Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-inet-ftp

INTERNET

FTP, FTPS i SFTP, czyli trzy sposoby przewożenia paczek

W firmie transportowej „Trzy Litery i Magazyn” Grzesiu postanowił przesłać jeden plik. Na bramie wisiały trzy szyldy: FTP, FTPS i SFTP. Wszystkie obiecywały dostarczyć paczkę, ale każdy kierowca miał inny samochód, inne klucze i inny pomysł na bezpieczeństwo. Grzesiu spojrzał na plik o nazwie „ostateczna_wersja_NAPRAWDE_7.zip”. — Panowie, ja tylko chcę go wysłać! 📦🤣

Dwie bramy do jednego magazynu

— Dzień dobry, FTP — przedstawił się kierownik pierwszego magazynu.

— File Transfer Protocol? — spytał Grzesiu.

— Zgadza się. Od dawna zajmuję się przesyłaniem plików między klientem a serwerem.

— To czemu macie dwie bramy?

— Jedną do rozmowy, drugą do przewożenia paczek.

W klasycznym **FTP** klient nawiązuje **połączenie sterujące**, zwykle do portu TCP 21. Przez nie wysyła polecenia, loguje się, wybiera katalog, pyta o listę plików. Do przesyłania zawartości plików i list katalogów służy osobne **połączenie danych**.

— Czyli przez pierwszą bramę krzyczę „poproszę paczkę”, a przez drugą przyjeżdża samochód?

— Dokładnie.

— A dlaczego nie jedną bramą?

— Bo tak zaprojektowano protokół. Proszę nie przebudowywać nam magazynu w pierwszym dniu pracy.

Aktywnie, czyli kurier dzwoni do Grzesia

— Wypróbujemy tryb aktywny — zarządził kierownik.

— Aktywnie to ja mogę biegać — ucieszył się Grzesiu.

— Tutaj chodzi o to, kto rozpoczyna połączenie danych.

W **aktywnym FTP** klient informuje serwer, pod jakim adresem i portem oczekuje na połączenie danych. Serwer próbuje wtedy nawiązać to połączenie z powrotem do klienta. Tradycyjnie po stronie serwera używano portu źródłowego TCP `20`, choć szczegóły mogą się różnić zależnie od implementacji i trybu.

Kurier stanął przed mieszkaniem Grzesia i nacisnął domofon.

— Dzień dobry, paczka z magazynu!

— A kto pana zapraszał?! — wrzasnął router.

— Przecież Grzesiu zamówił!

— Zamówienie zamówieniem, ale niezapowiedzianych połączeń z Internetu nie wpuszczam!

To klasyczny problem przy kliencie schowanym za **NAT-em lub firewallem**: serwer ma sam rozpocząć nową sesję do klienta, a urządzenie po drodze może ją zablokować.

— Czyli działało, dopóki nie zamknęliśmy drzwi?

— Tak. A otwieranie całego budynku na oścież nie jest najlepszym lekarstwem.

Pasywnie, czyli Grzesiu sam jedzie po paczkę

— Spróbujmy trybu pasywnego — zaproponowała pani Agnieszka.

— Czyli nie robimy nic?

— Nie, panie Grzesiu. Nadal robimy. Tylko inicjatorem połączenia danych jest klient.

W **pasywnym FTP** serwer wskazuje klientowi adres i port, na którym czeka na połączenie danych. Klient zestawia połączenie w kierunku serwera. Służą do tego m.in. polecenia `PASV` i `EPSV`. Serwer często wykorzystuje skonfigurowany zakres portów pasywnych, który musi być właściwie dostępny przez firewall.

— Czyli teraz ja wychodzę z domu i jadę do magazynu?

— Dokładnie. Routerowi zwykle łatwiej obsłużyć połączenie rozpoczęte od pana.

— A jak serwer poda prywatny adres, pod który nie da się dojechać?

— Wtedy źle skonfigurowany NAT lub odpowiedź serwera nadal może wszystko popsuć. Właśnie dlatego istnieje też EPSV, który pomaga uniknąć części problemów z adresami.

— To pasywny jest zawsze magicznie bezproblemowy?

— Nie. W informatyce magii szukamy w dziale reklamy.

Hasło na pocztówce

Przy bramie FTP Grzesiu podał login i hasło.

— Proszę wpisać tutaj — powiedział ochroniarz, podając przezroczystą kopertę.

— PRZECIEŻ WSZYSCY MOGĄ TO ZOBACZYĆ!

— Właśnie poznaje pan największy problem klasycznego FTP.

Zwykły **FTP nie szyfruje** standardowo poleceń logowania ani przesyłanej treści. Osoba mogąca podsłuchiwać właściwy odcinek sieci może odczytać wrażliwe informacje. To protokół o długiej historii, ale dziś przesyłanie haseł i danych otwartym tekstem przez niezaufane sieci jest złym pomysłem.

— A jak nazwę plik „ściśle tajne” i wpiszę osiem wykrzykników?

— To nadal nie jest szyfrowanie.

— A jeśli hasło jest bardzo długie?

— Długość hasła nie pomoże, jeśli ktoś może je podejrzeć podczas transmisji.

Grzesiu odłożył przezroczystą kopertę.

— Poproszę transport z zamkniętymi drzwiami.

FTPS, czyli stary magazyn z plombami TLS

Do bramy podjechała ciężarówka z napisem **FTPS**.

— Jestem nadal FTP, ale chronię transmisję przy użyciu TLS — oznajmił kierowca.

— Czyli wystarczyło dodać literkę S?

— Nazwa tak sugeruje, ale technicznie chodzi o FTP zabezpieczone TLS, z zachowaniem rozdzielenia połączeń sterującego i danych.

W wariancie **explicit FTPS** klient zwykle łączy się do portu `21` i poleceniem `AUTH TLS` rozpoczyna negocjację szyfrowania. Istnieje też historyczny wariant **implicit FTPS**, tradycyjnie na porcie `990`, w którym TLS rozpoczyna się od początku połączenia. Ochrona połączenia danych także wymaga odpowiednich ustawień, na przykład `PROT P`.

— To teraz firewall wie, gdzie ma jechać drugi samochód?

— Niekoniecznie. Gdy rozmowa sterująca jest zaszyfrowana, urządzenie sieciowe nie może po prostu podejrzeć poleceń FTP i automatycznie odgadnąć potrzebnych portów.

— Czyli ciężarówka jest bezpieczniejsza, ale portier ma trudniej?

— Zgadza się. Dlatego trzeba poprawnie ustawić zakres portów, reguły i adresy.

— Nie można było zrobić tego od razu prościej?

— Proszę spytać architektów historii.

SFTP nie jest FTP w innym kapeluszu

Przy trzeciej bramie stał kierowca z identyfikatorem SSH.

— SFTP. Zapraszam.

— To pan jest FTPS, tylko literki się panu zamieniły? — zapytał Grzesiu.

— Absolutnie nie!

SFTP oznacza protokół przesyłania plików działający w ramach połączenia **SSH**. To odrębne rozwiązanie od FTP i FTPS. Zwykle używa pojedynczego połączenia do serwera SSH na porcie TCP 22, o ile administrator nie wybrał innego. Nie ma klasycznego dla FTP rozdziału na kanał poleceń i osobne sesje danych.

— Czyli wjeżdżam jedną bramą?

— Tak. Uwierzytelnienie i transport korzystają z mechanizmów SSH.

— Hasło albo klucz publiczny?

— Zależnie od konfiguracji. Przy logowaniu kluczem używa się pary kluczy SSH; serwer weryfikuje uprawnienia klienta.

— A czy serwer ma własną tożsamość?

— Ma klucz hosta. Warto sprawdzić jego odcisk przy pierwszym zaufanym połączeniu i nie ignorować bezmyślnie ostrzeżeń o zmianie.

— To nie jest zwykłe FTP z kłódką?

— Nie. A za następne takie pytanie doliczę opłatę edukacyjną.

Komenda skasuj to nie prośba o urlop

Grzesiu w końcu połączył się z magazynem.

— Widzę katalog! Mogę wysłać paczkę, pobrać ją, zmienić nazwę albo usunąć?

— Jeśli pozwalają na to uprawnienia konta i serwera — odpowiedziała Agnieszka.

Programy takie jak FileZilla czy WinSCP udostępniają wygodny interfejs do pracy z plikami, ale używany protokół nadal ma znaczenie. Dobrze dobrane uprawnienia, wydzielone konta i katalogi pomagają ograniczać skutki pomyłek. Szyfrowany transport nie chroni przed świadomym usunięciem pliku przez użytkownika, który ma do tego prawo.

— Czyli jeśli usunę wszystko, to połączenie SSH mnie nie uratuje?

— Nie. Szyfrowanie chroni przesyłanie, nie naprawia złych decyzji.

— A backup?

— Bardzo potrzebny. To osobna kopia, a nie inny przycisk w kliencie FTP.

— To ja może jednak najpierw wyślę jeden plik.

— Od tego zaczęliśmy, panie Grzesiu.

— Nie przypominaj.

Co z dużym plikiem i przerwanym łączem?

Kurier ruszył z plikiem ważącym kilka gigabajtów. W połowie drogi zniknął Internet.

— PACZKA ZAGINĘŁA! — wrzasnął Grzesiu.

— Spokojnie. Sprawdźmy, ile danych rzeczywiście trafiło na serwer.

Wiele klientów i serwerów obsługuje **wznawianie transferu**, ale konkretna możliwość zależy od protokołu, programu, serwera i sposobu obsługi pliku. Przy klasycznym FTP istnieje na przykład polecenie REST, a SFTP ma operacje odczytu i zapisu od wskazanych pozycji. Warto też zweryfikować integralność rezultatu, np. porównując sumy kontrolne, gdy wymagana jest pewność zgodności danych.

— Czyli jak plik wygląda na cały, to na pewno jest cały?

— Nie zakładajmy. Rozmiar może pomóc, ale nie zawsze dowodzi zgodności zawartości.

— A jeśli wysłałem stary plik pod poprawną nazwą?

— Nawet idealny protokół nie zgadnie, że wziął pan niewłaściwą paczkę.

Grzesiu poszedł szukać pliku „ostateczna_wersja_NAPRAWDE_8.zip”.

Raport z magazynu

Na zakończenie dnia kierownik ustawił trzy ciężarówki obok siebie.

— FTP?

— Klasyczny transport, osobne połączenie sterujące i danych, bez szyfrowania w zwykłej postaci.

— FTPS?

— FTP zabezpieczone TLS, nadal z dwiema rolami połączeń.

— SFTP?

— Oddzielny protokół przesyłania plików przez SSH.

Wybór metody zależy od zgodności urządzeń, wymagań bezpieczeństwa i sposobu zarządzania dostępem. Dla nowych usług przesyłających dane przez niezaufaną sieć warto preferować bezpiecznie skonfigurowany SFTP albo FTPS, zamiast przesyłać hasła zwykłym FTP. Osobno należy zaplanować uprawnienia, kontrolę poprawności i kopie zapasowe.

— Czy wreszcie mogę wysłać mój plik?

— Tak.

— To gdzie on jest?

— W koszu na pulpicie.

W magazynie zapadła cisza.

— Niech pan tam nie zagląda! — krzyknął Grzesiu.

Zarząd firmy „Trzy Litery i Magazyn” informuje: brama sterująca FTP działa, porty pasywne zostały uporządkowane, ciężarówki FTPS otrzymały plomby, a SFTP odmówiło przyjęcia kolejnego zamówienia podpisanego „to samo, tylko bardziej S”. Grzesiu przesłał wreszcie plik. Niestety był to skrót do pliku. Dostawa zakończyła się sukcesem technicznym i katastrofą organizacyjną. 🧀🚚🤣❤️