

Secure / FTP

- ▶ **Every single FTP command and SITE subcommand gets secured at the level of user-id, password and IP-address**
- ▶ **Set up of all security specifications by the standard SAF security system that is being used**
- ▶ **Real-time GUI monitoring of complete FTP-session including security monitoring**
- ▶ **Automated FTP post-processing, controlled from FTP-Client**
- ▶ **Fully integrated with SAF (RACF, ACF2, TSS)**
- ▶ **Security beyond the firewalls**
- ▶ **Minimal overhead**
- ▶ **Full Audit Trail**

The Need

An obvious benefit of FTP is that it is available in the TCP/IP-stack that comes with every single operating system. FTP operates according to the RFCs on each of these platforms, and has added specific SITE commands for each platform. This makes FTP a very powerful tool.

The weakness of FTP lies in its lack of automation, control and security facilities. Specifically in the OS/390 domain, which has a history of tight control and security, organizations are conscious that they have to address this weakness.

Automation

Usually data files get transferred to OS/390 with the intention to perform some processing on this data. It is however difficult to exactly determine when the transfer has been completed and when the post-processing should be started.

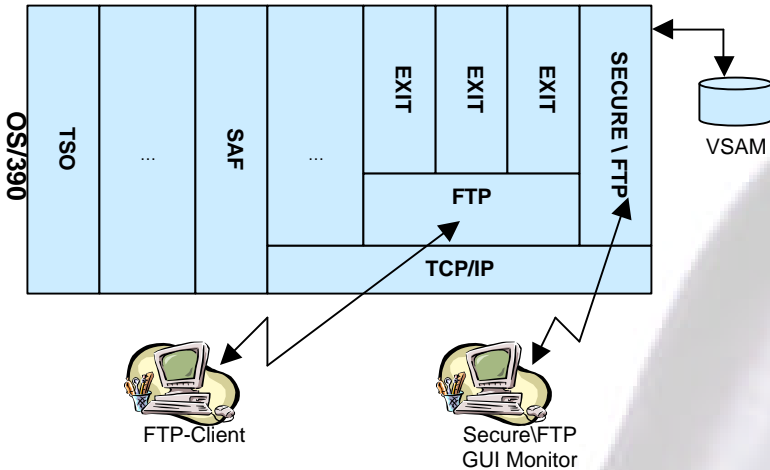
Secure \ FTP allows to control from the FTP-client which OS/390 process should be started and to effectively start this process from within the FTP session.

Online Monitoring

Standard SMF-data can give after-the-facts information about data files that were successfully transferred to or from OS/390.

Secure \ FTP however provides as well online monitoring as history reporting on complete FTP sessions: which commands have been executed? for which files?

As a result of the integration with its security facilities, Secure \ FTP includes all security-related data in its online monitoring and history reporting: which rules have been checked for this command? Which users have tried to execute specific FTP-commands but were not allowed to?



The Architecture

Secure \ FTP makes use of all available exits in the FTP server of the OS/390 TCP/IP stack.

It runs as a started task in its own address-space where all data that are communicated from the exits, are written into a set of VSAM files, which can be queried for online monitoring purposes from a GUI Monitor. For historical purposes the information in the VSAM files gets dumped into a workstation environment where statistical data is provided.

Secure \ FTP integrates via the SAF-interface with all popular security tools on OS/390, which enables OS/390 security officers to protect FTP traffic with the same type of rules as their other applications.

Security

Typically organizations have set up firewalls and/or VPNs to protect them from unauthorized external TCP/IP traffic.

They also secure access to data files on OS/390 with SAF-tools (RACF, ACF2, TSS).

This type of protection proves to be insufficient.

Firewalls will provide or deny access to FTP as a whole, they cannot give authorizations to individual FTP-(sub)-commands.

SAF-tools look at data access, no matter from where this access originates (TSO, FTP-client, etc).

Secure \ FTP provides the ability to secure every single FTP-(sub)-command, including all SITE commands, at the level of user-id/password, combined with originating IP-address and destination OS/390 port.

Some data files simply belong on the OS/390 mainframe and the sole fact that a user has read-access to these files from TSO or another mainframe application, shouldn't mean that this user is automatically allowed to transfer these data files to other environments (OS/390, NT, Unix, etc).

FTP-commands like List, CWD (Change Working Directory), etc do not imply direct access to datasets and cannot be protected by standard SAF-tools. Still companies want to disallow FTP users of even browsing directories and seeing that datasets, originating from or reserved for other users, are available. Like all other FTP-commands, also these can be secured with Secure \ FTP.

In this way, Secure \ FTP allows to provide access to a 'limited FTP facility' to each individual user.

Requirements

Secure \ FTP runs with IBM OS/390 eNetwork Communications Server V2R5 (or higher) or NetworkIT TCPAccess 5.2 (or higher).

The Secure \ FTP monitor requires a Microsoft 32bit environment.

The Partnership

Advanced Software Products Group, Inc. (ASPG, Inc.) has been selected as the exclusive agent for the Secure / FTP products for the United States and Canada.



Link \ Manage is a Belgian company, specialising in the opening of the MVS (OS/390) mainframe to the open environment and securing it. The technical team that is working at Link \ Manage, has been assisting multiple organizations in their move from SNA to IP since 1991.



Since 1986, Advanced Software Products Group, Inc. has provided the mainframe community with cutting edge software solutions, support and services. With a worldwide network of support, including an active role as an IBM™ PartnerWorld Partner In Development, ASPG remains a leader in the optimization of data center performance