



Etablering av pakkefilter

UNINETT2004

17 Juni 2004

Per Arne Enstad

Rune Sydskjør

# Ting som må tas hensyn til ved etablering av pakkefilter

- 1. Nettsegmentering
- 2. Pakkefilter/brannmur
- 3. Endesystemsikkerhet

# Hva mener vi med nettsegmentering?

- Identifisere objekter med tilnærmet like behov for sikring
  - ◆ Objekter = brukere, tjenere..
- Organisere objektene i separate nett
  - ◆ Kompromiss – ”you gain some, you loose some..”

# Hva mener vi med nettsegmentering? (2)

- Vanlig organisering i UH-sektoren:
  - ◆ Administrasjonsnett
  - ◆ Ansattnett (aka fagnett)
  - ◆ Studentnett

# Data pakke

- Hver enkelt datapakke består av et hode og en kropp .
- Hodet inneholder informasjon som er egnet til å identifisere avsender, mottaker samt en del andre ting.
- Kroppen representerer selve nytteinnholdet i pakken.

# Hva er pakkefiltrering?

- Pakkefiltrering skjer ved inspeksjon av pakkehodet. Ut fra innholdet av denne kan filteret bestemme skjebnen til pakken (=forkast/videresend)
- Avanserte brannmurer ser gjerne på nytteinnholdet i pakken i tillegg til pakkehodet når pakkens skjebne skal avgjøres

# Protokoller/porter

- En tjeneste er bundet opp/lytter på en port
- De vanligste tjenestene bruker transportprotokollene tcp eller udp  
Noen kan bruke begge.
- En webserver lytter for eksempel (normalt) på port 80/tcp.

# Noen vanlige porter

- 22            ssh            tcp            ssh
- 25            smtp           tcp            sende mail
- 53            dns            udp/tcp       navneforespørsler
- 67/68        dhcp           udp            auto tildeling ip
- 80            web            tcp            web-surfing
- 110           pop3           tcp            henting mail
- 123           ntp            udp            network time prot.
- 135-139,445  
                 netbios    tcp/udp       windows nettverk
- 143           imap           tcp            henting mail
- 443           https          tcp            kryptert surfing

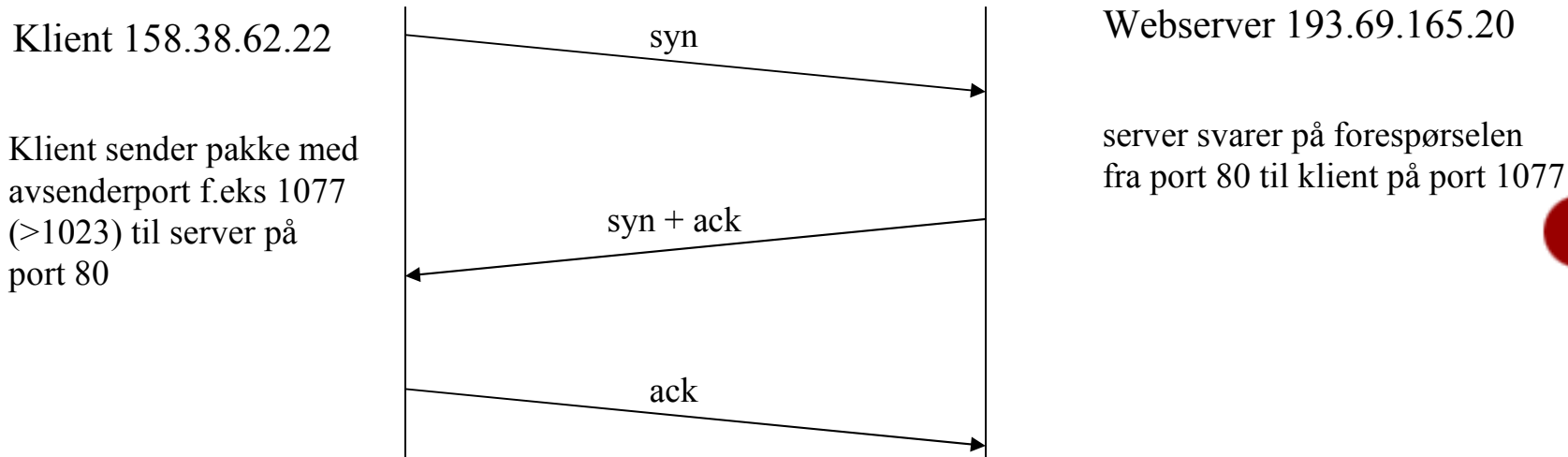
# udp

- Forbindelsesløs
- Kan sammenlignes med det å sende et brev. Man sender ut en pakke, og forventer at den kommer frem. Du har imidlertid ingen garanti for at dette skjer. Forhåpentligvis får du svar...
- Upålitelig

# tcp

- Forbindelsesorientert
- Kan sammenlignes med en telefonsamtale, der det opprettes kontakt før man begynner å utveksle data, og at man hele tiden hører/vet at motparten er med.
- Pålitelig - det finnes mekanismer for å detektere at pakker mistes, for deretter å få disse sendt om igjen

## tcp 3-way handshake (rune surfer www.vg.no)



Avsender		Mottaker		flagg
Ip	Port	Ip	Port	
158.38.62.22	1077	193.69.165.20	80	syn
193.69.165.20	80	158.38.62.22	1077	syn+ack
158.38.62.22	1077	193.69.165.20	80	ack

# Brannmur versus pakkefilter

- Med tcp har man mulighet for etablere en "established" regel i pakkefilteret. "Established" innebærer returtrafikk på sesjoner som er etablert fra innsiden får passere uhindret.
  - ◆ "Established" godtar pakker med TCP ACK- eller RST flagg satt.
- Ved stateful inspection vedlikeholder ruter/brannmuren en oversikt over trafikk som går igjennom i den ene retningen (src-IP, src-port, dst-IP, dst-port), og slipper igjennom tilhørende pakker i den andre retningen.
- Den største fordel med separate brannmurer er at de foretar innholdsinspeksjon. De ser altså ikke bare på pakkehodet.
  - ◆ Straffen er langsommere pakkehåndtering

# Policy ved pakkefilter

- Pakkefiltere kan etableres i både inn- og utgående retning på hvert av interfascene i ruterer.
- Det hender vi stenger utgående SMTP for alle maskiner unntatt registrerte MTA'er for å unngå spam. Det samme gjelder SMB/CIFS/Netbios for å unngå at infiserte maskiner "støyer" på nettet. Dette vha. enkle pakkefilter på trafikk ut fra høgskolene mot omverdenen.
- På trafikk inn mot høgskolene har vi som regel generelle filtere som nekter adgang for SMB/CIFS/Netbios. I tillegg er det ofte egne spesialdefinerte pakkefilter på hvert VLAN

## Policy ved pakkefilter(2)

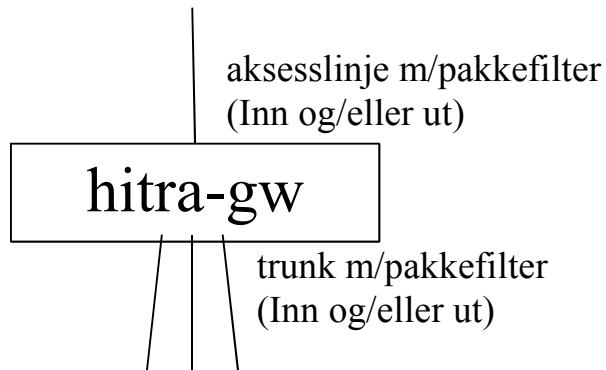
- Adm nett bør ha stengt ende og kan ha full tilgang til fag og stud.
- Fag bør ha stengt ende og kan ha full tilgang til stud
- Stud har som regel hatt åpen ende frem til i dag. Trenden endrer seg derimot her, pga av sterk økning i innbrudd og støy fra kompromitterte maskiner.

# Forberedelser

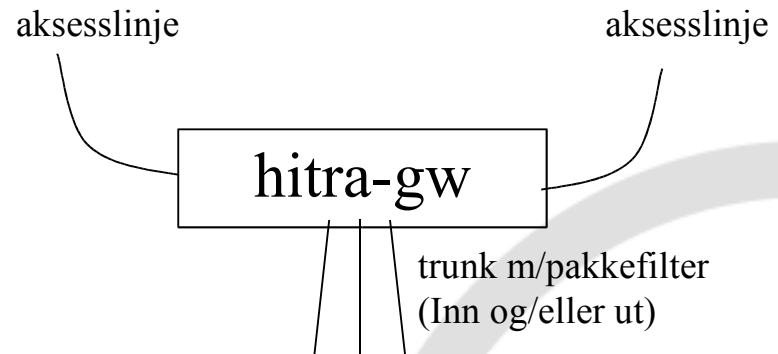
- Skaffe oversikt over nett/tjenester
- Hva skal vi beskytte/risikovurdering
- Arbeidsmengde/nytteverdi
- ”Litt hjelper mye ”(f.eks ved å stenge NetBIOS/SMB/CIFS til og fra omverden)

# Eksempel på nett

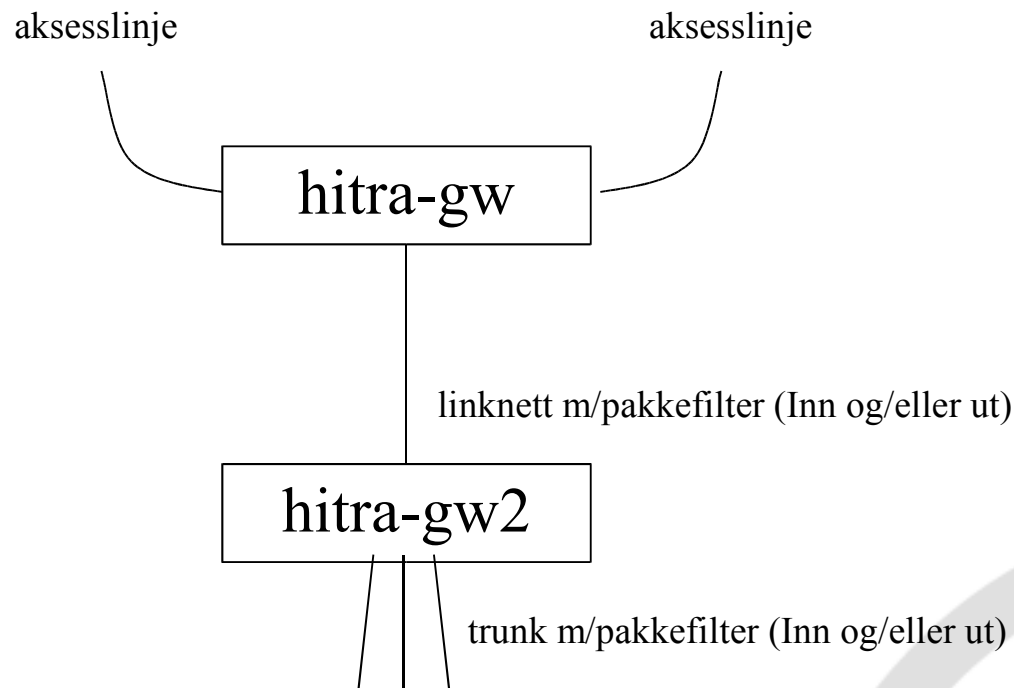
Tradisjonelt:



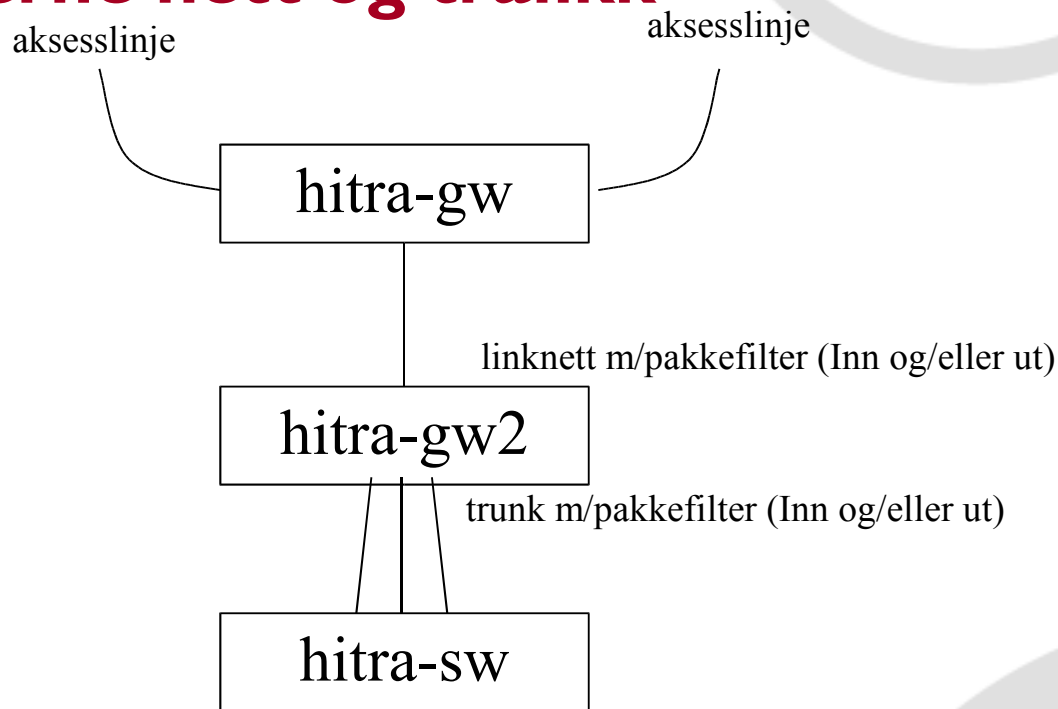
Dagens situasjon  
(mellomfase):



# Gigacampus type løsning



# Interne nett og trafikk



18

- Trafikk mellom maskiner på forskjellige interne nett går via ruter og pakkefilter på vlan-interfacene.
  - ◆ "Trombone-effekten"
- Trafikk mellom maskiner på samme nett går bare via svitsj, og blir dermed ikke berørt av pakkefiltrene.

# Generelt om pakkefilter

- Traverseres sekvensielt – starter på toppen og fortsetter nedover til ”treff”
- Med en gang en regel i lista ”treffer” blir pakken enten rutet eller kastet avhengig av regel (permit/deny), og traverseringen slutter.
- To typer sikkerhetsfilosofier:  
Alt som ikke eksplisitt er tillatt er nektet (deny ip any any tilslutt)  
Alt som ikke eksplisitt er nektet er tillatt. (permit ip any any tilslutt)  
Disse kan selvsagt kombineres.

# access lists format

- access-list [list number] [permit|deny] [protocol] [source spec.] [destination spec.] [protocol qualification] [logging]
- protocol: ip/tcp/udp/icmp++ (navn eller nummer)
- source spec.: [ip address][wildcard mask][port number spec. (bare for tcp og udp)]
- destination spec.: [ip address][wildcard mask][port number spesification (bare for tcp og udp)]
- ip address: ip-adresse brukt til sammenligning
- wildcard mask: valgfri for å angi flere ip-adresser

## access lists format (2)

- port number spec.: valgfri felt som brukes til å angi portnummer (eq/lt/gt/range)
- protocol qualifiers: protokoll spesifikke ting. (f.eks echo for icmp og established for tcp)
- logging: for å logge pakkeinformasjonen for en pakke. Veldig nyttig til oppbygning av lister.
- Appliseres på interface slik:  
interface FastEthernet0/0  
    ip access-group <number> out|in

# Wildcard

- Med subnettmaske er vi ute etter å finne nettverksnummer
- Med wildcard i access-lister er vi ute etter å finne alle host'er i det nettet
- Et nett med ip og maske 158.38.60.0 255.255.255.0 vil defineres som ip og wildcard 158.38.60.0 0.0.0.255 i en accessliste
- Et nett med ip og maske 158.38.60.0 255.255.255.192 vil defineres som ip og wildcard 158.38.60.0 0.0.0.63 i en accessliste
- 158.38.60.10 255.255.255.255 = host 158.38.60.10
- 0.0.0.0 255.255.255.255 = any
- Bruk "ip-kalkulator" dersom du er usikker  
Eks. <http://jodies.de/ipcalc>

# Fremgangsmåte

- Legg inn innslag på de tjenester du vet skal gå. Godkjente tjenester.
- Lag en 'permit ip any any' regel til slutt som logger(syslog-server anbefales!)
- Nå vil du få logg over de tjenester du ikke har redegjort for ovenfor.
- Se i logg og utvid lista over godkjente tjenester. De vil da ikke komme i loggen.
- Etter hvert har du redegjort for all godkjent trafikk du vil skal kunne gå, og du kan bytte ut 'permit ip any any' med 'deny ip any any'.

# Veldig enkelt starteksempel

source spec.: destination spec. prot.quali/log

**! Først fjerne innslag som ligger inne fra før.**

no access-list 104

**! Tillat svar på sesjoner initiert innenfra**

access-list 104 remark Tillat svar på sesjoner initiert innenfra

access-list 104 permit tcp any any gt 1023 established

**! Tillat navneforespørslers til 10.0.0.1(resolver)**

access-list 104 permit udp any host 10.0.0.1 eq 53

access-list 104 permit tcp any host 10.0.0.1 eq 53

**! Tillat svar på navneforespørslers fra 10.0.0.1 til andre dns-servere**

access-list 104 permit udp any eq 53 host 10.0.0.1 eq 53

access-list 104 permit udp any eq 53 host 10.0.0.1 gt 1023

**! Tillat icmp utenfra**

access-list 104 permit icmp any any

**! Tillat traceroute utenfra (90 porter)**

access-list 104 permit udp any any range 33434 33523

**! Tillat resten med logg**

access-list 104 permit ip any any log-input

## Fremgangsmåte (2)

- Dersom det er mye ”støy” under bearbeiding av pakkefilteret, kan det være lurt å nekte/tillate utvalgt trafikk før ”permit ip any any log-input”. Da slipper du at denne trafikken genererer logg.

25

	source spec.:	destination spec.	prot.quali/log
.....			
access-list 104 permit ettellerannet	ettellerannet		
<b>! Unngå logging av SMB/CIFS/NetBios som likevel skal nektes</b>			
access-list 104 deny tcp	any	any range 135 139	
access-list 104 deny udp	any	any range 135 139	
access-list 104 deny tcp	any	any eq 445	
access-list 104 deny udp	any	any eq 445	
<b>! Logg resten</b>			
access-list 104 permit ip	any	any	log-input

# Til slutt

- Ikke sperr for alle typer icmp, den kan inneholde viktig nyttetraffic.
- Du slipper ikke å tenke på endesystemsikkerhet selv om du har pakkefilter!!!
- Du kan klare deg uten pakkefilter/brannmur.
- Du kan ikke klare deg uten endesystemsikkerhet!!! Patch opp, overalt, alltid. 😊
- Pakkefilter må vedlikeholdes.

# Helt tilslutt

- [www.hih.no/uninett2004.....](http://www.hih.no/uninett2004.....)
- [rune.sydskjor@uninett.no](mailto:rune.sydskjor@uninett.no)
- [per.a.enstad@uninett.no](mailto:per.a.enstad@uninett.no)