

Operační systémy

Aplikační protokoly

Protokol	Účel	Typické porty	Poznámka
HTTP (Hypertext Transfer Protocol)	Přenos webových stránek (nezabezpečený)	80	Používaný v klasickém webovém prohlížení
HTTPS (HTTP Secure)	Zabezpečený přenos webových stránek	443	HTTP přes TLS/SSL
FTP (File Transfer Protocol)	Přenos souborů	20 (data), 21 (řízení)	Nezabezpečený, nahrazován SFTP/FTPS
SFTP (SSH File Transfer Protocol)	Zabezpečený přenos souborů přes SSH	22	Často zaměňován s FTPS
FTPS (FTP Secure)	Šifrované FTP přes TLS/SSL	990 (implicitní)	
SMB (Server Message Block)	Sdílení souborů, tiskáren	445	Hlavně Windows, Samba pro Linux
NFS (Network File System)	Sdílení souborových systémů	2049	Hlavně Unix/Linux
WebDAV (Web Distributed Authoring and Versioning)	Sdílení a správa souborů přes HTTP	80 (HTTP), 443 (HTTPS)	Rozšíření HTTP
rsync (protokol rsync přes SSH)	Synchronizace a kopírování souborů	873 (rsync daemon)	Přes SSH bezpečné
iSCSI (Internet Small Computer Systems Interface)	Připojení vzdálených disků	3260	Na úrovni blokového zařízení
SMTP (Simple Mail Transfer Protocol)	Odesílání e-mailů	25 (nezabezpečený), 587 (s autentizací)	
POP3 (Post Office Protocol v3)	Stahování e-mailů na klienta	110	POP3S (šifrování) běží na 995

IMAP (Internet Message Access Protocol)	Správa a synchronizace e-mailů	143	IMAPS (šifrování) běží na 993
DNS (Domain Name System)	Překlad domén na IP adresy	53	Používá UDP i TCP
Telnet	Vzdálený přístup na zařízení (nezabezpečený)	23	Dnes nahrazen SSH
SSH (Secure Shell)	Zabezpečený vzdálený přístup	22	
DHCP (Dynamic Host Configuration Protocol)	Přidělování IP adres klientům	67 (server), 68 (klient)	UDP
SNMP (Simple Network Management Protocol)	Správa zařízení v síti	161 (dotazy), 162 (trapy)	
NTP (Network Time Protocol)	Synchronizace času v síti	123	UDP
RDP (Remote Desktop Protocol)	Vzdálená plocha Windows	3389	
LDAP (Lightweight Directory Access Protocol)	Přístup ke katalogovým službám (adresáře)	389	LDAPS (zabezpečený) běží na 636
MQTT (Message Queuing Telemetry Transport)	Lehký protokol pro IoT komunikaci	1883 (nezabezpečený), 8883 (šifrovaný)	
CoAP (Constrained Application Protocol)	Protokol pro IoT zařízení (malá a úsporná komunikace)	5683	UDP

Pozn.: SFTP a FTPS

Vlastnost	SFTP	FTPS
Plný název	SSH File Transfer Protocol	FTP Secure (FTP přes SSL/TLS)
Bezpečnostní vrstva	Šifrování pomocí SSH	Šifrování pomocí SSL/TLS
Používaný port	TCP 22	TCP 990 (implicitní režim), TCP 21 (explicitní režim)
Architektura	Jednoduché spojení přes jedno připojení (command + data přes stejný kanál)	Oddělené kanály pro příkazy (control) a data (data)
Autentizace	Uživatelské jméno a heslo nebo SSH klíče	Uživatelské jméno a heslo, případně certifikáty
Firewall konfigurace	Snadnější (1 port)	Složitější (potřeba otevřít více portů pro data)
Kompatibilita	Vhodné pro Unix/Linux servery	Lépe podporováno v systémech Windows (např. IIS)
Protokolová základna	SSH protokol	FTP protokol rozšířený o TLS/SSL

Pozn.: Pasivní a aktivní režim FTPS

Vlastnost	Pasivní režim (PASV)	Aktivní režim (PORT)
Navázání datového spojení	Klient se připojuje na port serveru	Server se připojuje na port klienta
Role klienta	Klient otevírá nové spojení k serveru	Klient naslouchá na určitém portu a čeká na připojení serveru
Firewall a NAT	Vhodnější (klient iniciuje všechny spojení)	Problémové (klient musí otevřít port pro server)
Používané porty	Server otevře náhodný port (např. 50000–51000) a oznámí klientovi	Klient určí port, který otevře pro příchozí spojení
Kompatibilita	Lepší za NAT/firewallem (domácí sítě, internet)	Lepší v jednodušších sítích (bez NAT, firewally s výjimkami)
Bezpečnostní rizika	Mírná (otevřený port na serveru)	Větší (klient musí povolit příchozí spojení)
Standardní porty	Control connection: TCP 21 + dynamické porty pro data	Control connection: TCP 21 + klientský port pro data

✓ **Pasivní režim** se dnes používá **téměř všude** — hlavně proto, že:

- Klient **nepotřebuje otevřený port z internetu**.
- Firewall konfigurace je **jednodušší** (pouze příchozí spojení na server).

✗ **Aktivní režim** je starší metoda, dnes se používá **výjimečně**, typicky v **interních sítích** bez NAT/firewallu. ..

Pozn.: Explicitní a implicitní FTPS

✓ **Explicitní FTPS**: běžné FTP na portu 21 + příkaz `AUTH TLS`, **běžnější dnes**.

✓ **Implicitní FTPS**: komunikace **okamžitě šifrovaná** na portu 990, **starší a méně používaný režim**.

Pozn.: přehled protokolů sdílení

- **Windows** tradičně používá **SMB**.
- **Linux/Unix** typicky používá **NFS** nebo **SSHFS**.
- **MacOS** používalo **AFP**, dnes se ale také preferuje **SMB**.
- **WebDAV** je fajn univerzální metoda (funguje přes HTTP/HTTPS).
- **rsync** je hlavně na efektivní **kopírování** a **zálohování** (ne klasické připojení jako disk).