

Consolidation of ftp servers



Jessie

Background

- 7/02: DOI mandate for Bureaus to discontinue use of anonymous ftp.
- 8/02: GIO responded -- USGS uses anonymous ftp for critical activities and, at this time, we could not comply with this mandate.

Background cont.

- 11/02: Waiver process for READ ONLY anonymous ftp servers available
- A few days later word came down from the Regions that the waiver process was on hold until further notice.
- We continue anonymous ftp as usual

Problems

- We are not in compliance with (draft) DOI Perimeter Security minimum firewall config
- Every office will need a DMZ and a waiver to continue using READ-ONLY anonymous FTP
- Additional hardware to split server functions
- Lotus groups do not want us to exchange huge files using email
- WRD has varied legitimate needs... (discussed ahead)

Where do we start?

- Understand DOI requirements
- Understand and document our needs
- Determine where Bureau efforts lie
- Decide if Bureau timeframe is good for WRD or if WRD should move spearhead this project.

DOI Security Perimeter Document (Appendix 1) states: Firewalls must be configured to only allow ftp access into the DMZ and that anonymous ftp will not be allowed.

	Standard				
Service	Inside to Outside		Outside to Inside		Standard
	Status ₁	Auth ²	Status ₁	Auth ²	
FTP	Yes	No	No	No	FTP access will be allowed from the internal network to the external. For transmission of sensitive information, encryption must be implemented. No FTP access will be allowed externally through the Firewall to FTP servers within DOI's trusted network. FTP servers in the DMZ will be allowed. Anonymous FTP servers are not allowed.

Lets Break it down

- 1) FTP access will be allowed from the internal network to the external.
- 2) For transmission of sensitive information, encryption must be implemented.
- 3) No external FTP access will be allowed ~~externally~~ through the Firewall to FTP servers within DOI's trusted network.
- 4) FTP servers in the DMZ will be allowed. Anonymous FTP servers are not allowed.

WRD's perspective on Anonymous ftp

- It can safely be used from non-USGS hosts to “get” data but not to “put” data on our systems.
- Requiring userids (i.e. sftp) will be more dangerous
- httpd will probably meet all needs to serve data to the public.

FTP needs

(as defined by Schmid, Bergstedt, Senko, Winkless and Boldt)

1. Archive files for public distribution
2. Back end database call through a web application creates a file and puts it in ftp depot for customer retrieval.
3. Exchange of large files with external users.
4. Exchange of files by internal users
5. Method of reducing large email attachments

Examples of existing automated uses of FTP

- NWQL uses ftp to transfer data to distributed NWIS servers.
 - Script developed to set up sftp-- not used
- RPM uses ftp.
 - RPM is used by SAs to automate Unix software/security updates.
- Home-grown scripts/programs?

Next Steps

- Request that DOI allow us to use anonymous ftp “read-only” from a DMZ
- Share list of ftp needs with Districts to ensure all needs are listed
- Decide if WRD will take on this project or the Bureau and pin down funding

Next Steps

- Develop solutions for:
 - an ftp archive
 - anonymous drop/pick-up by internal and external users
 - sensitive/secure sharing of “large” files