

## Praktisk epost-filtrering med Postfix

Relevante artikler om SPAM og epost i tidligere utgaver av Mellvik-Rapporten:

- "SPAM: Det nytter å slåss" – nr. 106
- "SPAM-politiet: Effektivt og tilgjengelig" – nr. 107
- "Trenger du en epost-arkitektur?" – nr. 115
- "Exchange under press" – nr. 116
- "SPAM – synlig progresjon" – nr. 122
- "Epost-filtrering: Enkelt, billig, effektivt" – nr. 125 (om MailScanner)

Flere artikler om SPAM finnes på vår Web-tjeneste, der også spesialrapporten "Effektiv sikring av epost" blir lagt ut ved åpningen av vår nye kunnskapsportal i juni måned.

### Mer praktisk stoff?

Er du blant dem som ønsker flere praktisk orienterte artikler i Mellvik-Rapporten?

I forbindelse med den forestående åpningen av vår kunnskapsportal, er større vekt på slikt stoff under vurdering. Har du synspunkter i så henseende – send dem til [hanne@mellvik.no](mailto:hanne@mellvik.no).

Du har en unik mulighet til å påvirke fremtiden. Benytt den!

*30 milliarder meldinger traverserte Internettet daglig i 2004 – ifølge IDC. Et sted mellom 75 og 90% av dem hører hjemme i kategorien SPAM. Internettet er blitt en søppelfylling av kolossale dimensjoner som truer med å trenge seg langt inn i våre mer eller mindre private nettverk. Alle indikasjoner forteller at verre skal det bli.*

Bedre incentiv trenger de færreste av oss for å bringe eget hus i orden – et forhold vi også diskuterer på lederplass i denne utgaven (se side 2). Hvem som har ansvaret for all denne forsøplingen er naturligvis et interessant spørsmål, men en diskusjon som ikke vil forandre den belastningen våre epost-systemer og -tjenere skal møte hver eneste time døgnet rundt (se kommentar på side 25).

### Fra teori til praksis

Her er handling det eneste som gir resultater. Vi har diskutert både mekanismer, produkter, tiltak og erfaringer ved en rekke anledninger i Mellvik-Rapporten i løpet av de siste årene – supplert med gode råd og hint om veier til målet. I denne miniserien skal vi gå mer praktisk til verks. Med utgangspunkt i erfaringer over en 3-års periode med egen epost-tjeneste og en rekke klientprosjekter, skal vi gjennomgå et praktisk oppsett for SPAM-bekjempelse.

Vi tar først for oss en samling krav og målsettinger for løsningen, og presenterer deretter hvordan Open Source-produktet Postfix kan konfigureres for å tilfredsstille kravene. Postfix er valgt av flere årsaker. For det første er produktet lett tilgjengelig – inkludert i de fleste Linux-distribusjoner, Mac OS X og enkelte Unix-systemer, og kan lett installeres på øvrige Linux- og Unix-systemer. For det andre har Postfix bedre, mer fleksible og mer forståelige mekanismer for nettopp SPAM-filtrering enn noen andre generelle epost-agenter på markedet, kommersielle eller Open Source.<sup>8</sup> Og for det tredje er Postfix kjent for høy effektivitet, skalerbarhet og pålitelighet.

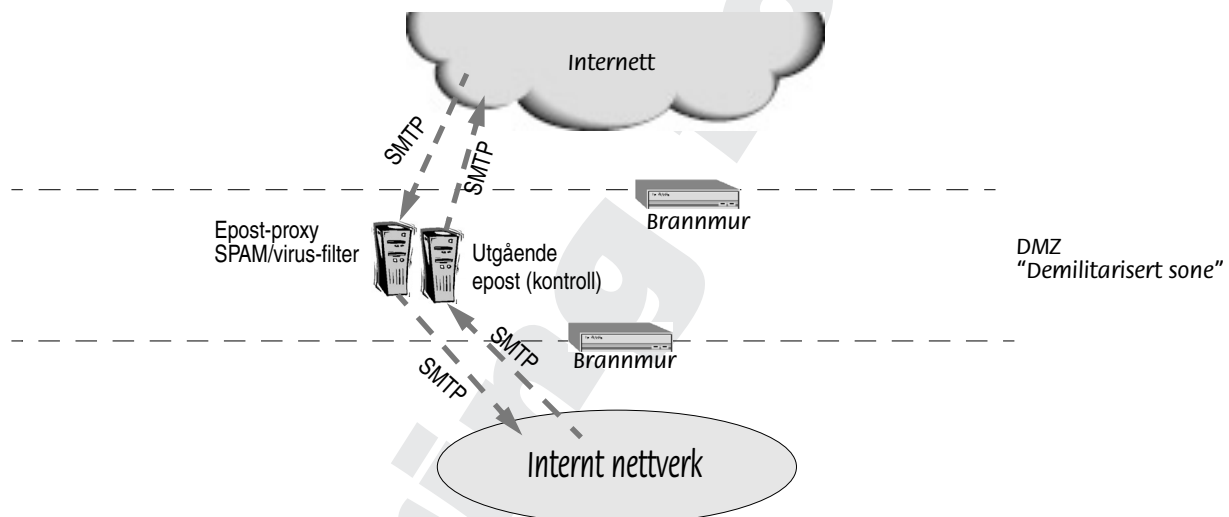
I og med at Postfix er forhåndsinstallert på de fleste Linux- og Apple-tjenere, er idriftsettingen i mange miljøer kun et spørsmål om konfigurasjon. Videre tar vi utgangspunkt i at virksomhetens eksisterende epost-tjeneste i første omgang ikke skal røres. Dette er den både vanligste og foretrukne fremgangsmåten, som gjør at kostnadene ved introduksjonen av et SPAM-filter blir minimale. Brukerne merker ikke noe annet enn at SPAM blir borte – og i de fleste tilfeller at responsen blir vesentlig bedre.

<sup>8</sup> Det finnes flere spesialprodukter og -tjenester på markedet som har enklere brukergrensesnitt og et funksjonsspekter som noenlunde tilsvarer Postfix. Prisen – ved siden av betydelige lisenskostnader – er høyere ressurskrav og i noen tilfeller begrenset skalerbarhet. ZixMail og Postini er to av dem, og vi skal komme tilbake til flere slike i fremtidige utgaver.

### Filtrering begge veier

Det er ønskelig at SPAM-filtring tar hånd om både inngående og utgående epost – av såvel sikkerhetsmessige som etiske årsaker. Som ansvarlig aktør på Internettet bør enhver organisasjon eliminere SPAM og annen unødig trafikk fra sin utgående datastrøm, og samtidig blokkere utgående epost-trafikk som ikke kommer fra én eller et par utvalgte epost-agenter. Både virus og *spyware* er notoriske misbrukere av epost, og forsøker typisk å sende meldinger direkte tilbake til sine 'foresatte' fra infiserte klienter. Ved å blokkere epost-trafikk fra vanlige klienter i brannmuren, og eventuelt sørge for at den automatisk omrutes til epost-tjeneren<sup>9</sup> eller SPAM-filtringen, har vi slått to fluer i ett smekk.

Prinsippskissen av oppsettet blir dermed som figur 1 nedenfor, der vi har fordelt innkommende og utgående trafikk på to tjenerer for å vise hvor lett løsningen kan skaleres. For de fleste små og mellomstore virksomheter vil det ikke være behov for en slik splitting. Likeledes vil



**Figur 1** Et SPAM-filtring kan introduseres uten komplikasjoner i et hvilket som helst nettverk, og bør ta hånd om trafikken begge veier. I tillegg til å filtrere SPAM kan et slikt filter også foreta virus-kontroll, blokkere epost til ugyldige adresser og generelt skjerme den interne epost-tjeneren.

det i mange tilfeller være tilstrekkelig med én brannmur, og med den demilitariserte sonen som en 'arm' på denne.

### Krav, prioriteringer, målsettinger

Følgende punkter oppsummerer de krav og målsettinger vårt epost-filtring skal oppfylle:

- ✓ Filteret skal implementere de epost-relaterte elementene i virksomhetens sikkerhets-policy.

<sup>9</sup> Ansvarlige ISP'er sørger for en slik automatisk omruting av utgående epost-trafikk fra alle privatkunder, og bidrar på den måten til å hindre at egen kundebase blir utnyttet i forbindelse med spredning av SPAM og virus.

- ✓ Leveringssikkerhet er viktigere enn filtrering. Det er bedre å slippe igjennom enkelte SPAM-meldinger enn å avvise legitime meldinger.
- ✓ Løsningen skal avvise meldinger med ikke-godkjente vedleggstyper. Avsender skal informeres om årsaken til avvisningen.
- ✓ Meldinger til ikke-eksisterende brukere skal avvises 'i døra', det vil si uten å motta meldingenes innhold. Dette punktet alene vil redusere epost-trafikken hos mange virksomheter med 50% eller mer.
- ✓ Løsningen skal i utgangspunktet ikke ha noen karantene-funksjon som involverer sluttbrukere. Å involvere sluttbrukere skaper uten unntak flere problemer enn det løser i en slik sammenheng.
- ✓ Løsningen skal være skalerbar. Dette punktet er i virkeligheten ivaretatt ved å velge Linux/Unix og Postfix som plattform.

## Konfigurasjon av Postfix

Postfix konfigureres via en tekstfil – main.cf – som normalt er å finne i katalogen /etc/postfix. Konfigurasjonsfilen har en betydelig størrelse, ikke bare fordi produktets fleksibilitet er nærmest endeløs, men også fordi den i høy grad er selvdokumenterende. Den 'innebygde' dokumentasjonen er viktig og nyttig, men ikke tilstrekkelig til å gi nykommere full forståelse av effekter og konsekvenser.

De fleste systemer som leveres med Postfix, har en håndfull konfigurasjonsfiler inkludert, tilpasset de mest alminnelige rollene produktet brukes i. Disse representerer gode utgangspunkt for videre konfigurasjon, og kan benyttes uten videre dersom tjeneren kun skal formidle epost mellom eksterne og interne nettverk.

For tilpasning av parametre som ikke er relatert til filtrering og SPAM, henviser vi til [www.postfix.com](http://www.postfix.com) og til en håndfull bøker om Postfix – tilgjengelige for eksempel fra Amazon.com. Siste versjon av Postfix er 2.2.2 – og anbefales, mens 2.0 eller nyere er tilstrekkelig for funksjonene som benyttes i denne artikkelen.

### Kontroll – trinn 1

Første trinn i formidlingen av en epost-melding er at en klient (sender) kobler seg opp mot mottaker og identifiserer seg. Dette kalles 'HELO' på fagspråket, fordi dette er den første kommandoen fra sendersiden.<sup>10</sup> Allerede her har vi en rekke muligheter for kontroll av om senderen er akseptabel eller ikke. Listing 1 tar for seg de viktigste kontrollene som kan etableres på dette trinnet.

Linje 1 er en pussighet som krever spesiell forklaring. I henhold til standarden for epost-protokollen (SMTP), kan en oppkobling avvises av mottaker når som helst. En rekke kommersielle (og meget utbredte)

<sup>10</sup> Dersom kommandoen i stedet staves EHLO, indikerer det at senderen støtter et utvidet kommandosett, og ber om bekreftelse på at mottaker gjør det samme.

## Listing 1 – kontroll av fase 1, oppkoblingen

```

1  smtpd_delay_reject = yes
2  smtpd_error_sleep_time = 30
3  smtpd_soft_error_limit = 1
4  smtpd_hard_error_limit = 6
5  smtp_banner = $myhostname ESMTP
6  smtpd_helo_required = yes
7  strict_rfc821_envelopes = yes
8  smtpd_helo_restrictions =
9      permit_mynetworks,
10     check_helo_access hash:/etc/postfix/helo_access,
11     reject_non_fqdn_hostname,
12     reject_invalid_hostname,
13     permit

```

epost-produkter går imidlertid 'i spinn' dersom de blir avvist før de kommer til trinn 3 i oppkoblingen. En slik 'spinn'-situasjon er like ille for mottakeren (for eksempel 100 nye forsøk på oppkobling fra samme sender per sekund) som for senderen, og bør unngås. Derfor legger vi inn denne kommandoen, som forteller Postfix at selv om vi i trinn 1 eller 2 konstaterer at senderen er uakseptabel, venter vi til trinn 3 med å gjøre den oppmerksom på forholdet.

Også de neste linjene er generelle av natur: *Sleep\_time* forteller hvor lenge vår tjener skal vente med å svare dersom senderen gjør en feil. SPAMmere som prøver seg frem, gjør gjerne slike feil. Relativt lang ventetid mellom forsøkene får slike avsendere til å gi opp, mens profesjonelle epost-produkter tåler lange ventetider. *Soft\_error\_limit=1* forteller Postfix at forsinkelsen skal inn-tre allerede etter den første feilen, mens *hard\_error\_limit* angir hvor mange forsøk senderen får før vi dropper forbindelsen.

Linje 6 forbyr oppkobling uten HELO-kommandoen, egentlig en selv-følge, hvilket stenger ute klienter som ikke holder seg til protokollen. Neste linje presiserer et tilsvarende krav med hensyn til hvordan meldingen er pakket inn, og kommer først til anvendelse på trinn 3. Begge disse har beskjeden, men viktig effekt ved at de stenger ute de mest amatørmessige SPAM-programmene – og enkelte epost-klienter for Windows fra 90-tallet.

HELO-kommandoens format er "HELO navn", for eksempel "HELO mailhost.mellvik.no". Linjene 8-12 forteller hvordan navnedelen av kommandoen skal kontrolleres. Årsaken til at dette er viktig, er at SPAMmere ofte fyller inn en falsk, ikke eksisterende, tilfeldig eller feil-formatert adresse både her og senere i prosessen – i et forsøk på å skjule sin egentlige identitet. Kontrollene vi legger inn er at navnet har riktig syntaks (linje 12) og at det er et 'fullt kvalifisert' domenenavn, dvs. inkluderer et gyldig topp-domene (.no, .com, .net etc.). Linje 9 forteller at lokale klienter skal aksepteres uten videre, mens linje 10 illustrerer hvordan kontroll-kommandoer kan plasseres i egne filer i stedet for direkte i konfigurasjonsfilen.

## Listing 2 – ekstern fil med kontrollkommandoer (/etc/postfix/helo\_access)

```

1  macmini.mellvik.no    OK
2  mellvik.no           REJECT Fake address
3  193.71.53.10         REJECT Fake address
4  obscene.hotmail.com  REJECT Go away

```

Listing 2 viser formatet på en slik fil, og hvordan den kan brukes til å styre tilgangen på detaljert nivå dersom vi ønsker det. Filen har tre felter: Dersom det 1. er identisk med navnefeltet i HELO-kommandoen, utføres kommandoen i felt 2. Og dersom felt 2 er REJECT, brukes felt 3 som melding tilbake til sender. Tilsvarende mekanisme kan brukes i en rekke sammenhenger i Postfix-konfigurasjonen.

I kontrollen av HELO-kommandoen (listing 1) er det fristende å også legge til restriksjonen *reject\_unknown\_hostname*, som betyr at oppkoblingen skal avvises dersom navnet i HELO-kommandoen ikke har gyldig reversoppslag i Internettets oppslags-tjeneste (DNS). SMTP-protokollen forlanger at et slikt reversoppslag skal finnes, men ignoreres dessverre av systemadministratorer flest, trolig på grunn av inkompetanse. Vi forsøkte å aktivisere denne restriksjonen for et par år siden, men fant raskt ut at selv store norske og internasjonale organisasjoner har 'amatører' i sin driftsorganisasjon. Bruk av denne restriksjonen er derfor ikke å anbefale, et beklagelig forhold som kompliserer kampen mot SPAM vesentlig.

### Hjelp til feilsøking

For å forenkle testingen av slike restriksjoner, introduserte Postfix versjon 2 konfigurasjons-kommandoen *warn\_if\_reject*. I stedet for å ta sjansen på at legitime meldinger blir avvist, gir *warn\_if\_reject* anledning til å prøvekjøre nye regler uten konsekvenser. Listing 3 viser hvordan den nevnte *reject\_unknown\_hostname*-restriksjonen kan testes. Postfix logger (typisk til */var/log/maillog*) hva som ville ha skjedd, men later forøvrig som ingen ting. Et uvurderlig hjelpemiddel i forbindelse med feilsøking.

Listing 3– feilsøkingen forenkles og ufarliggjøres med *warn\_if\_reject*

```
1 warn_if_reject,  
2 reject_unknown_hostname
```

Når vi først er inne på feil og feilsøking, er det verdt å nevne en gylden regel fra mannen bak Postfix, den ikke helt ukjente Wietse Venema, som de siste årene har arbeidet for IBM: Han

anbefaler å gjøre maksimalt 3 endringer i Postfix' konfigurasjonsfil per gang, for så å teste. Det er fort gjort å gå seg vill i alle mulighetene, for deretter å ikke vite hvilke endringer som gir hvilke konsekvenser.

## Neste utgave

I neste utgave fortsetter vi med fase 2 og 3 i oppkoblingen, og går deretter videre med å se på bruk av Greylisting, SPF og samspillet mellom Postfix og eksterne tjenester som SpamAssassin og ClamAV (antivirus). ■

### Haster det?

Haster det å komme videre med oppsett av en epost-proxy som stopper SPAM, virus og annen uønsket trafikk? 2. del av denne artikkelen er ferdig, og vil som en 'ekstraservice' bli gjort tidlig tilgjengelig for spesielt interesserte. Send en epost til [helge@mellvik.no](mailto:helge@mellvik.no), oppgi hvem som er 'eier' av abonnementet og fortell samtidig hvilken plattform du vil kjøre Postfix på.

**NUUG** – den norske Unix-brukergruppen – avholdt sin årskonferanse i mars, med blant annet et foredrag om SPAM og SPAM-bekjempelse. Torkel Hasle fra Bibliotek-Systemer i Larvik holdt foredraget, som er tilgjengelig i PDF-format og vel verd en titt: [www.nuug.no/aktiviteter/20050317-spamstopp/](http://www.nuug.no/aktiviteter/20050317-spamstopp/)