Internett-brannvegger

kurs UNINETT'95

Nils Harald Berge & Knut Soelberg

Norsk Regnesentral

Innhold

Del 1

Introduksjon - brannmurer
Komponenter
Arkitekturer
Pakkefiltrering
Introduksjon til Proxy

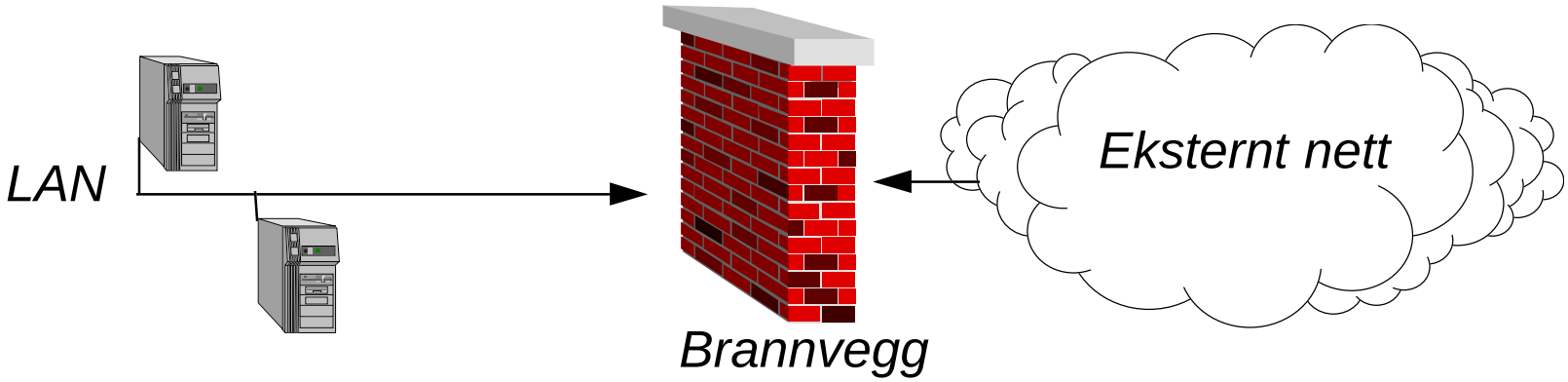
Del 2

Produkter
Konfigurasjon
Administrasjon

Hva er en brannvegg?

***Egenskaper**:*

- *Barriere mellom to nettverk*
- *Trafikk passerer gjennom et "nåløye"*
- *Trafikk som ikke er i henhold til organisasjonens sikkerhetsstrategi blir blokkert*



Hva kan en brannvegg beskytte?

En brannvegg kan beskytte:

- *Informasjon*
- *Ressurser*
- *Ens eget renomme....*

  - *Brannveggen reflekterer en organisasjons sikkerhetsstrategi mhp. ekstern kommunikasjon*

Hva kan ikke en brannvegg?

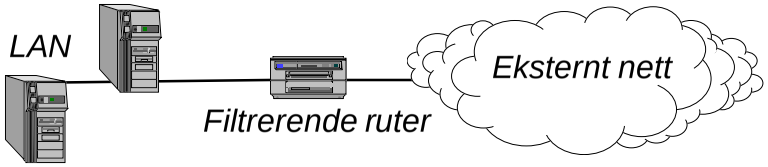
En brannvegg kan ikke beskytte mot:

- *Nye trusler/sikkerhetshull*
- *Virus*
- *Utro tjenere (interne trusler)*
- *Uhell forårsaket av brukere som ikke vet bedre*

  - *Det at man har installert en brannvegg betyr ikke at man kan glemme andre sikringstiltak*
  - *Opplæring vil ofte være den viktigste sikkerhets-foranstalningen man kan gjøre*

Komponenter i en brannvegg

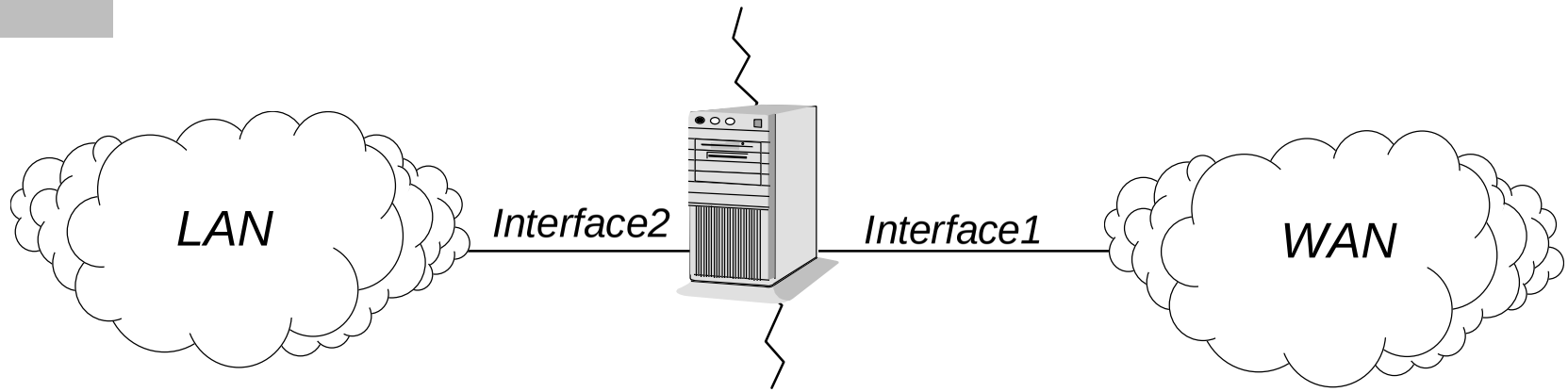
- *Filtrerende ruter*
  - *grunnleggende komponent i de fleste løsninger*



- *Grensemaskin/Bastion Host*
  - *generell datamaskin som definerer “porten” ut og inn fra ditt interne nett*

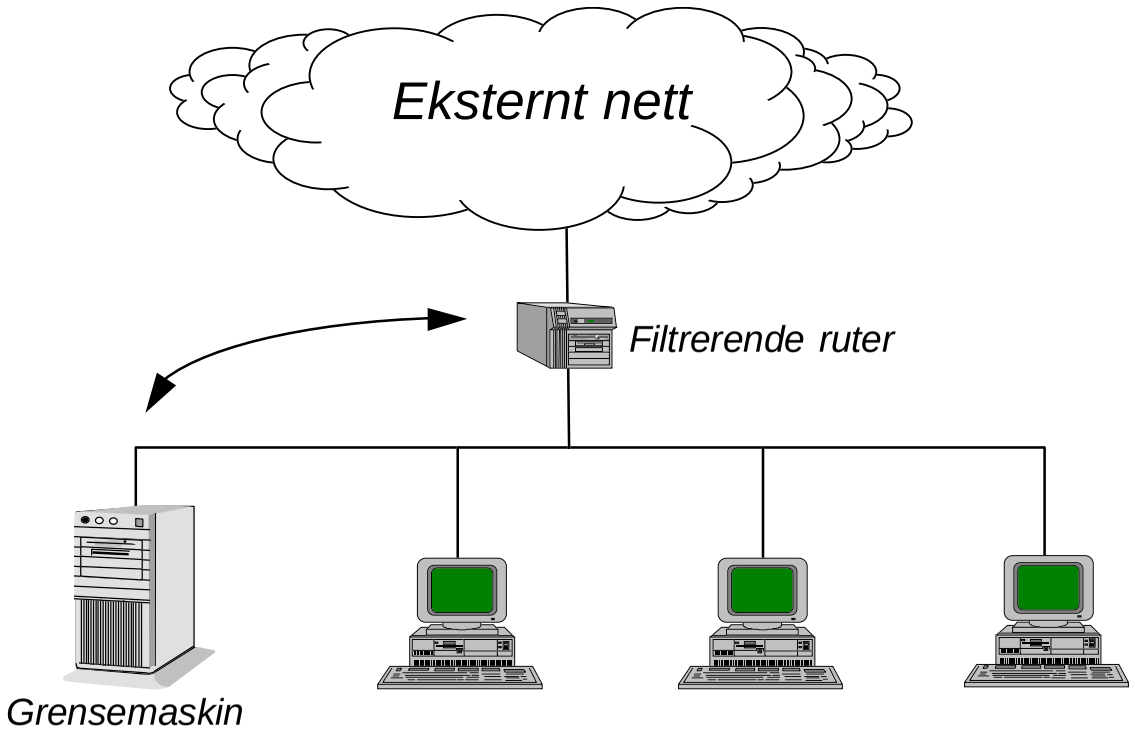
Typiske arkitekturer I

- ***Dual homed host***
  - *Generell maskin med to nettverkskort. En dual homed host er en grensemaskin.*



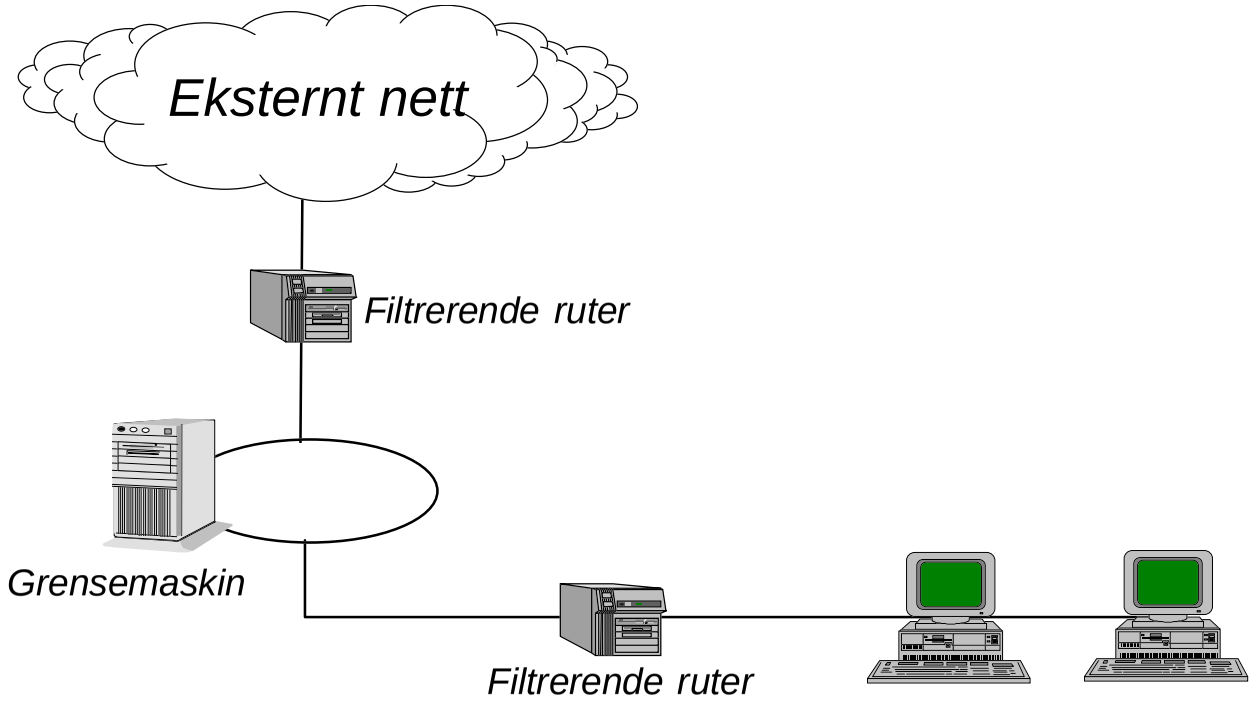
Typiske arkitekturer II

- ***Screened host***
  - *kombinasjon av filtrerende ruter og grensemaskin*



Typiske arkitekturer III

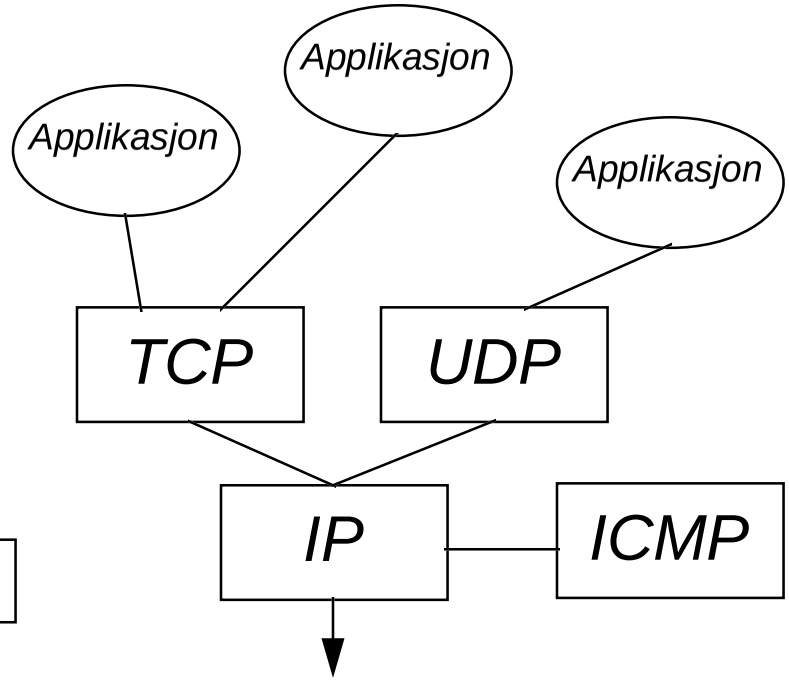
- ***Screened subnet***
  - *et subnett mellom ditt interne nett og det eksterne*



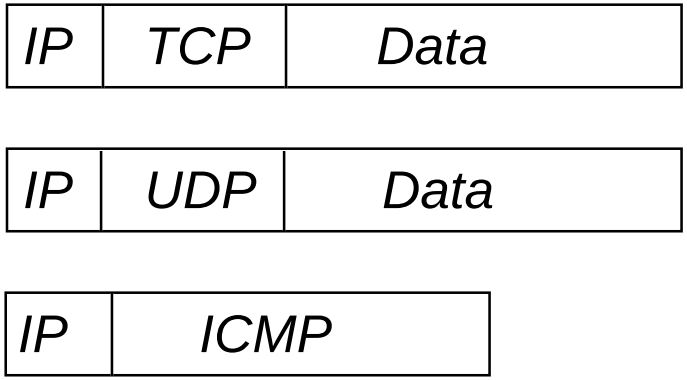
Pakkefiltrering

- *Blokkere trafikk basert på protokoll-informasjon i hver enkelt pakke*
- *Viktige protokoller: IP, TCP og ICMP*
- *Typisk blir pakker kontrollert med tanke på:*
  - *hvilken maskin de kommer fra*
  - *hvilken maskin de skal til*
  - *transportprotokoll*
  - *tjeneste pakken skal til/stammer fra*

Internett protokoll-stakken



Pakkestruktur:



IP - Internet Protocol
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
ICMP - Internet Control Message Protocol

Pakkefiltrering - IP

Viktige informasjon:

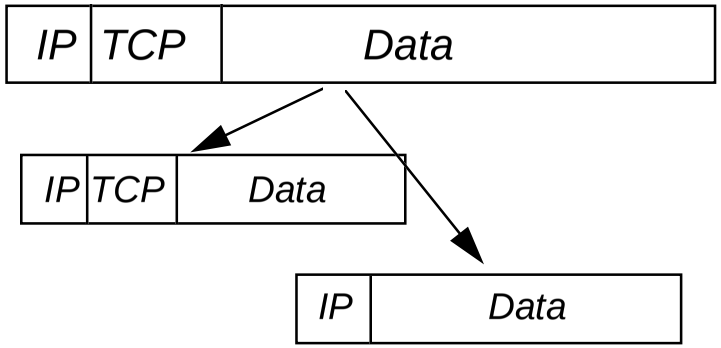
- *Avsenderadresse (IP-adresse)*
- *Mottakeradresse (IP-adresse)*
- *Protokoll*
  - *TCP, UDP, ICMP*
- *Opsjoner*
  - *Source Routing*

Problemer:

- *Du kan aldri stole 100% på en avsenderadresse*
- *Source-routing kan utnyttes av en angriper*

Filtrering av fragmentert trafikk

- *Filtrer kun på første fragment*
- *Fragmentring kan utnyttes (nektelse av tjeneste angrep)*
- *Ikke returner ICMP-melding "packet reassembly time expired"*



Pakkefiltrering - TCP

Viktig informasjon:

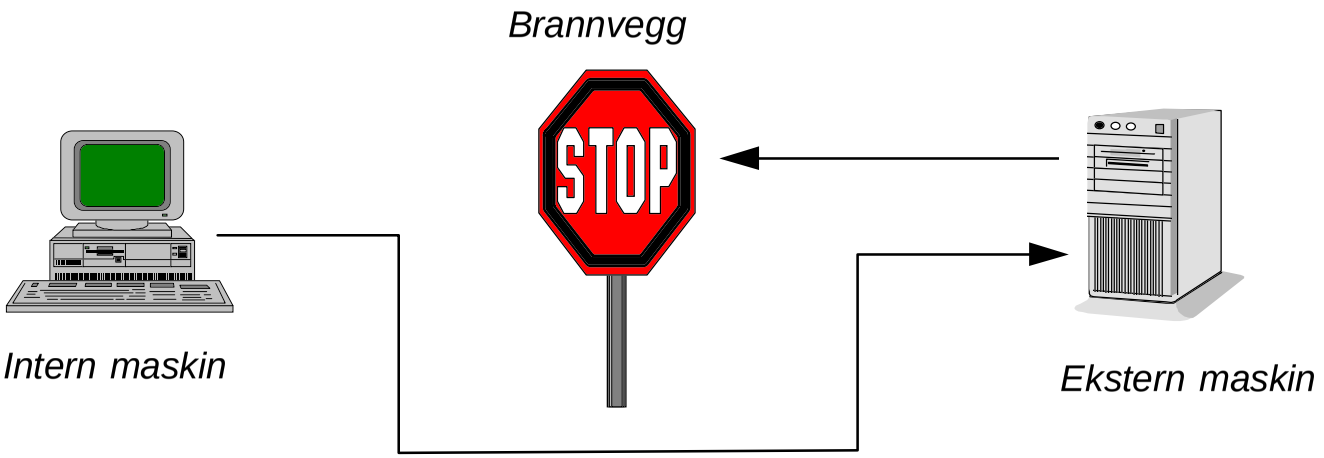
- *Avsender-portnummer*
- *Mottaker-portnummer*
- *ACK-bit (i flagg-feltet)*

Problemer:

- *Du kan aldri stole 100% på avsender-portnummeret*
- *Alle tjenester ligger ikke i portnr. intervallet 0-1023*

Blokkering av inngående TCP-forbindelser

- *Konfigurer aksesslister som utnytter ACK-bitet*



Filtrering av andre protokoller

- *User Datagram Protocol (UDP)*
  - *Vanskelig å filtrere sikkert. Anbefaling: blokker UDP-trafikk med unntak av DNS, NTP og Archie*
- *Internet Control Message Protocol (ICMP)*
  - *Generelt bør ICMP-trafikk blokkeres av en brannvegg*
  - *Brannveggen selv kan svare på ICMP-meldinger*
- *Remote Procedure Call (RPC) protokoller*
  - *“Farlige” RPC-baserte tjenester bygger stort sett på UDP*

På trappene: neste generasjon IP - IPv6 (IPng)

Eksempel - utgående Telnet

Følgende filter tillater kun utgående telnet-sesjoner:

Regel	Retning	AvsenderAdr	MottakerAdr	Protokoll	Avsenderport	Mottakerport	ACK	Aksjon
A	Ut	Intern	X	TCP	>1023	23	X	tillat
B	Inn	X	Intern	TCP	23	>1023	ja	tillat
C	X	X	X	X	X	X	X	blokker

X-vilkårlig

- *Regel A tillater pakker til eksterne Telnet-tjenere*
- *Regel B tillater returpakker fra eksterne Telnet-tjenere*
- *Regel C "default" regel: blokker alt!*

Pakkefiltrering - fordeler og ulemper

Fordeler

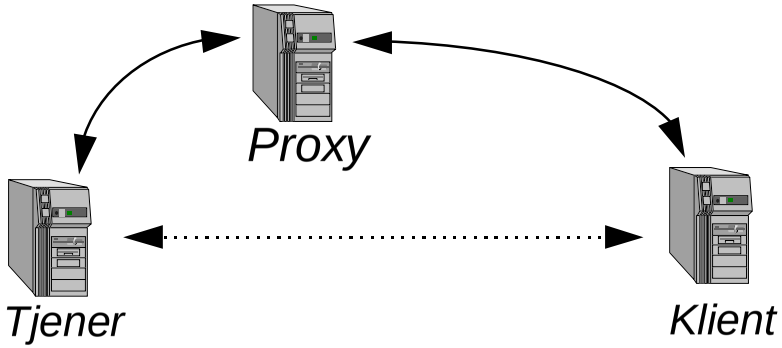
- *Du oppnår mye med et strategisk plassert pakkefilter*
- *Er helt transparent for brukere (og tjenester), krever ingen form for opplæring eller innføring i nye rutiner*
- *Er tilgjengelig i de fleste moderne rutere*
- *Effektivt, gir god kapasitet.*

Ulemper

- *Ofte vanskelig å konfigurere og test*
- *Noen protokoller er lite egnet for pakkefiltrering*
- *Gir bare sikkerhet på "de nedre lag" - kan eksempelvis ikke brukes til å autentisere brukere eller applikasjoner*

Introduksjon til proxy-systemer

- *Ikke direkte forbindelse mellom internt og ekstern system*



To typer:

- *Transportnivå - de generiske proxy'ene*
- *Applikasjonsnivå - en proxy-tjener for hver tjeneste, kalles gjerne "applikasjonsgateway"*

Brannveggprodukter - fritt tilgjengelige

- *Pakkefilter*
  - *Drawbridge, fra TAMU*
- *Transportnivå*
  - *SOCKS, fra NEC*
- *Applikasjonsportnere*
  - *Firewall Toolkit, fra TIS*
  - *Freestone, fra SOS*

Brannveggprodukter - kommersielle

- *Pakkefiltre*
  - *Pakkefiltrerende rutere, Cisco*
  - *Firewall-1, Checkpoint*
- *Applikasjonsportnere*
  - *Gauntlet, Trusted Informations Systems*
- *Hybrider*
  - *Brimstone, SOS Corporation*
  - *CyberGuard, Harris Computer Systems*

Leverandører

- *Basis tjenester*
  - *Sette opp og konfigurere løsningen*
  - *Opplæring*
  - *Skreddersydd dokumentasjon for installasjonen*
- *Tilleggstjenester mange kan tilby*
  - *Utarbeide sikkerhetsstrategi*
  - *Outsourcing*

Leverandører

- *De fleste har kun en type løsning*
- *Varierende kompetanse om*
  - *produktet*
  - *brannmurer og sikkerhet generelt*
- *Ofte kun en sentral kompetanseperson*
- *Velg ikke første og beste produkt og leverandør*

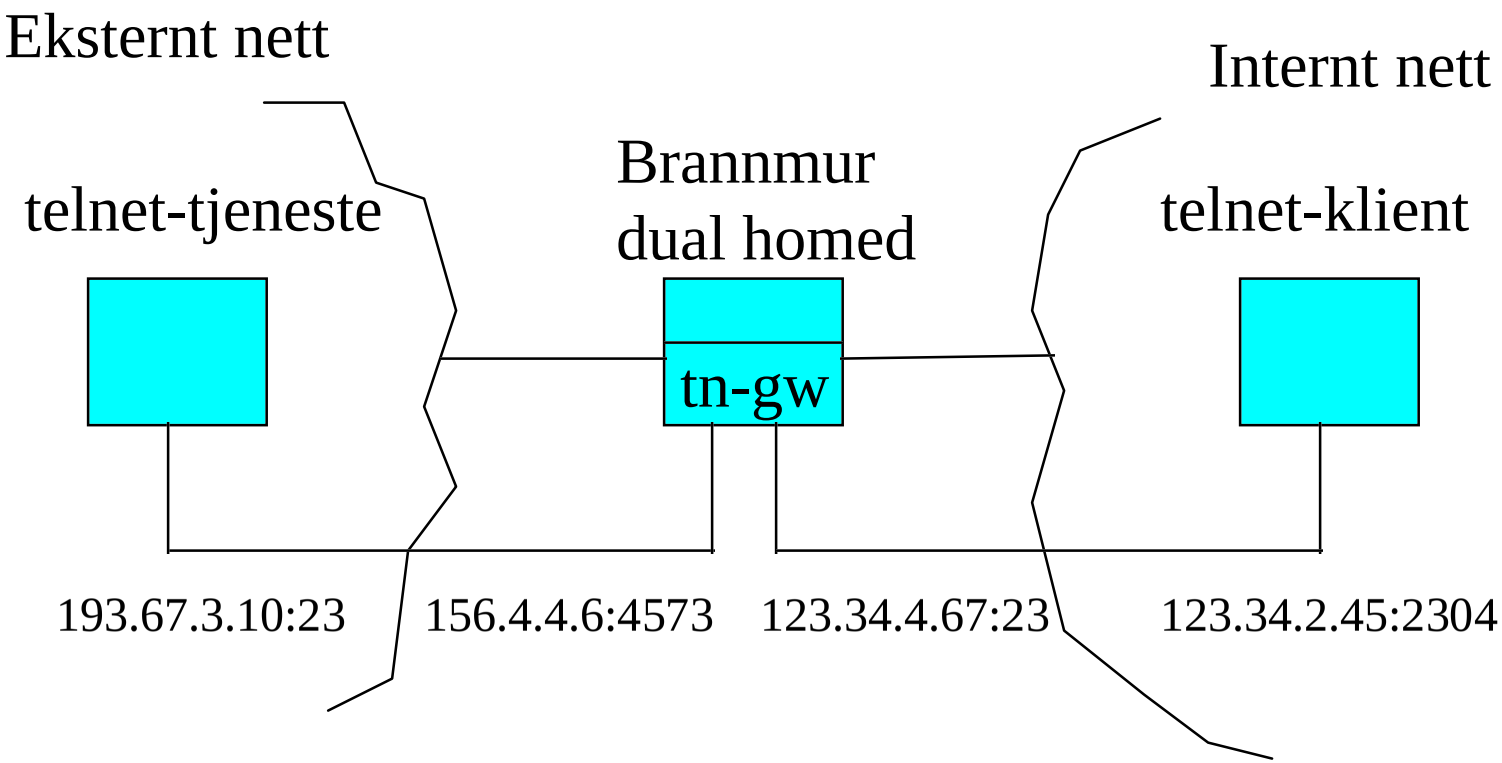
Firewall Toolkit (fwtk)

- *Et sett med programvareverktøy for å konstruere applikasjons gw brannvegger*
- *Alle verktøyene har*
  - *minimal, kun helt nødvendig funksjonalitet*
  - *lite kode, enkle og oversiktlige*
  - *tjenestene kjører uten privilegier hvis mulig*
- *Proxier*
- *Sterk autentisering*

Fwtk - telnet eksempel

*%-> **telnet gatekeeper***
Trying 192.33.112.117 ...
Connected to gatekeeper.
Escape character is '^]'
gatekeeper telnet proxy (Version v1.0) ready:
*tn-gw-> **help***
Valid commands are: (unique abbreviations may be used)
connect hostname [port]
help/?
quit/exit
*tn-gw-> **c somebox. domain***
SomeOS UNIX (somebox)
*login: **you***
Password: #######
Last login: Mon Sep 27 21:22:16 from some other.box
*somebox% **logout***
%->

Proxytjeneste skjematisk fremstilling



Det er ingen direkte forbindelse mellom intern klient og ekstern tjeneste

Konfigurering og administrasjon

- *Tekstbaserte konfigurasjonsfiler*
- *Kommersielle løsninger kan ofte tilby*
  - *Grafiske brukergrensesnitt*
  - *Terminalbasert som gir mulighet for automatisering*
- *For brukervennlige grensesnitt kan føre til falsk trygghet*

Konfigurering av fwtk

- *En sentral fil - netperm-table*
  - *Aksesskontroll (netacl)*
  - *Konfigurasjon av proxy-tjenester*
  - *Evt. bruk av autentiseringstjenester*
- *Rekonfigurering av inetd.conf*
  - *netacl startes istedenfor den egentlige tjenesten*
  - *netacl starter selv tjenesten hvis ok*

Konfigurasjon av bastion host

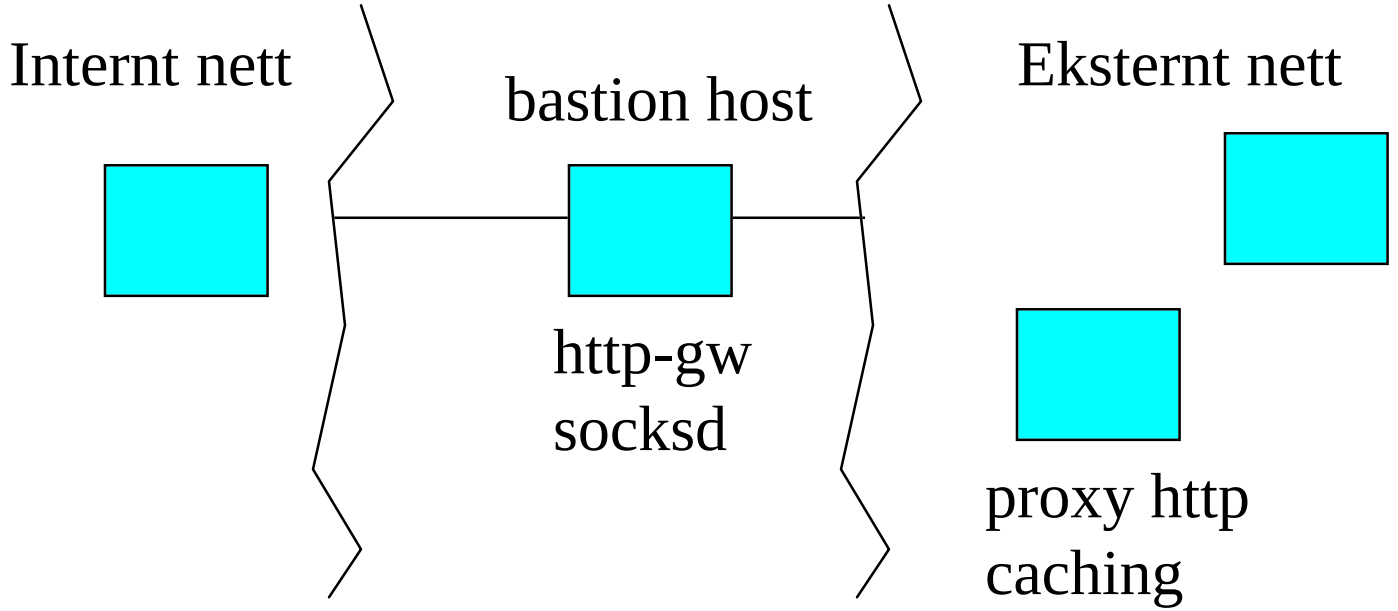
- *Benytt det operativsystemet du kjenner best*
- *Fjern unødvendig programvare og tjenester*
- *Fjern slik som NFS støtte fra kjernen*
- *Sørg for et høyt sikkerhetsnivå (Cops, tiger)*
- *Sørg for utstrakt bruk av logging & varsling*
- *Kjør proxiene i et chroot miljø*
- *Skru av IP-forwarding*

Konfigurasjon av DNS

- *DNS navnetjeneste kan by på problemer*
- *Valg*
  - *Operere med en egen uavhengig navnetjeneste med egne roottjenere*
  - *Skjule navn på interne noder*
  - *La navn på interne noder være kjent*

World Wide Web

- *Den tjenesten brukerene vil ha*
- *Genererer mange forbindelser*
  - *Store krav til ytelse på http-gw*



Applikasjonsgateway
Hva med nye tjenester?

- *En proxy for hver tjeneste*
  - *Ny tjeneste => behov for ny proxy*
- *Hva med*
  - *Realaudio (udp-basert)*
  - *Nye betalingstjenester*
- *Brannveggprodusenter vil utvikle proxier for nye tjenester*
  - *men proxien vil alltid komme i ettertid*

Brannvegger - Plug and Play?

- *Mange kommersielle brannvegger har*
  - *lettfattelig grafisk brukergrensesnitt*
    - *– forenkler installasjon og konfigurasjon*
  - *alt du trenger i en enhet for*
    - *– sikker tilkobling til Internett*
    - *– å tilby web-, ftp-tjenester mm. ut på Internett*
- *Lav brukerterskel*
  - *løsningen "er på lufta" med et museklikk*

Tilfredstillende totalløsninger krever

- *Oppsett & konfigurasjon basert på din organisasjons sikkerhetspolitikk*
- *Tilfredstillende drift og vedlikehold*
  - *Må forstå konsekvensene av en endring*
- *Gode rutiner for endringshåndtering*
- *Klare ansvarsforhold og koordinering*
- *Brannvegger er **ikke** plug 'n play!*

Endringshåndtering

- *En ansvarshavende for totalløsningen*
  - *bastion host, screening routers og programvare*
- *Ingen endringer (hardware og software)*
  - *uten konsekvensvurdering og klarsignal fra ansvarshavende*
- *Prosedyrer for de vanligste endringene*
- *Oppdater dokumentasjon etter hver endring*

Se på helheten

- *Ikke installér en ståldør i hovedinngangen når kjøkkendøra står på vidt gap*
  - *Ikke glem at tilkoblingen til Internett kun er en av mange trusler*
  - *Vurder også krav til sikkerhet ved tilkobling til andre nett*
  - *"Private" modem tilkoblet det interne nett kan være store sikkerhetshull*

Brannvegger - dilemma

- *Større krav til sikkerhet medfører større begrensninger og mindre brukervennlighet for brukerene*
- *Brukervennlighet kontra grad av sikkerhet må vurderes før valg av løsning*

Valg av type brannvegg

- *Avgjør hva du ønsker å oppnå*
  - *Blokkere alle innkommende sesjoner eller noen*
  - *Stoler du på dine egne brukere, kan de gjøre hva de vil?*
  - *Blokkere for den tilfeldige “hacker’n”*
  - *Tilby sikre forbindelser med sterk autentisering og kryptering*

Sikkerhet på brukernivå

- *Bevisstgjør brukeren om å være påpasselig med hva de sender hvor av informasjon*
- *Retningslinjer for bruk av lokale og internettressurser*
- *Tilrettelegg for å unngå virusproblemer mm*
  - *La frivillige vedlikeholde kataloger med populær fritt tilgjengelig programvare*

Oppsummering

- *Ikke la en brannvegg bli en falsk trygghet*
- *Ikke tro at en brannvegg er "hyllevare"*
  - *Plug and Play er **ikke** målet*
- *Ikke tro at brannveggen er sikker bare teknologien er på plass*
  - *En tilfredstillende brannvegg totalløsning:*
    - *20% teknologi*
    - *80% administrasjon*