Co je to IPsec

- Soubor protokolů pro zajištění bezpečnosti na síťové úrovni
    - Ověřování původu
    - Integrita dat
    - Utajení dat
- Vzhledem k transportním protokolům a aplikacím je transparentní – nevidí ho
- Vzhledem k linkovému protokolu neprůhledný – nerozumí přenášeným datům
- Přizpůsobivý

Režimy činnosti

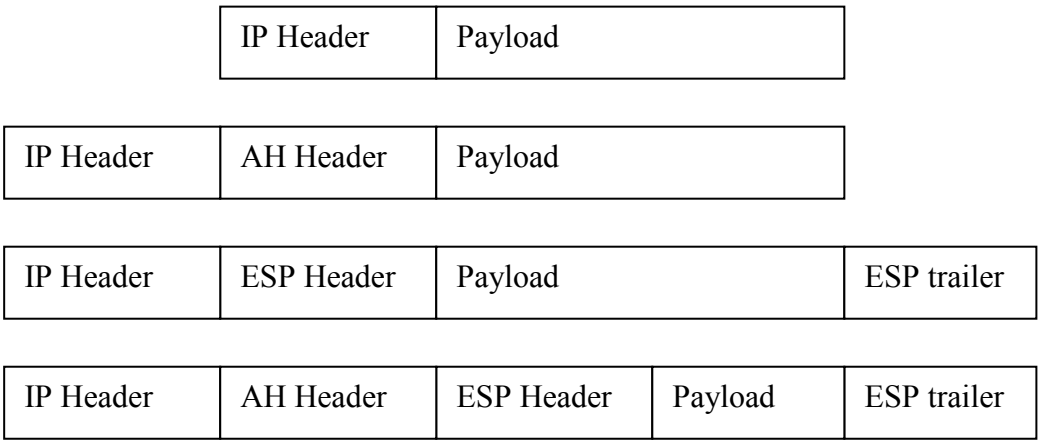
- Transparentní – mezi koncovými uživateli
- Tunelovaní – mezi dvěma síťovými prvky (směrovači, obrannými valy, …)
- Kombinace předcích – mezi koncovým uživatelem a síťovým prvkem

IPsec – vzdálený pohled

- Přenosové protokoly
    - Encapsulation Security Payload (ESP) – šifrování zpráv
    - Authentication Header (AH) – ověřování
- Ochrana
    - Přístupová práva
    - Konfigurace
- Správa klíčů
    - Manuální
    - Automatická (Photuris, IKE)

Přenosové protokoly

- Zapouzdření uživatelských dat s jejich šifrováním (Encapsulation Security Payload (ESP))
    - Důvěrnost (confidentality)
    - Integritu dat
    - Ověřování původu (Origin authentication) - implicitní
    - Ochrana proti „přehrávání“ (Replay protection)
- Ověřovací záhlaví (Authentication Header (AH))
    - Integrita dat
    - Ověřování původu (Origin authentication) - explicitní
    - Ochrana proti „přehrávání“ (Replay protection)
- Zapouzdření záhlaví

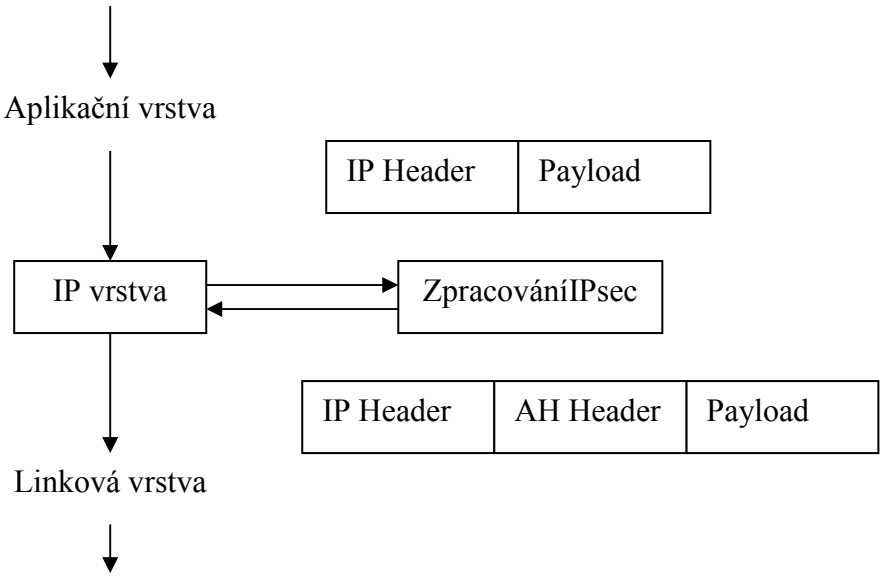


Formát rámců

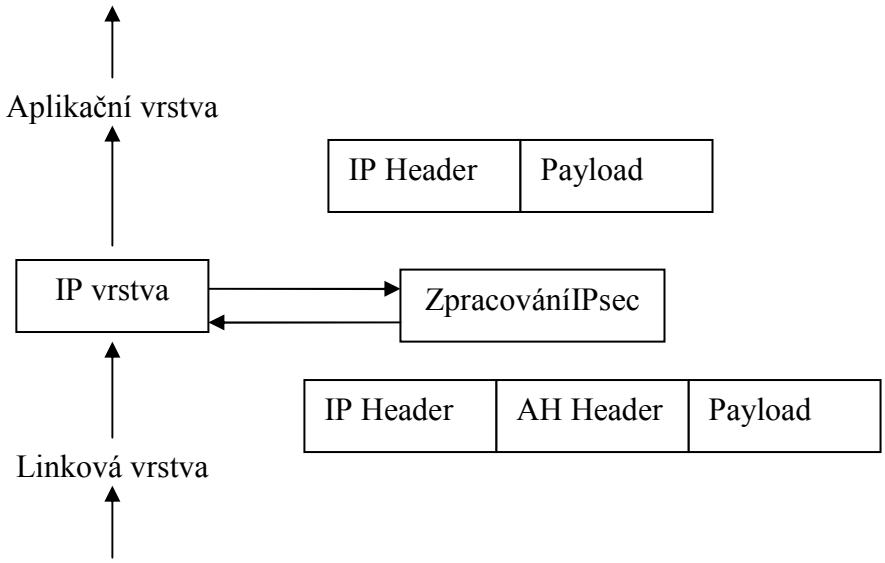
SA Security Association – bezpečné propojení

- SA – vztah mezi dvěma nebo více entitami, který popisuje, jak budou entity využívat bezpečnostní služby k bezpečné komunikaci
- SA je identifikován dvojicí bezpečnostní protokol, SPI
- SPI je Security Parameter Index – může být implementačně závislý na systému, protokolu, atd.
- Informace týkající se toku dat v IPsec
    - Kryptografické algoritmy
    - Klíče
- Security Policy Database (SPD)
    - Příchozí/odchozí politika
    - Co akceptovat, co odmítnout, zpracování IPsec

Odchozí zpracování



Příchozí zpracování



Správa klíčů

- Manuální/statická správa klíčů
  - Obtížná
  - Vyžaduje významný zásah člověka
  - Náchylný k chybné konfiguraci
  - Typicky slabé klíče
  - Špatně rozšiřitelný (škálovatelnost)
  - Otravný
- Správu klíčů je třeba automatizovat

Požadavky na správu klíčů

- Vyjednávání parametrů
- Silná bezpečnost
  - Ověřování, klíče
- Dynamická změna klíče
- Minimální konfigurace
- Nezávislost na algoritmu
- Ochrana identity
- Potřeba bezpečného forwardování
- Výkonnost
- Rozšiřitelnost

Dostupné prostředky

- Všeobecně dostupné šifrovací protokoly a systémy
    - Diffie-Hellman výměna klíčů,
    - RSA/DSA,
    - 3DES/AES,
    - MDA5, SHA1

- Struktura pro psaní bezpečnostních protokolů
    - Standardizovaná struktura uživatelských dat
    - Zavedeny typy výměny
    - Pravidla pro zpracování uživatelských dat
    - Přizpůsobivost
- Domain of interpretation concept

ISAKMP - přesně definuje procedury a formáty paketů pro vytvoření, dohadování, modifikaci a zrušení SA (Security Association). SA obsahuje všichny informace požadované pro vykonávání různých síťových bezpečnostních služeb, jako jsou služby IP vrstvy (ověřování záhlaví AH a zapouzdření dat ESP), služby transportní a aplikační vrstvy, nebo vlastní ochrana přenosu při dohadování. ISAKMP definuje data pro výměnu klíčů a ověřování dat. Tyto formáty poskytnou shodný základ pro přesun klíče a ověřování dat která jsou nezávislá na technice generován klíče, algoritmu šifrování a mechanizmu ověřování.
ISAKMP je odlišný od protokolů výměny klíčů protože jasně odděluje detaily ovládání SA (a správu klíčů) od detailů výměny klíčů. Může existovat mnoho různých protokolů pro výměnu klíčů, každý s různými bezpečnostními vlastnostmi. Avšak společný rámec je potřeba pro dohadování na formátu SA atributů, pro vyjednávání, modifikaci a rušení SA. ISAKMP slouží jako běžný základ.
ISAKMP může být implementovaný nad jakýmkoliv transportním protokolem.
Všechny implementace musí zahrnovat posílání a příjem kapabilit (schopností) pro ISAKMP prostřednictvím UDP/500.

Internet key exchange (IKE)

- Kombinace ISAKMP a Oakley
- Používá UDP/500
- Dvoufázový protokol
    - Vytvoření bezpečného kanálu
    - Ověřování účastníků
    - Výměna aplikačních parametrů
- Existují různé ověřovací mechanizmy
- Existují různé mechanizmy pro výměnu klíčů
    - Diffie-Hellman
    - Kerberos