FTP/Guardian™
Raise the bar on z/OS FTP Security

FTP/Guardian Security Interface

Through a hierarchy of SAF rules you can control who has access to FTP, what they can accomplish with it, what data they can access and where it can travel. FTP/Guardian easily enables you to:

- Control access to individual FTP commands
- Restrict access to sensitive data
- Restrict the movement of data to and from the Enterprise
- Protect data from accidental (or intentional) deletion or replacement via FTP
- Restrict access to job submission, job output review and deletion
- Make only limited FTP services available to casual users
- Make all FTP services available to trusted users

The granularity this provides enables you to tailor a security policy to the needs of your organization.

How It Works

FTP/Guardian's Security Interface takes advantage of defined z/OS FTP interfaces to enable SAF authority checking on all FTP activity. All you need to do is define SAF rules to allow or deny FTP usage at whatever level of detail you need.

FTP usage rules are defined in the FACILITY class. At the highest level, rules are defined to control access to individual FTP commands. More granular control of FTP usage is implemented with more granular SAF rules.

Many FTP actions actually result in a series of SAF checks, starting at the highest level (request to download an MVS dataset) and working down to the details (dataset name, IP address where it is going).

Access can be allowed or denied at any level of the hierarchy.

An Example

The example below shows how a simple hierarchy of rules can be used to allow downloading of a dataset containing sensitive data to systems behind the firewall and block downloading outside the firewall.

At the highest level, you can enable (by default) access to MVS datasets via the GET (download) command for a particular user:

```
PERMIT FTPR#GETMVS ID(uid) ACCESS(READ)
```

Now, a rule enabling general access to the dataset whose high-level qualifier is SENSITIV:

```
PERMIT FTPR#GETMVS.SENSITIV.**
ID(uid) ACCESS(READ)
```

Now, one rule that denies access for downloading the dataset to all remote IP addresses, followed by one that enables access for IP addresses starting with 10.1:

```
PERMIT FTPR#GETMVS.IP.*.*.*.*.SENSITIV.**
ID(uid) ACCESS(NONE)

PERMIT FTPR#GETMVS.IP.10.1.*.*.SENSITIV.**
ID(uid) ACCESS(READ)
```

The result is that an FTP user on a system with an IP address that starts with 10.1 will be allowed to download the dataset and an FTP user on a system with any other IP address will be denied.

More Information

Software Assist Corporation specializes in providing Security and Controls for responsible FTP usage to large and medium-sized enterprises. Our range of innovative software products helps customers worldwide become more secure, more compliant and more efficient.

For more information please contact us or visit our website.

Phone: (678) 965 0885 · Email: sales@ftpsentry.com · Web: http://www.ftpsentry.com