



# PROTOKOL SFTP A FTPS

Antonín Vojtěch 3. IT



# Co je to FTP protokol a k čemu slouží?

- Je to protokol pro přenos souborů mezi počítači pomocí počítačové sítě.
- Definován byl v roce 1985 v RFC 959 a rozšířen byl v roce 1997 v RFC 2228.
- RFC je v informatice označení řady dokumentů popisujících internetové protokoly, systémy apod.

# Protokol SFTP

- SFTP slouží ke stejnému účelu jako FTP, s tím rozdílem, že SFTP je zabezpečen pomocí protokolu SSH-2.
- Často lidé mylně tvrdí, že SFTP je FTP zabezpečeno pomocí protokolů SSL nebo SSH, SFTP je samostatný protokol.
- Běží na portu 22, FTP využívá porty 20 a 21 a běží výhradně přes TCP protokol.
- Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť.
- Nezabezpečený i zabezpečený přenos dat se dá odchytit např. pomocí programu WireShark

# Klady a zápory SFTP

- Má standardy, které přísně definují většinu (pokud ne všechny) aspekty provozu.
- Má pouze jedno připojení (není potřeba samostatné připojení pro data). Spojení je vždy zabezpečené.
- Protokol obsahuje operace pro oprávnění a manipulaci s atributy, zamykání souborů a další funkce.
- Klíče SSH je těžší spravovat a ověřovat .
- Žádné operace kopírování ze serveru na server a rekurzivní odstranění adresáře.

# Protokol FTPS

- Je zabezpečen pomocí protokolů SSL a TLS.
- Existují dvě metody, jak použít lze FTPS.
- První metodou je Implicitní FTPS, běží na portu 990. Pokud se klient připojí přes port 990, server předpokládá, že SSL bude vyvolán a automaticky hledá autentizační pověření. Pokud tyto nejsou k dispozici, je připojení ukončeno.
- Druhou metodou je Explicitní FTPS, běží na portu 21. Vyžaduje se, aby klient výslovně uvedl, že hodlá používat SSL. Jakmile server obdrží tento příkaz, vyhledá ověřovací pověření. Explicitní FTPS umožňuje klientovi dosáhnout zvýšené bezpečnosti, nebo vyšší rychlosti.

# Klady a zápory FTPS

- Široce známé a používané.
- Poskytuje služby pro přenos souborů ze serveru na server.
- Vyžaduje sekundární kanál pro data, ztěžuje použití za Firewall.
- Ne všechny FTP servery podporují SSL / TLS.

# Praxe – Zachycení FTP komunikace

- Takto vypadá zachycená FTP komunikace:

ftp						
No.	Time	Source	Destination	Protocol	Length	Info
✓ 42	8.223919	88.86.120.160	192.168.0.103	FTP	80	Response: 220 FTP Server ready.
43	8.224435	192.168.0.103	88.86.120.160	FTP	70	Request: USER tonyytest Username
45	8.264036	88.86.120.160	192.168.0.103	FTP	92	Response: 331 Password required for tonyytest
46	8.264448	192.168.0.103	88.86.120.160	FTP	72	Request: PASS [REDACTED] Heslo
47	8.311965	88.86.120.160	192.168.0.103	FTP	88	Response: 230 User tonyytest logged in.

# Praxe – Zachycení FTP komunikace

ftp-data						
No.	Time	Source	Destination	Protocol	Length	Info
74	8.790003	88.86.120.160	192.168.0.103	FTP-DATA	422	FTP Data: 368 bytes (PASV) (MLSD)
814	129.481023	88.86.120.160	192.168.0.103	FTP-DATA	422	FTP Data: 368 bytes (PASV) (MLSD)
1104	250.054611	88.86.120.160	192.168.0.103	FTP-DATA	422	FTP Data: 368 bytes (PASV) (MLSD)
1229	305.330850	192.168.0.103	88.86.120.160	FTP-DATA	392	FTP Data: 338 bytes (PASV) (STOR README.txt)
1249	305.676009	88.86.120.160	192.168.0.103	FTP-DATA	554	FTP Data: 500 bytes (PASV) (MLSD)
2656	426.513659	88.86.120.160	192.168.0.103	FTP-DATA	554	FTP Data: 500 bytes (PASV) (MLSD)

Název souboru + přípona

Přenesená data

```
[Setup method: PASV]
[Command: STOR README.txt]
Command frame: 1223
[Current working directory: /]
Line-based text data (10 lines)
Welcome to the family,\r\n
\r\n
We are a strong and friendly community. We are gamers and we are a family. \r\n
If you love our website, please introduce it to your friends, or any ideas you want.\r\n
\r\n
"We are gamers \226 We are a family"\r\n
\r\n
\r\n
```



# Praxe – Zachycení FTP komunikace

No.	Time	Source	Destination	Protocol	Length	Info
2448...	840.069788	66.220.9.50	192.168.0.103	FTP	238	Response: 220 Welcome to the most popular FTP hosting service! Save on hardware, software, hosting and admin...
2448...	840.070238	192.168.0.103	66.220.9.50	FTP	64	Request: AUTH TLS
2448...	840.239419	66.220.9.50	192.168.0.103	FTP	105	Response: 234 AUTH Command OK. Initializing TLS connection.
2448...	840.903443	192.168.0.103	66.220.9.50	FTP	571	Request: \026\003\001\002\000\001\000\001\374\003\003W\1364\333r\345\265& \232\231\027<&\314\242\221\031\\32...
2448...	841.087747	66.220.9.50	192.168.0.103	FTP	1466	Response: \026\003\003\F^\002\000\000M\003\003J\332\317Y\277\316*\301\031\225\323\036"D;\317\302\032\226\275...
2448...	841.088129	66.220.9.50	192.168.0.103	FTP	1466	Response: @\b\375\002!\000\347R\b#x\356\001\F\222!l \266\242\265Q\A\375\#\327\235\311\020\002\343z\b\213P=o0
2448...	841.088130	66.220.9.50	192.168.0.103	FTP	401	Response: >\207\031^\351\370!\026YS\F\000\001I\003\000\027A\004\372\226'\321\232\334F\$,2[\0300\225\206\236f'...
2448...	841.228628	192.168.0.103	66.220.9.50	FTP	236	Request: \026\003\003\000F\020\000\000BA\004\366\203\211W\272w\221\363\241\335\217\276\020\267\v \243\253\31...
2448...	841.409825	66.220.9.50	192.168.0.103	FTP	161	Response: \024\003\003\000\001\001\026\003\003\000`>tG\0258\001\A\363\r\334\230\212\272\362\303?\220R%\320{...
2448...	842.640398	192.168.0.103	66.220.9.50	FTP	139	Request: \027\003\003\000P\221\255\304Qj\357\A-Z\006\376\344\252\231e@\237\303\321w\257\306\311\300\000 k\33...
2448...	842.815642	66.220.9.50	192.168.0.103	FTP	171	Response: \027\003\003\000p\237\000\373b\367\345\242\230\t\001\256\317\367,\332'\267\365\305' Gl\343\036\$ \344...
2448...	842.816275	192.168.0.103	66.220.9.50	FTP	155	Request: \027\003\003\000`\303\377Y\223\330
2448...	842.993992	66.220.9.50	192.168.0.103	FTP	203	Response: \027\003\003\000\220\323\311\vju\253i\275N\311\342\325\3362\033\273\331u\331\325,b\310\006y3\276\3...
2448...	842.994614	192.168.0.103	66.220.9.50	FTP	139	Request: \027\003\003\000P\262Q\$\261dj*\024\033\346\244\237\347\362\3215\304\313\263\341\340\374\240\201\366...
2448...	843.165027	66.220.9.50	192.168.0.103	FTP	171	Response: \027\003\003\000p\335\205\\226\177\334\326\353K\313\305\361\277i+ \217\337\322\016\024H\366\234\250...
2448...	843.166068	192.168.0.103	66.220.9.50	FTP	139	Request: \027\003\003\000P\035\253g\210\020\307\030#\203\333,?\221\027\233a\366r\027Y\371\231\204R\323HXQ\3...
2448...	843.338744	66.220.9.50	192.168.0.103	FTP	251	Response: \027\003\003\000\300\337\306\203\375\333s#\256Y\337)\$\245\345\307\264\301\272\230mH\262j\022 f0\30...
2448...	843.349905	192.168.0.103	66.220.9.50	FTP	139	Request: \027\003\003\000P\227<\322\330\315\242\2271\257\213#\2629N\_254s\214\ts.\365GjJ(\214\266\274?\257T\...
2448...	843.523147	66.220.9.50	192.168.0.103	FTP	155	Response: \027\003\003\000`b\272v\227\3160\350%? \270'\333\374\325\205\367""\260

```
> Frame 244862: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_de:3a:fc (84:16:f9:de:3a:fc), Dst: LiteonTe_64:3a:6b (20:16:d8:64:3a:6b)
> Internet Protocol Version 4, Src: 66.220.9.50, Dst: 192.168.0.103
> Transmission Control Protocol, Src Port: 21, Dst Port: 4470, Seq: 1, Ack: 1, Len: 184
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

# Zdroje

- <https://cs.wikipedia.org/wiki/FTPS>
- [https://cs.wikipedia.org/wiki/File\\_Transfer\\_Protocol](https://cs.wikipedia.org/wiki/File_Transfer_Protocol)
- [https://cs.wikipedia.org/wiki/SSH\\_file\\_transfer\\_protocol](https://cs.wikipedia.org/wiki/SSH_file_transfer_protocol)
- <https://www.secureblackbox.com/kb/articles/FTPS-vs-SFTP.rst>
- <https://www.thorntech.com/2019/07/ftp-ftp-sftp-differences/>