

Metody zabezpečeného přenosu souborů

Radek Dostál
Petr Koloros

Cryptofest
15.11.2003

Úvod

- Co všechno šifrovat
- SSL FTP x SFTP, SCP
- SSL FTP – Implicit x Explicit – jak poznat
- Windows – klienti, servery
- Linux – klienti, servery
- Přenos souborů přes SSH
- Seznam odkazů

Co všechno šifrovat

- Šifrovat pouze kontrolní kanál
 - Jméno heslo, příkazy
- Šifrovat výpisy adresářů
- Šifrovat i přenos dat = vše
 - Rychlost x Bezpečnost

FTP SSL x SFTP, SCP

- FTP SSL
 - Zašifrovaný protokol FTP
 - 2 spojení - pro příkazy a data
 - ♦ Problémy s firewally
- SFTP, SCP
 - Nemá nic společného s FTP – nadstavba SSH
 - Jedno spojení pro příkazy i data

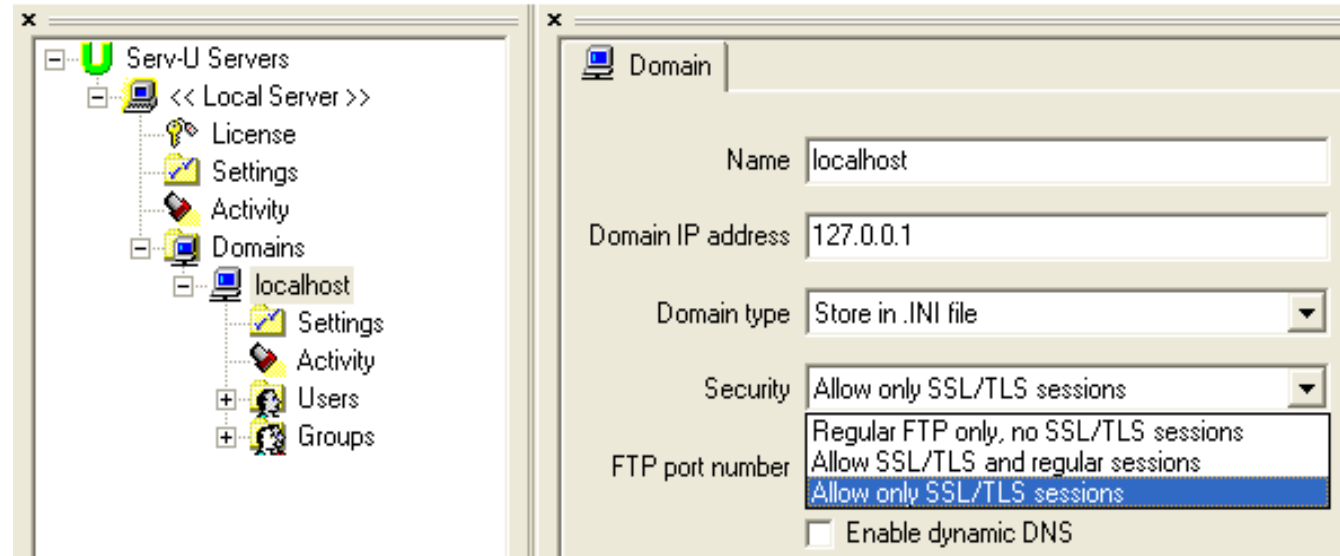
FTP SSL - Implicit x Explicit

- Rozdíl v začátku spojení
- Port 990 x 21
- telnet server port (např telnet localhost 21)
 - 220 ready, dude (vsFTPD 1.0.1: beat me, break me)
- Openssl s_client -connect localhost:990
- www.glub.com - Secure FTP Command Line
 - V Javě

Windows - server(y)?

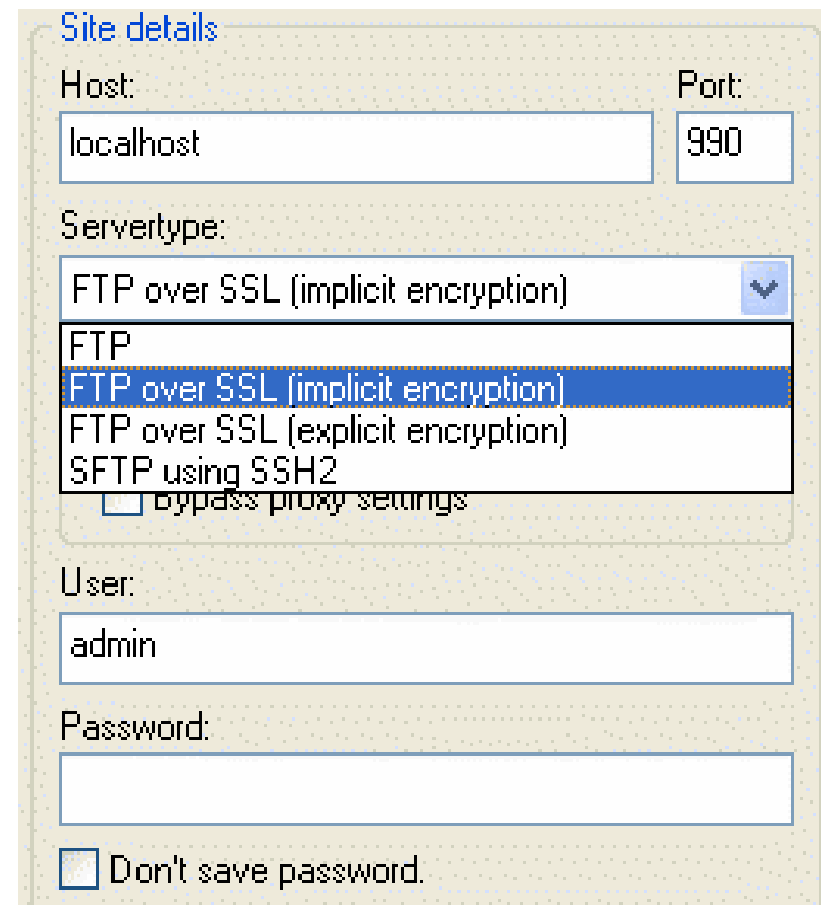
Serv-U

- Serv-U
- Podpora – Implicit
- Snadné ovládání
- Ukázka



Windows - klienti

- **Filezilla** - ukázka
- Cute FTP
- Flash XP
- Core FTP
- FTP Voyager

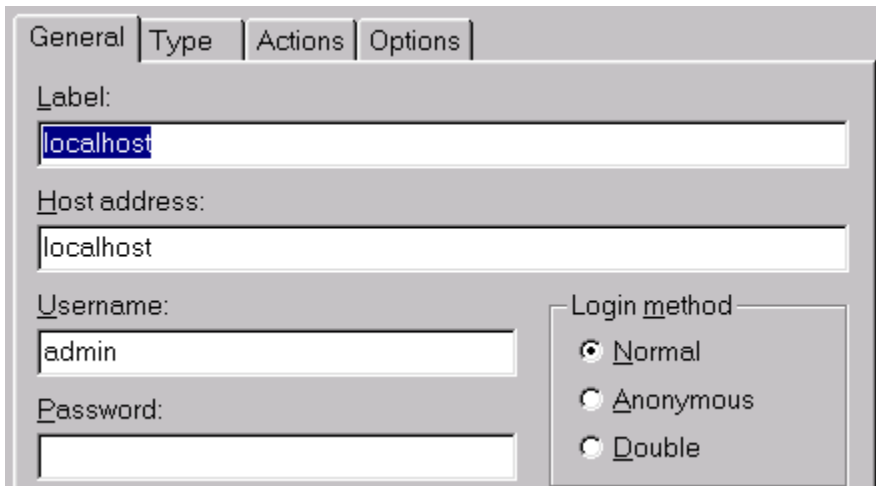
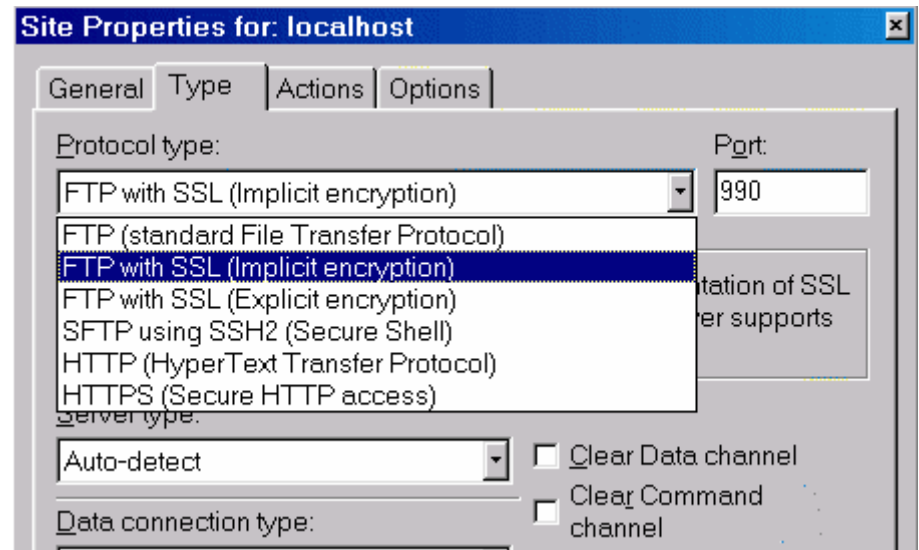


The image shows a screenshot of the FileZilla Site Manager dialog box. The title is "Site details". It contains the following fields and options:

- Host:** localhost
- Port:** 990
- Servertype:** A dropdown menu is open, showing the following options:
 - FTP
 - FTP over SSL (implicit encryption) (highlighted)
 - FTP over SSL (explicit encryption)
 - SFTP using SSH2
- bypass proxy settings
- User:** admin
- Password:** (empty field)
- Don't save password.

Cute FTP

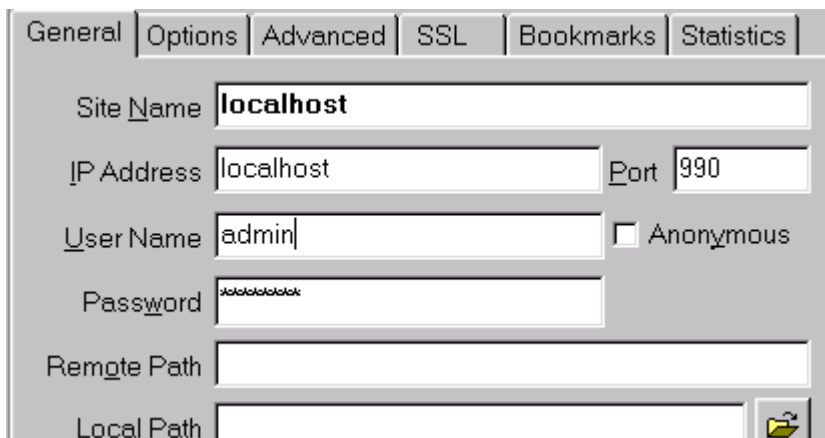
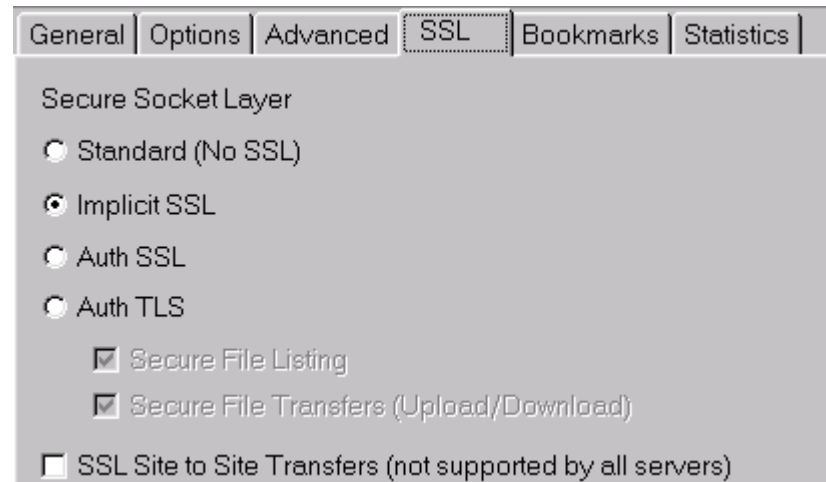
- Komerční
- Dobře fungují verze 3.0 a 3.3



- Slušné možnosti konfigurace
- Implicit, Explicit, SFTP

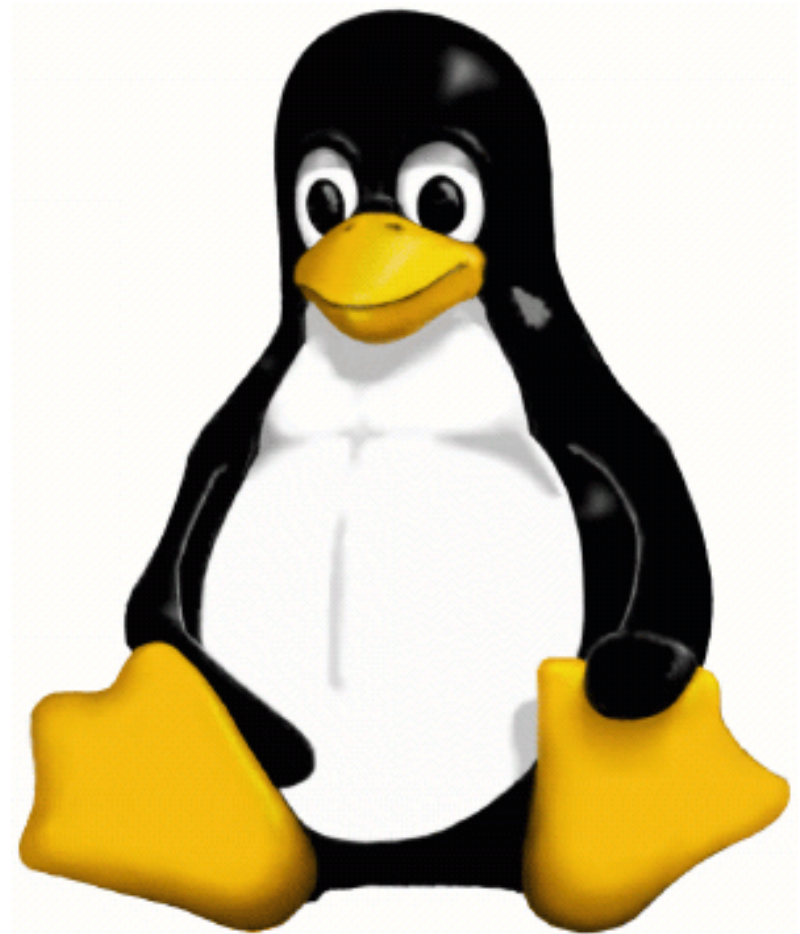
Flash XP

- Komerční
- Množství voleb konfigurace



Linux Server

- proFTPd
- glFTPd
- pureFTPd



ProFTPD

- Šifruje i soubory
- Možnost autentifikace proti sql
- Nepodporuje implicit SSL
- `./configure --with-modules=mod_tls`
- Ukázka konfiguráků

GLftpd

- Oddělené uživatelské účty od systémových
- Explicit i Implicit (**-z sftp** v inetd.conf)
- Odmítá spojení od neznámých IP
- Credity, ratio, statistiky, oddělení admini,...

- Nejsou k dispozici zdrojové kódy

s SSL i bez zreadme:TLS 100% security

- Vývoj se štěpí

```
userrejectsecure !*
userrejectinsecure !*
denydiruncrypted !*
denydatauncrypted !*
```

```
userrejectsecure !*
userrejectinsecure *
denydiruncrypted *
denydatauncrypted *
```

- Config dle IP

PureFTPd

- Open Source
- Nepodporuje šifrovaný přenos dat
- Nepodporuje Implicit
- Možnost autentifikace proti mysql
- Z readme.tls
 - ./configure --with-tls ...
 - v inet.d --tls=0(default), 1, 2

Linux Klient

- Lftp
 - Explicit – protokol `ftp://nekdo@nekde.cz`
 - ◆ `set ftp:ssl-allow yes`
 - ◆ `set ftp:ssl-protect-data yes`
 - ♦ Vhodné umístit do `~/.lftp/rc` nebo `lftp.conf`
 - Implicit – `ftps://nekdo@nekde.cz`
 - SSH – protokol `fish://nekdo@nekde.cz`
 - `~/.lftp/bookmarks` – lze s heslem
`ftps://ja:heslo@tady.cz:999`
- Secure FTP `www.glub.com` - pouze Implicit (grafický)

SSH - přenos souborů

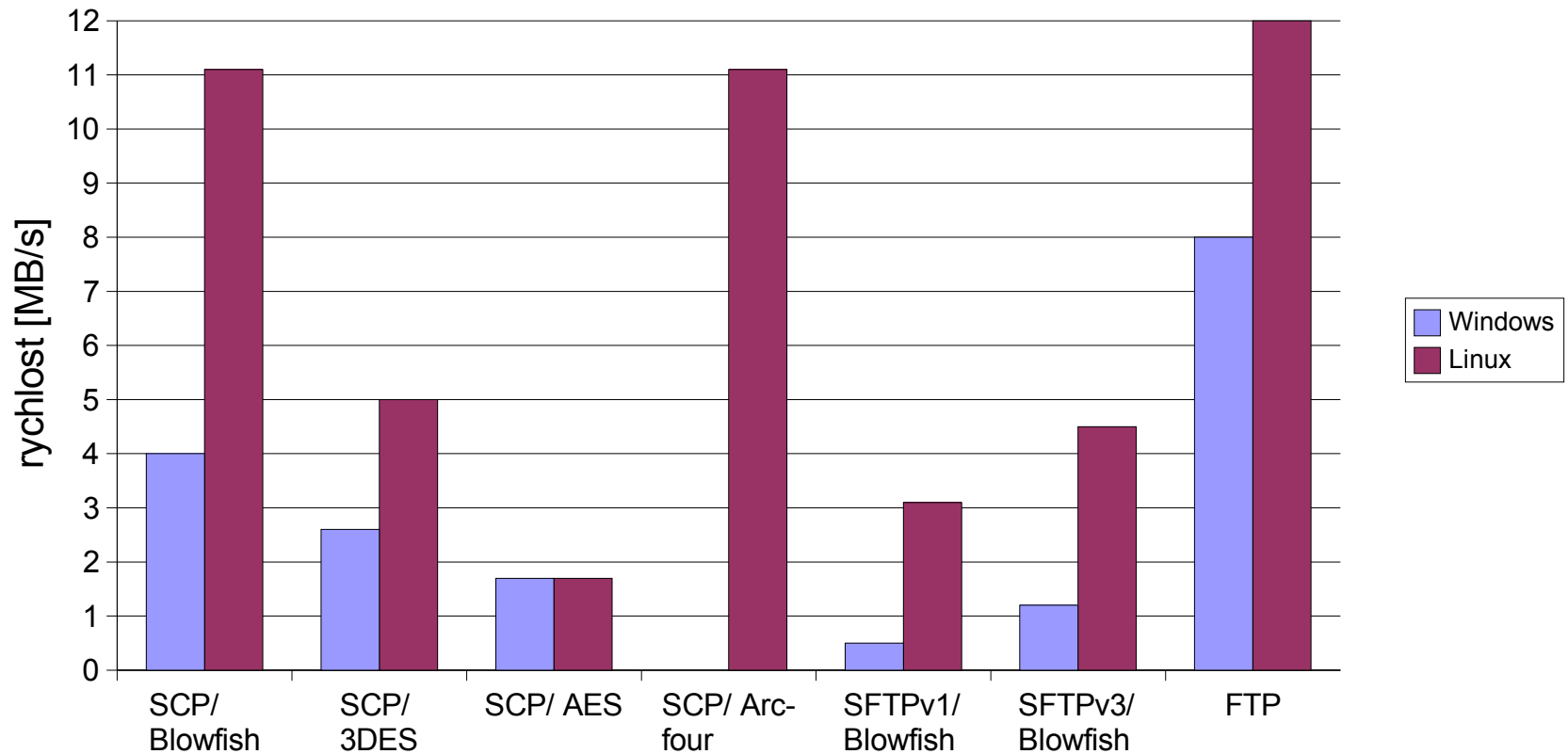
- SSH umožňuje dvě metody:
 - 1) **SFTP** – pomocí SSH démona
 - 2) **SCP** – secure copy
- Klienti i pro Windows: např. WinSCP
- Možnost volby šifrování:
 - Blowfish, 3DES, AES, ..

SSH – rychlosti přenosu

| Prostředek | Šifra | Windows [MB/s] | Linux [MB/s] |
|------------|----------|----------------|--------------|
| SCP | Blowfish | 4,0 | 11,1 |
| | 3DES | 2,6 | 5,0 |
| | AES | 1,7 | 1,7 |
| | Arcfour | -- | 11,1 |
| SFTP v1 | Blowfish | 0,5 | 3,1 |
| SFTP v3 | Blowfish | 1,2 | 4,5 |
| FTP | | 8,0 | 12 |

SSH – rychlosti přenosu

SSH přenos - srovnání rychlostí



Závěrem

- Co všechno šifrovat
- Rozdíl SSL FTP x SSH FTP
- SSL FTP – Implicit x Explicit – jak poznat
- Windows – klienti, servery
- Linux – klienti, servery
- Přenos souborů přes SSH

Děkujeme za pozornost

- Tato prezentace
 - www.cryptofest.cz/SSLSoubory/
- Přehled klientů, serverů, principu fungování
 - www.ford-hutchinson.com/~fh-1-pfh/ftps-ext.html
- lftp.yar.ru
- filezilla.sourceforge.net
- www.proftpd.org
- www.glub.com
- www.pureftpd.org
- www.flashFXP.com
- www.glftpd.com
- www.serv-u.com
- www.openssh.org
- winscp.sourceforge.net