20. VPN a IPsec

**1. Účel a výhody použití VPN**

* **Účel VPN:**

VPN slouží k vytvoření bezpečného, šifrovaného tunelu mezi zařízeními nebo sítěmi přes veřejnou síť (internet). Umožňuje vzdáleným uživatelům nebo pobočkám bezpečně přistupovat k interním zdrojům organizace, jako by byla fyzicky připojena k privátní síti.

* **Výhody použití VPN:**
  + **Zabezpečení:** Data jsou šifrována, což zajišťuje ochranu proti odposlechu a neoprávněnému přístupu.
  + **Důvěrnost a integrita:** Zajišťuje, že data nejsou modifikována během přenosu.
  + **Flexibilita a mobilita:** Uživatelé mohou bezpečně pracovat z jakéhokoli místa, což podporuje telepráci a vzdálený přístup.
  + **Snížení nákladů:** VPN **eliminuje** potřebu **drahých privátních spojů**, protože využívá veřejnou infrastrukturu.
  + **Anonymita a ochrana soukromí:** Skrývá interní síťovou strukturu před vnějším světem, což pomáhá chránit před útoky.

**2. Typy VPN**

VPN lze rozdělit podle způsobu připojení, architektury a způsobu implementace. Mezi hlavní typy patří:

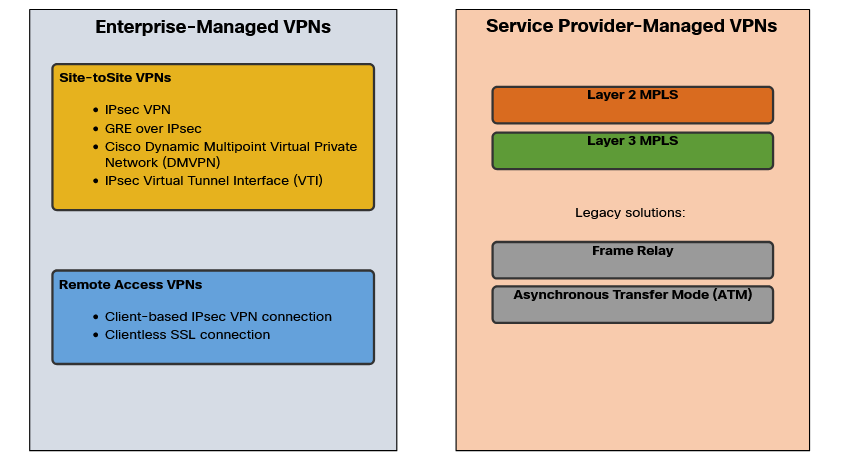
**A. Client-based VPN**

* **Definice:** Vyžaduje instalaci specializovaného VPN klienta na zařízení uživatele (notebo software integrovaný v operačním systému).
* **Příklady použití:** Uživatelé pracující na notebooku či mobilním zařízení se připojují k firemní síti prostřednictvím nainstalovaného VPN klienta, který zajišťuje šifrovaný tunel.

**B. Clientless VPN**

* **Definice:** Nepotřebuje speciální software – přístup je zajištěn prostřednictvím webového prohlížeče.
* **Příklady použití:** Poskytuje vzdálený přístup k webovým aplikacím a intranetovým službám pomocí HTTPS. Vhodné pro příležitostné či rychlé přístupy, kde není nutná plná VPN konfigurace.

**C. Enterprise VPN vs. Service Provider VPN**



* **Enterprise VPN:**
  + **Definice:** VPN řešení implementovaná a spravovaná přímo uvnitř organizace (např. pro propojení poboček, vzdálený přístup zaměstnanců).
  + **Charakteristiky:**
    - Řídí ji interní IT oddělení.
    - Často využívá technologie jako IPsec, SSL VPN nebo kombinaci obou.
    - Zaměřeno na specifické bezpečnostní politiky a integraci s interní infrastrukturou (Active Directory, firemní servery).
* **Service Provider VPN:**
  + **Definice:** VPN služby poskytované telekomunikačními nebo internetovými poskytovateli zákazníkům.
  + **Charakteristiky:**
    - Poskytovatel VPN (např. MPLS VPN, SD-WAN řešení) zajišťuje bezpečné propojení mezi různými zákaznickými lokalitami.
    - Nabízí centralizovanou správu a často také SLA (Service Level Agreement) pro zajištění dostupnosti a kvality připojení.
    - Umožňuje firmám využívat VPN bez nutnosti rozsáhlé interní infrastruktury.

**D. Remote-Access VPN vs. Site-to-Site VPN**

* **Remote-Access VPN:**

Umožňuje jednotlivým uživatelům bezpečně se připojit ke vzdálené síti (**často využívá client-based nebo clientless přístup**).

* **Site-to-Site VPN:**

Propojuje dvě nebo více sítě (například pobočky firmy) pomocí tunelů, které se nastavují mezi **VPN gateway** zařízeními.

**E. Dynamic Multipoint VPN (DMVPN)**

Dynamic Multipoint VPN (DMVPN) je technologie vyvinutá společností Cisco, která umožňuje dynamické a škálovatelné VPN propojení mezi více lokalitami. DMVPN kombinuje IPsec pro zabezpečení s multipoint GRE (mGRE) a Next Hop Resolution Protocol (NHRP) pro dynamické vytváření tunelů.

**Klíčové vlastnosti DMVPN:**

* **Dynamická tunelace:**Umožňuje vytváření tunelů on-demand mezi pobočkami (spokes) bez nutnosti manuální konfigurace každého spojení. To snižuje administrativní zátěž.
* **Hub-and-Spoke a Full-Mesh topologie:**Standardně se používá v hub-and-spoke architektuře, kdy všechny pobočky komunikují přes centrální hub, ale umožňuje také dynamické přímé spojení mezi pobočkami, když to je potřeba.
* **Integrace s IPsec:**DMVPN využívá IPsec k zabezpečení dat přenášených přes mGRE tunely, což poskytuje šifrování, autentizaci a integritu dat.
* **Next Hop Resolution Protocol (NHRP):**Umožňuje pobočkám (spokes) dynamicky zjistit veřejné IP adresy ostatních poboček, což umožňuje přímou komunikaci bez průchodu centrálním hubem, čímž se zvyšuje efektivita a snižuje latence.
* **Škálovatelnost:**Díky dynamické konfiguraci a schopnosti vytvářet přímé tunely umožňuje DMVPN snadné rozšiřování VPN sítě, aniž by bylo nutné předem definovat statické spojení mezi každou dvojicí lokalit.

**3. Generic Routing Encapsulation (GRE)**

* **Definice a účel:**
  + GRE (Generic Routing Encapsulation) je tunelovací protokol, který umožňuje zapouzdření (encapsulaci) různých síťových protokolů do jediného tunelovaného rámce přes IP síť.
  + Slouží k vytvoření virtuálních spojení mezi zařízeními, kdy se původní paket vloží do nového IP paketu s GRE hlavičkou, čímž je možné přenášet i ne-IP protokoly.
* **Funkce a vlastnosti:**
  + **Zapouzdření:** GRE umožňuje, aby se data z libovolného protokolu (například IPv4 nebo IPv6) přenášela uvnitř jiného IP paketu.
  + **Tunelování:** Vytváří logické spojení (tunel) mezi dvěma zařízeními, což umožňuje propojení vzdálených sítí, aniž by byla nutná fyzická přímá cesta.
  + **Stateless:** GRE neudržuje stav spojení a sám o sobě nepřidává mechanismy pro zabezpečení, šifrování nebo autentizaci – tyto funkce musí být doplněny například o IPsec.
* **Použití v kombinaci s IPsec a DMVPN:**
  + GRE se často používá v kombinaci s IPsec (např. v DMVPN řešeních), kde GRE tunely poskytují flexibilitu a dynamické vytváření spojení mezi lokalitami, zatímco IPsec zajišťuje šifrování a bezpečnost dat.
  + Umožňuje vytvářet multipoint tunely, které mohou podporovat dynamické směrování a přímou komunikaci mezi pobočkami bez nutnosti fixního tunelování přes centrální hub.
* **Výhody a omezení:**
  + **Výhody:**
    - Flexibilita: Umožňuje zapouzdření různých typů síťových protokolů.
    - Kompatibilita: Funguje na standardním IP a je podporován většinou routerů a VPN řešení.
    - Dynamické tunelování: Umožňuje vytváření a rušení tunelů podle aktuálních potřeb sítě.
  + **Omezení:**
    - Nedostatek bezpečnostních funkcí: GRE sám o sobě neprovádí šifrování ani autentizaci, proto je třeba jej kombinovat s dalšími bezpečnostními protokoly, jako je IPsec.
    - Režie: Přidání GRE tunelu znamená další režii v podobě zvýšené velikosti paketů kvůli GRE hlavičce.

**4. Základní principy IPsec**

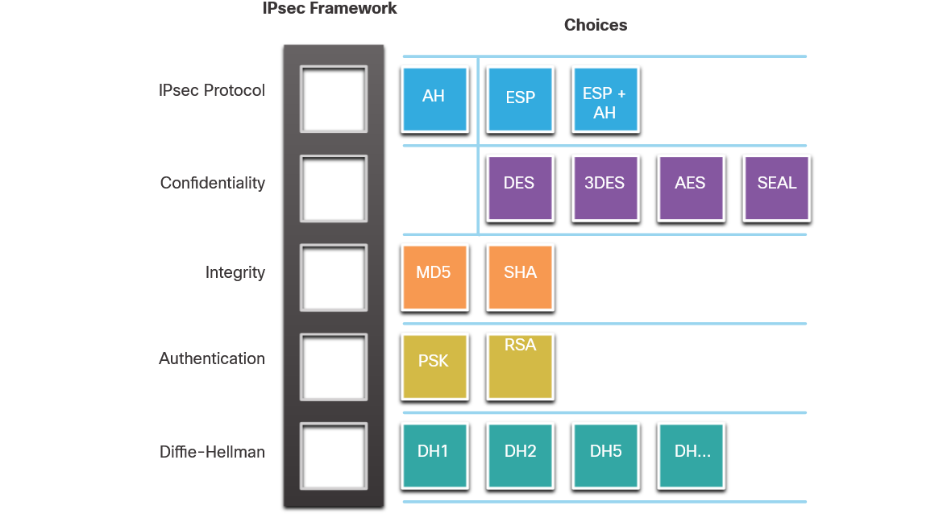
Zajišťuje bezpečnost na L4 až L7

IPsec má dva režimy: (pak dále ještě vysvětleno)

1. Transportní — Vloží bezpečnostní hlavičky mezi hlavičku IP a hlavičku protokolu transportní vrstvy
2. Tunelový — Celý IP paket vloží do dalšího IP paketu, za kterým následuje bezpečností hlavička

IPsec využívá L3 hlavičku a v kontrolních počtech započítává i adresu

* Proto při využití NAT, která narušuje end-to-end konektivitu, tak IPsec má problémy s ověřením autentizací dat (paket pochází z jiné IP, než byl zašifrován)



**IPsec protokoly:**

**A. Authentication Header (AH)**

* **Funkce AH:**
  + Zajišťuje autentizaci a integritu dat.
  + Každý paket opatří autentizační značkou, která ověřuje, že data nebyla během přenosu změněna.
* **Poznámka:** AH neprovádí šifrování, takže data zůstávají nešifrovaná. Jeho hlavní využití je v případech, kdy je prioritou ověření zdroje a integrity, nikoli důvěrnost.

**B. Encapsulating Security Payload (ESP)**

* **Funkce ESP:**
  + Poskytuje šifrování dat (důvěrnost) a také autentizaci a integritu.
  + Data jsou šifrována, což zabraňuje jejich čtení třetími stranami.
* **Výhoda ESP:** Kombinací šifrování a autentizace se ESP stal **nejpoužívanějším protokolem v IPsec implementacích.**

**C. Internet Key Exchange (IKE)**

* **Funkce IKE:**
  + IKE slouží k dynamické výměně klíčů mezi zařízeními, která komunikují pomocí IPsec.
  + Zajišťuje, že obě strany se dohodnou na bezpečnostních parametrech (šifrovacích algoritmech, autentizačních metodách, dobách platnosti klíčů) pro zabezpečení komunikace.
* **Verze IKE:**
  + IKEv1 a modernější IKEv2 – IKEv2 přináší zjednodušený proces a lepší podporu pro mobilitu a znovupřipojení.
* **Šifrování (Confidentiality):**

IPsec využívá šifrovací algoritmy (např. AES, 3DES) k ochraně dat před neoprávněným čtením. To znamená, že obsah IP paketů je zašifrován, takže i kdyby byl přenášen veřejnou sítí, útočník jej nebude schopen dešifrovat a přečíst.

* **Integrita (Integrity):**

Pro zajištění, že data nebyla během přenosu změněna, IPsec využívá hashovací algoritmy (např. SHA-1, SHA-256). Tyto algoritmy vytvářejí digitální otisk (hash) z obsahu paketu, což umožňuje příjemci ověřit, zda paket nebyl pozměněn.

* **Autentizace původu (Origin Authentication):**

IPsec využívá Internet Key Exchange (IKE) protokol pro **autentizaci zdroje a cíle komunikace** (potvrzení). Metody autentizace mohou zahrnovat:

* + **Předsdílené klíče (pre-shared keys):** Jednoduché heslo nebo sdílený tajný klíč.
  + **Digitální certifikáty:** Certifikáty vydané certifikační autoritou pro ověření identity.
  + **RSA certifikáty:** Použití veřejného a soukromého klíče podle standardu RSA pro zabezpečenou autentizaci.
  + (Za pomocí **PSK** a **RSA)**
* **Diffie-Hellman Key Exchange:**

IPsec využívá algoritmus Diffie-Hellman (DH) pro bezpečnou výměnu šifrovacích klíčů mezi komunikujícími stranami. Tento proces probíhá obvykle v rámci různých skupin DH, což umožňuje oběma stranám dynamicky a bezpečně dohodnout sdílený klíč bez předchozího sdílení tajných informací.

**5. Režimy IPsec**

IPsec může fungovat ve dvou hlavních režimech, které určují, jaká část IP paketu je chráněna:

**A. Transportní režim**

* **Charakteristika:**
  + Šifruje a autentizuje pouze datovou část IP paketu (tzv. payload), nikoliv samotný IP hlavičku.
* **Použití:**
  + Typicky se používá pro zabezpečení komunikace mezi dvěma koncovými zařízeními (např. mezi dvěma servery).
  + Transportní režim umožňuje zachovat původní IP adresaci, což je výhodné pro koncové aplikace.

**B. Tunelový režim**

* **Charakteristika:**
  + Celý IP paket (včetně hlavičky) je zabalen do nového IP paketu a následně šifrován a autentizován.
  + Původní IP paket se stává datovou částí nového paketu.
* **Použití:**
  + Vhodný pro site-to-site VPN, kdy se zabezpečuje komunikace mezi dvěma sítěmi.
  + Tunelový režim umožňuje maskovat původní adresaci a vytvářet bezpečné tunely mezi VPN bránami.

**6. Bezpečnostní asociace a databáze**

* **Security Association (SA):**
  + SA představuje dohodu mezi dvěma zařízeními o tom, jak budou chránit komunikaci.
  + Je definována parametry jako šifrovací algoritmus, autentizační klíče, typ protokolu (AH nebo ESP) a doba platnosti.
  + Každá SA je jednosměrná, takže pro obousměrnou komunikaci jsou potřeba dvě SA.
* **Databáze politik (SPD – Security Policy Database):**
  + Určuje, která komunikace (na základě IP adres, portů a protokolů) má být chráněna pomocí IPsec.
* **Databáze asociací (SAD – Security Association Database):**
  + Uchovává informace o aktivních SA, včetně parametrů, které byly dohodnuty mezi zařízeními.

**Shrnutí**

* **Účel a výhody VPN:**

VPN umožňují bezpečné, šifrované připojení přes veřejné sítě, čímž zajišťují ochranu dat, flexibilitu vzdáleného přístupu a úsporu nákladů na privátní spojení.

* **Typy VPN:**
  + **Client-based VPN** vyžaduje instalaci klientského softwaru, zatímco **clientless VPN** využívá webový prohlížeč.
  + **Enterprise VPN** je spravována interním IT oddělením a je integrována s firemní infrastrukturou, zatímco **service provider VPN** je poskytována externím dodavatelem a často využívá MPLS nebo SD-WAN technologie.
  + **Remote-access VPN** umožňuje individuálním uživatelům přístup do sítě, zatímco **site-to-site VPN** propojuje celé sítě (například pobočky firmy).
* **IPsec:**

Je klíčovou technologií pro zajištění bezpečnosti VPN. Poskytuje šifrování, autentizaci a integritu dat pomocí protokolů AH a ESP a využívá IKE pro správu klíčů.