IKEv2 (Internet Key Exchange version 2)

IKEv2 je síťový protokol patřící do rodiny **IPsec**, který slouží k bezpečnému ustanovení a správě šifrovaného spojení (Security Association - SA) mezi dvěma body. Byl vyvinut společnostmi Microsoft a Cisco jako nástupce staršího IKEv1.

Jeho hlavním úkolem je autentizace obou stran a bezpečné dohodnutí šifrovacích klíčů, které pak následně používá protokol ESP (Encapsulating Security Payload) pro samotný přenos dat.

Klíčové vlastnosti IKEv2

* **MOBIKE (Mobility and Multihoming):** Nejsilnější stránka IKEv2. Umožňuje uživateli změnit IP adresu (např. při přechodu z Wi-Fi na mobilní data), aniž by došlo k rozpadu VPN spojení. * **Odolnost proti DoS útokům:** Obsahuje mechanismus „cookies“, který nutí odesílatele potvrdit svou identitu dříve, než server začne provádět náročné kryptografické operace. * **Nízká latence:** K navázání spojení vyžaduje mnohem méně výměn zpráv (round-trips) než IKEv1, což zrychluje připojování. * **Nativní podpora NAT Traversal:** Automaticky detekuje přítomnost NAT a provádí zapouzdření do UDP portu 4500.

Průběh navazování spojení

Komunikace IKEv2 probíhá v několika fázích výměny zpráv:

```
1. **IKE_SA_INIT:** Dohodnutí kryptografických algoritmů (šifry, hashe) a výměna Diffie-Hellman veřejných hodnot pro vytvoření společného klíče.
2. **IKE_AUTH:** Autentizace stran (pomocí certifikátů nebo PSK) a vytvoření prvního tunelu pro data (Child SA).
```

Srovnání IKEv2 vs. IKEv1

Vlastnost	IKEv1	IKEv2
Rychlost	Pomalé (vícenásobné výměny)	Velmi rychlé (2 základní výměny)
Mobilita	Nepodporuje (tunel spadne)	Podporuje (MOBIKE)
Spotřeba dat	Vyšší režie	Nižší režie (vhodné pro mobily)
Spolehlivost	Časté problémy s „mrtvými“ tunely	Vestavěný mechanismus Liveness Check

Bezpečnostní aspekty

IKEv2 podporuje moderní šifrovací algoritmy jako **AES-GCM**, které jsou efektivnější na moderních procesorech. Pro autentizaci lze využít:

- **Pre-Shared Key (PSK):** Sdílené heslo (méně bezpečné pro velké sítě).
- **Certifikáty (RSA/ECDSA):** Digitální podpisy (vysoká bezpečnost).

- **EAP (Extensible Authentication Protocol):** Umožňuje autentizaci uživatelským jménem a heslem (vhodné pro vzdálený přístup zaměstnanců).

> **Tip pro praxi:** IKEv2 je standardním protokolem pro Windows, macOS a iOS „nativní“ VPN klienty. Často je preferován před OpenVPN díky lepší integraci v systému a nižší spotřebě baterie na mobilních zařízeních.

— **Viz také:** IPsec, VPN, MTU