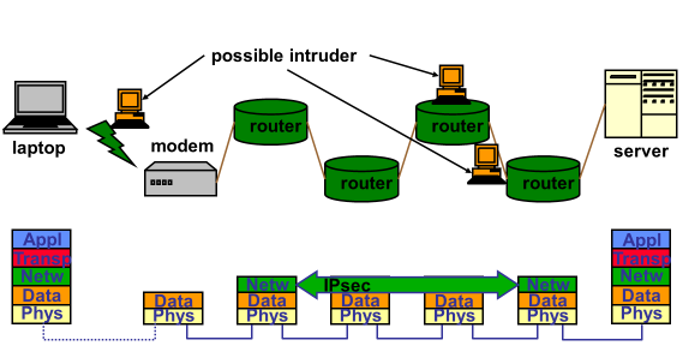
* Netwerk laag

(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

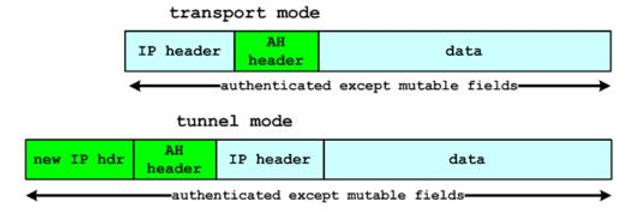
## Transport mode

* 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

## Encapsulating Security Payload

Todo vanaf slide 13