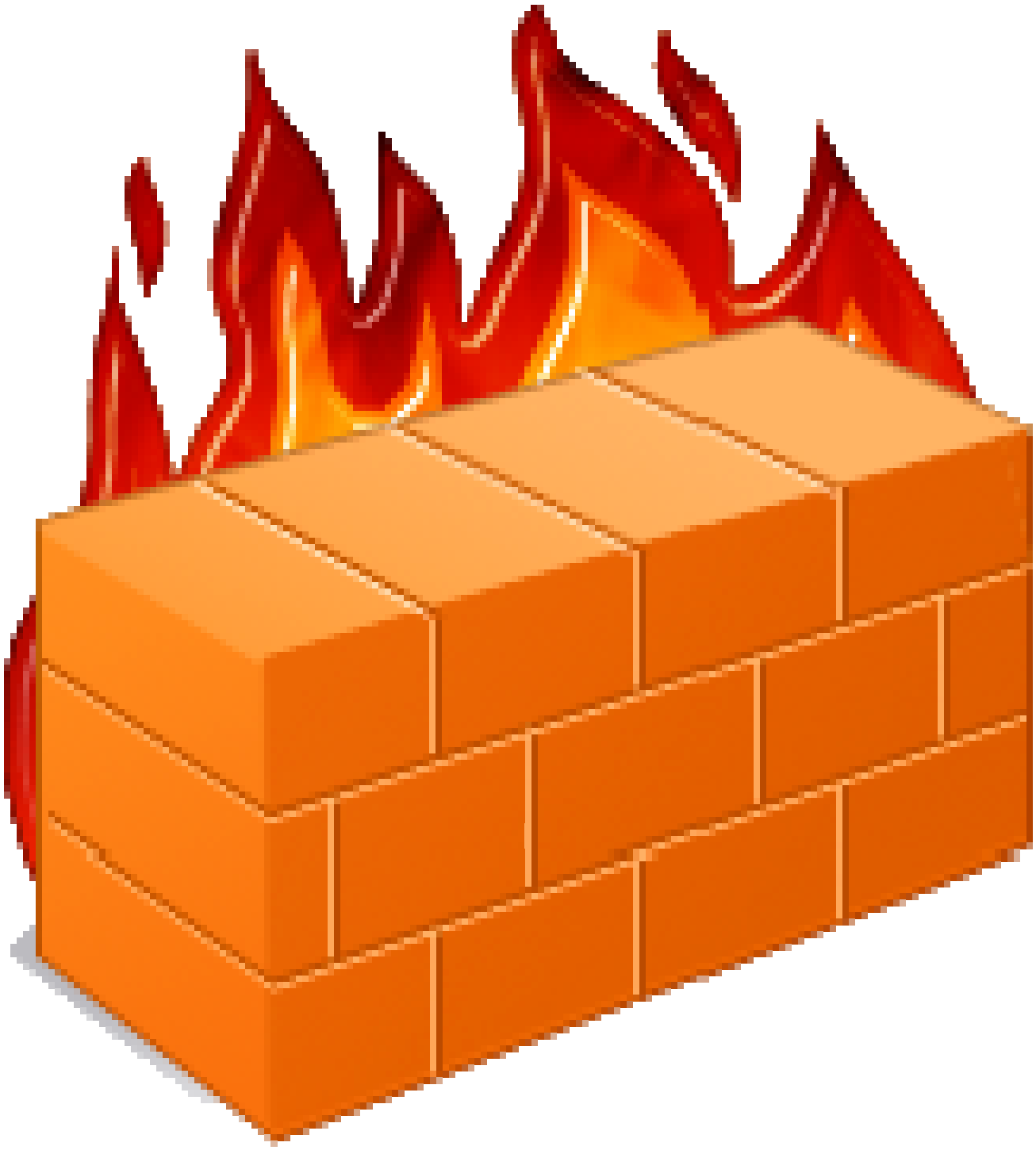
Firewalls



Overzicht

Netwerkbeveiliging: – een cascade van beveiligde zones

- Secure routers, packet filtering firewalls, application gateways (proxies)
- Firewall functies

Technologieën

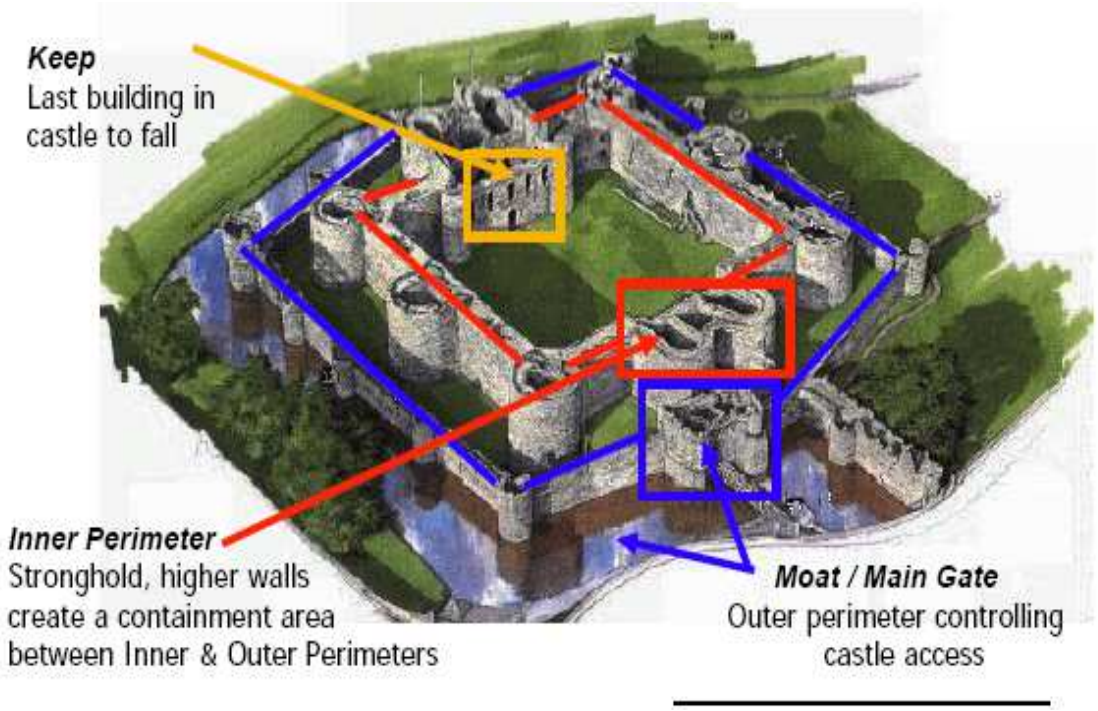
- Voorbeeldfirewall – Linux Netfilter
- Packet filtering – filter rules
- Application gateway
- Proxy services
- Stateful inspection technology
- Network address translation (NAT)
- Port address translation (PAT)

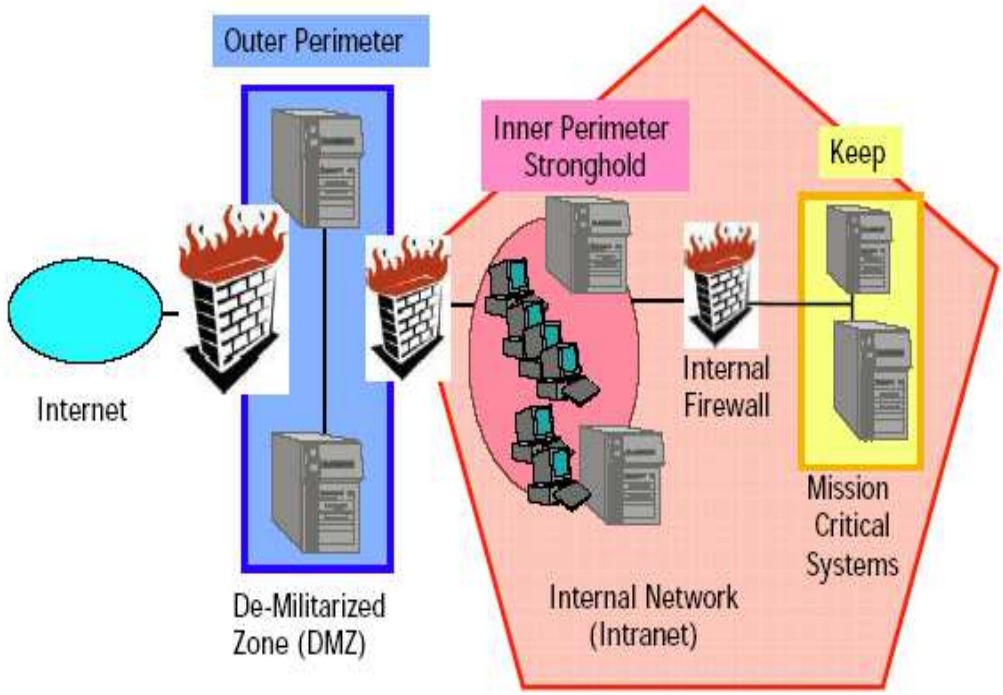
Beheer

- Remote Administration
- Examples: Checkpoint FireWall-1 and Linux IPCop
- Monitoring and Logging

Overzicht

- Netwerkbeveiliging: – een cascade van beveiligde zones





Een duidelijke **structuur, organisatie** helpt bij het verbeteren van de veiligheid. Eén manier van organiseren is het klasseren van documenten; een andere manier is het structureren van het netwerk;. De meeste ondernemingen delen een netwerk op in diverse **zones**, maar er zijn geen algemeen aanvaarde definities van die zones noch bestaat er een schema voor naamgeving van zones.

De typische indeling die door bedrijven gehanteerd wordt, voorziet minstens **drie** zones:

1. **Internet** (onveilige zone): deze zone is onveilig omwille van haar praktische doeleinden. Hier bestaan geen middelen ter bescherming van het netwerk tegen anderen. De enige beveiliging in deze zone komt uit de machine zelf.

2. **Gedemilitariseerde zone** (DMZ): deze zone is gescheiden van het internet door een eerste deel van een firewall (doorgaans een filtering firewall). Hier bevinden zich gewoonlijk ook die servers die veelvuldig benaderd worden vanuit het internet (bijv. bedrijfswebserver, DNS met de publieke adressen, MailServer)

3. **Intranet** (beveiligde zone, vertrouwde zone): deze zone wordt gescheiden van de DMZ door een tweede deel van een firewall (meestal een proxy-server dwz Application Level Firewall), die aanvragen om verbindingen vanuit het interne netwerk naar de buitenwereld verwerkt.

Er kunnen nog andere specifiek beveiligde zones binnen het intranet bestaan, die beschermd zijn tegen aanvallen van hosts uit het intranet. Deze zones bevatten bedrijfskritische systemen of maken onderdeel uit van organisaties met hoge beveiligingseisen (bv. het politiedepartement binnen een overheidsorganisatie).

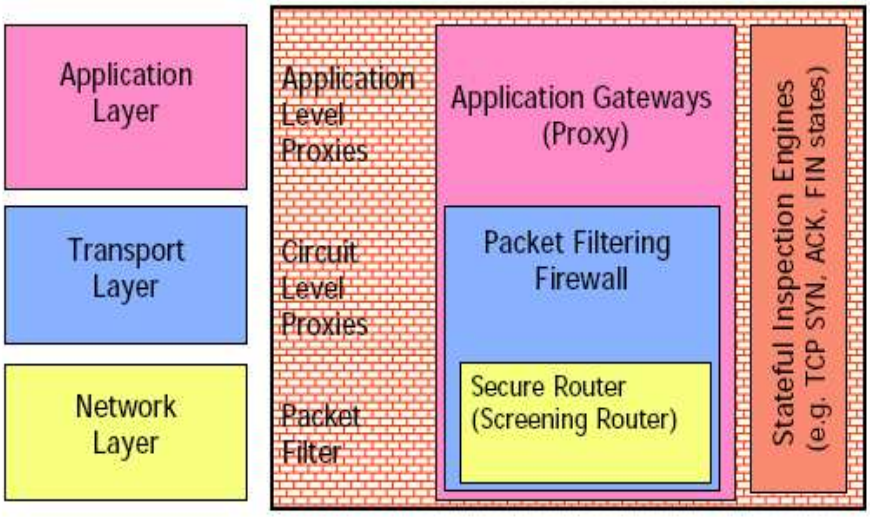
-

Secure routers, packet filtering firewalls, application gateways (proxies)

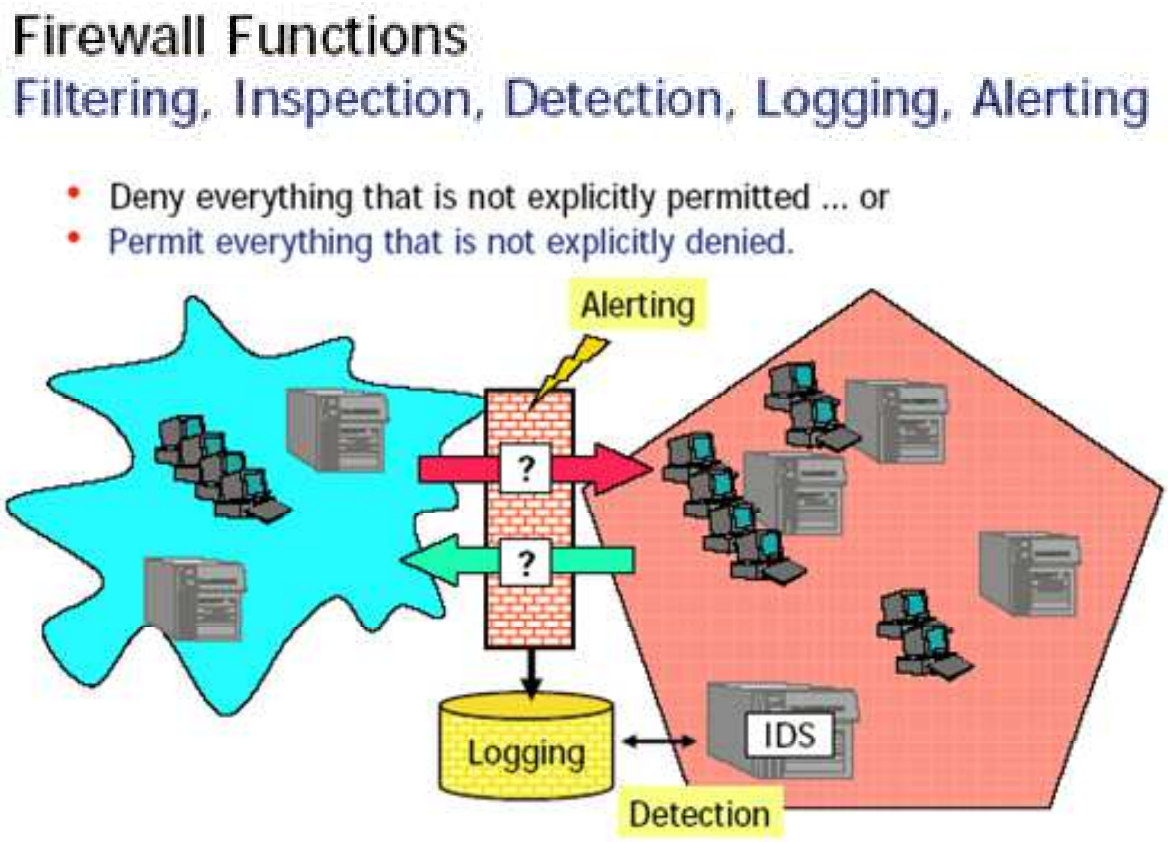
De belangrijkste firewall-technologieën zijn:

Packet filtering: controleren de header-informatie van de pakketten
Deep packet inspection: bekijken de applicatie-inhoud van de pakketten
Application Gateways: sluiten verbindingen af en scannen eveneens op applicatie-inhoud van de pakketten

Sommige firewalls controleren de pakketten enkel één voor één. **Stateful inspection firewalls** kijken naar pakketstromen en proberen de verbindingen een bepaalde status toe te kennen.
Het merendeel van de moderne firewalls zijn **hybride** producten die niet gemakkelijk in één bepaalde categorie ondergebracht kunnen worden.



Firewall functies



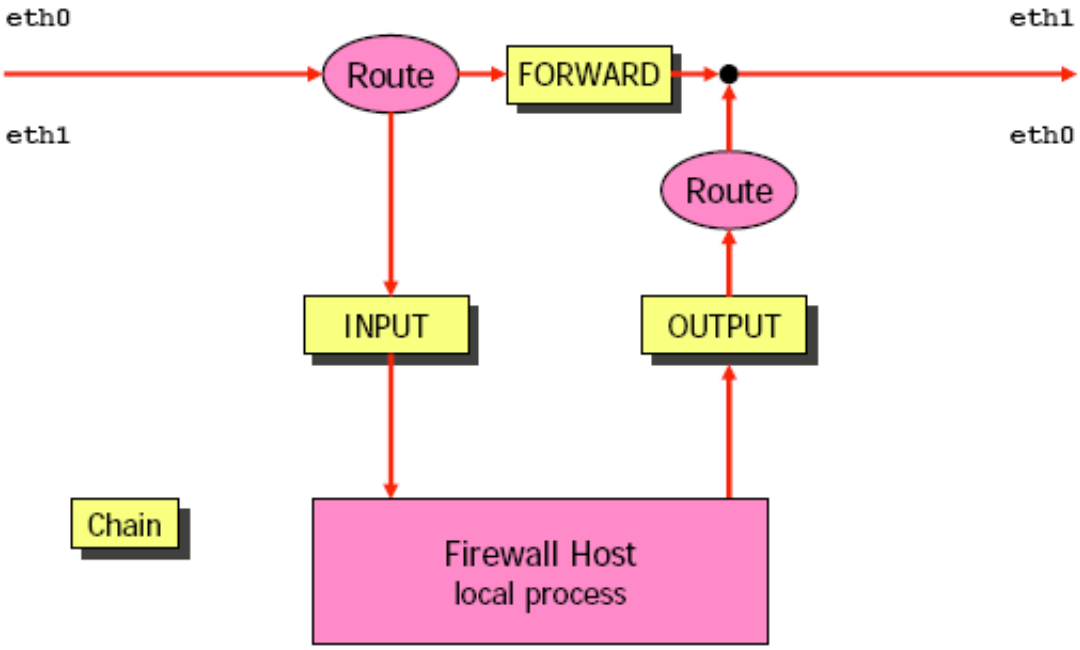
Een firewall kan verscheidene functies vervullen:

• filteren en inspecteren van het verkeer
• gebeurtenissen (en verkeer) loggen
• inhouden screenen (virusscanning, bepaalde inhouden blokkeren, url-filtering, Protocol compliance testen)

• hergebruik van adressen toelaten (uitvoeren van Network Address Translation, NAT functie), interne structuur verbergen
• Detectie van aanvallen, alarmsignalen versturen, communiceren met andere apparatuur zoals bv een 'intrusion' detection system (Open Platform for Security, OPSEC)
• als virtual private network (VPN)-server fungeren
• beheerders authenticeren (gebruik van tokens / smart cards of 2-factor authenticatie)

Technologieën

- Voorbeeld firewall: Linux Netfilter



http://www.netfilter.org

Filter Rules – Default Policy

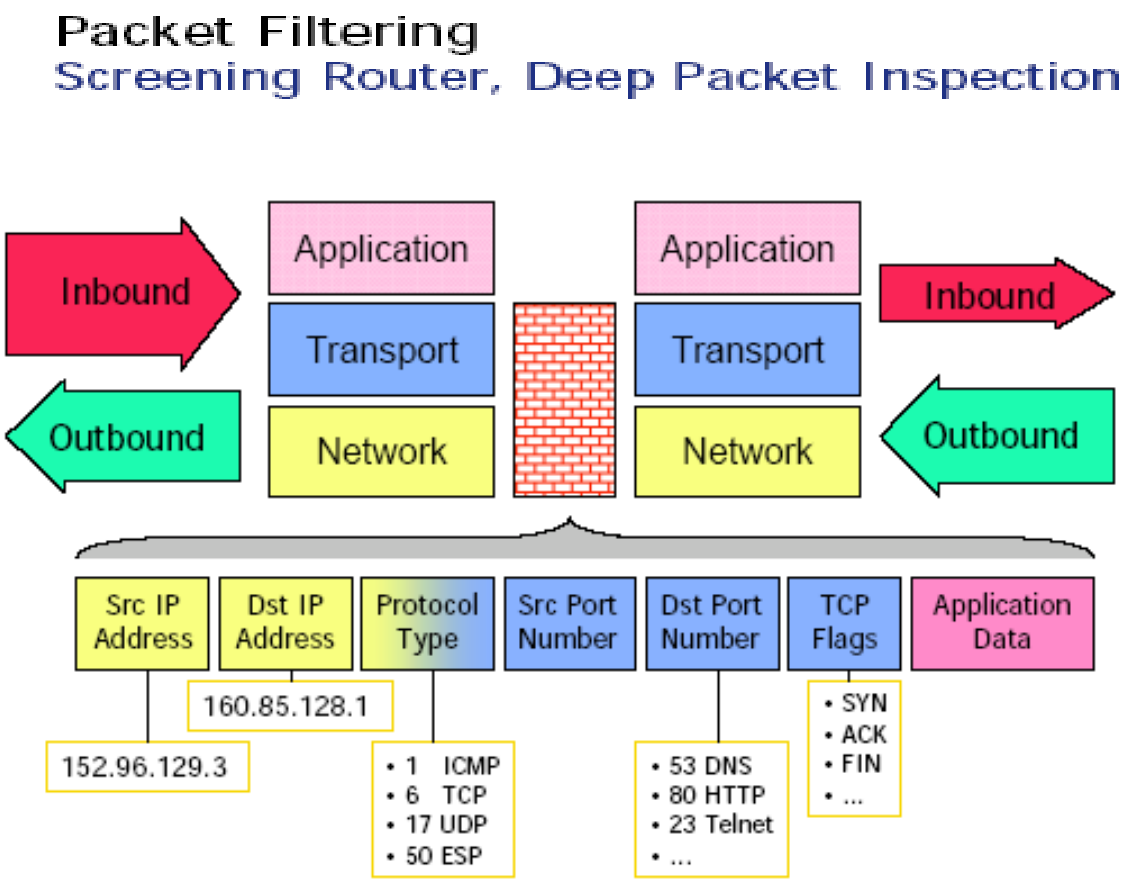
- Permit everything that is not explicitly denied.

```
iptables –P INPUT ACCEPT
iptables –P FORWARD ACCEPT
iptables –P OUTPUT ACCEPT
```

- Deny everything that is not explicitly permitted.

```
iptables –P INPUT DROP
iptables –P FORWARD DROP
iptables –P OUTPUT DROP
```

- Packet filtering – filter rules



Packet-Filtering Firewalls voorzien in netwerkbeveiliging door netwerkverbindingen te filteren op basis van informatie in de TCP/IP headers van elk packet. Packet-Filtering Firewalls worden ook wel “Screening Routers” of “Filtering gateway firewalls” genoemd.
Een deep-packet inspection (DPI) firewall controleert ook de inhoud van elk packet.
Packet-Filtering Firewalls maken gebruik van een speciale rule set om IP, TCP, ICMP, en andere packets te filteren die langs de netwerkinterface passeren.
Binnenkomende en uitgaande packets worden gefilterd op type, source address, destination address, en port information in elk packet.
Een filtering gateway behoeft geen krachtige hardware en een oude x468 box en een gespecialiseerde one-floppy Linux mini-distributie kunnen al volstaan.

Voorbeelden van Packet Filtering

- Default Policy: Deny everything that is not explicitly permitted.

```
iptables –P INPUT DROP
iptables –P FORWARD DROP
iptables –P OUTPUT DROP
```

- Allow ssh login to firewall host from outside

```
iptables –A INPUT –i eth0 –p tcp --dport ssh –j ACCEPT
```

```
iptables –A OUTPUT –o eth0 –p tcp --sport ssh –j ACCEPT
```

- Allow pings from all interfaces

```
iptables –A INPUT –p icmp –-icmp-type echo-request –j ACCEPT
iptables –A OUTPUT –p icmp –-icmp-type echo-reply –j ACCEPT
```

- Drop any traffic coming from host 80.63.5.7

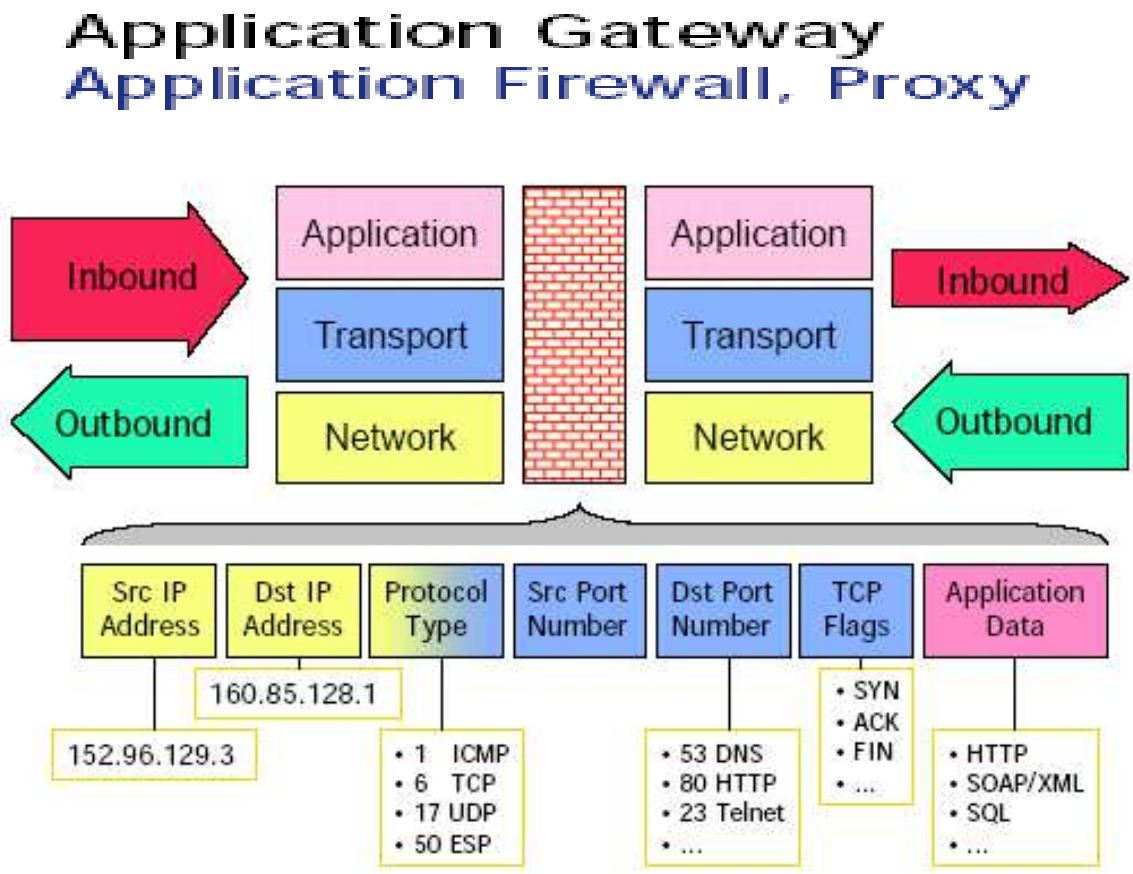
```
iptables –I INPUT 1 –i eth0 –s 80.63.5.7 –j DROP
```

Er bestaan diverse strategieën voor de implementatie van packetfilters. De volgende twee zijn nogal courant:

• **Stel regels op van heel specifiek tot minder specifiek**!
De meeste packetfilters verwerken de regels “top to bottom” en de verwerking stopt zodra er een ‘match’ is.

• **Plaats de meest actieve regels bovenaan de lijst**!
Het screenen van packets is een processor-intensieve aangelegenheid. Bijgevolg zal de plaatsing van de “populaire” regels bovenaan de queue ervoor zorgen dat de processor niet nodeloos alle regels moet verwerken voor elk afzonderlijk pakketje.

- Application gateway



- Application Gateway is een synoniem geworden voor termen als “bastion host, proxy gateway”, en “proxy server”. Een application gateway beslist over toegang op basis van packet info op alle (zeven) lagen van het OSI- model. Een application gateway kan bovendien ingesteld worden om bezwaarlijke inhouden, zoals ActiveX of Javascripts uit webpagina ’s te weren.
- Sommige proxies zijn onzichtbaar voor “end-systems” en worden daarom „transparante proxies“ genoemd (in tegenstelling tot „visible proxies“).
- Een proxy moet elke service “verstaan”. Proxies voor nieuwere services zijn doorgaans moeilijk te vinden.

Proxy Services

- Circuit-level gateway

  bouwt een TCP-verbinding op volgens welbepaalde regels (security policy) Geen content filtering mogelijk, geen gebruikersauthenticatie.

- Application-level gateway

  bouwt TCP-verbindingen met een application- level gateway op de plaats.

Een beheerder kan de toegang controleren tot applicaties/netwerkservices naar wens (bv. HTTP, SOAP/XML, enz...). Ook content filtering en gebruikersauthenticatie behoren tot de mogelijkheden.

Application Gateways of Proxy Firewalls bevatten gewoonlijk bijkomende beveiligingsmogelijkheden voor ondersteunende software zoals een VPN server, sterke authenticatieservices (tokens, smart cards), of virusscan- engines. Proxy Firewalls ook gekend als “**Proxy services”** opereren tussen externe en interne netwerken en bieden een vervangende connectie ipv rechttstreekse connecties met remote services. Proxies trachten min of meer transparent te werken. Proxy firewalls vereisen krachtige hardware. Men kan deze categorie in 2 groepen verdelen: