Dienstbeschrijving SURFmailfilter

Auteur(s): Maurice van den Akker, Paul Dekkers, Xander Jansen

Versie: 4.01

Datum: November 2013

Radboudkwartier 273
3511 CK Utrecht

Postbus 19035
3501 DA Utrecht

030 - 2 305 305
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Inhoudsopgave

1 Inleiding

Deze dienstbeschrijving beschrijft de dienst SURFmailfilter. Dit document is bedoeld voor instellingen binnen de SURFnet doelgroep die e-mailfiltering (spam, virussen, phishing) voor binnenkomende én uitgaande e-mail wensen uit te besteden.

In dit document komen achtereenvolgens aan de orde:

1. De opzet van de dienst;
2. De functionaliteit;
3. Service levels;
4. Tariefinformatie en informatie over aanvraag, wijziging en storingsprocedures.

2 Afkortingen en terminologie

In onderstaande tabel zijn afkortingen met hun betekenis opgenomen die in dit document worden gebruikt.

Tabel 2.1 Afkortingen met betekenis

Afkorting/term	Betekenis
Spam	E-mailberichten welke in bulk worden verstuurd, zonder dat de ontvangers daarom hebben verzocht
Virus (e-mail)	E-mailbericht welke (deels) bestaat uit een uitvoerbaar, meestal kwaadbedoelend programma, welke zich installeert zonder (bedoelde) toestemming van de gebruiker
Instelling	Een op het SURFnet netwerk aangesloten/aan te sluiten instelling
Realm	Domein (bijvoorbeeld SURFnet.nl)
POP3	Post Office Protocol, bedoeld voor het overbrengen van e-mail vanuit een server naar een client
IMAP	Internet Message Access Protocol, bedoeld voor de toegang tot de mailbox vanuit een client naar de server
Phishing (e-mail)	E-mailbericht, primair bedoeld om de lezer op te lichten. Het gaat hier bijvoorbeeld om het afhandig maken van (persoonlijke) informatie of aanzetten tot actie op (valse) websites.

3 Beschrijving dienst SURFmailfilter

3.1 Inleiding

SURFmailfilter stelt instellingen in staat om, via een centraal platform van SURFnet, al haar binnenkomende en uitgaande e-mailberichten te laten filteren op virussen, phishing en spam. In dit hoofdstuk wordt de functionaliteit van deze dienst beschreven.

3.2 SURFmailfilter voor inkomende e-mailberichten

SURFMailfilter stelt instellingen in staat om al haar binnenkomende e-mailberichten te laten filteren op ongewenste berichten, zoals virussen, phishing en spam, voordat ze bij de eigen mailservers aankomen. (Filteren wil zeggen: het bericht zichtbaar voor de eindgebruiker markeren via bijvoorbeeld de subjectheader, onzichtbaar via de X-header of direct en permanent verwijderen).

De instelling kan zelf per domein of subdomein via een webinterface de filtereigenschappen en de vervolgens te nemen acties aanpassen naar eigen inzicht. Voor zover toegestaan door de instelling kunnen eindgebruikers van de instelling deze filterregels vervolgens naar eigen inzicht aanpassen.

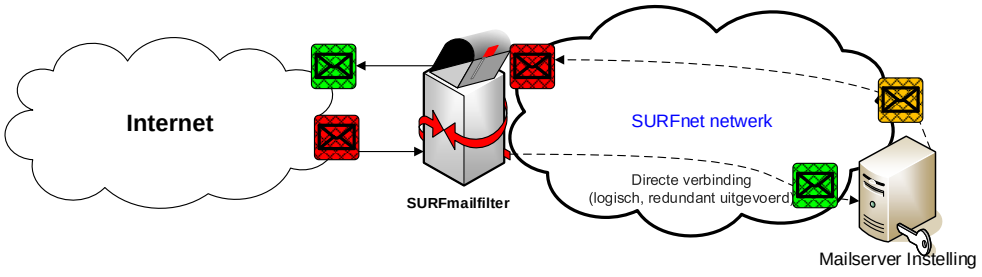
Ook zonder interactie met de beheerder of de gebruiker werkt het filter effectief, omdat het zich automatisch en continu aanpast. SURFmailfilter werkt op basis van het product CanIT Pro (domain) van het Canadese softwarebedrijf Roaring Penguin Software inc. Dit product bestaat uit open source softwarecomponenten aangevuld met enkele componenten die de kwaliteit van filtering aanzienlijk verhogen. De belangrijkste toevoeging is het zogenaamde RPTN (Roaring Penguin Training Network). RPTN zorgt ervoor dat alle gebruikers (wereldwijd) van CanIT pro gegevens delen met betrekking tot de herkenning van spam. Zie ook: http://www.roaringpenguin.com/files/rptn.pdf

3.3 SURFmailfilter voor uitgaande e-mailberichten

Naast het filteren van binnenkomende mail, kan SURFmailfilter ook voorkomen dat via de mailserver van de instelling spam wordt verstuurd of gebruikers de dupe worden van internetfraude via phishing. Het uitgaande filter controleert onder andere op spam-inhoud, virussen, het aantal mails dat wordt verstuurd en berichten naar zogenaamde phishing dropboxen. Verder houden we goed in de gaten dat onze uitgaande mailservers een goede reputatie behouden en niet bijvoorbeeld op blacklists terechtkomen.

3.4 Opzet van de dienst

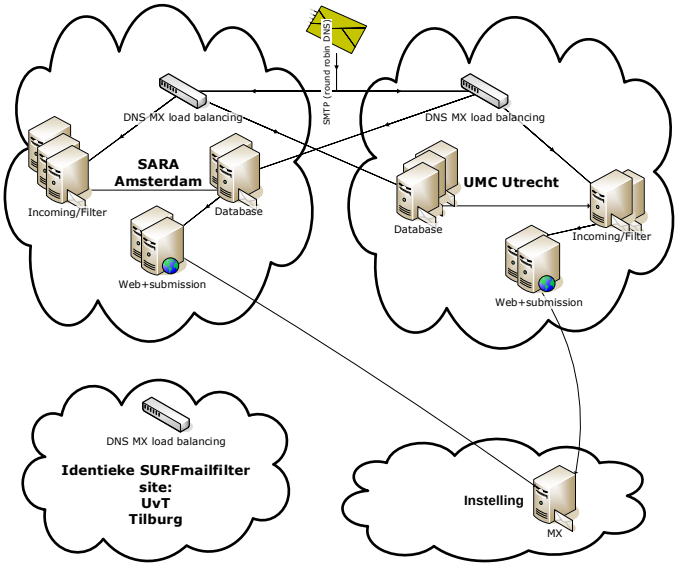
De logische opzet van de dienst is als een *black box*, zoals hieronder is afgebeeld:



SURFmailfilter is een centraal ingerichte dienst. Op deze manier kan er een schaalvoordeel behaald worden. De instellingen hoeven niet allen afzonderlijk een spam-, phishing- en virusfilters aan te schaffen, te installeren en te onderhouden en besparen daarmee op capaciteit en resources (licenties, machines, menskracht en kennis) met betrekking tot mailfiltering.

SURFmailfilter is een krachtige, flexibele en robuuste dienst:

- De dienst is ingericht met (eenvoudig uitbreidbare) krachtige hardware
- De dienst is geografisch redundant opgezet: op drie geografisch gescheiden plaatsen in het SURFnet netwerk staat een identieke configuratie welke per site zodanig gedimensioneerd is om met de uitval van één locatie de gehele belasting aan te kunnen. Indien de groei van het gemiddelde aantal e-mails hierom vraagt kan eenvoudig de netwerk-, reken- en diskcapaciteit worden uitgebreid. De technische opzet staat hieronder afgebeeld:



3.5 Functionaliteit

De filtereigenschappen **voor binnenkomende mail** zijn via een webinterface te configureren. Door de beheerder, maar ook (na toestemming van de beheerder) door een gebruiker. Qua basisfiltering zijn de volgende mogelijkheden te onderscheiden:

- Spam/virus/phishing labelen (via de subjectheader of X-header) alvorens door te sturen naar de mailserver van de instelling, of
- niet doorsturen/verwijderen (door de SURFmailfilter dienst).

NB. er is dus geen sprake van een ‘quarantaine mailbox’ zoals in sommige anti-spam oplossingen wel het geval is. Dit is in de meeste gevallen ook niet nodig, omdat spam toch direct in een aparte (spam)folder bij de gebruiker terechtkomt.

Daarnaast zijn er diverse configuratiemogelijkheden die het filteren beïnvloeden: (agressiveness, black & white list for senders, spamtraining door het toevoegen van klikbare links en andere specifieke zaken). De gebruiker kan eventueel zelf alias-e-mailadressen toevoegen binnen hetzelfde realm.

Authenticatie en autorisatie is voor eindgebruikers mogelijk op basis van SURFconext of IMAP/POP3 username/password zoals deze (nu al) bij de instellingen bekend is. Voor realm-beheerders wordt gebruik gemaakt van een door SURFnet voorgeschreven authenticatie en autorisatiemethode.

De filtereigenschappen **voor uitgaande mail** zijn (uitsluitend voor beheerders) via een webinterface te configureren. Het gaat hier bijvoorbeeld om het deblokkeren van gebruikers of configureren van whitelists.

De SURFmailfilterdienst beschikt over een uitvoerige real-time statistiek-, log- en rapportagefunctie. Hiermee is het mogelijk de statistieken van een (of meerdere) domeinen in te zien, maar bijvoorbeeld ook om daar periodiek rapportages van toegestuurd te krijgen per mail (PDF). Daarnaast geeft logging inzicht in de mail die is doorgelaten, geblokkeerd en getagged en welke rules hiervoor verantwoordelijk waren.

SURFmailfilter is bedoeld voor alle op SURFnet aangesloten instellingen die e-mail, bestemd voor (e-mailadressen) van een of meerdere van haar (sub)domeinen, door SURFnet wil laten controleren/filteren op ongewenste berichten, zoals virussen, phishing en spam, voordat deze mail wordt afgeleverd op haar eigen mailserver(s) of verstuurd via haar eigen mailserver(s). SURFmailfilter is beschikbaar voor IPv4 en IPv6.

Specifieke gebruikershandleidingen zijn te vinden via de knop “links SURFmailfilter” op het SURFnet dashboard: https://dashboard.surfnet.nl.

3.6 SLS en karakteristieken

De karakteristieken van deze dienst worden gepubliceerd via de SURFnet Service Level Specificatie. De meest recente versie van de SLS is te vinden op het adres:

http://www.surfnet.nl/diensten/sls/ . Rapportage over de karakteristieken van SURFmailfilter worden gepubliceerd op SURFdashboard. Inhoudelijke statistieken, logging en rapportage kunnen binnen de SURFmailfilterdienst worden ingezien (zoals beschreven in vorige paragraaf).

3.7 Aanvraag, wijziging, storing en tarieven

De SURFmailfilter dienst is exclusief beschikbaar voor SURFnet aangesloten instellingen. Voor onderwijsinstellingen geldt een tarief1 van 810, en voor niet-onderwijsinstellingen een tarief van 304 euro per maand exclusief btw.

Daarnaast dient de instelling SURFnet te vrijwaren. Dit kan direct bij de aanvraag van de dienst op SURFdashboard, of via de fax (zie Appendix A).

[1] Genoemde tarieven gelden per 1-1-2014

- Voor de **aanvraag of wijziging** van de SURFmailfilter dienst, kan een instelling terecht op het zelf-service portaal SURFnet dashboard, of bij de afdeling Account Advisering van SURFnet.
- Bij een **storing** dient de daarvoor bevoegde persoon binnen de instelling zich te melden bij de SURFnet helpdesk.

In de volgende tabel staan de contactgegevens:

Wanneer?	Door wie?	Contact	Tijden
Bij een aanvraag of wijziging	Instellings Contact Persoon (ICP)	https://dashboard.surfnet.nl SURFnet Account Advisering Tel. +31 30 2 305 305 E-mail: aa@surfnet.nl	Kantoor
Storing	Bevoegde helpdeskbellers	SURFnet Helpdesk Tel. 088 - SURFNET (088 - 7873 638) E-mail: helpdesk@surfnet.nl http://www.surf.nl/over-surf/contact/24-uurs-helpdesk/index.html	24 x 7

Appendix A: Vrijwaringverklaring

Bij aanmelding voor de dienst, dient de instelling met de volgende vrijwaring akkoord te gaan door middel van een akkoordverklaring op SURFdashboard, of door te ondertekenen en retour te sturen of faxen (030 – 2 305 329) naar SURFnet:

SURFnet biedt middels de dienst een e-mail-filterdienst aan voor de op SURFnet aangesloten instellingen. De dienst stelt instellingen in staat om al haar e-mailberichten te laten controleren danwel te filteren op virussen en spam *voordat* ze worden afgeleverd op de eigen mailserver of verstuurd via haar eigen mailserver(s). De instellingsbeheerder en eventueel de medewerkers en/of studenten indien geautoriseerd en geauthenticeerd door de instelling, kunnen zelf via een webinterface de filtereigenschappen aanpassen naar eigen inzicht.

De aangesloten instelling is zelf verantwoordelijk voor het gebruik van de dienst en de consequenties die dat met zich meebrengt voor de e-maildienstverlening aan haar gebruikers. De instelling is verantwoordelijk voor de voorlichting aan haar gebruikers en de eventuele instemming van haar gebruikers met deze dienst. De Instelling vrijwaart SURFnet voor alle mogelijke aanspraken van haar gebruikers, die betrekking hebben of in verband staan met deze dienst.

Ondergetekende* verklaart kennis te hebben genomen van deze bepalingen en hiermee in te stemmen.

Naam: **----------**

Instelling: **----------**

Functie: **----------**

Datum: **----------**

Handtekening: **----------**

(*) Deze verklaring dient te worden ondertekend door de aanvrager van de SURFmailfilter dienst van SURFnet. Aanvrager is Contractant, InstellingsContactPersoon of InstellingsCoördinator en bevoegd tot ondertekening van deze verklaring.