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's "Security Control Checkpoints: Proxy Servers"

"Introduce strict controls over DMZ access for Multi-Platform System Management procedures"

1. Overview:

In addition to the existing security features offered in Sysgem's products, e.g. by the "*Software Component Authentication*" architecture; and the ability to encrypt internal network traffic using *Blowfish-256* encryption; Sysgem now adds: "Security Control Checkpoints: Proxy Servers" to their Sysgem Enterprise Manager (SEM) architecture.

"Security Control Checkpoints: Proxy Servers" enable communication routes between SEM workstations and SEM managed agents to be channelled through a set of security controls that protect the varying levels of security zones in a customer's multi-platform network. They control:

- which SEM users are permitted to connect to each security zone,
- which scripts / menu options are permitted to be used in each security zone.

Furthermore, Sysgem's Proxy Servers introduce "*SSH Tunnelling*" and "*Connection Auditing*" to SEM's already impressive list of security and auditing safeguards.

2. The Need:

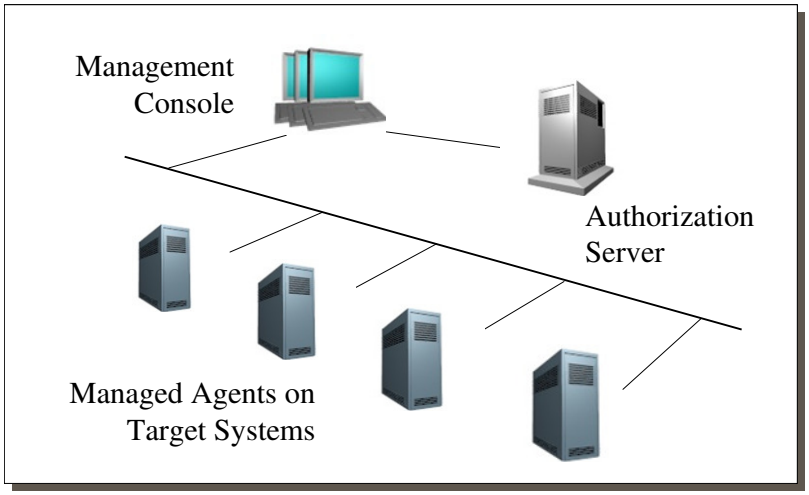
Misappropriation of elements in a corporate IT infrastructure can lead to the misappropriation of corporate funds and result in corporate catastrophes, as has been seen in recent events in the banking world. All corporations have a need to examine their IT management practices and eliminate any risks that may exist. To this end, and to safeguard Sarbanes and Oxley recommendations in a customer network, a number of requirements have been foreseen for SEM:

1. 'Security control' not only at the source of the management system, but also at the destination servers.
2. Verification ('Sealing') of scripts to ensure their Integrity.
3. Authentication of 'Sealed' scripts at the destination servers.
4. Registration of user access at the destination servers.
5. SSH Tunnelling.
6. A break in the direct link between non-privileged workstations and privileged agents.
7. An additional layer of Auditing.

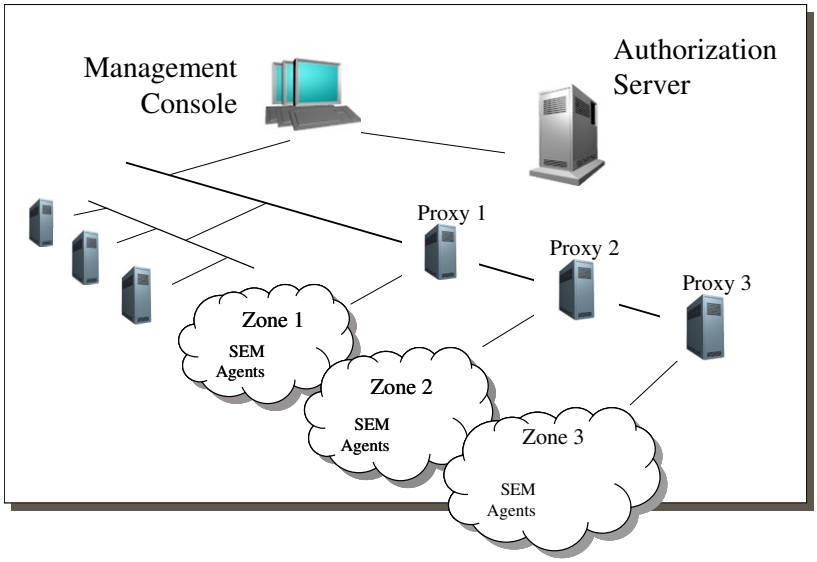
Additional explanation of these requirements can be found in Appendix 2.

3. How it works:

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



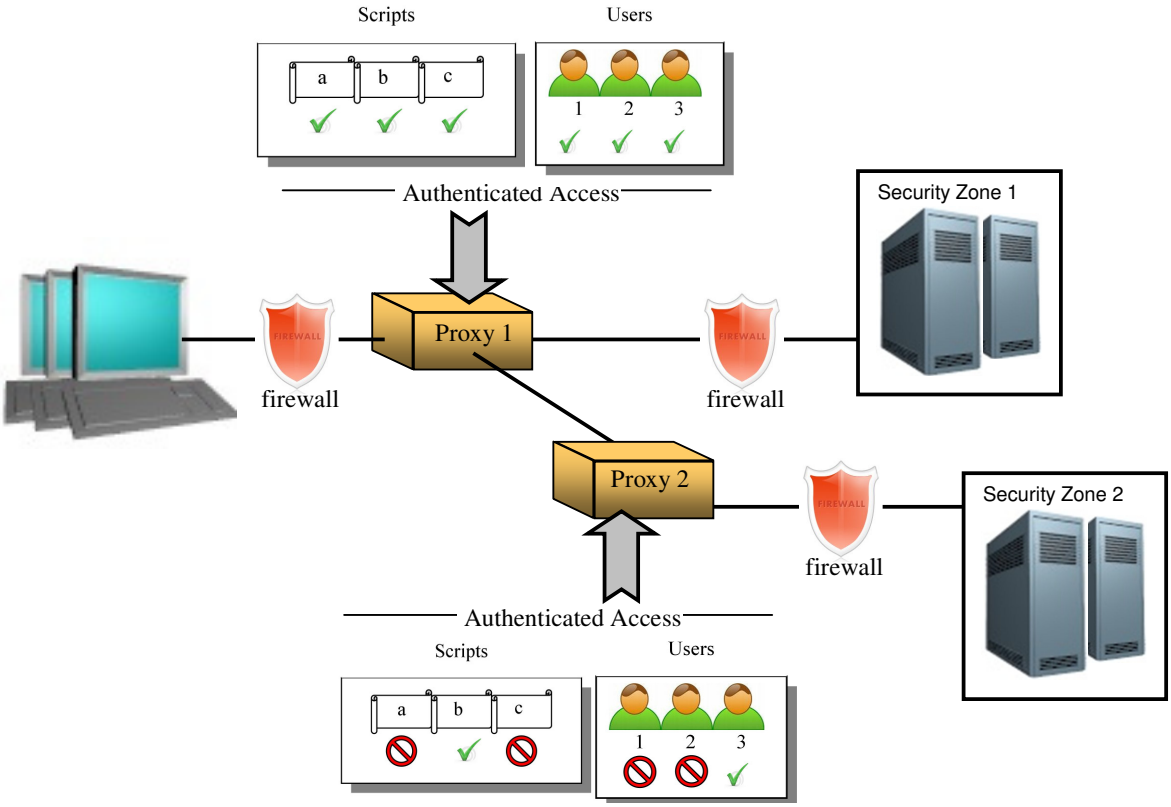
… but introduce SEM Proxy Servers into a customer network and zones can be defined in which only authorized users and nominated scripts / menu options may operate:



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.

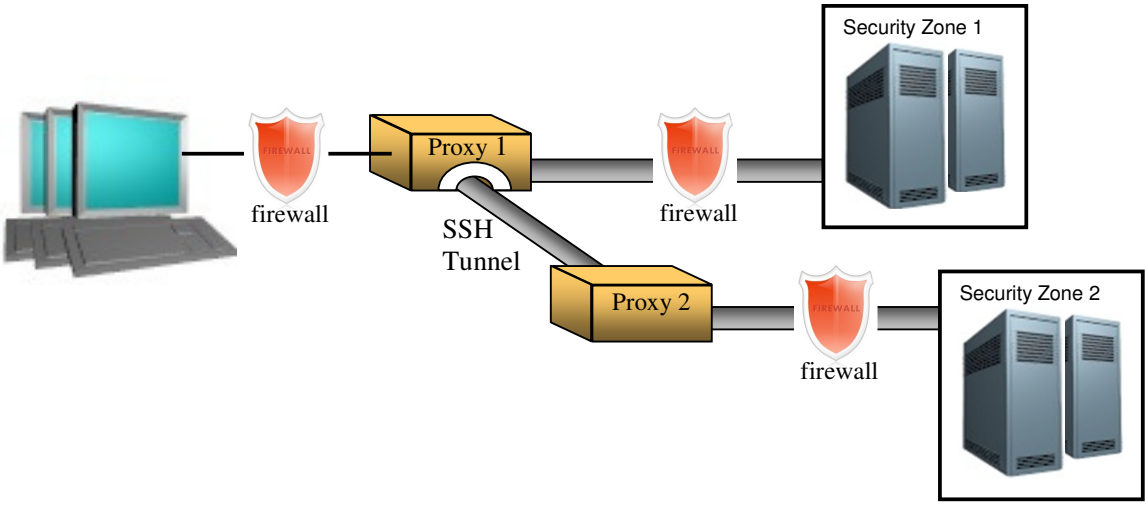
3.1 Cascaded Security Access

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. SEM users and scripts / menu options are authenticated for access at the different Proxy Servers.



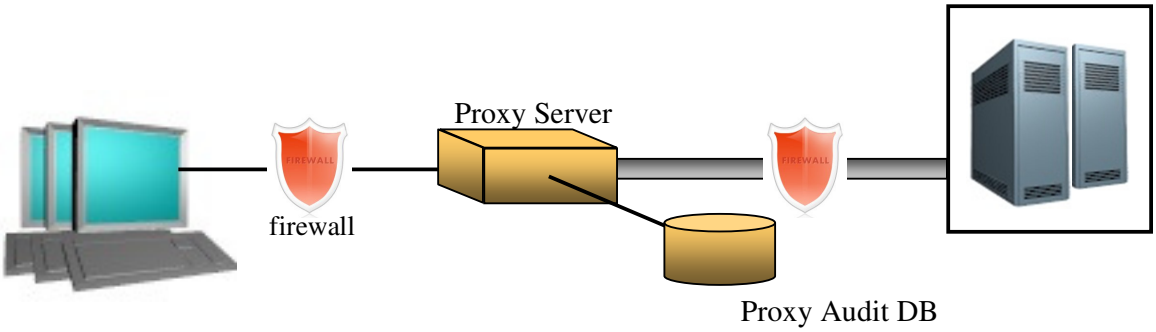
3.2 SSH Tunnelling

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



3.3 Connection Auditing

Proxy Servers may be configured to audit transactions to various depth of detail, e.g. to record who has connected; which Authorization Server / workstation they used; failed connections; message types; transaction information such as field types, agent lists; etc.



An example of how a customer may use SEM Proxy Servers is sown in Appendix1.

4. Advantages:

1. Power with Safety: SEM is a powerful product and provides a valuable tool for the System Manager and User Account Administrator. The introduction of Sysgem's Proxy Servers in a corporate network allows the power of the product to be used with confidence and safety.

2. Sealed scripts and the verification of those "seals" gives resilience in the system and resistance to interference by accidental or fraudulent changes.

3. Only authorized access is permitted, with the control being dispersed to the 'business-end' of the network.

4. Flexibility and security with mixed permissions appropriate to the mixed requirements of different network security zones.

5. No direct link to SEM Agents without the 'break-&-check' in the network connection.

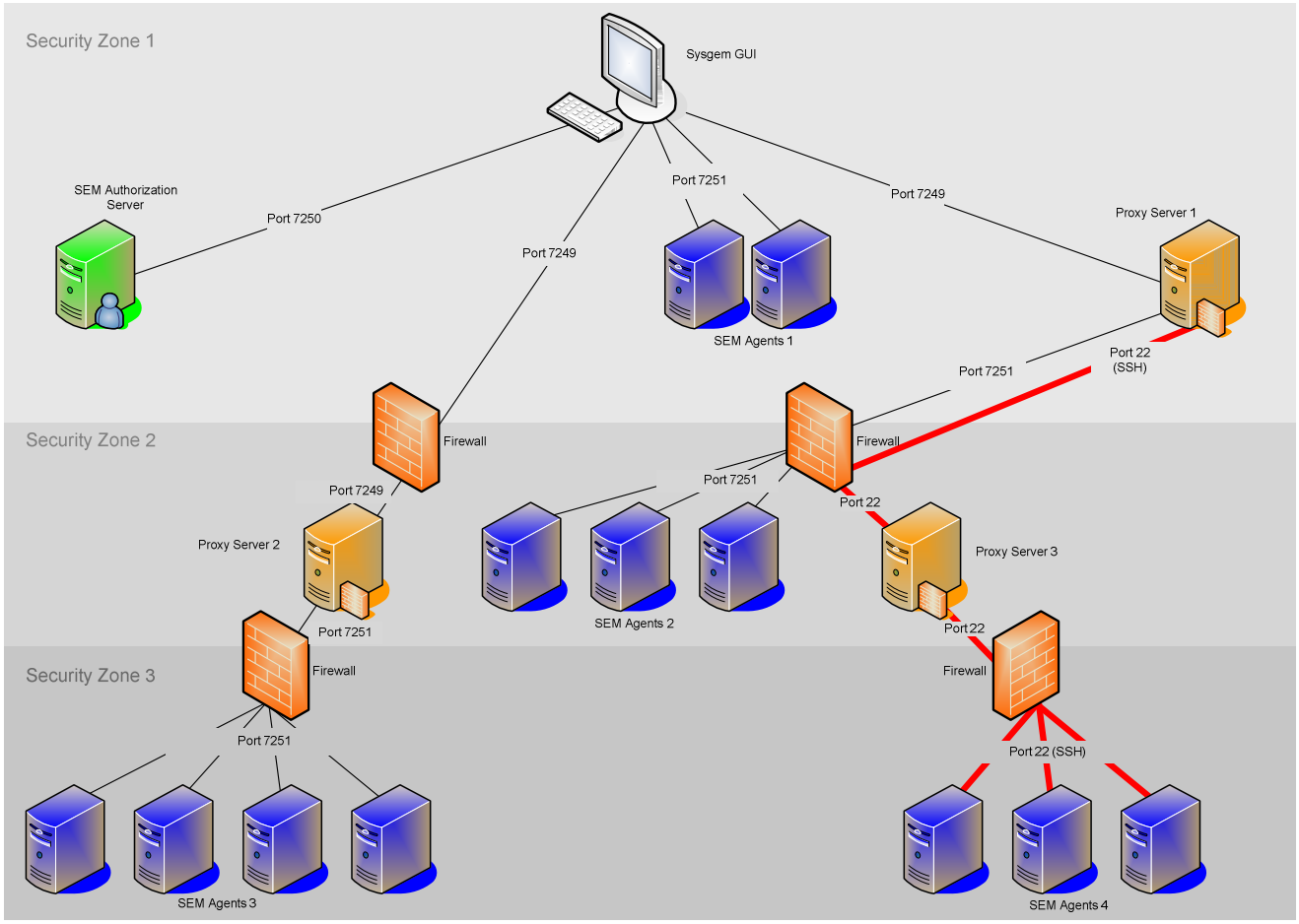
6. Accountability through enhanced auditing.

7. A closer realization to the perfect scenario of 'Total Security'.

For further information please contact: marketing@sysgem.com

Appendix 1: Example of Customer Network

An example of how a customer network may incorporate Sysgem's Proxy Servers:



In this example:

- "SEM Agents 1" in Security Zone 1 are connected directly to the SEM GUI via port 7251
- "SEM Agents 2" in Security Zone 2 do not have any direct connection with the SEM GUI. They are connected only to Proxy Server 1 via port 7251 which in turn is connected to the SEM GUI via port 7249. The firewall settings ensure that only Proxy Server 1 has access to these agents.
- "SEM Agents 3" in Security Zone 3 are connected to the Proxy Server 2. Firewall settings ensure that there is no direct connection between the SEM GUI and the Agents.
- "SEM Agents 4" are connected via Proxy Server 3 which in turn is connected to Proxy Server 1. Communication between Proxy Server 1 and the agents is via an SSH Tunnel (using Port 22) and an SSH Server on each of the Agent machines.
- Each of the Proxy Servers may have different configuration settings permitting access by a different set of users and scripts / menu options.

Appendix 2: Detailed Requirements

1. **'Security control' not only at the source of the management system, but also at the destination servers:** Restrictions on user permissions may already be established at the central SEM Authorization Server but individual target servers, or a group of target servers, need to be able *independently* to impose restrictions on 'who' can do 'what' on the target machines.

2. **Verification ('Sealing') of scripts to ensure their Integrity:** Scripts that have been developed; customised; tested; certified and approved need to be "Sealed" so that they not only remain unaltered and intact, but it can be 'proven' at run-time that they are in the same state as they were when they were approved.

3. **Authentication of 'Sealed' scripts at the destination servers:** Some actions may be appropriate on some servers, but not on others. At the same time, one SEM user may have authority to access multiple sets of servers, and to have permission to perform multiple types of actions. To safeguard against the accidental or fraudulent use of a restricted action on a restricted server and at the same time permit unrestricted actions on all servers, there needs to be some local restriction on the target set of servers to ensure that only the appropriate scripts are permitted to run on those target servers.

4. **Registration of user access at the destination servers:** To safeguard against the accidental or fraudulent access of a server or set of servers by unauthorised SEM users, it is required that a further set of checks are made on who is accessing servers at a point other than the central SEM Authorization Server. Both the SEM username and the identity of the SEM Authorization Server need to be included in this check.

5. **SSH Tunnelling:** Some customers demand that SSH Tunnelling be used across certain security zones within their network.

6. **A break in the direct link between non-privileged workstations and privileged agents:** It is not a good practice to have 'non-privileged users' on workstations able to make a direct link to 'privileged processes' on security sensitive machines without there being a break-&-check in that link. User should be forced to access agents via an intermediary service (i.e. via a 'Proxy Server') and not to have direct access to the target agent. If SSH Tunnelling is in use, then the Proxy Server should interpret the messages, validate the content and authenticity of the sender before reformatting the message into another SSH Tunnel for onward transmission to the agent.

7. **An additional layer of Auditing:** The Security Control Checkpoint - Proxy Server software should be capable of recording varying levels of detail of the messages flowing through it. It is not required for all details of the transaction to be recorded, indeed it is required that all details are NOT recorded (e.g. user account passwords should never be logged anywhere). However, details such as the following should be recorded:

    a. timestamp,
    b. id of proxy server,
    c. SEM username of the requestor,
    d. workstation id;
    e. SEM Authorization Server they logged into,
    f. Target Server;
    g. next machine in the chain.

Auditable events should include:

- establishing a connection,
- a failure in establishing a connection (permission denied / host down / mis-configured),
- message-by-message summary (showing message type),
- message-details option includes a “list” of all the field types in the message.