

FTPS - konfiguracija SSL/TLS-a u Vsftpd-u



FTP ([File Transfer Protokol](#) [1]) protokol je star vjerojatno jednako kao i sam Internet (tada se još zvao [ARPANET](#) [2]). Njegova specifičnost je da se naredbe prenose preko jednog komunikacijskog kanala (**ftp** na portu 21), a sami podaci preko drugog (**ftp-data** na portu 20). Sam protokol nećemo ovdje opisivati, jer je na njega potrošeno previše "digitalne tinte". Ono što nam je problem koji pokušavamo riješiti je slanje zaporka u čitljivom obliku, koji osnovni FTP protokol redovito radi.

Ako ste pomislili "pa čemu uopće rabiti FTP, postoji scp, sftp, Secure FTP..."? Pa, kao i uvijek, zadržati kompatibilnost unatrag je jako korisno, kako se vaši korisnici ne bi previše bunili. S vremenom ćete ih već sve prebaciti na FTPS.

FTPS nemojte buniti s SFTP-om, niti bilo kojim drugim oblikom kvazi-ftp protokola ili tuneliranjem preko SSH-a. Ovo je "čisti" FTP protokol, s dodanom podrškom za SSL, odnosno TLS. Za ovo mu trebaju, dakako, dva nova TCP porta (**ftps-data** na **989** i **ftps** na **990**), ali zbog kompatibilnosti, može u nekim uvjetima nastaviti raditi na starim portovima 20 i 21. Možda mislite da ne postoji mnogo klijenata s podrškom za FTPS, ali mogli bi se prevariti. Podržava ga mnoštvo Linux/Unix i Windows klijenata (CuteFTP, cURL, FireFTP, WS FTP, WinSCP itd.)

FTPS ima, u principu, dva načina rada: FTPS i FTPeS. Prvi je bezuvjetni, implicitni oblik, i ukoliko vaš klijent ne podržava FTPS, neće se moći spojiti. Drugi je uvjetni, eksplicitni oblik, gdje klijent određuje koji će dio komunikacije biti enkriptiran, kojim načinom enkripcije i slično. Stari programi će se moći spojiti na ovakav poslužitelj. FTPeS je fleksibilan, i klijenti će moći primjerice zahtijevati da je autentikacija enkriptirana, ali sâm prijenos podataka ne (time se dobije nešto na brzini).

U članku "Certifikati za servise" na adresi <http://sistemac.carnet.hr/node/315> [3] smo opisali kao dodati certifikat u vsftpd. Nije toliko bitno je li certifikat službeni ili samogenerirani, iako preporučujemo prvi (kako ga dobiti pogledajte u članku http://www.carnet.hr/sc_servis [4]).

Postavke za vsftpd, koje dodajemo u /etc/vsftpd.conf i koje omogućuju i uobičajeni način rada su:

```
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=NO
force_local_logins_ssl=NO
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
rsa_cert_file=/etc/ssl/certs/mojserver.pem
rsa_private_key_file=/etc/ssl/private/mojserver.key
```

Slijede postavke koje će omogućiti da klijent izabere hoće li rabiti stari načina rada, ili rabiti neki od sigurnih protokola (izbacit ćemo ponovljene retke):

```
ssl_enable=YES
allow_anon_ssl=NO
force_anon_logins_ssl=YES
force_anon_data_ssl=YES
```

```
force_local_data_ssl=YES  
force_local_logins_ssl=YES
```

Ukoliko želite da i anonimni korisnici imaju pristup preko sigurne konekcije, postavite varijablu **allow_anon_ssl** na YES. Ukoliko ne želite da se i sami podaci enkriptiraju, stavite **NO** na varijable **force_anon_data_ssl** i **force_local_data_ssl** (prijava korisnika će i dalje biti enkriptirana).

U čemu je prednost FTPS-a nad drugim oblicima enkriptiranog prijenosa podataka? Ukoliko rabite neki od SSH protokola, morate imati korisnike na sustavu. Za FTPS to ne morate imati, dakle sigurnost je samo uvećana. Ovo je odlično ukoliko imate web hosting, gdje korisnici samo trebaju uploadati svoje web stranice, a mail i ostalo im ne treba.

- [Logirajte](#) [5] se za dodavanje komentara

čet, 2010-09-30 23:38 - Željko BorošKuharice: [Linux](#) [6]

Kategorije: [Software](#) [7]

[Servisi](#) [8]

Vote: 4.5

Vaša ocjena: Nema Average: 4.5 (2 votes)

story_tag: [ftp](#) [9]

[ftps](#) [10]

[ssl](#) [11]

[tls](#) [12]

[sigurni ftp](#) [13]

Source URL: <https://sysportal.carnet.hr/node/776>

Links

[1] https://en.wikipedia.org/wiki/File_Transfer_Protocol

[2] <https://en.wikipedia.org/wiki/ARPANET>

[3] <https://sysportal.carnet.hr/node/315>

[4] http://www.carnet.hr/sc_servis

[5] <https://sysportal.carnet.hr/sysportallogin>

[6] <https://sysportal.carnet.hr/taxonomy/term/17>

[7] <https://sysportal.carnet.hr/taxonomy/term/25>

[8] <https://sysportal.carnet.hr/taxonomy/term/28>

[9] <https://sysportal.carnet.hr/taxonomy/term/77>

[10] <https://sysportal.carnet.hr/taxonomy/term/78>

[11] <https://sysportal.carnet.hr/taxonomy/term/79>

[12] <https://sysportal.carnet.hr/taxonomy/term/80>

[13] <https://sysportal.carnet.hr/taxonomy/term/81>