Brannmurer

Brannmurer

- **fire wall** *(noun)*: A fireproof wall used as a barrier to prevent spread of fire.

  -American Heritage Dictionary

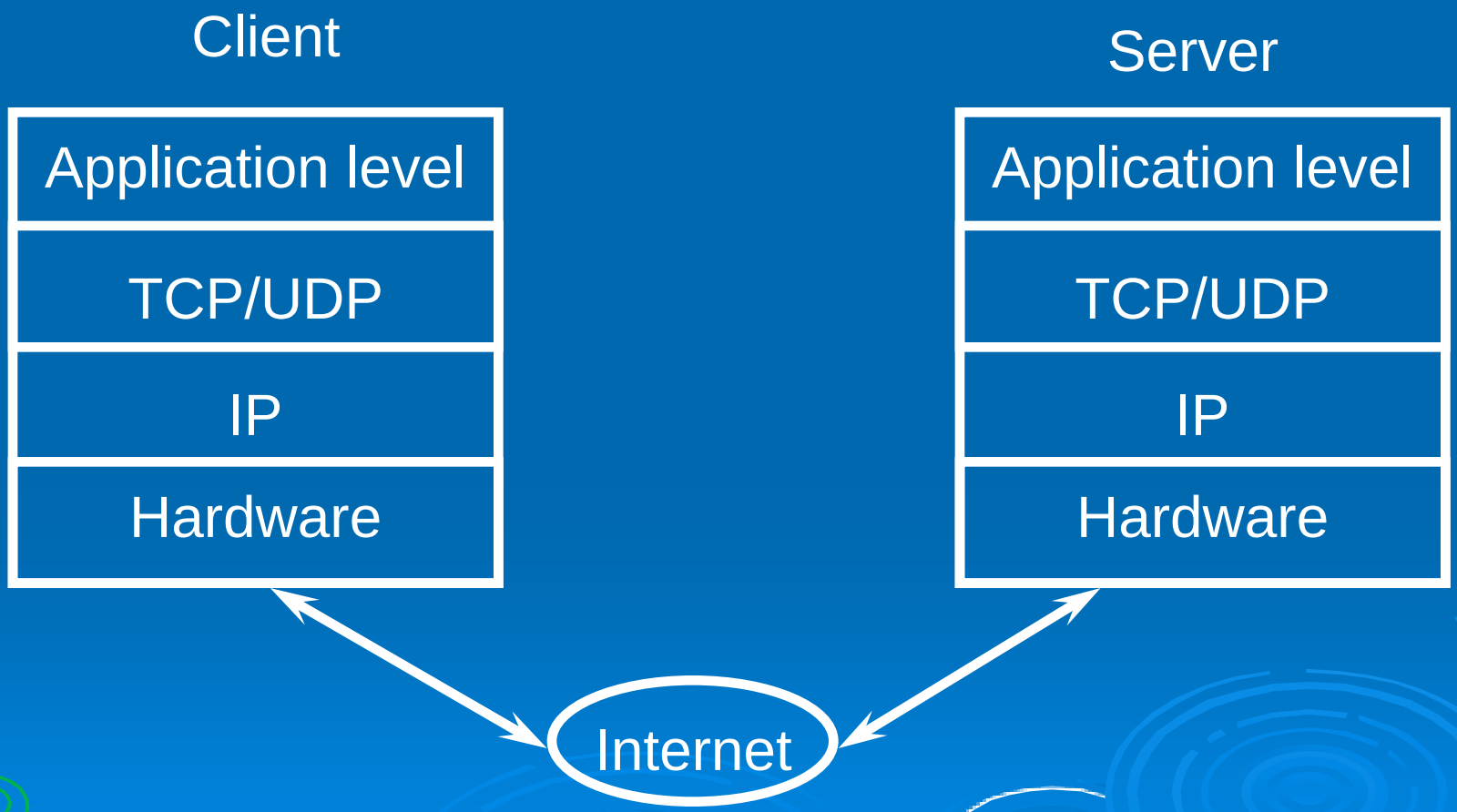
- **fire wall** *(noun, internet)*: Internet firewalls are intended to keep the flames of Internet hell out of your private LAN.

  -Mark Grennan

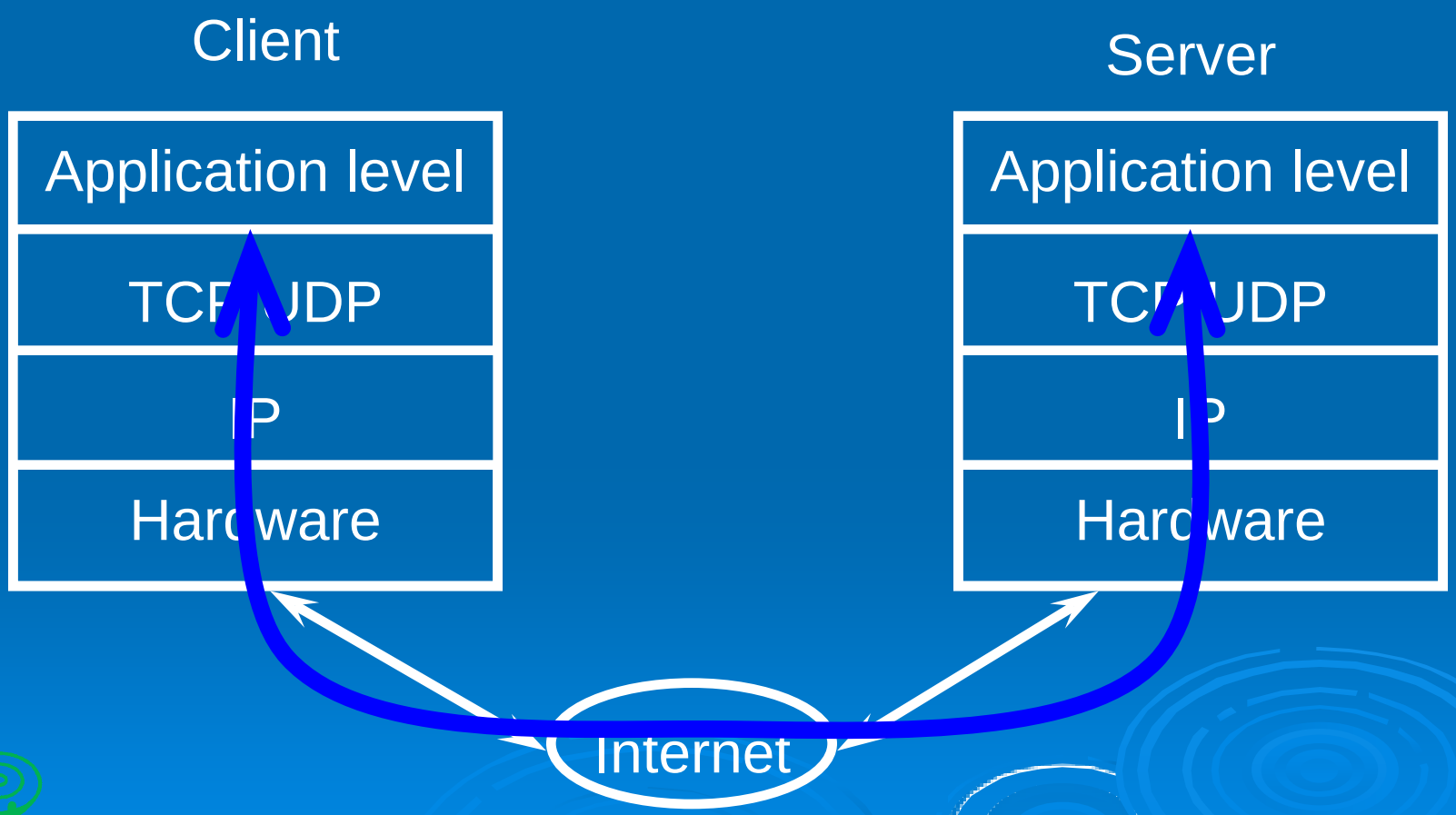
Brannmur

- System som utøver en aksesskontoll politikk mellom to nettverk.
- Brannmur egenskaper
  - En brannmur har typisk to nettverkskort, et internt og et eksternt.
  - Sikkerhetspolitikk på brannmur bestemmer hvilken trafikk som kan passere og hvillken som forkastes
  - En brannmur kan være en svart boks eller et program på en datamaskin.

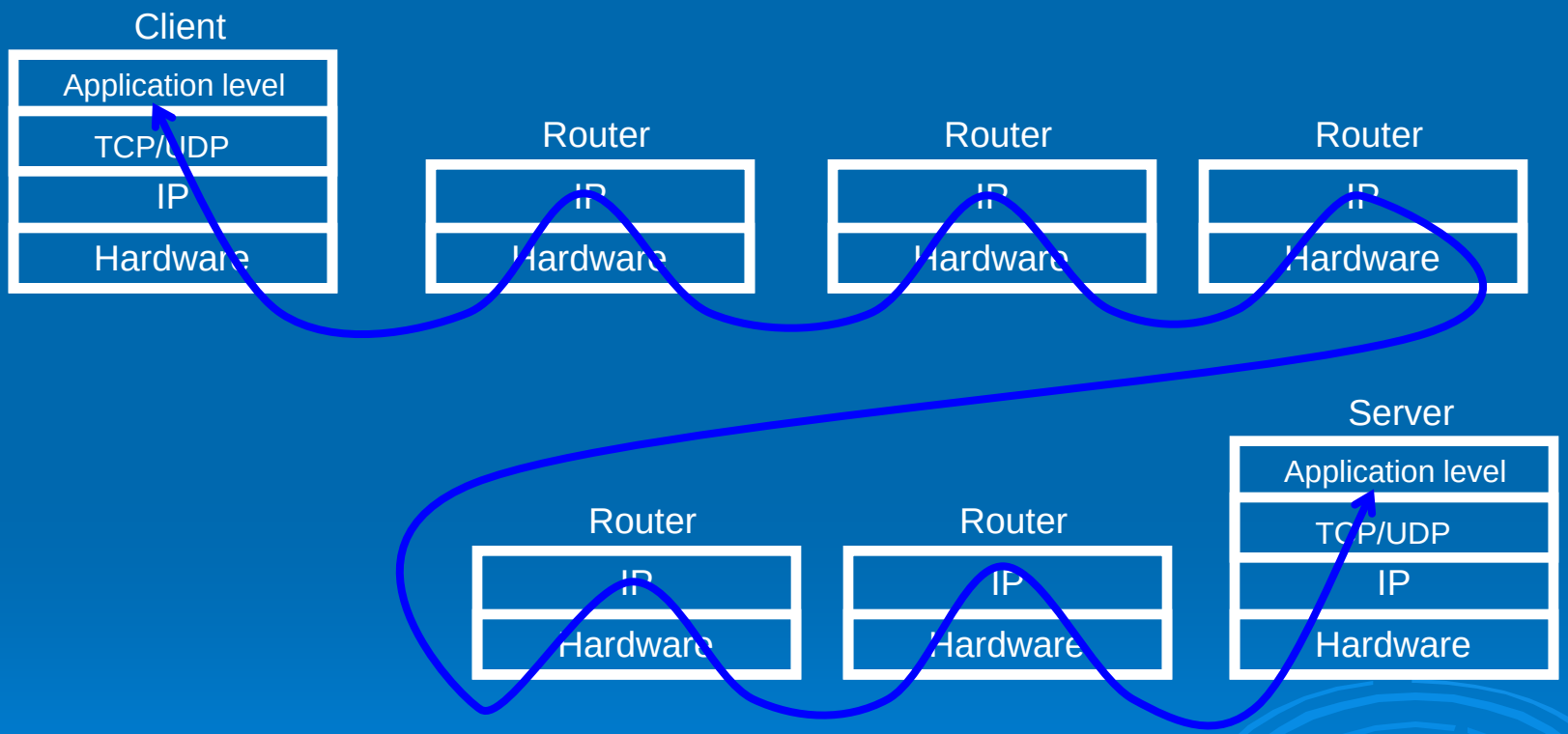
TCP/IP lagmodell



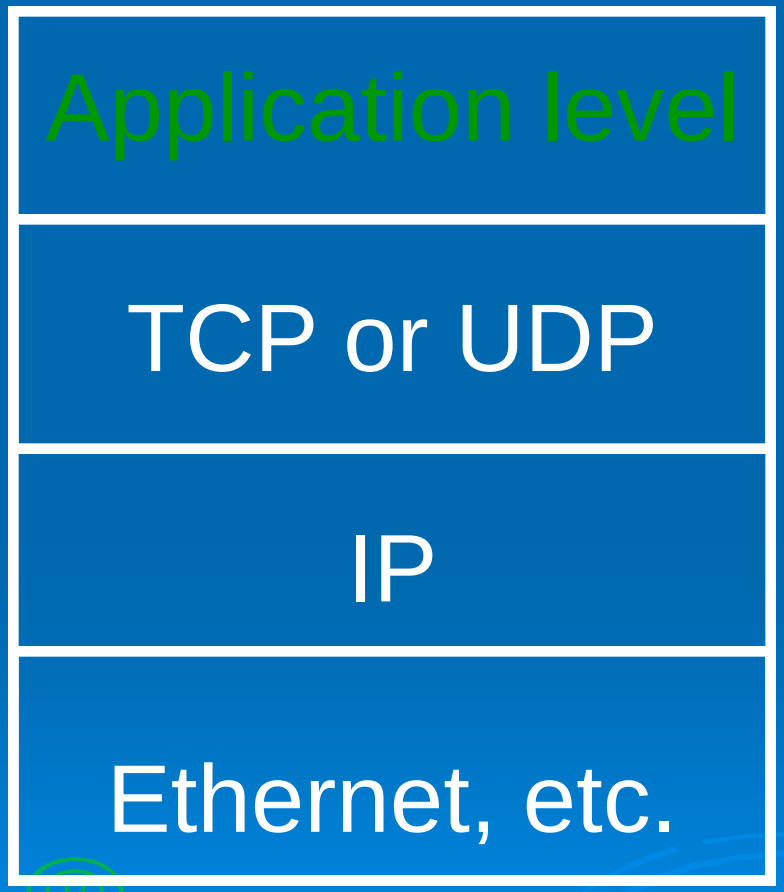
TCP/IP applikasjonslag



Ruting av applikasjonsprotokoll

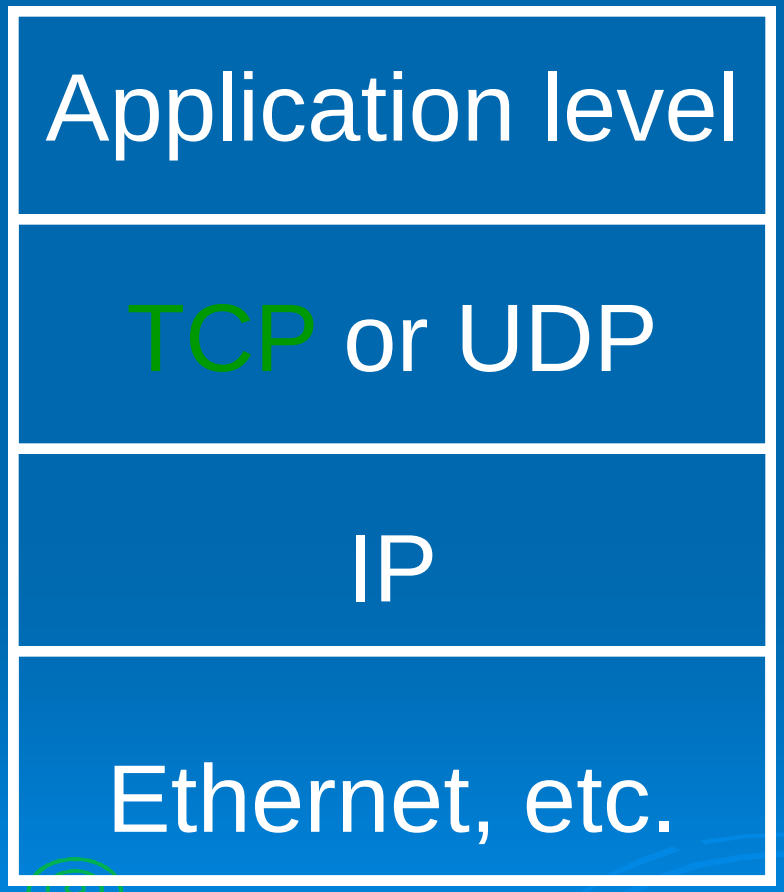


Applikasjonslag



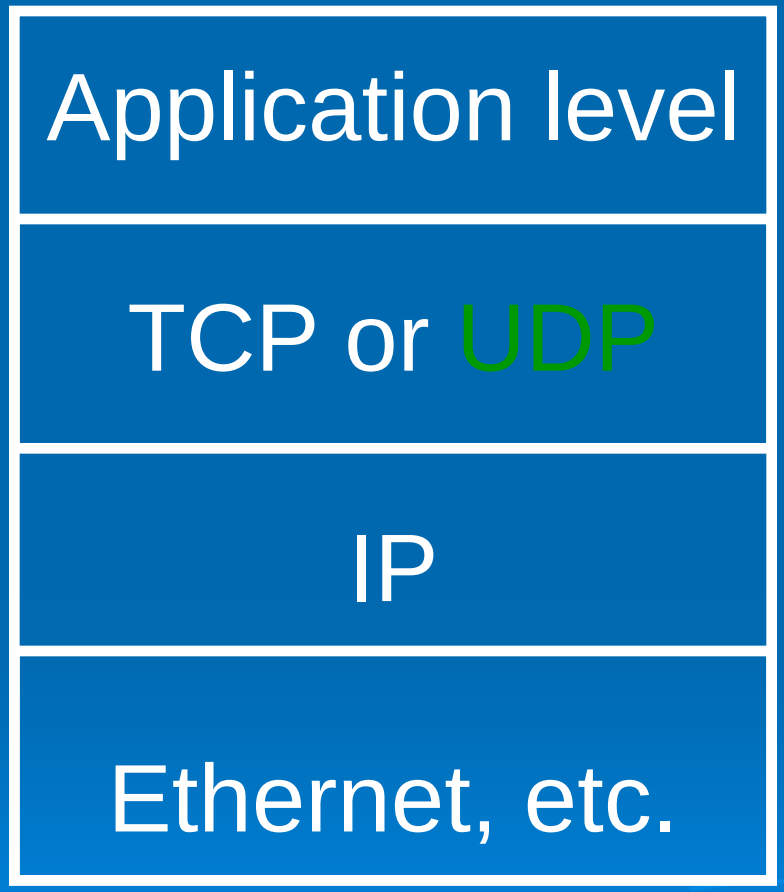
- Kommunikasjon til et annet system, som oftest klient/tjener basert
- Eksempel
  - SMTP, POP3, IMAP (mail)
  - telnet, rlogin (login)
  - HTTP (web access)
  - DNS (name service)
  - RIP, BGP4, OSPF (routing)
  - NFS, SMB (network file access)
- Hvem som helst kan lage sin egen protokoll mellom to systemer.

TCP



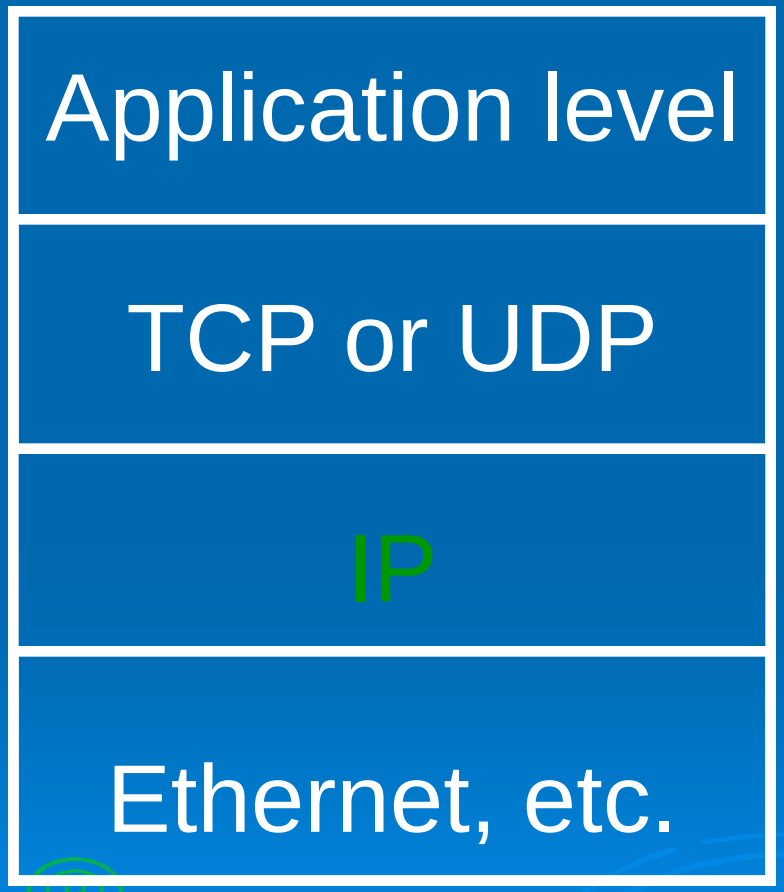
- TCP tilbyr en pålitelig og feilfri forbindelse mellom sender og mottaker
- Setter opp forbindelse mellom klient og tjener
- Sender bryter ned datastrømmer til pakker
- Mottaker setter sammen pakker til datastrøm
- Tjeneste porter 1 – 65535
  - 1-1024 er priviligerte porter

UDP



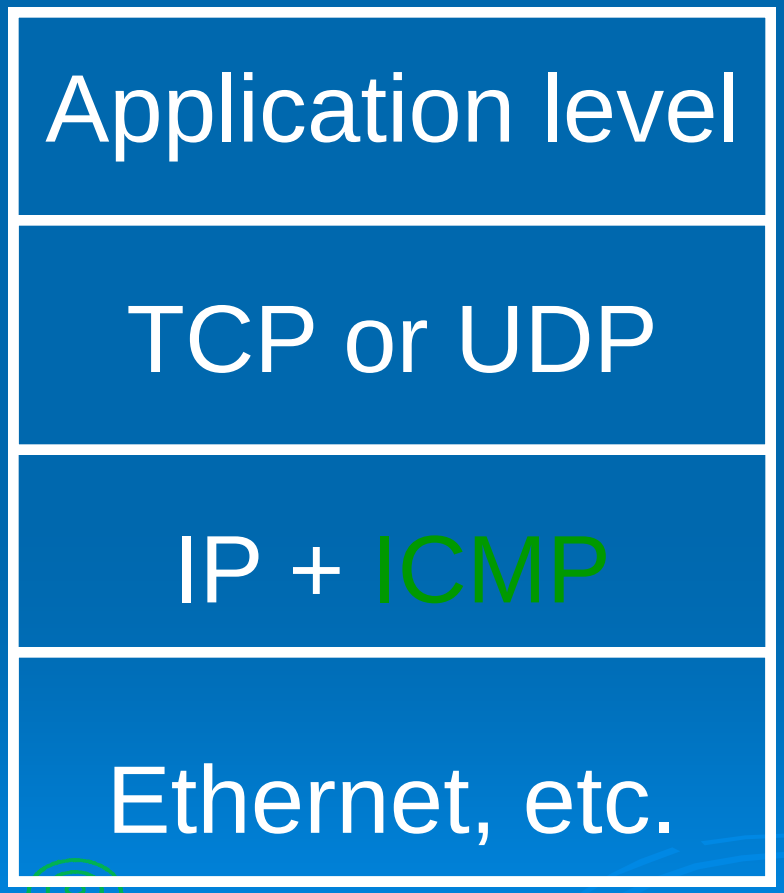
- Forbindelsesløse meldinger
- Ingen feil korrigering
- Ingen flyt kontroll
- Passer for noen nettverkstjenester som benytter få meldinger for kommunikasjon
- Tjeneste portnummer
  - 1-65535
    - 1-1024 er priviligerte porter
- UDP's forbindelsesløse natur gjør protokollen farlig sett fra et sikkerhetsmessig synspunkt

IP



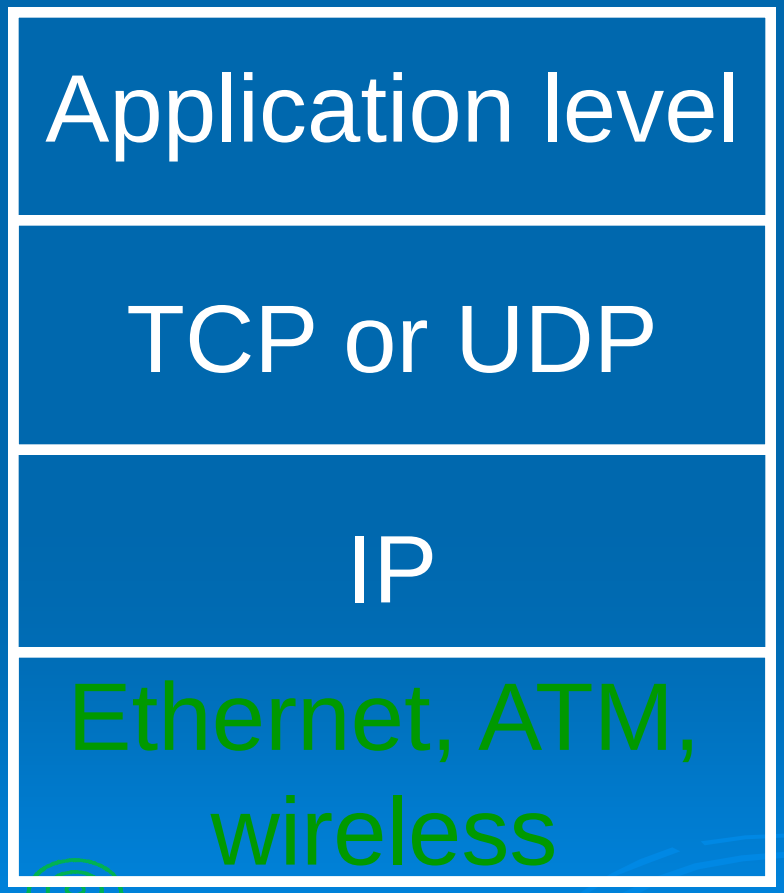
- En forbindelsesløs upålitelig datagram tjeneste
- Adressering med IP nummer
- Ingen garanti for at senderadressen er riktig
- Pakker har begrenset størrelse
- Pakker kan forkastes av nettverket underveis
- Pakker kan ankomme mottaker i uriktig rekkefølge
- IP/SEC gir sikker autentisering av sender og mottaker + evt. kryptering
- Kan tunneleres

ICMP



- Tilbyr diverse kontoll og andre funksjoner:
  - *ping* (echo request)
  - *ping* svar (echo reply)
  - TTL time exceeded, benyttes av *traceroute*
  - source quench (TCP only) for flow control
  - net unreachable
  - host unreachable

Hardware nivå



- Kan avlyttes(sniffing) når på samme nettverk.
- Nettverksmonitorer følger med OS som et feilsøkingsverktløy

IP

- IP pakke inneholder følgende informasjon benyttet ved pakkefiltrering
  - IP kildeadresse
  - IP destinasjonsadresse
  - IP protokoll type
    - TCP, UDP eller ICMP
  - IP opsjoner
- IP fragmentering
  - Kan skape problemer for pakkefiltrering

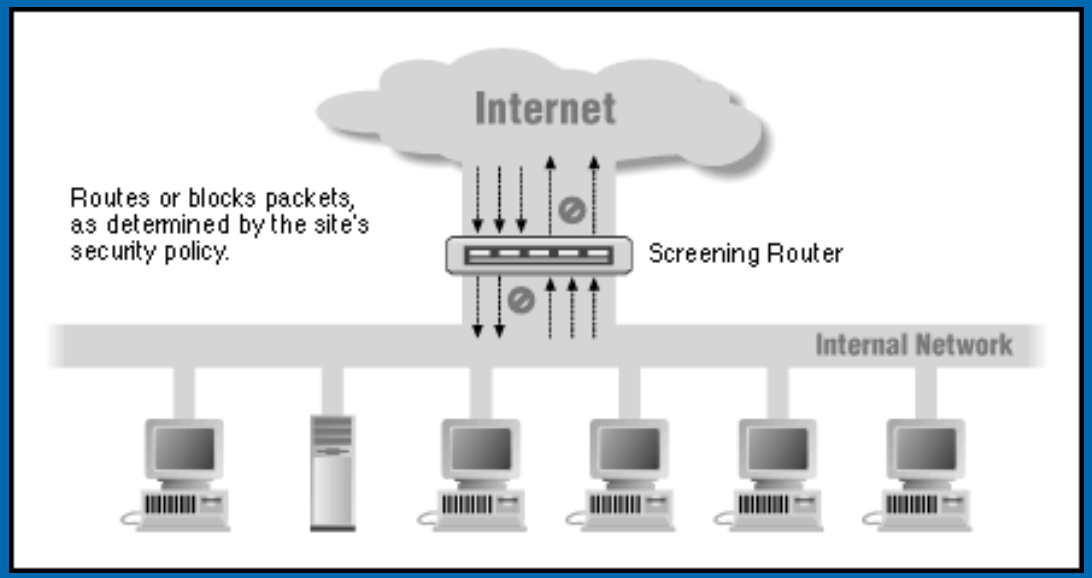
TCP

- TCP benyttes av mange tjenester
  - HTTP, SMTP, FTP, NNTP, SSH etc.
- Kilde port og destinasjons port benyttes v/filtrering
- ACK og SYN biter viktige i forbindelse med oppsett av TCP forbindelse
  - 3-way handshake
  - ACK=0 kjennetegner første oppkobling av TCP forbindelse
  - Alle andre TCP meldinger har ACK=1
  - Kan benyttes i pakkefiltrering for å hindre oppkoblinger

UDP

- Kjennetegn:
  - Lav overhead,
  - Forbindelsesløs, alle pakker er selvstendige
  - Ingen leveringsgaranti
  - Kilde port og destinasjons port benyttes v/filtrering

Pakke filtrering



- Pakkefiltrering utføres av ruter/host
  - Kontroll av alle utgående og innkommende pakker

Pakke filtrering

- Pakkeinformasjon som benyttes ved filtrering
  - IP kildeadresse
  - IP destinasjonsadresse
  - Protokolltype (TCP, UDP,ICMP)
  - TCP/ UDP kildeport
  - TCP/ UDP destinasjonsport
  - ICMP meldingstype
  - Pakkestørrelse
- Annen informasjon som har betydning
  - Hvilket nettverkskort som pakken kommer inn på og hvilket nettverkskort pakken vil forlate systemet på

Pakke filtrering

- Tilstandsfull (stateful) pakke filtrering
  - Filtreringen kan ta hensyn til historiske data, dvs. systemet ”husker” om en innkommende pakke kan være svaret på en pakke som tidligere har forlatt systemet
  - Systemet tar vare på historiske data en viss tid, deretter forkastes disse

Pakke filtrering

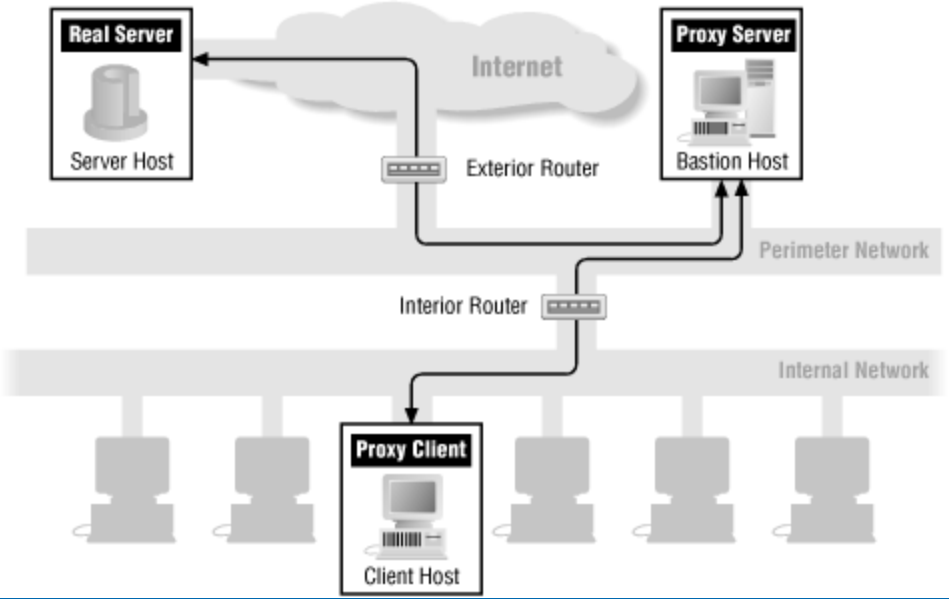
- Pakkefiltrering resulterer i følgende
  - Pakken videresendes
  - Pakken forkastes, ingen melding tilbake til mottaker
  - Pakken forkastes, send en feilmelding tilbake til avsender (Reject)
  - Log informasjon om pakken
  - Sett opp alarm, varsling

Filtrering fordeler & ulemper

- Fordeler
  - En pakkefiltrerende ruter kan beskytte et helt nettverk
  - Enkle pakkefiltre er effektive
  - Lett tilgjengelig på rutere og datasystemer
- Ulemper
  - Ytelse på ruter avtar
  - Filtreringsverktøy vanskelig å benytte, regler vanskelig å konfigurere
  - Ønsket sikkerhetspolitikk kan ikke alltid bli utført av pakkefiltrerings rutere

HØGSKOLEN I NARVIK

DMZ (Perimeter network)

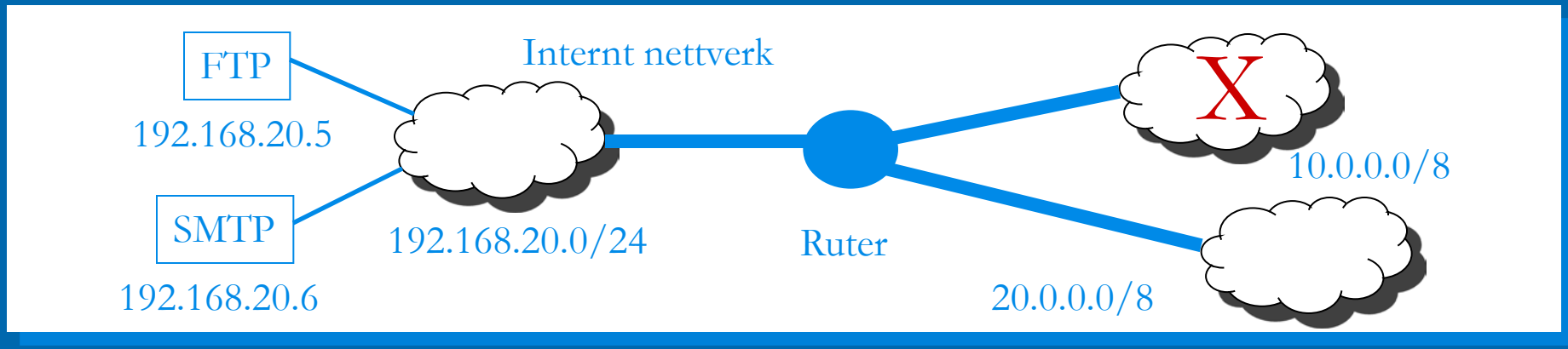


- Benytter flere forsvarsverk
  - Perimeter network mellom ytre og indre nett
  - Systemer som skal tilby tjenester mot Internett settes opp på dette nettverket som bastion hosts (ekstra sikkert system)

Pakkefiltrering

- **Konfigurering av pakkefilter:**
  - Ha en veldefinert sikkerhetspolitikk som forteller hva som skal tillates og hva som ikke tillates
    - Dersom en ikke har en sikkerhetspolitikk vil innføringen av en brannmur medføre at en sikkerhetspolitikk må etableres
    - Trusselvurdering/risikoanalyse definerer nivå for sikkerhet som er nødvendig
    - Sikkerhetspolitikk må dokumenteres
  - Regler for pakkefiltrering må legges inn på brannmur i språk som denne benytter og testes
    - Uttesting av politikk ofte vanskelig

Pakke filtrering eksempel



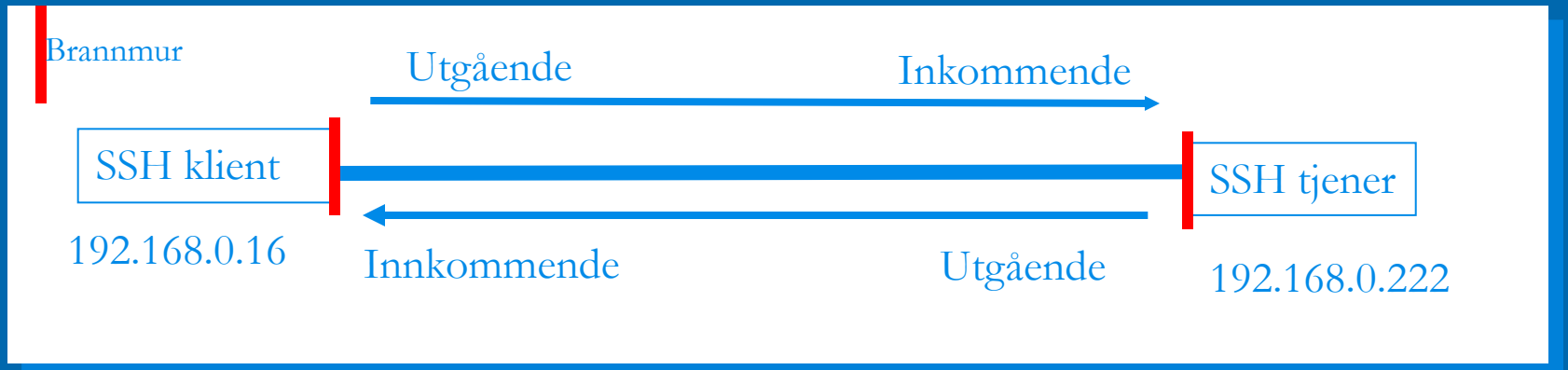
Typiske regler for pakkefiltrering

Type	Src. Addr	Src Port	Dest. Add	Dest Port	Action
tcp	10.0.0.0/8	*	*	*	DENY
tcp	20.0.0.0/8	*	192.168.20.5	20	ALLOW
tcp	20.0.0.0/8	*	192.168.20.6	25	ALLOW
tcp	192.168.20.6	25	*	*	ALLOW

Pakkefiltrering

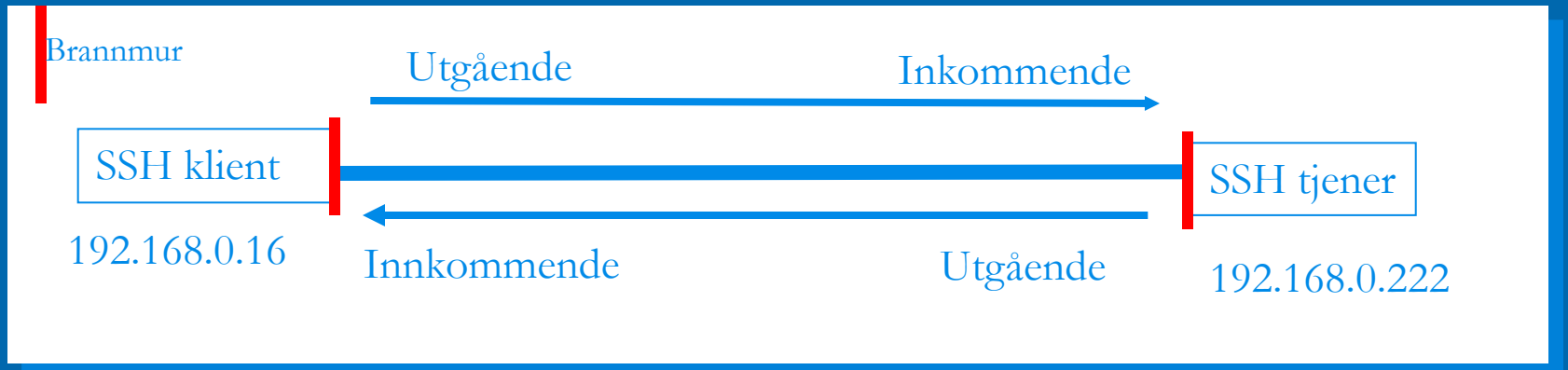
- Filtrering basert på IP adresse
  - Enkelt
  - Fare for falsk IP adresse begrenser bruk
  - Benyttes oftest for filtrering av pakker med interne adresser som kommer inn utenfra
- Filtrering basert på tjenestetype
  - Noe mer komplisert, må kjenne til virkemåte for tjeneste/protokoll som benyttes

Pakke filtrering SSH eksempel



- Kommunikasjon SSH klient og SSH tjener
  - Klienten kontakter tjeneren, dette genererer utgående pakker fra SSH klienten
    - Kjennetegn:
      - IP kilde 192.168.0.16
      - IP destinasjonsadresse 192.168.0.222
      - TCP protokoll,
      - TCP destinasjonsport 22,
      - TCP kildeport er tilfeldig >1023,
      - Første pakke vil ikke ha ACK bit satt

Pakke filtrering SSH eksempel



- Kommunikasjon SSH klient og SSH tjener
  - Svaret fra tjeneren
    - Kjennetegn:
      - IP kilde 192.168.0.222
      - IP destinasjonsadresse 192.168.0.16,
      - TCP protokoll,
      - TCP kildeport 22,
      - TCP destinasjonsport tilsvarende som for utgående pakke,
      - ACK bit satt

IPTABLES

- IPTables / NetFilter er tilsvarende IPChains i kosept og syntaks.
- Fungerer med Linux Kernel 2.0 og høyere
  - Standard på de fleste distribusjoner basert på 2.4
- Har diverse fordeler over IPChains.

IPTABLES

Forbedringer:

- Har støtte for tilstandsfull pakke filtrering
- Har bedre egenskaper for inspeksjon av pakker
- Kan benyttes for MAC adresse filtrering
- Kan begrense trafikkmengde
- Kan filtrere på pakkeinnhold

Pakke filtrering

IPChains/IPtables (Netfilter)

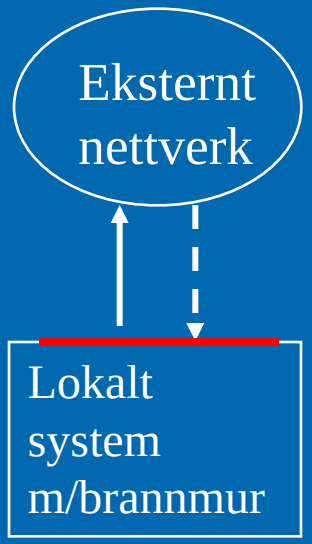
- Chains er lister med regler.
- 3 standard kjeder (chains), egne kjeder kan.
- Beskrivelse:
  - INPUT – For alle pakker beregnet for det lokale systemet vil Linux kjernen bestemme dens videre skjebne basert på regler i denne kjeden.
  - FORWARD – For alle pakker som skal videresendes vil FORWARD kjeden benyttes for filtrering.
  - OUTPUT – For lokalt genererte pakker vil regler i OUTPUT kjeden avgjøre deres videre skjebne.

Tilstandsfull pakke filtrering

- Brannmur beholder informasjon om forbindelser i minne
  - Kan tillate trafikk basert på hva som har skjedd tidligere
    - state NEW – tillater nye oppkoblinger
    - state ESTABLISHED – tillater trafikk basert på at oppkoblingen allerede har funnet sted
    - state RELATED – tillater relatert trafikk basert på at oppkoblingen har funnet sted
  - Enkelt for TCP pga. den er forbindelsesorientert
  - For en UDP forbindelse, benytter timeouts, en forbindelse huskes en begrenset tid

Tilstandsfull pakke filtrering eksempel

- Tillat nye oppkoblinger fra lokalt system med svar tilbake.
- Ingen oppkoblinger utenfra tillates

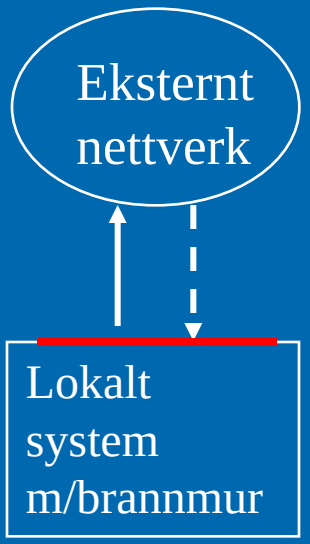



```
iptables -P INPUT DROP    // DROP alt som standard
iptables –P OUTPUT DROP

## Tillatt ny trafikk ut og kun relatert og etablert trafikk inn til lokalt system

iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

IPTABLES eksempel

- Kun Web trafikk
  - Tillater utgående webforespørsler fra nettleser og innkommende svar fra webtjener
  - Web karakteristikk:
    - Webtjener port 80, webklient benytter port >1023

```
iptables -A OUTPUT -p tcp --destination-port 80 \
   -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -p tcp --source-port 80 -m state --
   state \
   ESTABLISHED,RELATED -j ACCEPT
```



IPTABLES regler

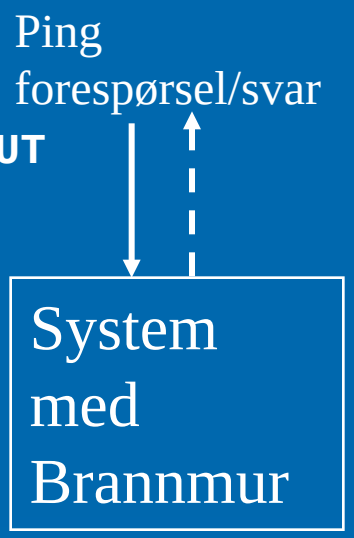
- Regler i kjeder gjennomgås fra topp til bunn, stopp ved match på kriterier
  - Rekkefølgen på regler meget viktig !
- Anbefalning:
  - Sett standard for alle kjeder til å være DROP
    - Dette stenger systemet helt
  - Deretter åpner en for den trafikk som skal tillates
    - Mest benyttede protokoller (for eksempel http) bør komme først i listen

HØGSKOLEN I NARVIK

Eksempel – PING

PING skal tillates ut fra lokalt system med svar tilbake, all annen trafikk forkastes

Her benyttes kun INPUT og OUTPUT kjedene




```
## Sett standard politikk til å være DROP for INPUT og OUTPUT kjedene

# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
```

Nå slipper vi ut ICMP pakkene som ping genererer, dette gjøres ved å legge til en regel i OUTPUT kjeden der vi spesifiserer at ICMP protokollen tillates ut.

```
# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
```

For at ping skal virke må vi også slippe inn svaret på pakkene fra det systemet vi sendte forespørselen til. Dette kan vi gjøre på følgende måte:

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

`iptables` flags

Flag	Beskrivelse
- t table	Angir tabell, filter, nat eller mangle
-A	Legger til regel
-D	Sletter regel
-F	Flush alle regler
-I	Setter inn regel
-L	Skriver ut regler
-N	Lager nye kjede
-P	Angir standard politikk for en kjede
-R	Erstatter regel
-X	Sletter kjede med regler

`iptables` opsjoner

Opsjon	Beskrivelse
`-d address[/mask]`	Angir destinasjons IP adresse/nett, kan angi DNS navn
`-i navn`	Inkommende nettkort navn
`-o navn`	Utgående nettkort navn
`-j target`	Spesifiserer mål for en regel
`-p protocol`	Angir protokol, kan være tcp, udp eller icmp
`-s address[/mask]`	Angir kilde IP adresse/nett, kan angi DNS navn
`-m match`	match kan være **`mac`, `limit`, `mark`, `owner`, `state`, `unclean` eller `tos`.**
`-v`	Verbose output, viser mer informasjon ved listing av regler

`iptables` protokoll filtrering

Protokoll	Match extension	Beskrivelse
`-p tcp`	`--sport [!] port[:port]`	Angir kildeport, enkel port eller område for eksempel 0:1023. Kan angi navn fra /etc/services, ! benyttes for utelukkelse av porter
	`--dport [!] port[:port]`	Angir destinasjonsport, spesifikasjon som over
	`--tcp-flags mask comp`	Angir hvilke TCP flagg som skal undersøkes. mask angir hvilke flagg som skal undersøkes, comp angir hvilke flagg av disse som må være satt
	`[!]--syn`	Tilsvarer `--tcp-flags SYN,RST,ACK SYN`
`-p udp`	`--sport [!] port[:port]`	Angir kildeport, spesifikasjon som over for tcp
	`--dport [!] port[:port]`	Angir destinasjonsport, spesifikasjon som over for tcp
`-p icmp`	`--icmp-type type`	Angri hvilke ICMP meldingstyper som skal undersøkes

`iptables` match tillegg

match extension	Opsjon	Beskrivelse
`-m mac`	`--mac-source [!] adresse`	Angir MAC adresse
`-m limit`		Benyttes for å begrense antall treff mot en regel, benyttes for å forhindre DoS angrep og logging. Standard er 3 pr. time.
	`--limit rate`	Kan angi egen grense for eksempel 1/s er 1 pr. sekund, standard er 3/h
`-m state`	`--state state`	`Benyttes ved tilstandsfull filtrering, verdier er INVALID, ESTABLISHED, NEW, RELATED`

`iptables` aksjoner

Aksjon	Beskrivelse
`ACCEPT`	Tillat pakke
`DROP`	Forkast pakke uten ICMP melding
`REJECT [--reject-with opsjon]`	Som DROP, men sender ICMP pakke til avsender med feilkode
`MASQUERADE [--to-ports port]`	Kun i `nat/POSTROUTING` kjeden og ved bruk av DHCP, oversetter kildeadresse med adresse for utgående nettkort.
`DNAT –to-destination ipaddr`	Benyttes kun i `nat/POSTROUTING` og `nat/OUTPUT` kjeden. Erstatter destinasjons IP på pakkene.
`SNAT –to-destination ipaddr`	Benyttes kun i `nat/POSTROUTING` kjeden. Erstatter kilde IP på pakkene.
`LOG [–log-prefix ”string”]`	Logging av pakker via syslogd

iptables-save & iptables-restore

- iptables-save
  - Benyttes for lagring av regler som er aktive, lagrer alle tabeller og kjeder
  - F.eks:

```
iptables-save > /etc/iptables.up.rules
```

- iptables-restore
  - Leser lagrede regler og aktivere disse
  - F.eks:

```
cat /etc/iptables.up.rules | iptables-restore
```

iptables
Aktivering ved oppstart

- Ubuntu
  - Lagre reglene som beskrevet til filen **/etc/iptables.up.rules**
  - Legg inn følgende i filen **/etc/network/interfaces**

```
pre-up iptables-restore < /etc/iptables.up.rules
```

- Fedora/RedHat
  - Regler lagres til **/etc/sysconfig/iptables**
  - Sjekk at tjenesten iptables er aktivert ved oppstart

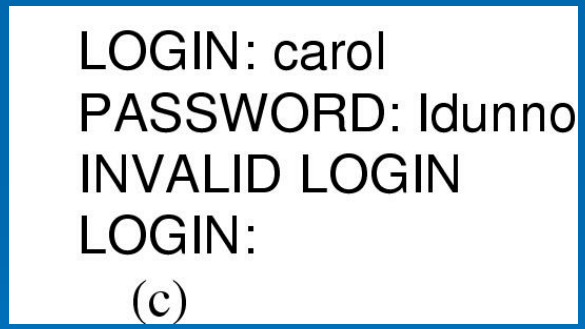
User Authentication

Basic Principles. Authentication must identify:

1. Something the user knows
2. Something the user has
3. Something the user is

This is done before user can use the system

Authentication Using Passwords



(a) A successful login

(b) Login rejected after name entered

(c) Login rejected after name and password typed

Authentication Using Passwords

```
LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uucp
PASSWORD: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL
```

- How a cracker broke into LBL
  - a U.S. Dept. of Energy research lab

Authentication Using Passwords

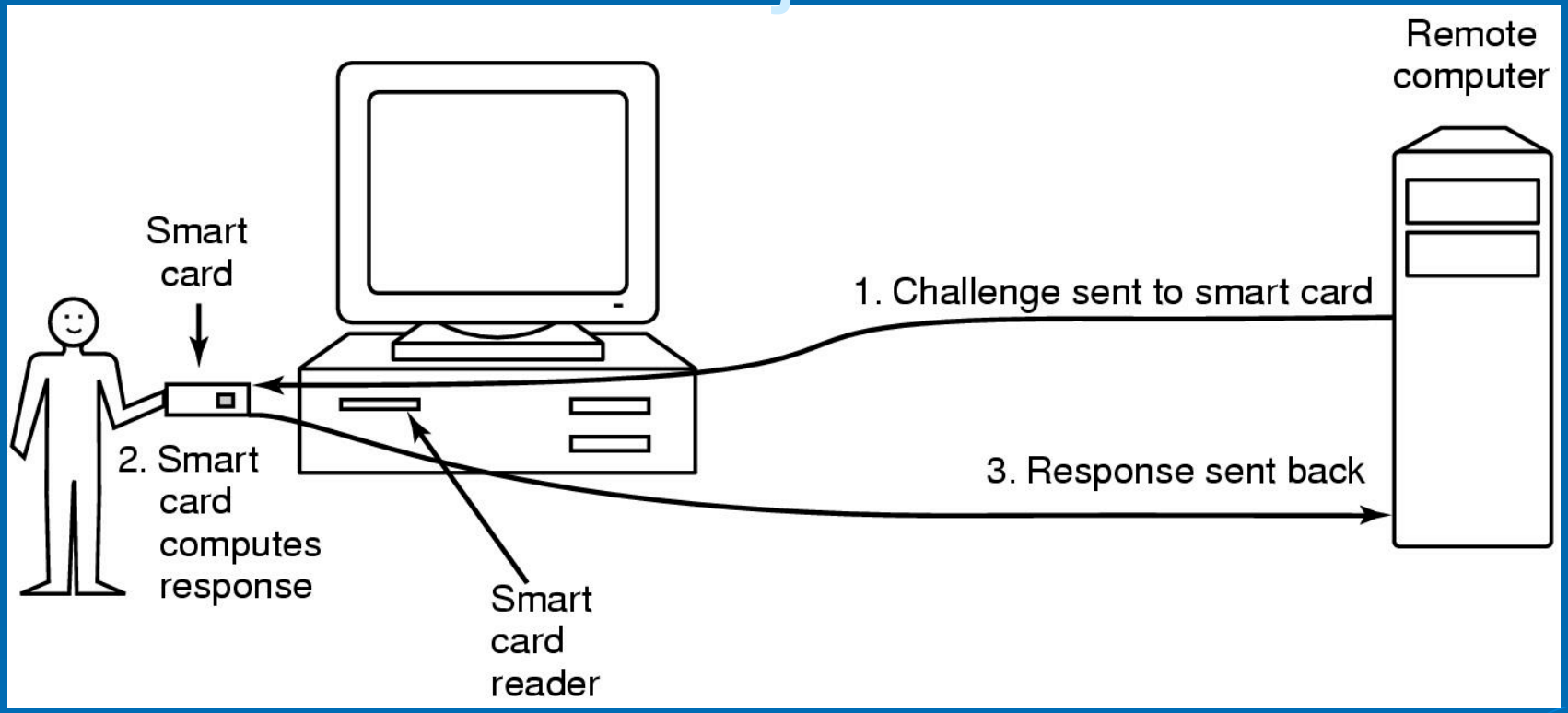
Bobbie, 4238, e(Dog4238)
Tony, 2918, e(6%%TaeFF2918)
Laura, 6902, e(Shakespeare6902)
Mark, 1694, e(XaB@Bwcz1694)
Deborah, 1092, e(LordByron,1092)

Salt

Password

The use of salt to defeat precomputation of encrypted passwords

Authentication Using a Physical Object



- Magnetic cards
  - magnetic stripe cards
  - chip cards: stored value cards, smart cards

Passord anbefalinger

- Minst 8 karakterer langt, helst >=16 på Windows
- Ikke bruke ord fra ordliste
- Bruke små og store bokstaver, tall og tegn i en kombinasjon
- Eks: Don.2-ald
- NB! Skriv aldri ned passordet

Tiltak for bedre passord

- Tidsbegrensning på passord
- Minimum lengde
- Historieliste over bruker (logg)
- Bruker får ikke velge tidligere valgte passord
- Analyse av passord mulig; forkaster for lette passord
- Genererte passord, OPSYS tilbyr vanskelige passord til brukerne

HØGSKOLEN I NARVIK