

## SFTP VA FTPS PROTOKOLLARINING XAVFSIZLIK FARQLARI

Sobirjonov Begzod

FarDu Axborot texnologiyalari kafedrası o'qituvchisi

[behzodbekqahramonovich@gmail.com](mailto:behzodbekqahramonovich@gmail.com)

Yusufjonova Xojiraxon Nuriddin qizi

FarDu Axborot tizimlari va texnologiyalari yo'nalishi 2-bosqich talabasi

[hojiraxonmurotaliyeva@gmail.com](mailto:hojiraxonmurotaliyeva@gmail.com)

<https://doi.org/10.5281/zenodo.20079919>

### ANNOTATSIYA

Mazkur maqolada SFTP va FTPS protokollarining xavfsizlik jihatlari, ularning ishlash prinsipi hamda amaliy qo'llanilishidagi farqlar tahlil qilinadi. Shifrlash usullari, autentifikatsiya mexanizmlari va tarmoq xavfsizligiga ta'siri yoritiladi.

Kalit so'zlar: SFTP, FTPS, SSH, SSL/TLS, fayl uzatish, autentifikatsiya, shifrlash, kiberxavfsizlik.

### АННОТАЦИЯ

В статье анализируются различия безопасности протоколов SFTP и FTPS, принципы их работы и практическое применение. Рассматриваются методы шифрования, механизмы аутентификации и влияние на сетевую безопасность.

**Ключевые слова:** SFTP, FTPS, SSH, SSL/TLS, передача файлов, аутентификация, шифрование, кибербезопасность.

### ANNOTATION

This article analyzes the security differences between SFTP and FTPS protocols, their operating principles, and practical use. Encryption methods, authentication mechanisms, and network security impacts are discussed.

**Keywords:** SFTP, FTPS, SSH, SSL/TLS, file transfer, authentication, encryption, cybersecurity.

### KIRISH

Hozirgi axborot texnologiyalari rivojlangan davrda ma'lumotlarni xavfsiz uzatish dolzarb masalalardan biri hisoblanadi. Korxonalar, davlat tashkilotlari hamda shaxsiy foydalanuvchilar turli hajmdagi fayllarni internet orqali yuborish va qabul qilish jarayonida ishonchli himoyaga muhtoj bo'ladi. Oddiy FTP protokoli ma'lumotlarni ochiq ko'rinishda uzatgani sababli xavfsizlik talablariga javob bermaydi. Shu sababli uning xavfsiz variantlari sifatida SFTP va FTPS protokollari ishlab chiqilgan.

Mazkur protokollar fayl uzatish jarayonida ma'lumotlarni shifrlash, foydalanuvchini tekshirish va ruxsatsiz kirishlarning oldini olish imkonini beradi. Ammo ularning ishlash prinsipi, himoya usullari va qo'llanilish sohalarida muhim farqlar mavjud.

### ASOSIY QISM

SFTP (SSH File Transfer Protocol) SSH protokoli asosida ishlaydi. U alohida FTP ga qo'shimcha emas, balki mustaqil protokol hisoblanadi. SFTP orqali barcha buyruqlar, login-parol ma'lumotlari va uzatilayotgan fayllar yagona xavfsiz kanal orqali shifrlangan holda yuboriladi. Bu esa tarmoqdagi hujumchilar tomonidan ma'lumotlarni kuzatish yoki o'g'irlash ehtimolini kamaytiradi.

FTPS esa FTP protokolining xavfsizlashtirilgan ko'rinishi bo'lib, SSL/TLS texnologiyasi asosida ishlaydi. U an'anaviy FTP tizimiga qo'shimcha xavfsizlik qatlamini qo'shadi. FTPS server

va mijoz o'rtasida sertifikatlar orqali ishonchni tekshiradi hamda ma'lumotlarni shifrlaydi. FTPS explicit va implicit rejimlarda ishlashi mumkin.

SFTP va FTPS o'rtasidagi asosiy xavfsizlik farqlari quyidagilardan iborat:

Shifrlash usuli:

SFTP SSH protokoliga asoslangan bo'lsa, FTPS SSL/TLS texnologiyasidan foydalanadi.

Portlardan foydalanish:

SFTP odatda bitta port (22-port) orqali ishlaydi. FTPS esa boshqaruv va ma'lumot uzatish uchun bir nechta portlardan foydalanishi mumkin.

Autentifikatsiya:

SFTP login-parol bilan birga SSH kalitlari orqali autentifikatsiyani qo'llaydi. FTPS esa ko'proq sertifikatlarga tayanadi.

Firewall bilan ishlash:

SFTP yagona port ishlatgani sababli firewall va NAT muhitida oson sozlanadi. FTPS esa ko'p port ishlatgani uchun murakkabroq bo'lishi mumkin.

Moslashuvchanlik:

FTPS eski FTP infratuzilmasiga ega tashkilotlarda qulay. SFTP esa yangi va zamonaviy tizimlarda kengroq qo'llaniladi.

Amaliyotda server boshqaruvi, hosting xizmatlari va masofaviy tizimlarda SFTP ko'proq tanlanadi. Korporativ sertifikat tizimi mavjud bo'lgan yirik tashkilotlarda esa FTPS samarali yechim bo'lishi mumkin.

### **XULOSA**

Xulosa qilib aytganda, SFTP va FTPS protokollari fayl uzatishda yuqori darajadagi xavfsizlikni ta'minlaydi. Biroq ularning texnik ishlash usullari turlicha. SFTP sodda konfiguratsiyasi, yagona port orqali ishlashi va kuchli himoya mexanizmi sababli ko'plab hollarda afzal ko'riladi. FTPS esa mavjud FTP tizimlarini yangilash va sertifikat asosida ishlash zarur bo'lgan joylarda qulay hisoblanadi.

Kelajakda axborot xavfsizligi talablari ortib borishi bilan ushbu protokollarning ahamiyati yanada oshib boradi.

### **Adabiyotlar, References, Литературы:**

1. Kurose J., Ross K. Computer Networking: A Top-Down Approach.
2. RFC 4217 – Securing FTP with TLS.
3. SSH Communications Security. SFTP Specifications.
4. Stallings W. Network Security Essentials.