rather, why are we allowing them to take place?”
(Larry Johnson, Criminal Investigative Division/US Secret Service)

The Increasing Security Threat

The 2004 E-Crime Watch survey* conducted among security and law enforcement executives by CSO magazine shows a significant number of organizations reporting an increase in electronic crimes (e-crimes) and network, system or data intrusions.

Forty-three percent (43%) of respondents report an increase in e-crimes and intrusions versus the previous year and 70% report at least one e-crime or intrusion was committed against their organization. Respondents say that e-crime cost their organizations approximately \$666 million in 2003

Over half of the organizations (56%) experienced operational losses, 25% state financial loss and 12% declare other types of losses. As much as forty-one percent (41%) of respondents indicate they do not have a formal plan for reporting and responding to e-crimes.

Who are the E-Criminals?

Nearly a third (30%) of respondents in organizations experiencing e-crimes or intrusions in 2003 do not know whether insiders or outsiders were the cause. Respondents who do know report that an average of 71% of attacks come from outsiders compared to 29% from insiders.

The survey shows that 36% of respondents organizations experienced unauthorized access to information, systems or networks by an insider compared to 27% committed by outsiders. Both sabotage and extortion are committed equally by insiders and outsiders for organizations responding to the survey.

An electronic crime is defined as: Any criminal violation in which electronic media is used in the commission of that crime. An insider is defined as: a current or former employee or contractor. An outsider is defined as: non-employee or non-contractor.

*The 2004 E-Crime Watch survey was conducted among security and law enforcement executives by CSO magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center.

SCM – Managed Security Solution

Controlled Access with SCM – Secure Connection Manager

The proactive prevention of security breaches before they happen is a matter of controlling who has access to the network. SCM forms the foundation for any organization with the aim of maximizing remote access security while increasing operational efficiency.

SCM is a truly unique access management tool, which restricts access to customer placed equipment.

Application sessions can be established with full support for Authentication, Authorization, Auditing and Accounting (AAAA). SCM provides scripting capabilities that allow total control of connection activities and login sessions down to the level of Service Access Points (SAPs). SCM supports proprietary Internet and Terminal client applications as well as protocols accessible using standard Internet clients, and controls the network infrastructure that is necessary for establishing connections to remote applications. This includes plain IP, PPP, VPN and Terminal Dial-up.

The SCM Web User Interface (WUI) provides intuitive and convenient methods for quickly connecting to the designated remote applications. Not only can users control their application sessions using the WUI, they can also view and control sessions at the network, interface, and user levels.

SCM provides a transparent gateway to the applications that the user needs to access on diverse systems and applications. The user simply clicks on the system link to connect to the remote application and then starts using the application, either via a turnkey application interface or via an external client application that communicates with the remote server application. The remote server application is automatically initiated via proxy services that run within SCM. The user does not have to deal directly with the proxy service, nor with the numerous systems, security protocols and network protocols that may be involved in connecting to the applications.

SCM – Increased Security Level

With SCM as a one unified access tool for all network access, every user is forced through the same centralized gateway in order to perform remote services. The flexibility and power of SCM allows any organization to specifically **define one common remote access method**.

The administration of both **users** (UserID, Passwords, authorization levels) and **remote sites** (IP addresses, phone numbers, remote passwords, authorization levels) is executed in one **unified interface**. SCM enables remote access to designated equipment **without concealing vital access information**.

This entirely eliminates the need for personal (password) lists and dedicated technician PCs, both of which constitute a major security risk if they end up in the wrong hands.

The SCM authentication and authorization features control which users have access to which network resources, and when. This limits users to only viewing and performing tasks they are authorized to do.

The unprecedented SCM Proxy concept provides enhanced security to the remote service using adapted proxies for SSH, SSL and https.

The comprehensive log and reporting facility gives a complete historic overview of activity records at domain, site and user level. The SCM Session Monitoring enables the administrator to control and monitor who does what to the network, and when. The threshold level for users attempting to abuse their access privileges will be significantly higher.

SCM – Increased Operational Efficiency

Given that most networks are made up of diverse devices from different vendors, each with its own operation system and tools, there are typically several entry points into the network.

SCM facilitates a **single point of user profile management**, enabling the administrator to assign specific privileges across predefined user groups. The defined user profile assigns the user with access privileges ensuring that the right person will be at the right place at the right time. A specific user profile can easily be deleted, when the user leaves the organization.

The SCM Sites configuration facilitates a logical grouping of Sites, Domains and Systems. This provides the users with a transparent and self-explanatory overview of the network infrastructure

SCM serves as **one centralized gateway** for all user-based access to remote equipment. This unified access method implies that all users only need to know their personal SCM login credentials. All further information (i.e. remote addresses, passwords etc.) and necessary management tools will be provided by SCM. The SCM Application Proxy feature automatically launches the appropriate application for remote service work. As a consequence, the number of user-initiated applications will be greatly reduced.

The robust SCM Connection Engine will increase the login “hit rate” considerably.

The unrivalled SCM Template Concept enables fast, easy and accurate configuration of the remote network, equipment and application access. When configuring new sites, SCM will automatically generate the necessary connection procedures for fast remote login. New equipment and application types can easily be added to the templates for later use.