

HANDLEIDING

ANTI-VIRUS & ANTI-SPAM

VERSIE 2.0



PREMIUM ANTI-VIRUS & ANTI-SPAM (SAV)

Naast de standaard virusscanner en SPAM-filter kan NedStars u een premium oplossing aanbieden. Dit is een hoogwaardige en geavanceerdere scanner. Deze filter is in staat meer dan 98% van de SPAM succesvol te weren. Dit is de zwaarste beveiliging die er momenteel in de markt beschikbaar is: drie servers zorgen voor een zeer efficiënte filtering op basis van intelligente regels en zwarte lijsten met bekende spammers (wordt dagelijks geüpdate!).

WERKING FILTER

Als er een mail naar uw domein wordt gestuurd wordt deze allereerst afgeleverd op de server met het Premium Anti-Virus & Anti-SPAM Pack (verder SAV server genoemd). Deze SAV server voert diverse controles uit alvorens de mail naar de standaard mail server gaat.

STAP 1

De server is voorzien van een blacklist met servers die bekend staan om het versturen van SPAM. Een mail afkomstig van een server op de blacklist wordt geweigerd. Deze mail komt niet aan op de SAV server en de afzender krijgt een bouncemail alsof uw adres niet bestond. De status van de mail wordt dan ook **'REJECTED'** genoemd.

STAP 2

Als een mail niet geweigerd is, wordt deze gescand door de virusscanner. Deze verwijdert de eventuele aanwezige virussen of gevaarlijke bijlagen. Verwijderde bijlagen worden niet meer in de mail meegezonden, maar wel op de SAV server opgeslagen zodat uw beheerder deze alsnog kan downloaden.

STAP 3

De virusvrije mails worden vervolgens gescand door de SPAM-scanner. Deze wijst strafpunten aan de mails toe, gebaseerd op een set van meer dan 1000 intelligente regels. Bijvoorbeeld mails met veel erotische termen krijgen al snel veel strafpunten. Als een mail 9 strafpunten of meer heeft gekregen krijgt de mail de status **'HIGH SCORING SPAM'**. De mail wordt niet meer in uw mailbox afgeleverd. Als een mail 4 strafpunten of meer heeft kregen twijfelt de filter of het SPAM is of niet. De mail krijgt dan de status **'SPAM'** en de onderwerp regel wordt gemarkeerd met **{Spam?}**. De mail wordt vervolgens wel bij u afgeleverd. Als een mail minder dan 4 strafpunten heeft krijg het de status **'CLEAN'** en wordt het gewoon bij u afgeleverd.



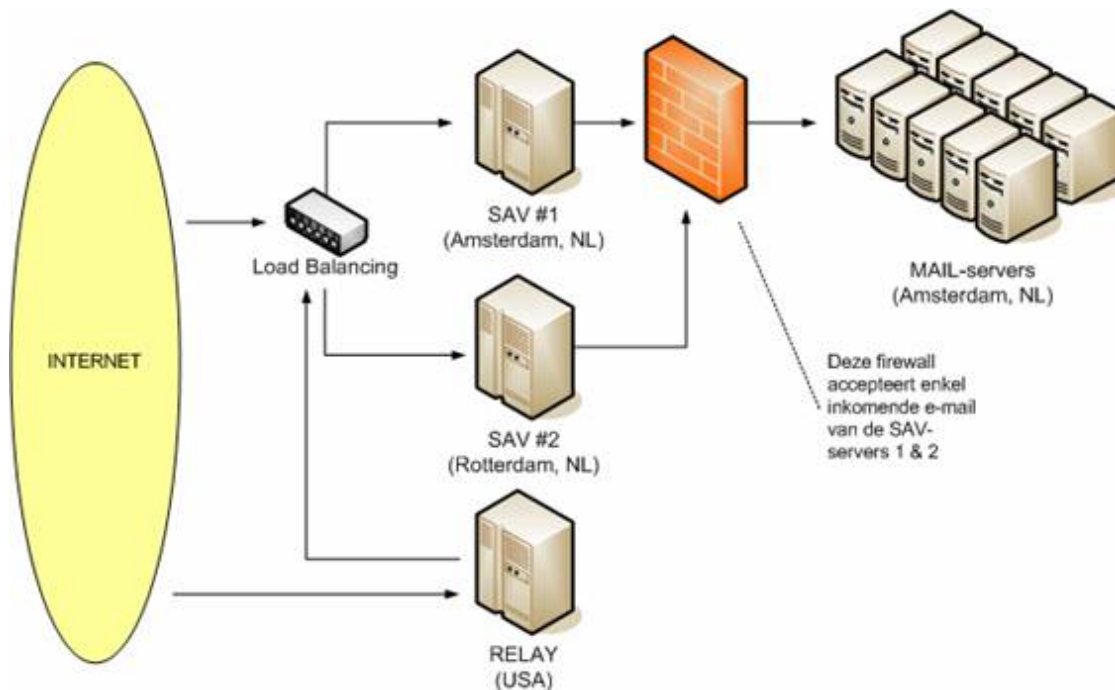
STAP 4

Als de SAV server klaar is met stap 1 tot en met 3 wordt de mail op de normale mailserver afgeleverd (bijvoorbeeld de Plesk server of uw eigen mail server). Daar zal de standaardscanner nog een extra controle doen, maar meestal geen nieuwe SPAM of virussen vinden. Als u de Premium scanner gebruikt kunt u dan ook de standaardscanner uitschakelen. Als de standaardscanner klaar is met scannen komt de mail in uw eigen mailbox terecht.

FAIL-OVER OPZET

Aan het netwerk zijn twee zeer hoogwaardige SAV (SPAM & Anti-Virus) servers toegevoegd die de filtering uitvoeren. Tussen deze twee servers vindt zogenaamde "Load Balancing" plaats, zodat de werklust over beiden servers wordt verdeeld. Nadat een e-mail is gescand en eventueel verwijderd of gemarkeerd (met {Spam?} of {Disarmed?} in het onderwerp) wordt het afgeleverd op het normale netwerk.

Aan het netwerk is tevens een server in de Verenigde Staten toegevoegd. Mocht het netwerk in Amsterdam én in Rotterdam uitvallen, dan kunnen we automatisch uitwijken naar de Verenigde Staten. De opzet is volledig redundant. Ook in het geval dat er problemen zijn op de normale mail server dan worden de mails op de SAV servers vastgehouden voor 30 dagen lang totdat uw mailbox weer bereikbaar is. Op deze manier kunnen wij gemakkelijk een mail up-time van ruim 99,99% garanderen!



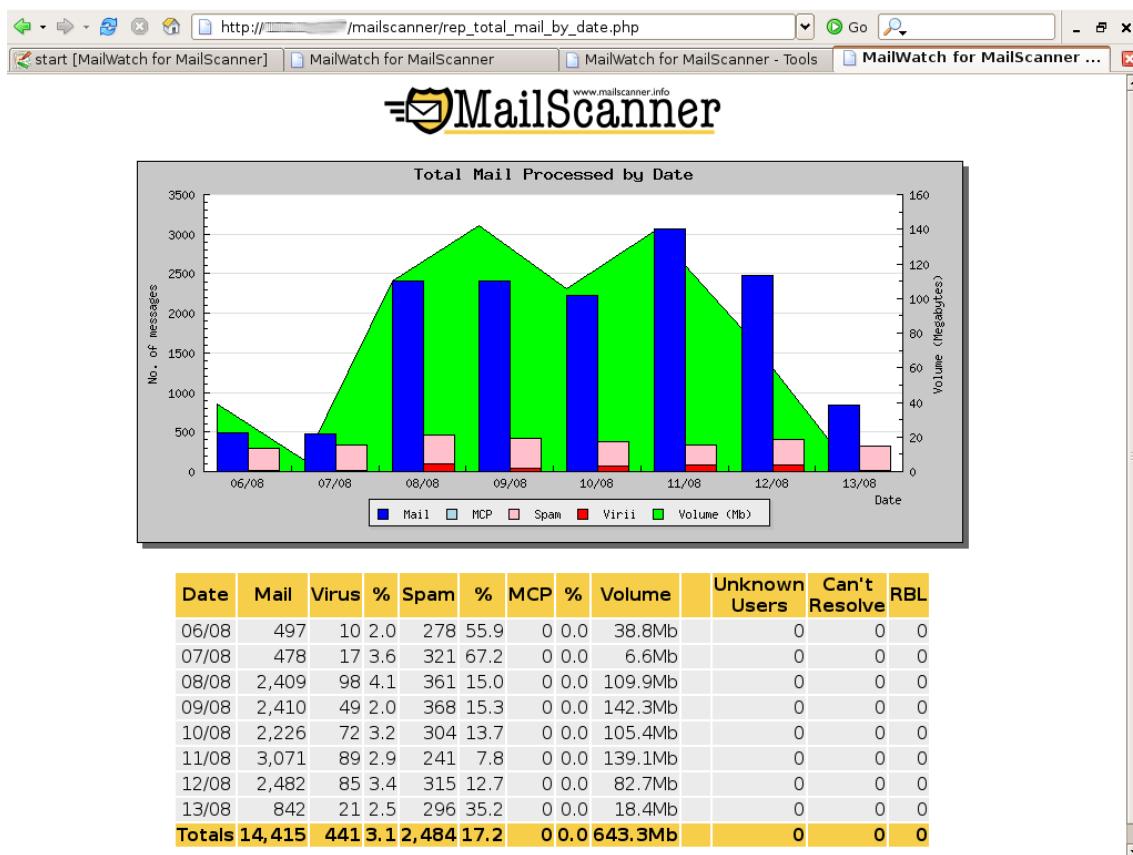
FILTER ACTIVEREN OF DEACTIVEREN

Indien u het pakket wenst de activeren of deactiveren kan NedStars dit voor u uitvoeren. Neem hiervoor contact met ons op. Voor een geactiveerd pakket worden jaarlijks kosten in rekening gebracht. Gebruikers van een webhosting- of Hosted Exchange oplossing van NedStars kunnen deze dienst gratis gebruiken.

FILTER CONFIGUREREN / STATISTIEKEN

Bij de Premium Scanner mag u gratis gebruik maken van het programma 'MailWatch' van NedStars. Hier kunt u als beheerder diverse informatie raadplegen:

- Alle mails tot 14 dagen terug die naar uw domein zijn verstuurd bekijken of downloaden
- Statistieken inzien hoeveel SPAM en/of virussen er zijn verwijderd
- Diverse grafieken genereren met statistieken inzake uw mailgebruik (zie ook onderstaand voorbeeld)
- Verwijderde bijlagen bekijken of downloaden
- De SPAM filter persoonlijk configureren



INLOGGEN

Ga naar <http://sav1.nedstars.nl/mailscanner> en meld u zich hier aan met de inloggegevens voor de Premium Scanner die u van NedStars hebt gekregen.

The screenshot shows the MailWatch for MailScanner web interface. At the top, there is a navigation menu with options: Recent Messages, Lists, Quarantine, Reports, Tools/Links, Documentation, and Logout. Below the menu is a table titled "Last 50 Messages (Refreshing every 30 seconds)". The table has the following columns: #, Date/Time, From, To, Subject, Size, SA Score, and Status. The messages listed are all marked as "Spam".

#	Date/Time	From	To	Subject	Size	SA Score	Status
1	13/08/05 16:32:40	[Redacted]	[Redacted]	Full-color business cards are no charge	7.8Kb	16.68	Spam
2	13/08/05 16:32:39	[Redacted]	[Redacted]	Kim, Diapers for 1 year on us	6Kb	13.77	Spam
3	13/08/05 16:32:39	[Redacted]	[Redacted]	Stan, Diapers for 1 year on us	6.1Kb	13.77	Spam
4	13/08/05 16:32:38	[Redacted]	[Redacted]	08/13/05 Luxury property in Costa Rica	3.6Kb	7.45	Spam
5	13/08/05 16:32:38	[Redacted]	[Redacted]	Find out how Sirius Satellite Radio could be yours free!	5.6Kb	23.51	Spam
6	13/08/05 16:32:38	[Redacted]	[Redacted]	Slim Amateur Giving Blowjob In Toilet Hardcore	1.2Kb	21.01	Spam
7	13/08/05 16:32:23	[Redacted]	[Redacted]	Find out more information on 1031 exchanges.	3.3Kb	18.20	Spam
8	13/08/05 16:32:18	[Redacted]	[Redacted]	Register today and \$25 Gift Card Is Yours...	2.7Kb	14.98	Spam
9	13/08/05 16:32:18	[Redacted]	[Redacted]	Find out how Sirius Satellite Radio could be yours free!	5.6Kb	23.51	Spam
10	13/08/05 16:32:13	[Redacted]	[Redacted]	You could be the next winner! Win a Mustang GT!	2Kb	15.68	Spam
11	13/08/05 16:32:10	[Redacted]	[Redacted]	Get 3000 Bucks Tomorrow - Without Any Hassle	5.6Kb	18.41	Spam
12	13/08/05 16:32:04	[Redacted]	[Redacted]	Refi or Buy a Home, there's still time	5.8Kb	11.98	Spam

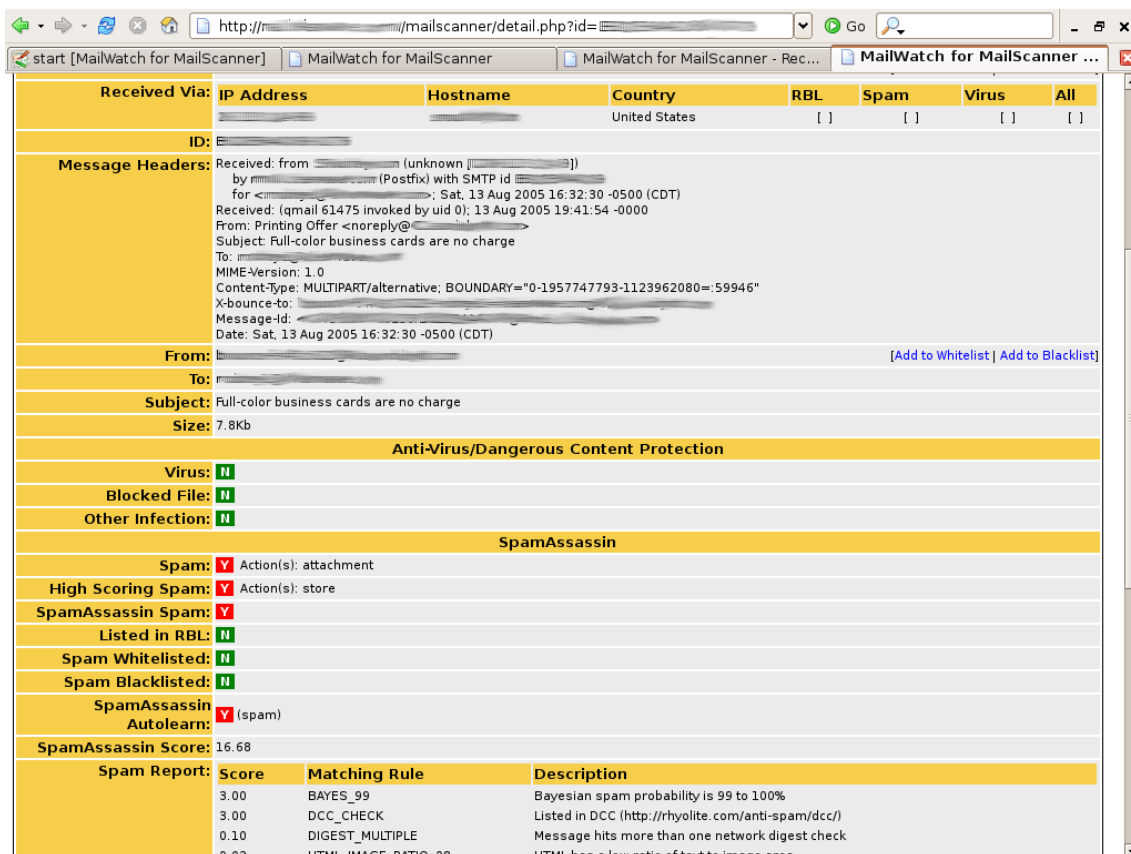
Summary panels on the right side of the interface:

- Color Codes:** Bad Content/Infected (Red), Spam (Pink), High Spam (Light Pink), MCP (Light Blue), High MCP (Blue), Whitelisted (Green), Blacklisted (Black), Clean (White).
- Status:** MailScanner: YES (10 children), Postfix: YES (1 procs), Load Average: 1.07 0.99 0.99. Mail Queues: Inbound: 0, Outbound: 0.
- Today's Totals:** Processed: 22,218 (216.5Mb), Clean: 2,830 (12.7%), Viruses: 33 (0.1%), Top Virus: Worm.Bagle.BB-gen, Blocked files: 0 (0.0%), Others: 0 (0.0%), Spam: 2,037 (9.2%), High Scoring Spam: 17,318 (77.9%), MCP: 0 (0.0%), High Scoring MCP: 0 (0.0%).



MAILOVERZICHT

U komt na het inloggen op een pagina waar u diverse statistieken (rechtsboven) kunt zien en waar u de laatste 30 mails ziet staan die aan uw domein zijn verstuurd. U ziet hier ook welke status de mail heeft gekregen (o.a. HIGH SCORING SPAM, SPAM of CLEAN). Merk dus op dat REJECTED mail niet in deze lijst voorkomt! Door op het vierkantje [] helemaal links te klikken kunt u een mail openen en ziet u de headers en diverse informatie van de SAV server (o.a. technische details hoe de strafpunten tot stand zijn gekomen). Onderaan deze pagina met headers vind u ook een link waar u het betreffende mailtje kunt lezen (incl. bijlagen). Zie ook onderstaande afbeelding.



The screenshot shows a web browser window with the URL `http://mailscanner/detail.php?id=...`. The page content is as follows:

Received Via:	IP Address	Hostname	Country	RBL	Spam	Virus	All
			United States	[]	[]	[]	[]

Message Headers:

```

Received: from [redacted] (unknown [redacted])
  by [redacted] (Postfix) with SMTP id [redacted]
  for [redacted] <[redacted]>, Sat, 13 Aug 2005 16:32:30 -0500 (CDT)
Received: (qmail 61475 invoked by uid 0); 13 Aug 2005 19:41:54 -0000
From: Printing Offer <noreply@[redacted]>
Subject: Full-color business cards are no charge
To: [redacted]
MIME-Version: 1.0
Content-Type: MULTIPART/alternative; BOUNDARY="0-1957747793-1123962080=-59946"
X-bounce-to: [redacted]
Message-Id: [redacted]
Date: Sat, 13 Aug 2005 16:32:30 -0500 (CDT)
  
```

From: [redacted] [\[Add to Whitelist\]](#) [\[Add to Blacklist\]](#)

To: [redacted]

Subject: Full-color business cards are no charge

Size: 7.8Kb

Anti-Virus/Dangerous Content Protection

Virus: N

Blocked File: N

Other Infection: N

SpamAssassin

Spam: Action(s): attachment

High Scoring Spam: Action(s): store

SpamAssassin Spam: Y

Listed in RBL: N

Spam Whitelisted: N

Spam Blacklisted: N

SpamAssassin Autolearn: Y (spam)

SpamAssassin Score: 16.68

Spam Report:	Score	Matching Rule	Description
	3.00	BAYES_99	Bayesian spam probability is 99 to 100%
	3.00	DCC_CHECK	Listed in DCC (http://rhyolite.com/anti-spam/dcc/)
	0.10	DIGEST_MULTIPLE	Message hits more than one network digest check
	0.03	HTML_IMAGE_RATIO_08	HTML has a low ratio of text to image area

WACHTWOORD WIJZIGEN / SPAM-FILTER CONFIGUREREN

Bij Tools/Links en dan User Management kunt u uw wachtwoord wijzigen. U kunt hier ook de vereiste scores veranderen hoe SPAM gemarkeerd wordt. Standaard is de SPAM score 4 en de HIGH SPAM score 9. Zie ook het onderdeel 'werking filter'. Als u nul invult, wordt de standaardwaarde van NedStars gebruikt.



OVERIGE FUNCTIONALITEITEN

Het MailWatch systeem biedt diverse mogelijkheden voor statistieken, rapportage en geavanceerde instellingen. Dit is bedoeld voor gevorderde gebruikers bekend met het MailWatch systeem.

