Doména za VPN

Hodně firem používá pro lokální služby například jen hostname (například `jira`) nebo domény typu `.local`, `.corp` nebo `.sl`. Použití těchto domén (nebo hostname) s sebou nese hodně nevýhod.

Hlavní nevýhoda je, že na ně nejde vystavit validní certifikát (například od Let's Encrypt). Musíte mít vlastní autoritu a tu přidat do všech klientských PC a to jak do browseru, tak na servery. Za mě je to hrozně nepraktický způsob, jak se zbavit vlastní autority.

Pokud tedy chci certifikáty od Let's Encrypt, musím mít validní doménu. Já v SikaLabs používám doménu `sl.zone`. Je dostatečně krátká, jasně, není to `.sl`, ale pořád dostatečně krátká. Nových domén je spousta, určitě si nějakou najdete. I když by to bylo třeba `.wtf`, proč ne.

Pokud nechci používat žádnou další doménu, můžu například použít `i.sikalabs.com` nebo `int.sikalabs.com`, kde **i** a **int** znamená internal.

Na tuto doménu můžeme jednoduše vystavit certifikát, který bude validní všude, bez nutnosti vlastní certifikační autority.

Pokud je naše infrastruktura za VPN a není na ni přístup z internetu, nemůžeme využít HTTP challenge od Let's Encrypt. Respektive můžeme, ale není to moc praktické.

Místo toho můžeme použít DNS challenge. V public DNS nastavíme validační TXT záznam, proti kterému Let's Encrypt ověří, že doména je naše. Pokud máme DNS u dobrého poskytovatele (více v kapitole DNS), tak s tím není problém. Většina Let's Encrypt klientů má podporu Cloudflare, AWS a mnoho dalšího.

Pokud z nějakého důvodu nechceme používat DNS challenge, tak můžeme použít i HTTP challenge, ale je to trochu složitější. Musíme mít 2 oddělené DNS servery, jeden v interní síti za VPN a druhý veřejný, které budou mít rozdílné záznamy. Potom ten veřejný nesměřujeme na nějaký server, který bude ověřovat certifikáty a distribuovat do vnitřní sítě. DNS ve vnitřní síti bude ukazovat záznamy na konkrétní servery.

Nevýhodou je, že pokud klienti mají nastavené vlastní DNS servery (já například používám 1.1.1.1, což je veřejné DNS od Cloudflare), mají s rozdílnými DNS problém. Proto radši používám DNS challend a mám své interní záznamy na veřejném DNS.

Chápu, že mít interní záznamy na veřejném DNS serveru může být potencionální leak informací o infrastruktuře, ale nevidím to jako zásadní problém. Každopádně pořád můžu mít 2 dns servery: veřejný jen pro TXT ověřovací záznamy a interní, kde budu mít všechny záznamy.