SSH (Secure Shell)

SSH je síťový protokol, který umožňuje bezpečné a šifrované spojení mezi dvěma počítači v nezabezpečené síti. V naší **digitální architektuře** je to primární nástroj pro administraci **VPS** serverů, správu síťových prvků a bezpečný přenos dat.

SSH pracuje na architektuře klient-server a standardně využívá port **22**. Na rozdíl od protokolu **TELNET** jsou veškerá data (včetně hesel) šifrována, což znemožňuje jejich odposlech v rámci **WAN**.

Klíčové funkce SSH

1. Vzdálený přístup (Terminal)

Umožňuje uživateli získat textové rozhraní (**TTY**) vzdáleného stroje. To je nezbytné pro správu operačních systémů **Linux**, které běží v našem **VPC**.

2. Bezpečný přenos souborů

Protokoly jako **SFTP** (SSH File Transfer Protocol) a **SCP** (Secure Copy) využívají SSH tunel k bezpečnému kopírování dat. Jde o bezpečnou alternativu k protokolům **TFTP** nebo FTP.

3. SSH Tunelování (Port Forwarding)

Umožňuje „zabalit“ nešifrovaný provoz jiné aplikace do šifrovaného SSH spojení. Tímto způsobem lze například bezpečně přistupovat k interní databázi přes veřejný internet.

Autentizace v naší síti

V rámci **kybernetické bezpečnosti** využíváme dva hlavní způsoby přihlášení:

- **Heslo:** Základní metoda, vyžaduje silná hesla splňující firemní politiku.
- **SSH klíče (Doporučeno):** Využívá asymetrickou kryptografii (veřejný a soukromý klíč). Je mnohem bezpečnější a umožňuje automatizaci bez nutnosti zadávat heslo. Soukromé klíče doporučujeme ukládat v hardware typu **TPM**.

Bezpečnostní pravidla (Best Practices)

Naše **IT Podpora** vynucuje tato nastavení pro všechny servery v **ZIF**:

- **Zákaz root přihlášení:** Je zakázáno přihlašovat se přímo pod účtem `root`. Uživatel se musí přihlásit pod svým **UID** a následně použít příkaz `sudo`.

- **Změna portu:** U veřejně dostupných serverů často měníme port z 22 na náhodně zvolené číslo, aby se omezily útoky automatických botů.
- **Fail2Ban:** Naše brány **UTM** automaticky blokují IP adresy, které se opakovaně pokoušejí o neúspěšné přihlášení.

Srovnání: SSH vs. SSL/TLS

Vlastnost	SSH	TLS (HTTPS)
Vrstva	Aplikační	Transportní
Použití	Vzdálená správa, terminál	Webové stránky, e-mail
Identita	Často klíče/hesla	Digitální certifikáty
Příklad	Přístup k **VPS** konzoli	Přihlášení do systému **Jira**

> **Tip pro vývojáře:** Při generování nových klíčů používejte algoritmus **Ed25519**, který nabízí nejlepší poměr mezi rychlostí a bezpečností v rámci našich moderních **IoT zařízení**.

— **Související stránky:** ZIF, TELNET, VPS, Tux, VPC, WAN, TTY, TFTP, Kybernetická bezpečnost, TPM, UID, UTM, TLS, Jira