# Firewalls

* Laag tussen lokaal network en internet
* Veilig systeem kwa toeganklijkheid
* Beheert in/uit verkeer
* Welke internetservices toegestaan (binnen of buiten) en hoe
* Welke gebruikers toegelaten

Nadeel:

* Geen interne beveiliging
* Scrubnubs kunnen hotspots maken op uw bedrijf dus zijn er openingen
* Beperte bescherming vs. malware

## Packet filter

In/out IP pakketten toelaten/blokkeren

Op basis van

* Bron/doel IP adres
* Bron/doel IP adres [transportlaag]
* Gebruikt transport protocol
* Router interface naarwaar packet vandaag/verstuurd wordt

Dingen die niet expliciet geblokkeerd worden ofwel:

* Blocked
* Allowed

### Voordelen

* Basis beveiliging, simpel, goedkoop, transparant, snel
* Niet cryptografisch (geen key management)

### Nadelen

* Geen applicatielaag beveiliging
* Geen deftige user authentication (tenzij IPSec combo)
* Configuratiefouten frequent

### Problemen

IP spoofing

* Verzender doet geloven dat verkeer van vertrouwde omgeving komt (oplossing IPSec)
* Fragmentation attack: kleine packetten zodat TCP header in volgende packet zit.

### Verbetering

Stateful inspection:

Open connecties in de gaten houden en automatische timeouts. Toekomstige verbindingen zelfde flow worden toegestaan.

## Circuit level gateway

Relay op TCP niveau

1. De gateway krijgt client request binnen om TCP verbinding te starten
2. Gateway doet client authentication en de authorization
3. De gateway maakt een TCP verbinding met de server in naam vd client
4. Alle verkeer verloopt nu via deze gateway

Voordeel:

* applicatie onafhankelijk, gateway moetet zelf ni weten.
* Kan geauthenticeerd verkeer door de firewall laten
* Combinatie me proxy server

Nadeel:

* Detecteert geen applicatie threads: java applets, activeX, sql injection,...

## Application level gateaway (proxy)

* Applicatie specifiek
* Inspecteert applicatie laag packetten (http, ftp, smtp,..)
* Alles moet via de proxy verlopen

1. User vraagt een service aan de proxy
2. De proxy valideert de request en doet eventueel aan user authentication
3. Bij authenticati kan hij kiezen sommige functionaliteiten te achterhouden
4. De authenticatie kan outsourced worden naar een authentication server
5. De proxy stuurt de request door en het resultaat terug naar de client

Voordeel:

* Veiliger dan packet filters en circuit gateways want gelimiteerd aantal applicaties te checken, logging makkelijker en meer info toegankelijk dan want in IP packets staat

Nadeel:

* Aanpassing nodig van user procedure (eerst inloggen in proxy server)
* Specifiek voor 1 applicatie
* Dubbele connectie: meer processing per connectie nodig
* Niet eenvoudige support voor proxies bij alle services

Voorbeeld waar proxy nodig en andere 2 niet mogelijk:

Interne en externe gebruikers moeten op FTP server kunnen uploaden. Maar enkel interne mogen lezen  
Solution: proxy server laat PUT methodes toe. Maar blokkeert alle GET requests dat door de firewall willen gaan

Voorbeeld 2: wanneer ge wilt dat web services geblokkeerd worden

# Bastion

* Gateway op intern netwerk te beveiligen
* Veilig OS
* Enkel essentials op geinstalleerd
* Mogelijkheid sterke authenticatie voor proxy verbindingen
* Meestal ook een externe packet filter tussen internet en bastion: laat enkel verkeer door naar bastion
* en een interne packet filter tussen bastion en intern netwerk: laat enkel verkeer door naar bastion
* al het verkeer moet bij bastion passeren. Performantieproblemen mogelijk
* als bastion dood gaat, geen verbindingen meer mogelijk
* applicatie protocols zonder proxy support niet mogelijk
* ook mogelijk voor extern subnetwerk voor niet critische services