SFTP VA FTPS PROTOKOLLARINING XAVFSIZLIK FARQLARI

Behzod Sobirjonov Qahramonivich
FarDu Axborot tehnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Ergasheva Feruzaxon Ilhomjon qizi
FarDu Axborot tizimlari va texnologiyalari yo‘nalishi 2-bosqich talabasi
feruzazokirova2005@gmail.com
Telefon raqam: 90-059-05-10
https://doi.org/10.5281/zenodo.19938709

Annotatsiya

Ushbu maqolada fayllarni xavfsiz uzatish jarayonida keng qo‘llaniladigan SFTP (Secure File Transfer Protocol) va FTPS (FTP Secure) protokollarining xavfsizlik jihatlari tahlil qilinadi. Maqolada ushbu protokollarning ishlash mexanizmlari, ma’lumotlarni shifrlash usullari, autentifikatsiya jarayonlari hamda tarmoq xavfsizligiga ta’siri o‘rganilgan. Shuningdek, SFTP va FTPS o‘rtasidagi asosiy farqlar, ularning afzallik va kamchiliklari, hamda turli amaliy holatlarda qaysi protokoldan foydalanish maqsadga muvofiqligi yoritib berilgan. Tadqiqot natijasida xavfsiz fayl uzatishni ta’minlashda samarali yondashuvlar va zamonaviy himoya strategiyalari bo‘yicha tavsiyalar keltirilgan.

Kalit so‘zlar: Kiberxavfsizlik, SFTP, FTPS, Ma’lumotlarni shifrlash, Autentifikatsiya, Tarmoq xavfsizligi, Fayl uzatish protokollari.

Аннотация

В данной статье анализируются аспекты безопасности протоколов SFTP (Secure File Transfer Protocol) и FTPS (FTP Secure), широко используемых в процессе безопасной передачи файлов. В статье рассматриваются механизмы работы этих протоколов, методы шифрования данных, процессы аутентификации и их влияние на сетевую безопасность. Также освещены основные различия между SFTP и FTPS, их преимущества и недостатки, а также какой протокол целесообразно использовать в различных практических ситуациях. В результате исследования были представлены рекомендации по эффективным подходам и современным стратегиям защиты для обеспечения безопасной передачи файлов.

Ключевые слова: Кибербезопасность, SFTP, FTPS, Шифрование данных, Аутентификация, Сетевая безопасность, Протоколы передачи файлов.

Abstract

This article analyzes the security aspects of SFTP (Secure File Transfer Protocol) and FTPS (FTP Secure) protocols, which are widely used in the process of secure file transfer. The article examines the operating mechanisms of these protocols, data encryption methods, authentication processes, and their impact on network security. It also highlights the main differences between SFTP and FTPS, their advantages and disadvantages, as well as which protocol should be used in various practical situations. As a result of the study, recommendations were provided for effective approaches and modern protection strategies to ensure secure file transfer.

Keywords: Cybersecurity, SFTP, FTPS, Data Encryption, Authentication, Network Security, File Transfer Protocols.

Zamonaviy axborot tizimlarida ma’lumotlarni xavfsiz uzatish masalasi muhim ahamiyat kasb etadi. Ayniqsa, tarmoqlar orqali fayllarni almashish jarayonida maxfiylik, yaxlitlik va autentifikatsiya talablariga qat’iy rioya qilish zarur. Shu nuqtai nazardan, SFTP (Secure File Transfer Protocol) va FTPS (FTP Secure) protokollari keng qo‘llanilib, ular orqali ma’lumotlar uzatishda yuqori darajadagi xavfsizlik ta’minlanadi. Biroq ushbu ikki protokolning ishlash mexanizmlari va himoya yondashuvlari o‘zaro sezilarli darajada farq qiladi.

SFTP protokoli SSH (Secure Shell) asosida ishlaydi va barcha ma’lumot almashinuvi yagona shifrlangan kanal orqali amalga oshiriladi. Bu esa uzatilayotgan ma’lumotlarning uchinchi tomon tomonidan o‘qib olinishi yoki o‘zgartirilishining oldini oladi. SFTP’da autentifikatsiya parol yoki maxfiy kalitlar yordamida bajariladi, bu esa xavfsizlikni yanada kuchaytiradi. Bundan tashqari, u faqat bitta port orqali ishlagani sababli tarmoq qurilmalarida sozlash jarayoni ancha sodda va qulay kechadi. Shu jihatlari bilan SFTP zamonaviy tizimlarda ishonchli va samarali yechim sifatida qaraladi.

FTPS esa an’anaviy FTP protokolining kengaytirilgan ko‘rinishi bo‘lib, unda SSL/TLS shifrlash texnologiyalari qo‘llaniladi. FTPS’da boshqaruv va ma’lumot uzatish jarayonlari alohida kanallar orqali amalga oshiriladi va har bir kanal alohida himoyalanishi mumkin. U implicit va explicit rejimlarda ishlashi bilan ajralib turadi. Biroq bir nechta portlardan foydalanilishi sababli, ba’zi hollarda xavfsizlik devorlari bilan ishlash murakkablashadi. Shuningdek, sertifikatlarni boshqarish va sozlash jarayoni ham qo‘shimcha e’tibor talab qiladi.

Umuman olganda, SFTP va FTPS protokollari bir xil maqsadga — xavfsiz fayl uzatishni ta’minlashga xizmat qilsa-da, ularning yondashuvi turlicha. SFTP yagona kanal va sodda arxitekturasi bilan ajralib tursa, FTPS mavjud FTP infratuzilmasini saqlagan holda xavfsizlikni oshirish imkonini beradi. Amaliyotda esa tizim talablari va infratuzilma imkoniyatlaridan kelib chiqib, ushbu protokollardan birini tanlash maqsadga muvofiq bo‘ladi.

Yuqoridagi tahlillardan ko‘rinib turibdiki, SFTP va FTPS protokollari fayllarni xavfsiz uzatishda muhim o‘rin egallaydi, biroq ularning ishlash yondashuvi va xavfsizlik mexanizmlari turlicha. SFTP yagona shifrlangan kanal orqali ishlashi, oddiy konfiguratsiyasi va yuqori darajadagi yaxlit xavfsizlik modeli bilan ajralib turadi. FTPS esa an’anaviy FTP asosida qurilgan bo‘lib, SSL/TLS yordamida himoyalanadi va mavjud infratuzilmani saqlab qolish imkonini beradi, ammo sozlash va boshqarish jihatidan nisbatan murakkabroq hisoblanadi.

Adabiyotlar, References, Литературы:

1. OWASP Foundation. *Transport Layer Security Cheat Sheet*, 2024.
2. IBM. *Secure File Transfer: SFTP vs FTPS Security Comparison*, 2023.
3. Microsoft. *Secure File Transfer Protocols and Best Practices*, 2024.
4. National Institute of Standards and Technology. *Guidelines for Secure File Transfer and Data Protection*, 2023.