Sysgem AG
Via Plauna 431
P.O. Box 159
CH-7031 Laax GR
Switzerland

Tel: +41 (0) 81 921 6853

marketing@sysgem.com
**www.sysgem.com**

SYSGEM®

SEM Proxy Servers

"Need stricter controls over access to your DMZ by System Management procedures?"

In addition to the existing security features offered by Sysgem's unique "*Software Component Authentication*" architecture and the ability to encrypt internal network traffic using *Blowfish-256* encryption, Sysgem now adds "SEM Proxy Servers" to their SEM architectural design.

"SEM Proxy Servers" enable communication routes between SEM workstations and SEM managed agents to be channelled through a set of control filters. A SEM Proxy Server will restrict which SEM users are permitted to connect, and which scripts / menu options are permitted to be used in certain security zones of a customer's network. Furthermore, SEM Proxy Servers introduce "SSH Tunnelling" and "Connection Auditing" to SEM's already impressive list of security and auditing safeguards.

How it works:

Sysgem's "*Software Component Authentication*" architecture already prevents unauthorized access to agent software in a three-layer software structure:
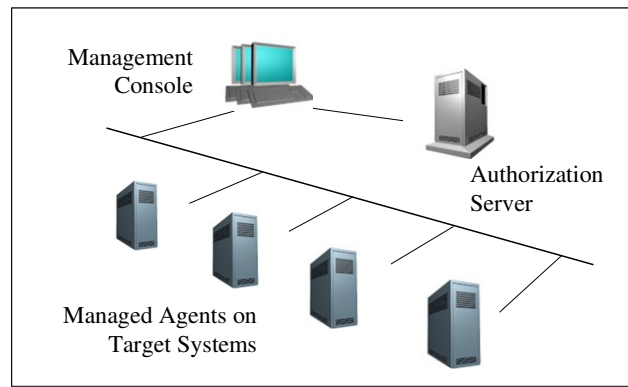

… but introduce SEM Proxy Servers into a customer network and zones can be defined in which only authorized users and nominated scripts / menu options may operate:
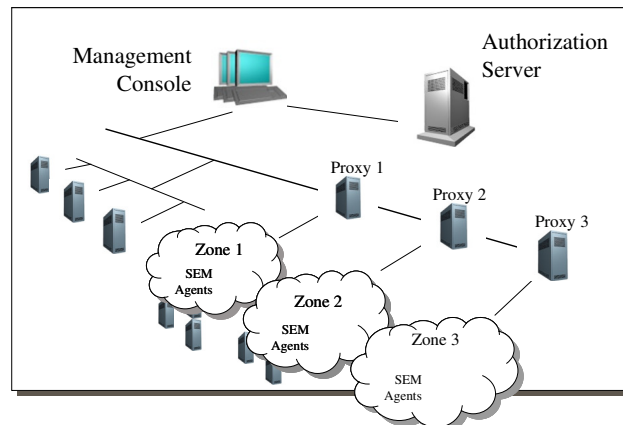
SEM users, who have logged in using a nominated SEM Authorization Server, are "registered" with the Proxy Servers and only they may connect to the SEM Agents in each of the zones supported by those Proxy Servers.
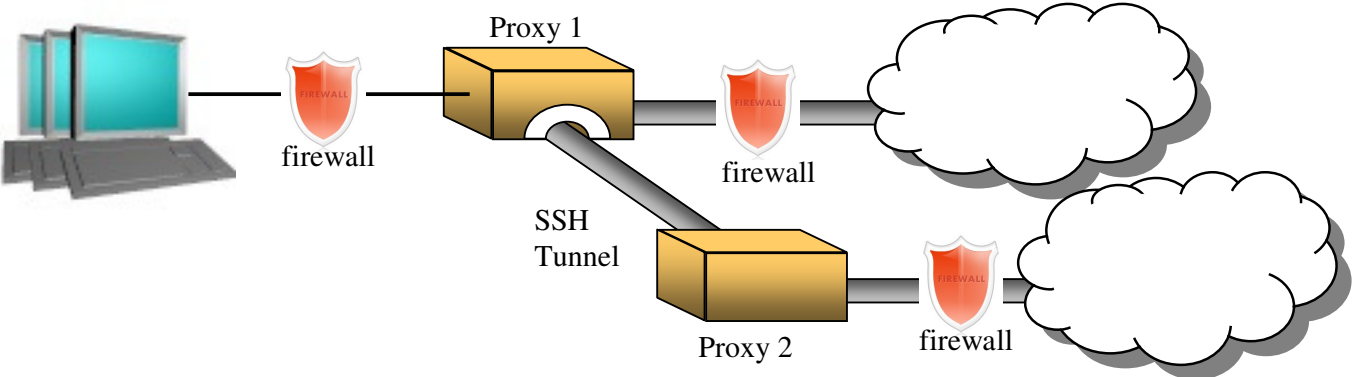
Cascaded Security Access:

Proxy Servers may connect to other Proxy Servers to permit a hierarchical cascading of security restrictions right down to the inner core of a customer's DMZ.
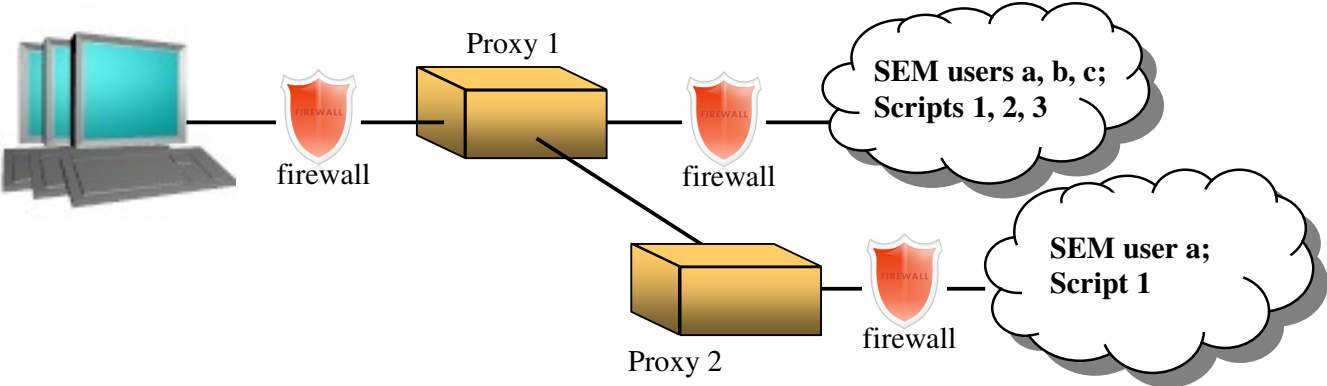

SSH Tunnelling

For still greater security, SSH Tunnels may be set up between Proxy Servers or between Proxy Servers and end target-servers where SEM agents are installed.

Connection Auditing

Proxy Servers may be configured to audit transactions to various depth of detail, e.g. who has connected, which Authorization Server / workstation they used, failed connections, message types, field types, agent lists, etc.
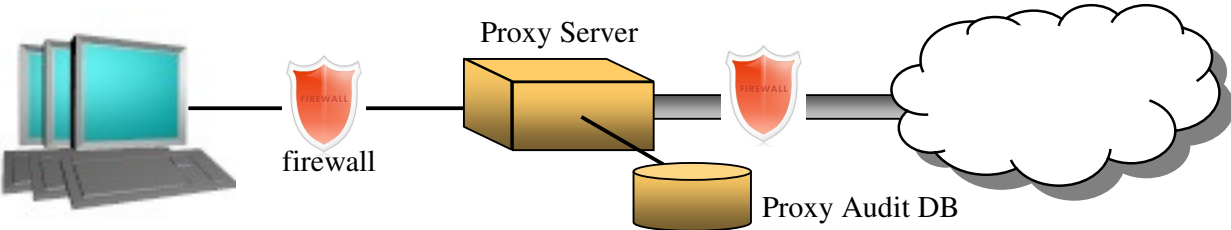
For further information please contact: *marketing@sysgem.com*