FAGSPESIFIKASJON FRA UNINETT

BESTE PRAKSIS FOR PAKKEFILTRERING I UH-SEKTOREN

UFS nr.:	106
Versjon:	1
Status::	Godkjent
Dato:	20. 12. 2007
Tittel:	Beste praksis for pakkefiltrering i UH-sektoren
Arbeidsgruppe:	GC-sikkerhet
Ansvarlig:	Rune Sydskjør
Kategori:	Anbefaling

Sammendrag

Dette dokumentet skal gi en generell anbefaling på hvordan man bør filtrere datatrafikk til/fra sine interne nettverk. Filtreringen kan implementeres med pakkefilter i en ruter, eller ved regler i en brannmur. Ordet pakkefilter vil bli brukt for begge løsninger gjennom hele dokumentet. En eventuell egen oppskrift (som er beskrevet i egen UFS) vil beskrive filtreringen i detalj for leverandørspesifikke produkter. Dokumentet skal gi en vurdering av tiltak som kan benyttes, og beskrive ulemper/fordeler ved disse.

Innhold

1. Introduksjon

Forsøk på datainnbrudd, automatiserte eller manuelle skjer hver dag, og derfor er det viktig å sikre institusjonens ressurser mot tilgang fra uvedkommende.
Ved en stor institusjon er det ofte snakk om tusenvis av maskiner, og det er ofte slik at noen maskiner vil bli avglemt og dermed ikke patchet/oppdatert. Det viser seg ofte også at systemer som telefoni/låsesystemer/kassaapparat etc. er systemer som ikke kan patches pga. at de kun fungerer på gitte patchenivå. Slike systemer er det ekstra viktig å isolere med pakkefilter.
Det er viktig å merke seg at dette dokumentet inneholder et sett med anbefalinger og ikke krav. Målsetningen med dokumentet er ikke å være uttømmende, men å beskrive hovedtrekkene i oppbyggingen av pakkefiltre.

2. Forhåndskunnskap

Det forutsettes at man har forhåndskunnskap om TCP/IP og IP-baserte tjenester.

3. Pakkefilter i ruter versus brannmur

I utgangspunktet må man igjennom det samme arbeidet uansett hvilken løsning man velger for implementasjon av pakkefiltrering. Den samme kompetansen er nødvendig for å forstå reglene, og de samme beslutningene må taes på hvilke tjenester man skal tilby og hvilke man skal stenge. Brannmurer har som regel mer funksjonalitet enn pakkefiltrering på ruter, og er minst like komplisert å sette opp og vedlikeholde som pakkefilter på en ruter. Vi ser ganske ofte at innkjøpte brannmurer er konfigurert slik at den mest avanserte funksjonaliteten ikke blir utnyttet. Pakkefilter på ruter er derfor ofte tilstrekkelig, og mange kunne ha spart penger på å bruke rutere til filtrering i stedet for unødvendig dyre brannmurer.

Pakkefilter på ruter:
Fordeler:
Ikke et problem med flaskehals på grunn av filtrering.
Man får ikke flere virksomhetskritiske bokser i nettet som man må vedlikeholde og ha kompetanse på.
Billig løsning (siden du ikke trenger å investere i nytt utstyr).

Ulemper:
Ikke like mye funksjonalitet som brannmurer, og kan bare filtrere på headerinformasjon i pakker.

Brannmur:
Fordeler:
Kan ha dyp pakkeinspeksjon, og dermed bedre sikkerhet enn pakkefilter i ruter.
Har som regel "stateful inspection" (se under definisjonen allerede etablert trafikk)

Ulemper:
Kan være en potensiell flaskehals i nettet da det nå stort sett er Gigabit hastigheter i nettene.
Ny virksomhetskritisk boks man må ha kompetanse på.
Dyrt. Både i innkjøp og i drift dersom man ikke skal vedlikeholde boksen selv.
Selgere har en evne til å selge brannmurløsninger uten å nevne at det er arbeid med oppsett og vedlikehold. Oppsett og vedlikehold av brannmurer er minst like komplisert som oppsett og vedlikehold av pakkefilter på ruter.

4. Åpent vs. lukket

Et forsknings og utdanningsmiljø har en filtreringspolicy som gjerne er forskjellig fra kommersielle bedriftsnett, og det å finne balansegangen mellom tilstrekkelig/effektiv sikkerhet og åpenhet kan være vanskelig.
Tilgangen fra utsiden bør begrenses til det som er nødvendig for normal drift, slik at slike sårbare maskiner ikke blir tilgjengelig for angrep fra utsiden. Samtidig er det viktig å tenke på behovet for åpenhet, ende-til-ende funksjonalitet og ytelse.
Svært enkle regler kan hjelpe veldig mye, slik at institusjoner som ikke har noe filtrering fra før kan ved hjelp av enkle men effektive regelsett bedre sikkerheten betraktelig.

Institusjoner ved UH-sektoren er ofte oppdelt i flere nett/vlan, og en del av teksten i dette dokumentet forutsetter en slik oppdeling. Mindre institusjoner som har bare ett nett kan se bort ifra teksten som omhandler trafikk mellom interne nett.

5. Risikovurdering

Vurder arbeidsmengden versus nytteverdien på arbeidet du gjør. Det er en balansegang på hvor mye tid det er fornuftig å bruke på oppsett og vedlikehold av pakkefilter. Dersom du ser at du vil ende opp med mange og uoversiktlige regler kan det ofte lønne seg å ta "snarveier". Dette vil kanskje føre til mer åpenhet enn ønskelig, men samtidig vil det lette vedlikeholdet og oppsettet betraktelig. I design av regler vil du ende opp i mange avgjørelser hvor du må spørre deg selv om dette er en tjeneste som skal være "lovlig", eller om tjenesten er forbundet med risiko. Du vil kanskje ikke komme frem til et konkret svar, så det blir opp til din organisasjon å komme frem til en policy.

6. Basis kommunikasjon

Det er veldig viktig å merke seg at protokoller kommuniserer toveis.
De vil nærmest alltid ha en side som sender melding/signal, og en annen side som sender et svar tilbake av en eller annen type. Så man må med andre ord huske på at pakker flyter begge veier. Det er for eksempel lite nytte i å tillate web trafikk ut mot verden, dersom du ikke tillater svarpakkene å komme tilbake igjen.

7. Navn og kommentarer

Ved å sette forklarende navn på filtrene kan det være mye enklere å skaffe seg oversikt. Et eksempel på dette kan være å navngi et utgående filter på et administrasjonsnett. admout.acl. Nummereres filtrene kan det for eksempel være en ide å bruke partall til utgående filter, og oddetall til inngående.
Kommentarer er også viktige når man skal lage regler. Reglene kan ofte være vanskelig å forstå, og inneholder gjerne IP-adresser i stedet for navn på ressurser. En forklarende kommentar kan derfor lette lesingen av reglene betraktelig.

8. Strategi

Default permit versus default deny
Det er i utgangspunktet to forskjellige måter man kan lage regler i et pakkefilter:
Alt som ikke er tillatt blir nektet. (Stengt ende)
Alt som ikke er nektet blir tillatt. (Åpen ende)

Det er den første av disse som vi bruker mest. Men vi har også bruk for den andre metoden i visse sammenhenger. I såkalte sugefilter er dette en metode vi bruker.
En kombinasjon av disse er også vanlig å bruke. Dette kan være dersom man har enkelte tjenester man vil sperre ut, men ikke likevel ha åpen ende.

9. Arbeidsmåte

For å kunne etablere fornuftige regler må man ha oversikt over sitt eget nett og tjenester. Dette er nødvendig uansett om man selv skal lage reglene, eller man skal betale noen andre for å gjøre det. Det er til slutt institusjonens ansvar at reglene er hensiktsmessig, og da må man ha oversikt over sine ressurser.

UNINETT har over lang tid vært med på å utarbeide nye regler for sine medlemsinstitusjoner. Metoden som blir brukt krever utstrakt bruk av logging.

- Legg inn innslag på de tjenester du vet skal være tillatt. Dette blir en liste over godkjente tjenester.
- Lag en regel til slutt som tillater alt annet, men som også logger alle innslag i denne ene regelen. Du kan også velge å ikke tillate denne trafikken, men da kan du ende opp med at brukerne opplever tjenester som ikke virker lenger. (Og erfaringsmessig klarer du ikke å «huske» å ta med alle godkjente tjenester.)
- Nå vil du ha en fin logg over hvilke tjenester du ikke har gjort rede for i din liste over godkjente tjenester.
- Se i logg etter tjenester/trafikk du vil skal tillates, og utvid den opprinnelige lista over godkjente tjenester. Trafikk som blir fanget opp i de nye innslagene vil da ikke logges lenger.
- Etterhvert har du redegjort for all den godkjente trafikken du vil skal være tillatt, og du vil kun ha «støy» igjen i loggen.
- Du kan da velge å snu den siste regelen som tillater alt til å nekte alt i stedet.
- Etterhvert vil det sannsynligvis dukke opp en del ting som må tillates, som man har oversett i første omgang. Erfaringsmessig er det veldig vanskelig å klare å fange opp all trafikk som skal tillates. Så vær forberedt på at noe ikke vil virke.
- Dersom du har mye støy i loggen (fra scanninger etc.) under etablering av filtrene kan det være vanskelig å finne de innslagene som du faktisk er interessert i. Da kan det være en ide å filtrene bort/nekte den støyende trafikken eksplisitt i en egen regel uten logg for å få den bort ifra loggen.

10. Definisjoner

- Må - Dette punktet må følges dersom tjenesten skal fungere.
- Anbefales - Ut fra sikkerhetshensyn anbefales disse punkt å følges.
- Allerede etablert trafikk - for trafikk som for eksempel er etablert fra interne ressurser kan man ved TCP lage en regel som tillater svarpakker tilbake. Brannmurer omtaler dette ofte som stateful inspection. De kan også ha denne funksjonaliteten for UDP også, selv om vi her ikke kan være sikker på at denne trafikken er etablert fra innsiden.
- IP - IP ligger på et lag under TCP og UDP. Filtrering på portnummer gir ingen mening her, og man kan bare filtrere på avsender og mottaker addresser og ikke porter.
- TCP – se nedenfor

- UDP – se nedenfor
- ICMP – se nedenfor
- URPF – Unicast reverse path forwarding (Antispoofing)
- Åpen ende - Se under punkt 8 strategi.
- Lukket ende - Se under punkt 8 strategi.
- Dialogretning - Dialogretning forteller hvilken vei en "sesjon" blir satt opp. Hvem er det som skal nå hvem? En dialog som blir satt opp fra interne ressurser vil ha en utgående oppkobling. Men du vil ha både innkommende pakker og utgående pakker. Det samme gjelder for en inngående oppkobling. Det er to vidt forskjellige ting å sette opp regler for de to forskjellige dialogretningene.
    - Utgående oppkobling – Interne ressurser prøver å nå en ekstern tjeneste
    - Inngående oppkobling – Eksterne ressurser prøver å nå en intern tjeneste
- Pakke retning - Pakke retning forteller hvilken vei pakkene går. Men en innkommende pakke kan være enten et svar fra et anrop innenfra, eller forsøk på å etablere en sesjon utenfra. Se også Dialog retning.
    - Inngående pakker – Pakker som kommer inn mot den ressursen du vil beskytte.
    - Utgående pakker – Pakker som kommer fra den ressursen du vil beskytte.
- Rekursiv navnetjener - Dine interne klienter bruker denne for DNS-oppslag.
- Autorativ navnetjener - Eier du et domenenavn, er en navnetjener satt opp til å være autorativ for dette domenet. Merk her at det kan også være snakk om både primær og sekundær tjener.
- Botnet – En samling maskiner som er infisert med ormer/virus/bakdører etc. og blir fjernstyrt og brukt til lyssky virksomhet.
- Låvedør - En åpning i pakkefilter som er uhensiktsmessig åpent kan omtales åpen som en låvedør.
- Sugefilter – generelle regler (som gjerne legges på linken ut mot verden) for sperring av utvalgte tjenester som du ikke vil ha inn/ut av noen av dine nett. Eks. Netbios/CIFS.

11. De vanligste protokollene

TCP er den vanligste protokollen som tjenester bruker idag. TCP er en pålitelig protokoll, toveis, og er forbindelsesorientert. En TCP oppkobling kan sammenlignes med det å ringe noen. Du slår nummeret, og etter et lite øyeblikk har du en "pålitelig" linje til den du ringer.

UDP er forbindelsesløs. Kan sammenlignes med det å sende brev. Dersom du sender ut 10 brev til samme mottaker kan du ikke være sikker på at de kommer frem i samme rekkefølge som de ble sendt, og du vet heller ikke om alle brevene kommer frem. Man sender ut en pakke og forventer at den kommer frem. Forhåpentligvis får du svar. Det er opp til applikasjonen å sørge for resending av pakker dersom noen blir mistet. Har ikke "oppkoblingspakker" slik som TCP har.

ICMP er en protokoll som man ofte blir anbefalt å filtrere/stenge. ICMP er designet for å rapportere feil, og kan inneholde nytteinformasjon som er viktig i nettverkskommunikasjon. Vi

anbefaler derfor ikke å stenge slik trafikk. ICMP echo og echo reply er også nyttig ved feilsøking. Dessuten har den lav "exploit rate". Det er like viktig å tenke på «rate-limiting» av ICMP dersom man vil minke effekten av ICMP baserte angrep. Dersom man likevel velger å sperre for ICMP anbefales det å åpne for disse ICMP typene:

Navn	Type	Code	Kommentar
ICMP_ECHO	8	0	Ping
ICMP_ECHOREPLY 0	0	Ping svar	
ICMP_UNREACH	3	4	Brukes av path MTU for å finne optimal MTU
ICMP_TIMXCEED	11	0	Brukes av traceroute

Ved å tillate disse ICMP typene vil man kunne bruke nyttige verktøy for å ha en effektiv drift av sine IP nettverk.

12. Oppkoblingspakker

Dersom man vil sperre for en TCP oppkobling holder det å sperre for den første pakken under oppkoblingen. Denne pakken kjenner man igjen siden den ikke inneholder ACK-flagget. Alle andre pakker, uansett hvilken retning den går vil inneholde ACK-flagget.
Ved å gjenkjenne disse □hstart-pakkene□h kan man etablere en policy som sier at interne klienter skal få lov til å koble opp mot eksterne servere, mens eksterne klienter ikke skal få lov til å koble opp mot interne servere. Dette gjør du ved å kun tillate slike □hstart-pakker□h på utgående trafikk, mens du nekter det på inngående trafikk. Denne metoden brukes når vi snakker om det å tillate allerede etablert trafikk. Se også på definisjonen "Allerede etablert trafikk"

13. Logging

Logging er et uvurderlig hjelpemiddel ved oppsett av regler. Det er sjelden man klarer å huske alle tjenester ved oppsett av regler, og logging vil kunne avsløre hva du har glemt. Se forøvrig under punkt 9 Arbeidsmåte for tips om hvordan du bruker logging som hjelpemiddel til oppsett av pakkefilter.

14. De vanligste tjenestene

Sperring på utgående oppkoblinger nevnes ikke med mindre det er behov for det. Det er få tjenester vi anbefaler å sperre på utgående oppkoblinger, da det som regel er lite/ingen risiko forbundet med dette.
For de mindre vanlige tjenestene er det ikke nevnt noe om karakteristikk.
Enkelte av tjenestene har ikke egne anbefalinger.

14.1 DNS (Navnetjeneste)

DNS må sees på i to sammenhenger. Alle institusjoner har som regel en autorativ navnetjener som svarer for sitt domene. Denne må svare på forespørsler fra omverdenen, i tillegg til soneoverføringer fra sekunder navnetjener. I tillegg har man rekursive navnetjenere som man bruker til oppslag i DNS-treet.

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Frapor t	Tilport	AC K	Kommentar
Inn	Ekstern	Intern	UDP/TCP	>1023	53	*	Eksternt oppslag mot din autorative navnetjener
Inn	Intern	Ekstern	UDP/TCP	53	>1023	*	Svar på oppslag. Din autorative navnetjener mot ekstern klient.
Inn(sett fra rekursiv navnetjener)	Intern(klie nt)	Intern(rekursiv navnetjener)	UDP/TCP	>1023	53	*	Intern klient med forespørsel mot din rekursive navnetjener.
Inn(sett fra rekursiv navnetjener)	Intern(rek ursiv navnetjene r)	Intern(klient)	TCP	53	>1023	*	Rekursiv navnetjener sender svar på forespørsel til klient.
Ut	Intern(rek ursiv navnetjene r)	Ekstern	TCP/UDP	>1023	53	*	Intern rekursiv navnetjener med forespørsel mot ekstern autorativ navnetjener.
Ut	Ekstern	Intern(rekursiv navnetjener)	TCP/UDP	53	>1023	*	Svar på forespørsel. Ekstern autorativ navnetjener mot din interne rekursive navnetjener

* For TCP: ACK er ikke satt på første pakke (ved oppkobling) men ved resten av sesjonen. For UDP: UDP pakker har ikke ACK flagg.

Anbefaling:

- Trafikk til autorativ navnetjener.
- UDP og TCP trafikk fra hele verden fra porter over 1023 må tillates inn mot din autorative navnetjener mot port 53.

- Trafikk til/fra rekursive navnetjenere(DNS-tjenere som brukes til oppslag)
  - UDP trafikk fra hele verden fra port 53 må tillates inn til din rekursive navnetjener mot porter over 1023. TCP vil som oftest bli omfattet av regel for allerede etablert trafikk.
  - UDP og TCP trafikk fra alle dine interne adresser (som bruker denne tjeneren som rekursiv navnetjener) må tillates mot din rekursive navnetjener mot port 53.
  - UDP trafikk fra din rekursive navnetjener fra port 53 må tillates inn til alle dine interne ressurser (som bruker denne tjeneren som rekursiv navnetjener.)

14.2 MAIL

Det kan være fornuftig å sperre utgående mail/smtp fra andre enn dine mailservere for å unngå at infiserte maskiner får lov til å sende spam. All utgående mail kanaliseres gjennom dediserte mailservere som ikke blir nektet i filtrene. Eventuelle forsøk fra ikke mailservere kan logges, og da vil man ved å følge med i loggen med en gang plukke opp eventuelle spammere.

- **14.2.1 SMTP** (sending av mail mellom postkontor)

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Fraport	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	TCP	>1023	25	*	Innkommende mail, sender til mottaker
Inn	Intern	Ekstern	TCP	25	>1023	Ja	Innkommende mail, mottaker til sender
Ut	Intern	Ekstern	TCP	>1023	25	*	Utgående mail, sender til mottaker
Ut	Ekstern	Intern	TCP	25	>1023	Ja	Utgående mail, mottaker til sender

* ACK er ikke satt på første pakke (ved oppkobling) men ved resten av sesjonen.

Anbefaling:

- TCP trafikk fra hele verden fra porter over 1023 må tillates til din mailserver mot port 25.
- Utgående TCP trafikk fra dine mailservere fra porter over 1023 må tillates mot hele verden mot port 25.

- Utgående TCP trafikk fra resterende systemer anbefales å sperre mot hele verden mot port 25.

- **14.2.2 POP/POPS** (henting av e-mail fra mailserver)
  Merk: POP er en usikker tjeneste da brukernavn og passord overføres i klartekst.

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Fraport	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	TCP	>1023	110/995	*	Innkommende POP oppkobling, klient til server.
Inn	Intern	Ekstern	TCP	110/995	>1023	Ja	Svar på innkommende POP oppkobling, server til klient.
Ut	Intern	Ekstern	TCP	>1023	110/995	*	Utgående POP oppkobling, klient til server.
Ut	Ekstern	Intern	TCP	110/995	>1023	Ja	Svar på utgående POP oppkobling, server til klient.

* ACK er ikke satt på første pakke (ved oppkobling) men ved resten av sesjonen.

Anbefaling:

- TCP trafikk fra dine interne maskiner fra porter over 1023 må tillates mot din mailserver mot port 110. (port 995 ved pops)

- **14.2.3 IMAP/IMAPS** (henting av e-mail fra mailserver)
  Merk: IMAP er en usikker tjeneste da brukernavn og passord overføres i klartekst.

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Fraport	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	TCP	>1023	143/993	*	Innkommende IMAP oppkobling, klient til server.
Inn	Intern	Ekstern	TCP	143/995	>1023	Ja	Svar på innkommende

Ut	Intern	Ekstern	TCP	>1023	143/995	*	IMAP oppkobling, server til klient. Utgående IMAP oppkobling, klient til server.
Ut	Ekstern	Intern	TCP	143/995	>1023	Ja	Svar på utgående IMAP oppkobling, server til klient.

* ACK er ikke satt på første pakke (ved oppkobling) men ved resten av sesjonen.

Anbefaling:

- TCP trafikk fra dine interne maskiner fra porter over 1023 må tillates mot din mailserver på port 143. (port 993 ved imaps)

14.3 WWW

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Frapor t	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	TCP	>1023	80/443	*	Innkommende oppkobling, klient til server.
Inn	Intern	Ekstern	TCP	80/443	>1023	Ja	Svar på innkommende oppkobling, server til klient.
Ut	Intern	Ekstern	TCP	>1023	80/443	*	Utgående oppkobling, klient til server.
Ut	Ekstern	Intern	TCP	80/443	>1023	Ja	Svar på utgående oppkobling, server til klient.

* ACK er ikke satt på første pakke (ved oppkobling) men ved resten av sesjonen.

Anbefaling:

- TCP trafikk fra hele verden fra porter over 1023 må tillates mot din webserver mot port 80. (port 443 ved https)

14.4 SSH

Kryptert trafikk, som med fordel kan brukes istedet for FTP og/eller TELNET.

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Fraport	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	TCP	>1023	22	*	Innkommende oppkobling, klient til server.
Inn	Intern	Ekstern	TCP	22	>1023	Ja	Svar på innkommende oppkobling, server til klient.
Ut	Intern	Ekstern	TCP	>1023	22	*	Utgående oppkobling, klient til server.
Ut	Ekstern	Intern	TCP	22	>1023	Ja	Svar på utgående oppkobling, server til klient.

Anbefaling:

- TCP trafikk fra hele verden/utvalgte addresser fra porter over 1023 må tillates mot dine SSH-servere mot port 22. Dersom du har mange *NIX systemer anbefales det å kun tillate denne tjenesten mot noen få systemer. Såkalte hop-hosts. Scanning etter sårbare SSH-tjenere er vanlig, og antall åpne SSH-tjenere kan med fordel holdes til et minimum.

14.5 NTP

Brukes for å synkronisere klokken. UDP-basert tjeneste.

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Fraport	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	UDP	>1023	123	*	Innkommende oppkobling, klient til server.
Inn	Intern	Ekstern	UDP	123	>1023	*	Svar på innkommende

							oppkobling, server til klient.
Ut	Intern	Ekstern	UDP	>1023	123	*	Utgående oppkobling, klient til server.
Ut	Ekstern	Intern	UDP	123	>1023	*	Svar på utgående oppkobling, server til klient.
Inn	Ekstern	Intern	UDP	123	123	*	Oppkobling eller svar på oppkobling mellom servere.
Ut	Intern	Ekstern	UDP	123	123	*	Oppkobling eller svar på oppkobling mellom servere.

* Ikke noe som heter ACK i UDP-pakker.

Anbefaling:

- Man kan vudere å bruke NTP kun internt. Dette krever da oppsett av en intern NTP-server, som interne maskiner oppdaterer klokka si imot. Dersom man bruker en ekstern NTP-server anbefales det å filtrere ut trafikk kun fra denne serveren. UDP-trafikk fra ekstern NTP-server fra port 123 må tillates til IP-adresser man vil oppdatere klokka på, mot porter over 1023.

14.6 TELNET

Merk: Autorisasjon og all kommunikasjon går i klartekst, slik at dette er en usikker tjeneste.

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Fraport	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	TCP	>1023	23	*	Innkommende oppkobling, klient til server.
Inn	Intern	Ekstern	TCP	23	>1023	Ja	Svar på innkommende oppkobling, server til klient.
Ut	Intern	Ekstern	TCP	>1023	23	*	Utgående oppkobling, klient til server.
Ut	Ekstern	Intern	TCP	23	>1023	Ja	Svar på utgående oppkobling, server til klient.

* ACK er ikke satt på første pakke (ved oppkobling) men ved resten av sesjonen.

Anbefaling:

- Dersom du likevel velger å bruke telnet må TCP trafikk fra hele verden/utvalgte addresser fra porter over 1023 tillates mot dine TELNET-servere mot port 23.

14.7 FTP

Merk: Autorisasjon og all kommunikasjon går i klartekst, slik at dette er en usikker tjeneste FTP bruker to seperate TCP oppkoblinger, en for kommandoer og en for datatrafikk. I tillegg opererer FTP i to modus, og det er viktig å skjønne forskjellen på disse før man kan lage regler for FTP. Se nedenfor for detaljer.

Karakteristikk:

DialogRetning	Avsender	Mottaker	Protokoll	Fraport	Tilport	ACK	Kommentar
Inn	Ekstern	Intern	TCP	>1023	21	*	Innkommende oppkobling, klient til server.
Inn	Intern	Ekstern	TCP	21	>1023	Ja	Svar på innkommende oppkobling, server til klient.
Inn	Intern	Ekstern	TCP	20	>1023	*	Datakanal oppkobling for innkommende oppkobling, normal modus, server til klient.
Inn	Ekstern	Intern	TCP	>1023	20	Ja	Svar på oppkobling av datakanal ved innkommende oppkobling passive modus, klient til server.
Inn	Ekstern	Intern	TCP	>1023	>1023	*	Datakanal oppkobling for innkommende oppkobling passive modus, klient til server.
Inn	Intern	Ekstern	TCP	>1023	>1023	Ja	Svar på oppkobling av datakanal ved innkommende

							oppkobling passive modus, server til klient.
Ut	Intern	Ekstern	TCP	>1023	21	*	Utgående oppkobling, klient til server.
Ut	Ekstern	Intern	TCP	21	>1023	Ja	Svar på utgående oppkobling, server til klient.
Ut	Ekstern	Intern	TCP	20	>1023	*	Datakanal oppkobling for utgående oppkobling normal modus, server til klient.
Ut	Intern	Ekstern	TCP	>1023	20	Ja	Svar på oppkobling av datakanal ved utgående oppkobling normal modus, klient til server.
Ut	Intern	Ekstern	TCP	>1023	>1023	*	Datakanal oppkobling for utgående oppkobling passive modus, klient til server
Ut	Ekstern	Intern	TCP	>1023	>1023	Ja	Svar på oppkobling av datakanl ved utgående oppkobling passive modus, server til klient.

* ACK er ikke satt på første pakke (ved oppkobling) men ved resten av sesjonen.

Anbefaling:

- Autorisasjon og all kommunikasjon går i klartekst, slik at dette er en usikker tjeneste. Man kan med fordel derfor bruke andre løsninger dersom det er mulig.
- Er det FTP-klienten du skal beskytte anbefales det å bruke passive modus. Da unngår du å måtte åpne alle porter mot klienten fra FTP-serverne.
- Dersom du driver en egen FTP-tjener anbefales det å bruke et fast portnummer som klientene tar kontakt på ved passive modus. Da unngår du å måtte åpne for alle porter inn mot denne serveren.

- Passive modus
  Ved passive modus er tjeneren man kontakter passiv. Det vil si at det er klienten som

oppretter både kontrollkanal og datakanal.

- Regler for tjener
  På enkelte FTP-tjenere kan man for datakanalen velge hvilken port man vil at klienter skal kontakte tjeneren på. Klientene får da beskjed om dette portnummeret ved oppsett av kontrollkanal.
  Trafikk fra (utvalgte) klienter fra alle porter over 1023 må tillates til tcp port 21 og datakanalporten (default port 20).
- Regler for klient
  Dersom man bruker passiv ftp vil all trafikk være initiert innenfra (sett fra klienten). Svar tilbake fra server vil derfor komme inn under allerede etablert trafikk, slik at man ikke trenger flere åpninger i filter for å få dette til å fungere.

- Normal modus
  Ved normal modus er tjeneren man kontakter aktiv. Det vil si at klienten oppretter kontrollkanalen, men det er tjeneren som oppretter datakanalen mot klienten tilbake.
  - Regler for tjener
    Trafikk fra utvalgte addresser fra porter over 1023 må tillates til dine FTP-tjenere mot port 21.
  - Regler for klient
    Trafikk fra FTP-servere fra alle porter må tillates til dine FTP-klienter til alle porter. Her må filtrene åpnes som en låvedør, og dette er ikke anbefalt løsning sett fra klienten sin side!

14.8 Active Directory

AD-servere kommuniserer seg imellom og med klienter med mange forskjellige protokoller, og det anbefales derfor å åpne på IP-nivå mot disse. Alternativt kan man velge å åpne for hver protokoll/tjeneste. Erfaringsmessig fører dette til mer administrasjon enn hva det er verdt.

Anbefaling:

- IP trafikk fra alle dine interne maskiner må tillates mot dine AD servere. (Alternativt kan man velge å åpne per tjeneste.)

14.9 NETBIOS/CIFS

Blir sett på som en "farlig" tjeneste med mange sårbarheter. Denne "tjenesten" bør holdes internt/utenfor dine egne nett, både på utgående og inngående trafikk.

Anbefaling:

- TCP og UDP trafikk fra hele verden fra alle porter anbefales å sperres mot alle dine interne ressurser mot portene 135-139 og 445.
- TCP og UDP trafikk fra alle dine ressurser fra alle porter anbefales å sperres mot hele verden mot portene 135-139 og 445.

14.10 IRC

IRC er en legitim og nyttig tjeneste som brukes av mange. Den blir brukt til chatting, men dessverre også til mer lyssky virksomhet. Botnet er i vinden, og de styres ofte via IRC-kanaler.

Denne tjenesten kan vurderes å sperres, men man må være oppmerksom på at man tar bort en nyttig tjeneste som har stor nytteverdi for mange. Brannmurer med mulighet for pakkeinspeksjon kan sperre på tjenestenivå, og kan dermed plukke opp ukryptert IRC-trafikk på andre porter.

14.11 SNMP

SNMP er en standardisert protokoll som brukes til overvåkning og styring av blant annet nettverksutstyr. I utgangspunktet vil du ikke at noen fra utsiden skal kunne styre utstyret ditt, så SNMP bør sperres fra utsiden. Det er også verdt å merke seg at SNMP jevnlig har fått avslørt nye sårbarheter.

Anbefaling:

- TCP og UDP trafikk fra hele verden fra alle porter anbefales å sperres mot alle dine interne ressurser mot portene 161 og 162.
- UDP trafikk fra din overvåkningspc fra alle porter over 1023 må tillates mot ditt nettverksutstyr mot port 161

14.12 MSSQL

Det er ingen spesiell grunn til å tilby MSSQL utenfor institusjonen. Slammer infiserte i sin tid veldig mange maskiner, og det finnes fortsatt sårbare maskiner. Det anbefales derfor å sperre for trafikk utenfra mot UDP port 1434.

Anbefaling:

- UDP trafikk fra hele verden fra alle porter anbefales å sperres mot alle dine interne ressurser mot port 1434

14.13 NOVELL

Det kan være komplisert å etablere fornuftige pakkefilteringsregler for NOVELL per tjeneste. Her anbefales det derfor å ha generelle åpninger for NOVELL trafikk internt i dine nett.

Anbefaling:

- TCP og UDP trafikk fra dine interne NOVELL ressurser fra alle porter over 1023 anbefales å tillates til alle andre NOVELL ressurser mot port 427
- TCP og UDP trafikk fra dine interne NOVELL ressurser fra alle porter over 1023 anbefales å tillates til alle andre NOVELL ressurser mot port 524
- TCP og UDP trafikk fra dine interne NOVELL ressurser fra port 427 anbefales å tillates til alle andre NOVELL ressurser.
- TCP og UDP trafikk fra dine interne NOVELL ressurser fra port 524 anbefales å tillates til alle andre NOVELL ressurser.

14.14 RPC

RPC blir sett på som en "farlig" tjeneste som anbefales å sperres ute fra omverdenen. Dersom man trenger åpning fra eksterne maskiner kan man velge å åpne for hele IP-addresser.

Anbefaling:

- TCP og UDP trafikk fra hele verden fra alle porter anbefales å sperres mot alle dine interne ressurser mot port 111.

14.15 Multicast

En del tjenester bruker multicast for kommunikasjon på nettverket. WINS og Norton Ghost er eksempler på dette. En del av denne multicast trafikken bør holdes internt på hver institusjon. Dette løses ved at man definerer et eget internt «rendezvouz» punkt med tilhørende pakkefilter der multicast trafikk som bør begrenses internt blir stoppet. Multicast-strømmer som skal eksternt vil bli sluppet ut eksternt og blir tatt hånd om av det sentrale «rendezvouz» punktet i UNINETT.

Anbefaling:

- Protokollene PIM og IGMP må tillates mellom dine rutere.
- Protokollene PIM og IGMP må tillates mellom dine rutere og «randevouz» punkt.

14.16 Antispoofing

- Inngående - Det anbefales å nekte trafikk fra utsiden som har samme avsenderaddresse som dine interne nett.
- Utgående - Dersom ruteren/nettutstyret ikke støtter URPF anbefales det å sperre for falske avsenderaddresser fra dine egne interne nett.

15. Minimumsoppsett

Lite arbeid hjelper veldig mye! Her er det kun snakk om noen få regler, men disse vil bedre sikkerheten betraktelig. Det eneste man gjør her er å etablere generelle filter på linken ut mot verden, som da vil gjelde for alle dine nett. Trafikk mellom dine interne nett flyter seg imellom uten regler.

- Innkommende sugefilter på linken ut mot verden som stenger en del felles tjenester som du ikke vil ha utenfra, og med åpen ende.
  - Nekt alle IP-pakker som har avsenderaddresser med samme adresse som dine interne nett. (antispoofing)
  - Nekt IP-pakker med avsenderadresser ifra ikke rutbare nett mot alle dine ressurser.
  - Tillat all IP-trafikk fra dine andre studiesteder mot alle dine ressurser. (Gjelder bare dersom din institusjon har flere studiesteder.)
  - Nekt all TCP/UDP trafikk fra hele verden mot alle dine ressurser mot portene 161 og 162 (SNMP)
  - Nekt all TCP/UDP trafikk fra hele verden mot alle dine ressurser mot porter 135 – 139 og 445. (NETBIOS/CIFS)
  - Nekt all TCP/UDP trafikk fra hele verden mot alle dine ressurser mot port 111. (RPC)
  - Nekt all UDP trafikk fra hele verden mot alle dine ressurser mot port 1434. (MSSQL)
  - Tillat resten
- Utgående sugefilter som stenger en del tjenester som du ikke vil sende ut fra dine egne nett

- Tillat all TCP trafikk fra dine interne mailservere til hele verden mot port 25.
- Nekt all TCP trafikk fra dine interne nett til hele verden mot port 25. (disse 2 siste reglene vil sørge for at det kun er dine mailservere som får sendt mail ut mot verden)
- Nekt all TCP/UDP trafikk fra alle dine interne nett mot hele verden mot port 135 – 139 og 445.
- Tillat all IP-trafikk fra alle dine interne nett mot hele verden.
- Nekt resten. (de 2 siste reglene vil sørge for at ingen på innsiden kan forfalske avsenderadresser)

16. Middels oppsett:

Ikke så veldig stor forskjell ifra minimumsoppsettet, men her må du i tillegg legge på filter på dine interne nett.

- Bruk de samme sugefiltrene som i minimumsoppsettet.
- I tillegg har du regler ut mot hvert enkelt vlan/nett. På hver av disse:
  - Tillat tcp-trafikk som er etablert innenfra.
  - Tillat all IP-trafikk fra dine interne nett.
  - Tillat trafikk mot de interne tjenestene som skal være nåbare utenfra. De viktigste du må huske er MAIL, DNS og WWW. Se egne beskrivelser tidligere i dokumentet på for oppsett av regler på disse.
  - Nekt resten.
- Dette oppsettet er et veldig godt utgangspunkt for å gå over til et avansert oppsett.

17. Avansert oppsett

Veldig likt middels oppsett, men i stedet for å tillate all trafikk mellom dine interne nett, lager du regler for hva som skal være lov internt også. Dette krever mye arbeid, og dette dokumentet gir ikke ett komplett oppsett. Viktige hjelpemidler for å få laget slike oppsett er logging. (Se pkt om arbeidsmåte)
Her kan man også kombinere med at sikre nett kan nå alle andre nett, mens usikre nett ikke kan nå nett som er definert som sikrere enn seg selv. Et eksempel er at administrasjonsnett kan fritt nå fag og studentnett, fagnett har ikke rettigheter til å nå administrasjonsnett men kan fritt nå studentnett, mens studentnettet ikke har rettigheter til å nå de andre to nettene.

18. Akutte tiltak

Ved akutte tiltak kan det være behov for å sperre enkelte tjenester eller maskiner. DDoS angrep, eller "løpske" maskiner på innsiden er eksempel på slike anledninger. Dokumentering og opprydning er viktig å huske.

19. Vedlegg.

UNINETT-spesifikke tjenester eller høgskole spesifikke tjenester spesifiseres i vedlegg.
Trofast
Telefonsentral
Arkivsystem
NAV/Verktøykasse
Målepåle

Domenekontrollere
SIP

20. Referanser

Building Internet Firewalls, D. Brent Chapman and Elizabeth D. Zwicky

21. Intellektuelt eierskap

Forfatter med arbeidsgruppe står ansvarlig for innholdet i dette dokument.

22. Forfatters adresse

Rune Sydskjør
UNINETT
Abels gt 5 - Teknobyen
7465 Trondheim
Norway
Telefon: 735 57944
Epost : rune.sydskjor@uninett.no