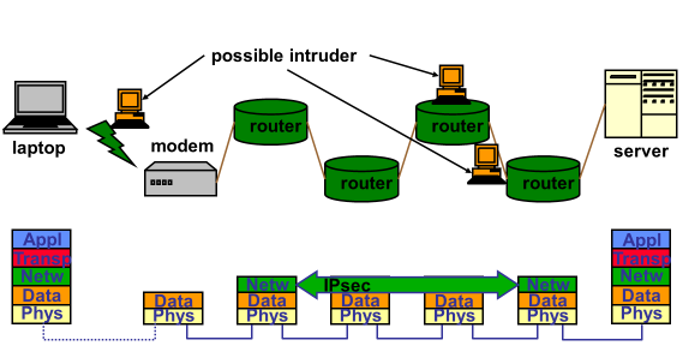
Netwerk laag: IPSec

(zoiets zal ie mss wel op examen vragen vo kruisjes te zetten)

Beveiliging tegen:

* Source spoofing
* Replay attacks
* Data integriteit/confidentialiteit
* Authenticeert routing berichtingen: advertisements, updates,...

# Types

## LAN to LAN

VPN:

* Doet alsof subnetwerken met elkaar verbonden zijn onder één LAN
* Veilige data overdracht over tussen tussenliggende publieke netwerken voor communicatie tussen de 2 private netwerken

## Client to LAN

* Noemen ze meestal ook VPN
* Voor veilige connectie te krijgen tot een bepaald netwerk over een onveilig tussenliggend netwerk

## Voordelen

* Applicatie onafhankelijk
* Beveiligingsmechanismen beperkt tot paar acces points: dus goede beveiliging voor alles wat daar doormoet en weinig intern verkeer
* Transparant eindgebruikers

## Nadelen

* Geen beveiliging na de veilige gateway
* Gebruikt veel systeemresources
* Complexiteit

# Modes

## Layer 2 tunnel mode

* Meestal voor IP verkeer tussen 2 gateways te verbinden
* Beveiligigd het hele diagram: ook de IP headers dus. En voegt dan zelf een nieuwe IP header toe voor routing
* Automatische NAT traversal

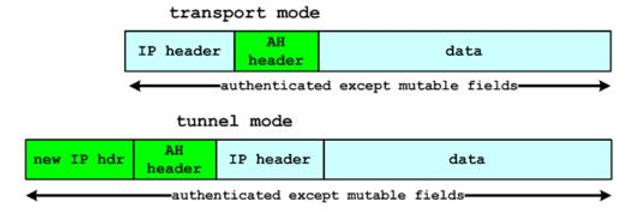
## Transport mode

* Enkel de payload is encrypted
* Beveiligingsmethode voor protocollen op de bovenste laag

# Protocollen (2)

Beide modes kunnen authenticatie, data integriteit, confidentialiteit geven door 1 of beide protocollen toe te passen

## Authentication header



* Authenticatie(gaat replay attacks en spoofing tegen) en dataintegriteit voor datagrammen
* Via one-way hash functie op datagram op basis van shared secret key om een MAC bericht digest te maken
* Wanneer de ontvanger de hash functie opnieuw toepast zal hij zien indien het was aangepast
* Tfeit da er die shared secret key is betkent dat er dus ook authenticatie is.
* Hash wordt toegepast op het hele datagram behalve op ip headers die constant veranderen zoals TTL

1. IP header en data wordt gehashed
2. Deze hash wordt gebruikt om de AH header te maken die aan de data wordt toegevoegd
3. Dit nieuw pakket wordt verstuurd naar de IPSec peer router
4. Deze zal van het ontvangen bericht dan terug een hash maken van de IP header en data.
5. Dan vergelijkt hij da me da hash da eraan toegevoegd was

## ESP Encapsulating Security Payload

* Confidentialiteit (data [+ IP Header] encrypted), data oorsprong authenticatie, integriteit, anti-replay, en beetje traffic flow confidentialiteit

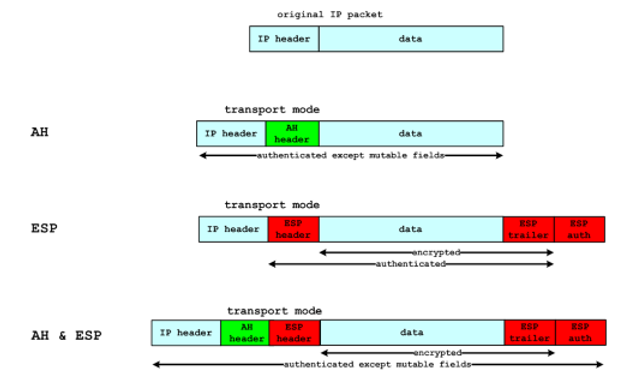
### Transport mode

* Van 1 apparaat naar een ander
* Encryptie/authenticatie
* Geen traffic flow confidentialiteit
* Bv. Voor teleworking

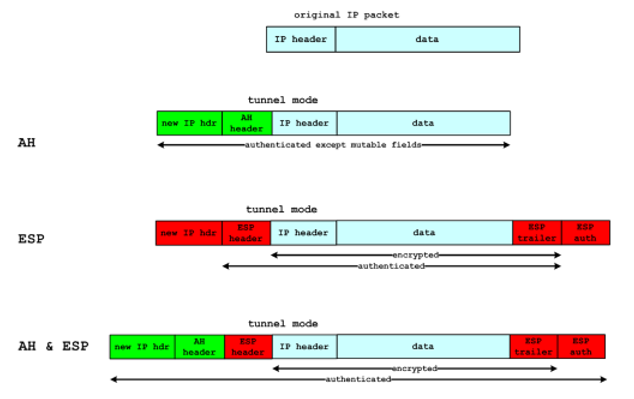
### Tunnel mode

* Encrypted tunnels met IP verkeer
* VPN tussen twee netwerken leggen. Niet elk apparaat tussen de verbinding moet dan IPSec ondersteunen, enkel een gateway verbonden aan het lokale netwerk

## Transport mode mogelijkheden



## Tunnel mode mogelijkheden



# Security associations

Tussend zender en ontvanger in één richting

Identificatie door:

* SPI security parameters index
* Ip doeladres
* Identificatie van het beveiligingsprotocol
* AH / ESP voor één IP stream

Combineren tunnels mogelijk

* Niet persee zelfde eindpunt
* Verschillende mogelijke levels
* Iterated tunnels

## Tussen twee eindgebruikers

* Transport AH
* Transport ESP
* AH gevolgd door ESP in Transport
* Één van de vorige in een AH/ESP in Tunnel mode

## Tussen twee gateways

* Één tunnel met AH / ESP / ESP+auth is genoeg

## Combo beide

* Data wordt geauthenticeerd/confidentialiteit tussen gateways + bijkomende beveiliging voor eindgebruiker voor verkeer binnen het intranet

## Teleworker

Van device rechstreeks over internet naar gateway van den andere via tunnel. Dan nog beveiliging over lokaal netwerk

Netwerklaag: VPN

* Veilige tunnel tussen 2 sites.
* Niet enkel voor remote log-in bedoeld

## Mogelijke VPN opties

### Ipsec

+ gemaakt hiervoor  
+ deel van andere oplossingen  
- complex  
- samenwerkingsproblemen tussen verschillende implementaties  
- problemen met NAT en non-IPSec firewalls

### PPTP (point to point tunneling protocol)

+ client beschikbaar bijna elk platform  
 + easy  
 + snel  
 - niet veilig  
 - NSA ziet alles

### OpenVPN

+ heel configureerbaar  
 + heel veilig (zelf voor NSA)  
 + kan firewallss voorbij  
 + veel encryptie algoritme mogelijkheden  
 + open source  
 - third party software nodig  
 - moeilijke setup  
 - nog niet zo goede support op mobile  
 - beveiliging is bovenop transport laag en niet netwerklaag

### L2TP ( Layer 2 tunnel protocol)

* Op zijn eigen geen encryptie of confidentialiteit dus como met IPSec  
  + heel veilig  
  + easy setup  
  + beschikbaar alle moderne platformen  
  - NSA heeft het gecompromised  
  - verzwakt door NSA  
  - trager dan OpenVPN  
  - soms problemen met firewalls