



---

**Wydział Dziennikarstwa  
Informacji i Bibliologii**  
Uniwersytet Warszawski

---

inż. Adam Balcerzak

# **CMS i nawigacja stron**

[adam.balcerzak@uw.edu.pl](mailto:adam.balcerzak@uw.edu.pl)



- Porównanie protokołów FTP/SFTP/SSH
- SSL – jak działa i jakie są jego rodzaje?
- Czym jest REDIS i jak działa?
- Czym jest Content Delivery Network?
- Panel Wordpress – strony i wpisy – budujemy strukturę strony



- FTP, FTPS oraz SFTP są stosowane przez twórców stron WWW podczas przesyłania plików składających się na witryny na serwer WWW, na którym są publikowane. Główne różnice pomiędzy FTP, FTPS oraz SFTP są związane z kwestiami bezpieczeństwa, które warto poznać, aby uniknąć niedogodności podczas zarządzania zawartością swoich stron internetowych.

Źródło: <https://domenomania.pl/centrum-wiedzy/czym-roznia-sie-ftp-ftp-s-oraz-sftp>

# Czy jest FTP i FTPS?

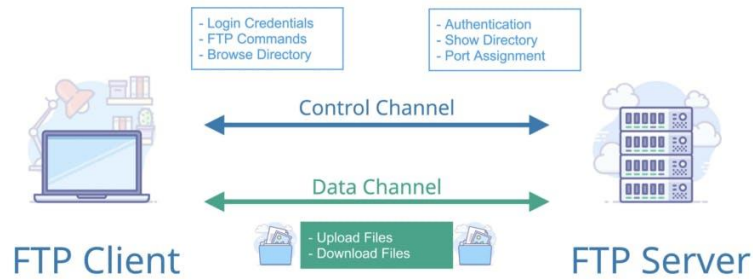


FTP jest skrótem pochodzącym z języka angielskiego i po rozwinięciu oznacza: File Transfer Protocol. Jak sama nazwa wskazuje – FTP jest protokołem, który służy do transmisji plików pomiędzy klientem (czyli programem do tego służącym), który znajduje się na Twoim komputerze i serwerem, na którym umieszczasz pliki i katalogi.

Stosowanie standardowego protokołu FTP może być niebezpieczne, ponieważ przesyłane za jego pośrednictwem pliki nie są szyfrowane. Pliki przesyłane za pośrednictwem FTP mogą zostać „podслuchane” przez osoby niepowołane (wraz z loginem i hasłem do serwera FTP). Z tego powodu używanie protokołu FTP nie jest zalecane z uwagi na niebezpieczeństwo wycieku danych dostępowych do serwera FTP.

Protokół FTPS jest o wiele bezpieczniejszą metodą przesyłania plików w porównaniu do standardowego FTP. Protokół FTPS działa bardzo podobnie jak FTP, a jego główną różnicą jest szyfrowanie przesyłanych danych dostępowych podczas połączenia z serwerem FTP.

Źródło: <https://www.exavault.com/blog/what-is-ftp-tutorial-video-blog> ; <https://domenomania.pl/centrum-wiedzy/czym-roznia-sie-ftp-fts-oraz-sftp> ; <https://www.goanywhere.com/managed-file-transfer/connectivity/fts>

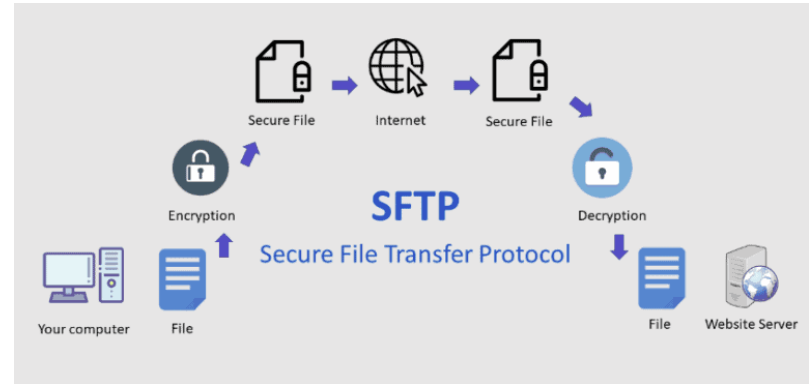


# Czym jest SFTP?



- Połączenie przez SFTP zapewnia szyfrowanie zarówno przesyłanych plików oraz danych dostępowych (loginu i hasła dostępu) do serwera FTP. Natomiast tradycyjne połączenie FTP nie zapewnia szyfrowania plików i danych dostępowych do serwera. Z tego względu połączenie przez SFTP jest uznawane za najbezpieczniejszą metodę przesyłania plików i katalogów na hosting.
- SFTP zapewnia dostęp do plików, przesyłanie ich oraz inne narzędzia do zarządzania plikami i katalogami poprzez bezpieczne połączenie SSH. SFTP to oddzielny i bezpieczny protokół, który nie jest zwyczajną metodą połączenia za pośrednictwem FTP z użyciem SSH.
- W porównaniu do połączeń FTP oraz FTPS, połączenie SFTP zapewnia szyfrowanie zarówno przesyłanych plików, loginu i hasła dostępu. Natomiast przy protokole FTPS szyfrowane jest tylko login i hasło.

Źródło: <https://domenomania.pl/centrum-wiedzy/czym-roznia-sie-ftp-ftp-s-oraz-sftp> ;  
<https://cloudinfrastructureservices.co.uk/what-is-sftp-and-how-sftp-works-secure-file-transfer-protocol/>

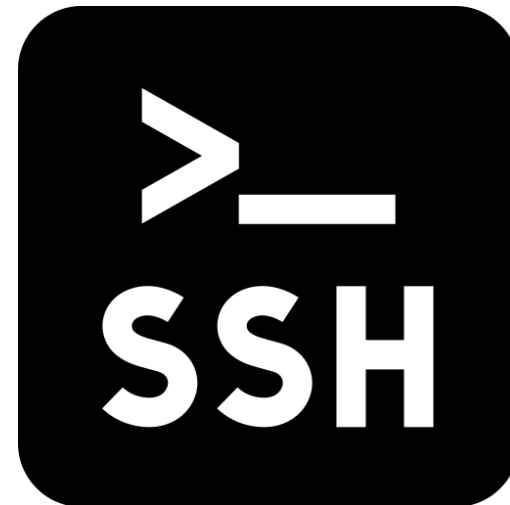


# Czym jest SSH?



- SSH (z angielskiego: Secure Shell) to protokół komunikacyjny wykorzystywany w sieciach TCP/IP, umożliwiający zdalne połączenie z serwerem. Wszystkie dane transferowane drogą SSH są szyfrowane, a uwierzytelnianie użytkowników zachodzi na wielu poziomach. Protokół SSH zastąpił Telnet, który niestety nie szyfrował danych, tym samym narażając je na wyciek. Protokół SSH działa na linii klient-serwer, domyślnie wykorzystując port 22. Dzięki technologii SSH można w bezpieczny sposób połączyć się z takimi systemami jak wirtualny serwer VPS i serwer dedykowany.
- Za pomocą protokołu SSH można zdalnie połączyć się z serwerem i tym samym uzyskać dostęp do jego powłoki systemowej, zwanej czasem również konsolą bądź terminalem. Powłoka systemowa pozwala na szeroki zakres działań: można dowolnie zarządzać serwerem, zmieniać uprawnienia plikom i katalogom, przekształcać je, tworzyć nowe. Z poziomu konsoli możemy też pakować i rozpakowywać archiwa. Innymi słowy, protokół SSH służy do zarządzania wszystkimi plikami opublikowanymi na serwerze, umożliwiając ich dowolną modyfikację.
- Zastosowanie protokołu SSH jest ogromne. Wykorzystuje się go, by zdalnie skonfigurować serwer lub niepoprawnie działający router czy uzyskać dostęp do zdalnych baz danych. Protokół zapewnia możliwość korzystania z poczty elektronicznej, pozwala też na bezpieczny transfer plików. Protokół SSH jest bardzo przydatny w codziennej pracy na zdalnym sprzęcie. Przy okazji znacząco wpływa też na bezpieczeństwo, ponieważ przy jego pomocy możemy zwalczyć atak na naszą stronę z zewnątrz, np. próbę przechwycenia hasła lub podszywanie się pod serwer DNS.
- Istnieje wiele aplikacji obsługujących protokół SSH, jednak najpopularniejszą, bezpłatną platformą jest zdecydowanie Putty. Putty jest dostępne zarówno dla użytkowników Windows, jak i Linux/UNIX. Dużym ułatwieniem jest fakt, że aplikacja nie wymaga instalacji; można z niej korzystać od razu po pobraniu.

Źródło: <https://www.sprintdatacenter.pl/blog/protokol-ssh-do-czego-mozna-go-wykorzystac-i-jak-podjac-pierwsze-kroki/> ; [https://www.flaticon.com/free-icon/ssh\\_5225347](https://www.flaticon.com/free-icon/ssh_5225347)



# SSL – czym jest i jakie są jego rodzaje?



- Certyfikat SSL to specjalny sieciowy protokół bezpieczeństwa. Jego zadaniem jest zapewnienie na stronie poufności dla przesyłanych danych na przykład podczas zakupów w sklepie internetowym. To dzięki niemu, wszystkie dane przekazywane pomiędzy przeglądarką internetową a serwerem WWW są szyfrowane oraz pozostają prywatne i zabezpieczone przed nieautoryzowanym dostępem cyberprzestępców.

Działanie certyfikatu SSL oparte jest na dwóch filarach – szyfrowaniu danych oraz uwierzytelnieniu.

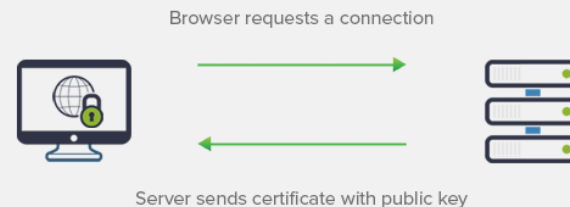
Szyfrowanie zabezpiecza przed przechwyceniem bardzo wrażliwych danych takich jak:

- dane osobowe wprowadzane przez Twoich klientów w formularzach zakupowych,
- dane autoryzacyjne dla kart płatniczych, kiedy taka forma płatności dostępna jest w sklepie internetowym,
- podczas przesyłania informacji o płatności,
- wiadomości przesyłane za pomocą formularza kontaktowego,
- Funkcja uwierzytelnienia pozwala na weryfikację oraz potwierdzenie tożsamość klienta – czyli przeglądarki internetowej z której korzysta użytkownik strony, oraz serwera, na którym zainstalowany jest certyfikat.

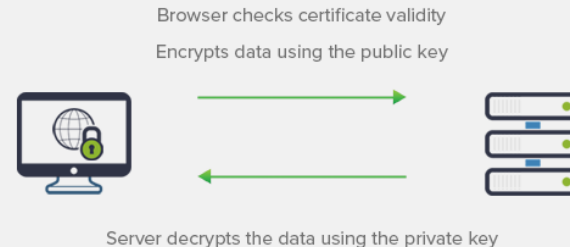
Źródło: <https://zenbox.pl/certyfikaty-ssl/> ;  
<https://www.wpbeginner.com/glossary/ssl/>

## HOW SSL WORKS

### STEP 1



### STEP 2



## SSL – czym jest i jakie są jego rodzaje?

---



### **Czym różni się darmowy certyfikat Let's Encrypt od rozwiązania komercyjnego?**

W kwestii bezpieczeństwa certyfikat Let's Encrypt nie różni się niczym w przeciwieństwie do płatnych certyfikatów. W przeciwieństwie do rozwiązań komercyjnych Let's Encrypt nie jest objęty żadną gwarancją wystawcy i jest też anonimowy.

### **Jakie „kruczki” kryją się w zapisach gwarancyjnych płatnych certyfikatów?**

Przede wszystkim wystawcy certyfikatów SSL jak ognia unikają słowa „do”. To że gwarancja wynosi „do 50.000 dolarów”, nie oznacza oczywiście, że właśnie taka suma zostanie wypłacona klientowi w razie włamania. W rzeczywistości będzie to znacznie mniej – np. 1000 dolarów, i to tylko w momencie, gdy klient udowodni, że wina leży po stronie certyfikatu.

Źródło: <https://zenbox.pl/pomoc/artikul/certyfikaty-ssl-w-zenbox/> ; <https://soluma.pl/blog-hosting,ac168/gwarancja-finansowa-od-wystawcy-certyfikatu-ssl-co-warto-o-niej-wiedziec,126410>

# SSL – czym jest i jakie są jego rodzaje?

---



Rodzaje certyfikatów możemy podzielić na 2 grupy w zależności od sposobu ich walidacji oraz samego typu certyfikatu.

Rodzaje certyfikatów względem sposobu ich weryfikacji:

1. **Certyfikaty DV (Domain Validation)** – certyfikat wystawiany jest na podstawie automatycznej weryfikacji prawa podmiotu do posługiwania się domeną. Zapewnia jedynie szyfrowanie, bez konieczności potwierdzenia tożsamości właściciela certyfikatu. Czas potrzebny na wystawienie certyfikatu to nawet kilka minut
2. **Certyfikaty OV (Organization Validation)** – certyfikat do wystawienia prócz podstawowej weryfikacji prawa do domeny, przeprowadzana jest weryfikacja podmiotu na podstawie przesłanych dokumentów. Wydanie certyfikatu trwa od 3 do 5 dni.
3. **Certyfikaty EV (Extended Validation)** – certyfikat najwyższego poziomu bezpieczeństwa. W celu jego wydania przeprowadzana jest szczegółowa weryfikacja podmiotu. Wydanie certyfikatu może potrwać od 7 do 14 dni.

Rodzaje certyfikatów według ich typów:

1. **Standard SSL** – standardowy certyfikat, obejmujący pojedynczą domenę zenbox.pl oraz jej subdomenę www.zenbox.pl
2. **Wildcard SSL** – certyfikat obejmujący ochroną domenę główną oraz wszystkie subdomeny się w niej znajdujące.
3. **Multi-Domain / SAN SSL** – certyfikat chroniący nawet do 210 domen wraz z ich subdomenami.
4. **Free SSL** – darmowe certyfikaty SSL. Najpopularniejszym certyfikatem jest certyfikat Let's Encrypt.

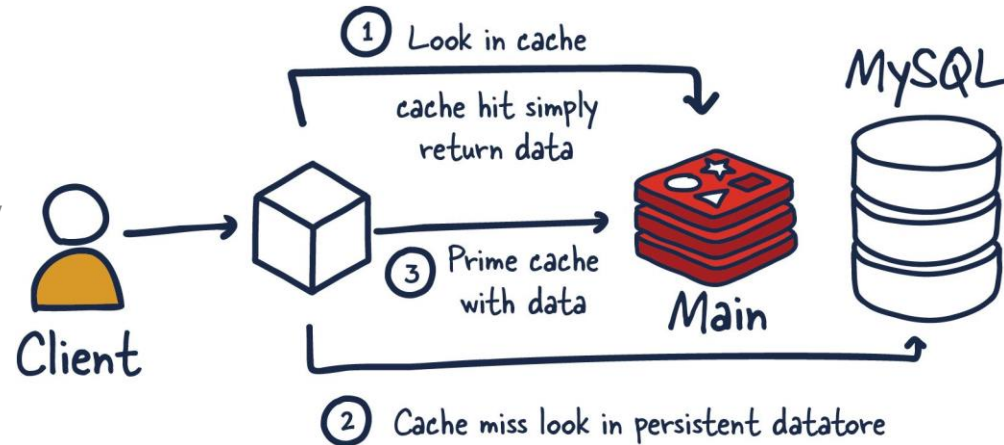
Źródło: <https://zenbox.pl/pomoc/artikul/certyfikaty-ssl-w-zenbox/>

# Czym jest REDIS i jak działa?



- REDIS jest bazą danych typu klucz – wartość, która przechowuje dane w pamięci RAM co czyni ją ekstremalnie wydajną. Jednak za wydajnością stoi ulotność danych, co w pewnych przypadkach jest niedopuszczalne. REDIS umożliwia nam w takim przypadku skonfigurowanie bazy w ten sposób żeby co pewien czas zrzuciła dane do pliku na dysku. Ma to oczywiście pewne konsekwencje, a w tym przypadku będzie to zmniejszenie wydajności.
- Object cache w WordPressie zaimplementowany jest za pomocą klasy WP Object Cache. Polega na cache'owaniu wyników zapytań SQL do bazy danych. Eliminuje to konieczność częstego łączenia się z bazą i pozwala na szybszy dostęp do danych.

## How is redis traditionally used



Źródło: <https://cyberfolks.pl/blog/redis-object-cache-w-wordpressie/> ;  
<https://czterytygodnie.pl/redis/wprowadzenie-do-redis-a.html> ; <https://architecturenotes.co/redis/>

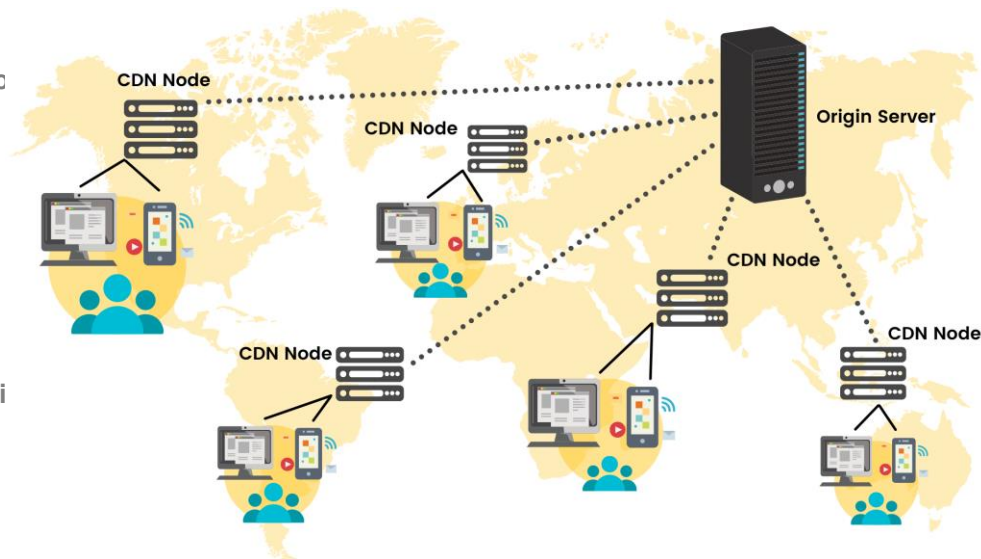
# Czym jest Content Delivery Network (CDN)?



Sieć dostarczania zawartości (ang. content delivery network, CDN) – rozproszona sieć serwerów, które pozwalają wydajnie dostarczać użytkownikom zawartość internetową. System dostarczania treści do wielu centrów danych i punktów wymiany ruchu (IX) w Internecie. Celem CDN jest wydajne udostępnianie zawartości o wysokiej dostępności końcowym użytkownikom.

Sieć składa się z:

- serwera źródłowego, który dostarcza treści do CDN,
- elementów znajdujących się w różnych częściach infrastruktury internetowej, gdzie treści są replikowane,
- systemu routingu, który zapewnia dostarczenie treści do użytkowników z najbliższego geograficznie węzła.
- Poszczególne węzły CDN są zwykle podłączone do szybkiej sieci szkieletowej Internetu. Ich liczba zmienia się w zależności od wybranej architektury i może wynosić nawet kilka tysięcy węzłów z dziesiątkami tysięcy serwerów. Optymalizacja z użyciem CDN przynosi zazwyczaj niższe koszty za usługi hostingowe. W związku z tym, że obsługę części ruchu przyjmują na siebie serwery CDN, zmniejsza się obciążenie serwera źródłowego i zapotrzebowanie na transfer. CDN przyspiesza ładowanie treści na stronach WWW dzięki płynnemu wczytywaniu obrazków, skryptów i innych dokumentów statycznych. Usługa zwiększa odporność na przejściowe zwiększenie natężenia ruchu na obsługiwanej stronie.



Źródło:  
[https://pl.wikipedia.org/wiki/Sie%C4%87\\_dostarczania\\_zawarto%C5%9Bci](https://pl.wikipedia.org/wiki/Sie%C4%87_dostarczania_zawarto%C5%9Bci) ; <https://nexnetsolutions.com/solutions/telecom-service-provider/content-delivery-network-cdn/>

# Panel Wordpress – strony i wpisy – schemat strony

---



Przemysłny teraz strukturę Państwa stron na zaliczenie przedmiotu, zbudujemy mapę strony z podziałem na strony i wpisy w Wordpress.

- **Wpisy (posty) WordPress** są przeznaczone na aktualne posty na blogu i mają datę publikacji, traktowane są jako treści aktualne o ograniczonej „dacie ważności”. Wpisy są głównym narzędziem tworzącym bloga internetowego, dzienniki, witryny z newsami. Znajdą zastosowanie wszędzie tam, gdzie kluczowa jest data publikacji treści. Wpisy są przeznaczone dla treści dynamicznych, a więc stale zmieniających się w czasie,
- **Strony WordPress** są przeznaczone do ponadczasowej zawartości statycznej i nie mają daty publikacji, nie mają też autora. Używane są do publikowania treści, która zwykle pozostaje niezmienną w czasie a jej aktualizacja nie ma większego wpływu na działanie witryny i jej pozycjonowanie. Strony używane są do publikacji informacji o firmie, oferty, stron kontaktowych i formularzy, galerii zdjęć.

Źródło: <https://pomoc.home.pl/baza-wiedzy/czym-roznia-sie-strony-od-wpisow-wordpress>

Materiał wideo na temat wpisów i stron w Wordpress: <https://www.youtube.com/watch?v=ZhdRIX8mdeo>



---

**Dziękuję za uwagę**

---

inż. Adam Balcerzak

**[WWW.WDIB.UW.EDU.PL](http://WWW.WDIB.UW.EDU.PL)**

[adam.balcerzak@uw.edu.pl](mailto:adam.balcerzak@uw.edu.pl)

---