IPsec (Internet Protocol Security)

IPsec je sada protokolů pro zabezpečení komunikace na **síťové vrstvě (L3)** modelu OSI. Na rozdíl od SSL/TLS (které chrání konkrétní aplikace jako webový prohlížeč), IPsec šifruje veškerý provoz mezi dvěma body bez ohledu na to, o jakou aplikaci se jedná.

Umožňuje autentizaci, kontrolu integrity dat a důvěrnost (šifrování) IP paketů.

Základní protokoly IPsec

IPsec se skládá ze tří hlavních protokolů, které spolupracují:

- **AH (Authentication Header):** Zajišťuje integritu a autentizaci. **Nešifruje data.** Dnes se používá zřídka, protože ESP umí totéž a lépe.
- **ESP (Encapsulating Security Payload):** Zajišťuje šifrování, autentizaci i integritu. Je to hlavní protokol používaný pro moderní VPN.
- **IKE/IKEv2 (Internet Key Exchange):** Protokol pro správu klíčů. Domlouvá šifry a parametry spojení dříve, než se začnou posílat data přes ESP.

Operační režimy

IPsec může pracovat ve dvou základních režimech, které určují, jak moc je původní paket změněn:

1. Transportní režim (Transport Mode)

Šifruje se pouze **payload** (obsah) IP paketu, ale původní IP hlavička zůstává viditelná.

- **Použití:** Komunikace „End-to-End“ (např. mezi dvěma servery).
- **Výhoda:** Menší režie (paket se nezvětšuje o novou hlavičku).

2. Tunelový režim (Tunnel Mode)

Šifruje se **celý původní IP paket** (včetně hlavičky) a ten se vloží do úplně nového IP paketu.

- **Použití:** Site-to-Site VPN (propojení poboček) nebo Remote Access VPN.
- **Výhoda:** Skrývá identitu koncových zařízení v rámci tunelu.

Architektura Security Association (SA)

Klíčovým konceptem IPsec je **SA**. Je to v podstatě „smlouva“ mezi dvěma uzly o tom, jaké šifry a klíče budou používat. * SA je **jednosměrná**. Pro obousměrnou komunikaci (duplex) jsou potřeba dvě SA. * Každá SA je identifikována pomocí **SPI** (Security Parameter Index), což je číslo v hlavičce paketu, díky

kterému příjemce pozná, jaký klíč má použít k dešifrování.

Výhody a nevýhody

Výhody	Nevýhody
Transparentnost pro aplikace (nemusí se měnit).	Vysoká režie na procesor (při šifrování).
Vysoká bezpečnost (šifrování na úrovni jádra OS).	Problémy s průchodem přes NAT (vyžaduje UDP zapouzdření).
Standardizované řešení napříč výrobci.	Komplexní konfigurace ve srovnání s TLS VPN.

> **IPsec a NAT:** Protože IPsec (zejména AH) hlídá integritu celého paketu, jakákoliv změna IP adresy nebo portu (NAT) by paket zneplatnila. Proto se používá **NAT-Traversal (NAT-T)**, který IPsec pakety balí do standardních UDP portů (obvykle 4500).

— **Viz také:** IKEv2, VPN, Šifrování

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=ipsec

Last update: **2026/01/06 17:44**